Денис Колисниченко

Беспроводная СЕТЬ

дома и в офисе

Санкт-Петербург

«БХВ-Петербург»

2009

УДК 681.3.06
ББК 32.973.26-018.2
К60

Колисниченко Д. Н.

К60 Беспроводная сеть дома и в офисе. — СПб.: БХВ-Петербург, 2009. — 480 с.: ил. — (Самоучитель)

ISBN 978-5-9775-0427-0

Книга поможет начинающему администратору домашней или офисной сети в кратчайшие сроки развернуть, настроить или модернизировать беспроводную сеть. Кратко изложены основы компьютерных сетей. Описаны беспроводные сети стандартов 802.11a, 802.11b, 802.11g, а также новейшего стандарта 802.11n. На практических примерах показано построение сети Wi-Fi, GPRS-соединение с Интернетом, а также объединение проводной и беспроводной сети Ethernet, реализация совместного доступа к Интернету, дан обзор технологии Power Line Communication (Интернет "из розетки"). Рассмотрены вопросы защиты с помощью антивирусов, брандмауэров, и на основе технологии виртуальных частных сетей даны рекомендации по повышению производительности сети. Все настройки приведены для операционных систем Windows XP, Vista и Linux.

Для опытных пользователей и начинающих 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*
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 30.03.09.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 38,7.
Тираж 2000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.60.953.Д.003650.04.08 от 14.04.2008 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 978-5-9775-0427-0

Оглавление

Введение

Эта книга посвящена построению сети для дома и офиса. С одной стороны, построение сети — занятие не очень сложное и под силу пользователю средней квалификации. С другой стороны, есть определенные нюансы, разобраться в которых мы здесь и постараемся. Приведу простейший пример. С удешевлением беспроводных технологий вы решили, что ваша сеть будет беспроводной. Правильно: зачем тянуть кабели, обжимать витую пару, если можно купить точку доступа, включить ее — и сеть готова. Казалось бы, ничего сложного в этом нет. Однако пользователь, создавший сеть таким вот способом, обнаружит, что его сеть или вообще не работает, или работает медленно, или доступ к ней получил кто-то посторонний. В первом случае причина, скорее всего, в неправильной настройке точки доступа. Во втором — в интерференции сигналов. В третьем — в пренебрежении основными правилами безопасности. Какими правилами? Что такое интерференция сигналов? Как правильно настроить точку доступа? Обо всем этом вы здесь и узнаете.

- В *первой части* книги мы рассмотрим сугубо теоретические вопросы. Вы познакомитесь с краткой историей и классификацией сетей, с основными сетевыми устройствами и так называемой *моделью взаимодействия открытых систем* (Open System Interconnection, OSI) — базовым сетевым стандартом. Настоятельно рекомендую вам не пропустить *главу 3*, в которой модель OSI подробно описана, — в последующих главах книги мы не раз будем к ней обращаться.
- Во *второй части* мы поговорим о подключении к уже существующей сети. Поскольку я более чем уверен, что у вас именно беспроводная сеть (ну, или смешанная, где есть как беспроводные, так и проводные подключения), то эта часть книги начинается именно с рассмотрения подключения к беспроводной сети. Затем мы рассмотрим подключение к сети Ethernet, а после него — подключение к Интернету в Windows и Linux. Отдельная глава посвящена GPRS-подключению — одному из вариантов беспроводного подключения к Интернету.

- *Третья часть* книги посвящена построению Ethernet-сети. Ведь ни для кого не секрет, что абсолютно беспроводные сети — редкость (если не считать ad hoc-сети или сети из одной точки доступа и одного-двух компьютеров). Чаще всего в современной сети есть как беспроводные, так и проводные клиенты. И построение такой смешанной сети принято начинать с проводной части, а уже потом "прикручивать" точку доступа — как правило, беспроводная сеть является расширением существующей проводной сети. Особое внимание здесь будет уделено предоставлению общего сетевого доступа к файлам и принтерам, а также общему доступу к Интернету (*главы 11* и *12* соответственно). Чтобы не усложнять изложение, мы рассмотрим монтаж домашней и офисной сети небольшого и среднего размеров, а построение огромных корпоративных сетей оставим "за скобками".
- В *четвертой части* мы поговорим о построении собственной беспроводной сети (наконец-то!). Мы рассмотрим основные теоретические принципы (как именно данные передаются "по воздуху"), разберемся с беспроводными стандартами, поговорим о выборе оборудования и, конечно же, построим собственную беспроводную сеть. Отдельное внимание будет уделено решению проблем, возникающих при настройке беспроводной сети.
- Защита вашей сети — довольно ответственное занятие, поэтому ей посвящена *пятая часть* книги. Мы поговорим о том, как можно защитить беспроводную сеть в целом и конкретно маршрутизатор в частности, рассмотрим использование виртуальной частной сети (VPN) для защиты информации, а также разберемся с выбором брандмауэра и антивируса (все антивирусы хороши, но есть и лучшие).
- Последняя, *шестая*, часть книги посвящена повышению производительности нашей сети. Здесь кроме модернизации старой сети будет рассмотрена также установка серверов, позволяющих повысить производительность сети в целом.

Ну, а теперь можно приступить к чтению книги.

Часть I

Основы построения сети

В первой части книги мы рассмотрим краткую историю сетей, модель взаимодействия OSI и разберемся, для чего предназначены основные сетевые устройства.

Глава 1

Классификация сетей

1.1. Краткая история сетей

С появлением первых электронно-вычислительных машин (не персональных компьютеров, а именно первых огромных вычислительных машин, которые занимали целые комнаты) возникла проблема переноса данных между ними. С того момента было создано много различных сетей. Сейчас мы вкратце рассмотрим историю сетей, чтобы вы знали, откуда они появились, а потом попробуем классифицировать все имеющиеся виды сетей.

1.1.1. 1941–1975 годы

Первый период развития вычислительных сетей начинается в 1941 году (тогда, если вы помните, появилась первая "большая" ЭВМ) и называется *лабораторным* — в то время сети, как впрочем и ЭВМ, не выходили за пределы лабораторий научных институтов. Казалось бы, как давно это было! Но самое интересное, что мы до сих пор используем решения, разработанные в то время. Последовательный интерфейс RS-232C и параллельный интерфейс Centronics (да, тот, который служит для подключения принтеров) используются до сих пор. Интерфейс RS-232C постепенно вытесняется современными последовательными интерфейсами: USB и IEEE 1394 (FireWire), и на некоторых современных компьютерах его больше нет вообще. Однако интерфейс Centronics имеется на каждом современном стационарном компьютере, хотя большинство производителей принтеров уже практически перешло на USB. Наличие "старых" интерфейсов зависит только от производителя материнской платы — как он решит, так и будет. Мой компьютер, на котором я пишу эти строки, был куплен в феврале 2008 года. Тогда я не обратил внимания на наличие/отсутствие старых интерфейсов, но потом выяснилось, что на материнской плате отсутствует RS-232C, но есть Centronics, а также USB, IEEE 1394, HDMI (правда, он не имеет никакого отношения к сетевым интерфейсам)

и другие современные разъемы, которых не было на более старых компьютерах. С другой стороны, в продаже до сих пор имеются материнские платы с RS-232C, а также предлагаются отдельные PCI-контроллеры, добавляющие два порта RS-232C, если в них возникает острая необходимость.

Интерфейсы RS-232C и Centronics — это, в принципе, хорошо, но они годятся только для связи "точка–точка", то есть для непосредственной связи отправителя и получателя данных. Понятно, что в сети может быть ЭВМ гораздо больше чем две, поэтому разработчики сетей на этом не остановились. С самого начала ставилась задача объединения в сеть ЭВМ без привязки к конкретной аппаратуре.

В 1974 году компания IBM представила универсальную архитектуру вычислительных сетей: SNA (System Network Architecture). Эта архитектура, помимо всего прочего, поддерживала *адресацию узлов* сети, смысл которой в том, что каждому узлу сети присваивается уникальный адрес, по которому можно обратиться к этому узлу. Сейчас для адресации узлов преимущественно используются протоколы IPv4 и IPv6, о которых мы поговорим в *главе 3*.

1.1.2. 1976–1982 годы

Второй период развития сетей начался в 1976 году, когда сети вышли за пределы лабораторий и начали активно разрабатываться сетевые архитектуры и технологии передачи данных. Тогда и появилось семейство протоколов X.25 — протоколов передачи данных в системах с коммутацией пакетов. Разработка протоколов X.25 стала очень важным событием, поскольку до появления Интернета они были единственными протоколами, используемыми для создания глобальных сетей, — именно X.25-сети связывали весь мир в единое целое. Далее на базе X.25 был создан протокол Frame Relay, а на его базе — технология ATM. Подробно рассматривать все производные протоколов X.25 мы не будем, поскольку нас сейчас интересуют только ключевые события в развитии сетей (описание истории появления каждого сетевого протокола займет целую книгу, прочитать которую у вас не хватит терпения). Отмечу только, что Frame Relay, как и ATM, здравствуют и по сей день.

В 1979 году был создан первый модем для персональных (!) компьютеров. Я даже догадываюсь о чем вы сейчас подумали: какие, мол, персональные компьютеры в 1979 году? Какой модем? Да, Personal Computer (PC) от IBM появился в 1981 году, но это не означает, что до этого не было *персональных компьютеров*. Персональный компьютер — это компьютер, предназначенный только для одного человека, для одного пользователя. Для работы с первыми ЭВМ обычно требовался целый штат специалистов, а настоящие персональные компьютеры появились еще до 1980 года — это были компью-

теры компании Apple. А то, что появилось в 1981 году, — всего лишь название продукта компании IBM. Конечно, IBM первая ввела термин PC (Personal Computer), и с того времени все компьютеры со сходной архитектурой команд считаются PC-совместимыми.

А все современные модемы являются Hayes AT-совместимыми. AT — это набор команд управления модемом, разработанный компанией Hayes. Несложно догадаться, что в 1979 году первый модем был разработан именно компанией Hayes. Он назывался Micromodem II и развивал скорость в 300 бод (бит/с). Этот модем и был предназначен для компьютеров Apple.

Еще в лабораторном периоде были разработаны *системы с произвольным доступом*. Впервые они были использованы в начале 1970-х годов в сети Alohanet, объединяющей Гавайские острова. Сначала эти системы считались бесперспективными, но в мае 1973 года Боб Меткалф (Bob Metcalf) усовершенствовал метод CSMA, на котором они были основаны. Усовершенствованный метод назвали CSMA/CD (Carrier-Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением коллизий). Боб Меткалф планировал использовать этот метод для совместного доступа к сетевым принтерам, но он позже "перерос" в то, что сейчас называется Ethernet-сетью. Тогда сеть CSMA/CD передавала данные по коаксиальному кабелю (как первые Ethernet-сети) со скоростью 2,94 Мбит/с (для того времени это была значительная скорость), а максимальное расстояние передачи данных составляло 1,5 км. В 1978 году Меткалф зарегистрировал копанию 3Com Corporation (наверное, все мы слышали название этой компании), а в 1982 году выпустил первый в мире серийный Ethernet-адаптер для компьютера Apple.

В 1979 году произошло еще одно важное событие — был организован альянс DIX (DEC, Intel, Xerox), результатом деятельности которого стала в 1980 году разработка стандарта Ethernet.

В 1980 году была разработана *модель взаимосвязи открытых систем* (Open System Interconnect, OSI), которую мы подробно рассмотрим в *главе 3*. Эта модель четко определяет семь уровней, которые обеспечивают передачу данных по сети. Модель OSI сугубо теоретическая, но она лежит в основе всех современных сетей.

1.1.3. 1983–1989 годы

Начиная с 1983 года, в институтах и даже некоторых офисах стали появляться первые локальные сети, связывающие компьютеры толстым коаксиальным кабелем. В то время сетевой адаптер стоил очень дорого (например,

для ЭВМ VAX стоимость сетевого адаптера превышала 3 тыс. долларов), поэтому локальную сеть могли себе позволить только самые крупные фирмы. Найти тогда "персоналку" с сетевым адаптером было сложно.

В 1985 году Институтом инженеров по электротехнике и электронике (IEEE) был прият стандарт IEEE 802.3 (10Base-5) — Ethernet-сеть на "толстом" коаксиальном кабеле. В 1989 году был принят стандарт IEEE 802.3a (10Base-2), предусматривающий передачу данных по "тонкому" коаксиальному кабелю. Подробно о стандартах Ethernet мы поговорим чуть позже в этой книге.

Понятно, что Ethernet-сети — не единственный вид локальной сети. В 1988 году IBM превзошла стандарт Ethernet, представив технологию Token Ring с максимальной скоростью передачи данных в 16 Мбит/с (Ethernet предусматривал передачу данных с максимальной скоростью в 10 Мбит/с).

В 1985 году компания StrataCom начала эксплуатацию первых линий T1 со скоростью передачи данных 1,54 Мбит/с. Чуть позже линии T1 стали доступны крупным компаниям и использовались в качестве магистралей для быстрой передачи данных на большие расстояния.

Индивидуальным пользователям в 1980-х годах сети "особо не светили", поскольку сетевое оборудование продолжало стоить весьма дорого. Так, в 1989 году компания Arc Electronics представила высокоскоростной модем (19,2 Кбит/с) стоимостью "всего" 3595 долларов. Интересно, что этот модем был относительно дешевле модемов других производителей, которые, к тому же, не обеспечивали достигаемой им скорости.

Кто мог позволить себе сети ISDN, радовался скорости передачи данных в 128 Кбит/с (сети ISDN BRI) или 1,54 Мбит/с (ISDN PRI). О цене говорить не будем — ISDN-сети стоили неприлично дорого.

Технологии — это, конечно, хорошо. Но сетевые адаптеры и прочее сетевое оборудование без программного обеспечения — просто железки. Чтобы компьютер мог работать в сети, нужна сетевая операционная система. В 1980-х годах сеть поддерживали следующие ОС: UNIX (и ее вариации), Novell Netware, Microsoft LAN Manager (оболочка для OS/2, появившаяся в 1987 году).

В 80-х годах прошлого века появились и первые сотовые сети — да, сотовая телефония! Первая система сотовой телефонной связи Nordic Mobile Telephone System (кто помнит — первые "мобилки", появившиеся у нас в 1990-х годах, поддерживали стандарт NMT) была запущена в Дании, Швеции, Финляндии и Норвегии в 1981 (!) году. В 1983 году заработали две сотовые сети в Северной Америке: AURORA-400 и AMPS.

1.1.4. 1990–1995 годы

В 1990 году произошел очередной "переворот" в Ethernet-сетях — был принят стандарт IEEE 802.3i (10Base-T), предусматривающий передачу данных по витой паре 3-й категории со скоростью 10 Мбит/с. Переворот заключался в том, что Ethernet-сети стали:

- *надежнее* — при использовании коаксиального кабеля все компьютеры подключались к общему кабелю, и если этот кабель обрывался, то вся сеть "падала". В случае с витой парой все компьютеры сети подключаются к центральному устройству сети — Ethernet-концентратору. Если происходит обрыв кабеля, ведущего к какому-нибудь узлу сети, этот узел исчезает из сети, но вся сеть продолжает работать;
- *проще в установке* — монтаж витой пары намного проще, чем коаксиального кабеля, особенно, если речь идет о "толстом" коаксиальном кабеле.

Позднее был принят стандарт IEEE 802.1D, в котором было определено понятие *моста* (bridge), и Ethernet-сети наконец-то стало можно делить на сегменты для локализации трафика. Сегментация сети особо важна для крупных сетей — ведь чем больше узлов, тем меньше производительность сети.

Через три года сети того времени стали напоминать уже современные сети — в них активно начали использоваться концентраторы и мосты, появились первые коммутаторы и двухуровневые сети. В двухуровневых сетях компьютеры одной рабочей группы (одного отдела компании) объединялись между собой концентратором, а сами рабочие группы (то есть концентраторы рабочих групп) подключались через мосты к общей корпоративной магистрали. В качестве магистрали обычно использовалось оптоволокно (стандарт 10Base-FL или IEEE 802.3j, принятый в 1993 году). С появлением 10Base-FL на оптоволокне Ethernet-сети выходят за пределы зданий и становятся средством для создания "кампусных" сетей. То есть если раньше Ethernet-сети использовались только для создания локальных сетей, то в 1994–1995 годах стандарт 10Base-FL применялся для связи локальных сетей, находящихся в разных зданиях.

Следующим шагом в создании корпоративных сетей стало изобретение многопортового устройства — центрального коммутатора, в котором были объединены все мосты сети. Такая конфигурация получила название collapsed-backbone ("магистраль в точке"). Примерно в это же время родилось понятие *структурированных кабельных сетей* (СКС).

Понятно, что сети росли и что скорости 10 Мбит/с для магистрали стало недостаточно. На тот момент существовала всего одна "быстрая" технология, обеспечивающая передачу данных по оптоволоконному кабелю со скоростью

100 Мбит/с — FDDI (Fiber Distributed Data Interface — распределенный волоконный интерфейс данных). Но в 1992 году компания Grand Junction начала разработку Ethernet-сети, работающей на скорости 100 Мбит/с, и она была стандартизирована в 1995 году (стандарт IEEE 802.3u, сети 100Base-TX, 100Base-T4 и 100Base-FX). В том же 1995 году компания Grand Junction была поглощена компанией Cisco Systems: закон выживания — выживают лишь сильнейшие. После принятия стандартов 100Base-* спрос на технологию FDDI резко пошел вниз, поскольку Ethernet-сети обеспечивали ту же скорость передачи данных, но стоили намного дешевле только за счет среды передачи данных — витая пара стоит намного дешевле, чем оптоволокно. А в 1998 году появились Ethernet-сети, передающие данные со скоростью 1 Гбит/с, но об этом позже.

А что же происходило в мире глобальных сетей? В 1990 году компания US Sprint начала предоставлять услуги объединения точек через Frame Relay по всей территории США. Тогда почти все высокоскоростные магистрали переводились на технологию ATM, но для подключения клиентов использовался Frame Relay. Однако в 1994 году компания Bell Atlantic начинает предлагать подключение клиентов по технологии ATM.

Не стоит забывать и об операционных системах. В 1993 году появилась первая действительно сетевая ОС от Microsoft — Windows NT, а в 1995 году — нашумевшая ОС Windows 95.

1.1.5. 1996–1999 годы

В эти годы ничего революционного в магистральных каналах связи не случилось, если не считать появления сервисов гарантирования качества обслуживания (QoS, Quality of Service). Но нас интересуют технологии, более близкие к пользователю. Можно сказать, что в эти годы (1995–1999) завершилась эра развития аналоговых модемов. В 1998 году был принят стандарт V.90, который используется и по сей день (если не считать его небольшого усовершенствования V.92, появившегося в 2000 году). Судя по всему, телефонные модемы отжили свое. Сегодня все больше и больше провайдеров предоставляют высокоскоростной доступ к Интернету, а обычные аналоговые модемы практически уже не используются.

Зарождение высокоскоростного доступа произошло как раз в 1995–1999 годах, когда появились первые кабельные и ADSL-модемы. Кабельные модемы (они передают данные по сетям операторов кабельного телевидения) преимущественно применялись в США. В Европе получили большее распространение ADSL-модемы, использующие для передачи данных обычный

телефонный кабель. К сожалению, в те годы в России о таких модемах только слышали, но никто их практически не видел.

В мире локальных сетей в 1998 году появилась технология 1000Base-X, передающая данные со скоростью 1 Гбит/с по оптоволокну, а в 1999 году — технология 1000Base-T, передающая данные со скоростью 1 Гбит/с по витой паре.

1.1.6. 2000 — наше время

Понятно, что развитие сетей не останавливается, а только начинается. Все еще впереди. Лет через десять все современные технологии будут казаться нам такими же "древними", какими сейчас кажутся решения 20-летней давности.

Из интересного в мире Ethernet можно отметить появление в 2003 году технологий передачи данных со скоростью 10 Гбит/с (10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-SW, 10GBase-LW, 10GBase-EW) и технологии PLC, обеспечивающей передачу данных по сети электропитания. В 2003 году это казалось странным, но сейчас — вполне нормально.

Если вы заметили, то в этой краткой истории практически ничего не было сказано о развитии беспроводных сетей. Это сделано умышлено. В *главе 9* мы поговорим о том, как данные передаются "по воздуху", рассмотрим краткую историю беспроводных сетей и существующие беспроводные стандарты.

1.2. Классификация сетей

Сети можно классифицировать по:

- занимаемой территории;
- топологии;
- ведомственной принадлежности;
- скорости передачи данных;
- типу среды передачи данных;
- организации взаимодействия компьютеров.

1.2.1. По занимаемой территории

По занимаемой территории сети могут быть локальными, региональными (они же муниципальные сети) и глобальными:

- *локальные* (LAN, Local Area Network) — сети, занимающие небольшую территорию, например, одну комнату или одно здание;

- *региональные* (MAN, Metropolitan Area Network) — сети, охватывающие город (отсюда другое название — муниципальные) или даже область;
- *глобальные* (WAN, Wide Area Network) — такие сети охватывают территории одного или нескольких государств или даже весь мир. Пример всемирной сети — Интернет.

С локальными и глобальными сетями все понятно, разберемся с сетями региональными. Сеть MAN, как правило, объединяет несколько сетей — например, MAN может объединять в единое целое сети двух или более зданий. При этом среда передачи данных сети MAN может как проводной, так и беспроводной. Беспроводная сеть обходится намного дешевле, чем сеть на базе оптоволокна, но она менее надежна и менее безопасна.

Беспроводные технологии очень полезны для MAN — не всегда есть возможность проложить кабель. С другой стороны, MAN часто выступает в качестве магистральной сети, поэтому производительности беспроводной сети может быть недостаточно.

Сейчас особой необходимости в MAN-сетях нет, поскольку можно организовать *виртуальную частную сеть* (VPN, Virtual Private Network), использующую каналы Интернета для передачи данных. Представим следующую ситуацию: есть организация, главный офис которой находится в Москве, затем эта компания открыла свой филиал в Санкт-Петербурге. Как объединить сети офисов вместе? Вы только представьте себе, сколько кабеля для этого понадобится! Причем витой парой здесь не отделаешься, придется использовать дорогой оптоволоконный кабель — ведь расстояние-то большое. Беспроводные технологии тоже из-за расстояния отпадают. Остается только одно — использовать для передачи данных каналы Интернета. Сеть каждого офиса подключается к Интернету через каналы местного интернет-провайдера, и через Интернет создается виртуальная частная сеть. И дешево, и быстро — ведь высокоскоростное подключение к Интернету в настоящее время вполне доступно. Понятно, что данные будут передаваться по незащищенным каналам, поэтому в виртуальной частной сети используется шифрование всех передаваемых данных. Механизмы VPN позволяют не только объединить две разные сети в единое целое, но и обеспечить безопасность передаваемых данных.

1.2.2. По топологии

Существуют следующие топологии сети:

- *линейная* (рис. 1.1) — подключение по принципу гирлянды: каждый узел сети подключается к следующему узлу сети. В такой сети от узла с номе-

ром 1 до узла *N* будет всегда одинаковый маршрут: через узлы 2, 3, 4, …, *N* – 1. Понятно, в случае отказа одного из узлов сети, линейная сеть прекратит свое существование. В настоящее время линейные сети практически не используются (если не принимать во внимание нуль-модемное соединение);

- *кольцевая* (рис. 1.2) — каждый узел сети соединен с двумя соседними узлами, все узлы сети образуют кольцо. Кольцевая топология используется технологиями Token Ring, FDDI и некоторыми другими;
- *звездообразная* (рис. 1.3) — в такой сети есть один центральный узел, с которым связан каждый узел сети. Такие сети еще называются *централизованными*. "Падение" центрального узла означает "падение" всей сети. Обычно в качестве центрального узла используется концентратор (hub) или коммутатор (switch). Пример звездообразной сети — Ethernet на базе витой пары;
- *общая шина* (рис. 1.4) — все узлы сети подключаются к единой среде передачи данных, например, к коаксиальному кабелю. Слабое место такой сети — сама среда передачи данных: обрыв кабеля означает сбой всей сети. Пример сети на общей шине — Ethernet на базе коаксиала;
- *древовидная* (рис. 1.5) — топологию этой сети проще представить, чем описать или вникать в определение. В древовидной сети есть более двух конечных узлов и, по крайней мере, два промежуточных узла. В древовидной сети между двумя узлами есть только один путь. Чтобы вникнуть в правильное определение древовидной сети, нужно знать теорию графов, поскольку древовидная сеть — это неориентированный ациклический граф, не содержащий замкнутых путей и позволяющий соединить единственным образом пару узлов;
- *ячеистая* (рис. 1.6) — в такой сети есть, по крайней мере, два узла, имеющих два или более пути между ними;
- *полносвязная* (рис. 1.7) — сеть, в которой есть связь между любыми двумя узлами. Это самая надежная топология сети, но она практически никогда не используется, поскольку является самой дорогой и труднообслуживаемой.

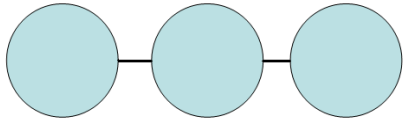


Рис. 1.1. Линейная топология

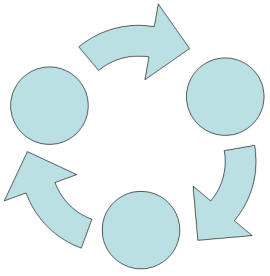


Рис. 1.2. Кольцевая топология

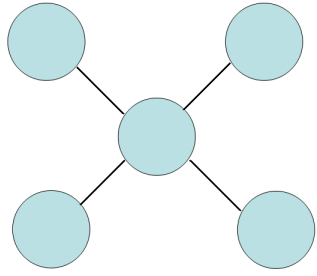


Рис. 1.3. Звезда

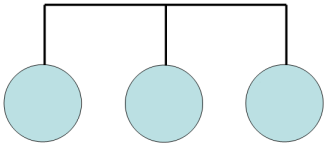


Рис. 1.4. Общая шина

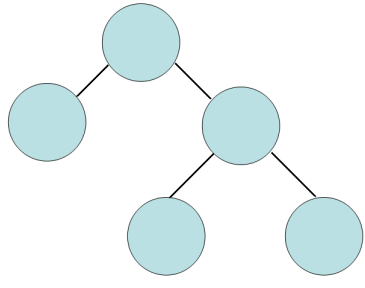


Рис. 1.5. Древовидная топология

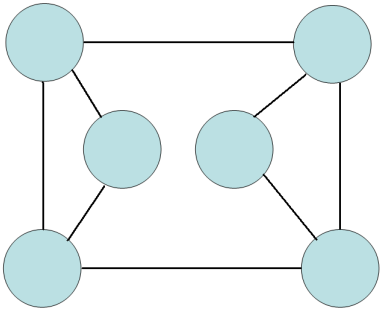


Рис. 1.6. Ячеистая топология

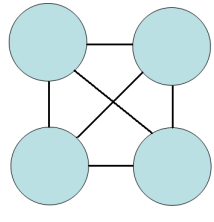


Рис. 1.7. Полносвязная топология

1.2.3. По ведомственной принадлежности

По ведомственной принадлежности различают следующие виды сетей:

- *ведомственные* — принадлежат какой-то организации и находятся на ее территории;
- государственные — используются в госструктурах.

1.2.4. По скорости передачи данных

По скорости передачи данных сети делятся на низко-, средне- и высокоскоростные. Основной критерий разделения — скорость передачи данных. Понятно, что скорость передачи данных — понятие непостоянное. То, что сегодня считается среднескоростным соединением, завтра будет отнесено к низкоскоростным. Тем не менее, сегодня низкоскоростной сетью считается сеть со скоростью передачи информации до 10 Мбит/с. Среднескоростная сеть передает данные со скоростью до 100 Мбит/с, а высокоскоростные сети передают информацию со скоростью свыше 100 Мбит/с.

1.2.5. По типу среды передачи данных

Казалось бы, тут все просто: сети бывают проводными или беспроводными. Но очень часто "в природе" встречаются *смешанные*, или *гибридные* сети, сочетающие как проводные, так и беспроводные технологии. В этой книге больше внимания будет уделяться именно таким сетям. Представьте, что у вас дома есть компьютер и ADSL-модем. Вы купили ноутбук. Подключать ноутбук по Ethernet-кабелю не очень-то хочется — ноутбук по своей природе мобильное устройство, и хотелось бы использовать его по всей квартире (а если у вас свой дом, то и во дворе). Поэтому вам понадобится *точка доступа*, которую вы подключите к существующей сети. Точка доступа в данном случае будет выполнять функцию моста между беспроводной и проводной сетью. Именно с ее помощью ваш ноутбук сможет подключиться к Интернету. Поэтому у вас дома появится смешанная сеть, созданная "своими руками".

1.2.6. По способу организации взаимодействия компьютеров

Сети бывают одноранговыми и типа клиент/сервер. В *одноранговой* сети нет выделенного сервера: каждый клиент сети может выступать как в роли сервера, то есть предоставлять услуги другим узлам сети, так и в роли клиента, то есть пользоваться услугами, которые предоставляют другие узлы сети.

В сети *клиент/сервер* есть выделенный сервер, предоставляющий определенные сетевые услуги (какие именно, зависит от самой сети).

Здесь мы остановимся, а в следующей главе поговорим об основных сетевых устройствах.

Глава 2

Основные сетевые устройства

2.1. Активное и пассивное сетевое оборудование

Для построения компьютерной сети, то есть для организации передачи информации между компьютерами, используется сетевое оборудование. Сетевое оборудование бывает активным и пассивным. *Активным* называется оборудование, обладающее неким "интеллектом" — например, коммутатор (switch), маршрутизатор (router). *Пассивное* сетевое оборудование "интеллектом" не наделено. К пассивному оборудованию относят кабели (например, коаксиальный или витая пара), розетки (RJ45, RG58 и др.), повторитель (repeater), концентратор (hub) и т. д.

Стоп! Если вы хоть немного знакомы с Ethernet-сетями, вы можете запутаться. Ведь концентратор, как и коммутатор, можно использовать в качестве центрального сетевого устройства в Ethernet-сети, почему тогда концентратор — это пассивное устройство, а коммутатор — активное? Дело в том, что концентратор не проявляет никакой интеллектуальной деятельности — он просто получает сигналы и копирует (повторяет) их на все свои порты, равно как и повторитель. Повторитель получает сигнал, усиливает его и повторяет на другой порт. Повторители обычно используются для увеличения дальности передаваемого сигнала. Коммутатор же "знает", к какому порту подключен какой компьютер, поэтому передает полученный сигнал не на все порты, а только на определенный порт, к которому подключен компьютер-назначение.

Различного сетевого оборудования очень много. Мы не будем пытаться объять необъятное, поэтому в этой книге рассмотрим только оборудование, необходимое для построения проводных Ethernet-сетей и беспроводных Wi-Fi-сетей.

2.2. Оборудование, необходимое для построения Ethernet-сети

Для организации современной Ethernet-сети (имеются в виду спецификации Fast Ethernet и Gigabit Ethernet) необходим всего один коммутатор (switch). Конечно, если сеть большая, то понадобится несколько коммутаторов, общее количество портов которых сможет обеспечить подключение всех узлов сети. На рис. 2.1 изображен так называемый *промышленный* коммутатор от Linksys.

Дизайн корпуса промышленного коммутатора обычно не очень эффектен, но сделано это умышленно — чтобы коммутатор можно было поместить в стойку сетевого оборудования. Ведь в больших корпоративных сетях обычно несколько коммутаторов, которые помещаются в специальную стойку (или в специальный шкаф сетевого оборудования, который можно закрыть и тем самым ограничить физический доступ к нему). На рис. 2.2 изображена типичная стойка с коммутаторами.

Рис. 2.1. 16-портовый коммутатор от Linksys

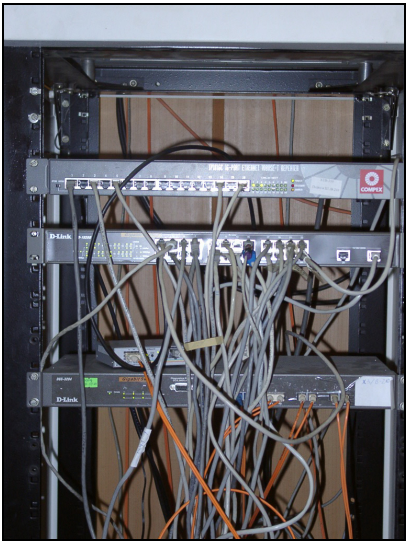


Рис. 2.2. Стойка с коммутаторами

А на рис. 2.3 изображен шкаф с коммутаторами. Такой шкаф может быть большего размера и содержать другое оборудование (например, серверы сети), но главное отличие шкафа от стойки — наличие двери, которая ограничивает доступ к сетевому оборудованию.

Рис. 2.3. Шкаф с сетевым оборудованием

Рис. 2.4. 8-портовый гигабитный коммутатор от D-Link

Если вы хотите построить небольшую домашнюю или офисную сеть, то можете выбрать коммутатор с более интересным дизайном, который лучше впишется в ваш интерьер. На рис. 2.4 изображен 8-портовый гигабитный коммутатор от D-Link. Вид у него более "дружелюбный", но в стойку его уже не поместишь, хотя при организации домашней сети никакой стойки у вас и не будет.

Давайте теперь уточним, почему в современных сетях не стоит использовать концентраторы (hub). Представим, что у нас есть сеть на четыре компьютера. Назовем их А, Б, В и Г. Пусть компьютер А отправляет данные компьютеру Г. Концентратор отправит полученный от компьютера А сигнал на все свои порты — то есть сигнал, отправленный компьютером А, получат все компьютеры сети. Затем каждый компьютер анализирует заголовки пакета, в которых указан компьютер-получатель. Если адрес компьютера совпадает с адресом получателя, компьютер принимает пакет, в противном случае — игнорирует его. Таким образом, использование концентратора приводит к "брожению" по сети паразитного трафика. По сути, концентратор — это обычный многопортовый повторитель (усилитель) сигналов. И чем больше сеть, тем медленнее она работает в случае использования концентратора, поскольку "брожение" паразитного трафика имеет лавинообразный характер. Вы только представьте, что в сети не четыре компьютера, а несколько десятков… Поэтому в больших сетях концентраторы существенно снижают производительность сети.

Коммутатор же, в отличие от концентратора, строит специальную таблицу соответствия, позволяющую однозначно узнать, к какому порту какой компьютер подключен (см., например, табл. 2.1).

Таблица 2.1. *Таблица соответствия портов коммутатора и адресов компьютеров*

Номер порта	Адрес компьютера
1	Б
2	А
3	Г
4	В

Когда компьютер А, подключенный ко второму порту коммутатора, отправляет пакет компьютеру Г, коммутатор знает, что компьютер Г подключен к третьему порту, и отправляет пакет только на третий порт. При этом снижается нагрузка на сеть, потому что компьютеры не получают "лишних" пакетов.

Кроме того, поскольку концентратор отправляет данные каждому компьютеру сети, становится очень простым перехват данных. Существуют специальные программы, переводящие сетевой адаптер в режим мониторинга, в котором он осуществляет принятие всех данных, даже тех, которые не адресованы этому компьютеру. Поэтому, если в сети используется концентратор, все передаваемые данные становятся общим достоянием — их может перехватить любой компьютер, подключенный к концентратору.

Итак, использование коммутатора позволяет повысить производительность сети и повысить ее безопасность. Ранее сети в основном строились на базе концентраторов, поскольку их стоимость была существенно ниже стоимости коммутаторов. Со снижением цен на коммутаторы концентраторы практически исчезли с магазинных полок. Однако в некоторых старых сетях они еще используются. Если вам придется обслуживать такую сеть, первым делом замените концентратор на коммутатор — вы сразу почувствуете разницу.

Какой коммутатор применить: Fast Ethernet (100Base-T) или Gigabit Ethernet (1000Base-T)? В первом случае максимальная (теоретическая) скорость передачи данных составляет 100 Мбит/с, во втором случае — 1000 Мбит/с. Коммутаторы Gigabit Ethernet стоят немного дороже (цены приводить не буду, поскольку через год они станут еще доступнее, а через два — о Fast Ethernet забудут, как в свое время забыли о коаксиале и концентраторах).

Учитывая, что сеть строится не на день и не на два, лучше выбрать Gigabit Ethernet. С точки зрения монтажа сети ничего не изменится — даже если вы сейчас установите коммутатор Fast Ethernet, то завтра без проблем сможете заменить его на Gigabit Ethernet. Но нужно помнить следующее: чтобы

сеть работала в режиме 1000Base-T, необходимо, чтобы 1000Base-T поддерживали сетевые адаптеры компьютеров. Практически на всех современных материнских платах встроенные сетевые адаптеры уже поддерживают 1000Base-T, но если в вашей сети есть компьютеры, которым 2–3 года, скорее всего, вам придется докупать для них сетевые адаптеры с поддержкой 1000Base-T.

Идем дальше — количество портов. Обычно в продаже есть коммутаторы на 5, 8, 16, 24 порта. Промышленные коммутаторы могут иметь большее число портов, например 32 или 48. Может быть, в скором времени появятся коммутаторы с большим числом узлов, но я сомневаюсь. Поскольку обычно один коммутатор обслуживает одну подсеть, я не думаю, что в одной подсети будет больше 48 компьютеров. А если это случится, такую подсеть желательно (из соображений локализации трафика) разделить на несколько подсетей с меньшим числом компьютеров.

Так что для домашней сети покупайте коммутатор, способный подключить все имеющиеся дома компьютеры, — большой запас портов вам вряд ли понадобится. Обычно в домашней сети 2–4 компьютера. В этом случае вам будет достаточно 5-портового коммутатора — 5-й порт пригодится для подключения этого коммутатора к другому коммутатору сети. В коммутаторах с большим числом портов для подключения к другому коммутатору обычно используется один из имеющихся портов (например, порт 1). Промышленные коммутаторы иногда имеют так называемый *магистральный* порт. Например, 16 портов, работающих в режиме 100Base-T, и один порт, работающий в режиме 1000Base-T, — для подключения к магистрали сети, работающей со скоростью 1000 Мбит/с. Иногда вместо порта 1000Base-T оборудуется оптоволоконный порт, например, 100Base-FB. В этом случае скорость магистрали такая же, как и скорость сети, но расстояние передачи сигнала намного выше (более 2 км), что позволяет использовать оптоволоконный кабель для соединения сетей двух (или более) зданий в одну большую сеть.

В случае с офисной сетью количество портов коммутатора должно в два раза превышать количество компьютеров сети. Например, если в вашей сети четыре компьютера, то нужен 8-портовый коммутатор. Дополнительные четыре порта могут понадобиться, если придется подключить дополнительные компьютеры, например, ноутбуки ваших клиентов, если у вас пока еще нет для них точки доступа Wi-Fi.

По большому счету, для организации сети больше ничего и не нужно (разумеется, кроме кабеля и коннекторов RJ45, но это уже детали, о которых мы поговорим в *третьей части* книги).

2.3. Оборудование, необходимое для построения сети Wi-Fi

Как и в случае с Ethernet-сетью, нам понадобятся сетевые адаптеры и центральное устройство сети. Только сетевые адаптеры нужны не обычные, а беспроводные. А роль центрального устройства сети будет играть *точка доступа* (access point).

Все современные модели ноутбуков по умолчанию оснащены адаптером Wi-Fi, а вот стационарные (настольные) компьютеры придется дооснастить беспроводными сетевыми адаптерами. Проще всего купить беспроводной адаптер, подключающийся к компьютеру по USB. Есть также адаптеры, выполненные в виде PCI-карты, устанавливаемой в свободный PCI-слот компьютера. Такие адаптеры используются редко, поскольку их установка требует вскрытия корпуса компьютера, что несколько неудобно (особенно, если компьютер еще на гарантии — тогда придется нести его в сервисный центр, а что делать, если таких компьютеров много?).

USB-адаптеры могут быть выполнены в разных корпусах. На рис. 2.5 изображен небольшой беспроводной адаптер, напоминающий по своим размерам флешку. У такого адаптера антенна встроенная, поэтому его можно использовать только, если компьютер находится в зоне уверенного приема. Если же компьютер установлен ближе к "мертвой" зоне, лучше выбрать адаптер, выполненный в виде отдельного устройства (рис. 2.6). Такой адаптер обычно имеет небольшой размер и подключается к компьютеру USB-кабелем (питание адаптер получает тоже по USB). Преимущество этого адаптера заключается в следующем — его можно легко передвинуть в пределах длины USB-кабеля, чтобы попасть в зону уверенного приема сети. Ноутбук можно легко переместить в эту зону — просто взяли и перенесли. Со стационарным компьютером такого не сделаешь — у каждого стационарного компьютера есть свое место. А что делать, если в том месте, где установлен компьютер, не обеспечивается уверенный прием беспроводных сигналов? Не переносить же компьютер? В этой ситуации поможет адаптер, изображенный на рис. 2.6. Иногда перемещение адаптера всего на несколько сантиметров дает весьма ощутимые результаты. Да и антенна у такого адаптера обладает большей чувствительностью, чем встроенная антенна адаптера, изображенного на рис. 2.5. К тому же к подобным адаптерам (с внешней антенной) обычно можно подключить дополнительную антенну с еще большей чувствительностью. Обо всем этом мы поговорим, когда будем строить свою собственную беспроводную сеть. А сейчас перейдем лучше к точке доступа.

Примечание

При выборе Wi-Fi-адаптера учитывайте наличие драйверов — особенно, если вы планируете использовать его в Linux. Чтобы не получилось так, что Linux не поддержит купленный Wi-Fi-адаптер.

Рис. 2.5. USB Wi-Fi-адаптер со встроенной антенной

Рис. 2.6. USB Wi-Fi-адаптер с внешней антенной

Рис. 2.7. Точка доступа от D-Link с тремя антеннами

Точка доступа (рис. 2.7) выполняет в беспроводной сети роль центрального устройства. Казалось было, все здесь просто: устанавливаем Wi-Fi-адаптеры, подсоединяем точку доступа, и беспроводная сеть готова — беспроводные клиенты могут обмениваться данными. Однако, если вы планируете купить точку доступа прямо сейчас, не следует покупать первую попавшуюся. Сначала желательно определиться, какие функции точки доступа вам нужны, затем "вычислить" модели точек доступа, обеспечивающие необходимые вам функции, и просмотреть в Интернете отзывы об этих моделях. Только так можно выбрать лучшую точку доступа.

Точка доступа может предоставлять дополнительные функции — например, функции *маршрутизатора*. Предположим, у вас дома есть несколько ноутбуков. К одному ноутбуку подключен ADSL-модем. Как организовать общий доступ к Интернету? Покупается точка доступа, к которой этот ADSL-модем и подключается. Ноутбуки (беспроводные клиенты) будут подключаться к Интернету по Wi-Fi, а точка доступа выступит в роли маршрутизатора.

2.4. Дополнительные сетевые устройства

Представим, что у нас есть два (или более) обычных (настольных) компьютера и одно ADSL-соединение. И нужно обеспечить общий доступ к Интернету. Это можно сделать средствами Windows. Тогда в один компьютер надо будет установить дополнительный сетевой адаптер. Первый сетевой адаптер будет использоваться для подключения к Интернету, а второй — для подключения к локальной сети (для связи с остальными компьютерами сети). Компьютер с двумя сетевыми адаптерами для остальных компьютеров сети будет выполнять роль *шлюза* (gateway). Преимущество такого решения — дешевизна: ведь мы обеспечили общий доступ к Интернету практически без дополнительных устройств. Недостаток заключается в том, что компьютер-шлюз должен быть постоянно включен, иначе остальные компьютеры не смогут подключиться к Интернету.

Решить эту проблему можно, купив отдельное устройство, называемое *маршрутизатором* (при рассмотрении выбора точки доступа мы это устройство уже упоминали). Маршрутизатор обеспечивает передачу пакетов по заданному маршруту. В нашем случае — от локальных компьютеров к интернет-провайдеру. Таким образом, все компьютеры сети будут подключаться к центральному коммутатору, а он, в свою очередь, — к маршрутизатору. Также к маршрутизатору будет подключен и ADSL-модем.

Маршрутизаторы бывают разные. Некоторые могут выполнять роль коммутатора. Купив такой маршрутизатор, вы сократите количество активного сетевого оборудования (а значит, сэкономите деньги) до двух единиц — маршрутизатора и ADSL-модема. Если же у вас в сети компьютеров немного (2–4), можно подыскать ADSL-модем с функциями маршрутизатора. В этом случае у вас будет всего одна "коробочка" — все компьютеры сети будут подключены к этому устройству, которое, в свою очередь, будет подключено к телефонной сети. Этим вы сэкономите еще больше средств. Поэтому очень важно перед построением сети спланировать сей процесс. Хорошее планирование не только позволяет сэкономить деньги, но и время, впоследствии потраченное на дальнейшую модернизацию сети.

А теперь представим, что в нашей сети есть два (или больше, количество — не принципиально) стационарных компьютера и несколько ноутбуков. Ноутбуки было бы хорошо подключать по Wi-Fi. Стационарные компьютеры принято подключать по Ethernet (хотя бы потому, что не хочется покупать для них беспроводные адаптеры). Так вот, можно купить устройство, которое одновременно является ADSL-модемом, беспроводной точкой доступа и коммутатором. Одним из таких устройств является DSL-2640U от D-Link (далее мы рассмотрим процесс настройки этого устройства). Это устройство (рис. 2.8) позволяет объединить в сеть несколько беспроводных клиентов (это наши ноутбуки) и четыре проводных клиента. Все клиенты (как проводные, так и беспроводные) автоматически настраиваются на доступ к Интернету по совместно используемому ADSL-каналу. Кроме того, это устройство обладает встроенным брандмауэром, что позволяет защитить вашу сеть от вторжения извне.

Рис. 2.8. ADSL-модем, маршрутизатор, коммутатор и беспроводная точка доступа D-Link DSL-2640U

Простота настройки сети с помощью такого устройства просто поражает. Все, что вам нужно — это включить устройство, подключить к нему клиентов, запустить программу настройки (как это сделать, написано в руководстве по устройству) и установить базовые параметры сети, а именно: имя пользователя и пароль для ADSL-соединения, идентификатор беспроводной сети (SSID) и выбрать тип шифрования беспроводных соединений. Вот и все — сеть будет работать. Клиентов можно вовсе не настраивать — они будут автоматически настроены по протоколу DHCP (Dynamic Host Configuration Protocol — протокол динамической настройки узла).

Впрочем, у всех комбинированных устройств есть один недостаток — плохая масштабируемость. Если ваша сеть будет расти, добавить новых клиентов

в нее будет сложно, а в некоторых случаях вовсе невозможно. Тогда придется покупать отдельные устройства. Например, коммутатор, к которому будут подключаться до 48 проводных клиентов, и точку доступа для подключения беспроводных клиентов. В свою очередь, точка доступа и коммутатор будут подключаться к ADSL-маршрутизатору. Хотя в сложных случаях целесообразнее использовать программный (не аппаратный) маршрутизатор — компьютер под управлением UNIX/Linux. Такой компьютер можно использовать в роли маршрутизатора и на нем запустить брандмауэр, DNS-, WWW-, FTP- и почтовый серверы.

Итак, в этой главе мы ознакомились с основными сетевыми устройствами. Следующая глава будет сугубо теоретическая. Мы поговорим о том, что должен знать каждый администратор и опытный пользователь любой сети, рассмотрим модель OSI и адресацию в TCP/IP-сети.

Глава 3

Модель OSI и адресация в современных сетях

3.1. Способы передачи данных

Любая сеть данных должна использовать какой-нибудь метод коммутации своих абонентов, то есть сеть должна знать, как отправить данные тому или иному компьютеру. В современных сетях распространены три основных метода коммутации: коммутация каналов, коммутация сообщений и коммутация пакетов.

Коммутация каналов используется в аналоговых (нецифровых) телефонных сетях. Для передачи компьютерных данных используется *коммутация пакетов*. Разница между этими методами просто огромна. В первом случае (коммутация каналов) для передачи данных нужен физический канал между двумя узлами. Понятно, что прокладывать кабель между каждой парой узлов сети (между каждой парой телефонов) экономически нецелесообразно, поэтому были созданы *коммутаторы* (сейчас мы говорим о телефонных коммутаторах), соединяющие между собой двух разных абонентов сети по их вызову.

В компьютерных сетях такой способ коммутации совершенно не годится, поскольку канал большую часть времени будет простаивать и без пользы занимать ресурсы коммутатора. Кроме того, при отправке большого количества информации по такой сети на коммутатор ляжет огромная нагрузка, поскольку данные будут переданы за один раз.

Метод коммутации пакетов заключается в том, что передаваемые данные разбиваются на части — *пакеты*. Каждый пакет отправляется отдельно, и, что интересно, два разных пакета, отправленные одним отправителем, могут дойти к получателю разными маршрутами. Например, вы отправляете пакеты компьютеру, не принадлежащему вашей сети. Сначала пакеты отправятся провайдеру, затем — какому-нибудь маршрутизатору Интернета, но если этот маршрутизатор окажется недоступен (мало ли чего может случиться),

автоматически будет задействован резервный канал, отправляющий данные через другой маршрутизатор. В итоге получится, что первый пакет будет доставлен одним маршрутом, а второй — другим. Однако оба пакета будут доставлены получателю.

К тому же метод коммутации пакетов позволяет использовать физически одну и ту же среду передачи данных (читайте — один и тот же кабель) для (почти) одновременной отправки данных несколькими компьютерами. Рассмотрим ситуацию: у вас в квартире установлено два параллельных телефонных аппарата, и вы разговариваете по одному из них. Если кто-то поднимет трубку второго телефона, то не сможет набрать номер, поскольку среда передачи информации (телефонный кабель) занята. В случае с коммутацией пакетов такого нет — в сетях с архитектурой "общая шина" (Ethernet) данные отправляются почти одновременно. Например, компьютерам А и Б нужно отправить данные. Допустим, первым получил доступ к общей среде компьютер А. Он отправляет пакет фиксированного размера. Пока компьютер А отправляет пакет, компьютер Б ожидает доступ к среде. После отправки пакета компьютером А компьютер Б сможет получить доступ к общей среде и отправить свой пакет. Компьютер А в это время делает небольшую паузу. Потом компьютер Б должен сделать паузу, за время которой компьютер А успеет передать следующий пакет. Сами понимаете, время ожидания настолько мизерно, что пользователям компьютеров А и Б кажется, что компьютеры отправляют данные одновременно. Если бы в компьютерной сети использовался метод коммутации каналов, то компьютер Б должен был ждать, пока компьютер А не передаст все данные.

Метод *коммутации сообщений* в чистом виде практически нигде не используется, но он послужил прототипом для метода коммутации пакетов.

3.2. Модель OSI

В 80-х годах прошлого века появилась необходимость стандартизировать различные сетевые технологии. Ведь без стандартизации в мире компьютерных сетей воцарился бы хаос: оборудование различных производителей не смогло бы работать вместе. Поэтому международная организация по стандартизации (International Organization for Standardization, OSI) разработала *модель взаимодействия открытых систем* (Open System Interconnection, OSI). Вы также можете встретить другие названия этой модели: *семиуровневая модель OSI*, или просто *модель OSI*. Эта модель предусматривает семь уровней взаимодействия систем:

1. Физический.
2. Канальный.

3. Сетевой.
4. Транспортный.
5. Сеансовый.
6. Представительный.
7. Прикладной.

Зачем нужна была такая система? Предположим, что нам нужно заставить вместе работать две сети, использующие разную среду передачи данных, — например, витую пару и радиоволны (беспроводную сеть). Если бы не было модели OSI, то для каждой сети пришлось бы разрабатывать модель взаимодействия, а потом придумывать способ, позволяющий заставить две разные по своей архитектуре сети работать вместе. В случае с моделью OSI не нужно "изобретать велосипед" заново. Следует взять за основу уже имеющуюся сеть (в данном случае Ethernet) и переписать физический уровень. В итоге нам не придется разрабатывать браузеры, почтовые клиенты и другие сетевые приложения для каждой сети — браузеру все равно, какая среда передачи данных используется. Как видите, модель OSI хоть и теоретическая, зато очень полезная. Рассмотрим ее уровни:

- на *физическом уровне* определяются характеристики электрических сигналов, то есть описывается физическая среда данных. На этом уровне и происходит физическая передача данных по кабелю или радиоволнам (в зависимости от типа сети). Пример протокола физического уровня: 1000Base-T — спецификация Ethernet, передающая данные по витой паре 5-й категории (о категориях витой пары мы поговорим позднее) со скоростью 1000 Мбит/с;
- *канальный уровень* используется для передачи данных между компьютерами (и другими устройствами, например, сетевыми принтерами) одной сети. Пример протокола канального уровня: PPP (Point-to-Point Protocol). Топология сети (шина, звезда и т. д.) определяется как раз на канальном уровне (в *главе 1* мы подробно рассмотрели все используемые топологии сетей). На канальном уровне все передаваемые данные разбиваются на части, называемые *кадрами* (frames). Канальный уровень передает кадры физическому уровню, а тот, в свою очередь, отправляет их в сеть.

  На канальном уровне вводится понятие MAC-адреса. *MAC-адрес* — это уникальный аппаратный адрес сетевого устройства (например, сетевого адаптера, точки доступа). Каждому производителю сетевых устройств выделяется свой диапазон MAC-адресов. В мире нет двух сетевых устройств с одинаковыми MAC-адресами;
- теперь рассмотрим *сетевой уровень*. Он используется для объединения нескольких сетей, то есть для организации межсетевого взаимодейст-

вия, — ведь протоколы канального уровня могут работать только в пределах одной сети. Канальный уровень не может передать кадр компьютеру, который находится в другой сети. Понятно, что если бы у нас был только канальный уровень и не было сетевого, мы не смогли бы передавать данные между двумя сетями, например, между локальной сетью и Интернетом. Пример протокола сетевого уровня: IP (Internet Protocol). Конечно, IP — это не единственный протокол сетевого уровня, но в этой книге мы будем рассматривать только TCP/IP-сети, поэтому нет смысла упоминать другие протоколы.

При всем своем желании мы не можем построить огромную сеть, охватывающую весь мир (даже если бы это и удалось, не думаю, что такая сеть работала бы быстро). Поэтому Интернет состоит из совокупности различных сетей, которые объединяются в одно целое маршрутизаторами. Расстояние между сетями исчисляется в количестве переходов пакетов (на сетевом уровне передаваемые данные разбиваются именно на пакеты) через маршрутизаторы. Единица такого перехода называется *хопом* (от англ. hop). Количество хопов равно количеству маршрутизаторов между двумя сетями. Например, от моего узла до узла **volia.net** 6 хопов (шесть переходов), что показано на рис. 3.1;

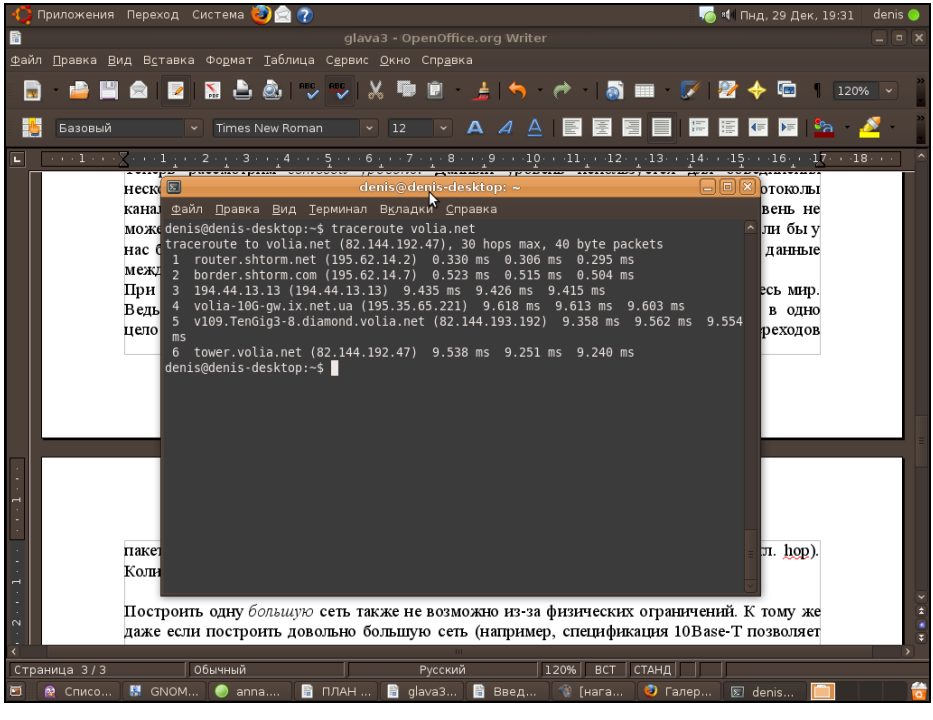


Рис. 3.1. Количество переходов от моего узла до узла **volia.net**

- *транспортный уровень* отвечает за доставку пакетов получателю. Не секрет, что при передаче по каналам связи данные могут быть повреждены или вовсе потеряны. Гарантирует доставку пакета в первозданном виде именно транспортный уровень. На этом уровне осуществляются обнаружение и исправление ошибок, восстановление прерванной связи и некоторые дополнительные сервисы вроде срочной доставки (приоритет пакета) и мультиплексирование нескольких соединений. Самым известным и распространенным протоколом транспортного уровня является TCP (Transport Control Protocol);
- *сеансовый уровень* отвечает за установку и за разрыв соединения между компьютерами. На этом уровне также предоставляются средства синхронизации. Сеанс сетевого уровня заключается в установке соединения (при установке стороны, между которыми будут передаваться данные, могут договариваться о дополнительных параметрах связи, например, обмениваться ключами), передаче информации и разрыве соединения.

  Многие часто путают сеансы сетевого уровня и сеанс связи. Вы можете установить сеанс связи (например, подключиться к Интернету), но не устанавливать логического соединения, то есть не запустить браузер для соединения с удаленным узлом;
- как было отмечено чуть ранее, на сеансовом уровне стороны могут договориться о дополнительных параметрах, были также упомянуты *ключи*. Однако само шифрование и дешифрование данных осуществляется *представительным уровнем*. Пример протокола этого уровня — SSL (Secure Socket Layer);
- последний (самый высокий) уровень — *прикладной*. На этом уровне работает множество разных протоколов, например, HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) и т. д.

3.3. Что такое протокол?

В этой главе довольно часто упоминалось слово "протокол". *Протокол* — это правила, определяющие взаимодействие компьютеров в вычислительной сети. Рассмотрим несколько самых важных протоколов.

В основе Интернета лежит протокол TCP/IP (Transmission Control Protocol/ Internet Protocol). Чтобы система смогла работать в Интернете, она должна поддерживать протокол TCP/IP. Вообще говоря, TCP/IP — это совокупность двух протоколов. Протокол TCP, как уже было отмечено ранее, отвечает за корректность передачи данных по Интернету (точнее, по любой сети,

использующий этот протокол), то есть гарантирует доставку данных по сети. Протокол IP используется для адресации компьютеров сети. Дело здесь в том, что у каждого компьютера сети имеется свой уникальный адрес (IP-адрес), и, чтобы передать данные компьютеру, нужно его IP-адрес знать. Чуть позже мы поговорим о системе доменных имен (DNS, Domain Name System).

Кроме протоколов TCP и IP посетители Интернета работают с теми или иными серверами, использующими следующие протоколы:

- HTTP (Hyper Text Transfer Protocol) — протокол передачи гипертекста. Все Web-серверы Интернета используют протокол HTTP или его безопасную версию HTTPS (HTTP Secure);
- FTP (File Transfer Protocol) — протокол передачи файлов. Используется для обмена файлами между компьютерами. Вы можете подключиться к FTP-серверу и скачать необходимые вам файлы или же, наоборот, закачать свои файлы на сервер, если вы обладаете надлежащими правами доступа к серверу. В Интернете много публичных FTP-серверов, к которым разрешен анонимный доступ. Как правило, с таких серверов скачивать файлы разрешено всем желающим. Иногда, но очень редко, разрешается и запись файлов на публичный сервер. В состав любой операционной системы входит FTP-клиент — программа ftp. К тому же многие браузеры можно использовать в качестве FTP-клиента;
- SMTP (Simple Mail Transfer Protocol) — простой протокол передачи почты. Используется для отправки почты (e-mail);
- POP (Post Office Protocol) — протокол, используемый для получения сообщений электронной почты;
- IMAP (Internet Message Access Protocol) — еще один протокол для получения почты, но, в отличие от протокола POP, этот протокол позволяет читать почту без ее загрузки на компьютер пользователя. Протокол IMAP, по сути, намного удобнее, чем POP. Ведь почта хранится на сервере, и вы можете получить доступ к ней с любой точки земного шара, используя любой клиент. К тому же IMAP поддерживает поиск писем на сервере, что позволяет найти нужное письмо без загрузки всех писем на свой компьютер. Однако у IMAP есть один существенный недостаток, благодаря чему до сих пор распространен протокол POP — IMAP требует постоянного соединения с сервером. Если нет соединения с сервером, то вы не прочитаете не только новые сообщения, но и те, которые были получены ранее, поскольку все они хранятся на сервере. Так что в случае с IMAP об автономной работе (без подключения к Интернету) можно забыть.

Примечание

На днях полностью "перекочевал" в Linux (после очередного "падения" Windows). Так вот, до сих пор не знаю, как перенести в Linux 20 тыс. сообщений (разбитых на множество папок со своими правами сортировки) общим объемом около 4 Гбайт. Почта хранилась в программе The Bat!, а я сейчас использую почтовый клиент Mozilla Thunderbird. Программы для конвертации почтового формата The Bat! в формат Thunderbird пока не разработано... Если бы я использовал протокол IMAP, проблема отпала бы автоматически.

3.4. Адресация компьютеров

Для идентификации узлов Интернета используются IP-адреса. IP-адрес представляет собой четыре числа, разделенные точками (или одно 32-разрядное число, которое записывается в виде четырех восьмиразрядных чисел, разделенных точками, — как кому больше нравится). Нужно сразу отметить, что такая идентификация неоднозначная, поскольку IP-адреса могут быть статическими (постоянными) и динамическими. *Постоянные* (статические) IP-адреса обычно назначаются серверам, а *динамические* — обычным пользователям. Так что сегодня определенный динамический IP-адрес может быть назначен одному пользователю, а завтра — другому. Поэтому если в случае с аппаратными MAC-адресами еще можно говорить о какой-то однозначности (и то существуют способы подделки MAC-адресов), то IP-адреса по определению однозначными не являются.

Рассмотрим примеры IP-адресов: 127.0.0.1, 192.168.1.79, 111.33.12.99. Как было сказано ранее, IP-адрес — это одно 32-разрядное число или четыре 8-разрядных числа. Возведем 2 в восьмую степень и получим максимальное значение для каждого из четырех восьмиразрядных чисел — 256. Таким образом, учитывая, что некоторые IP-адреса зарезервированы для служебного использования, протокол IP может адресовать примерно 4,3 млрд узлов. Однако с каждым годом количество узлов во Всемирной паутине увеличивается, поэтому была разработана шестая версия протокола IP — IPv6 (если упоминается просто протокол IP, то, как правило, имеется в виду четвертая версия протокола — IPv4). Новый протокол использует 128-битные адреса (вместо 32-битных), что позволяет увеличить число узлов до 10^{12} и количество сетей до 10^{9}. IPv6-адреса отображаются как 8 групп шестнадцатеричных цифр, разделенных двоеточиями. Вот пример адреса нового поколения: 1628:0d48:12a3:19d7:1f35:5a61:17a0:765d.

Примечание

Впрочем, массовый переход на IPv6 (который еще называют IPng — IP Next Generation) пока так и не состоялся, хотя его используют несколько сотен сетей

по всему миру. В этой книге мы будем рассматривать только протокол IPv4, поскольку, судя по всему, Интернет не перейдет на IPv6 в ближайшие несколько лет. Интересующиеся могут прочитать об IPv6 по адресу: **http://ru.wikipedia.org/wiki/IPv6**.

IP-адреса выделяются *сетевым информационным центром* (NIC, Network Information Center). Чтобы получить набор IP-адресов для своей сети, вам надо обратиться в этот центр. Но, оказывается, это приходится делать далеко не всем. Существуют специальные IP-адреса, зарезервированные для использования в локальных сетях. Ни один узел глобальной сети (Интернета) не может обладать таким "локальным" адресом. Вот пример локального IP-адреса — 192.168.1.1. В своей локальной сети вы можете использовать любые локальные IP-адреса без согласования с кем бы то ни было. Когда же вы надумаете подключить свою локальную сеть к Интернету, вам понадобится всего один "реальный" IP-адрес — он будет использоваться на маршрутизаторе (шлюзе) доступа к Интернету.

Чтобы узлы локальной сети (которым назначены локальные IP-адреса) смогли "общаться" с узлами Интернета, используется специальная технология *трансляции сетевого адреса* (NAT, Network Address Translation). Маршрутизатор получает пакет от локального узла, адресованный интернет-узлу, и преобразует IP-адрес отправителя, заменяя его своим IP-адресом. При получении ответа от интернет-узла маршрутизатор выполняет обратное преобразование, поэтому нашему локальному узлу "кажется", что он общается непосредственно с интернет-узлом. Если бы маршрутизатор отправил пакет как есть, то есть без преобразования, то его отверг бы любой маршрутизатор Интернета, и пакет так и не был бы доставлен к получателю.

Наверное, вам не терпится узнать, какие IP-адреса можно использовать без согласования с NIC? Об этом говорить пока рано — ведь мы еще ничего не знаем о *классах* сетей. IP-адреса используются не только для адресации отдельных компьютеров, но и целых сетей. Вот, например, IP-адрес сети — 192.168.1.0. Отличительная черта адреса сети — 0 в последнем октете.

Сети поделены на классы в зависимости от их размеров:

- класс A — огромные сети, которые могут содержать 16777216 адресов, IP-адреса сетей лежат в пределах 1.0.0.0 — 126.0.0.0;
- класс B — средние сети, содержат до 65536 адресов. Диапазон адресов — от 128.0.0.0 до 191.255.0.0;
- класс C — маленькие сети, каждая сеть содержит до 256 адресов.

Существует еще и классы D и E, но класс E не используется, а зарезервирован на будущее (хотя будущее — это IPv6), а класс D зарезервирован для служебного использования (широковещательных рассылок).

Представим ситуацию. Вы хотите стать интернет-провайдером. Тогда вам нужно обратиться в NIC для выделения диапазона IP-адресов по вашу сеть. Скажем, вы планируете сеть в 1000 адресов. Понятно, что сети класса C вам будет недостаточно. Поэтому можно или арендовать четыре сети класса C, или одну класса B. Но, с другой стороны, 65536 адресов для вас — много, и если выделить вам всю сеть класса B, то это приведет к нерациональному использованию адресов. Так что самое время поговорить о *маске сети*. Маска сети определяет, сколько адресов будет использоваться сетью, фактически — маска задает размер сети. Маски полноразмерных сетей классов A, B и C представлены в табл. 3.1.

Таблица 3.1. *Маски сетей классов A, B и C*

Класс сети	Маска сети
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Маска 255.255.255.0 вмещает 256 адресов (в последнем октете IP-адреса могут быть цифры от 0 до 255). Например, если адрес сети 192.168.1.0, а маска 255.255.255.0, то в сети могут быть IP-адреса от 192.168.1.0 до 192.158.1.255. Первый адрес (192.168.1.0) называется IP-адресом сети, последний — зарезервирован для широковещательных рассылок. Следовательно, для узлов сети остаются 254 адреса — от 192.168.1.1 до 192.168.1.254.

А вот пример маски сети на 32 адреса: 255.255.255.224 (255 – 224 = 31 + + "нулевой" IP-адрес, итого 32).

Предположим, у нас есть IP-адрес произвольной сети, например, 192.168.1.0. Как узнать, к какому классу она принадлежит? Для этого нужно преобразовать первый октет адреса в двоичное представление. Число 192 в двоичной системе будет выглядеть так: **110**00000. Проанализируем первые биты первого октета. Если первые биты содержат двоичные цифры 110, то перед нами сеть класса C. Теперь проделаем то же самое с сетью 10.0.0.0. Первый октет равен 10, и в двоичной системе он будет выглядеть так: 00001010. Первый бит — 0, поэтому сеть относится к классу A. Опознать класс сети по первым битам первого октета поможет табл. 3.2.

Таблица 3.2. *Опознание класса сети*

Класс сети	Первые биты
A	0
B	10
C	110
D	1110
E	11110

Теперь поговорим о специальных зарезервированных адресах. Адрес 255.255.255.255 является *широковещательным*. Если пакет отправляется по этому адресу, то он будет доставлен всем компьютерам, находящимся с отправителем в одной сети. Можно уточнить сеть, компьютеры которой должны получить широковещательную рассылку, например, таким образом: 192.168.5.255. Этот адрес означает, что пакет получат все компьютеры сети 192.168.5.0.

Вам также следует знать адрес 127.0.0.1. Этот адрес зарезервирован для обозначения локального компьютера и называется *адресом обратной петли*. Если отправить пакет по этому адресу, то его получит ваш же компьютер, то есть получатель является отправителем, и наоборот. Данный адрес обычно используется для тестирования поддержки сети. Более того, к локальному компьютеру относится любой адрес из сети класса A с адресом 127.0.0.0. Поэтому при реальной настройке сети нельзя использовать IP-адреса, начинающиеся со 127.

А теперь можно рассмотреть IP-адреса сетей, зарезервированные для локального использования. В локальных сетях вы можете использовать следующие адреса сетей:

- 192.168.0.0 — 192.168.255.0 — сети класса C (всего 256 сетей, маска 255.255.255.0);
- 172.16.0.0 — 172.31.0.0 — сети класса B (всего 16 сетей, маска 255.255.0.0);
- 10.0.0.0 — сеть класса A (одна сеть, маска 255.0.0.0).

Обычно в небольших домашних и офисных сетях используются IP-адреса из сети класса C, то есть из диапазона 192.168.0.0 — 192.168.255.0. Но поскольку назначение адресов контролируется только вами, вы можете назначить в своей локальной сети любые адреса, например, адреса из сети 10.0.0.0, даже если у вас в сети всего 5 компьютеров. Так что выбор сети — это дело вкуса. Можете себя почувствовать администратором огромной сети и использовать адреса 10.0.0.0.

3.5. Система DNS

Узлов в Интернете достаточно много, поэтому ни один человек не способен запомнить IP-адреса всех необходимых ему узлов. Да и гораздо легче запомнить символьный адрес, скажем, **www.bhv.ru** или **www.dkws.org.ua**, чем их IP-адреса. Тем более, относительно недавно появилась возможность регистрации доменных имен на русском языке. Не знаю, приживутся ли такие доменные имена, но то, что они существуют, — это факт.

За преобразование IP-адресов в доменные имена и обратно отвечает *система доменных имен* (DNS, Domain Name System). Когда вы вводите доменное имя в строке браузера, система сначала разрешает это имя в IP-адрес (путем обращения к DNS-серверу), а потом подключается к узлу по полученному IP-адресу.

Не нужно думать, что система DNS появилась недавно. Она более "древняя", чем вы можете предположить. Впервые DNS была представлена в 1984 году. Правда, тогда далеко не все сети перешли на использование DNS-серверов. До этого доменные имена разрешались в IP-адреса с помощью файла hosts, в котором содержалась таблица соответствия доменных имен IP-адресам. Понятно, что такой файл нужно постоянно поддерживать в актуальном состоянии. Когда количество узлов увеличилось и поддержка этого файла стала проблемой для администратора сети, вот тогда и началась эра DNS. Кстати, файлом hosts можно пользоваться до сих пор. Для обеспечения совместимости его можно использовать даже в самых современных ОС (как в UNIX/Linux, так и в Windows), но, сами понимаете, происходит это очень редко.

Система DNS более подробно будет рассмотрена в *главе 24*. Мы даже настроим собственный кэширующий DNS-сервер.

Часть II

Подключение к уже существующей сети

Во второй части мы поговорим о подключении к уже существующей сети — будь то Ethernet-сеть, беспроводная сеть или Интернет.

Глава 4

Подключаемся к беспроводной сети

4.1. Подключение к беспроводной сети в Windows XP

Построением своей сети мы займемся в *главе 15*, а в этой главе рассмотрим подключение к уже существующей беспроводной сети — например, к сети отеля, библиотеки, интернет-кафе.

Первым делом активируйте Wi-Fi-адаптер вашего ноутбука (обычно для этого на его корпусе имеется соответствующая кнопка). Возможно, он уже включен. Лично я выключаю Wi-Fi-адаптер, когда не работаю в сети. Во-первых, так более экономно расходуется заряд аккумулятора ноутбука, а во-вторых, уменьшается вероятность несанкционированного доступа к моему компьютеру.

Как только адаптер будет включен, в области уведомлений (system tray) появится значок беспроводного соединения (рис. 4.1). Если значок отображается вместе с красным крестиком — ничего страшного. Возможно, в пределах досягаемости работают беспроводные сети, для доступа к которым нужно ввести пароль (иногда его еще называют *ключом*), — компьютер не может подключиться к ним автоматически (поскольку мы еще не ввели пароль), и поэтому на значке отображается красный крестик.

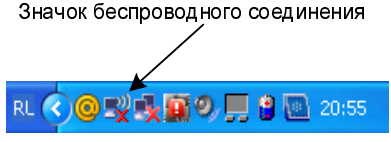


Рис. 4.1. Wi-Fi-адаптер включен

Дважды щелкните по значку беспроводного соединения, и вы увидите окно **Беспроводное сетевое соединение**, отображающее список доступных Wi-Fi-сетей (рис. 4.2). Выберите одну из безопасных сетей и нажмите кнопку **Подключить**.

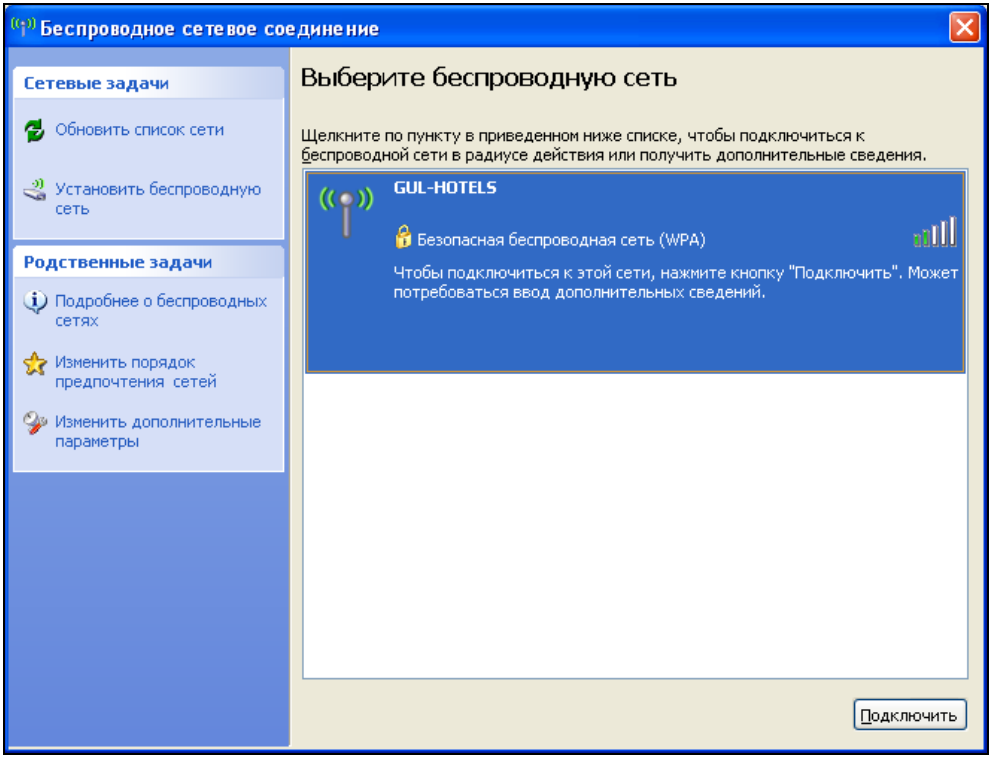


Рис. 4.2. Список беспроводных сетей

Если сеть защищена паролем, то после нажатия кнопки **Подключить** нужно будет ввести пароль. Узнать пароль можно у администратора сети. Сети отелей и библиотек обычно публичные, то есть не требующие ввода пароля.

Примечание

Вы только себе представьте — в отеле или библиотеке может быть очень много пользователей, и если каждый станет обращаться к администратору за паролем (ключом), то поработать у него не получится, — он будет целый день сообщать пароль доступа каждому желающему подключиться к сети. А закрыть сеть паролем и распечатать его на доске объявлений просто не имеет смысла — зачем тогда пароль?

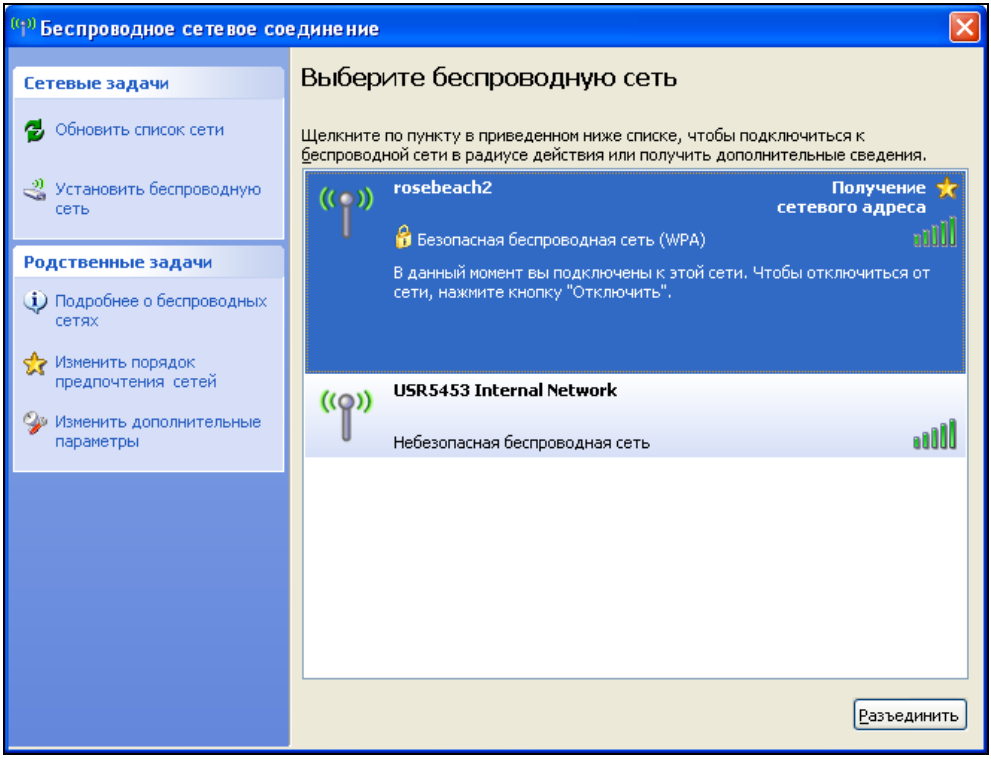


Рис. 4.3. В списке сетей есть небезопасная сеть

Посмотрим на рис. 4.3. Из него видно, что доступны две сети: **rosebeach2** и **USR5453**. Обратите внимание: вторая сеть небезопасная. Возможно, она развернута злоумышленником для перехвата передаваемых вами данных. Не стоит подключаться к таким сетям.

Собственно, на этом и все. Будем считать, что ничего чрезвычайного не произошло, и далее вы сможете продолжить работу в беспроводной сети.

> ***Примечание***
>
> Ноутбуки в целях экономии часто оснащаются комбинированными адаптерами WiFi + Bluetooth, а не двумя отдельными адаптерами. Такие адаптеры могут работать или в режиме Bluetooth, или в режиме Wi-Fi. Другими словами, если вы подключены к беспроводной сети, но вам понадобилось передать файлы на мобильный телефон или КПК по Bluetooth, то соединение с беспроводной сетью будет разорвано.

В Windows XP есть очень полезная функция, которая называется *списком предпочитаемых сетей*. Предположим, что вы очень часто работаете в офисе,

где доступно две или более беспроводных сети, но вам положено подключаться только к одной из них. По умолчанию адаптер пытается автоматически подключиться к сети с лучшим сигналом. Но это не всегда та сеть, к которой вам нужно подключиться. Чтобы адаптер подключался к беспроводным сетям в указанном вами порядке, щелкните правой кнопкой по значку беспроводного соединения и выберите команду **Свойства**. Перейдите на вкладку **Беспроводные сети**. Вы увидите список предпочитаемых беспроводных сетей (рис. 4.4). В этот список автоматически попадают сети, к которым вы уже подключались. Можно добавить сеть в список вручную, нажав кнопку **Добавить**. Используя кнопки **Верх/Вниз**, вы можете установить приоритет подключения к беспроводным сетям.

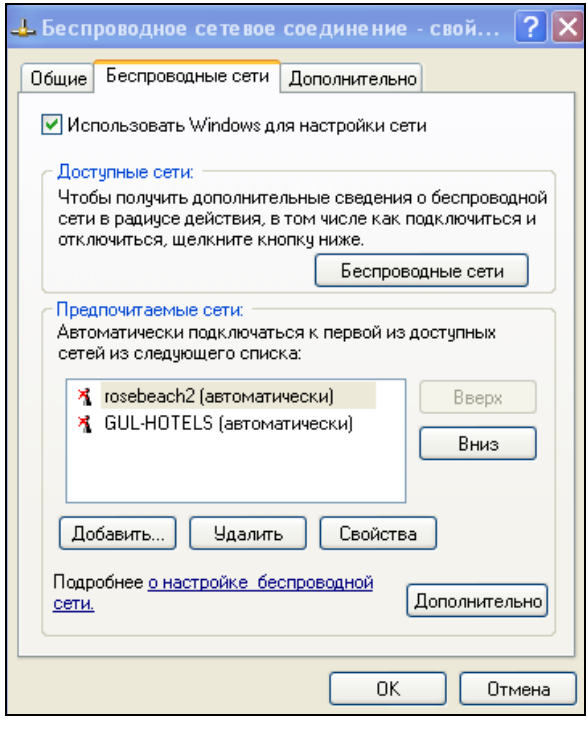


Рис. 4.4. Редактирование приоритета подключения к беспроводным сетям

Для просмотра или редактирования параметров сети выберите сеть и нажмите кнопку **Свойства**. В открывшемся окне свойств сети (рис. 4.5) вы сможете установить некоторые параметры ключа беспроводной сети (проверка подлинности, шифрование данных) и ввести сам ключ. Но обычно эти параметры

изменять не нужно, поскольку они устанавливаются автоматически при подключении к сети.

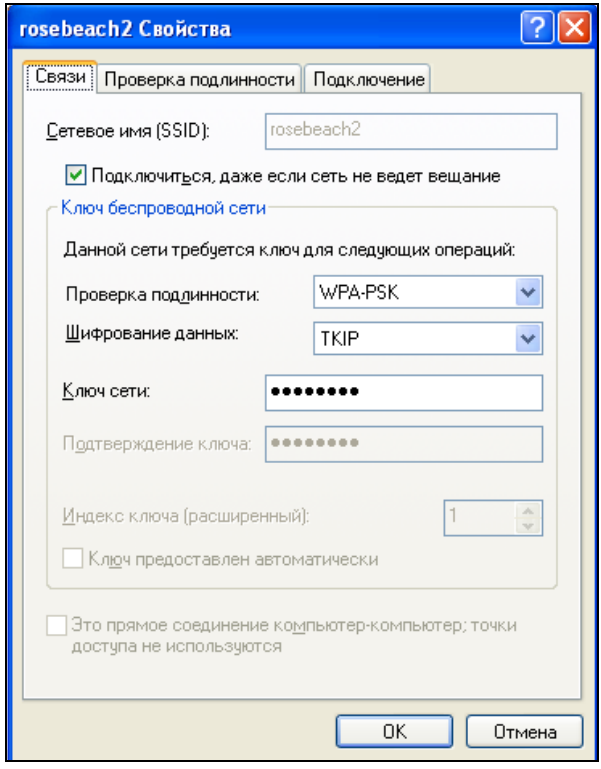


Рис. 4.5. Параметры беспроводной сети

Вернемся в окно, изображенное на рис. 4.4. Нажмите кнопку **Дополнительно**. В открывшемся окне (рис. 4.6) можно выбрать, к каким сетям нужно подключаться автоматически:

- **Любая доступная сеть (с точкой доступа)** — система будет автоматически подключаться к любой беспроводной сети. Этот вариант используется по умолчанию;
- **Сеть по точке доступа только (инфраструктура)** — система будет подключаться только к инфраструктурной сети, то есть к сети, где есть точка доступа;
- **Сеть компьютер-компьютер только (произв.)** — система будет подключаться только к сети ad hoc, то есть к сети компьютер-компьютер, организованной без точки доступа.

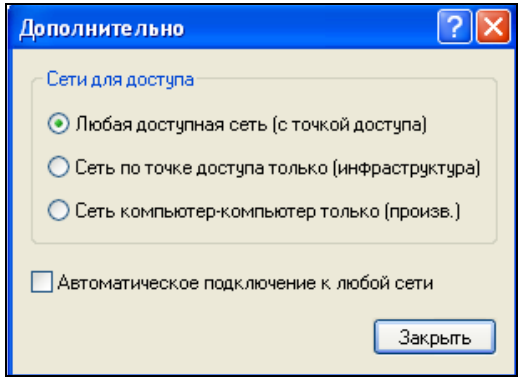


Рис. 4.6. Дополнительные настройки

Если вы не планируете подключаться к ad hoc-сетям, в целях безопасности нужно установить режим **Сеть по точке доступа только**. Иногда злоумышленники специально разворачивают ad hoc-сети с целью перехвата данных.

Чтобы отключиться от сети, или просто выключите беспроводной адаптер, или же выберите сеть из списка сетей и нажмите кнопку **Разъединить** (см. рис. 4.3).

4.2. Подключение к беспроводной сети в Windows Vista

Теперь рассмотрим подключение к беспроводной сети в Windows Vista. Как только вы окажетесь в зоне действия беспроводной сети (при условии, что беспроводной адаптер включен), вы увидите соответствующее уведомление (рис. 4.7).

Щелкните на надписи **Доступны беспроводные сети**. Откроется окно **Подключиться к сети** (рис. 4.8). Выберите беспроводную сеть и нажмите кнопку **Подключиться**.

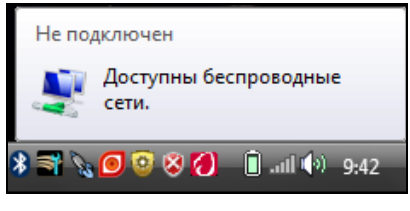


Рис. 4.7. Доступны беспроводные сети

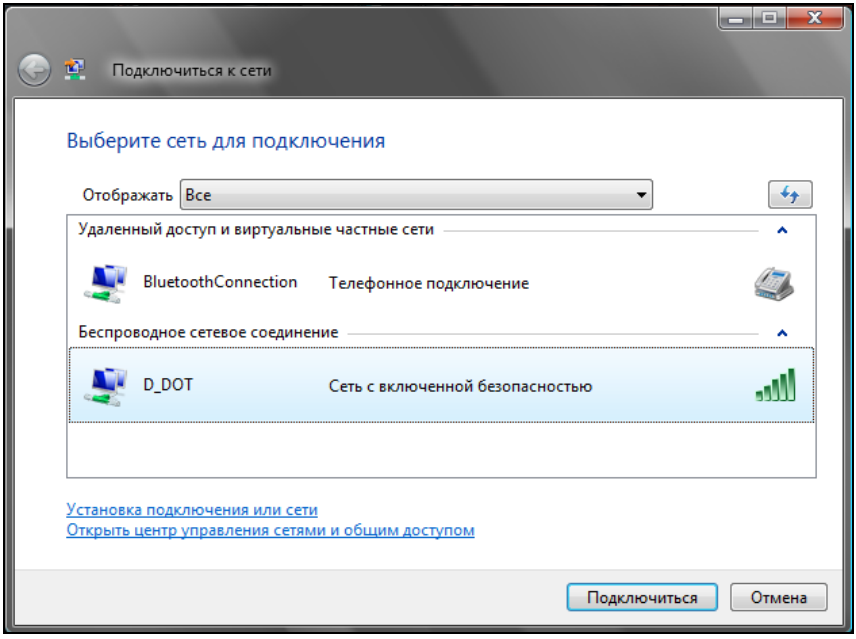


Рис. 4.8. Список беспроводных сетей

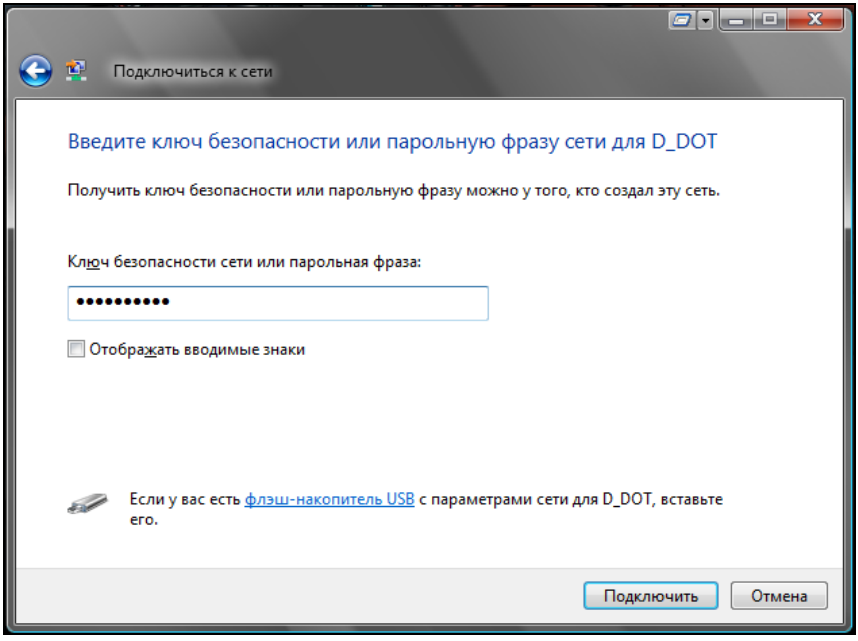


Рис. 4.9. Ввод пароля (если нужно)

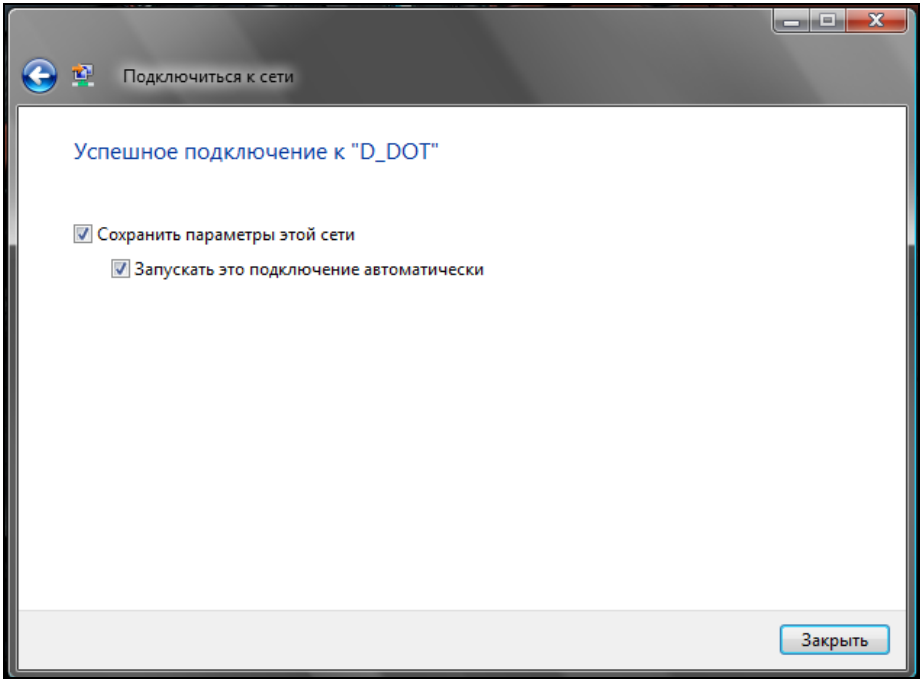


Рис. 4.10. Подключение установлено

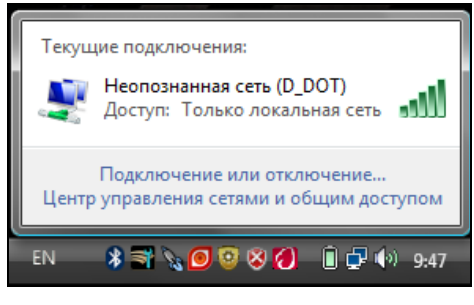


Рис. 4.11. Вы подключились к сети

Далее, если сеть защищена паролем (ключом безопасности), то нужно ввести этот пароль (рис. 4.9). Если же нет, тогда сразу начнется подключение к сети (рис. 4.10). Если вы планируете постоянно подключаться к данной беспроводной сети (например, это ваша домашняя сеть), тогда не выключайте параметры **Сохранить параметры этой сети** и **Запускать это подключение автоматически**. После успешного подключения к сети вы увидите соответствующее уведомление (рис. 4.11).

Итак, подключение к сети установлено и можно открывать браузер для соединения с узлом Интернета. Но мы пойдем чуть дальше. Щелкните на надписи **Центр управления сетями и общим доступом** (см. рис. 4.11) или вызовите **Центр управления сетями и общим доступом** через Панель управления Windows. В открывшемся окне вы увидите карту сети (рис. 4.12).

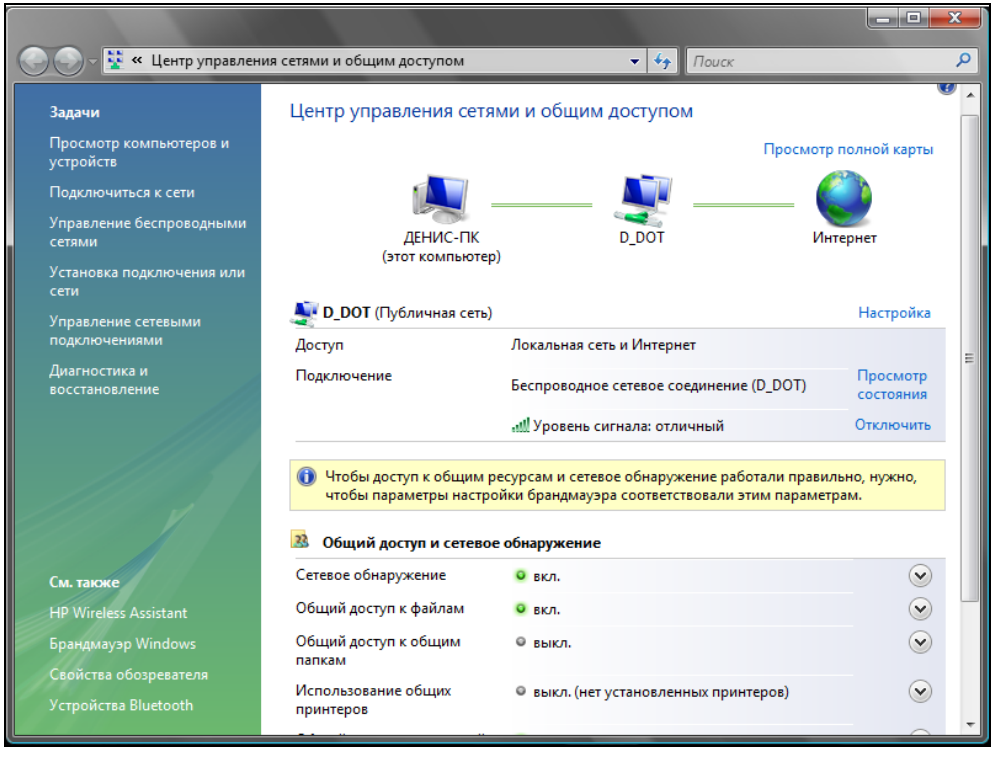


Рис. 4.12. Карта сети

В нижней части окна под картой сети приведен список доступных служб (например, службы доступа к файлам или папкам). Вы можете легко включить/выключить необходимые вам службы прямо отсюда.

Щелкните на ссылке **Просмотр состояния** у названия подключенной сети. В окне **Состояние – Беспроводное сетевое соединение** (рис. 4.13) вы можете получить следующую информацию:

- **Состояние носителя** — подключено соединение или нет;
- **SSID** — идентификатор сети;
- **Длительность** — длительность соединения в часах и минутах;

- **Скорость** — скорость соединения. Так, для стандарта беспроводных сетей 802.11g максимальная скорость соединения равна 54 Мбит/с;
- **Качество сигнала** — обратите внимание, что это качество сигнала, а не уровень сигнала. Уровень сигнала может быть высоким, например, когда вы находитесь недалеко от точки доступа, а качество сигнала может быть низким, поскольку поблизости есть источники интерференции радиосигнала. Некоторые программы управления беспроводным соединением (например, те, которые входят в комплект поставки беспроводного адаптера) выводят уровень сигнала, некоторые — и уровень, и качество сигнала. Качество сигнала — это более объективный показатель, на который нужно ориентироваться при тестировании сети;
- **Активность** — область содержит информацию о количество отправленной и принятой информации.

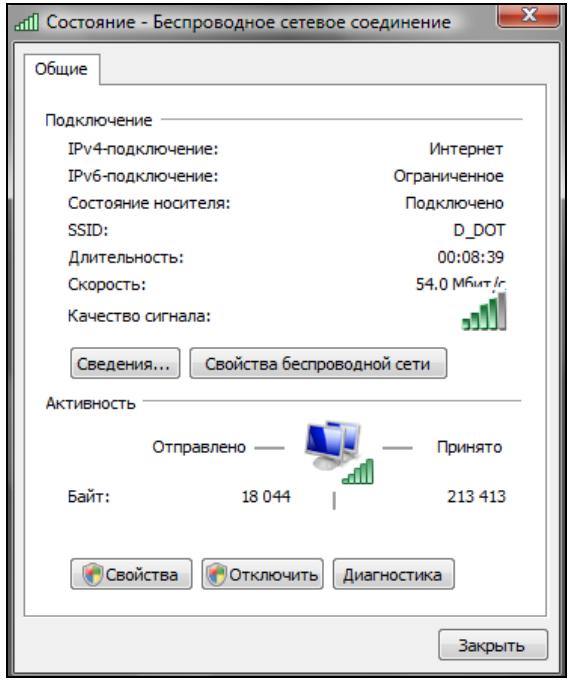


Рис. 4.13. Состояние беспроводного соединения

Нажмите кнопку **Свойства** (см. рис. 4.13). В открывшемся окне на вкладке **Подключение** (рис. 4.14) вы можете установить параметры автоматического подключения, например: **Подключаться автоматически, если сеть в радиусе действия**. Если сеть недоступна, то адаптер подключится к любой

другой подходящей сети, если она есть. Вы можете отключить этот режим, если хотите, чтобы адаптер подключался только к одной сети, например, только к вашей домашней.

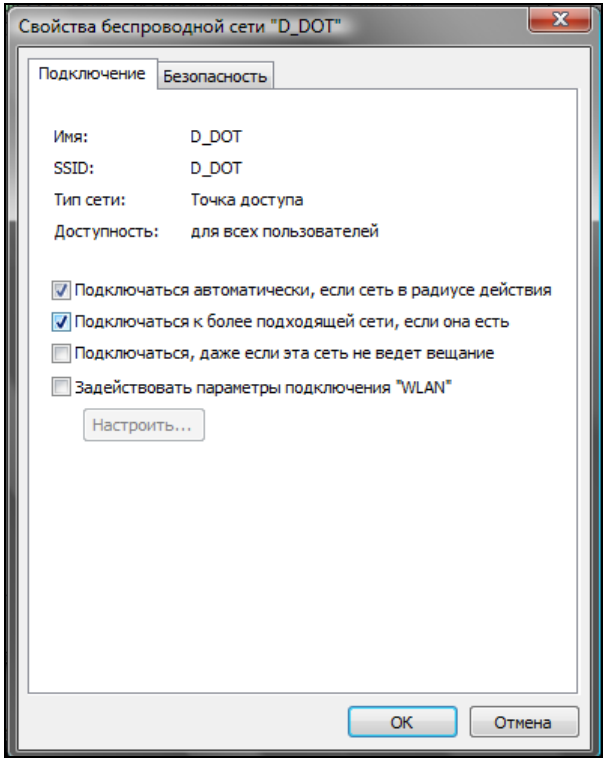


Рис. 4.14. Свойства подключения

На вкладке **Безопасность** (рис. 4.15) можно выбрать тип шифрования (WEP или WPA) и установить пароль для подключения к сети. Тип шифрования должен быть одинаковый на точке доступа и на всех клиентах сети. Обычно тип шифрования выбирается автоматически, но в случае надобности вы можете изменить его вручную.

Нажав кнопку **OK** или **Отмена**, вы вернетесь в окно, изображенное на рис. 4.13. Теперь нажмите кнопку **Сведения**. В открывшемся окне (рис. 4.16) можно просмотреть сведения о вашем беспроводном адаптере. Здесь отображается следующая информация:

- производитель беспроводного адаптера;
- физический адрес (MAC-адрес);

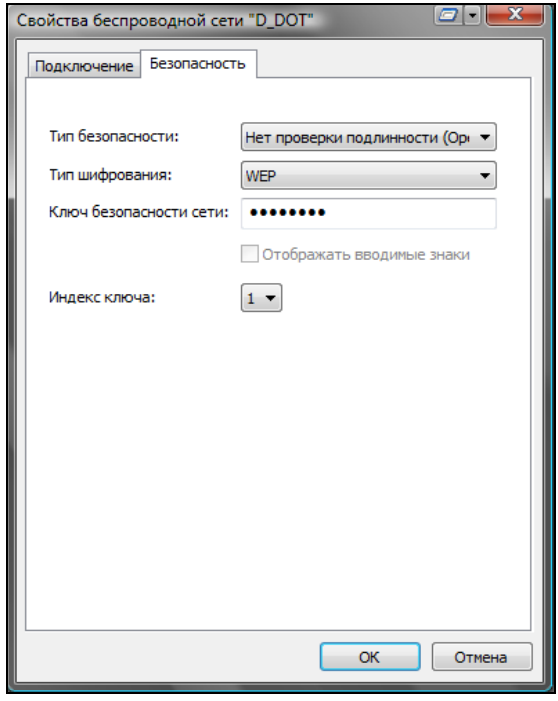


Рис. 4.15. Параметры безопасности

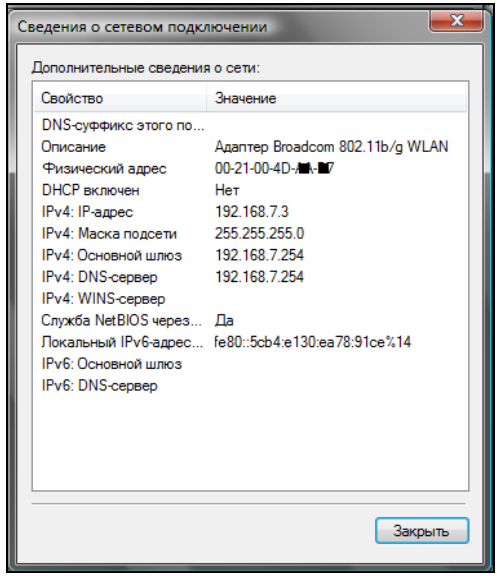


Рис. 4.16. Сведения о беспроводном подключении (свой MAC-адрес я скрыл)

- текущий IP-адрес (как IPv4, так и IPv6, если используется);
- маска подсети;
- IP-адреса шлюза и DNS-сервера.

Закройте окно сведений. Вы опять вернетесь в окно, изображенное на рис. 4.13. Теперь нажмите кнопку **Свойства беспроводной сети**. В открывшемся окне на вкладке **Сеть** (рис. 4.17) можно отключить сетевые протоколы и службы, которые не должны использоваться данным соединением. Например, если вы не планируете предоставлять пользователям сети свои собственные файлы и принтеры и не хотите использовать общие ресурсы сети (это тот случай, когда ваше соединение будет использоваться только для подключения к Интернету), нужно снять флажок **Служба доступа к файлам и принтерам сетей Microsoft**. Также практически всегда можно отключить **Протокол Интернета версии 6**.

На вкладке **Доступ** (рис. 4.18) вы можете определить, нужно ли предоставлять другим пользователям общий доступ к этому соединению. Для данного случая эту опцию также можно отключить.

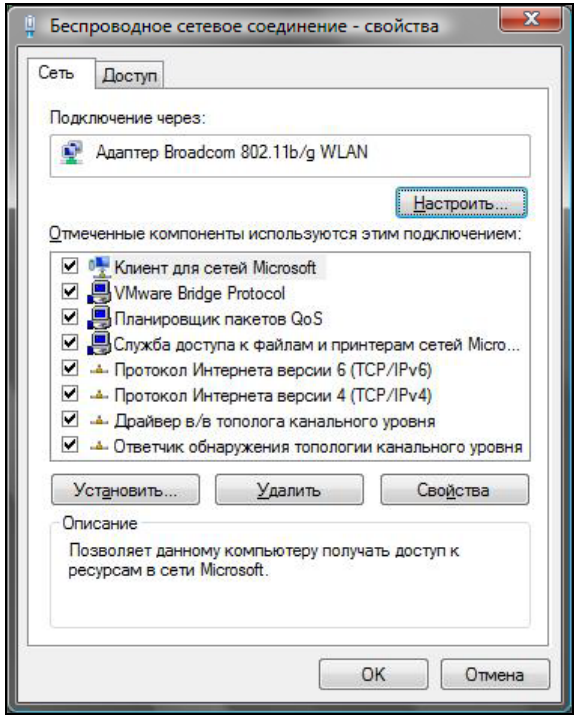


Рис. 4.17. Свойства беспроводного соединения

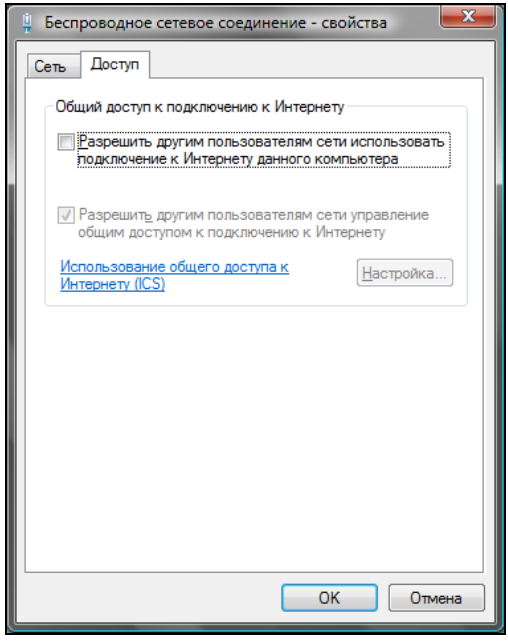


Рис. 4.18. Вкладка **Доступ**

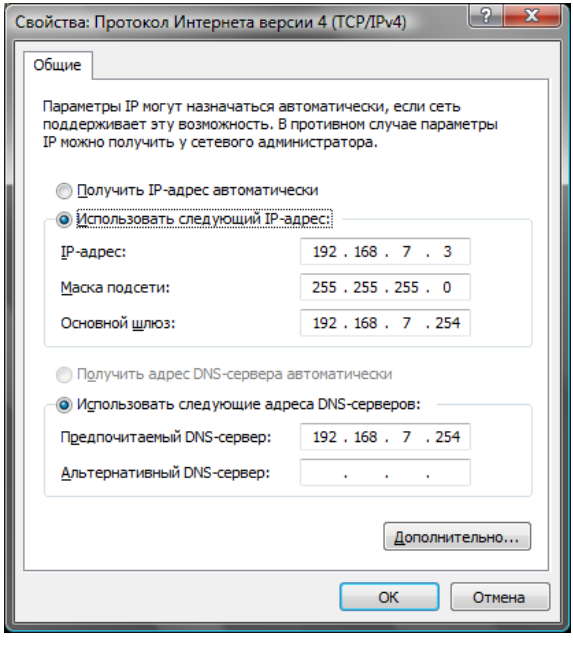


Рис. 4.19. Параметры TCP/IP

Обычно DHCP-сервер, работающий на точке доступа, предоставляет IP-адреса всем клиентам беспроводной сети. Однако иногда администратор настраивает ее так, что IP-адреса нужно указывать самостоятельно. Для этого перейдите на вкладку **Сеть** (см. рис. 4.17), выберите **Протокол Интернета версии 4** и нажмите кнопку **Свойства**. В открывшемся окне (рис. 4.19) вы можете указать IP-адрес компьютера, маску подсети, IP-адрес шлюза и IP-адреса первого и второго DNS-серверов.

Вернитесь в окно Центра управления сетями и общим доступом (рис. 4.20). Из списка **Задачи** (в левой части окна) выберите команду **Управление беспроводными сетями**. В открывшемся окне (рис. 4.21) вы можете просмотреть список беспроводных сетей, добавить новую сеть и изменить свойства беспроводного адаптера.

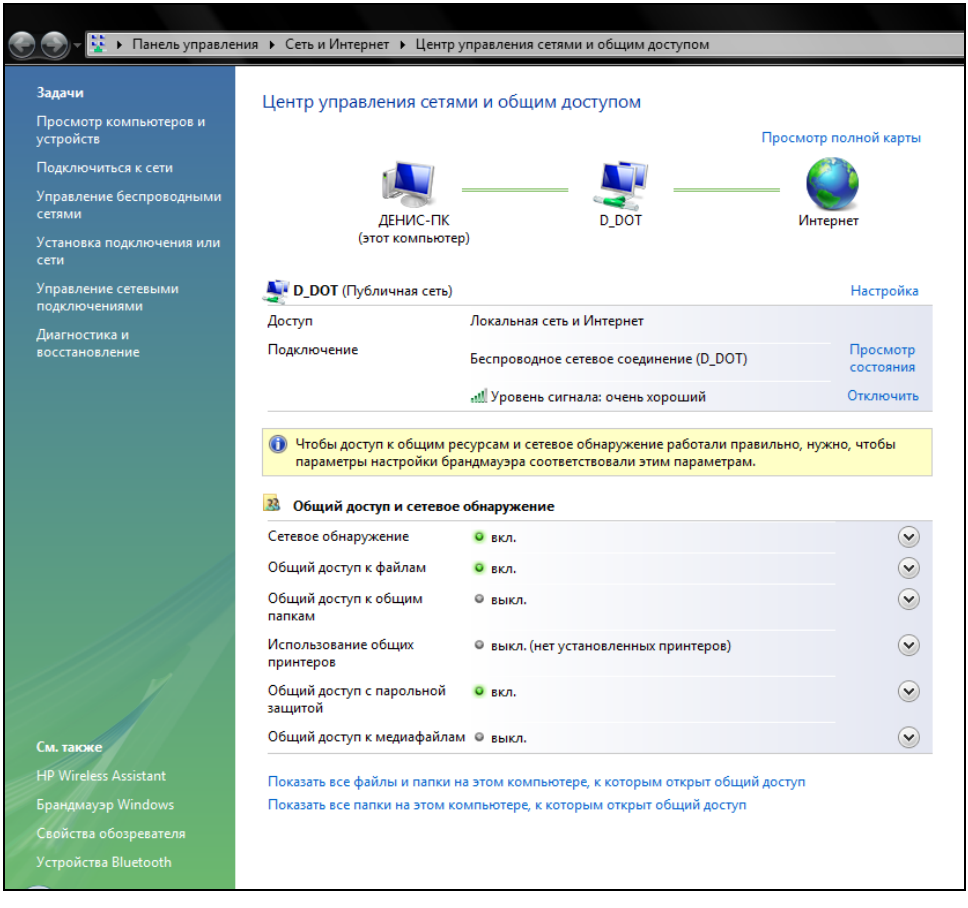


Рис. 4.20. Центр управления сетями и общим доступом (развернутое окно)

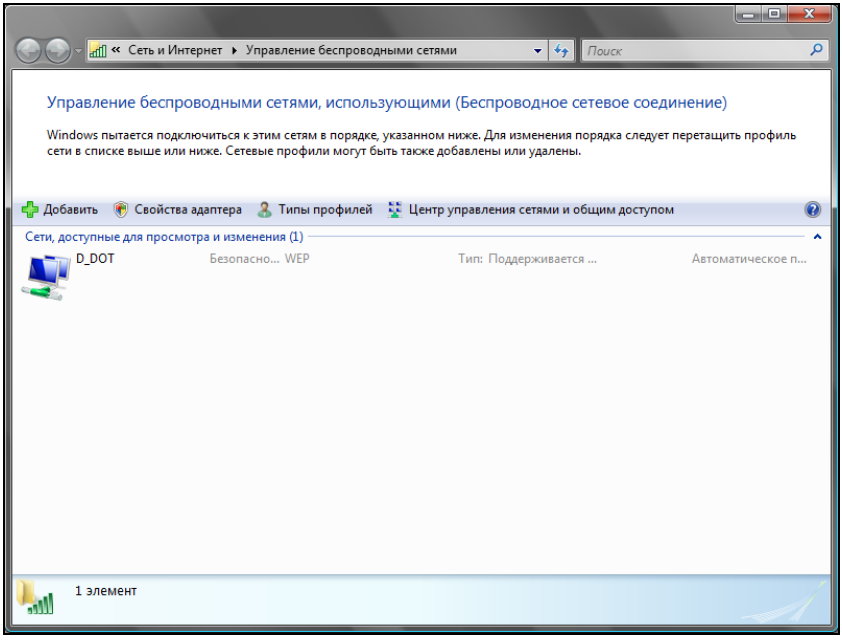


Рис. 4.21. Управление беспроводными сетями

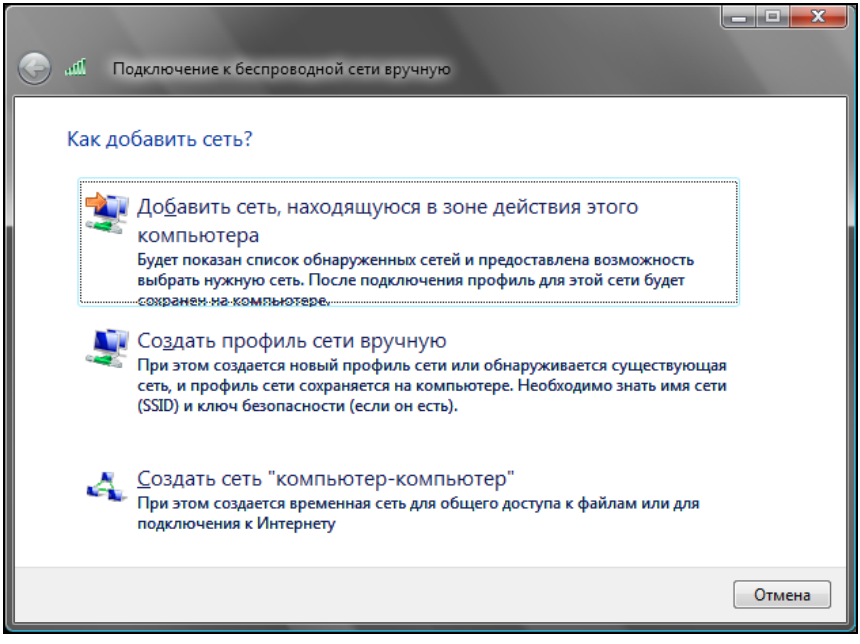


Рис. 4.22. Как добавить сеть?

Нажав кнопку **Добавить**, мы попадем в окно подключения к беспроводным сетям вручную (рис. 4.22). Здесь можно добавить сеть, в зоне действия которой находится ваш компьютер, а можно создать профиль сети вручную, но для этого нужно знать ее SSID и ключ безопасности (пароль). Дело тут в том, что некоторые администраторы отключают широковещание SSID, поэтому сеть не отображается в списке сетей, даже если компьютер находится в зоне ее действия. В этом случае, зная SSID и пароль, и можно добавить сеть вручную. В этом окне вы также можете создать сеть компьютер-компьютер для обмена данными между двумя компьютерами, оснащенными Wi-Fi-адаптерами.

В списке **Задачи** Центра управления сетями (см. рис. 4.20) есть еще одна полезная команда: **Диагностика и восстановление**. Если соединение "потерялось" без видимых причин, выполните эту команду. Даже если вы увидите сообщение **Неполадки сетевого подключения не обнаружены**, нажмите кнопку **Выполнить сброс сетевого адаптера "Беспроводное сетевое соединение"** (рис. 4.23).

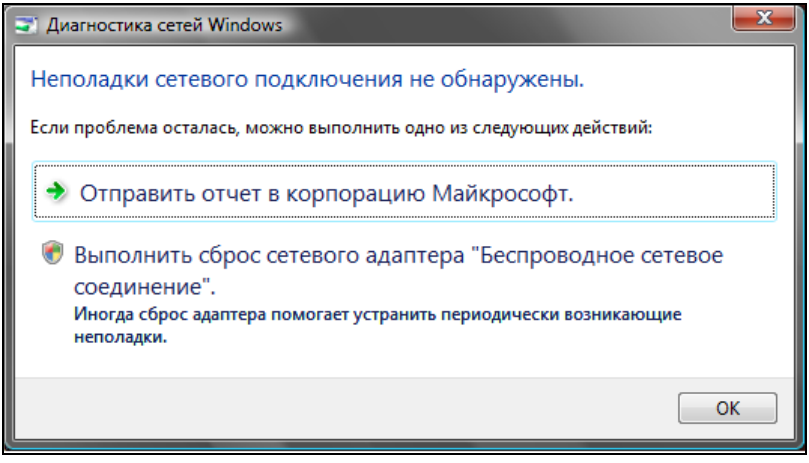


Рис. 4.23. Диагностика сети

Для настройки беспроводного соединения можно использовать не только инструменты Windows, но и утилиты, входящие в состав программного обеспечения беспроводного адаптера. В моем ноутбуке была установлена программа HP Wireless Assistant (рис. 4.24) — такая программа установлена на многих ноутбуках HP. Честно говоря, толку от нее мало. Да, вы можете отключить Bluetooth-модуль вашего адаптера, и тогда адаптер будет работать только в режиме Wi-Fi. Можно, наоборот, отключить Wi-Fi-модуль, если не

планируете его использовать. Теоретически, это поможет снизить энергопотребление, но на практике реального снижения не наблюдается (может, оно и есть, но не ощущается).

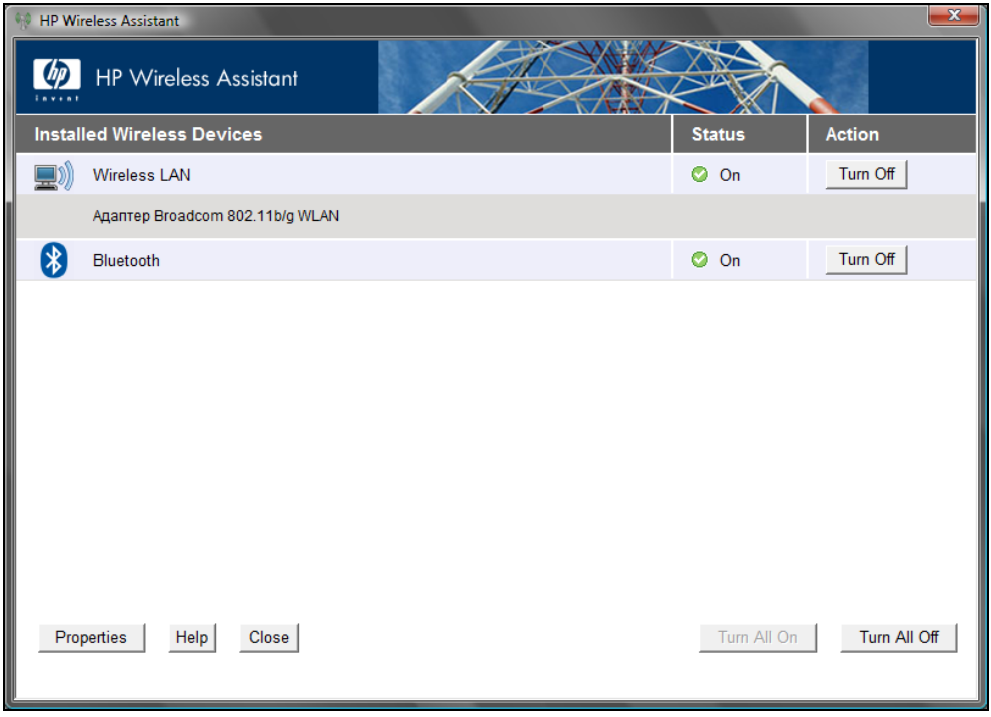


Рис. 4.24. HP Wireless Assistant

4.3. Подключение к сети Wi-Fi в Linux

О подключении к Wi-Fi-сети в Linux можно написать отдельную книжку. Небольшую, но все же книжку. Сложность настройки Wi-Fi заключается в том, что последовательность действий по настройке Wi-Fi в различных дистрибутивах разная. В этой главе мы рассмотрим настройку Wi-Fi в дистрибутивах Ubuntu 8.10/Denix/Fedora 10. Если на вашем компьютере установлен один из этих дистрибутивов, значит, в 99% случаев у вас не будет проблем с настройкой беспроводной сети. Если же у вас другой дистрибутив или старая версия одного из упомянутых (например, Ubuntu 8.10 или Fedora 8), тогда вам нужно или сменить/обновить дистрибутив, или же прочитать *разд. 4.3.2* — возможно, Wi-Fi и удастся настроить. А может получиться так,

что вы только провозитесь лишнее время, а потом все равно обновите версию дистрибутива.

> ***Примечание***
>
> Denix — дистрибутив, разработанный автором этой книги. Дистрибутив основан на Ubuntu 8.10, поэтому полностью совместим с ним. Подробно об этом дистрибутиве можно узнать по адресу **http://denix.dkws.org.ua**.

4.3.1. Простая настройка (Ubuntu 8.10/Denix/Fedora 10)

Включите ваш беспроводный адаптер и щелкните на значке соединения на панели GNOME. Из рис. 4.25 видно, что обнаружена сеть D_DOT, но автоматического подключения к ней не произошло, поскольку сеть защищена паролем. Справа от названия сети выводится индикатор уровня сигнала. Чуть ниже есть команды:

- **Подключиться к скрытой беспроводной сети** — для подключения к скрытой сети нужно знать ее SSID и пароль. Как уже отмечалось ранее, иногда администраторы из соображений безопасности отключают широковещание SSID, и сеть становится скрытой. Подключиться к такой сети можно, только если вы знаете SSID и пароль сети;
- **Создать новую беспроводную сеть** — можно создать одноранговую ad hoc-сеть (об этом мы поговорим в *главе 15*).

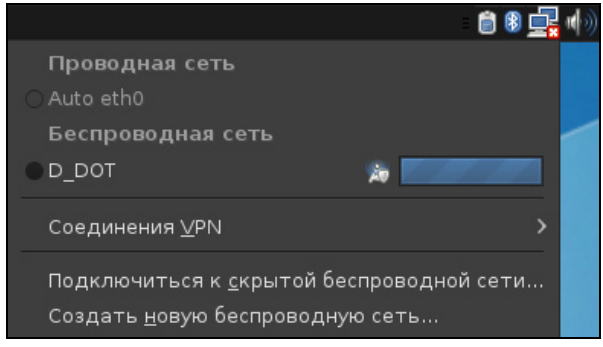


Рис. 4.25. Обнаружена защищенная паролем беспроводная сеть

Выберите сеть из списка, изображенного на рис. 4.25. Вы увидите окно ввода пароля (ключа) для подключения к сети (рис. 4.26). Если пароль правильный, вы увидите уведомление о подключении к сети (рис. 4.27).

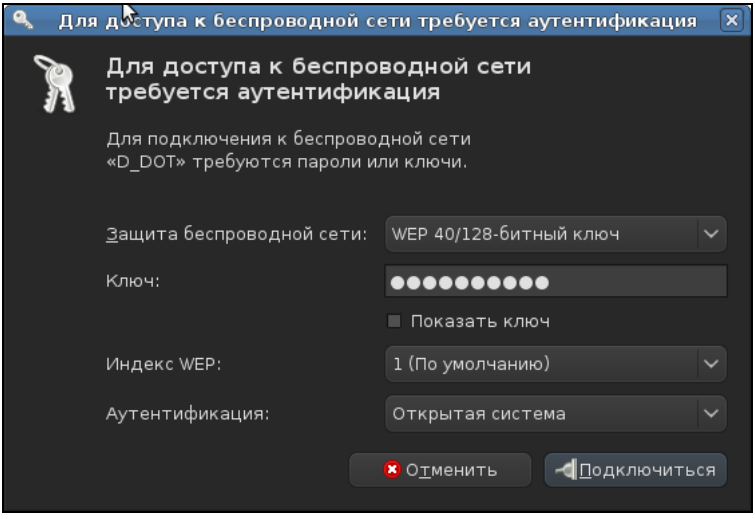


Рис. 4.26. Ввод пароля для подключения к сети

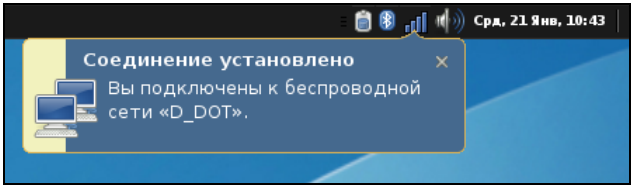


Рис. 4.27. Мы подключены к беспроводной сети

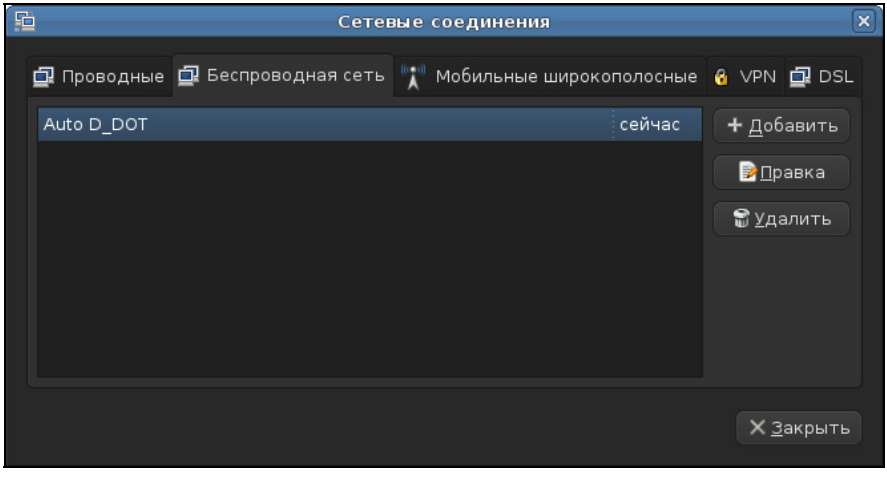


Рис. 4.28. Список беспроводных сетей

Список беспроводных сетей можно просмотреть, выполнив команду **Система | Параметры | Network Configuration** и перейдя на вкладку **Беспроводная сеть** (рис. 4.28).

Как видите, в современном дистрибутиве Linux беспроводная сеть настраивается так же легко, как и в Windows. В следующем пункте мы рассмотрим "тяжелый случай", когда нужно установить отсутствующий драйвер беспроводного адаптера.

4.3.2. "Тяжелый случай"

Когда я использовал дистрибутив Ubuntu 8.04, то по умолчанию определился только Bluetooth-адаптер, а вот чтобы заработал Wi-Fi-адаптер, пришлось повозиться. Хотя, может быть, вам повезет больше, чем мне, и ваш беспроводной адаптер будет определен по умолчанию или с наименьшими усилиями и затратами времени. На пошаговые инструкции здесь даже и не надейтесь. В этом разделе вы получите только минимально необходимый список средств, позволяющих настроить ваш беспроводной адаптер Wi-Fi.

Первым делом откройте терминал и введите команду `iwconfig`. Она покажет вам ваши беспроводные интерфейсы. Если беспроводной адаптер не обнаружен, тогда вы получите вывод, изображенный на рис. 4.29.

Вся проблема заключается в отсутствии подходящих драйверов беспроводных Wi-Fi-адаптеров для Linux. Основная ваша задача — сделать так, чтобы система увидела ваш беспроводный адаптер (далее просто адаптер) как сетевой интерфейс. Далее все настраивается довольно легко с помощью программы network-manager-gnome или другой утилиты, позволяющей задать параметры беспроводного доступа к сети (выбрать сеть, установить ее SSID, ввести пароль и т. д.).

Где взять драйверы? В некоторых случаях, драйверы уже будут в составе вашего дистрибутива. Все, что вам тогда нужно, — это просто настроить беспроводную сеть. Иногда драйвер адаптера можно найти на сайте производителя, но в большинстве случаев там вы найдете драйверы только для Windows.

Сожалею, но, скорее всего, Linux-драйверы вы не найдете. Впрочем, зная производителя адаптера, вы можете попытаться найти для него драйвер на сайте **http://linux-wless.passys.nl/**.

Если Linux-драйвера нет, тогда придется раздобыть Windows-драйверы. Как правило, их можно взять или на компакт-диске, который поставляется вместе с адаптером или ноутбуком, или на сайте производителя. В моем случае мне пришлось скачать драйвер для Windows XP с сайта HP.

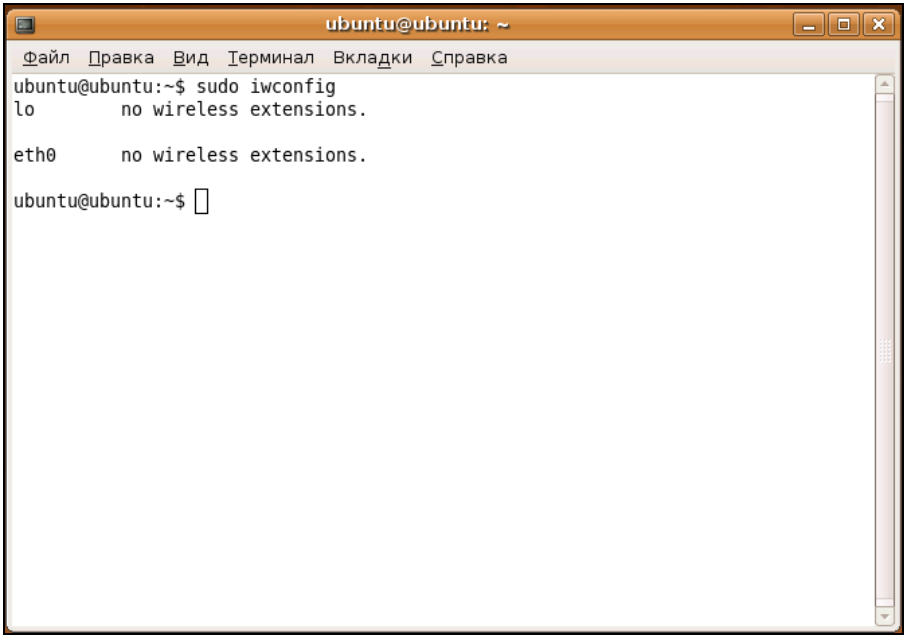


Рис. 4.29. Беспроводные адаптеры не обнаружены

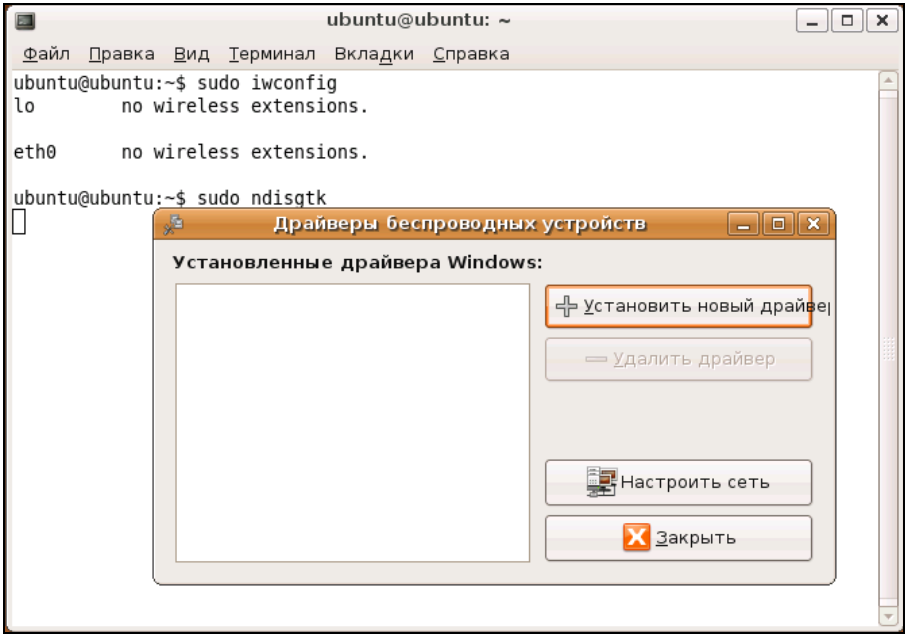


Рис. 4.30. Программа ndisgtk

Тут следует иметь в виду, что если для того или иного устройства имеются Windows-драйверы, то их тоже можно использовать в Linux с помощью программы ndiswrapper. Можете ее считать "эмулятором драйверов для Linux".

Итак, когда драйверы будут загружены, нужно установить программы ndiswrapper и ndisgtk (это графическая оболочка для ndiswrapper). Сделать это можно с помощью вашего менеджера пакетов. В большинстве случаев программа ndiswrapper или уже установлена в системе, или находится на дистрибутивном DVD, поэтому, даже если у вас нет соединения с Интернетом, программа все равно будет установлена.

Далее запустите программу ndisgtk и нажмите кнопку **Установить новый драйвер** (рис. 4.30). Затем нужно указать путь к INF-файлу драйвера (рис. 4.31).

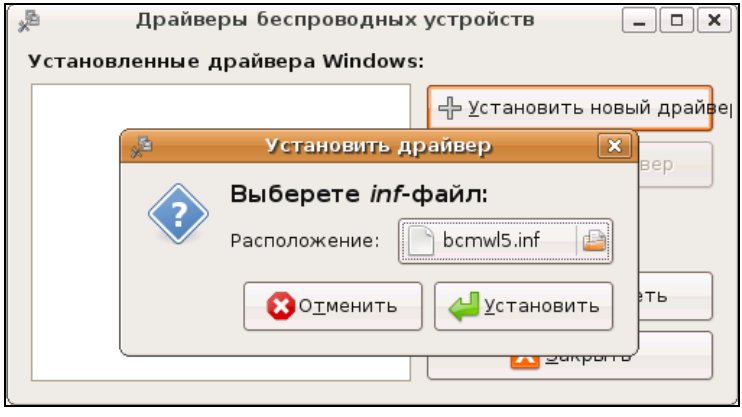


Рис. 4.31. Выберите INF-файл драйвера

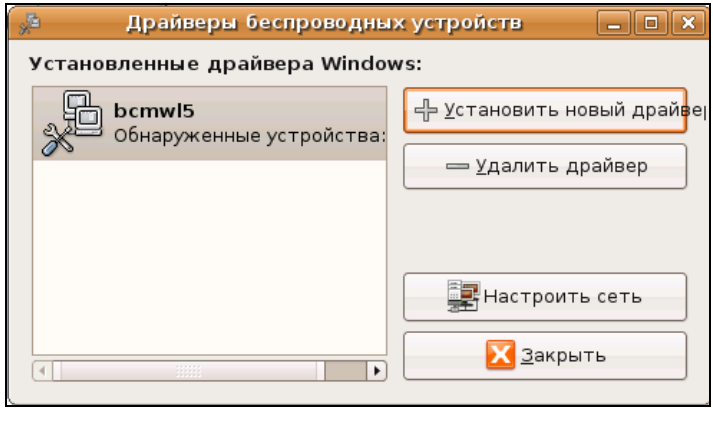


Рис. 4.32. Содержимое каталога, содержащего драйвер моего беспроводного адаптера

После этого драйвер появится в окне программы ndisgtk (рис. 4.32). Перезагрузите компьютер и введите команду `iwconfig wlan0`. Вы увидите примерно такой вывод:

```
iwconfig wlan0
```

wlan0 IEEE 802.11g ESSID:"MyHome.Net"

Mode:Managed Frequency:2.462 GHz Access Point: xx:xx:xx:xx:xx:xx

Bit Rate:54 Mb/s Tx-Power:10 dBm Sensitivity=0/3

RTS thr:4096 B Fragment thr:4096 B

Power Management:off

Link Quality:100/100 Signal level:-42 dBm Noise level:-128 dBm

Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0

Tx excessive retries:0 Invalid misc:0 Missed beacon:0

Теперь вам нужно щелкнуть правой кнопкой на значке сетевого соединения (он находится возле значка регулятора громкости и системной даты) и выбрать команду **Установить беспроводную сеть**. Используя открывшееся окно, вы без проблем подключитесь к сети.

У вас могут возникнуть сложности, как при установке драйвера, так и при настройке самого беспроводного интерфейса. Сначала рассмотрим набор команд, которые могут помочь настроить драйвер:

- `uname -a` — получить версию ядра. При установке настоящих Linux-драйверов (а не Windows-драйверов через ndiswrapper) нужно, чтобы *модуль* (так в Linux называются драйверы) был откомпилирован для соответствующей версии ядра;
- `lspci`, `lsusb`, `lshw` — помогают идентифицировать ваше устройство и выводят, соответственно, список PCI-устройств, список USB-устройств и список оборудования компьютера;
- `lsmod` — выводит список загруженных модулей (драйверов устройств).

Если у вас не получается установить драйвер имеющегося у вас устройства, можно попытаться приобрести и установить другой USB-адаптер, но перед покупкой убедитесь, что сможете его настроить.

Для настройки сетевого интерфейса пригодятся следующие команды:

- `iwconfig` — просмотреть информацию обо всех беспроводных интерфейсах;
- `iwlist scan` — найти беспроводные сети;

- `sudo dhclient wlan0` — обновить IP-адрес и другие сетевые параметры интерфейса wlan0 (имя может быть другим), предварительно получив их от DHCP-сервера;
- `route` — просмотр таблицы маршрутизации;
- `sudo /etc/init.d/networking restart` — перезапуск сети;
- `dmesg | less` — просмотреть сообщения ядра;
- `sudo killall NetworkManager` — остановить NetworkManager;
- `iwevent` — просмотреть события беспроводной сети;
- `sudo /etc/init.d/dbus restart` — перезапустить все сетевые демоны.

Глава 5

Подключаемся к Ethernet-сети

5.1. Физическое подключение к сети

В этой книге мы не будем рассматривать совсем уж старые сети, основанные на коаксиальном кабеле (правда, в *главе 9* мы с ними в общих чертах познакомимся — для общего развития). Также мы не будем рассматривать Ethernet-сети на базе оптоволоконного кабеля — они сложны в монтаже, а стоимость оптоволоконного кабеля все еще высока. Нам остаются сети на базе витой пары: 100Base-T и 1000Base-T. Как было отмечено ранее, стандарт 100Base-T обеспечивает максимальную скорость передачи данных 100Мбит/с, а 1000Base-T — 1000 Мбит/с. Напомню, чтобы ваша сеть работала со скоростью 1000 Мбит/с, нужно установить сетевые адаптеры и коммутатор, поддерживающие Gigabit Ethernet.

Для физического подключения к Ethernet-сети понадобится несколько метров витой пары, обжатой с двух сторон разъемами RJ-45 (рис. 5.1). В *главе 10* мы подробно поговорим о том, как сделать такой кабель самостоятельно, а пока будем считать, что вы его купили в магазине. В магазинах продаются уже готовые кабели разной длины — от 1 до 10 метров. Более короткий кабель не допускается стандартом Ethernet, а более длинный, как правило, нужно изготавливать под заказ (или самостоятельно, *см. главу 10*).

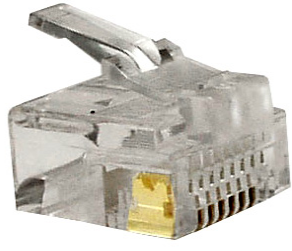


Рис. 5.1. Разъем RJ-45 для витой пары

Один разъем RJ-45 кабеля нужно подключить к сетевому адаптеру, а другой (на "той стороне" кабеля) — к коммутатору. Кабели можно подключать/отключать при работающем компьютере/коммутаторе — выключать компьютер при подключении или отключении кабеля совсем не обязательно.

После подключения кабеля обязательно посмотрите на индикаторы на сетевом адаптере и коммутаторе. На сетевом адаптере могут быть один или два индикатора. На коммутаторе обычно есть как минимум два индикатора для первого порта. Предположим, вы подключили ваш компьютер к первому порту коммутатора. В идеальном случае на коммутаторе должны гореть два имеющихся индикатора. Первый говорит о том, что к порту подключен компьютер (если он мигает, значит, идет обмен данными), а второй — о том, что порт работает на полной скорости (100 Мбит/с для сети 100Base-T и 1000Мбит/с для сети 1000Base-T). Конечно, на коммутаторе могут иметься и дополнительные индикаторы для каждого порта. Например, на некоторых коммутаторах индикатор связи (Link) совмещен с индикаторами активности, а на некоторых имеются целых три индикатора вместо этого одного:

- Link — если этот индикатор горит зеленым цветом, значит, к порту подключен кабель;
- Receive — мигает зеленым, если порт получает данные;
- Transmit — мигает зеленым, если порт отправляет данные.

Индикатор, сигнализирующий о том, что порт работает на полной скорости, обычно называется 100M или 1000M (в зависимости от поддерживаемого стандарта). Иногда на коммутаторе имеется также индикатор Collision. Если он мигает оранжевым цветом, то с данным портом возникла *коллизия* — так называется попытка одновременной передачи данных. Обычно в случае возникновения коллизии мигают два каких-то индикатора порта. Поскольку коллизия в современных сетях на базе коммутаторов — явление достаточно редкое, индикатор коллизии на современных коммутаторах практически всегда отсутствует.

Вы подключили кабель, но не горит индикатор связи (Link)? Сему могут быть две причины: повреждение кабеля или недостаточный контакт. Поскольку кабель мы только что купили в магазине (а не делали сами), то дефект кабеля исключаем. Отключите кабель и подключите его еще раз — до щелчка.

После физического подключения кабеля осталось произвести настройку операционной системы.

Примечание

Нужно отметить, что если в вашей сети используется DHCP-сервер (например, на маршрутизаторе), то можно больше ничего и не настраивать — все сетевые параметры будут автоматически установлены DHCP-сервером. Так что два последующих раздела вы можете спокойно пропустить.

5.2. Настройка сети в Windows XP

Выполните команду меню **Пуск | Настройка | Сетевые подключения**. В открывшемся окне (рис. 5.2) щелкните правой кнопкой мыши на значке **Подключение по локальной сети** и выберите команду **Свойства**.

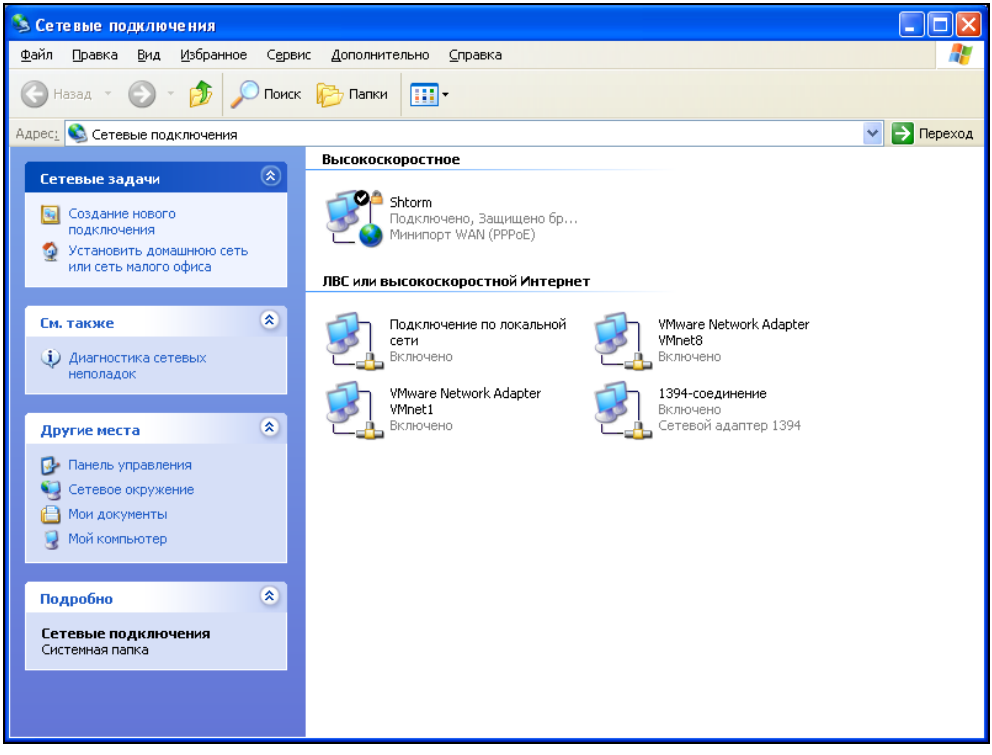


Рис. 5.2. Сетевые подключения

На вкладке **Общие** окна свойств соединения (рис. 5.3) можно настроить компоненты, используемые этим подключением:

- **Клиент для сетей Microsoft** — позволяет компьютеру получать доступ к ресурсам сети Microsoft;

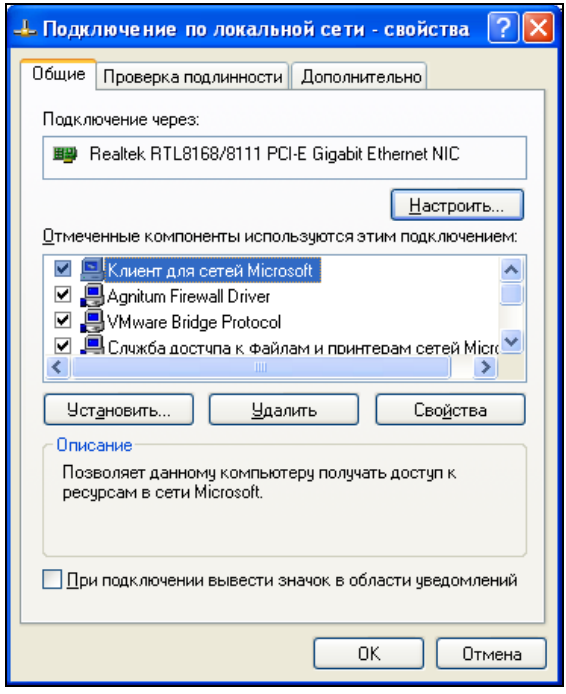


Рис. 5.3. Компоненты сетевого подключения

- **Служба доступа к файлам и принтерам сетей Microsoft** — если вы хотите не только использовать ресурсы сети Microsoft, но и предоставлять собственные ресурсы другим компьютерам сети, тогда не отключайте этот компонент;
- **Agnitum Firewall Driver** — этот компонент у вас появится, только если в системе установлен брандмауэр Outpost Security Suite Pro;
- **VMware Bridge Protocol** — скорее всего, у вас этого компонента не будет (он появляется после установки виртуальной машины VMware);
- **Планировщик пакетов QoS** — резервирует пропускную способность сети, об этом компоненте мы поговорим в *главе 23*;
- **Протокол Интернета (TCP/IP)** — сейчас мы займемся настройкой именно этого компонента.

Выделите компонент **Протокол Интернета** и нажмите кнопку **Свойства**. Откроется окно свойств протокола TCP/IP (рис. 5.4). По умолчанию система настроена на автоматическое получение IP-адреса. Установите переключатель **Использовать следующий IP-адрес**. Вот теперь нужно вручную установить сетевые параметры, а именно: IP-адрес, маску сети и основной шлюз.

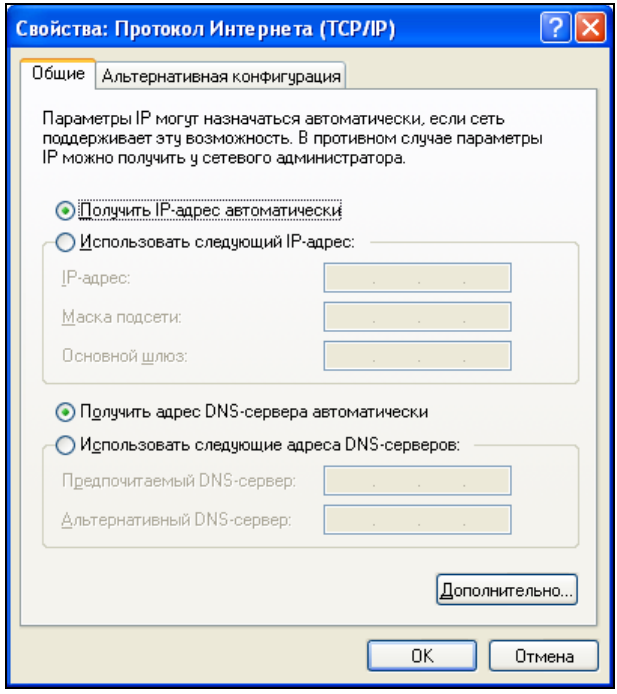


Рис. 5.4. Параметры протокола TCP/IP

Если вы подключаетесь к уже настроенной сети, то сетевые параметры можно узнать у системного администратора. А вот если вы сам себе администратор, то должны установить эти параметры самостоятельно. В локальной сети (как было отмечено в *главе 3*) можно использовать локальные адреса сетей классов A, B и C. Рекомендую использовать адреса вида 192.168.1.*N*, где *N* — номер компьютера вашей сети (он должен быть уникальным для каждого компьютера) и маску подсети 255.255.255.0. Шлюз по умолчанию пока можно не устанавливать — ведь пока в вашей сети нет маршрутизатора, и она не подключена к Интернету. Точно так же на этом этапе (пока ваша сеть не подключена к Интернету) можно не устанавливать и параметры DNS-серверов. Но вы должны знать, как их установить, когда вам это понадобится.

5.3. Настройка сети в Windows Vista

Откройте Панель управления, выберите опцию **Сеть и Интернет**, а затем — **Центр управления сетями и общим доступом** (рис. 5.5). В открывшемся окне (рис. 5.6) выберите задачу **Управление сетевыми подключениями**. Откроется окно, содержащее все имеющиеся сетевые подключения (рис. 5.7).

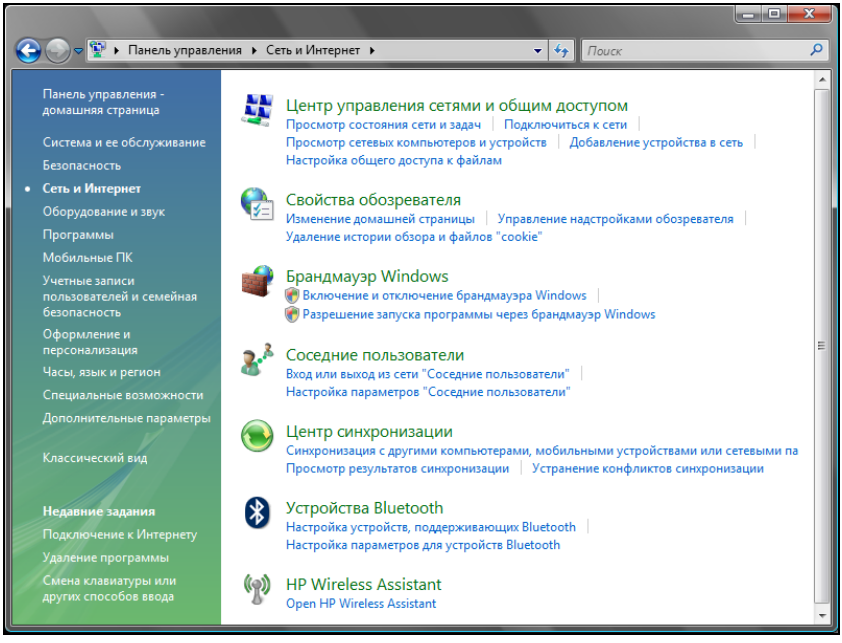


Рис. 5.5. Сеть и Интернет

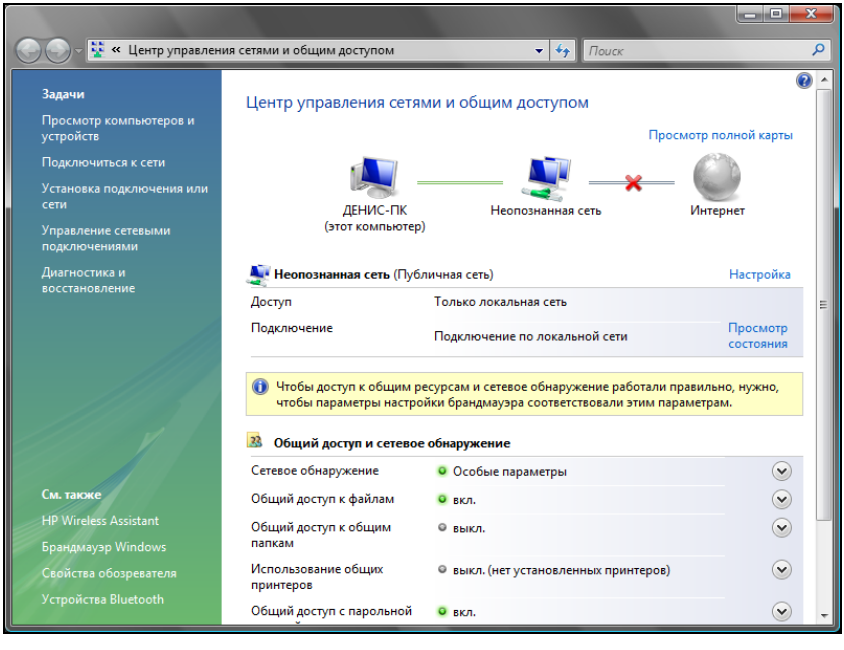


Рис. 5.6. Центр управления сетями и общим доступом

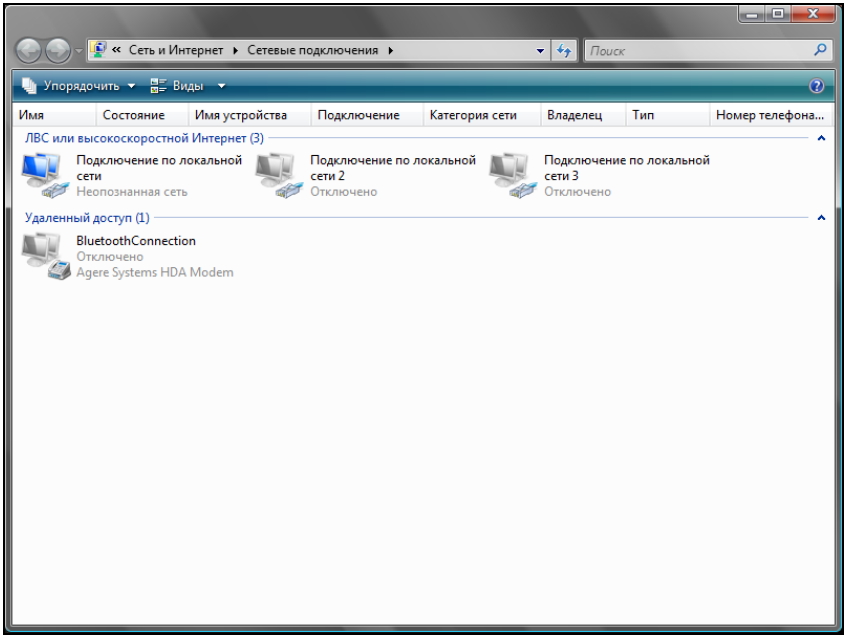


Рис. 5.7. Управление сетевыми подключениями

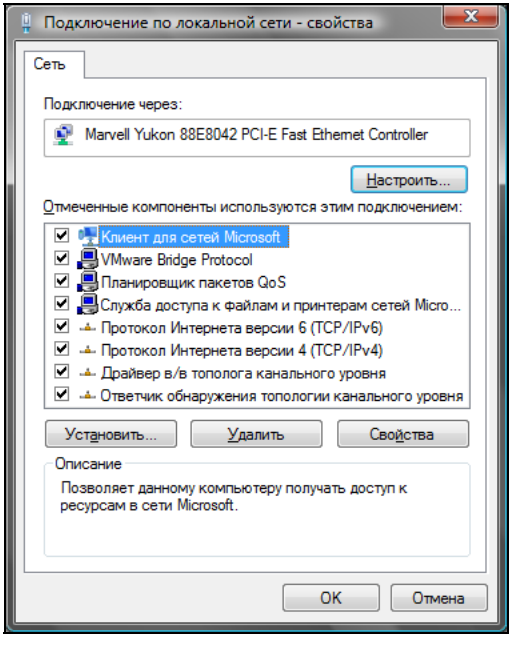


Рис. 5.8. Компоненты сетевого подключения

Далее ход настройки похож на настройку Windows XP — нужно выбрать **Подключение по локальной сети** (в окне на рис. 5.7 оно обозначено как **Неопознанная сеть**), нажать правую кнопку мыши и в открывшемся контекстном меню выбрать команду **Свойства**. Обратите внимание, что в списке компонентов сетевого подключения (рис. 5.8) появился **Протокол Интернета версии 6 (TCP/IPv6)**. Windows XP не поддерживает IPv6, поэтому, если ваша сеть использует новую версию протокола IP (впрочем, в этом я сомневаюсь), вам нужно использовать Windows Vista или Linux — эти операционные системы обладают поддержкой IPv6.

Как и в случае с Windows XP, выберите **Протокол Интернета версии 4**, нажмите команду **Свойства** и в открывшемся окне свойств протокола (рис. 5.9) введите IP-адрес, сетевую маску и адрес шлюза.

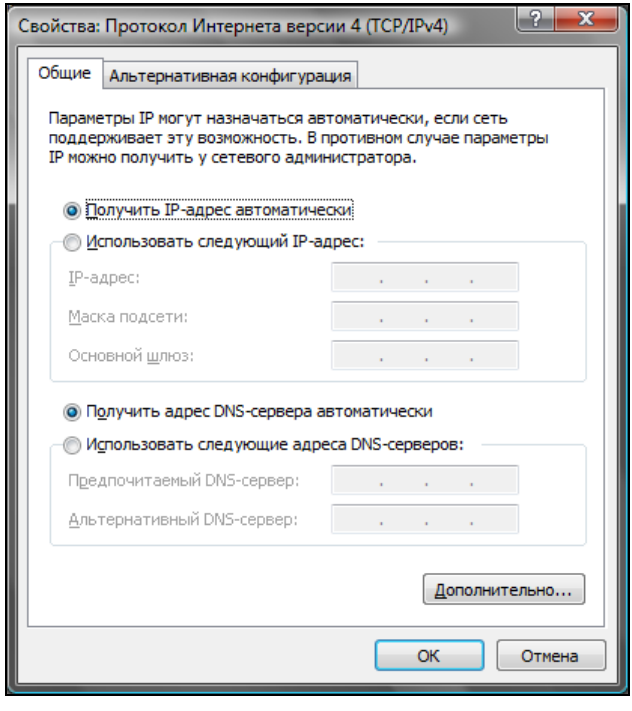


Рис. 5.9. Установка IP-адреса в Windows Vista

Примечание

Еще раз отмечу, что если в сети развернут DHCP-сервер, система не нуждается в такой настройке.

5.4. Настройка сети в Linux

Последовательность действий по настройке локальной сети в Linux зависит от используемого вами дистрибутива. В этой книге мы рассмотрим настройку локальной сети в трех популярных дистрибутивах: Fedora 10, openSUSE 11 и Ubuntu 8.10.

5.4.1. Fedora 10

В дистрибутиве Fedora сеть настраивается конфигуратором system-network-config, но в последних версиях (9 и 10) перед настройкой сети нужно заменить сервис NetworkManager (который почему-то работает не так, как бы нам этого хотелось) на уже проверенный временем сервис network, обеспечивающий поддержку сети. Для этого откройте терминал (**Приложения | Системные | Терминал**) и введите следующие команды:

```
# su
# /etc/init.d/NetworkManager stop
# /sbin/chkconfig --level 35 NetworkManager off
# /etc/init.d/network start
Bringing up loopback interface:                    [  OK  ]
Bringing up interface eth0:                        [  OK  ]
Bringing up interface isp:                         [  OK  ]
# /sbin/chkconfig --level 35 network on
```

После этого можно приступить к обычной настройке локальной сети. Введите команду:

```
# system-config-network
```

Откроется окно конфигуратора сети. Если соединение по локальной сети уже у вас создано (что происходит при загрузке), выделите его и нажмите кнопку **Изменить**. После чего установите параметры сети.

Если же соединений в окне конфигуратора сети нет, нажмите кнопку **Создать**, а затем выберите **Соединение Ethernet** и нажмите кнопку **Далее** (рис. 5.10).

Следующий шаг — это выбор сетевой платы (рис. 5.11). Выделите сетевую плату, через которую осуществляется настраиваемое соединение с сетью. Если у вас всего одна сетевая плата, выбирать вам не придется.

Теперь введите параметры сети: IP-адрес, маску сети и IP-адрес шлюза по умолчанию (рис. 5.12).

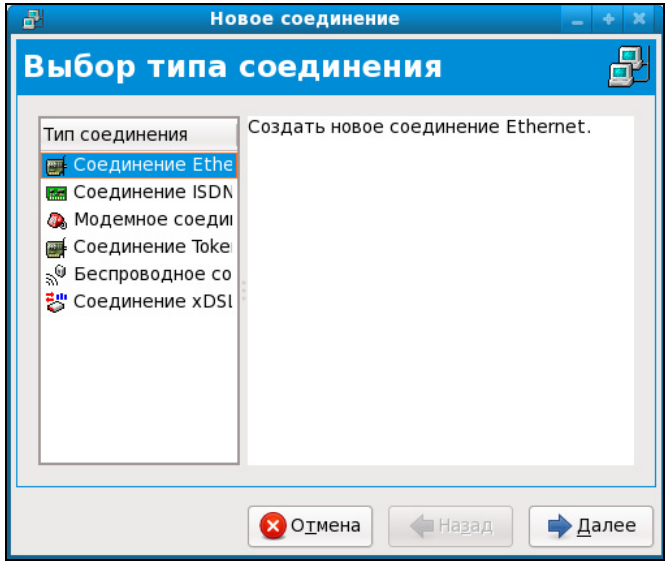


Рис. 5.10. Создание Ethernet-соединения

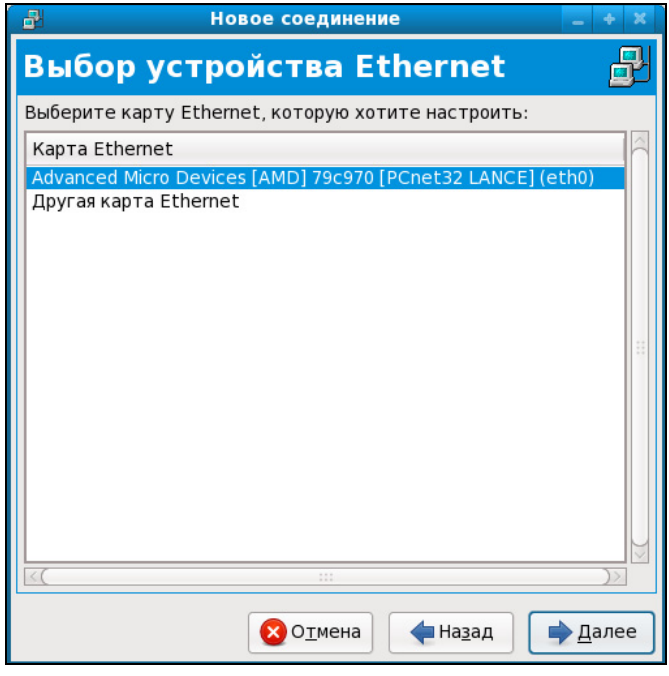


Рис. 5.11. Выбор сетевой платы

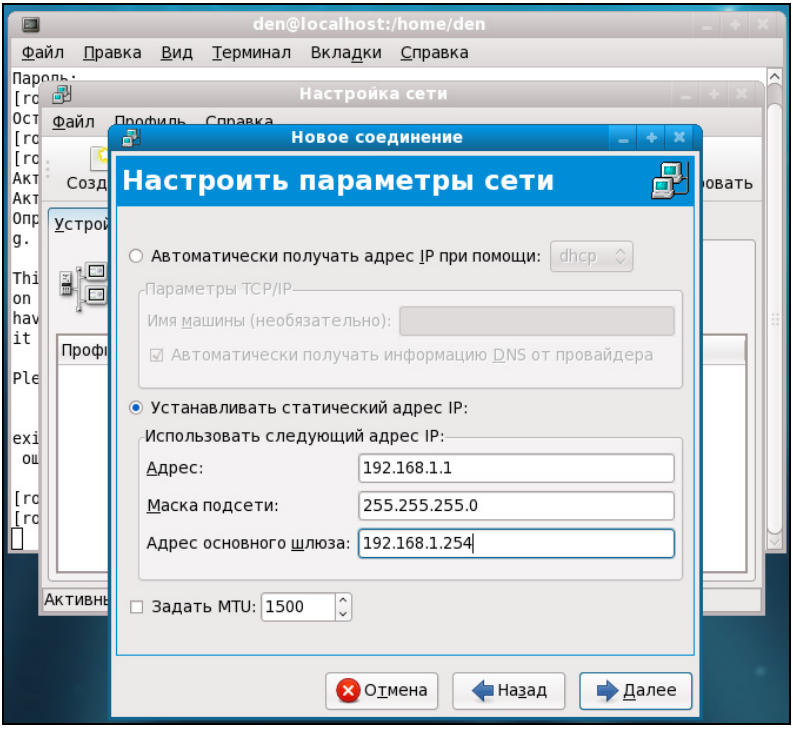


Рис. 5.12. Ввод параметров сети

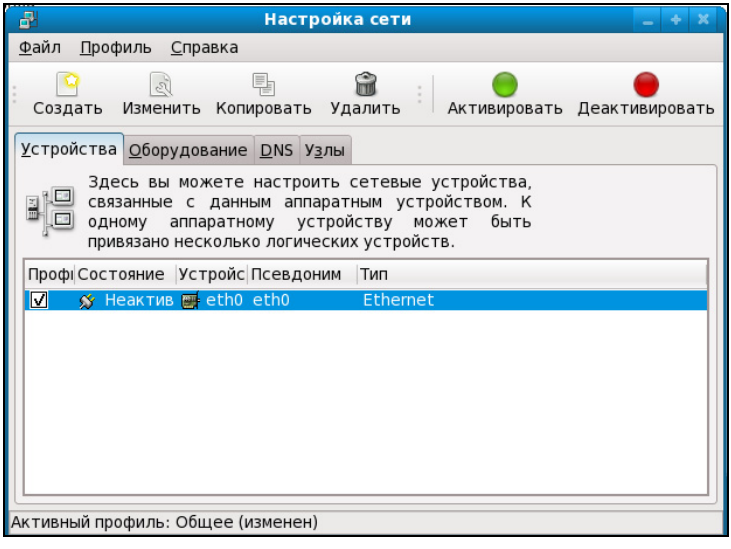


Рис. 5.13. Основное окно конфигуратора сети

На этом настройка сетевого интерфейса завершена. Проверьте введенные вами данные и, если все правильно, нажмите кнопку **Далее**. Откроется основное окно **Настройка сети** конфигуратора сети system-config-network, в котором будет отображен только что созданный вами интерфейс (рис. 5.13).

Сразу после настройки сетевой интерфейс неактивен. Нажмите кнопку **Активировать** для его активации. Изменить параметры интерфейса можно, нажав кнопку **Изменить**. В открывшемся окне (рис. 5.14) вы сможете изменить различные параметры сети, в том числе выбрать использование протокола DHCP для автоматического конфигурирования интерфейса.

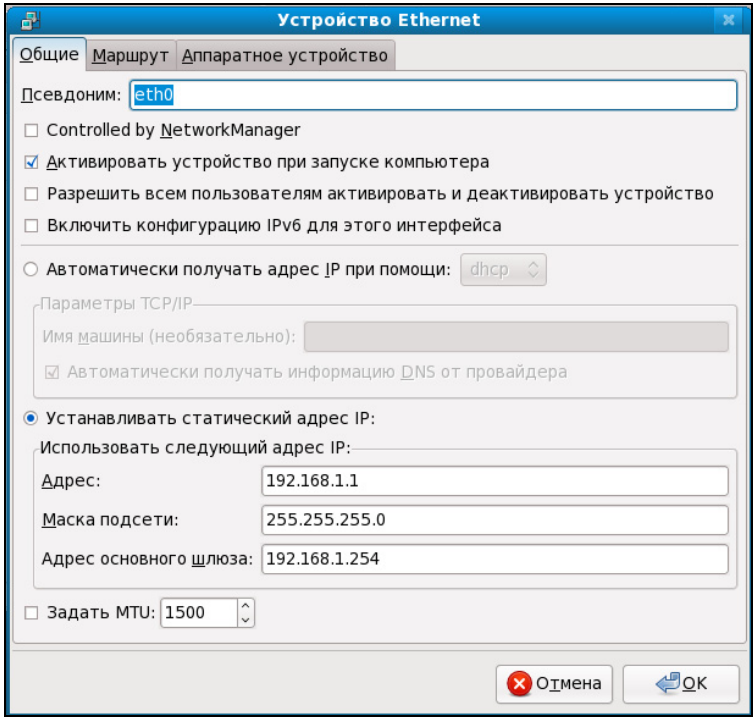


Рис. 5.14. Изменение параметров сети

Конфигураторы сети в других дистрибутивах, например, конфигуратор drakconf в Mandriva позволяет установить параметры DNS сразу при конфигурировании каждого сетевого интерфейса. С одной стороны — это удобно. С другой — несколько неправильно, потому что установки DNS общие для всех интерфейсов. Если вы зададите одни параметры DNS при настройке одного интерфейса и совершенно другие параметры DNS при настройке другого интерфейса, последние указанные параметры перезапишут параметры,

заданные ранее. Разработчики Fedora поступили правильно — они вынесли параметры DNS на отдельную страничку конфигуратора (рис. 5.15).

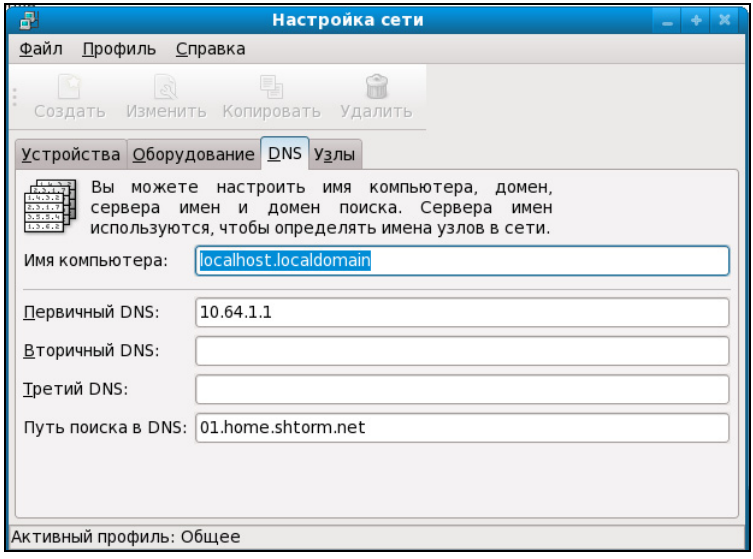


Рис. 5.15. Редактирование параметров DNS

На вкладке **DNS** (см. рис. 5.15) вы можете установить имя локального узла, IP-адреса трех серверов DNS.

> ***Примечание***
>
> Для тех, кто любит и умеет работать непосредственно с конфигурационными файлами Linux, отмечу, что при непосредственной правке файла /etc/resolv.conf можно записать не три, а четыре директивы `nameserver`, а также указать путь поиска домена (директива `search`).

Вкладка **Узлы** (рис. 5.16) предоставляет возможность редактирования файла /etc/hosts, в котором хранятся соответствия IP-адресов доменным именам. В данный файл для ускорения процесса разрешения доменного имени можно внести IP-адреса, к которым вы обращаетесь чаще всего, например, **www.mail.ru**, **www.google.com** и т. д. Только не забывайте со временем обновлять эту информацию, поскольку IP-адреса могут периодически меняться.

Для добавления записи в файл /etc/hosts нажмите кнопку **Создать**. Откроется небольшое окошко (рис. 5.17), в котором нужно будет ввести IP-адрес узла, его доменное имя и псевдоним (обычно — сокращенное имя). Например, если имя узла **den.mycompany.com.ru**, то сокращенное имя можно установить типа `den`.

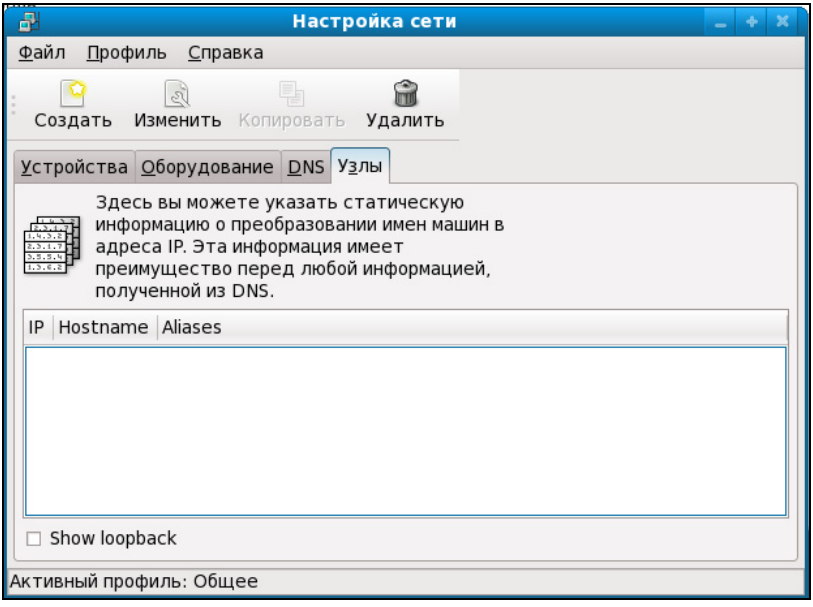


Рис. 5.16. Редактирование файла /etc/hosts

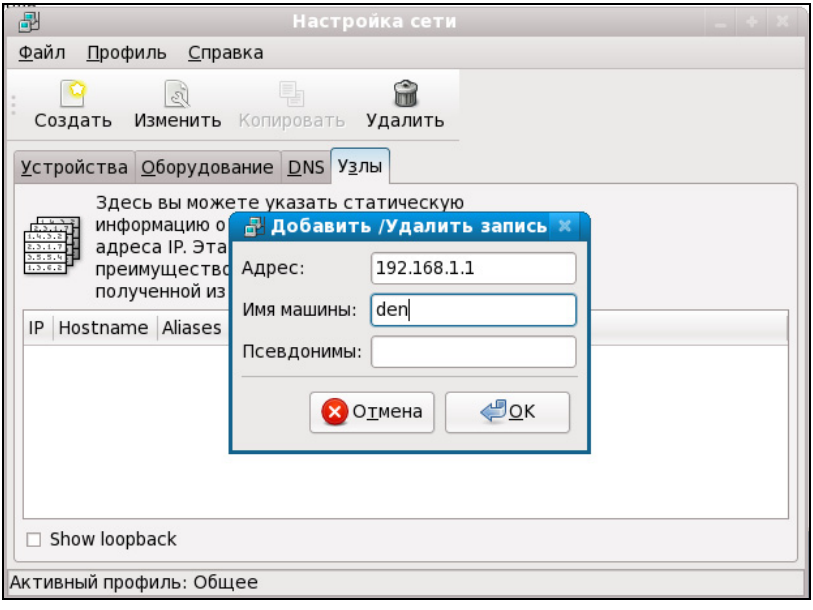


Рис. 5.17. Добавление записи в /etc/hosts

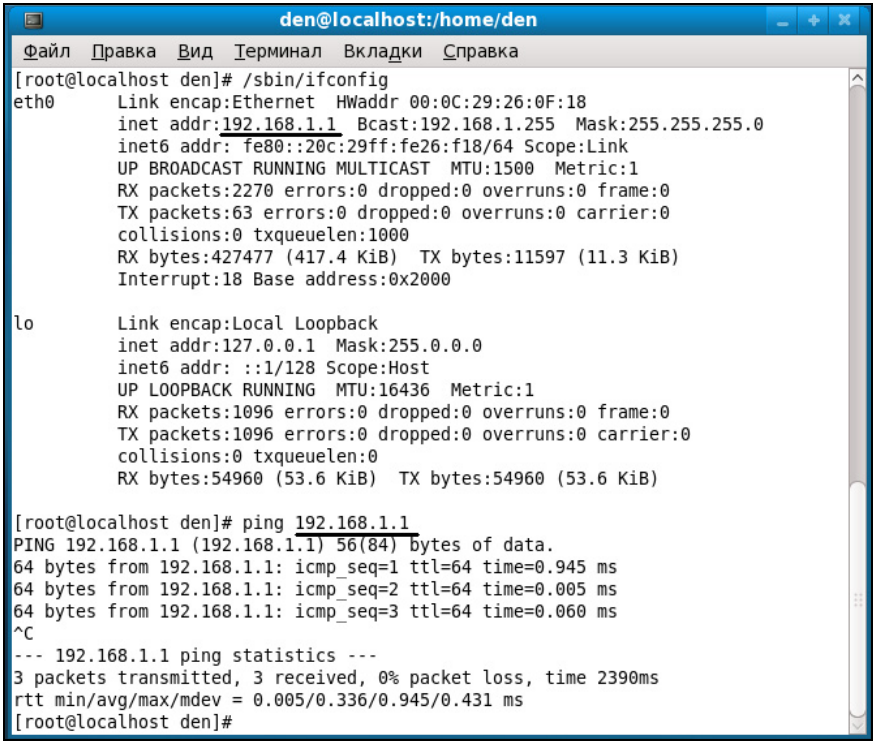


Рис. 5.18. Тестирование соединения

Настало время проверить работу сетевого интерфейса. Для этого сначала введем команду `/sbin/ifconfig`, чтобы убедиться, что сетевой интерфейс активен, а затем пропингуем (рис. 5.18) сетевой интерфейс по его адресу, который вы узнаете из вывода команды `ifconfig`, хотя и так должны его помнить — ведь вы только что настраивали сеть! Команду `ifconfig` в случае использования в сети DHCP-сервера нужно вводить обязательно — вы же не знаете, какой IP-адрес назначит вашему компьютеру сервер.

Во многих организациях доступ к Интернету осуществляется через *прокси-сервер*. Это означает, что кроме указания параметров сетевого интерфейса, нужно еще указать параметры прокси-сервера. Для этого выберите команду **Система | Параметры | Интернет и сеть | Сетевая прокси-служба**. В открывшемся окне (рис. 5.19) выберите **Ручная настройка прокси-службы** и введите адрес прокси-сервера и номер порта (обычно 3128 или 8080). Эти параметры вы можете уточнить у администратора сети. Если ваш прокси-сервер требует авторизации, тогда нажмите кнопку **Подробнее** и введите имя пользователя и пароль для подключения к прокси-серверу (рис. 5.20).

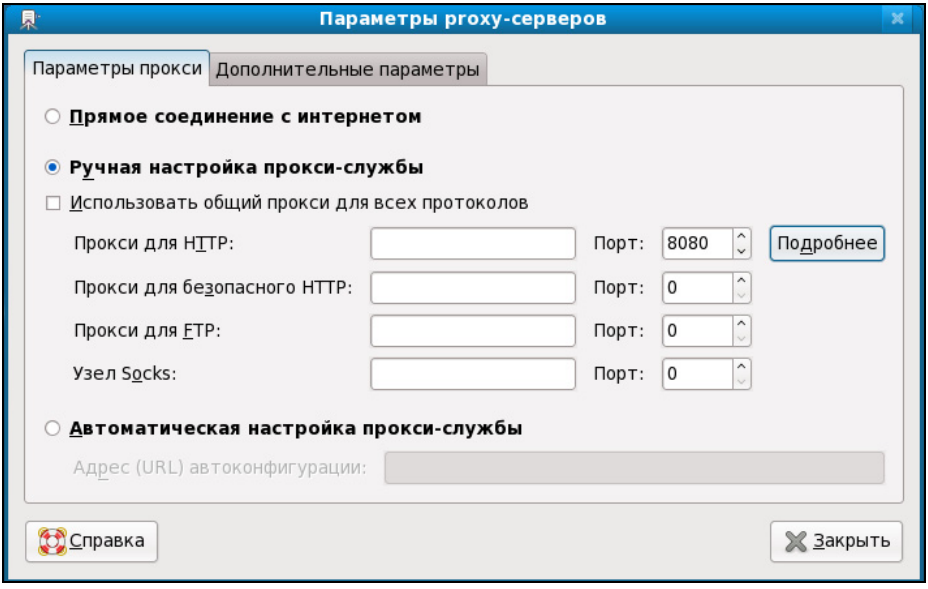


Рис. 5.19. Настройка прокси-сервера

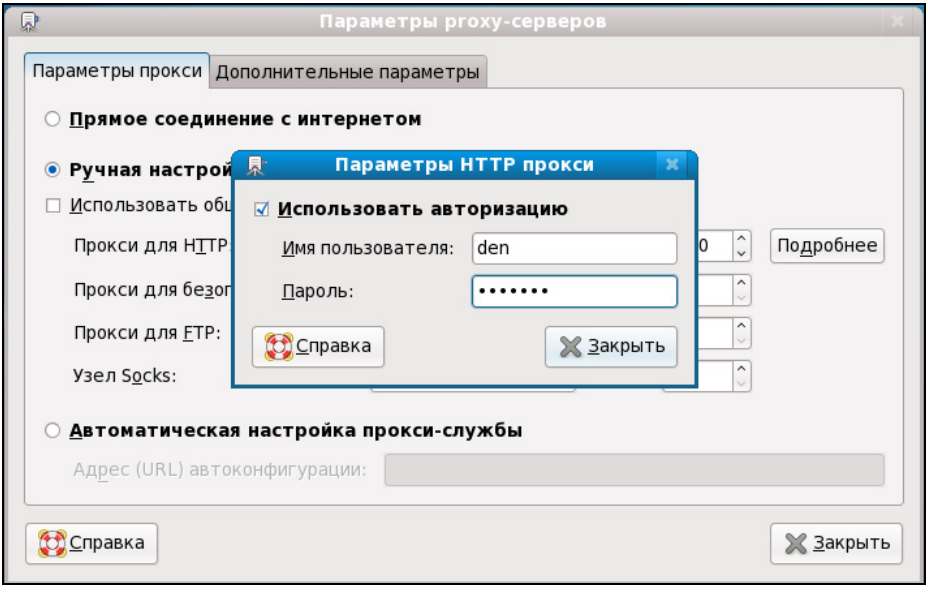


Рис. 5.20. Авторизация на прокси-сервере

5.4.2. openSUSE 11

Запустите **YaST** и выберите конфигуратор **Сетевые настройки** или запустите конфигуратор сети командой `/sbin/yast2 lan`.

В открывшемся окне конфигуратора (рис. 5.21) выберите сетевую плату и нажмите кнопку **Настройка**. В открывшемся окне (рис. 5.22) на вкладке **Адрес** вы можете задать IP-адрес сетевой платы, маску подсети и имя компьютера (**Hostname**). Понятно, что нужно выбрать режим **Статически присвоенный IP-адрес**.

Нажмите кнопку **Далее** — вы вернетесь в окно сетевых настроек. Перейдите на вкладку **Имя узла/DNS** (рис. 5.23). Здесь вы можете указать имя компьютера, имя домена, а также IP-адреса DNS-серверов.

Затем перейдите на вкладку **Маршрутизация** (рис. 5.24). На ней вы сможете задать IP-адрес шлюза — без этого не подключиться к Интернету. Вообще по поводу настройки Интернета по локальной сети вам нужно проконсультироваться с администратором сети. Если же вы сам себе администратор, то должны знать, что делаете.

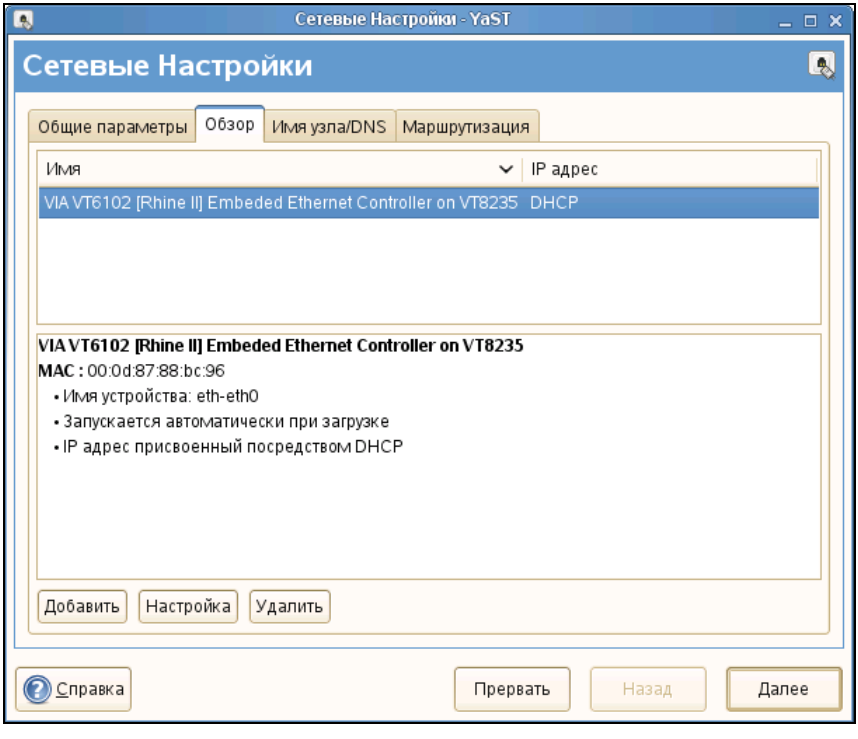


Рис. 5.21. Конфигуратор сети

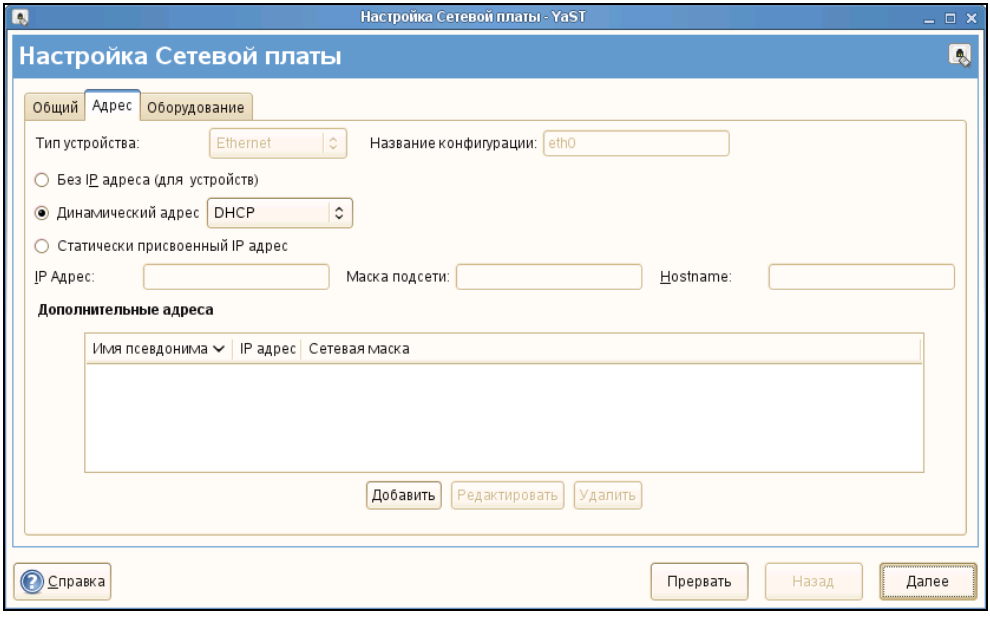


Рис. 5.22. Параметры сетевой платы

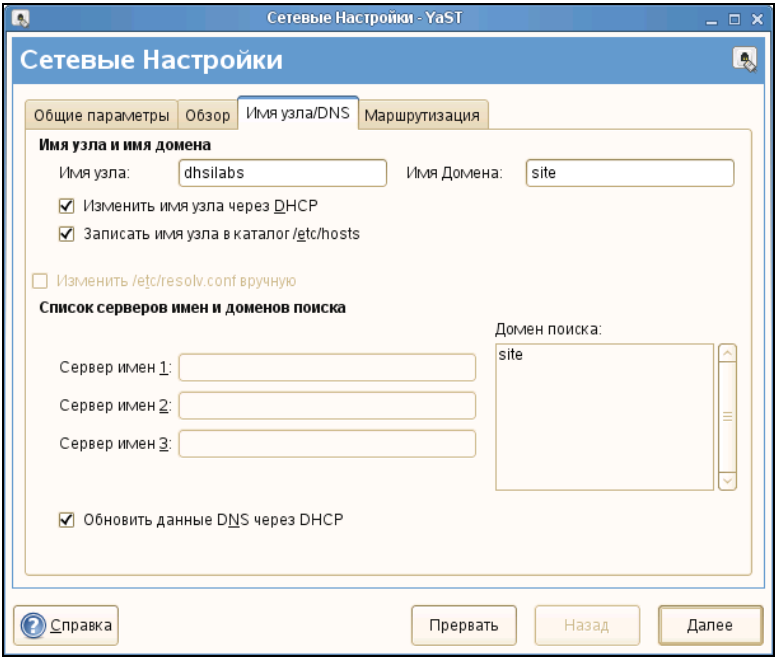


Рис. 5.23. Параметры DNS

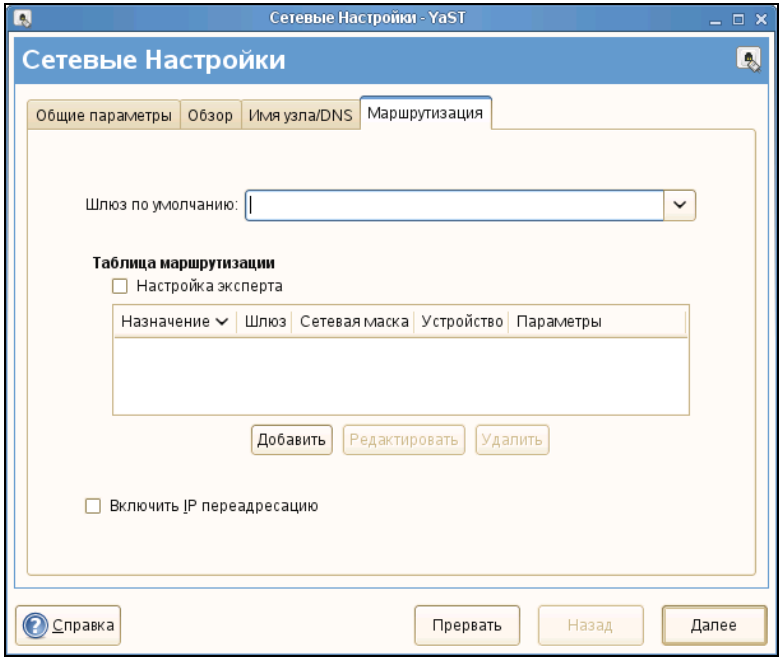


Рис. 5.24. Параметры маршрутизации

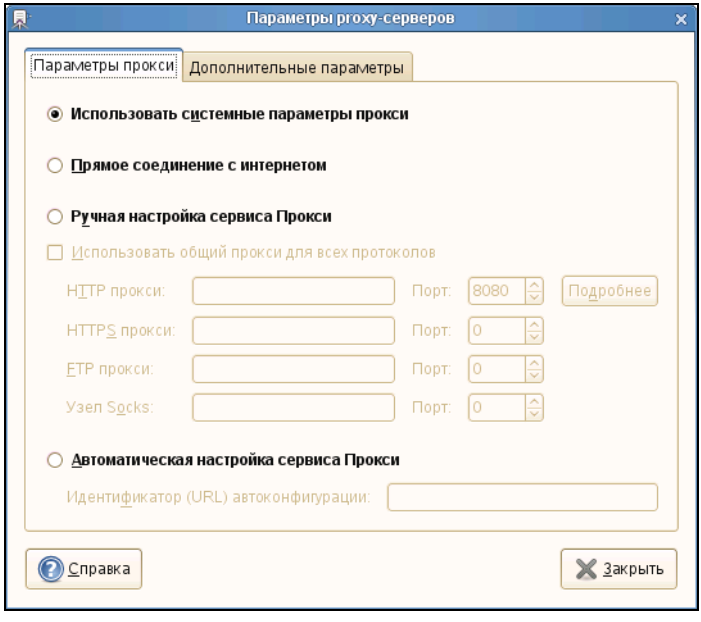


Рис. 5.25. Параметры прокси-сервера

Пользователям, подключающимся к Интернету по локальной сети, довольно часто нужно указать параметры прокси-сервера, через который осуществляется доступ к Интернету. Это можно сделать с помощью конфигуратора **Прокси-серверы сети** (**Центр управления | Прокси-серверы сети**). Параметры прокси-сервера (рис. 5.25) можно уточнить у администратора сети.

Здесь вы можете выбрать следующие опции:

- **Использовать системные параметры прокси** — будут использоваться параметры, заданные с помощью конфигуратора **YaST | Прокси**;
- **Прямое соединение с интернетом** — прокси не используется;
- **Ручная настройка сервиса Прокси** — нужно указать параметры прокси-сервера, полученные от администратора. Нажав кнопку **Подробнее**, можно установить имя пользователя и пароль для регистрации на прокси-сервере, если это необходимо.

Нужно отметить, что данный конфигуратор изменяет параметры только для пользователя, от имени которого он запущен. Для изменения системных параметров (действуют для всех пользователей) нужно использовать конфигуратор **YaST | Прокси** (рис. 5.26).

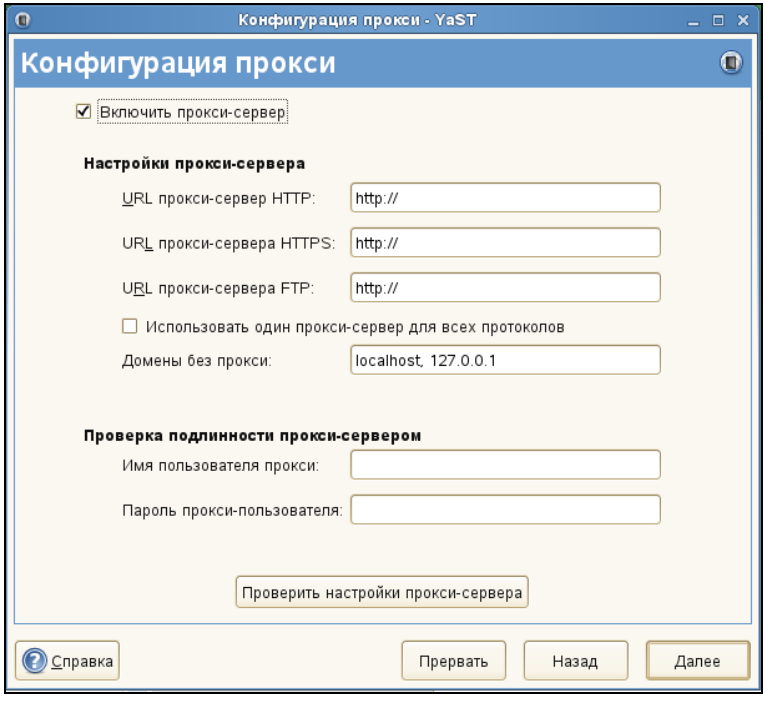


Рис. 5.26. Общесистемные параметры прокси-сервера

5.4.3. Ubuntu 8.10

После запуска конфигуратора network-admin (**Система | Администрирование | Сеть**) вы увидите список созданных сетевых интерфейсов. В данном случае обнаружен только один интерфейс — **Проводное подключение** (рис. 5.27).

> ***Примечание***
>
> По умолчанию окно конфигуратора заблокировано. Нажмите кнопку **Разблокировать** и введите ваш пароль (именно ваш пароль, а не пароль root).

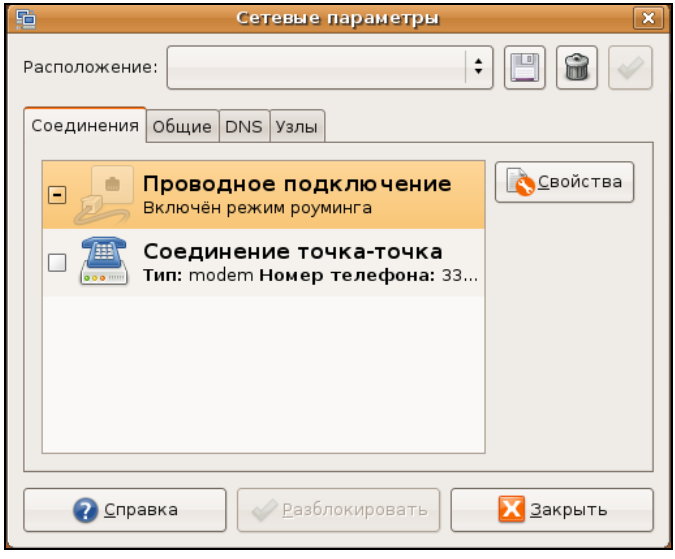


Рис. 5.27. Список сетевых интерфейсов

Выберите обнаруженный интерфейс и нажмите кнопку **Свойства**. В данном случае интерфейс настраивается по протоколу DHCP (рис. 5.28), то есть автоматически. Если вы хотите установить статический IP-адрес, из списка **Конфигурация** выберите **Статический адрес IP**, введите IP-адрес, маску сети и IP-адрес шлюза (**Gateway адрес**).

Далее на вкладке **Общие** можно установить сетевое имя компьютера и домен, на вкладке **DNS** (рис. 5.29) — IP-адреса DNS-серверов, а на вкладке **Узлы** вы увидите редактор файла /etc/hosts (редактирование файла /etc/hosts осуществляется аналогично описанному в *разд. 5.4.1*).

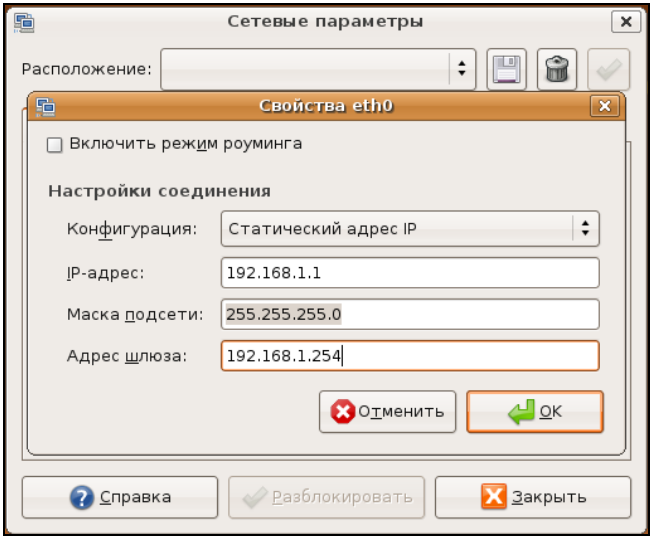


Рис. 5.28. Настройка сетевого интерфейса

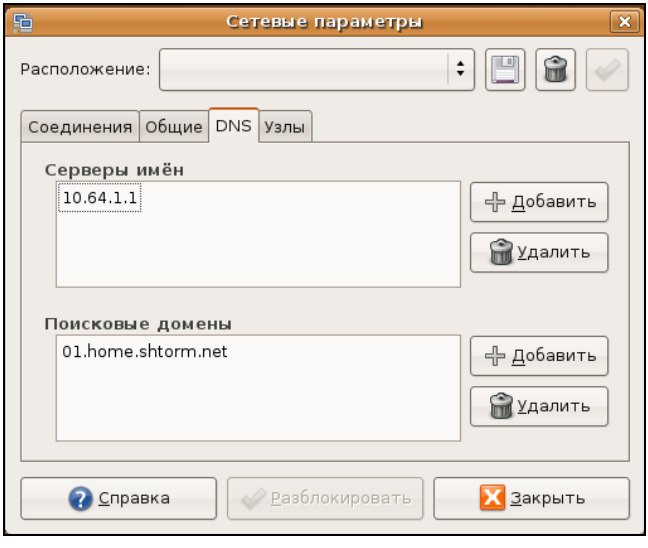


Рис. 5.29. Параметры DNS

Настроить параметры прокси-сервера можно с помощью такого же конфигуратора, как и в дистрибутиве Fedora (см. *разд. 5.4.1*). Для вызова конфигуратора прокси (рис. 5.30) выполните команду **Система | Параметры | Сервис Прокси**.

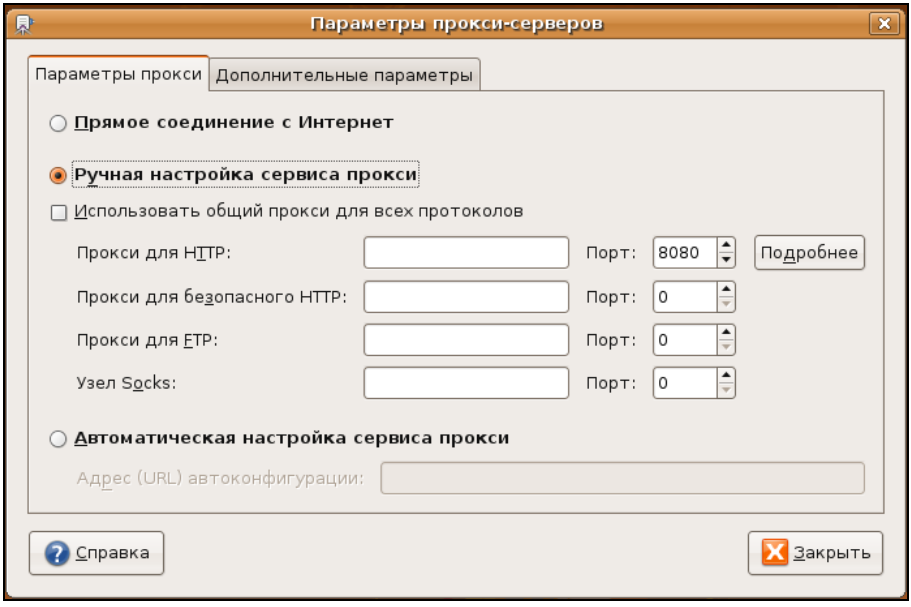


Рис. 5.30. Параметры прокси-сервера

В Ubuntu 8.10 вместо конфигуратора network-admin используется Network-Manager. Это совершенно другой уровень конфигуратора сети, позволяющий в одной программе настроить все поддерживаемые системой соединения: Ethernet-сеть, беспроводную Wi-Fi-сеть, GPRS, VPN и DSL-соединения. В этой главе мы рассмотрим только настройку Ethernet-соединения.

Для запуска конфигуратора выполните команду **Система | Параметры | Network Configuration**. В открывшемся окне на вкладке **Проводные** (рис. 5.31) обычно выводится список Ethernet-подключений. В данном случае оно одно и называется **Auto eth0**. Приставка **Auto** означает, что соединение настраивается автоматически по DHCP. Собственно, если в сети есть DHCP-сервер, то настраивать сеть в Ubuntu не нужно. А вот если нужно указать статический IP-адрес, то следует выделить соединение **Auto eth0** и нажать кнопку **Правка**. В открывшемся окне (рис. 5.32) перейдите на вкладку **Параметры IPv4**, выберите метод **Вручную**, затем нажмите кнопку **Добавить** и введите IP-адрес, маску сети и шлюз (если шлюза нет, введите 0.0.0.0). В нижней части окна можно указать (через пробел) серверы DNS и ваш домен. Параметр **Подключать автоматически** выключать не нужно, а вот параметр **Системная настройка** надо выключить. Можете также удалить приставку **Auto** из названия соединения — чтобы она не сбивала вас с толку. По окончании указания настроек нажмите кнопку **OK**.

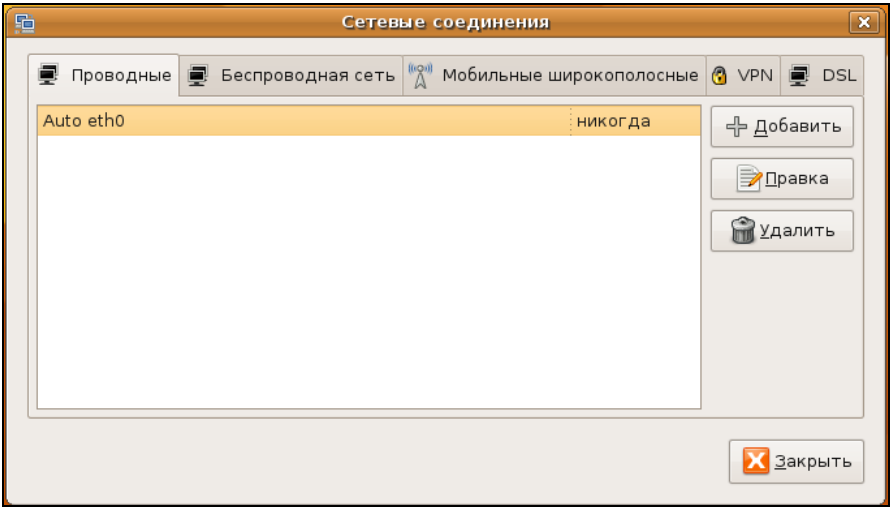


Рис. 5.31. Конфигуратор NetworkManager

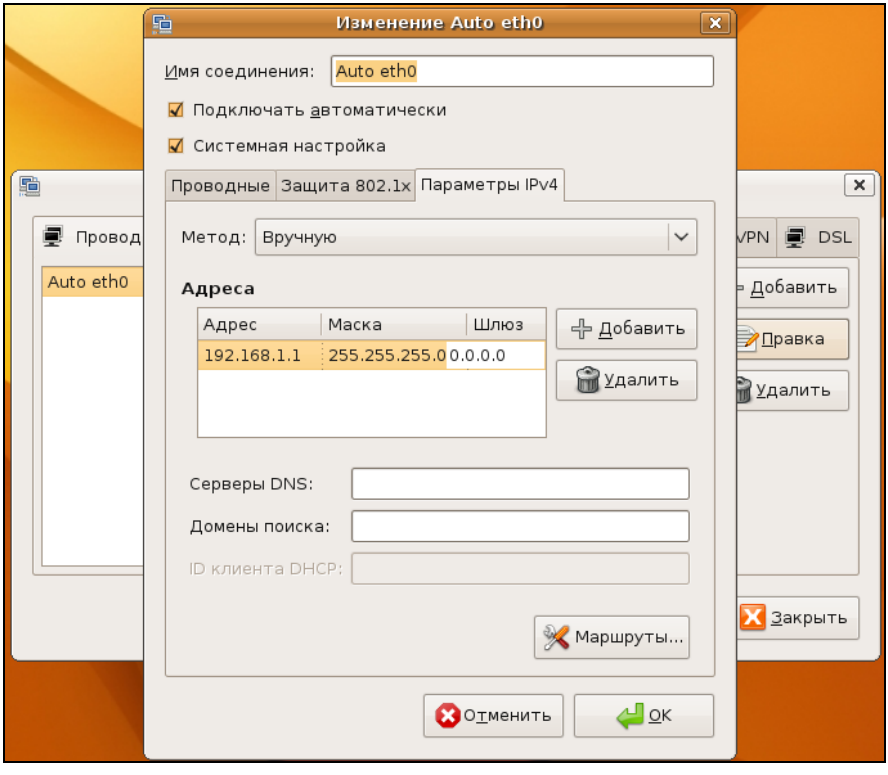


Рис. 5.32. Указание статического IP-адреса

Все, что вам осталось — это пропинговать присвоенный IP-адрес. Откройте терминал и введите команду `ping 192.168.1.1`. Если вы увидите сообщение **Network unreachable**, выполните команду (в терминале):

```
sudo mv /etc/network/interfaces /etc/network/interfaces_backup
```

После этого повторите настройку сети сначала.

Если в вашей сети нет DHCP-сервера, то особой необходимости в использовании NetworkManager тоже нет. Поэтому интерфейс можно настроить с помощью файла конфигурации /etc/network/interfaces. Откройте его в текстовом редакторе:

```
sudo gedit /etc/network/interfaces
```

Примерное содержимое для одного сетевого адаптера будет следующим:

```
auto lo
iface lo inet loopback
iface eth0 inet static
address <IP-адрес>
netmask <маска_сеть>
gateway <IP-адрес шлюза>
```

Например:

```
auto lo
iface lo inet loopback

iface eth0 inet static
address 192.168.1.1
netmask 255.255.255.0
gateway 0.0.0.0
```

Потом отредактируем серверы DNS:

```
sudo gedit /etc/resolv.conf

search <список доменов>
nameserver <IP-адрес 1>
nameserver <IP-адрес 2>
nameserver <IP-адрес 3>
nameserver <IP-адрес 4>
```

Всего можно указать четыре сервера DNS.

В заключение нужно отказаться от использования NetworkManager:

```
sudo update-rc.d -f NetworkManager remove
```

Подробно о ручной настройке сети в Ubuntu 8.10 вы можете прочитать по адресу: **http://www.dkws.org.ua/phpbb2/viewtopic.php?t=3839**.

Глава 6

Выбор соединения. Соединение с Интернетом в Windows

Существует много способов подключения к Интернету. Например — по беспроводной сети. Во многих отелях, аэропортах, библиотеках и учебных заведениях имеются точки беспроводного доступа, предоставляющие доступ к Интернету (доступ иногда бесплатный, а иногда платный — тут все зависит от владельца сети). Подключение к беспроводной сети было рассмотрено в *главе 4*.

> **Совет**
>
> Главное правило, о котором мы говорили в *главе 4*, — это не подключаться к неизвестным беспроводным сетям. Вполне возможно, что это сеть злоумышленника, который "развернул" ее специально для перехвата ваших данных, которые вы будете передавать через его сеть в Интернет.

Для подключения к Интернету также может использоваться Ethernet-соединение — если в вашей локальной сети есть шлюз, предоставляющий доступ к Всемирной паутине. В этой главе мы рассмотрим два типа соединения, которые в 99% случаев используются для подключения именно к Интернету.

> **Примечание**
>
> Сеть Ethernet, как и беспроводная сеть, могут быть попросту не подключены к Интернету, поэтому нельзя сказать, что эти два типа соединения используются *только* для подключения к Всемирной сети.

Как вы уже догадались, мы поговорим о модемном и об ADSL-соединении и в этой главе рассмотрим настройку таких соединений в операционной системе Windows (XP и Vista), а следующую посвятим настройке этих соединений в Linux.

6.1. Модемное соединение

Один из наиболее часто используемых способов подключения к Интернету — удаленное соединение *по коммутируемым сетям* общего пользования через *модем*, выполняющий МОдуляцию и ДЕМодуляцию (отсюда и название)

дискретных сигналов. Модем кодирует и декодирует каждый информационный бит, синхронизирует передачу сигналов по линиям связи (телефонным линиям), выполняет проверку правильности передачи, а также некоторые другие операции, например, компрессию и декомпрессию передаваемых данных.

Спрашивается, зачем нужна модуляция и демодуляция сигналов? Дело тут в том, что модемы предназначены для передачи цифровых данных по аналоговым линиям (для передачи информации по цифровым каналам модем не требуется). Ведь компьютер работает с данными в двоичной системе, т. е. оперирует наборами нулей и единиц, которые, в свою очередь, соответствуют некоторым выбранным уровням напряжения: например, есть напряжение — 1, нет напряжения — 0.

Итак, что делать, если вам нужно передать сигнал за пределы компьютера? Если расстояние небольшое, то можно соединить компьютеры напрямую, например, так называемым *нуль-модемом* (специальным кабелем, соединяющим два компьютера по COM- или LPT-портам) или с помощью сетевых карт и перекрестно обжатой витой пары. А если расстояние велико — скажем, когда удаленный компьютер находится в другом районе или городе. Первое, что иногда приходит в голову, — купить много кабеля. Но это может оказаться довольно дорогой затеей, к тому же вам придется бороться не только с затуханием сигнала (кроме кабеля для передачи данных на большие расстояния вам потребуются усилители сигнала), но и любителями поживиться за ваш счет — кабель могут просто украсть вместе с усилителями и другим оборудованием.

Вот тут действительно понимаешь, что самое дешевое решение — это передача данных по обычным телефонным линиям. Телефоны есть практически у всех, модем стоит дешево, подключаешь модем к компьютеру и к телефонной линии — и все, можно передавать данные.

Модемное (оно же коммутируемое, или dial-up) соединение остается одним из самых распространенных в нашей стране, несмотря на наличие альтернативных способов подключения к Интернету (ADSL, PPPoE и др.), зачастую более выгодных.

К преимуществам модемного доступа к Интернету можно отнести только дешевизну подключения. Из оборудования требуется телефонная линия (с этим сейчас проблем нет) и модем. Самый дешевый *внутренний* модем стоит около 300 рублей, более качественный *внешний* — около тысячи. Подключение к провайдеру часто вообще бесплатно, а час работы в бизнес-время обходится в сумму не более 25–30 рублей (в зависимости от региона страны и выбранного провайдера). На этом преимущества и заканчиваются.

А теперь рассмотрим недостатки:

- *низкое качество телефонных линий* — соединение через модем нередко обрывается;
- *высокая удельная стоимость передачи информации* — при больших объемах намного выгоднее оказывается ADSL-доступ. Давайте посчитаем. Час доступа к Интернету стоит 30 рублей. Эту сумму вы платите провайдеру. Еще нужно учесть стоимость часа обычного телефонного разговора — эту сумму в конце месяца вы заплатите вашему телефонному оператору. Допустим, еще 15 рублей[1]. Итого час обходится в 45 рублей. 8 часов работы в день, 22 рабочих дня. В месяц получится 176 часов, т. е. почти 8 тыс. рублей. Для сравнения — стоимость каждого гигабайта принятой или переданной информации по выделенной линии составляет примерно 600 рублей в месяц, а одного гигабайта вполне хватает для повседневной работы, если, конечно, не скачивать из Интернета полнометражные видеофильмы;
- *низкая скорость передачи данных* — заплатив за модемный доступ 8 тыс. рублей в месяц, удовольствия от работы в Интернете вы не получите. Что ни говори, а 33,6 Кбит/с (в идеальных условиях 56 Кбит/с) — это не сравнимо с 1 Мбит/с по выделенной линии.

С другой стороны, если вы работаете в Интернете редко (до 10 часов в месяц), модемное соединение — оптимальное решение для вас.

6.1.1. Выбор модема

В компьютерном магазине обычно предлагают широкий ассортимент модемов — от самых дешевых устройств, до довольно дорогих от известных брендов (например, ZyXEL и US.Robotics). Но модем модему рознь. Давайте попробуем выбрать оптимальный для вас модем.

Самые дешевые — внутренние модемы (рис. 6.1), представляющие собой плату расширения, устанавливаемую внутрь корпуса компьютера. Все современные внутренние модемы выполнены в виде PCI-платы. Цены на подобные устройства начинаются от 300 рублей. Но я настоятельно рекомендую вам отказаться от покупки внутреннего модема по следующим причинам:

- в случае "зависания" модема (а такое случается, особенно с дешевыми моделями) вы не сможете его "сбросить", т. е. перезапустить. Если такое произойдет с внешним модемом, то для перезапуска его достаточно

[1] Справедливости ради надо отметить, что в большинстве случаев телефонные операторы не взимают с клиентов плату за соединение с интернет-провайдером, если у данного оператора имеется с данным провайдером специальный на этот счет договор.

выключить/включить. А внутренний модем вы уже не выключите — тут или ждать, пока модем "подумает", или перезагружать компьютер;

- вы не можете контролировать состояние устройства — у внутреннего модема нет никаких индикаторов, отображающих его состояние (раньше выпускались внутренние модемы с панелью индикаторов состояния, которую можно было установить вместо заглушки в отсек корпуса);
- вы не сможете показать знакомым, на что потратили свои кровные 300 рублей (хотя лично я бы такое "счастье" и не показывал).

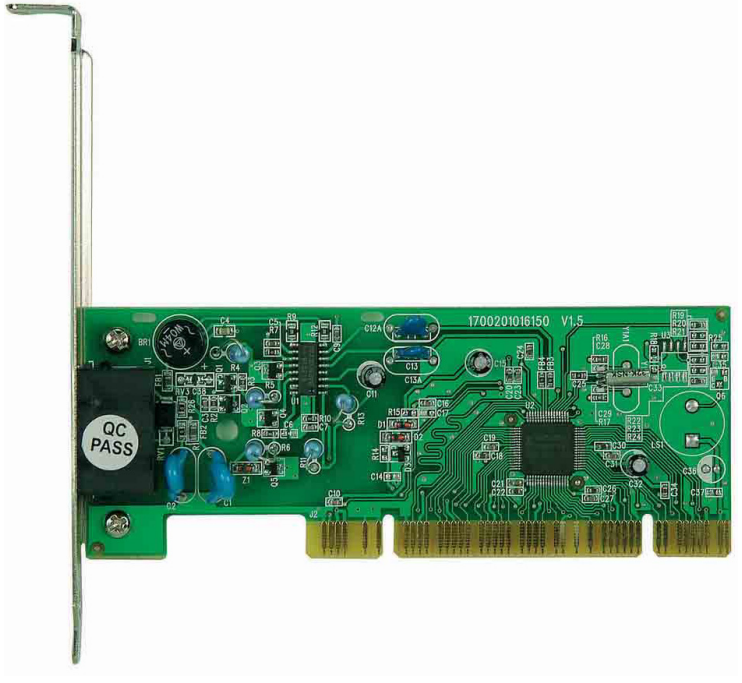


Рис. 6.1. Внутренний модем

Но приведенные причины, сами понимаете, не главные. А суть в том, что у модема могут быть собственный процессор и своя память, а могут и не быть. Модемы с собственным процессором называются *аппаратными*, а без такового — *программными* (win-модемы). В Windows-то все равно (если не считать, что такой модем расходует лишние системные ресурсы), а вот если вы захотите установить Linux, то win-модем в этой операционной системе работать не будет. Впрочем, если вы планируете использовать только Windows, тогда можете на этот счет не беспокоиться. Но в любом случае

рекомендуется покупать внешний модем (рис. 6.2) — только потому, что вы сможете его полностью контролировать, выключить, в конце концов, когда он вам не нужен. Тем более что внешние модемы совсем не дорогие — цены начинаются примерно от 900 рублей.

Рис. 6.2. Внешний модем

Итак, мы определились с типом модема. Теперь рассмотрим способы его подключения к компьютеру. Предпочтительнее покупать более современные модемы, подключаемые к USB-порту. Они работают так же хорошо, как и модемы, которые подключаются к COM-порту, но зато их можно подключать к компьютеру и отключать от него, не выключая сам компьютер. Очень удобно. Конечно, если количество USB-портов у вас ограничено, а устройств, которые к ним подключаются, много, тогда можно купить и COM-модем.

Теперь поговорим о производителе модема. Если у вас хорошая телефонная линия (в большинстве случаев это так), можно покупать модем любого производителя. Если же качество телефонной линии оставляет желать лучшего, тогда нужно задуматься о "вездеходе" — модеме, способном работать на любой телефонной линии. Я бы порекомендовал модемы фирмы ZyXEL. Не подумайте, что это реклама — просто практикой проверено, что они отлично работают даже на самых зашумленных телефонных линиях.

6.1.2. Подключение модема

Сначала нужно подключить модем к компьютеру. Если у вас COM-модем, то перед его подключением выключите компьютер. COM-модем (он же модем RS-232C) подключается к последовательному порту с помощью кабеля RS-232C (рис. 6.3). Не беспокойтесь — к другому порту вы его не подключите, разъем просто не подойдет.

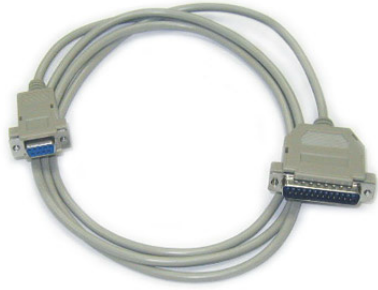


Рис. 6.3. Кабель для подключения модема к последовательному порту

Если же вы все-таки купили USB-модем, компьютер можете не выключать. У USB-модемов есть еще одно преимущество — они не нуждаются в блоке питания, поскольку получают питание по шине USB. В результате у вас под столом будет на один провод меньше.

Теперь подключите модем к телефонной линии. Обратите внимание: на задней панели модема (вне зависимости от типа — внутренний или внешний) имеются два гнезда с надписями соответственно LINE и PHONE. Телефонную линию нужно подключать к гнезду LINE — не перепутайте! К гнезду PHONE при необходимости можно подключить параллельный телефонный аппарат.

Если у вас внешний модем, не забудьте его включить (кнопка включения/выключения обычно находится на задней панели модема).

6.1.3. Настройка модемного соединения в Windows XP

При первом подключении модема Windows сообщит, что нашла новое устройство. Если драйвер для данного модема имеется в комплекте драйверов вашей версии Windows (попросту говоря, если Windows умеет работать с вашим модемом), то вам ничего делать не придется — операционная система все сделает за вас сама. А вот если драйвера для вашего модема в системе нет, то Windows попросит вас вставить компакт-диск с драйвером. Вставьте его — далее от вас ничего не требуется, только подождать. Windows сама найдет и установит нужный драйвер.

Итак, если Windows при первом подключении модема самостоятельно обнаружила модем и установила его драйвер, то первым делом нужно убедиться,

что драйвер этот установлен корректно. Для этого откройте окно **Панель управления** (**Пуск | Настройка | Панель управления**) и запустите апплет **Система**. Это же действие можно выполнить намного проще и быстрее — просто нажмите комбинацию клавиш <Win>+<Pause>. В открывшемся окне перейдите на вкладку **Оборудование** (рис. 6.4) и нажмите кнопку **Диспетчер устройств**. В случае правильной установки модема в группе **Модем** вы обнаружите свое устройство (рис. 6.5).

После установки драйвера модема можно приступить к созданию подключения. Откройте папку **Сетевые подключения** (**Пуск | Настройка | Сетевые подключения**). В левой части открывшегося окна (рис. 6.6) выберите опцию **Создание нового подключения**.

Вы увидите окно **Мастер новых подключений**. Пока просто нажмите кнопку **Далее**. Мастер предложит выбрать один из вариантов подключения к сети (рис. 6.7). Нам нужно выбрать переключатель **Подключить к Интернету** и нажать кнопку **Далее**.

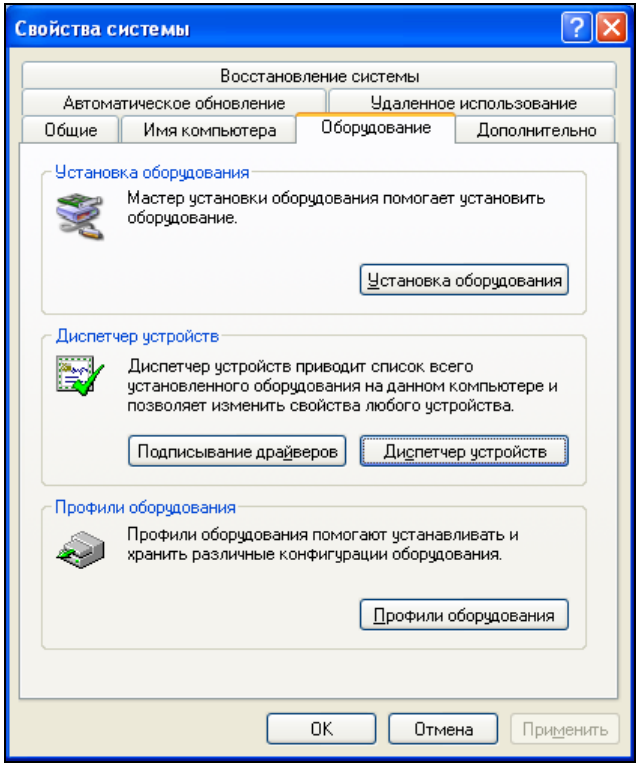


Рис. 6.4. Вкладка **Оборудование**

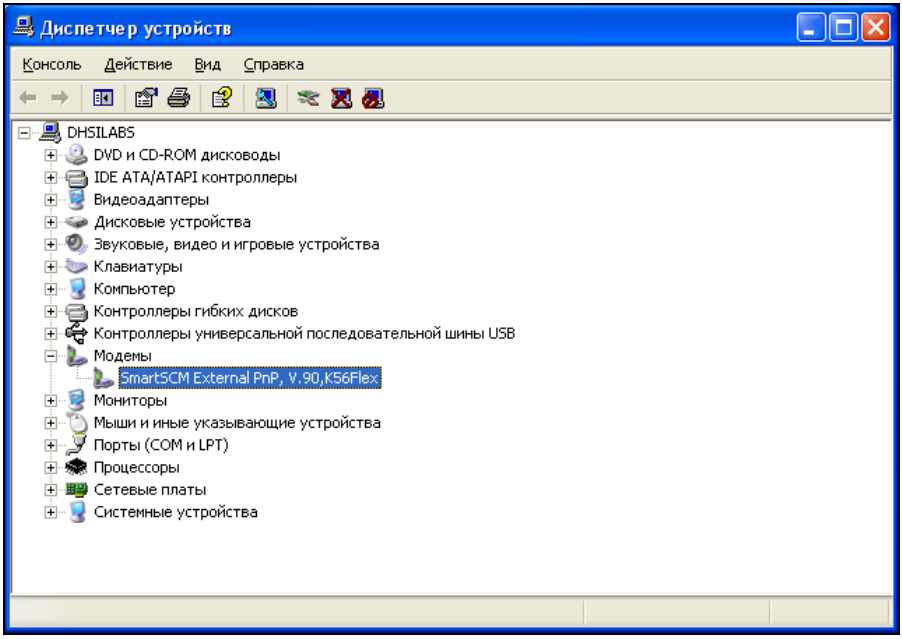


Рис. 6.5. Диспетчер устройств: модем установлен

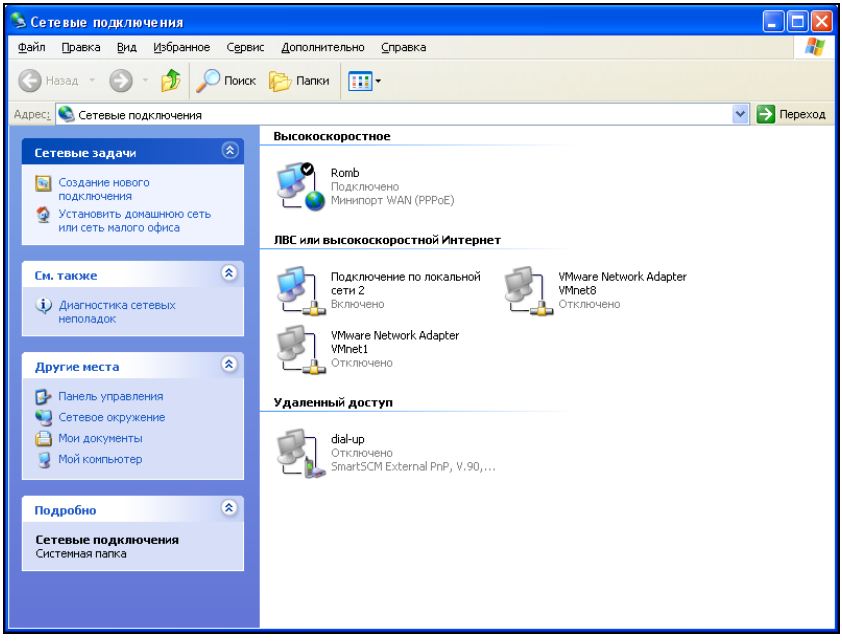


Рис. 6.6. Сетевые подключения

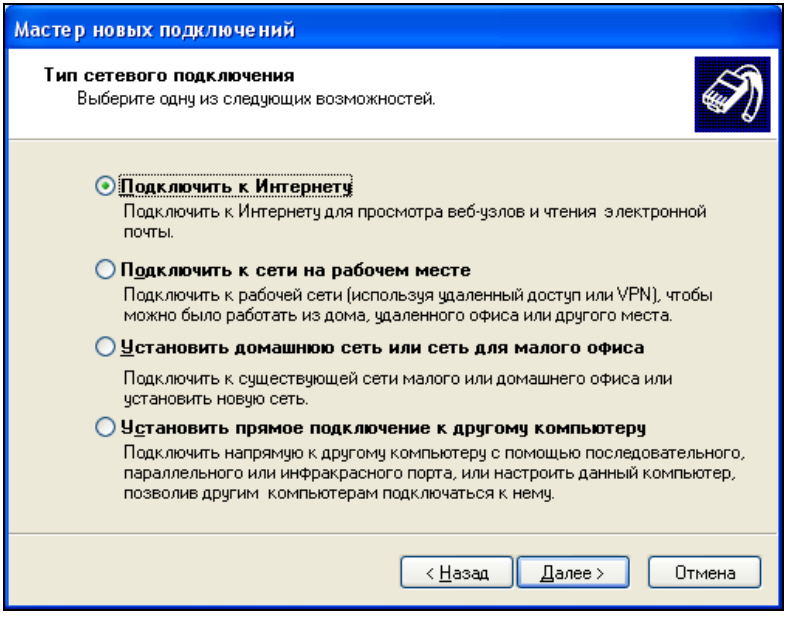


Рис. 6.7. Мастер новых подключений

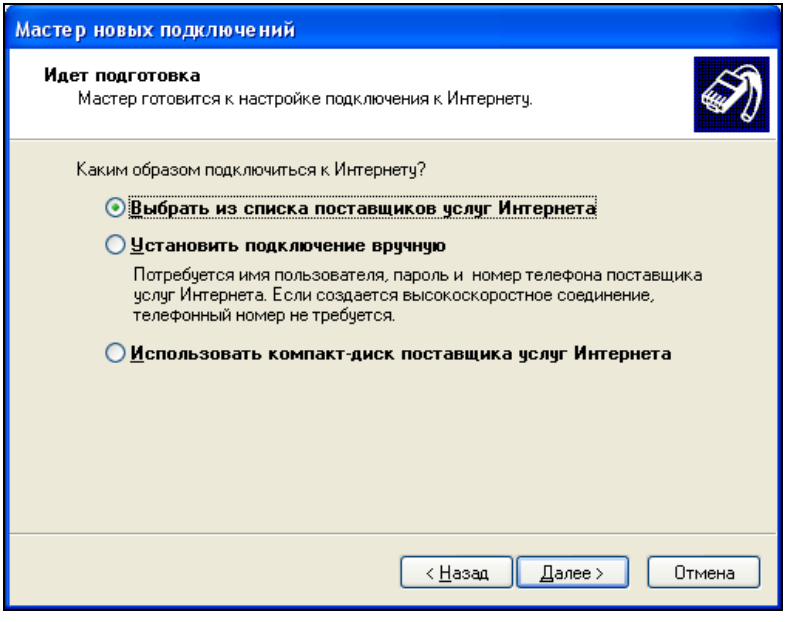


Рис. 6.8. Как подключиться к Интернету?

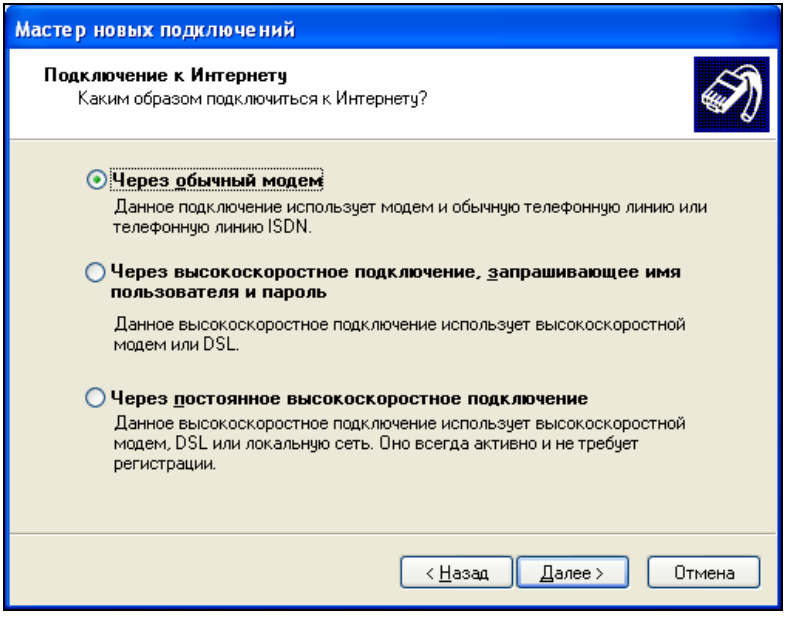


Рис. 6.9. Нужно выбрать первый вариант

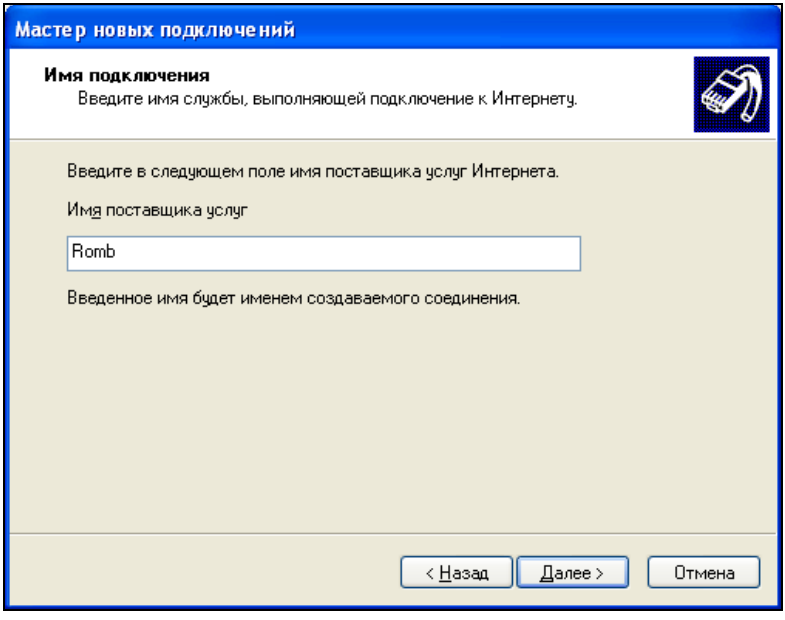


Рис. 6.10. Название провайдера

После этого мастер попросит вас уточнить, каким образом вы хотите подключиться к Интернету (рис. 6.8). Да, Windows умна, но не настолько, поэтому не нужно надеяться, что ваш провайдер будет в списке поставщиков услуг Интернета. Наши провайдеры, конечно, лучшие в мире, но установочный компакт-диск для автоматической настройки компьютера клиента тоже не предлагают. Поэтому нам остается второй вариант — **Установить подключение вручную**.

Наконец-то мы пробрались сквозь дебри настроек и дошли до самого основного — выбора типа подключения (рис. 6.9). Нам нужно выбрать опцию **Через обычный модем**. На остальные варианты пока не обращайте внимания — они вам сейчас не нужны.

Затем мастер попросит ввести название провайдера (рис. 6.10). Можете ввести что угодно, лишь бы вы запомнили, что ввели. Если вы планируете подключаться к нескольким провайдерам, тогда рекомендуется вводить значимые имена, чтобы вы могли понять, для подключения к какому провайдеру используется то или иное подключение.

Следующий шаг — ввод номера телефона вашего интернет-провайдера. Номер этот следует вводить как "городской", т. е. без кодов страны и города (если вы точно не знаете обратного), и без разделителей — просто цифры, например, 7775555, но не 777-55-55.

После этого нужно ввести имя пользователя и пароль (рис. 6.11), а также установить дополнительные параметры подключения:

- **Использовать следующие имя пользователя и пароль при подключении любого пользователя** — если вы работаете за компьютером не один и не хотите, чтобы другие пользователи, которые входят в систему под своей учетной записью, использовали ваше подключение, выключите этот режим. Если же за компьютером работают несколько пользователей, но все используют одну учетную запись, отключение этого режима вам не поможет — просто не вводите здесь пароль. Да, тогда вам придется вводить пароль при каждом подключении к Интернету, но другого способа ограничения нежелательного использования вашего подключения пока никто не придумал;
- **Сделать это подключение подключением к Интернету по умолчанию** — если вы не планируете других альтернативных способов подключения к Интернету, рекомендуется не выключать этот режим;
- **Включить брандмауэр для подключения к Интернету** — стандартный брандмауэр Windows — не предел мечтаний, но с ним все же безопаснее, чем без него.

Все! Подключение практически создано. Вы можете создать ярлык на рабочем столе для этого подключения, установив соответствующий флажок (рис. 6.12) — так доступ к подключению будет быстрее.

Как только вы нажмете кнопку **Готово**, откроется окно подключения к Интернету (рис. 6.13), но не спешите нажимать кнопку **Вызов**. Прежде нажмите кнопку **Свойства**, чтобы уточнить некоторые параметры соединения.

В окне свойств подключения (рис. 6.14) нужно установить флажок **Использовать правила набора номера**, а потом нажать кнопку **Правила**. Откроется окно **Телефон и модем**, в котором как раз и определяются правила набора номера (рис. 6.15).

Нажмите в окне **Телефон и модем** кнопку **Изменить**. Откроется окно **Изменение местонахождения** (рис. 6.16). В этом окне вы должны правильно указать свою страну и ввести код города. Обязательно сделайте это! Иначе Windows решит, что вы находитесь в другой стране, например, в США, и будет набирать номер в международном формате. В нижней части окна укажите тип набора номера — как правило, это **Импульсный**.

Теперь дважды нажмите кнопку **OK** — вы вернетесь в окно свойств подключения (см. рис. 6.14). Выберите страну, которую вы указали в окне на рис. 6.16, и введите код вашего города. Вот теперь ваш номер будет набран как нужно.

Почти все. Осталось только заглянуть на вкладку **Параметры** (рис. 6.17), чтобы установить дополнительные параметры подключения. Нас сейчас интересуют параметры повторного звонка. Эти параметры позволяют автоматизировать процесс дозвона, например, если сервер провайдера не ответил, или линия была занята. Установите количество повторов набора номера, интервал между повторами, время простоя до разъединения. Последний параметр довольно важный. Обычно в случае с модемным соединением вы платите не за количество принятой/переданной информации (трафик), а за время, проведенное в Интернете. Для экономии ваших средств и предназначен этот параметр. Если соединение не будет использоваться 20 минут (как по умолчанию), Windows разорвет его. Параметр **Перезвонить при разрыве связи** удобен, если соединение было разорвано (например, из-за помех на линии).

Вот теперь можно нажать кнопку **OK** в окне свойств подключения и перейти к окну подключения к Интернету (см. рис. 6.13). Нажмите заветную кнопку **Вызов** — Windows начнет набирать номер (рис. 6.18), а через некоторое время возле системных часов появится значок подключения — два компьютера (рис. 6.19). Если их мониторы мерцают, значит, в данный момент по соединению передаются данные.

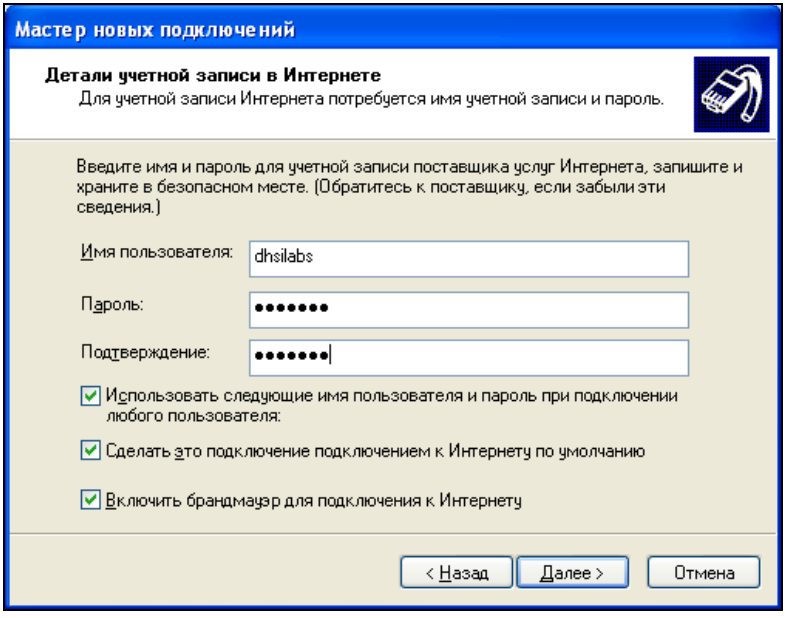


Рис. 6.11. Детали учетной записи

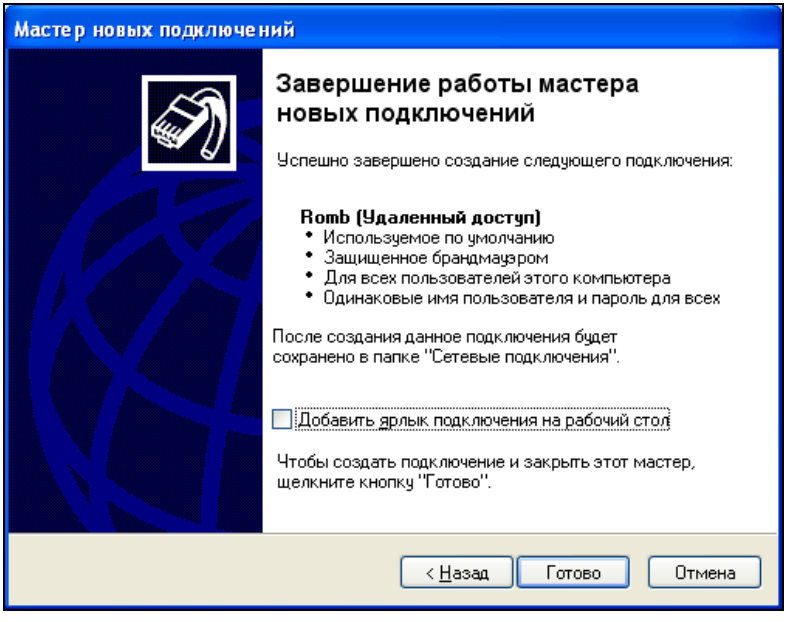


Рис. 6.12. Подключение создано

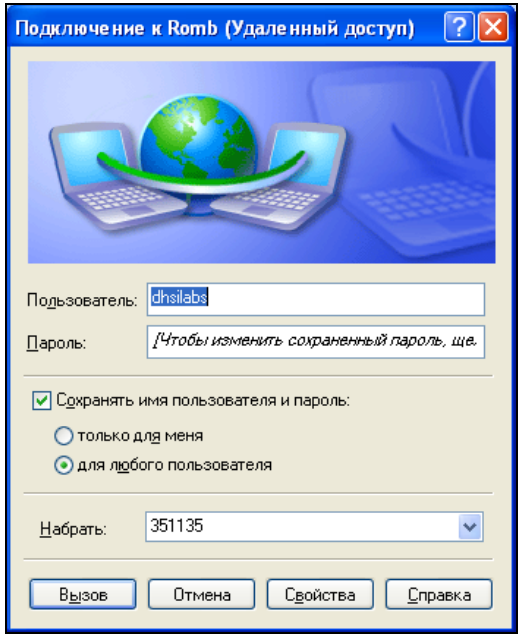


Рис. 6.13. Окно подключения к Интернету

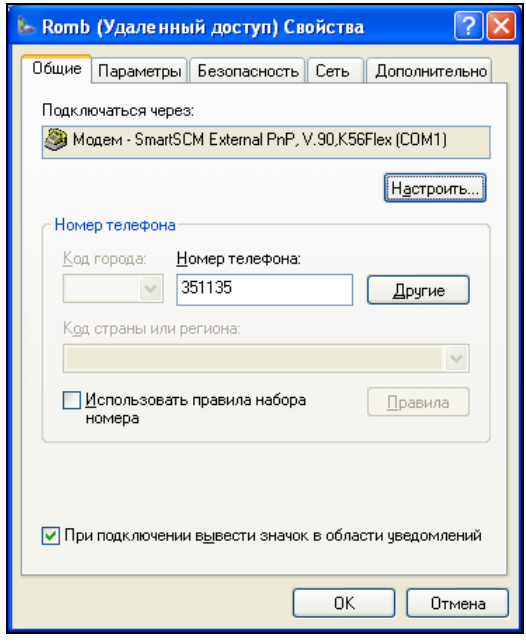


Рис. 6.14. Свойства подключения

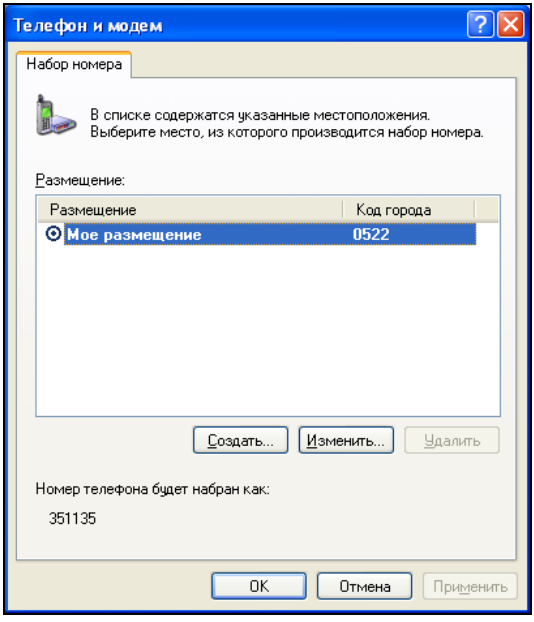


Рис. 6.15. Телефон и модем

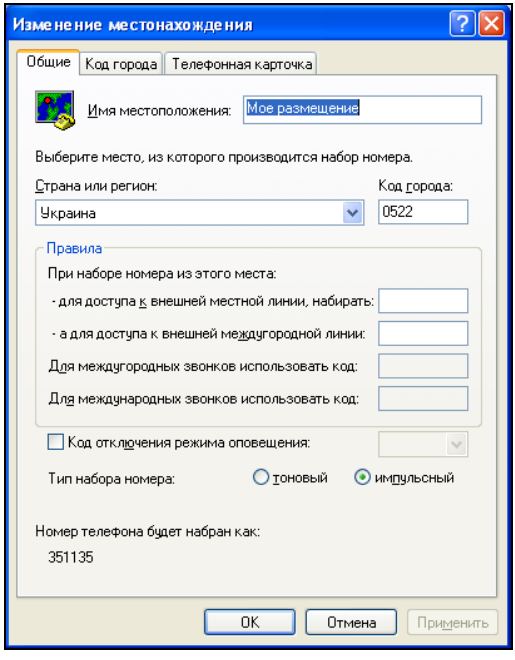


Рис. 6.16. Изменение местонахождения

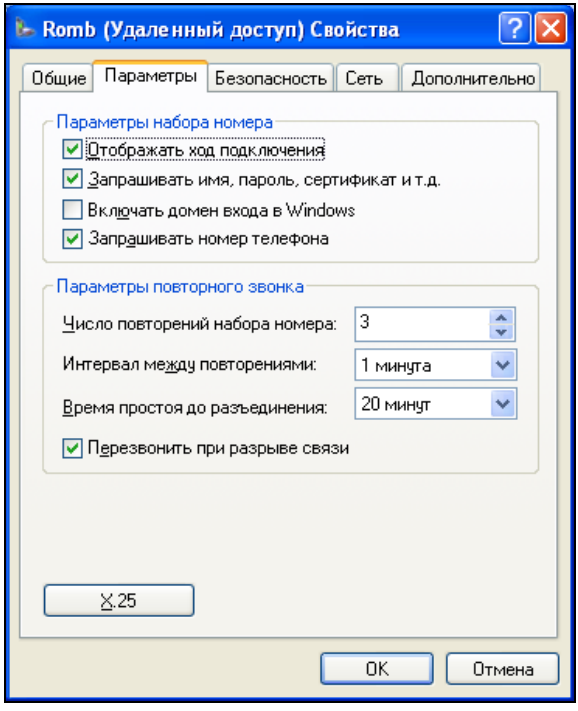


Рис. 6.17. Параметры подключения

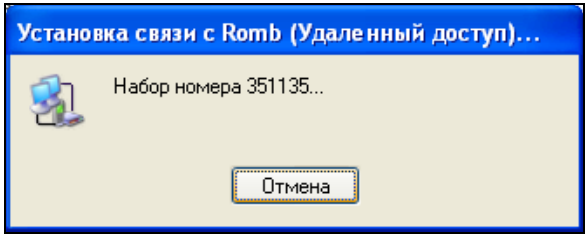


Рис. 6.18. Установка соединения

Рис. 6.19. Значок подключения

Теперь вы в Интернете! Можете запускать браузер Internet Explorer (пиктограмма для его запуска находится на вашем рабочем столе) и начинать бороздить просторы Интернета.

Для того чтобы отключиться, щелкните правой кнопкой мыши на пиктограмме соединения и выберите команду **Отключить** (рис. 6.20). Если вы хотите узнать, сколько времени уже провели в Интернете, выберите команду **Состояние**.

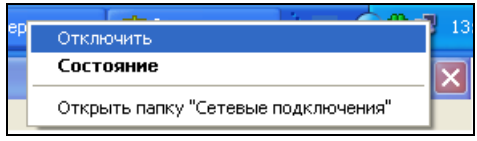


Рис. 6.20. Разъединение

Для повторной установки соединения вам нужно зайти в папку **Сетевые подключения** и дважды щелкнуть по пиктограмме вашего подключения (рис. 6.21). Все ваши модемные соединения будут находиться в группе **Удаленный доступ**.

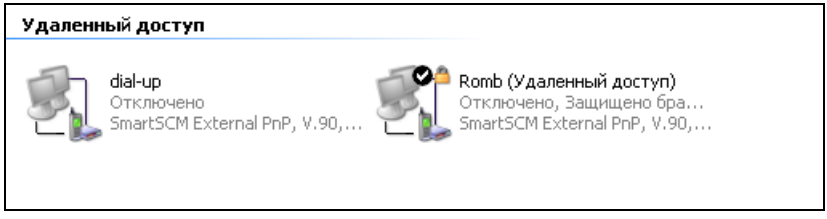


Рис. 6.21. Повторная установка соединения

6.1.4. Настройка модемного соединения в Windows Vista

Настройка модемного соединения в Windows Vista немного отличается от настройки модема в Windows XP. Первым делом подключите модем, включите его и затем включите компьютер. Если у вас USB-модем, то его можно подключить, не выключая питания компьютера.

Заметил одну особенность Windows Vista: если вы подключили не USB-модем, а обычный — RS-232C, но не включили его питание до запуска Windows Vista, то даже после включения питание модема Windows его не обнаружит. Чтобы

не перезагружать лишний раз компьютер, запустите **Диспетчер устройств**. Для быстрого запуска **Диспетчера устройств** нажмите комбинацию клавиш <Win>+<Pause>, а в открывшемся окне нажмите ссылку **Диспетчер устройств** (рис. 6.22).

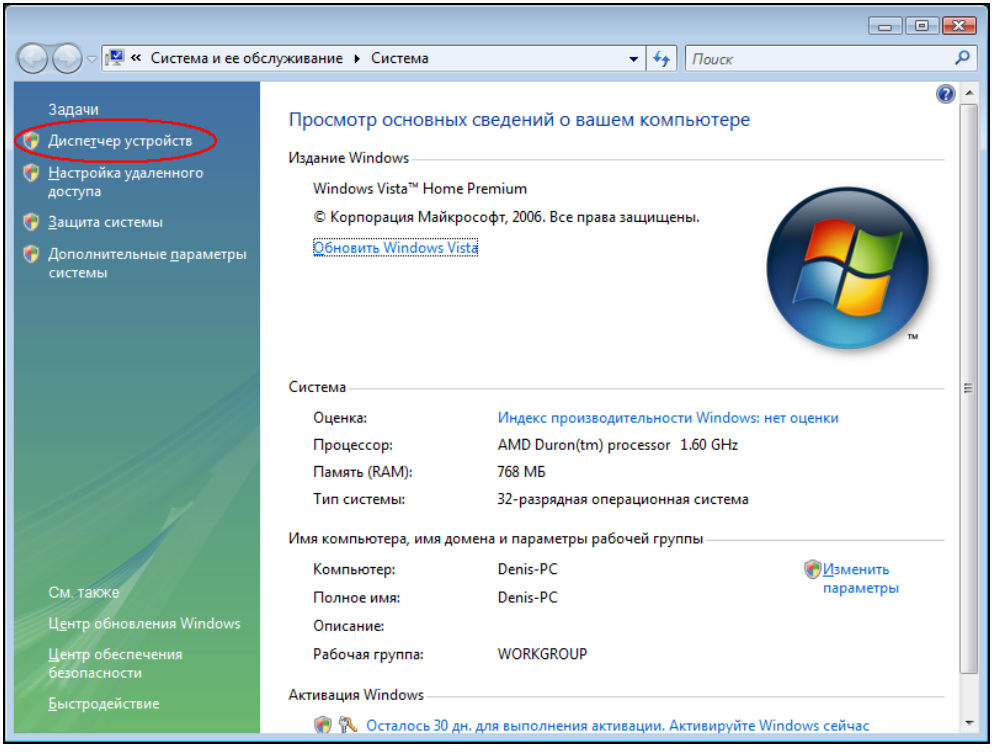


Рис. 6.22. Вызов **Диспетчера устройств**

Когда откроется **Диспетчер устройств**, выполните команду меню **Действие | Обновить конфигурацию оборудования**. После этого модем появится в списке оборудования (рис. 6.23), а Windows сообщит, что найдено новое оборудование (рис. 6.24).

Если у вас USB-модем (или вы включили COM-модем до запуска Windows Vista), то сразу увидите окно, представленное на рис. 6.24. Нажмите кнопку **Найти и установить драйвер (рекомендуется)**. Windows предложит вам произвести поиск драйвера в Интернете (рис. 6.25). Поскольку вы еще не подключены к Интернету (ведь модем еще не настроен!), можете выбрать любой вариант ответа на этот вопрос.

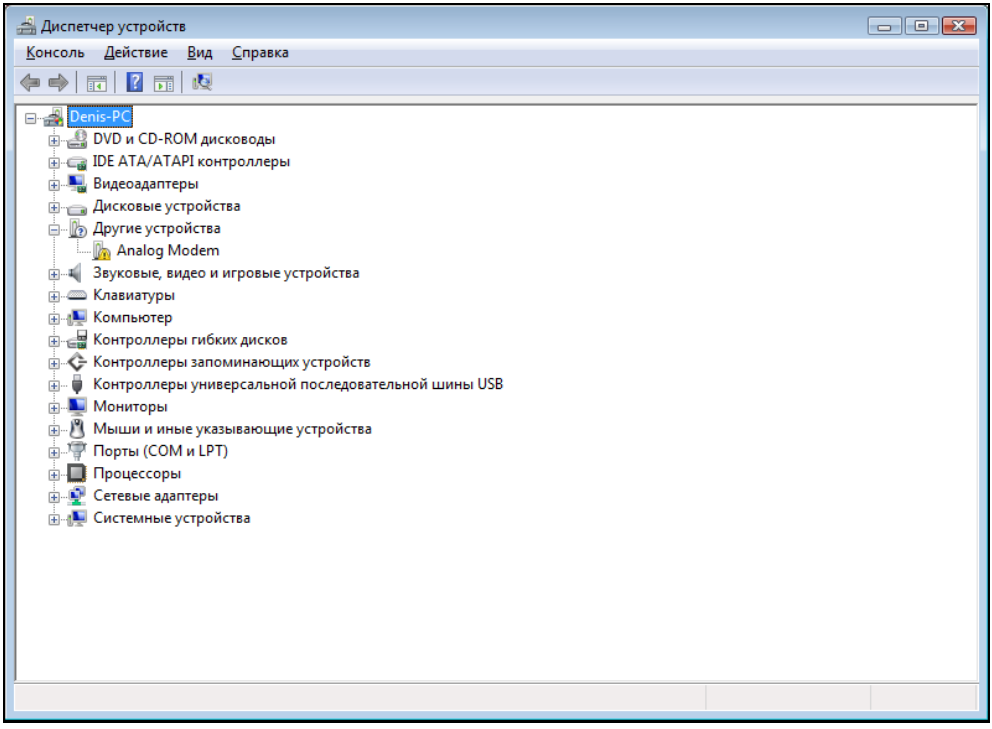


Рис. 6.23. Диспетчер устройств

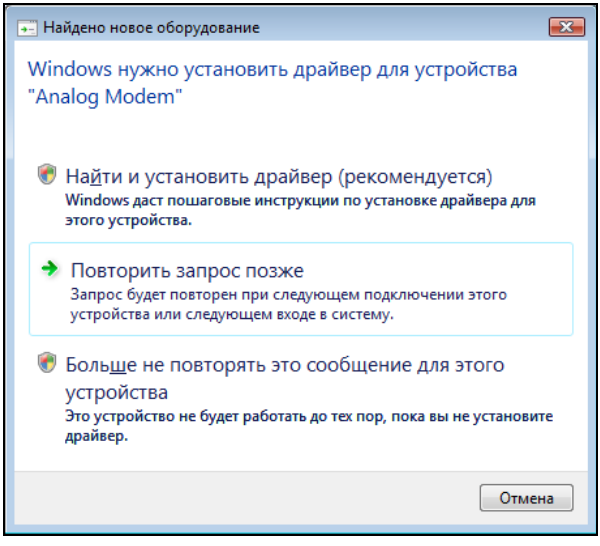


Рис. 6.24. Найдено новое оборудование

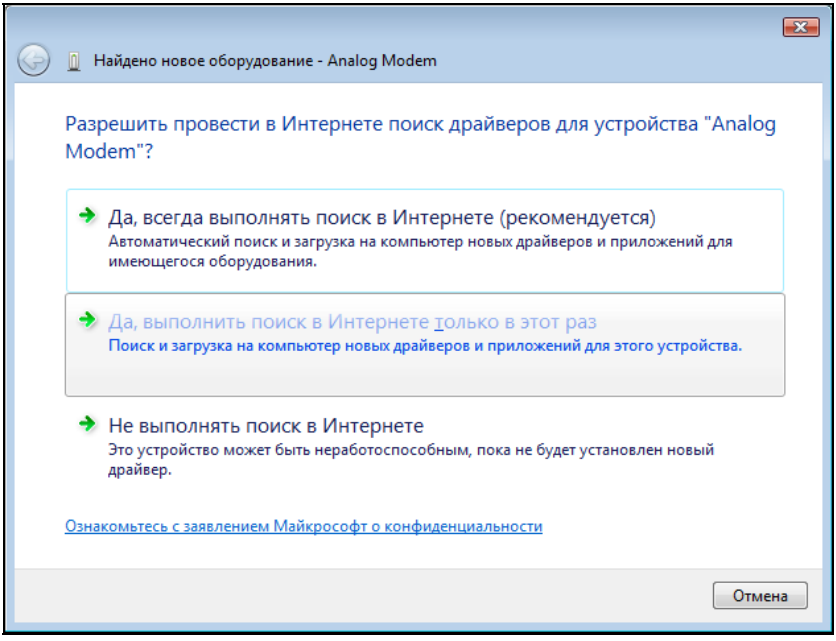


Рис. 6.25. Выбирайте любой вариант

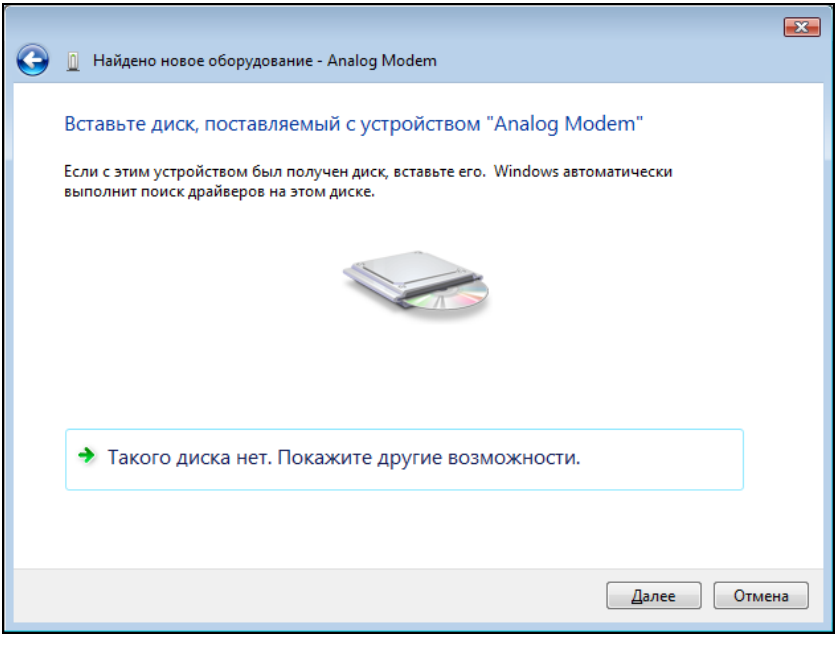


Рис. 6.26. Вставьте диск с драйвером

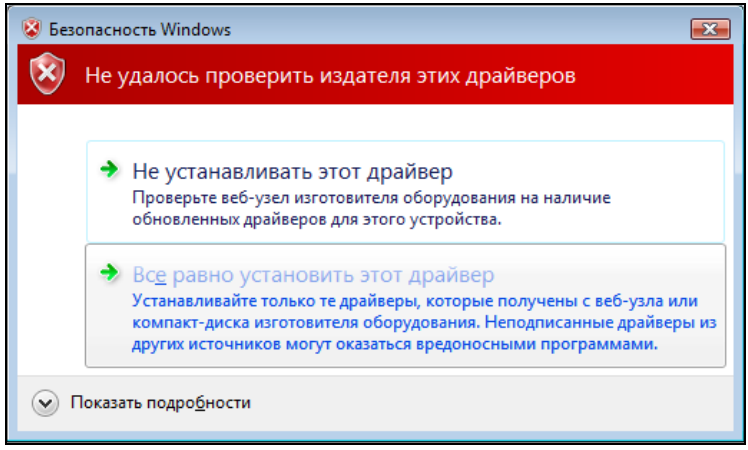


Рис. 6.27. Не удалось проверить издателя драйвера

Тогда Vista запросит диск с драйвером (рис. 6.26). Вставьте тот диск, который поставлялся вместе с модемом.

Поскольку к Интернету вы еще не подключены, Windows, скорее всего, отобразит сообщение о том, что не удалось проверить издателя драйвера (рис. 6.27). Нажмите кнопку **Все равно установить этот драйвер**.

Нужно отметить, что Vista в большинстве случаев нормально работает с драйверами для Windows XP, поэтому проблем с установкой драйвера у вас быть не должно. После установки драйвера Vista отобразит информационное окно (рис. 6.28).

Теперь с помощью меню **Пуск** (рис. 6.29) откройте окно **Панель управления**.

В группе **Сеть и Интернет** Панели управления выберите команду **Подключение к Интернету** (рис. 6.30, *а*). Vista отобразит возможные варианты подключения к Интернету (рис. 6.30, *б*). В моем случае — это **Высокоскоростное** и **Коммутируемое**. У вас, скорее всего, будет только **Коммутируемое**. В любом случае, поскольку нам нужно настроить модемное соединение, следует выбрать **Коммутируемое**.

Примечание

Если вы не можете найти команду **Подключение к Интернету** в группе **Сеть и Интернет**, выполните команду меню **Пуск | Подключение** и в открывшемся окне — команду **Установка подключения или сети**. Можно также щелкнуть на названии группы **Сеть и Интернет** и в группе **Центр управления сетями и общим доступом** выбрать команду **Подключиться к сети** (рис. 6.30, *в*). Внешний вид некоторых окон может изменяться в зависимости от версии Vista, например, вид Панели управления (рис. 6.30, *а*) в Vista Ultimate выглядит несколько иначе, но суть от этого не меняется.

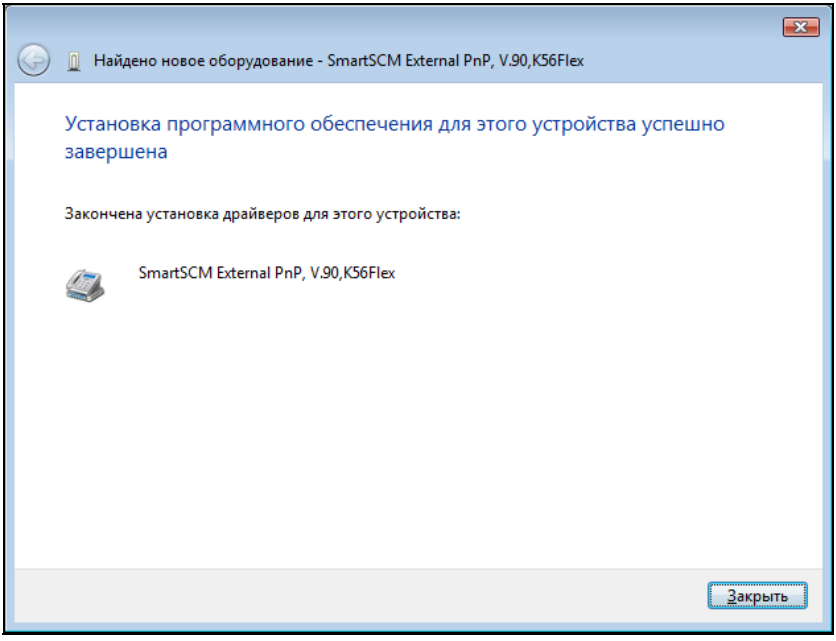


Рис. 6.28. Установка драйвера прошла успешно

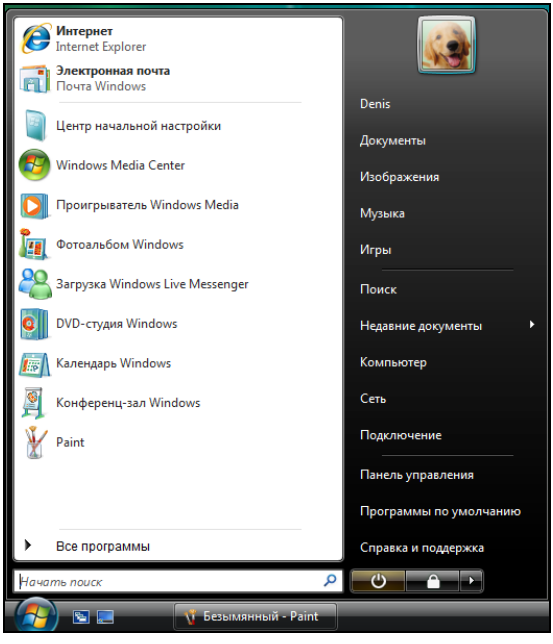
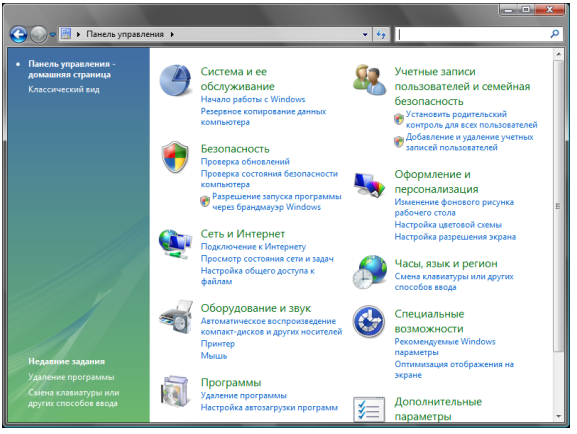
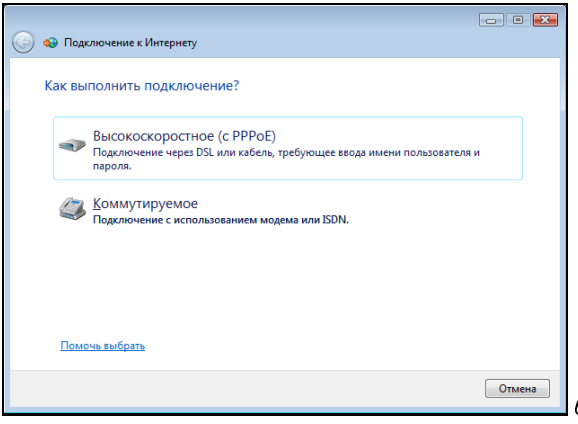


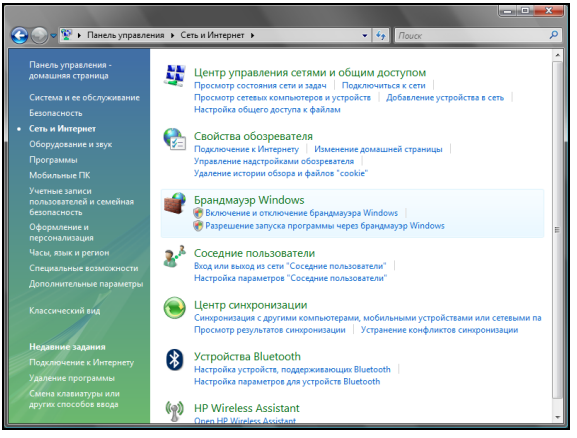
Рис. 6.29. Вызов Панели управления



а



б



в

Рис. 6.30. *а* — Панель управления; *б* — варианты подключения к Интернету; *в* — Сеть и Интернет

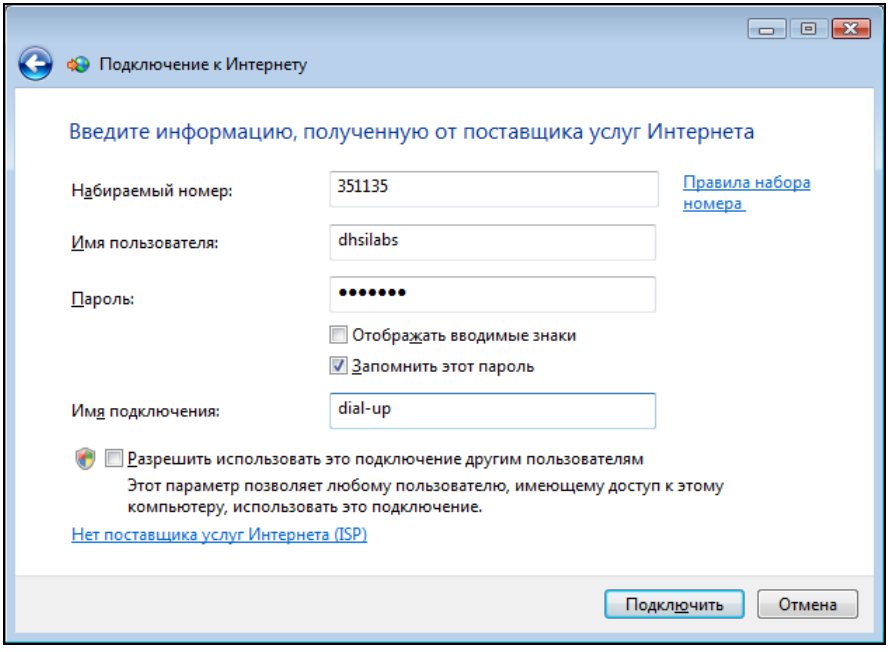


Рис. 6.31. Параметры соединения

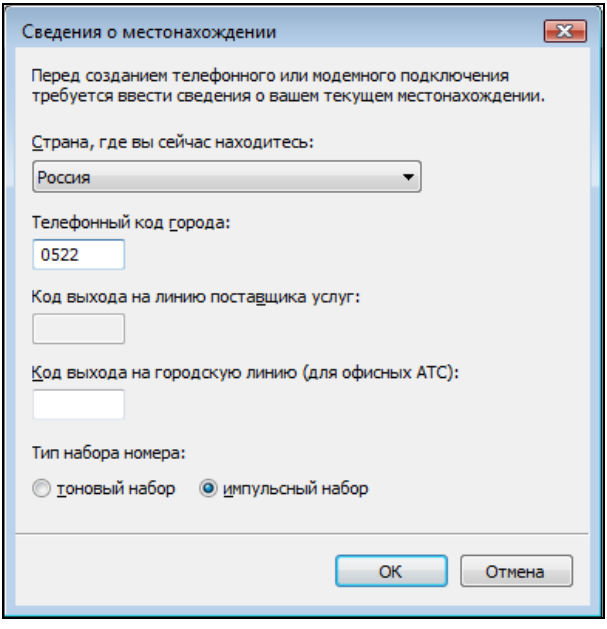


Рис. 6.32. Правила набора номера

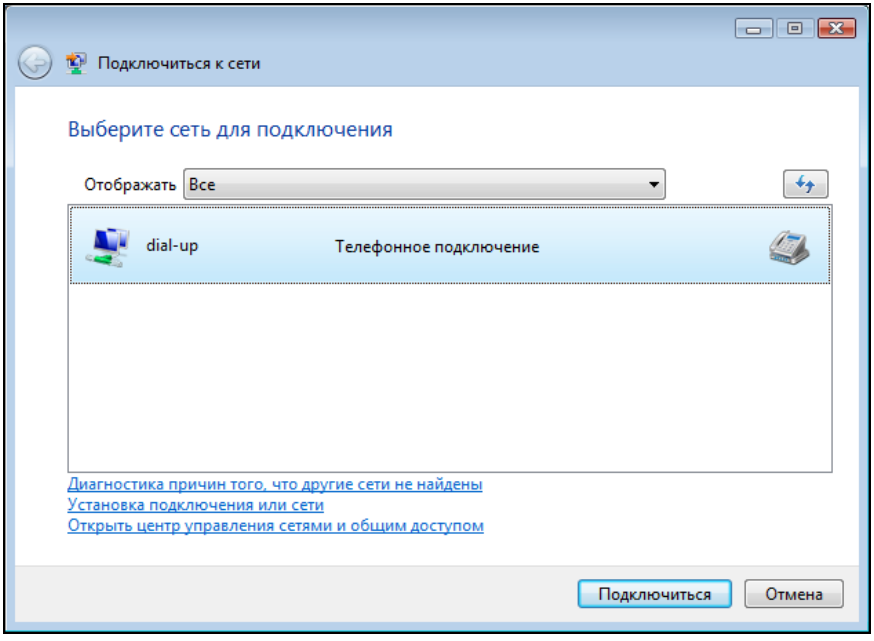


Рис. 6.33. Список подключений

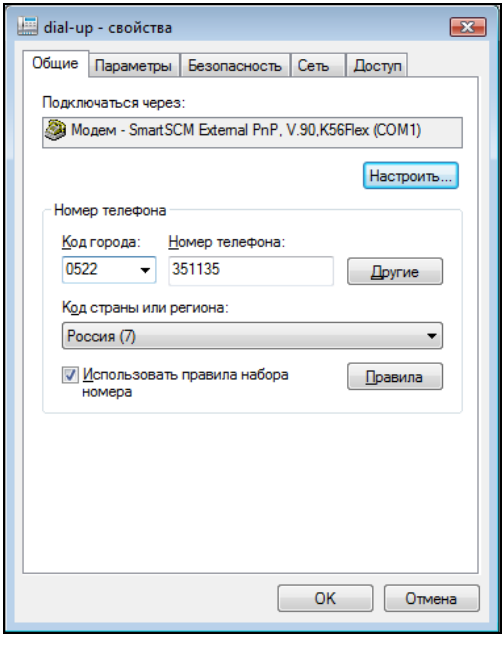


Рис. 6.34. Свойства подключения

После этого Vista запросит параметры соединения (рис. 6.31): номер телефона, имя пользователя и пароль, название соединения.

Нажмите ссылку **Правила набора номера** и в открывшемся окне (рис. 6.32) установите параметры набора номера, а именно: код города, префикс для выхода на городскую линию (если нужно) и тип набора номера.

Для проверки настроек можете нажать кнопку **Подключить**. Если у вас импульсная АТС, то подключиться, скорее всего, не получится, поскольку еще не задействованы правила набора номера. Для того чтобы задействовать эти правила, выполните команду **Пуск | Подключение**. Выберите из списка (рис. 6.33) ваше коммутируемое соединение, щелкните на нем правой кнопкой мыши и выберите команду **Свойства**.

В открывшемся окне нужно ввести код города и включить флажок **Использовать правила набора номера** (рис. 6.34).

После этого можно вернуться в окно списка подключений и нажать кнопку **Подключиться**. Вы увидите окно дозвона, очень похожее на аналогичное окно в Windows XP (рис. 6.35). Нажмите кнопку **Вызов** — через несколько секунд соединение будет установлено.

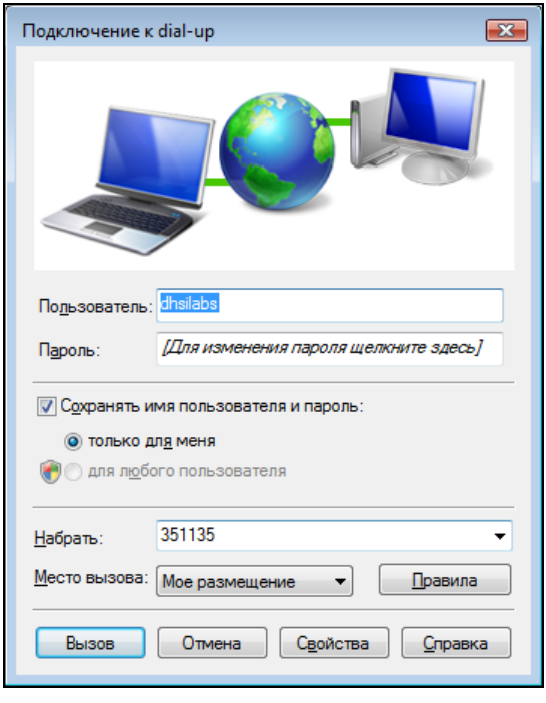


Рис. 6.35. Окно подключения

6.2. DSL-соединение

DSL (Digital Subscriber Line) — *цифровая абонентская линия*, позволяющая производить двунаправленный обмен данными по телефонной линии. Существует несколько вариантов DSL-линий: ADSL, VDSL, SDSL, RADSL. Наиболее распространены ADSL-линии. ADSL (Asymmetric DSL) — *асимметричная цифровая линия*, о ней мы в дальнейшем и будем вести речь. Для передачи данных используется витая пара телефонной сети. Скорость передачи данных зависит от расстояния до АТС — например, 1,5 Мбит/с при расстоянии в 5–6 км. Но обычно скорость ограничивается провайдером и зависит от тарифного плана. Самый доступный тарифный план подразумевает скорость передачи данных 64 Кбит/с.

6.2.1. Основная причина популярности: дешево и быстро

Почему ADSL-соединения стали такими популярными? Как гласит заголовок этого раздела, основная причина популярности — это скорость и дешевизна. Именно эти два фактора. Даже в самом "дешевом" варианте обеспечивается скорость передачи данных 64 Кбит/с. Это в два раза быстрее, чем позволяет модем (конечно, в идеальных условиях из модема можно "выжать" 56 Кбит/с, но на практике это получается далеко не всегда). И при этом никаких разрывов соединений!

Да, за подключение к провайдеру нужно заплатить определенную сумму (напомню, что модемное подключение бесплатно), но, поверьте, оно того стоит. Также понадобится специальный ADSL-модем (рис. 6.36), который стоит дороже обычного модема, но в большинстве случаев есть возможность взять модем в аренду у провайдера, а стоимость такой аренды просто смешная.

Рис. 6.36. ADSL-модем

Платить за работу в Интернете можно или почасово, или за реальный объем принятой/переданной информации (трафик). Что для вас выгоднее — решайте

сами. Если вы выбрали тарифный план с высокой скоростью соединения (от 512 Кбит/с), а Интернет нужен вам, в основном, чтобы скачивать что-то весьма объемное, например, видеофильмы, музыку, программы — тогда лучше выбрать почасовую оплату. Если же Интернет используется для обычной работы — и по сайтам побродить, и в ICQ пообщаться, тогда лучше выбрать тарифный план с оплатой по трафику.

Давайте прикинем — предположим, вы полдня провели за компьютером, общаясь в ICQ со своими друзьями. Вы передавали и принимали небольшие текстовые сообщения, т. е. реальный объем принятых и переданных данных был очень мал. Если платить почасово (учитывая, что в зависимости от вашего региона и жадности провайдера цена часа работы в Интернете может колебаться от 15 до 30 рублей), то за 4 часа работы вы заплатите от 65 до 130 рублей. А если считать по трафику, то это будет всего пара мегабайт (максимум) — даже при цене в 1,3 рубля (это максимальная цена, обычно ниже!) за мегабайт вы заплатите 3–5 рублей. Так выгоднее? Конечно!

Наоборот, если вам нужно скачать что-то объемное, например, видеофильм "весом" в 700 Мбайт, то при цене в 1,3 рубля за мегабайт фильм обойдется вам больше чем в 900 рублей (учитывая служебный трафик, за который вы тоже платите). Даже если принять, что обычная цена за 1 Мбайт ниже — примерно 0,8 рубля, то все равно выходит дорого — почти 600 рублей. При таких ценах дешевле купить этот фильм на CD. А вот если у вас почасовая оплата, то давайте посчитаем, что у нас получится. Если ваш тарифный план предполагает скорость передачи данных 512 Кбит/с (это 64 Кбайт/с), то за минуту вы скачаете 3,75 Мбайт. Следовательно, весь фильм скачается примерно за 186 минут. При стоимости часа работы в 30 рублей 186 минут закачки обойдутся вам в сумму около 100 рублей.

В любом случае к выбору тарифного плана нужно отнестись очень серьезно — ведь выбрав оптимальный план, вы сможете рационально расходовать средства на доступ к Интернету. Что же касается скорости доступа, то оптимальной является скорость не ниже 512 Кбит/с. Например, у меня сейчас тарифный план на 1,5 Мбит/с — поверьте, приятно наблюдать за тем, как файлы загружаются со скоростью 130–140 Кбайт/с.

Дешево, быстро — это все просто замечательно. Но есть еще одно преимущество — когда вы работаете в Интернете по ADSL, ваш телефон не занят, в отличие от модемного соединения. Но тут есть один нюанс — ADSL-соединение возможно не на каждой телефонной линии. Ваша телефонная линия должна быть цифровой, иначе ничего не получится.

6.2.2. Настройка ADSL-соединения в Windows XP

Установкой и настройкой ADSL-модема обычно занимается служба технической поддержки провайдера. Но вы просто должны знать, как все работает, — на случай, если когда-то придется настраивать его самому.

ADSL-модем подключается к телефонной линии через специальное устройство — ADSL-сплиттер, который обычно входит в комплект поставки модема. К ADSL-сплиттеру также подключается и обычный параллельный телефон. В свою очередь ADSL-модем подключается к компьютеру с помощью Ethernet-кабеля (витой пары), также входящей в комплект поставки. Схема подключения изображена на рис. 6.37.

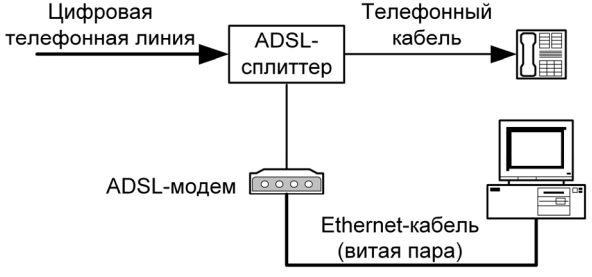


Рис. 6.37. Схема подключения ADSL-модема

Внимание!

Если у вас есть дополнительные параллельные телефоны, то не допускается их подключать к телефонной линии напрямую — только через ADSL-сплиттер.

После подключения модема к компьютеру нужно включить его питание — драйверы устанавливать не нужно. Для работы ADSL-соединения требуется только один драйвер, который уже обычно установлен — драйвер сетевой платы компьютера.

Примечание

Поясню, почему для ADSL-модема не нужен драйвер. Технология ADSL (как и многие другие технологии, например, Radio Ethernet) основывается на протоколе PPPoE (Point to Point Protocol over Ethernet). Протокол PPP используется обычным модемным соединением, в данном же случае получается, что PPP-кадры будут передаваться по сетевой плате (Ethernet), вот поэтому нам и не нужны никакие дополнительные драйверы. Если вы ничего не поняли, не беспокойтесь, а просто настраивайте соединение, как будет показано далее.

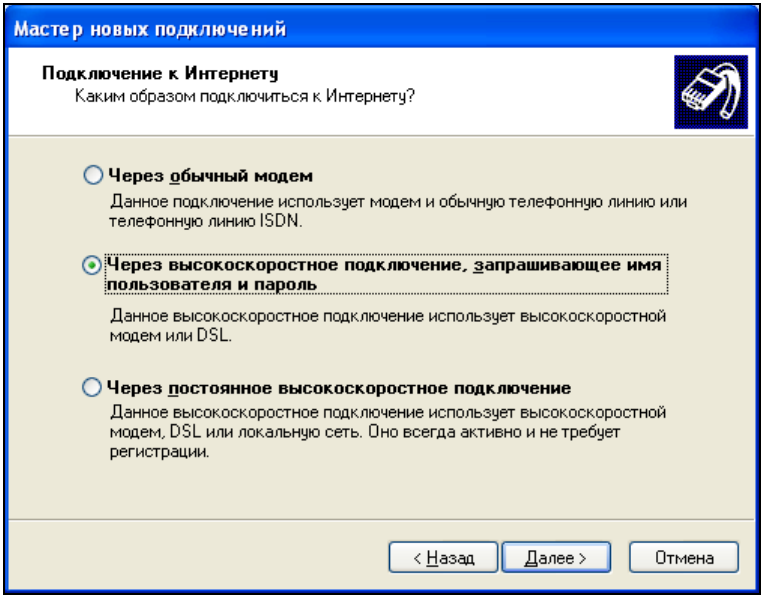


Рис. 6.38. Создание ADSL-соединения

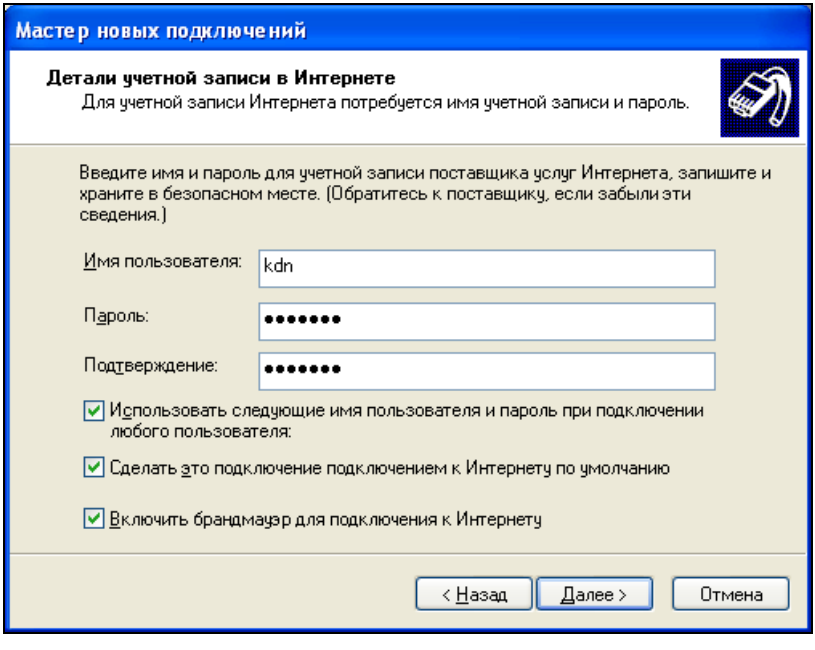


Рис. 6.39. Ввод имени пользователя и пароля

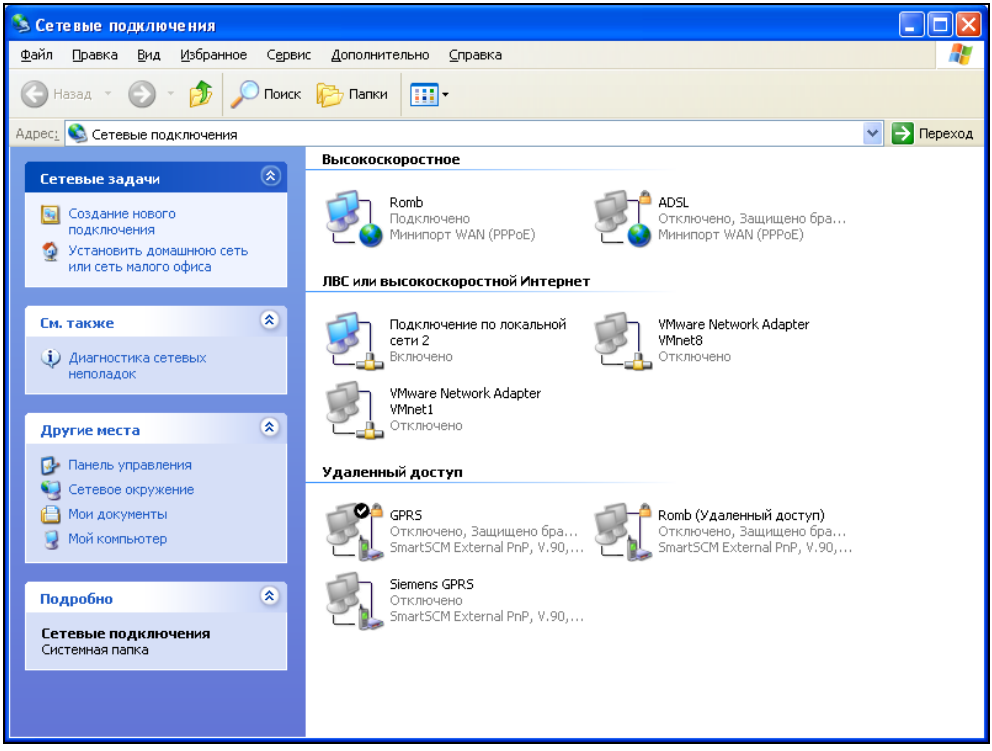


Рис. 6.40. Сетевые подключения

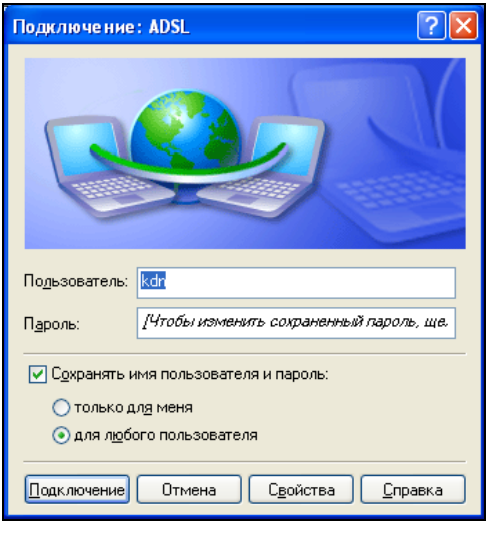


Рис. 6.41. Нажмите кнопку **Подключение**

Теперь приступим к настройке Windows. Откройте папку **Сетевые подключения** и запустите мастер новых подключений. Как обычно, выберите **Подключить к Интернету**, затем — **Установить подключение вручную**. После этого выберите опцию **Через высокоскоростное подключение, запрашивающее имя пользователя и пароль** (рис. 6.38).

Введите имя соединения (на свое усмотрение), затем имя пользователя и пароль (рис. 6.39).

В следующем окне нажмите кнопку **Готово**. Запустить соединение можно из папки **Сетевые подключения** (рис. 6.40) в группе **Высокоскоростное**.

Обычно не требуется устанавливать никакие дополнительные параметры — просто нажмите кнопку **Подключение** (рис. 6.41).

6.2.3. Настройка ADSL-соединения в Windows Vista

Подключив ADSL-модем к компьютеру, приступим к настройке ADSL-соединения. Откройте окно **Панель управления** (**Пуск | Панель управления**), выберите команду **Сеть и Интернет | Подключение к Интернету**. Если у вас уже есть подключения к Интернету, Windows об этом непременно сообщит. Вам следует выбрать **Нет, создать новое подключение** и нажать кнопку **Далее**. И в следующем окне выбрать тип подключения — **Высокоскоростное** (рис. 6.42).

> ***Примечание***
>
> Если вы не можете найти команду **Подключение к Интернету** в группе **Сеть и Интернет**, выполните команду меню **Пуск | Подключение** и в открывшемся окне — команду **Установка подключения или сети**. Можно также щелкнуть на названии группы **Сеть и Интернет** и в группе **Центр управления сетями и общим доступом** выбрать команду **Подключиться к сети** (см. рис. 6.30, *в*).

Как и в случае с модемным соединением, Vista запросит имя пользователя и пароль, а также название соединения (рис. 6.43).

Если имя пользователя и пароль правильные, Vista сообщит вам, что соединение успешно установлено, и предложит начать обзор Интернета (рис. 6.44).

Заново подключиться (после отключения) можно с помощью списка подключений (рис. 6.45), который вызывается командой меню **Пуск | Подключение**. Выберите соединение, нажмите кнопку **Подключиться**. Откроется окно установки соединения, в котором следует нажать кнопку **Подключение** (рис. 6.46).

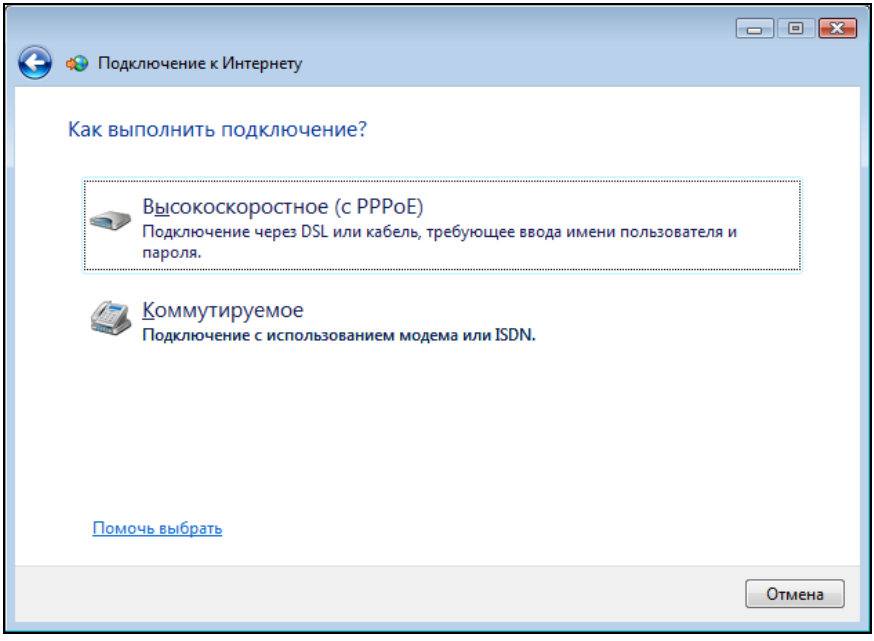


Рис. 6.42. Тип подключения

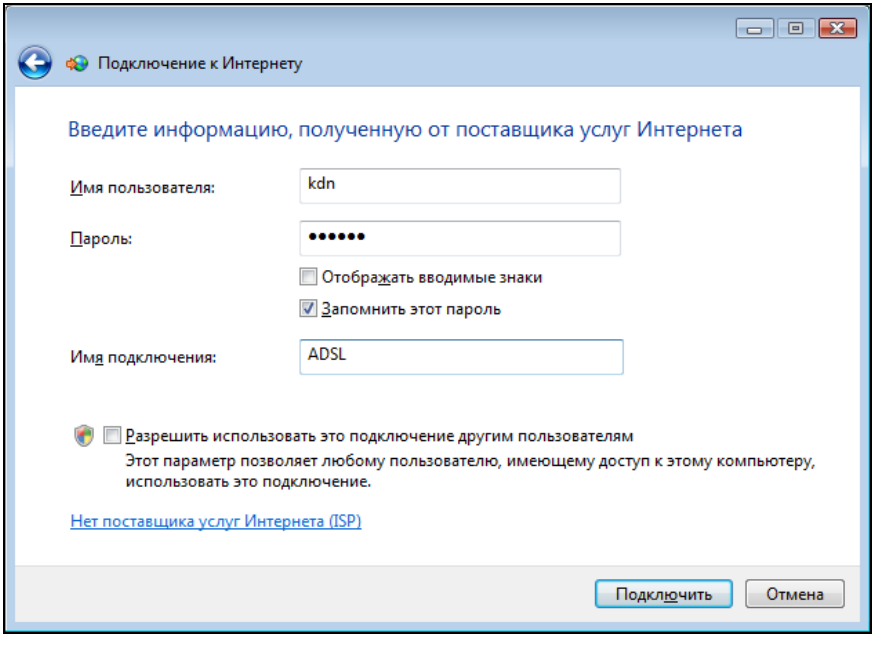


Рис. 6.43. Параметры соединения

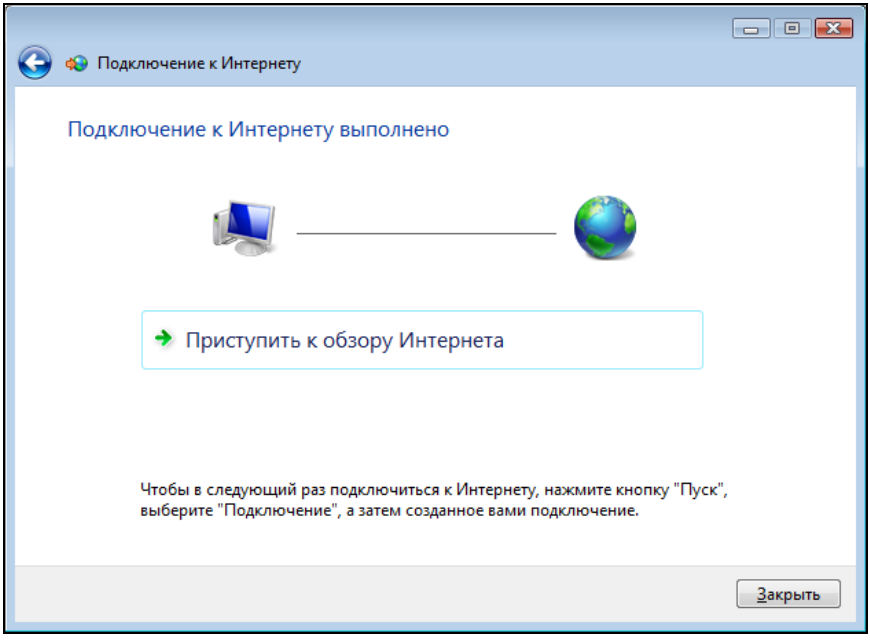


Рис. 6.44. Соединение установлено

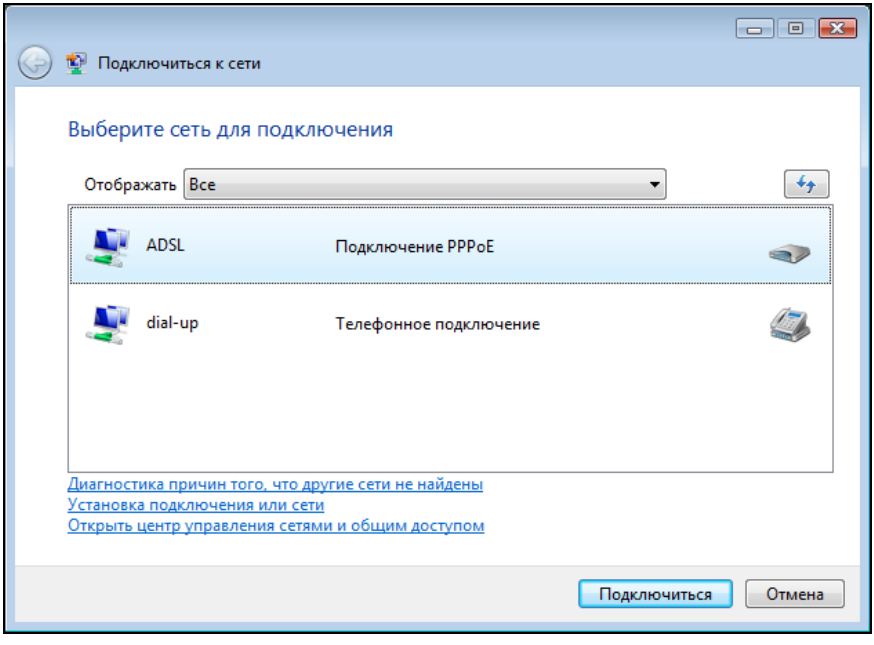


Рис. 6.45. Список подключений

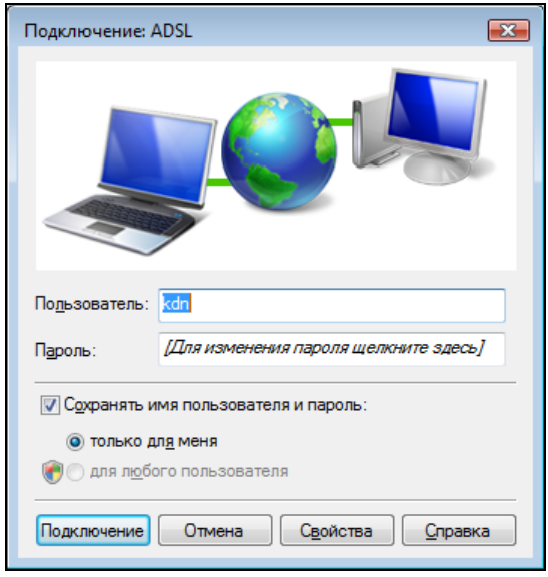


Рис. 6.46. Окно установки соединения

6.3. Альтернативные способы подключения к Интернету

Иногда нет возможности организовать ADSL-соединение (нет телефонной линии или телефонная линия не цифровая). Модемное соединение, как и GPRS, не устраивают по понятным причинам — оба эти соединения медленные, а второе вдобавок очень дорогое. Существуют альтернативные способы подключения к Интернету:

- выделенная линия;
- беспроводное подключение;
- спутниковое подключение.

> ***Примечание***
>
> Спутниковое соединение является "не совсем беспроводным", поэтому и выделено из состава беспроводных.

6.3.1. Выделенная линия

Выделенную линию организовать не всегда возможно, да и для домашнего пользователя организация выделенной линии и ее поддержка — весьма дорогое удовольствие. Поэтому данный способ сразу отпадает.

6.3.2. Беспроводное подключение и Radio Ethernet

В качестве беспроводных способов подключения к Интернету имеет смысл рассматривать, например, подключения Wi-Fi или Radio Ethernet. Первый случай — также "не совсем беспроводное" подключение. Суть его в том, что в вашей квартире (офисе) устанавливается *беспроводная точка доступа*, а все компьютеры в помещении оснащаются специальными Wi-Fi-адаптерами. От компьютеров до точки доступа данные передаются "по воздуху", а от самой точки доступа до оборудования провайдера, которое установлено в вашем доме (обычно в технических помещениях) прокладывается сетевой кабель (как правило, витая пара). Wi-Fi-доступ мы рассматривали в *главе 4* и не раз еще к нему в этой книге вернемся. Одно из преимуществ Wi-Fi-подключения заключается в том, что вам не нужно прокладывать в помещении кабели, которые портят интерьер.

А вот *Radio Ethernet* — это действительно выход из ситуации, когда организация ADSL-соединения невозможна. В этом случае данные с помощью специальной антенны передаются по воздуху прямо на сервер провайдера. Расстояние от вашего дома до помещения провайдера может составлять до 70 км, чего обычно вполне хватает. Понятно, что чем больше расстояние, тем меньше скорость обмена, но даже в самом плохом случае вы получите 128 Кбит/с, что в четыре раза превышает скорость модемного соединения.

Комплект оборудования Radio Ethernet состоит из направленной (или круговой) радиоантенны, которая подключается к точке доступа (access point). В свою очередь, точка доступа с помощью сетевого кабеля соединяется с вашим компьютером.

Настройка соединения Radio Ethernet аналогична настройке ADSL-соединения — нужно создать высокоскоростное подключение с помощью мастера новых подключений.

6.3.3. Спутниковое подключение

Соединение Radio Ethernet обычно организуется в пределах города (максимум — в пригороде), а вот если вы находитесь далеко от ближайшего провайдера Radio Ethernet, тогда единственный выход для вас — это спутниковое подключение. Но и тут есть свои нюансы. Спутниковое соединение обычно использует комбинированный способ передачи данных (так называемое *асинхронное спутниковое соединение*). Тогда по спутниковой антенне вы получаете информацию из Интернета (скорость получения информации при этом обычно не менее 128 Кбит/с), а вот отправка данных (в том числе служебных запросов) осуществляется по альтернативному каналу связи, например, по модему или GPRS-соединению.

Такое спутниковое соединение чревато двойной оплатой трафика. За принятый трафик и обслуживание спутниковой антенны вы платите "спутниковому" провайдеру, а за отправленный трафик платите другому провайдеру — сотовому оператору или провайдеру, предоставляющему модемный доступ.

> ***Примечание***
>
> Комплект асинхронного спутникового оборудования стоит от 4 тыс. рублей, а скорость приема может достигать 4 Мбит/с. Само собой, что скорость эта часто зависит от вашего тарифного плана.

Понятно, что если вы находитесь вне зоны покрытия сотового оператора, и у вас нет телефонной линии, организовать такое соединение не получится.

Выходом может стать *синхронное спутниковое соединение*. В этом случае передача и прием данных осуществляются с помощью специального приемно-передающего устройства. Достоинство одно — вы независимы от наземных линий и можете получить доступ к Интернету хоть на Южном полюсе. А вот недостаток тоже один — дороговизна:

- цена трафика на сегодняшний день не превышает 3 рублей за мегабайт (по сравнению с ADSL-соединением — это очень дорого);
- абонентская плата — порядка 6 тыс. рублей в месяц;
- необходима лицензия на использование СВЧ-радиопередатчика;
- стоимость оборудования — превышает 60 тыс. рублей.

Понятно, что такой вид подключения доступен немногим, но если другой возможности нет, а деньги — есть, тогда это единственный выход.

6.4. Правильное завершение работы в Интернете

Для правильного завершения работы в Интернете (все равно, какой тип подключения вы используете — модемное, ADSL или GPRS) в Windows XP нужно щелкнуть правой кнопкой мыши по индикатору соединения и выбрать команду **Отключить**. Об этом мы уже говорили, но стоит отметить отдельно (см. рис. 6.20). Если же вы хотите узнать, сколько времени провели в Интернете и сколько трафика израсходовали, выберите команду **Состояние** (рис. 6.47).

В Windows Vista нужно щелкнуть правой кнопкой мыши на индикаторе соединения, выбрать команду **Отключиться от**, а затем название соединения (рис. 6.48).

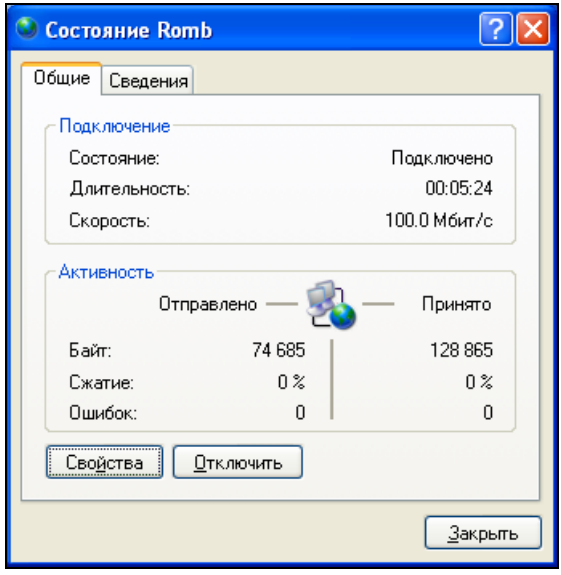


Рис. 6.47. Состояние соединения

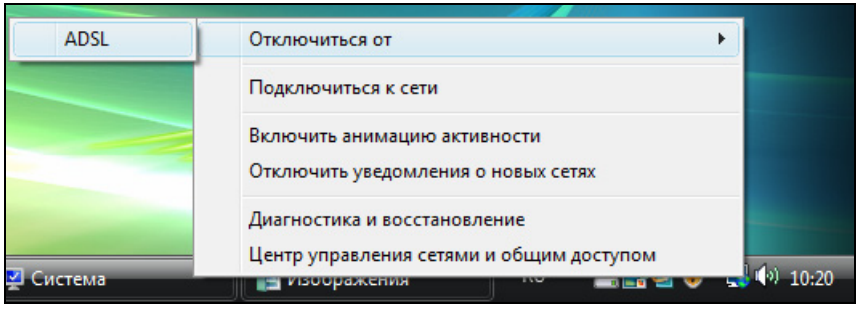


Рис. 6.48. Отключение соединения в Windows Vista

6.5. Решение некоторых проблем

В последнее время телефонные линии стали качественнее, а потому и проблем с ними меньше. В то же время широкое распространение получили высокоскоростные ADSL- или Radio Ethernet-соединения. Так вот, с этими соединениями иногда наблюдаются небольшие проблемы. Например, при попытке входа в сеть система сообщает, что удаленный компьютер недоступен (рис. 6.49).

"Лечится" такая проблема довольно просто — если у вас ADSL-модем, то нужно перезагрузить его, т. е. выключить, немного подождать и включить снова. Для соединения на основе Radio Ethernet следует перезагрузить точку доступа (access point). Если проблема не исчезла, придется обращаться в службу технической поддержки провайдера — вероятно, ошибка "на его стороне".

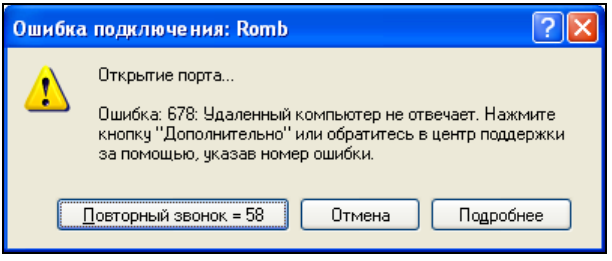


Рис. 6.49. Ошибка 678

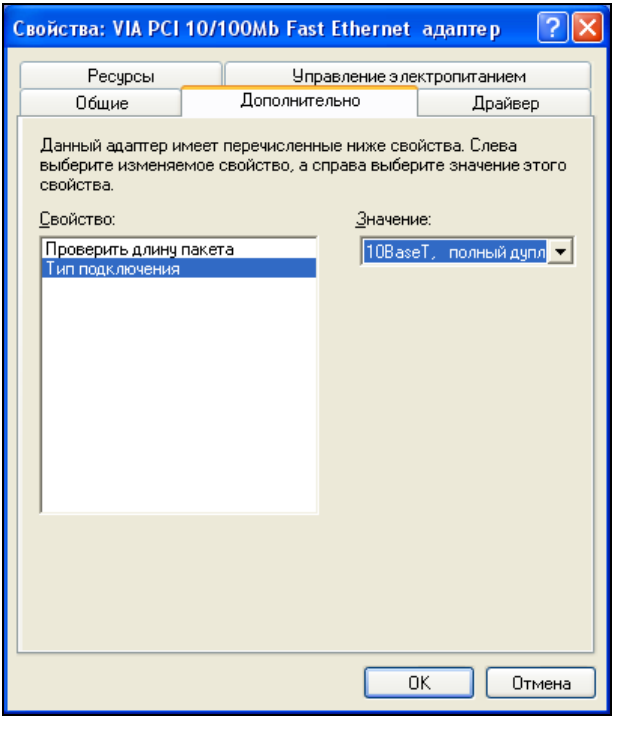


Рис. 6.50. Ограничение скорости работы сетевого адаптера

Иногда соединение начинает самопроизвольно и часто разъединяться. Симптомы следующие: вы вошли в сеть, поработали пару минут, потом соединение "упало". Вы соединяетесь заново, все отлично, но через некоторое время — опять разъединение. Если исключить неисправность оборудования (как с вашей стороны, так и со стороны провайдера), то причина может быть в неправильной работе драйвера сетевой платы. Попробуйте его переустановить. Можно также попытаться "зажать" сетевую плату на скорость 10 Мбит/с. Ведь по умолчанию сетевой адаптер работает в режиме Fast Ethernet, т. е. со скоростью 100 Мбит/с, а поскольку в большинстве случаев скорость ADSL-соединения не превышает 10 Мбит/с, то медленнее работать соединение от этого не станет, зато, возможно, будет работать стабильнее. Для ограничения скорости откройте свойства соединения по локальной сети. На вкладке **Общие** нажмите кнопку **Настройка**. В открывшемся окне (рис. 6.50) перейдите на вкладку **Дополнительно**, выберите тип подключения **10BaseT, полный дуплекс**.

Глава 7

Соединение с Интернетом в Linux

7.1. Модемное соединение

7.1.1. Подключение модема

В предыдущей главе мы рассмотрели преимущества и недостатки модемного соединения, поэтому здесь не вижу необходимости повторяться. Сейчас мы поговорим о подключении модема, а затем — о его настройке в Linux.

Сначала нужно подключить модем к компьютеру. Если у вас COM-модем, то перед его подключением выключите компьютер. Если же вы обзавелись USB-модемом, компьютер можете не выключать.

Затем подключите модем к телефонной линии. Обратите внимание: на задней панели модема (вне зависимости от типа: внутренний или внешний) имеются два гнезда с надписями: LINE и PHONE. Телефонную линию нужно подключать к гнезду LINE — не перепутайте! К гнезду PHONE при необходимости можно подключить параллельный телефонный аппарат.

В Linux файл устройства будет называться /dev/ttyS*n* для COM-модема или /dev/ttyUSB*n* для USB-модема. Здесь *n* — это порядковый номер устройства. Для COM-модемов он зависит от порта подключения: /dev/ttyS0 — COM1; /dev/ttyS1 — COM2 и т. д. Для USB-модемов — это просто его порядковый номер.

Далее для соединения с Интернетом вам нужно *программно* (ведь физически он уже подключен) настроить модем и соединение с провайдером.

Для соединения с провайдером по модемной линии возможны два протокола: SLIP (Serial Line Internet Protocol) и PPP (Point-to-Point Protocol). Первый сейчас уже не используется, поэтому мы будем рассматривать только PPP-соединения.

В этой главе мы рассмотрим четыре программы для установки dial-up-соединений: KPPP, GNOME PPP, KInternet и стандартную звонилку Ubuntu на базе той же GNOME PPP. Первая программа предназначена для использования в среде KDE, вторая — в среде GNOME. Обычно выбор графической среды происходит при установке системы. Если вы забыли выбрать среду или согласились с выбором по умолчанию, тогда вам придется использовать программу, основанную на библиотеках выбранной среды. Теоретически можно заставить программу KPPP работать в GNOME, но для этого потребуется установить библиотеки KDE, а это не имеет смысла, поскольку библиотеки занимают много места и устанавливать их ради одной KPPP (если сама KDE вам не нужна) — не разумно.

Программа Kinternet в основном применяется в openSUSE. И конфигуратор YaST при изменении параметров dial-up-соединения изменяет именно конфигурацию KInternet. Конечно, в openSUSE можно использовать GNOME PPP или KPPP, но я уверен практически на все 100%, что вы будете пользоваться именно KInternet.

Есть и еще одна программа — wvdial. Ее можно попробовать, если ни одна из упомянутых здесь программ недоступна. К тому же работает она в текстовом режиме, то есть графическая система X.Org для ее работы не нужна, что делает возможным использование программы на компьютерах без X.Org.

7.1.2. Программа KPPP

Настроить коммутируемое соединение можно с помощью конфигураторов настройки сети (system-config-network в Fedora или drakconnect в Linux Mandriva). Но намного удобнее (заметьте, я говорю "удобнее", а не "проще") воспользоваться имеющейся в любом дистрибутиве программой KPPP, что мы и сделаем.

Программа KPPP выполняет несколько функций. Во-первых, с ее помощью вы можете создавать, удалять и редактировать модемные соединения, причем она позволяет изменять намного больше параметров соединения, чем конфигураторы сети. Во-вторых, в отличие от конфигураторов сети некоторых дистрибутивов, KPPP способна самостоятельно установить соединение с Интернетом. В-третьих, программа KPPP доступна любому пользователю, а конфигуратор сети — только пользователю root.

Запустите программу KPPP с помощью одноименной команды (а можно выбрать ее из меню KDE — как кому нравится):

```
$ kppp
```

Если вы запускаете программу впервые и не настраивали модемных соединений с помощью конфигуратора сети, окно программы будет иметь вид, как показано на рис. 7.1.

Для начала настройки программы нажмите кнопку **Настроить**, и в открывшемся окне (рис. 7.2) — кнопку **Создать**.

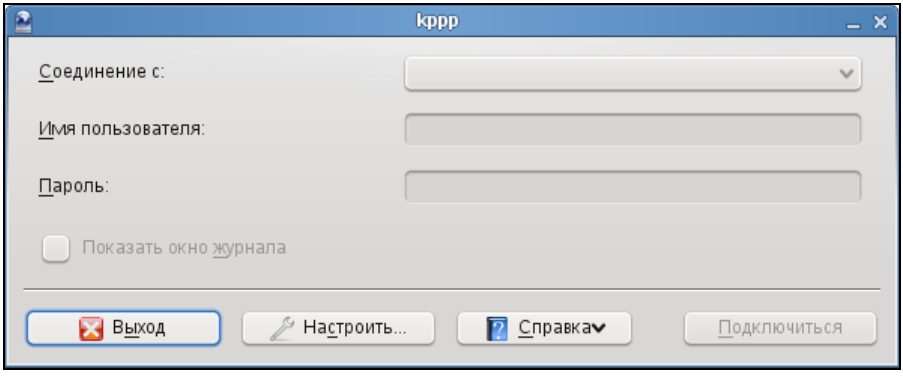


Рис. 7.1. KPPP — первый запуск

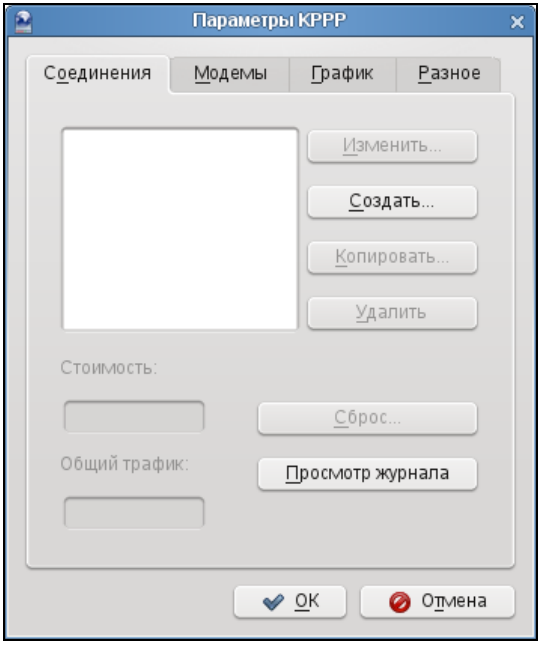


Рис. 7.2. Окно параметров KPPP

Программа спросит вас, желаете ли вы настроить соединение с помощью мастера или указать параметры вручную (рис. 7.3). Будет намного быстрее, если вы выберете ручную настройку.

Откроется окно нового соединения (рис. 7.4), где нужно указать название соединения и нажать кнопку **Добавить**, после чего ввести номер телефона модемного пула провайдера.

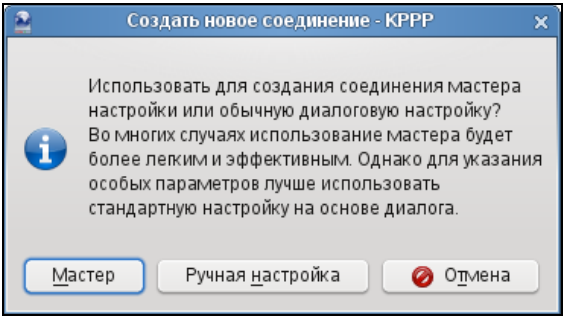


Рис. 7.3. Настраиваем соединение вручную

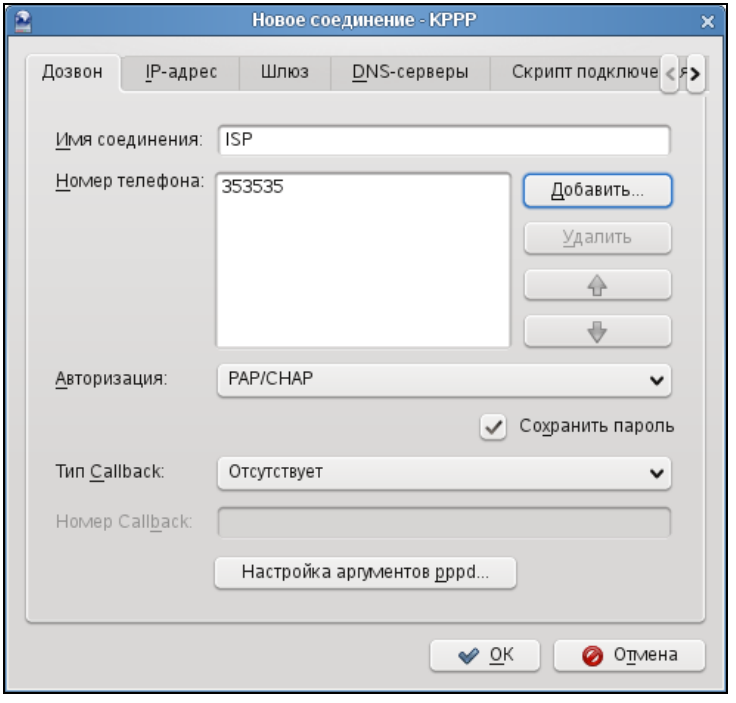


Рис. 7.4. Создание нового соединения

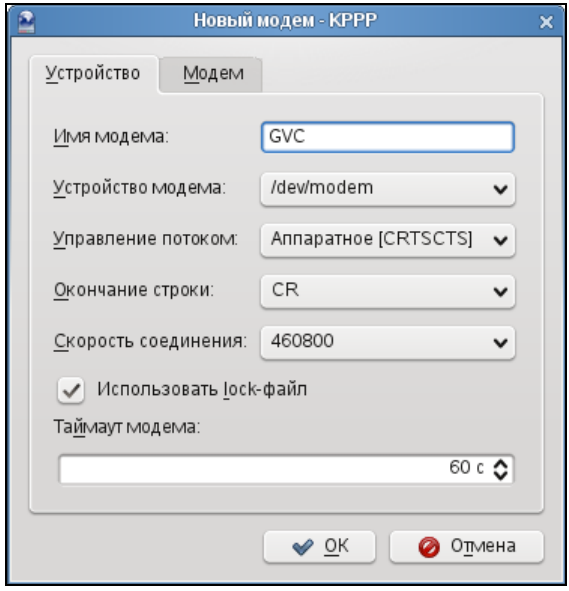


Рис. 7.5. Редактирование основных параметров модема

Больше никакие параметры соединения изменять не нужно, просто нажмите кнопку **OK**. В окне параметров KPPP (см. рис. 7.2) перейдите на вкладку **Модемы** и нажмите кнопку **Создать**. Откроется окно (рис. 7.5), в котором надо ввести название модема и указать файл устройства. Если у вас COM-модем, подключенный к COM1, укажите файл устройства /dev/ttyS0, для USB-модема — /dev/ttyUSB0. Для того чтобы точно узнать имя вашего USB-модема, воспользуйтесь утилитой usbview.

Теперь перейдите на вкладку **Модем** (рис. 7.6) и укажите громкость и время ожидания при занятой линии. Если вы введете 0 секунд, то программа автоматически наберет номер сразу же после получения сигнала "Занято".

Нажмите кнопку **Команды модема**. Найдите команду набора номера. По умолчанию задана команда ATDT. Если ваша АТС работает с импульсным, а не с тоновым типом набора номера, измените эту команду на ATDP (рис. 7.7), после чего нажмите кнопку **OK**.

Еще раз нажав кнопку **OK**, вернитесь в окно параметров KPPP (см. рис. 7.2) и перейдите на вкладку **Разное**. Поскольку KPPP — это оболочка для демона pppd, то в этом окне вы сможете узнать версию pppd, а также установить для него *тайм-аут* (время, которое дается на установку соединения, — если за это время соединение не будет установлено, связь разрывается). Отредактировать параметры демона можно в окне создания/редактирования соединения (см. рис. 7.4).

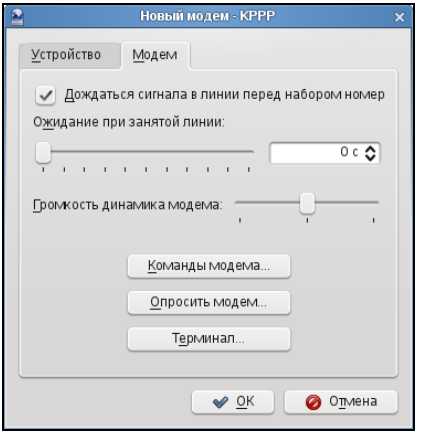


Рис. 7.6. Параметры модема

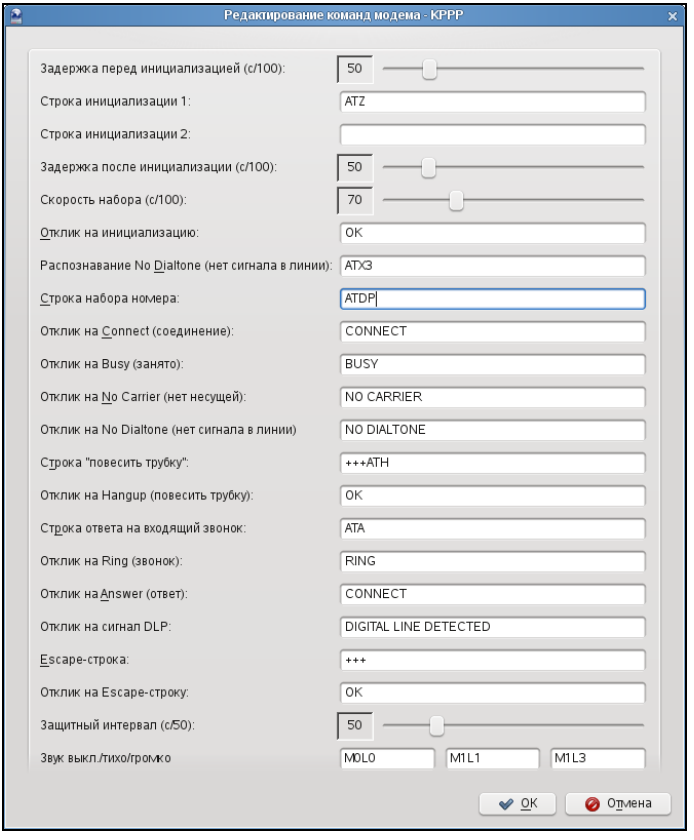


Рис. 7.7. Изменяем строку набора номера

На вкладке **Разное** вам доступны следующие опции:

- **Встроить в панель при соединении** — по умолчанию KPPP отображается в панели задач как обычное приложение, что не очень экономно по отношению к занимаемому на панели месту. Если данный режим включен, при установке соединения программа свернется в небольшой значок на панели задач (как в Windows);
- **Автодозвон при разъединении** — очень полезная опция: если соединение было разорвано (что часто случается), программа автоматически его восстановит;
- **Автодозвон при NO CARRIER**. Carrier — это несущая. Если модем не может определить несущую, особой надобности в повторном звонке нет — скорее всего, что-то случилось с телефонной линией;
- **Показывать время в строке заголовка** — программа будет показывать время соединения в строке заголовка;
- **Разъединить при остановке X-сервера** — если вы остановите X-сервер (или произойдет его сбой), программа автоматически разорвет соединение с Интернетом;
- **Выход при разъединении** — абсолютно бесполезная опция: если соединение будет разорвано, программа завершит свою работу;
- **Свернуть окно при соединении** — окно программы будет свернуто на панель задач при установке соединения.

Закончив настройку, нажмите кнопку **OK** в последний раз и в основном окне KPPP (рис. 7.8) введите имя пользователя и пароль. Нажмите кнопку **Подключиться** — через некоторое время соединение будет установлено.

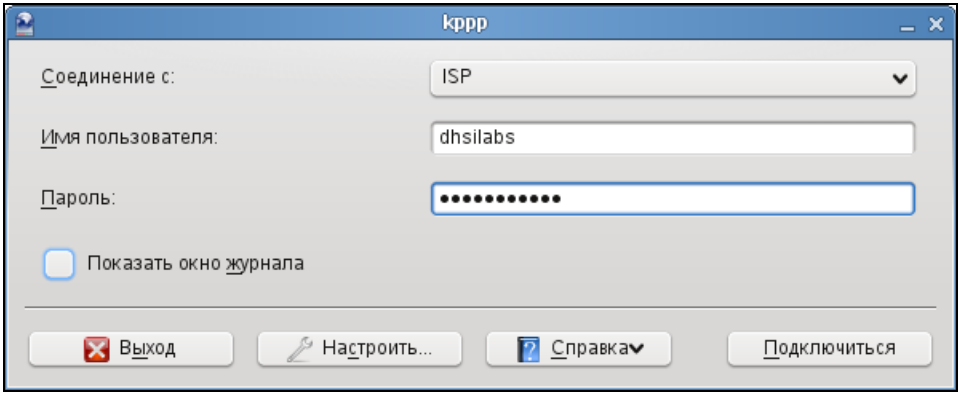


Рис. 7.8. Все настроено, можно подключаться

7.1.3. Программа GNOME PPP

Как уже было отмечено, программу KPPP можно использовать только, если вы работаете в графической среде KDE. В среде GNOME просто нет смысла устанавливать тяжеловесные библиотеки KDE только для запуска одной программы KPPP. Поэтому в GNOME вы будете пользоваться программой GNOME PPP. Пакет, содержащий программу GNOME PPP, называется аналогично, поэтому вы без проблем установите его с помощью менеджера установки пакетов.

В основном окне GNOME PPP (рис. 7.9) нужно указать имя пользователя, пароль и номер телефона провайдера. Но не спешите нажимать кнопку **Соединить** — следует еще настроить ваш модем.

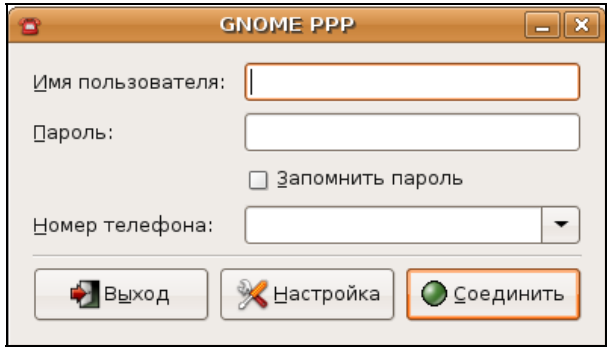


Рис. 7.9. Основное окно GNOME PPP

Нажмите кнопку **Настройка**. На вкладке **Модем** (рис. 7.10) нужно указать имя устройства модема (просто нажмите кнопку **Определить**). Затем надо задать максимальную скорость соединения. Не думайте, что если у вас модем 56К, а вы укажете скорость 115200, то он и будет работать с такой скоростью. Наоборот, иногда для большей надежности (на плохих линиях) требуется снизить скорость соединения. На старых линиях иногда полезно отключить параметр **Дожидаться гудка в линии** — тогда модем не будет дожидаться гудка, а сразу начнет набирать номер. Иногда это помогает, но, как правило, на такой линии хорошего соединения не будет.

Далее задаем способ набора номера: тональный или импульсный и громкость динамика. Если ваш модем требует указания специальной строки инициализации, вы ее можете задать, нажав кнопку **Строки инициализации**. Программа позволяет хранить несколько строк инициализации — на случай, если вы пользуетесь разными модемами.

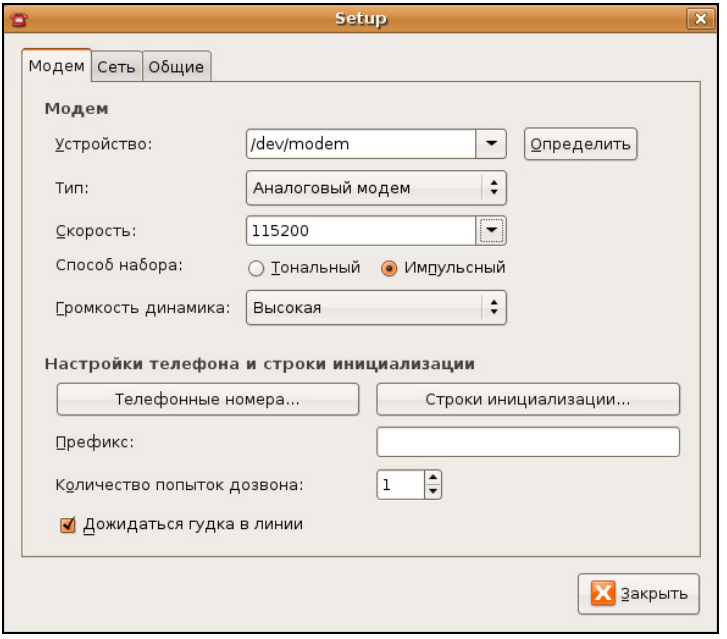


Рис. 7.10. Параметры модема

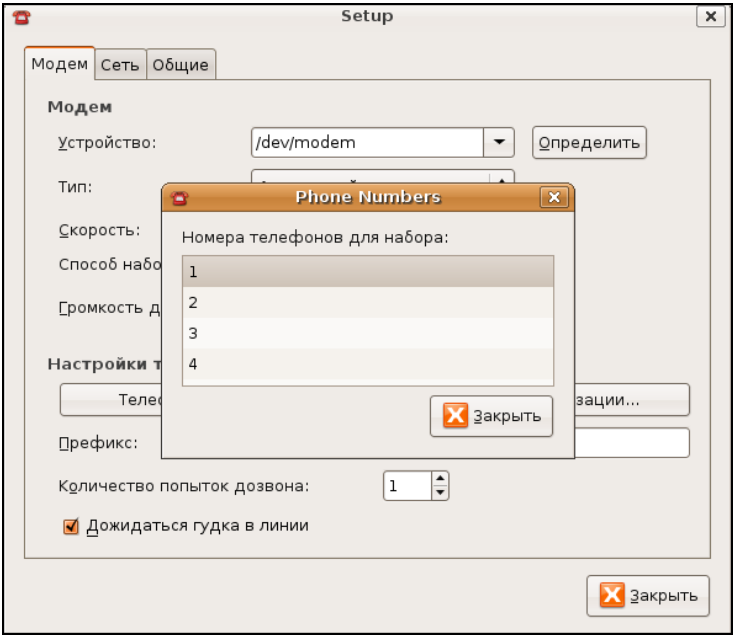


Рис. 7.11. Номера для дозвона к провайдеру

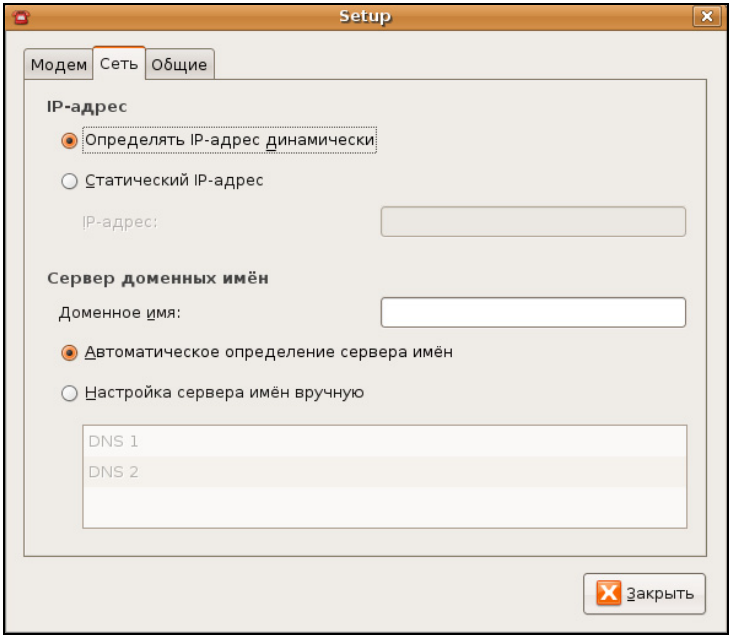


Рис. 7.12. Параметры сети — обычно устанавливаются автоматически

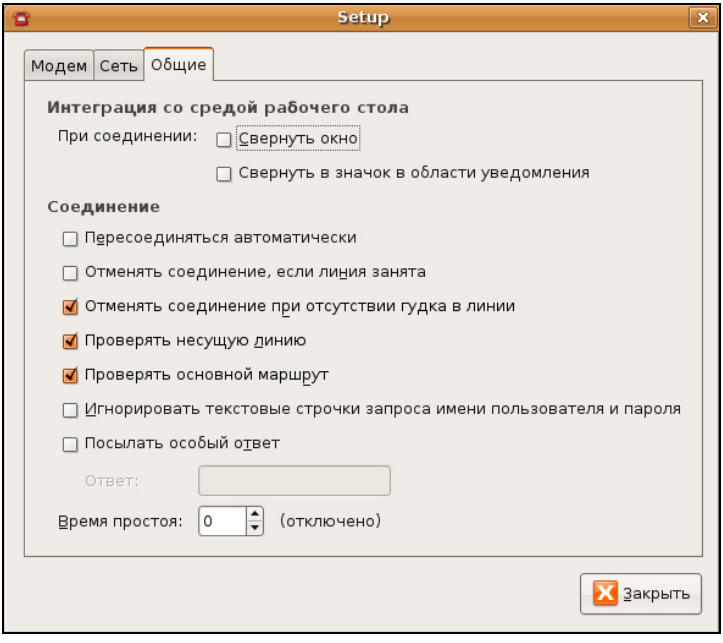


Рис. 7.13. Общие параметры программы

Кнопка **Телефонные номера** позволяет задать несколько номеров для дозвона к провайдеру (рис. 7.11).

Вкладка **Сеть** (рис. 7.12) позволяет задать IP-адрес и адреса DNS-серверов провайдера. Обычно эта информация приходит от DHCP-сервера провайдера, поэтому я не думаю, что вам нужно редактировать параметры, представленные на этой вкладке.

На вкладке **Общие** (рис. 7.13) можно определить общие параметры программы. Очень удобный параметр **Пересоединяться автоматически** позволяет в случае обрыва соединения установить его заново. Остальные параметры можно не изменять. Разве что установите параметр, сворачивающий программу в значок в области уведомлений, — так действительно удобнее.

Вот теперь можно нажать кнопку **OK**, а в главном окне (см. рис. 7.9) — кнопку **Соединить**.

7.1.4. Программа KInternet: модемное соединение в openSUSE

Для настройки модема запустите Центр управления и в группе **Оборудование** выберите **Модем** (рис. 7.14). Вы увидите окно обнаружения модема.

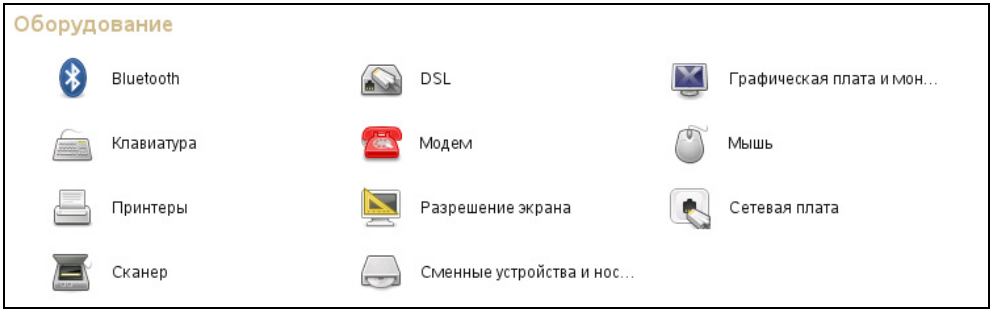


Рис. 7.14. Центр управления

> ***Примечание***
>
> Для непосредственного запуска (не через Центр управления) конфигуратора модема используется команда `/sbin/yast2 modem`.

Как только модем будет обнаружен, вы увидите окно, подобное изображенному на рис. 7.15.

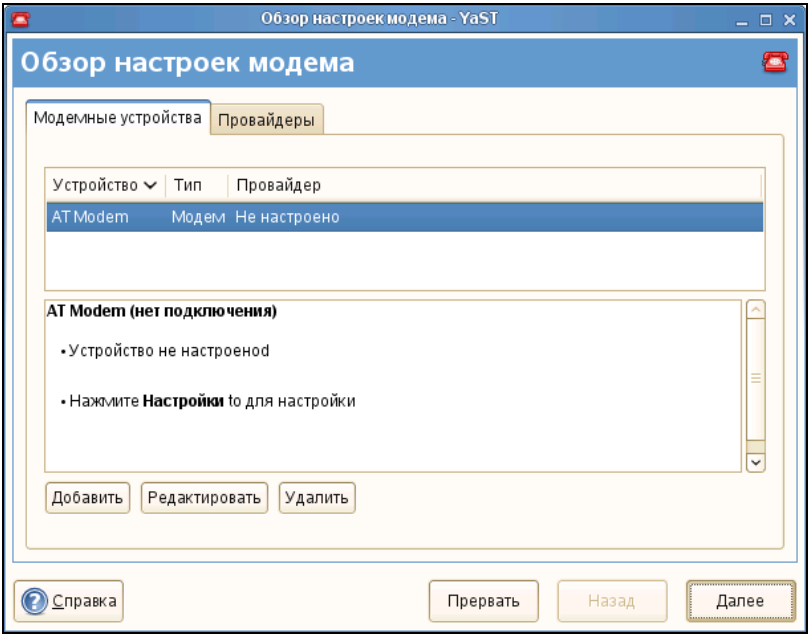


Рис. 7.15. Модем обнаружен

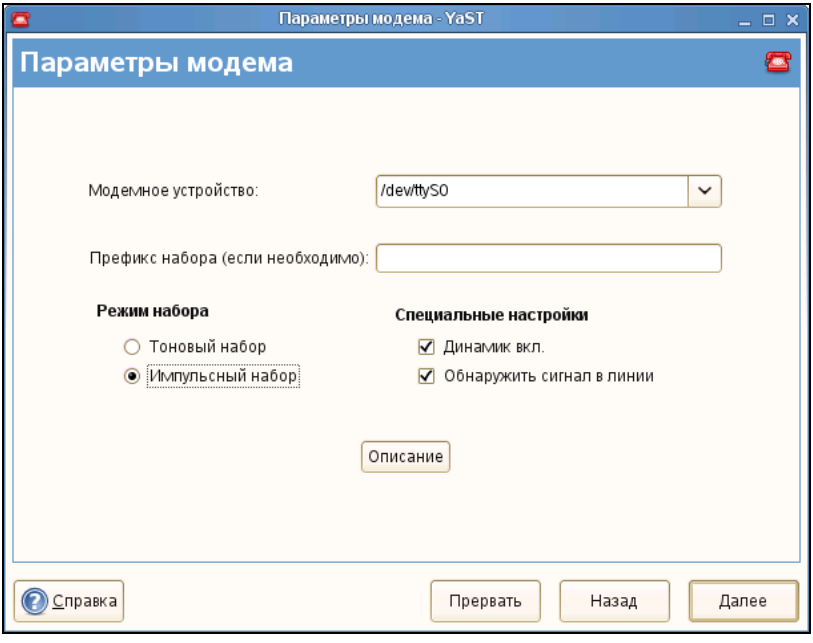


Рис. 7.16. Параметры модема

Нажмите кнопку **Редактировать** — ведь нам нужно сконфигурировать модем. В окне **Параметры модема** (рис. 7.16) вам нужно задать следующие параметры:

- **Модемное устройство** — обычно устройство правильно определяется конфигуратором, поэтому изменять его не нужно;
- **Префикс набора** — если ваш телефон принадлежит внутренней АТС;
- **Режим набора** — по умолчанию выбран тоновый набор, хотя в большинстве случаев используется импульсный.

После этого конфигуратор предложит вам выбрать провайдера (рис. 7.17). Даже не надейтесь, что ваш провайдер найдется в списке. Не теряя время на просмотр названий разных провайдеров, нажмите кнопку **Новый**. В открывшемся окне (рис. 7.18) введите название провайдера, номер телефона модемного пула, имя пользователя и пароль. Все эти параметры следует получить у провайдера.

Затем конфигуратор предложит установить параметры соединения (рис. 7.19). Обычно их можно не изменять.

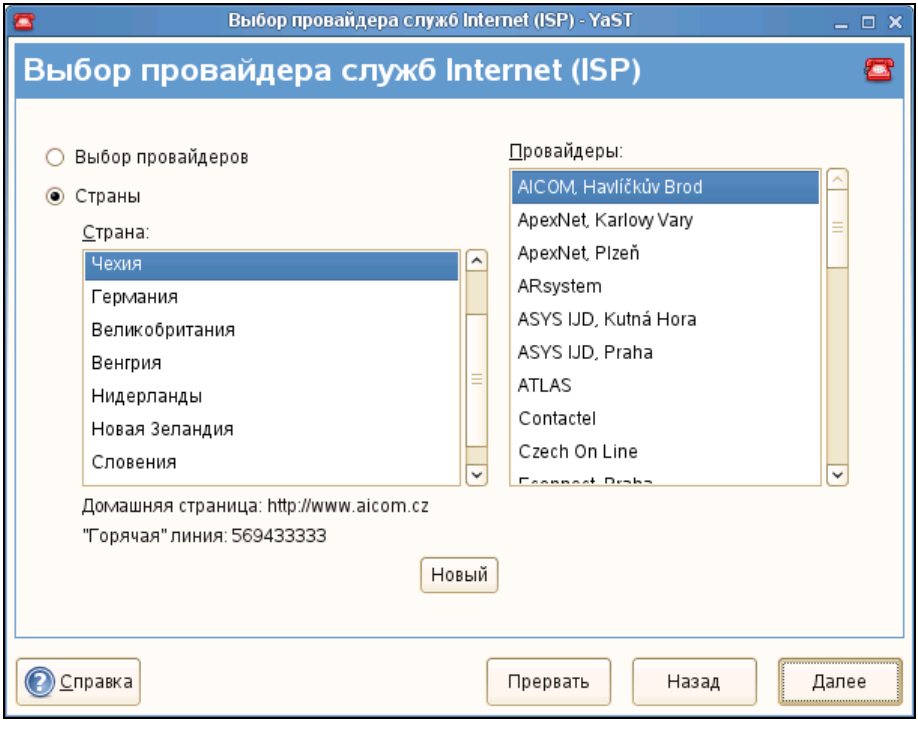


Рис. 7.17. Список провайдеров

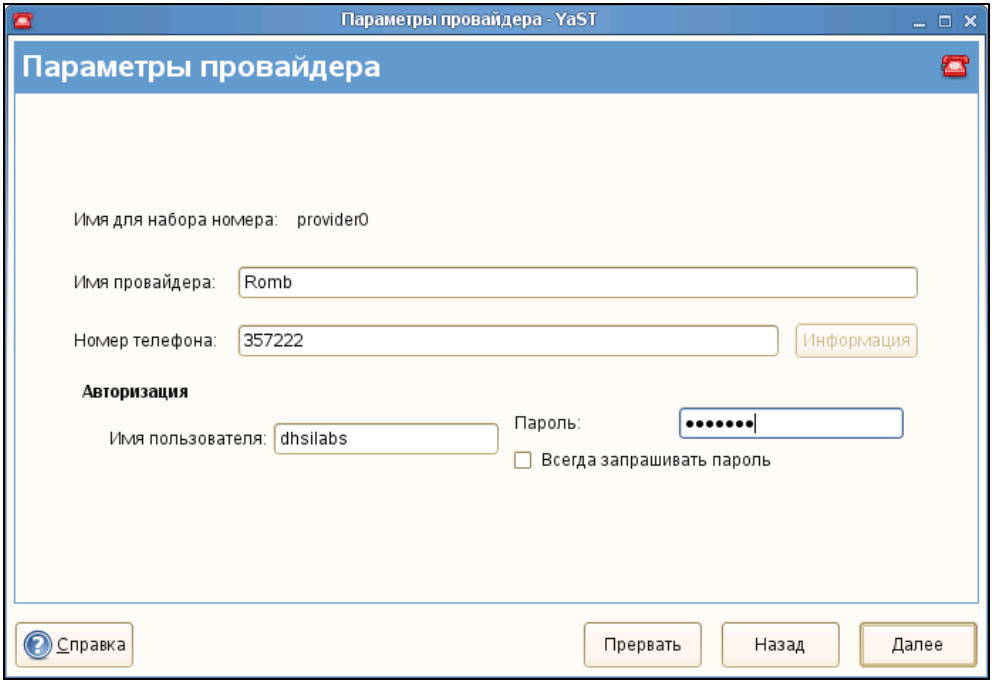


Рис. 7.18. Создание нового провайдера

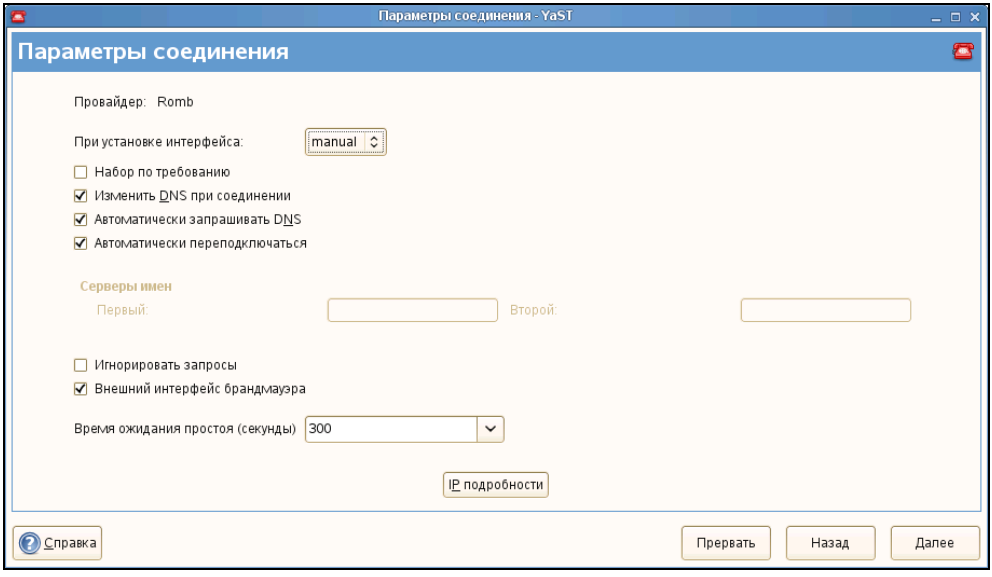


Рис. 7.19. Параметры соединения

Примечание

Иногда (в очень редких случаях) приходится принудительно указать имена DNS-серверов. Для этого следует снять флажок **Автоматически запрашивать DNS** и ввести IP-адреса первичного и вторичного DNS-серверов провайдера.

Нажав кнопку **Далее**, вы снова вернетесь в окно обзора настроек модема (рис. 7.20). Но перед нажатием кнопки **Далее** вставьте дистрибутивный диск openSUSE — конфигуратор установит некоторые дополнительные пакеты (smpppd, kinternet и др.).

Как уже было отмечено ранее, установка и разрыв интернет-соединения осуществляются с помощью программы KInternet, которая устанавливается в процессе настройки модема. Но почему-то сразу после установки программа может отказаться запуститься — тогда перезагрузите компьютер. После перезагрузки явно запускать программу не придется — она запустится автоматически. Обратите внимание на нижний правый угол экрана — программа KInternet отображается на панели GNOME в виде значка коннектора (рис. 7.21).

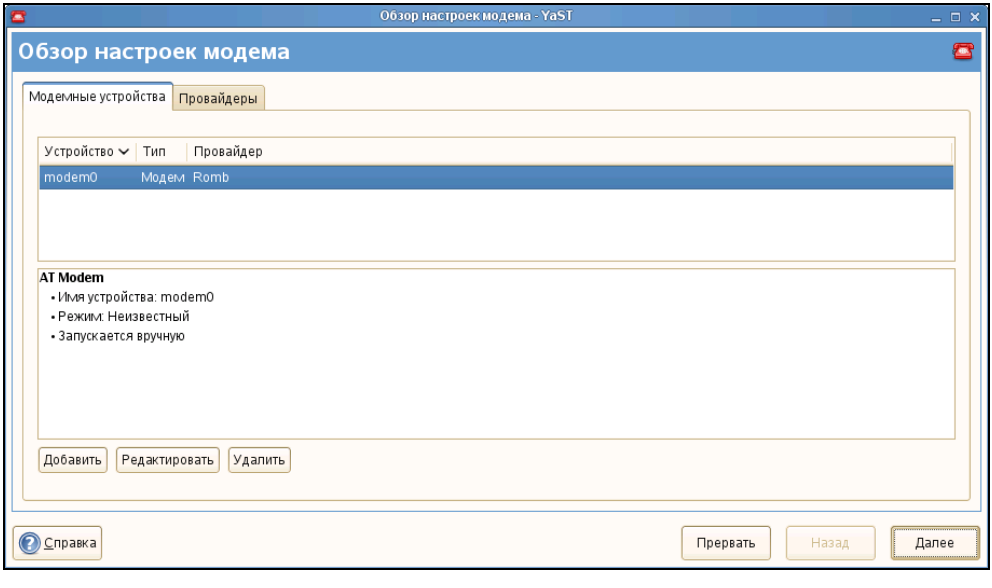


Рис. 7.20. Окно обзора настроек модема

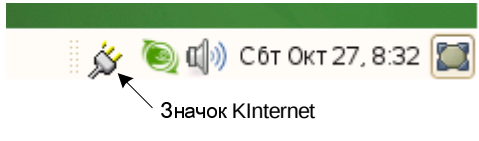


Рис. 7.21. Программа **KInternet** запущена

Как только вы щелкнете по значку **KInternet**, модем сразу же начнет набор номера. Далее следите за коннектором (значком программы) — если коннектор замкнут, значит, соединение установлено, и вы можете запускать браузер (**Компьютер | Firefox**) для путешествия по Интернету.

7.1.5. Настройка модемного соединения в Ubuntu

В Ubuntu используется графическая среда GNOME, но программа GNOME PPP не установлена по умолчанию. Чтобы установить ее, вам сначала нужно настроить dial-up-соединение с помощью стандартного конфигуратора, а затем ввести команду `sudo apt-get install gnome-ppp`. Запустить конфигуратор сети можно с помощью меню **Система | Администрирование | Сеть**. Нажмите кнопку **Разблокировать** для разблокировки конфигуратора, система запросит вас ввести пароль (нужно ввести ваш пароль, а не пароль root!). После чего выберите опцию **Соединение точка-точка** и нажмите кнопку **Свойства** (рис. 7.22). Далее вам нужно будет включить переключатель **Активировать соединение**, выбрать тип соединения: **Последовательный модем**, ввести имя пользователя, пароль, указать номер телефона (рис. 7.23) и способ набора номера (рис. 7.24).

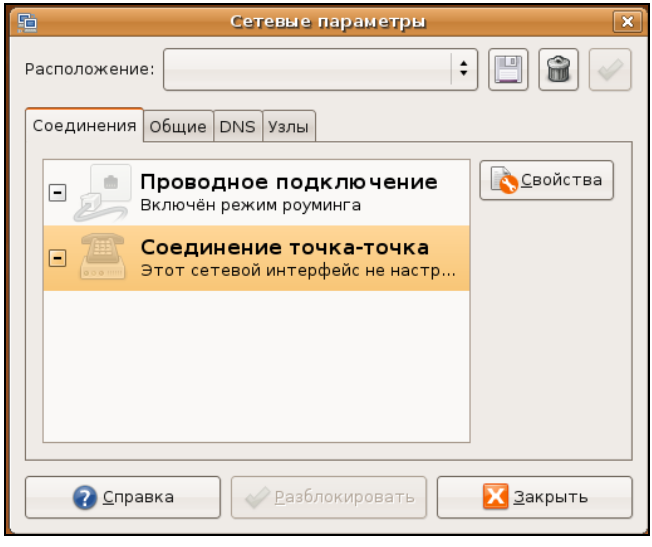


Рис. 7.22. Конфигуратор сети в Ubuntu

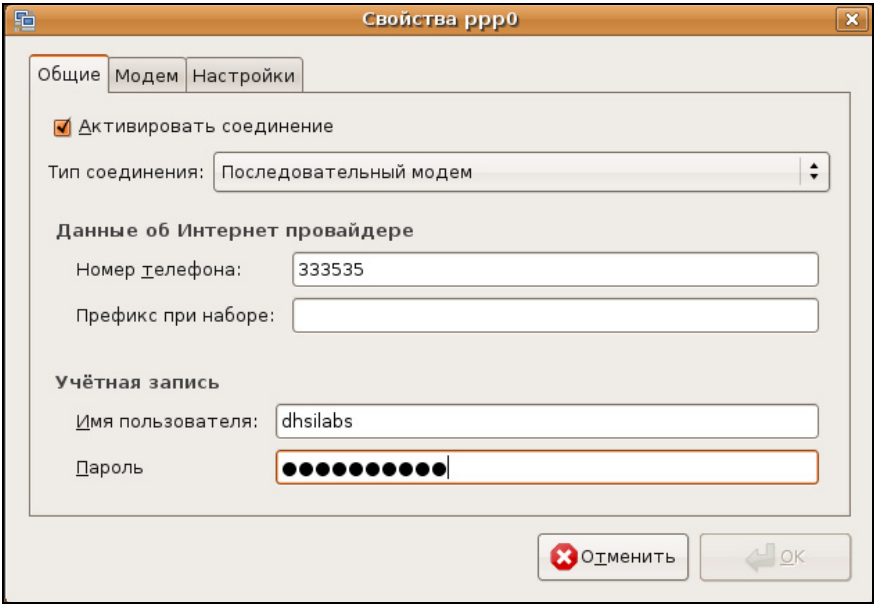


Рис. 7.23. Имя пользователя, пароль и номер телефона провайдера

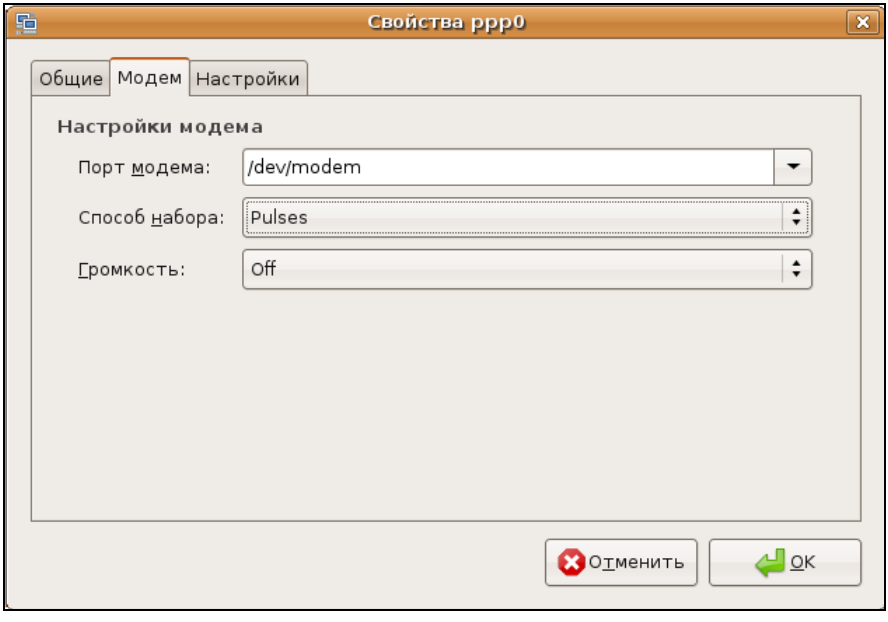


Рис. 7.24. Способ набора номера (тоновый или импульсный)

А теперь самое интересное: как же установить соединение? В более ранних версиях этого конфигуратора были кнопки **Включить/Выключить**. Сейчас же для установки соединения нужно нажать кнопку рядом со значком соединения. Когда соединение будет установлено, эта кнопка будет заменена на "галочку".

7.2. DSL-соединение

7.2.1. Настройка DSL-соединения в Fedora

В Fedora соединение проще всего настроить конфигуратором system-config-network. Запустите его и нажмите кнопку **Создать**, затем выберите опцию **Соединение xDSL** (рис. 7.25).

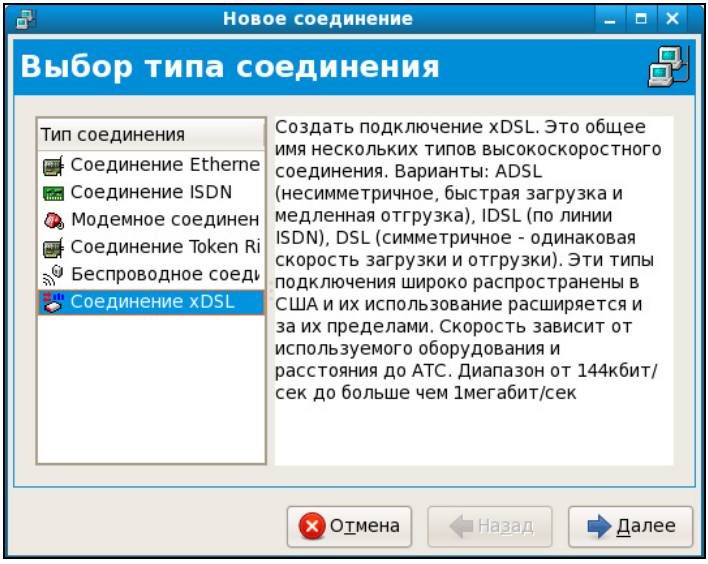


Рис. 7.25. Создание DSL-соединения в Fedora

Следующий шаг еще более важный — вам нужно выбрать устройство, которое соединено с точкой доступа, ввести имя провайдера, имя пользователя и пароль (рис. 7.26).

После чего нажмите кнопку **Далее**, а затем — кнопку **Применить**. Установить соединение можно командой `system-config-network`: выберите в открывшемся окне (рис. 7.27) ваше соединение и нажмите кнопку **Активировать**. Для разрыва соединения служит кнопка **Деактивировать**.

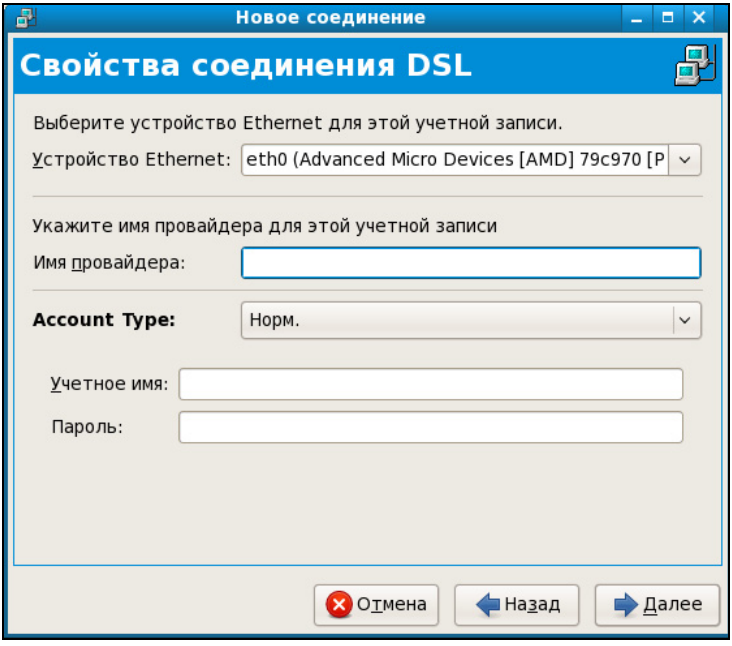


Рис. 7.26. Ввод параметров соединения

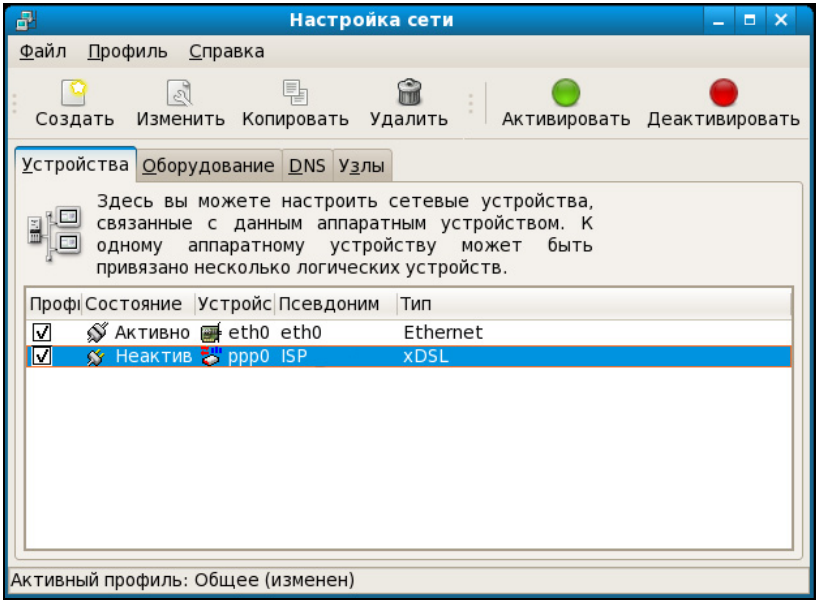


Рис. 7.27. Включение/выключение соединения

7.2.2. Настройка DSL-соединения в openSUSE

Запустите Центр управления и выберите **DSL**. Пользователям радио-доступа к Интернету (технология Radio Ethernet) тоже нужно использовать конфигуратор DS — настройка Radio Etherhet осуществляется аналогично настройке DSL.

> ***Примечание***
>
> Для непосредственного запуска (не через Центр управления) конфигуратора модема используется команда `/sbin/yast2 dsl`.

Конфигуратор попытается найти DSL-устройства — это может занять некоторое время, так что придется немного подождать (рис. 7.28). Затем вы увидите пустое окно обзора настроек DSL, как будто не найдено ни одного DSL-устройства. Не пугайтесь — так и должно быть. Просто нажмите кнопку **Далее**. Вам понадобится задать параметры DSL-соединения (рис. 7.29), а именно: выбрать режим PPP, выбрать сетевую плату, к которой подключен DSL-модем, выбрать режим активации устройства и обязательно разрешить управление соединением через KInternet (иначе вы просто не сможете использовать KInternet).

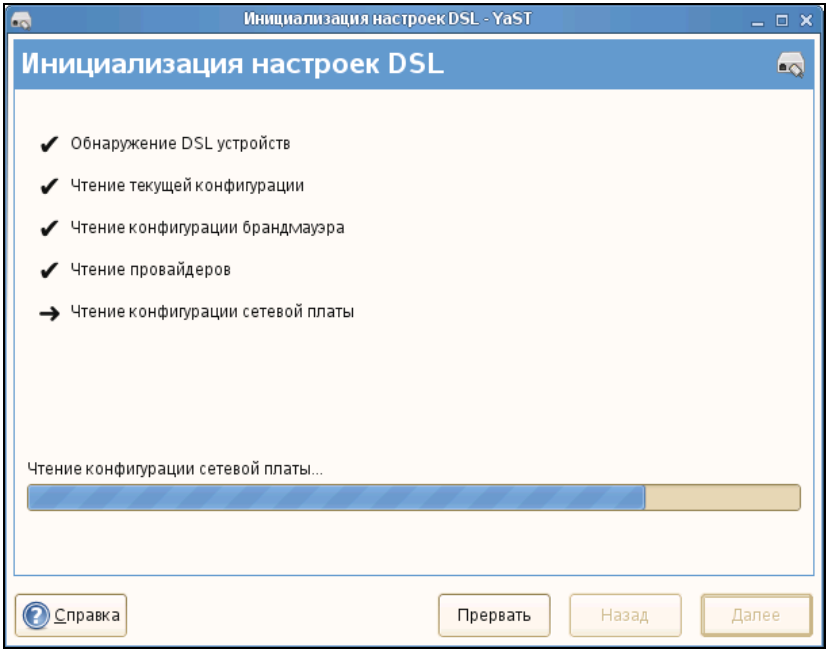


Рис. 7.28. Поиск DSL-устройств

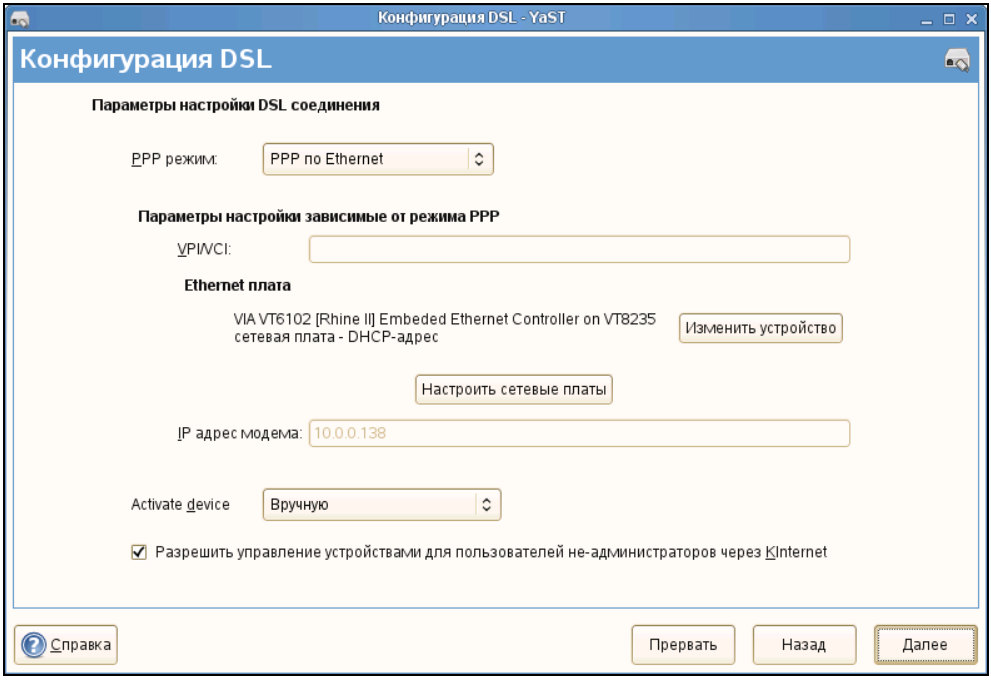


Рис. 7.29. Параметры DSL-соединения

Начнем с режима PPP. Обычно используется режим **PPP по Ethernet**. Технология ADSL (как и другие технологии, например, Radio Ethernet) использует протокол PPPoE (Point to Point Protocol over Ethernet).

> ***Примечание***
>
> Суть режима PPP по Ethernet в том, что PPP-кадры (обычно передаваемые по модемному соединению) здесь передаются по сетевой плате Ethernet.

Сетевая плата обычно выбирается конфигуратором правильно, поэтому ее не нужно изменять, тем более, что в большинстве случаев найденная сетевая плата является единственным сетевым адаптером в системе.

Режим активации устройства (**Activate device**) позволяет определить, как будет активироваться устройство — вручную или автоматически при запуске системы. Тут решать вам — можно запускать DSL-соединение и при запуске системы, но тогда отпадает необходимость в использовании KInternet.

Следующий этап настройки DSL-соединения — это выбор провайдера. Вашего провайдера не будет в списке, поэтому сразу нажимайте кнопку **новый** и вводите имя провайдера, имя пользователя и пароль (рис. 7.30).

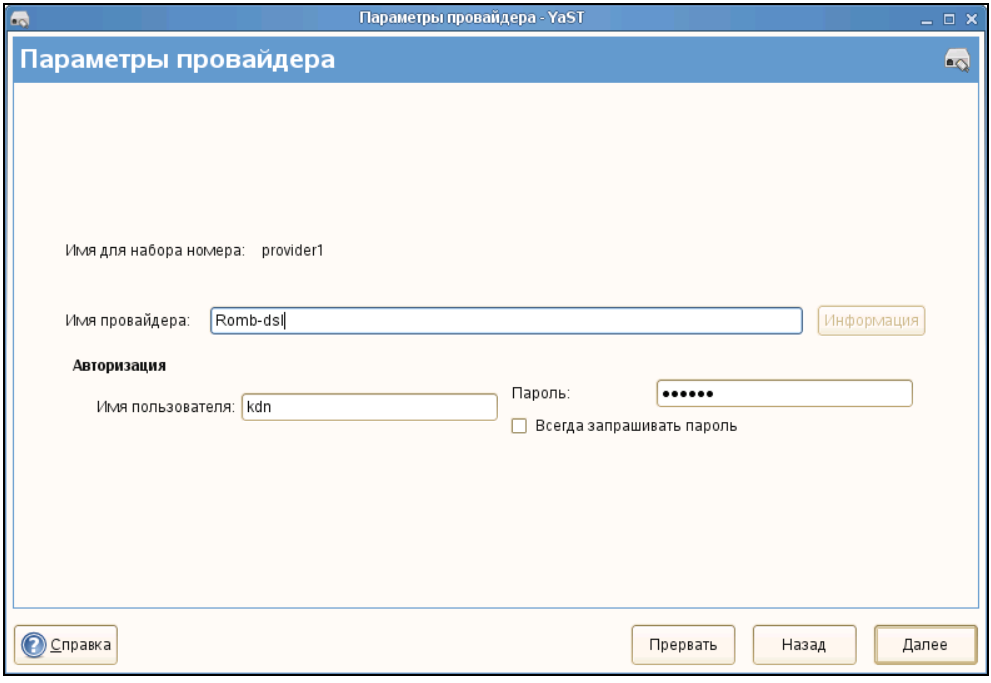


Рис. 7.30. Информация о провайдере

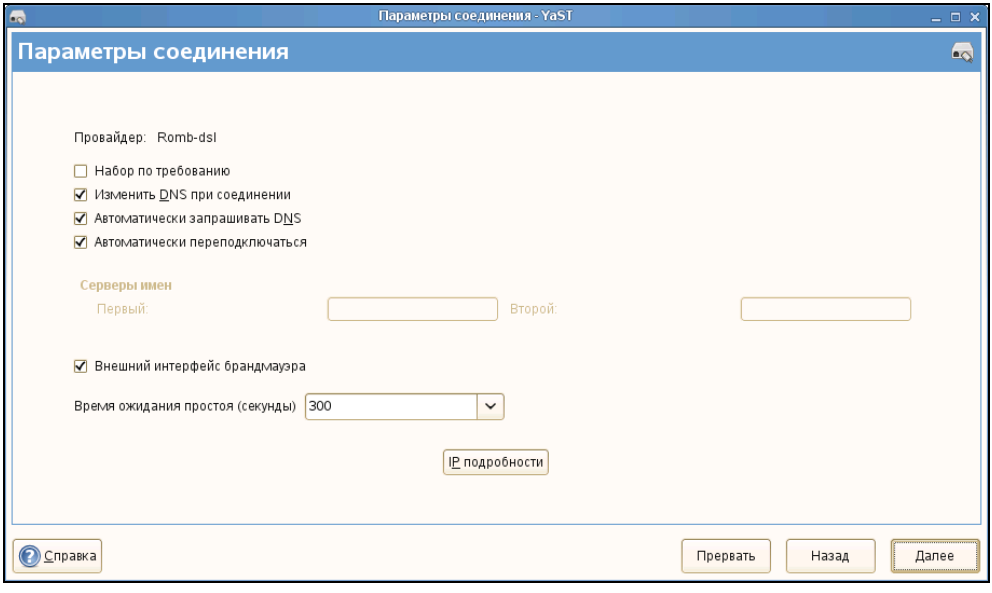


Рис. 7.31. Параметры соединения

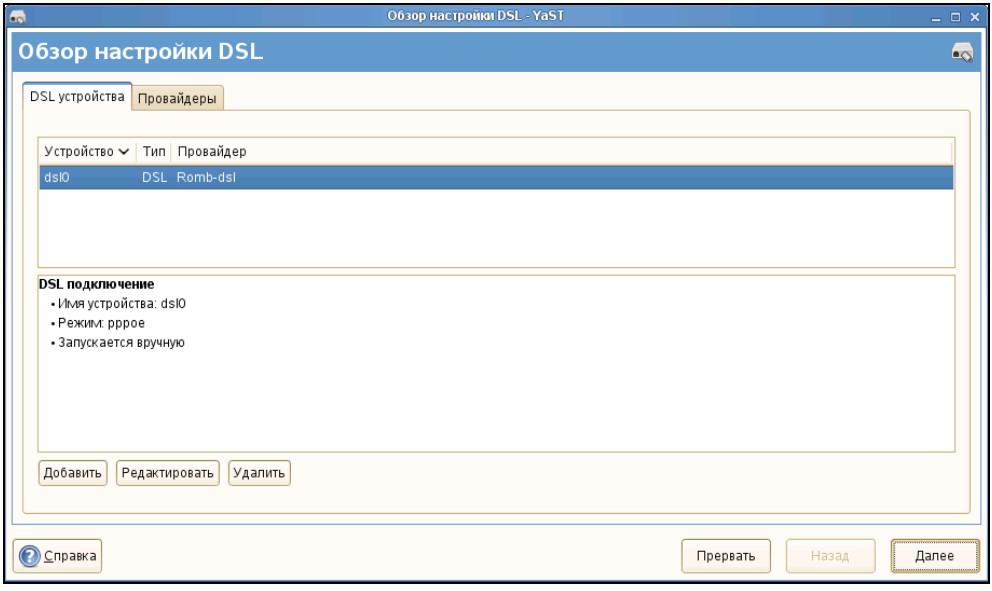


Рис. 7.32. Созданное соединение

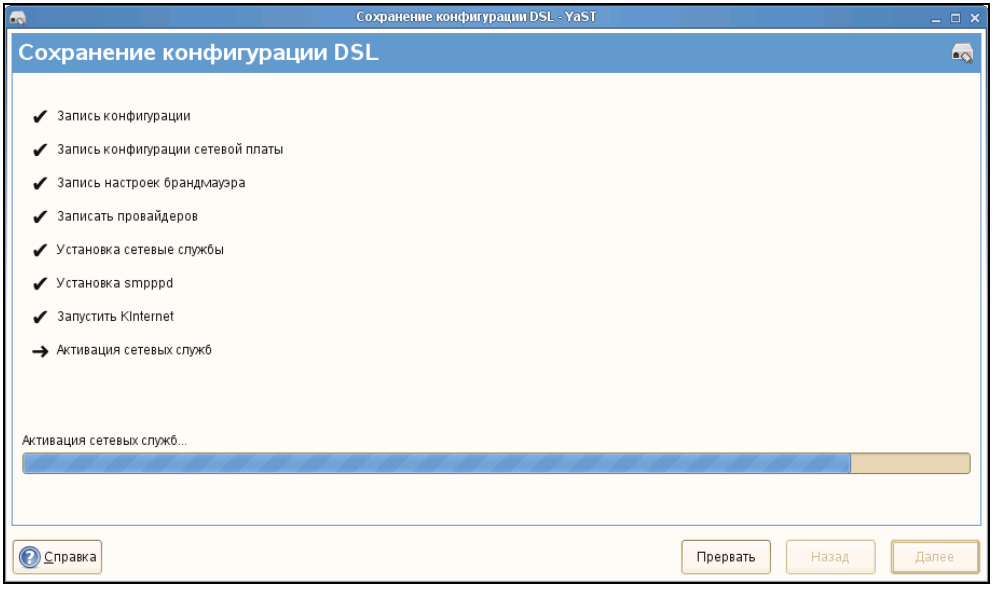


Рис. 7.33. Сохранение конфигурации

Теперь нужно определить некоторые параметры соединения. Параметры, предложенные конфигуратором, вполне приемлемы и устроят большинство пользователей, поэтому просто просмотрите их (рис. 7.31) и нажмите кнопку **Далее**. Вы вернетесь в окно обзора DSL-соединений, которое теперь не будет пустым, — в нем появится только что созданное соединение (рис. 7.32).

Все, что вам осталось — это нажать кнопку **Далее** и подождать, пока YaST сохранит конфигурацию системы (рис. 7.33).

Для подключения к Интернету нужно щелкнуть по значку **KInternet**. Но если вы до этого настраивали модемное соединение, то у вас теперь имеется два подключения (модемное и DSL), и сейчас надо выбрать DSL-подключение. Для этого предварительно щелкните правой кнопкой мыши по значку **KInternet** и из открывшегося меню выберите команду: **Интерфейс, dsl0**. Вот теперь можно щелкнуть по значку левой кнопкой мыши для установки соединения (рис. 7.34, *а*). Для отключения, как обычно, нужно снова щелкнуть по значку **Kinternet** (рис. 7.34, *б*).

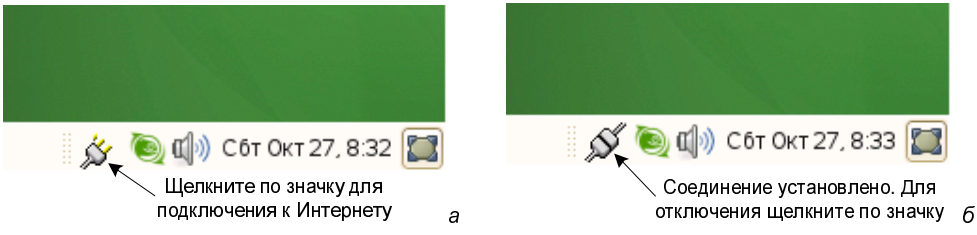


Рис. 7.34. Значок **Kinternet**: *а* — включаем соединение; *б* — отключаемся

7.2.3. Настройка DSL-соединения в Ubuntu

В дистрибутивах Debian и Ubuntu для настройки DSL-соединений используется конфигуратор pppoeconf. Введите команду:

```
sudo pppoeconf
```

> ***Примечание***
>
> В Ubuntu 8.10 появился еще один конфигуратор DSL-соединения, запустить который можно с помощью команды меню **Система | Параметры | Network Configuration**. Создать DSL-соединение можно на вкладке **DSL**.

Согласно спецификации PPPoE существуют две стадии процесса: стадия поиска и стадия сессии. На первой стадии производится отправка специальных

пакетов PADI (PPPoE Active Discovery Initiation), которые позволяют найти активные концентраторы доступа PPPoE (рис. 7.35). Стадия сессии — это само соединение и передача информации.

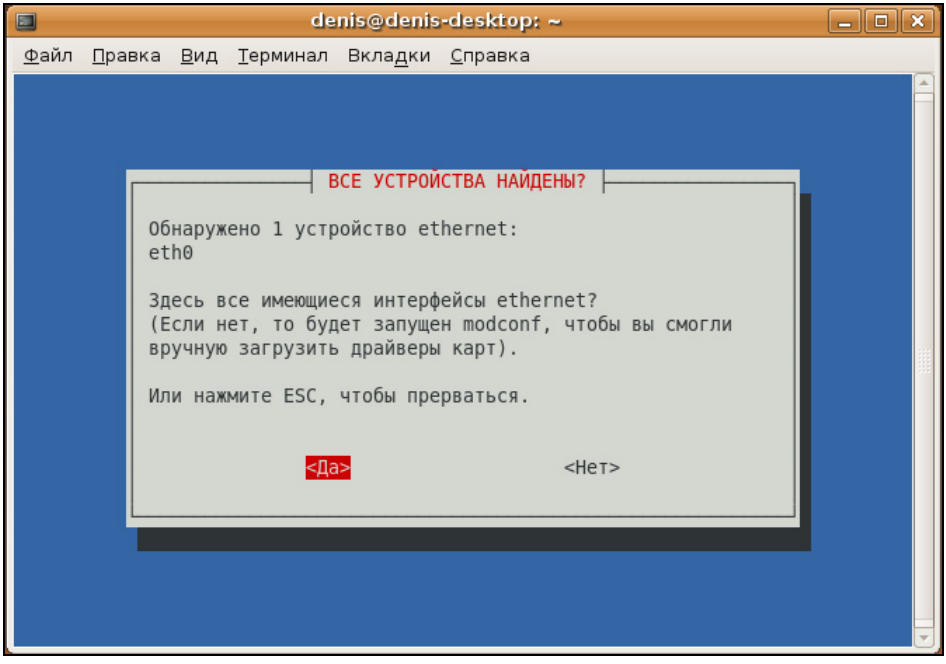


Рис. 7.35. Конфигуратор pppoeconf нашел Ethernet-устройство

Итак, после запуска конфигуратор pppoeconf нашел ваше Ethernet-устройство (рис. 7.35). Затем конфигуратор попытается найти активный концентратор доступа (рис. 7.36). После того как концентратор доступа будет найден, программа предложит вам установить популярные опции соединения (`noauth` и `defaultroute`) — не стоит от них отказываться, поскольку их использует большинство провайдеров (рис. 7.37).

Следующие два шага — ввод имени пользователя и пароля, которые используются для аутентификации на сервере провайдера. После этого программа предложит вам добавить полученные от провайдера IP-адреса DNS-серверов в файл /etc/resolv.conf. Не стоит от этого отказываться (рис. 7.38).

На следующий вопрос (рис. 7.39) можно просто ответить **Да**, не вникая в подробности. Если же вам интересно, прочитайте следующее пояснение.

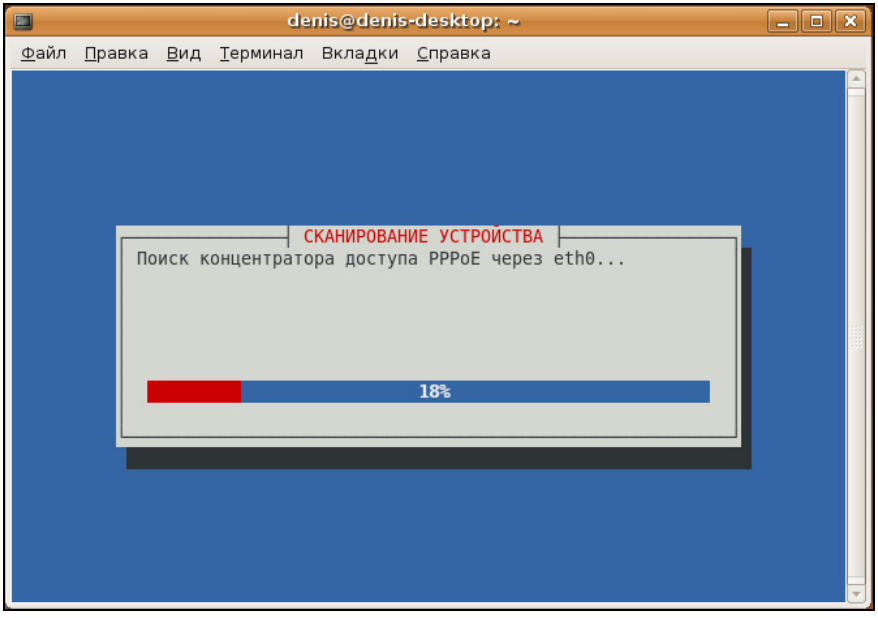


Рис. 7.36. Поиск активного концентратора доступа

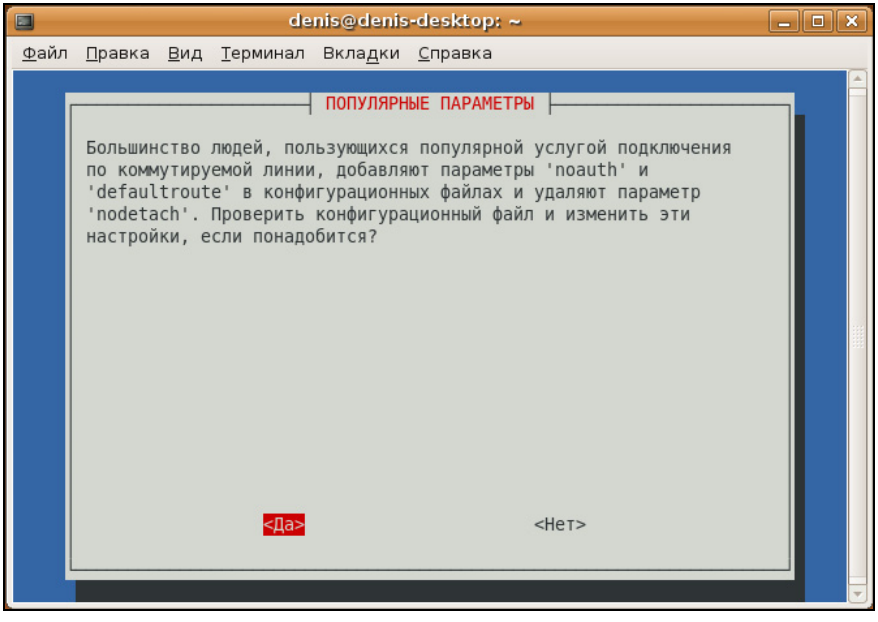


Рис. 7.37. Популярные опции соединения

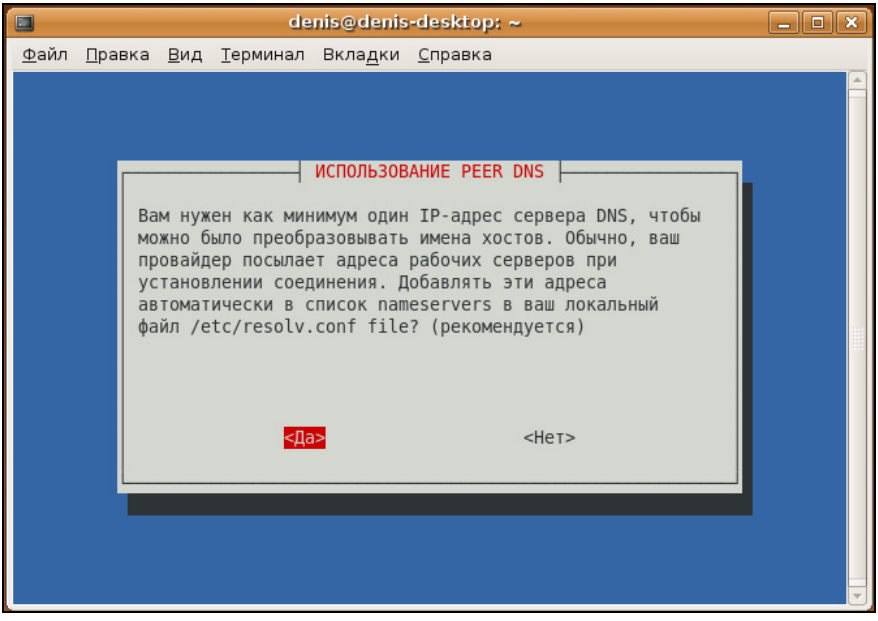


Рис. 7.38. Добавляем IP-адреса DNS-серверов в файл /etc/resolv.conf

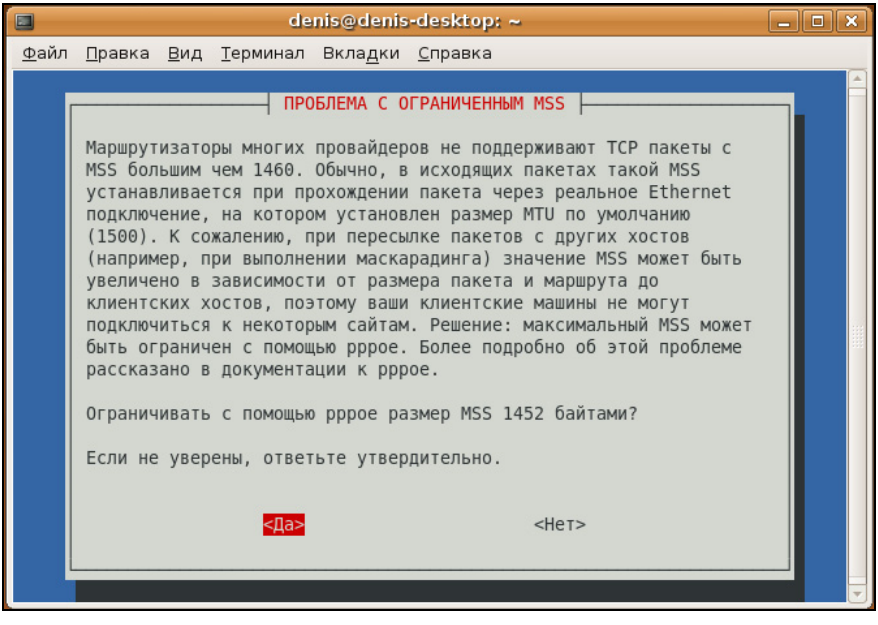


Рис. 7.39. Установка размера MSS

Пояснение

Параметр MTU (Maximum Transmit Unit) задает максимальный размер пакета. По умолчанию данное значение может быть установлено автоматически, но не всегда оптимально. Если размер пакета окажется бóльшим, чем позволяет машрутизатор провайдера, то пакет будет разделен на несколько пакетов, что, естественно, скажется на скорости и пропускной способности соединения. Если размер пакета окажется меньше, чем положено, это тоже не хорошо — канал будет использован нерационально, ведь начнут проходить полупустые кадры. Поскольку мы пользуемся протоколом PPPoE, то нужно учитывать несколько факторов. Максимальный размер кадра Ethernet составляет 1518 байтов, из которых 18 уходят на заголовок и контроль, поэтому для полезных данных остается 1500 байтов. Обычно данное значение и указывается для Ethernet. Но ведь по Ethernet мы собираемся передавать пакеты PPP, а PPPoE отбирает еще 6 байтов, PPP — 2 байта. Получается, что для PPPoE значение MTU должно быть равно 1492. При установке TCP-соединения каждая сторона устанавливает параметр MSS (Maximum Segment Size) — максимальный размер TCP-сегмента. По умолчанию его размер равен MTU минус размер заголовков TCP/IP, которые занимают еще 40 байтов. То есть размер MMS для PPPoE равен 1452 байта (для обычного Ethernet — 1460). Вот откуда взялось значение 1452.

Следующий вопрос — хотите ли вы устанавливать соединение при загрузке системы. Тут уж решайте сами. А после этого программа спросит вас, хотите ли вы установить соединение немедленно. Конечно, да! Можно сразу запускать браузер и заходить на любимую страничку.

Для включения/отключения DSL-соединения используются следующие команды:

```
sudo pon dsl-provider
sudo poff dsl-provider
```

Глава 8

GPRS-соединение с Интернетом

8.1. Особенности GPRS-подключения

GPRS (General Packet Radio Service) — это технология *беспроводной пакетной передачи данных*. Для организации GPRS-подключения нам понадобятся компьютер, современный мобильный телефон, поддерживающий GPRS, и кабель для подключения мобильного телефона к компьютеру. Как вы уже догадались, наш мобильный телефон мы будем использовать в качестве модема.

Зайти в Интернет можно и без компьютера — практически все современные телефоны позволяют подключаться к Интернету, а в составе стандартных приложений есть Web-браузер и даже иногда ICQ-клиент. Но работать в Интернете с мобильного телефона не интересно: маленький экран, неудобная клавиатура. Гораздо приятнее работать в Интернете, подключив мобильный телефон к персональному компьютеру или ноутбуку.

Нужно отметить, что GPRS-соединения достаточно дорогие даже сегодня, да и скорость передачи данных невысока — обычно не превышает 18 Кбит/с (максимальная теоретическая скорость составляет аж 171 Кбит/с, но на практике получается почти в 10 раз меньше). Поэтому GPRS-соединения полезно использовать в крайних случаях:

- когда основное соединение недоступно;
- когда нет другой возможности подключиться к Интернету (например, вы в пути и вам нужно зайти в Интернет со своего ноутбука).

Реальная скорость передачи данных зависит не только от количества одновременно работающих в сети сотового оператора пользователей, но и от самого мобильного телефона. Существуют разные классы (стандарты) GPRS. От того, какой класс поддерживает телефон, зависит скорость соединения. Современные мобильные телефоны поддерживают GPRS Class 10 и имеют

4 таймслота (*таймслот* — это единица разделения канала связи) для закачки информации из сети, что позволяет скачивать данные со скоростью 85 Кбит/с. На отправку обычно имеется всего два таймслота, поэтому скорость отправки данных в любом случае будет меньше примерно в два раза.

Современные телефоны поддерживают технологию EDGE (Enhanced Data rates for GSM Evolution). В этом случае максимальная скорость передачи данных составляет 474 Кбит/с. Важно, чтобы технологию EDGE поддерживал не только телефон, но и оператор связи, иначе вы будете по-прежнему работать в режиме GPRS.

Суперсовременные телефоны третьего поколения (3G) обеспечивают скорость передачи данных в несколько Мбит/с. Но 3G пока поддерживается не всеми операторами связи, а телефоны третьего поколения еще весьма дороги. Однако, если вам не хочется выкладывать приличную сумму за 3G-телефон, вы можете купить 3G-модем, который стоит примерно в два раза дешевле телефона, а использовать его можно как с ноутбуком, так и со стационарным компьютером. Только перед покупкой убедитесь, что там, где вы планируете использовать беспроводное интернет-подключение 3G, имеется покрытие того оператора, к которому вы хотите подключиться.

8.2. Подключаем мобильный телефон к компьютеру

Для подключения мобильного телефона к компьютеру вам понадобится так называемый *data-кабель*. Иногда он входит в комплект поставки, иногда его нужно покупать отдельно. Если вы покупаете кабель отдельно, то убедитесь, что он предназначен именно для вашего мобильного телефона, — так, кабелем от Nokia телефон Siemens к компьютеру вы не подключите.

Кабели бывают двух типов: RS-232C, используемые для подключения к последовательному (COM) порту компьютера, и кабели USB. Предпочтительнее покупать USB-кабель, поскольку с его помощью мобильный телефон может подзаряжать свой аккумулятор.

Кроме data-кабеля для подключения мобильного телефона к компьютеру можно использовать инфракрасный порт (IrDA) или технологию Bluetooth. Эти два способа преимущественно применяются для подключения мобильного телефона к ноутбуку. Использование же data-кабеля является универсальным способом, позволяющим подключить телефон как к стационарному компьютеру, так и к ноутбуку. О подключении мобильного телефона к ноутбуку по Bluetooth мы поговорим отдельно *(см. разд. 8.6)*. Помните, что Bluetooth-соединение по своей природе довольно капризно, поэтому если вам нужна надежная связь, лучше использовать USB-кабель.

8.3. Подготовка к настройке соединения

Перед тем как приступить к настройке, вам нужно уточнить у своего оператора мобильной связи следующие параметры подключения:

- строку инициализации;
- номер дозвона;
- имя пользователя и пароль;
- IP-адреса серверов DNS.

Строка инициализации, имя пользователя и пароль обычно зависят от оператора, а номер дозвона — от модели телефона. IP-адреса серверов DNS обычно устанавливаются сервером автоматически, но иногда их приходится вводить вручную.

> ***Примечание***
>
> Уточните, поддерживается ли мобильный Интернет в вашем тарифном плане. Иногда эту услугу нужно активировать.

В табл. 8.1 приведены параметры доступа для некоторых популярных операторов мобильной связи.

Таблица 8.1. *Параметры доступа*

Параметр	Beeline	МТС	Мегафон	Киевстар	UMC
Точка доступа	internet.beeline.ru	internet.mts.ru	internet	www.kyivstar.net	www.umc.ua
Имя пользователя	beeline	mts	gdata	igprs	<указывать не нужно>
Пароль	beeline	mts	gdata	internet	<указывать не нужно>
Номер дозвона	*99#	*99#	*99#	*99***1#	*99#
IP-адреса серверов DNS	194.067.002.114, 194.190.195.066	213.087.000.001, 213.087.001.001	Автоматически	Автоматически	Автоматически

Примечание

В табл. 8.1 сначала указан первичный сервер DNS, затем — вторичный.

Номер дозвона зависит не только от оператора, но и от самого телефона, например:

- *99# — для телефонов Nokia, Ericsson, Motorola, Sony Ericsson, Sendo;
- *99***1# — для телефонов Siemens, Alcatel, Handspring, LG, Panasonic, Mitsubishi, Sagem;
- *99**1*1# — для Samsung.

Но для большей уверенности лучше уточнить номер дозвона у оператора.

IP-адреса серверов DNS следует указывать вручную только в случае соединения с Beeline и МТС.

Одним словом, первым шагом в настройке GPRS-соединения должен стать звонок в службу поддержки оператора связи. У него вы узнаете все параметры соединения и уточните тарифы. Напомню, что GPRS-соединения довольно дорогие (к сожалению, это так). Иногда операторы предлагают *пакеты данных* — заранее предоплаченные объемы информации. Как правило, покупка такого пакета более выгодна, чем помегабайтная оплата соединения. В некоторых случаях можно даже купить неограниченный доступ за вполне вменяемые деньги.

8.4. Настройка GPRS-соединения в Windows XP

Настройку GPRS-соединения будем рассматривать на примере мобильного телефона Nokia 6680. У вас, скорее всего, другой мобильный телефон, но последовательность действий будет такой же.

Подключите мобильный телефон к компьютеру с помощью data-кабеля. Windows сразу определит его (рис. 8.1). После этого запустится мастер установки нового оборудования (рис. 8.2). Вставьте установочный компакт-диск и нажмите кнопку **Далее**.

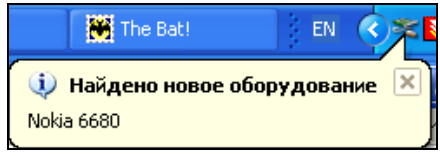


Рис. 8.1. Windows определила телефон

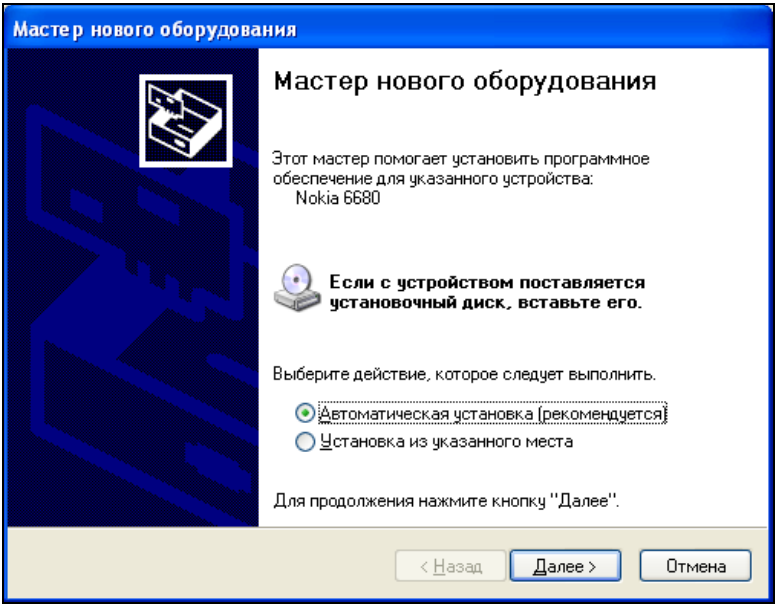


Рис. 8.2. Попытка установить драйвер

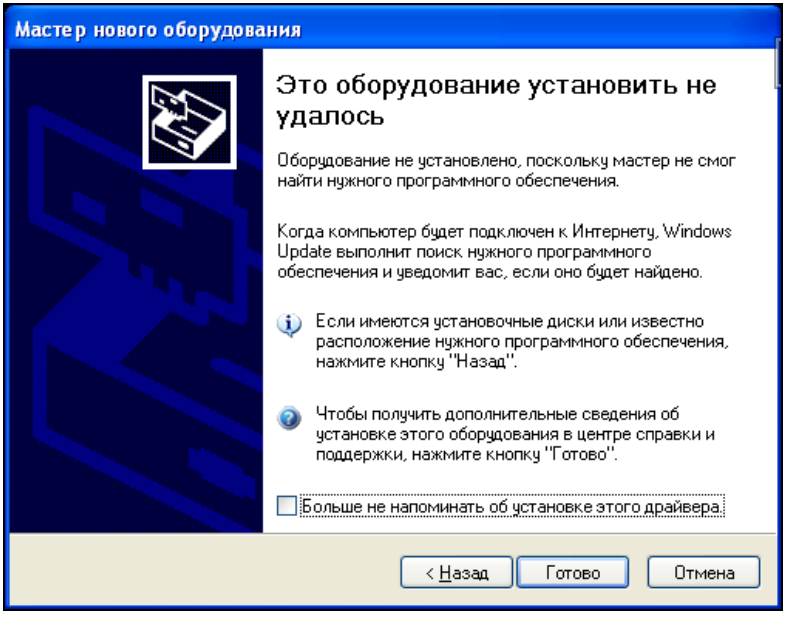


Рис. 8.3. Windows не нашла драйвер

В случае с моим телефоном драйвер обычным способом установить не удалось — Windows просто не нашла драйверов на компакт-диске (рис. 8.3).

Вполне вероятно, что Windows найдет на компакт-диске драйверы вашего телефона (конечно, если это не Nokia). Если же у вас Windows тоже не нашла драйверов телефона, не нужно паниковать. Откройте окно **Мой компьютер** и щелкните двойным щелчком на пиктограмме привода CD/DVD, в котором находится установочный диск. Запустится программа автозапуска (на рис. 8.4 изображена программа для телефона Nokia). Выберите пункт меню **Установка программного обеспечения**. Для другого телефона название этого пункта может быть иным — например, **Установка драйвера**.

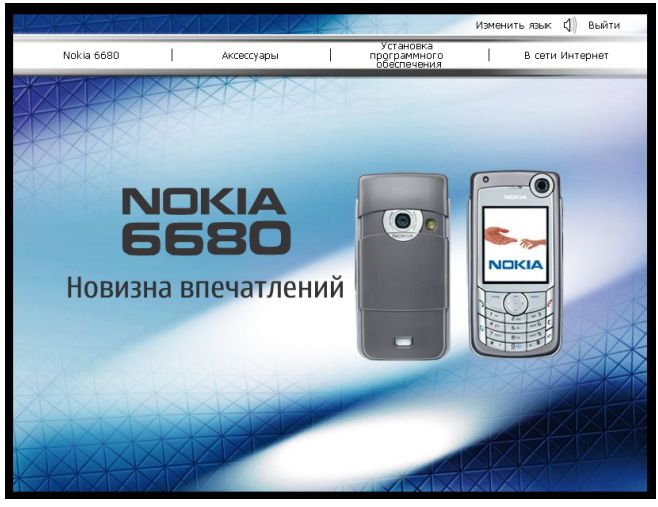


Рис. 8.4. Программа установки ПО для Nokia

В случае с Nokia следует выбрать опцию **Nokia PC Suite | Установить PC Suite**. Пакет Nokia PC Suite содержит драйверы телефона и программу для управления телефоном. Сразу после запуска мастер установки PC Suite попросит вас выбрать язык установки и отключить ваш телефон от компьютера (рис. 8.5).

На следующем шаге мастер спросит вас, согласны ли вы с лицензионным соглашением, попросит указать каталог, в который следует установить PC Suite, и начнет копирование файлов. Просто нажимайте кнопку **Далее**.

После копирования файлов запустится **Мастер настройки подключения**. В первом окне следует нажать кнопку **Далее**, а вот во втором надо выбрать тип подключения телефона к компьютеру — с помощью кабеля или через инфракрасный порт (рис. 8.6). Поскольку мы так долго и тщательно выбирали кабель, то нужно выбрать **Подключение с помощью кабеля**.

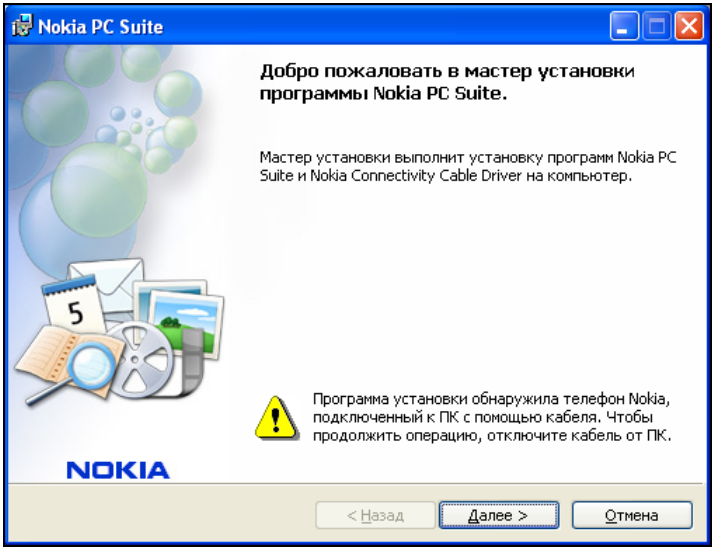


Рис. 8.5. Нужно отключить телефон от компьютера

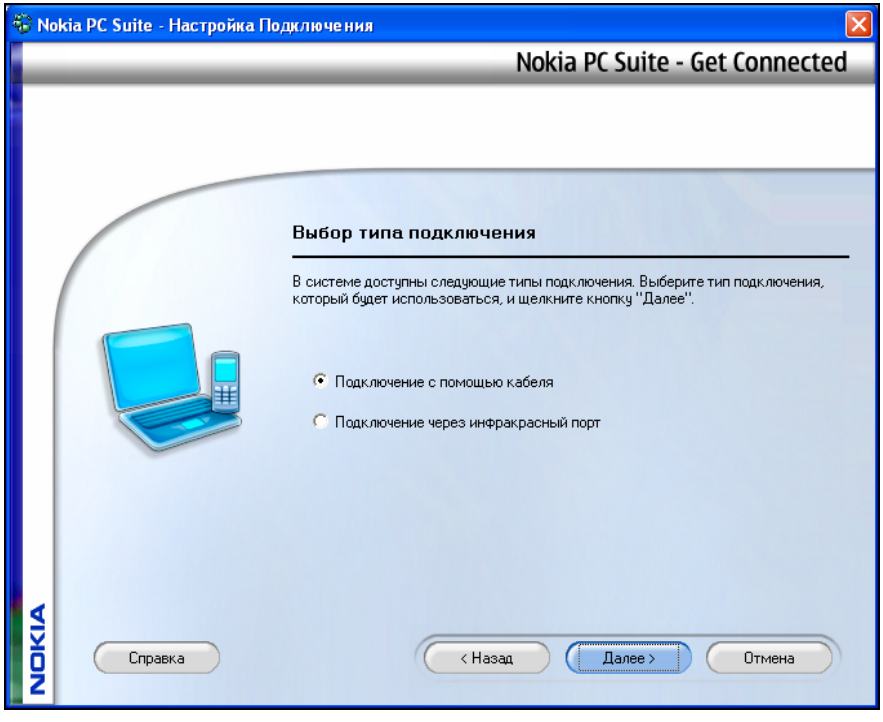


Рис. 8.6. Выбор типа подключения

И тут наступит момент истины: Windows установит драйвер модема для нашего телефона (рис. 8.7), а мастер настройки подключения радостно сообщит, что у нас доступно подключение Nokia 6680 (рис. 8.8).

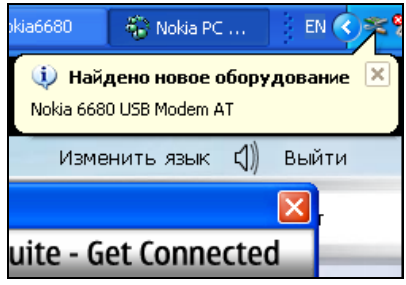


Рис. 8.7. Установка драйвера модема

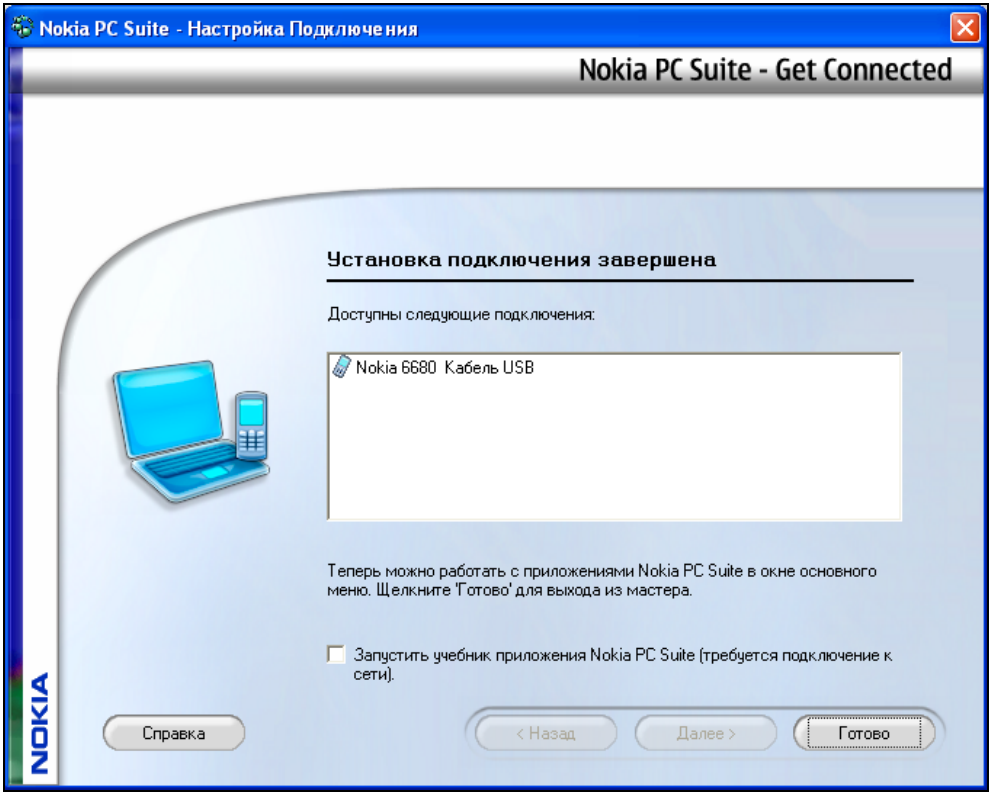


Рис. 8.8. Доступно подключение Nokia 6680

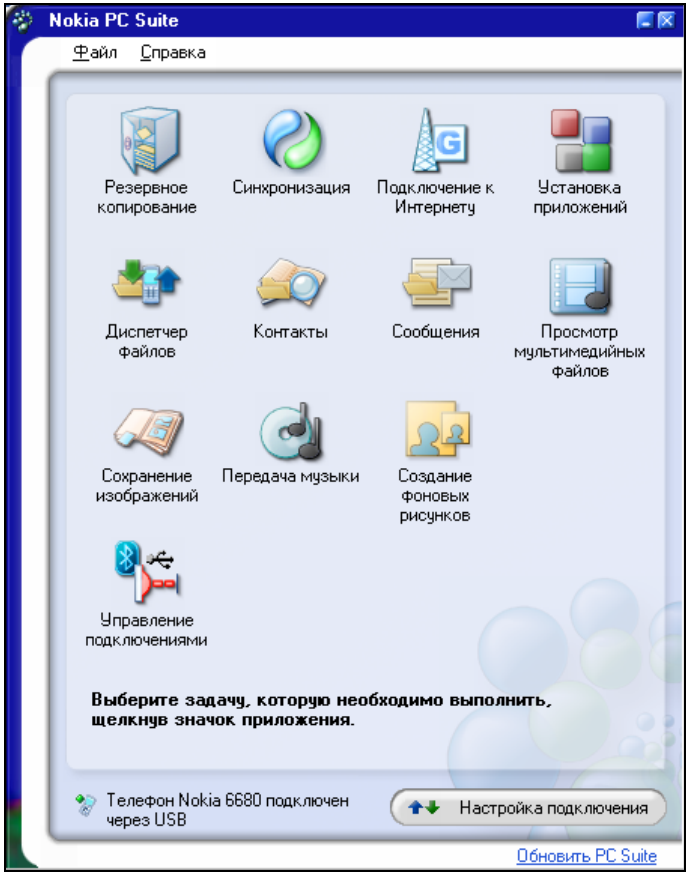


Рис. 8.9. Nokia PC Suite

Сразу после завершения установки драйверов запустите PC Suite (рис. 8.9). С ним вам придется разбираться самостоятельно, а мы здесь займемся дальнейшей настройкой GPRS-соединения.

Настройка GPRS-соединения выполняется аналогично настройке обычного модемного соединения. Напомню основные этапы:

1. Откройте папку **Сетевые подключения (Пуск | Настройка | Сетевые подключения)**. В левой части открывшегося окна выберите **Создание нового подключения**.
2. Вы увидите окно **Мастер новых подключений**. Пока просто нажмите кнопку **Далее**. Мастер предложит выбрать один из вариантов подключения к сети. Нам надо выбрать **Подключить к Интернету** и нажать кнопку **Далее**.

3. Далее выбираем **Установить подключение вручную**.
4. После этого нужно выбрать **Через обычный модем**. Здесь Windows предложит вам выбрать модем (если у вас их несколько: например, обычный модем и мобильный телефон), как показано на рис. 8.10.
5. Следующий шаг — это ввод имени соединения. Мы будем использовать имя GPRS, чтобы не запутаться.
6. Затем нужно указать номер телефона дозвона (рис. 8.11). Для Nokia и ряда других мобильных телефонов это: *99#. Тем не менее, номер телефона желательно уточнить у вашего сотового оператора.
7. После этого следует ввести имя пользователя и пароль (рис. 8.12). В табл. 8.1 приведены некоторые стандартные имена и пароли, но желательно также предварительно уточнить имя пользователя и пароль у сотового оператора.
8. Нажмите кнопку **Готово** — соединение создано. Запустить соединение можно через папку **Сетевые подключения**.

На этом настройка соединения не завершена — надо еще настроить модем. Откройте окно **Панель управления** и запустите апплет **Телефон и модем**. Перейдите на вкладку **Модемы** (рис. 8.13), выберите модем вашего мобильного телефона и нажмите кнопку **Свойства**.

В открывшемся окне перейдите на вкладку **Дополнительные параметры связи** (рис. 8.14). В поле **Дополнительные команды инициализации** введите строку инициализации. Обычно она выглядит так:

```
AT+CGDCONT=1,"IP","точка доступа"
```

Синтаксис строки инициализации следует уточнить у вашего сотового оператора, а значение параметра точки доступа можно найти в табл. 8.1. Если вашего оператора нет в таблице, то нужно позвонить в его службу поддержки и узнать параметры GPRS-соединения. На рис. 8.14 указана строка инициализации для Мегафона.

Можно сказать, что уже почти все настроено. Если ваш оператор требует самостоятельного ввода IP-адресов серверов DNS, щелкните двойным щелчком на пиктограмме соединения в папке **Сетевые подключения** и в открывшемся окне (рис. 8.15) нажмите кнопку **Свойства**.

В окне **GPRS Свойства** перейдите на вкладку **Сеть** и выделите опцию **Протокол Интернета**, как показано на рис. 8.16. Нажмите кнопку **Свойства**.

В открывшемся окне свойств протокола Интернета (рис. 8.17) выберите переключатель **Использовать следующие адреса DNS-серверов** и введите требуемые IP-адреса, которые можно уточнить у вашего сотового оператора. После этого нажмите кнопку **OK**.

Я вас поздравляю! Настройка GPRS-соединения завершена.

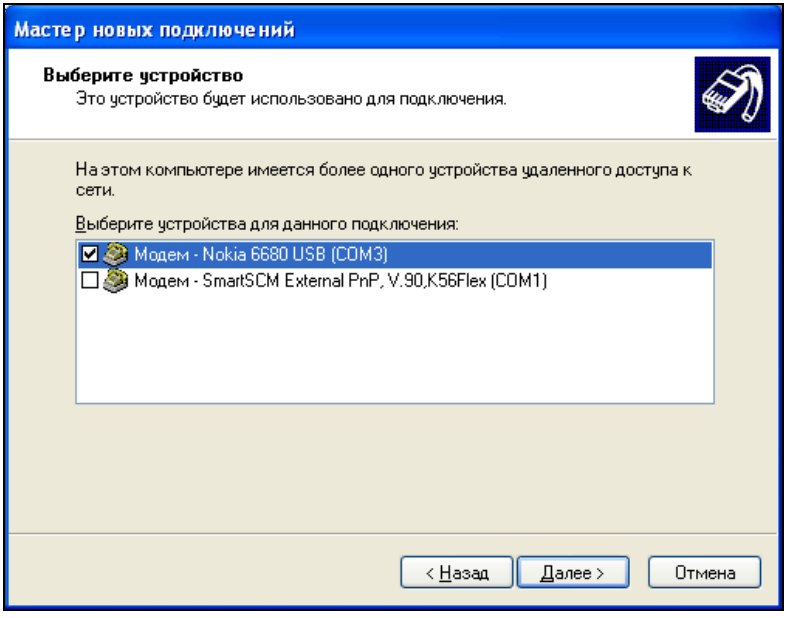


Рис. 8.10. Выбор модема

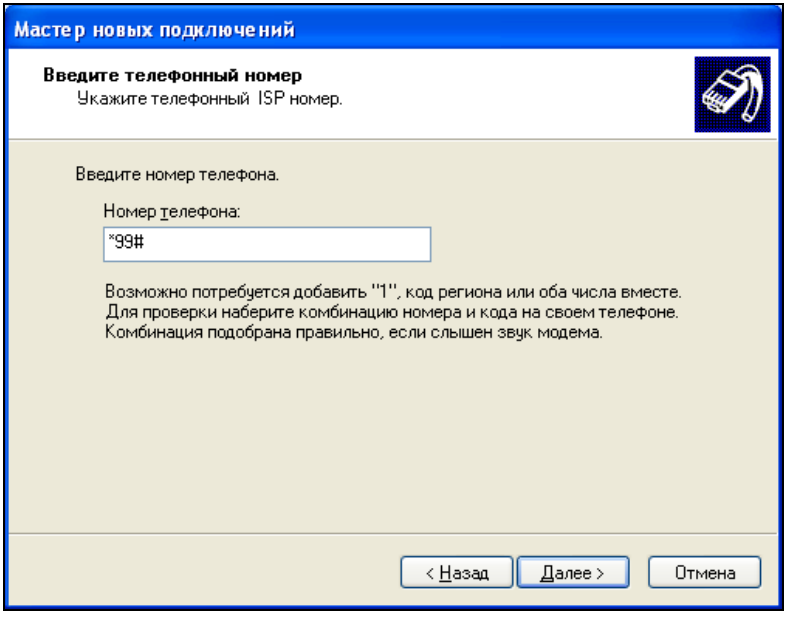


Рис. 8.11. Ввод номера телефона

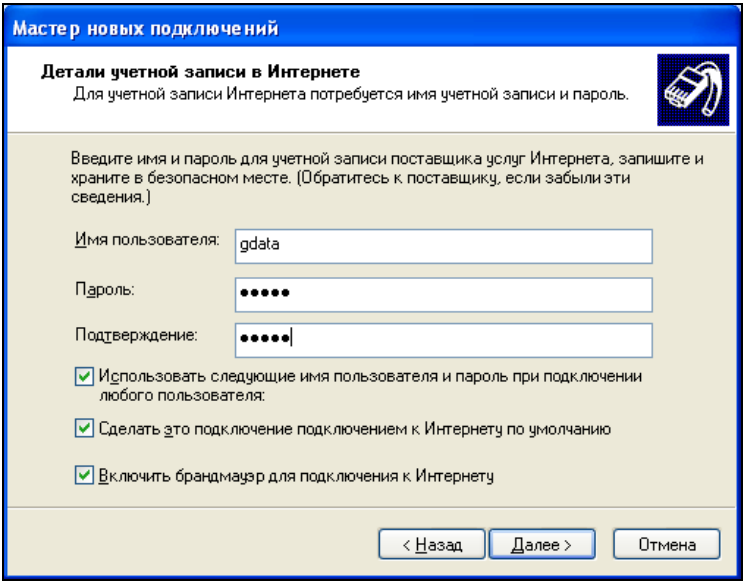


Рис. 8.12. Ввод имени пользователя и пароля (для Мегафона)

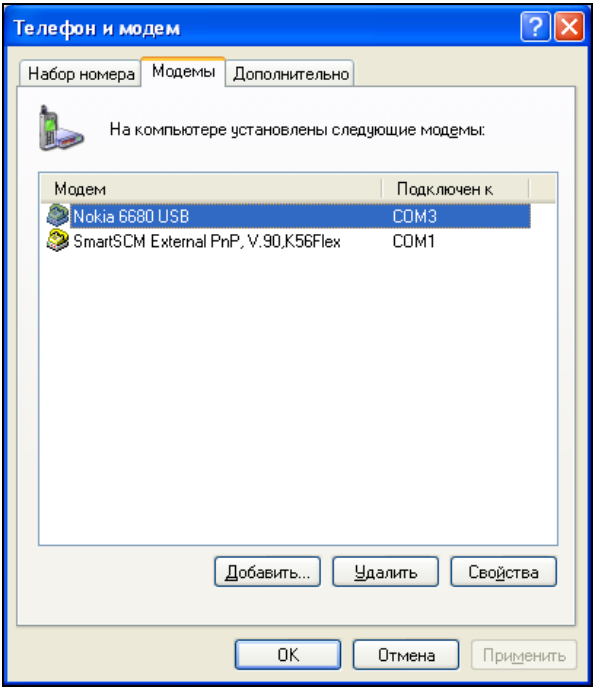


Рис. 8.13. Список модемов

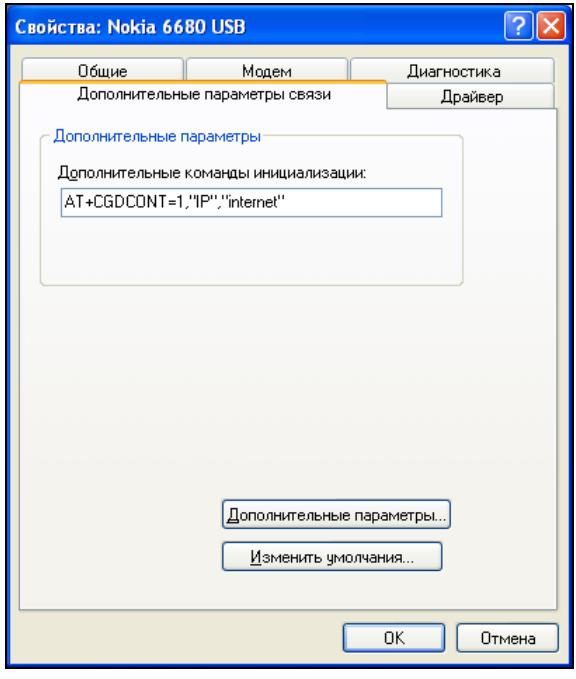


Рис. 8.14. Строка инициализации

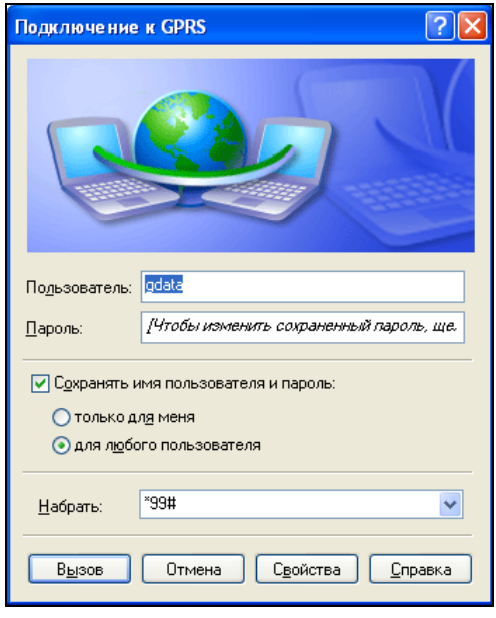


Рис. 8.15. GPRS-подключение

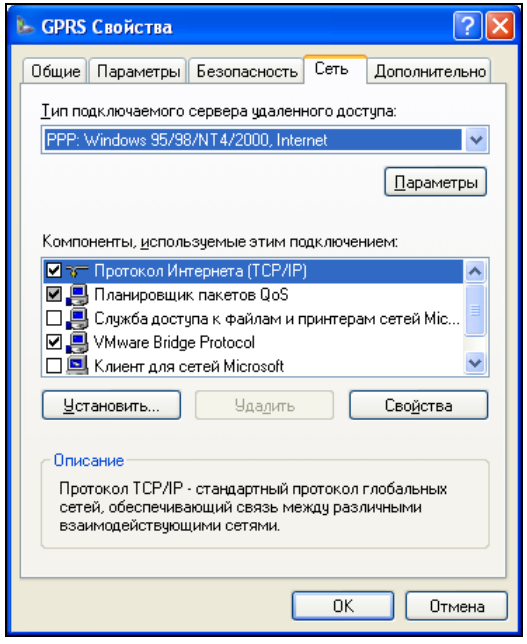


Рис. 8.16. Свойства GPRS-соединения

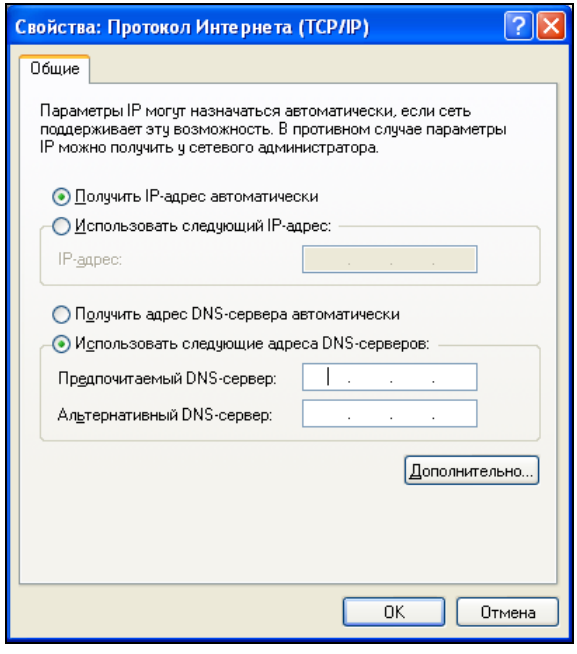


Рис. 8.17. Параметры протокола Интернета

8.5. Настройка GPRS-соединения в Windows Vista

Настройка GPRS-соединения в Windows Vista аналогична настройке GPRS-соединения в Windows XP. Если вы не читали предыдущий раздел, тогда напомню, что настройку GPRS мы будем осваивать на примере телефона Nokia 6680. Если у вас другой телефон, то последовательность действий будет такая же, но вид экранов программы установки драйвера, понятно, окажется иным.

Vista, как и Windows XP, при подключении телефона к компьютеру с помощью кабеля определяет телефон (рис. 8.18) и запрашивает диск с драйверами.

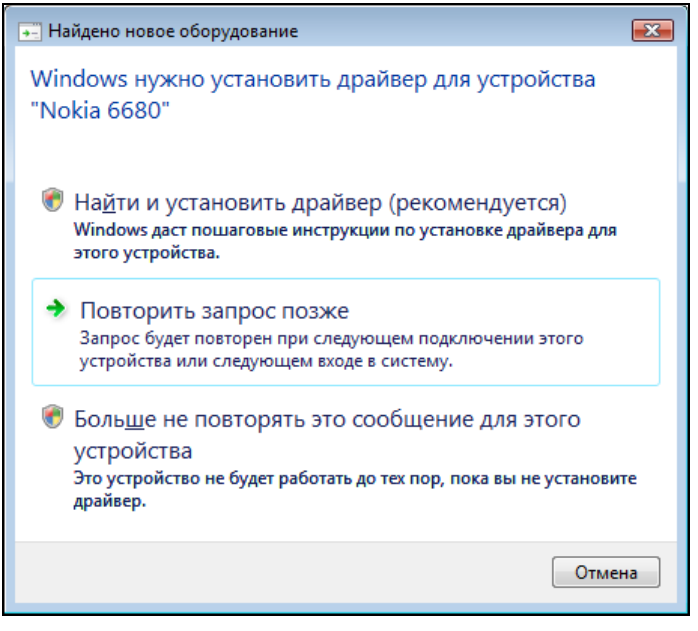


Рис. 8.18. Windows Vista определила телефон

Но именно в случае с Nokia драйверы на диске не обнаруживаются — надо отдельно запускать программу установки. Кстати, программа установки драйверов запускается автоматически при установке компакт-диска в привод CD/DVD (для других телефонов тоже должно так быть — это обычная функция автозапуска). В случае с Nokia нужно выбрать пункт **Установка программного обеспечения** (см. рис. 8.4), а затем — **Nokia PC Suite | Установить PC Suite**.

Рис. 8.19. Тип подключения телефона к компьютеру

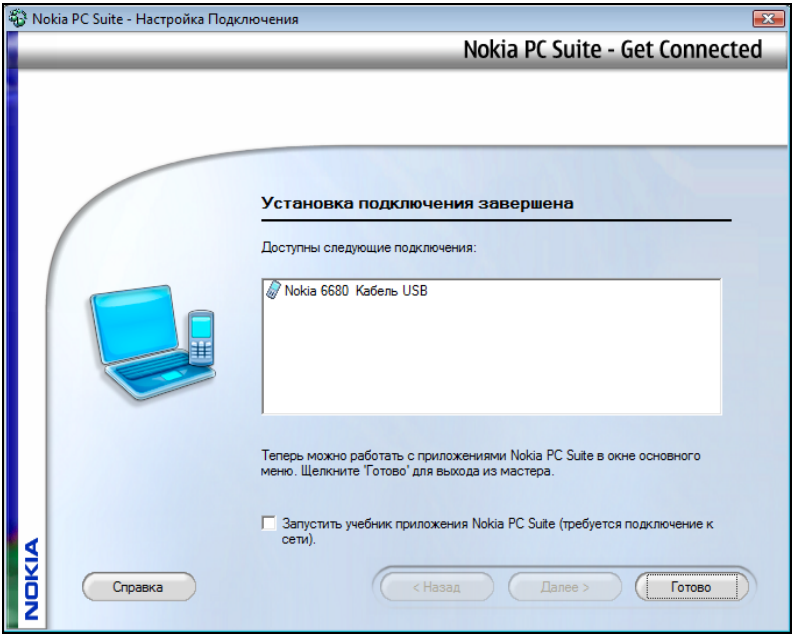


Рис. 8.20. Информация о доступных подключениях

В процессе установки программа попросит уточнить тип подключения телефона к компьютеру (рис. 8.19): кабель, инфракрасный порт или Bluetooth. Выбираем переключатель **Подключение с помощью кабеля**. Программа попросит подключить (для проверки) телефон к компьютеру с помощью кабеля, а потом выведет информацию о доступных подключениях (рис. 8.20).

После установки драйвера можно приступить к настройке GPRS-соединения. Для этого откройте окно **Панель управления** (**Пуск | Панель управления**). Выберите **Сеть и Интернет | Подключение к Интернету** (рис. 8.21). Откроется окно **Подключение к Интернету** (рис. 8.22).

> ***Примечание***
>
> Если вы не можете найти команду **Подключение к Интернету** в группе **Сеть и Интернет**, выполните команду меню **Пуск | Подключение** и в открывшемся окне выберите команду **Установка подключения или сети**. Можно также щелкнуть на названии группы **Сеть и Интернет** и в группе **Центр управления сетями и общим доступом** выбрать команду **Подключиться к сети**.

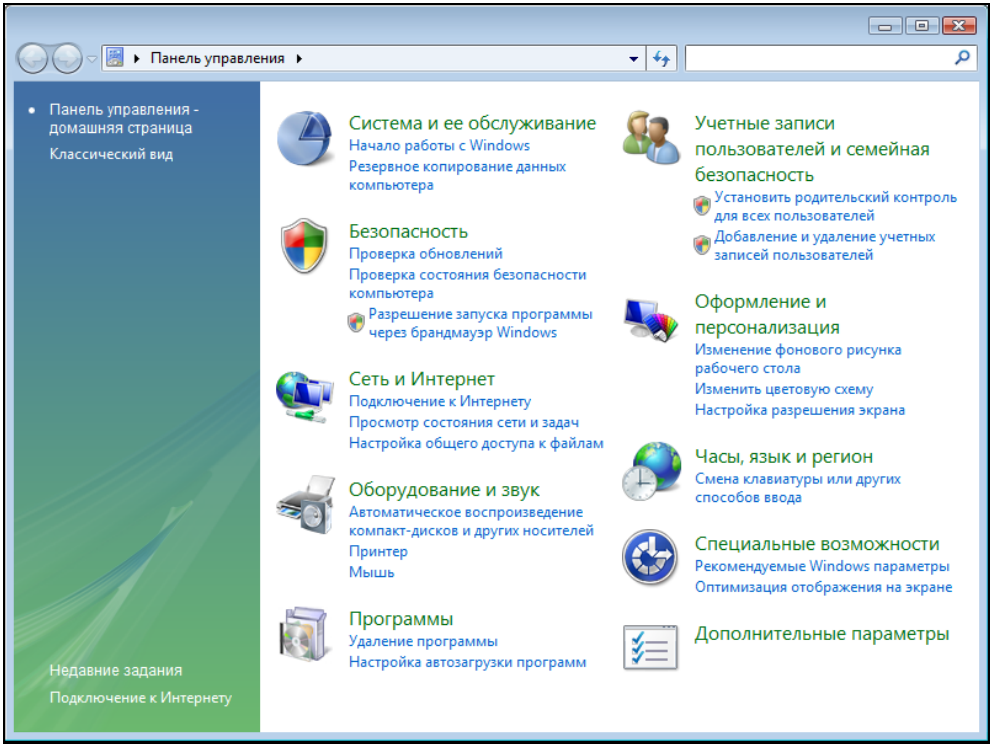


Рис. 8.21. Панель управления Windows Vista

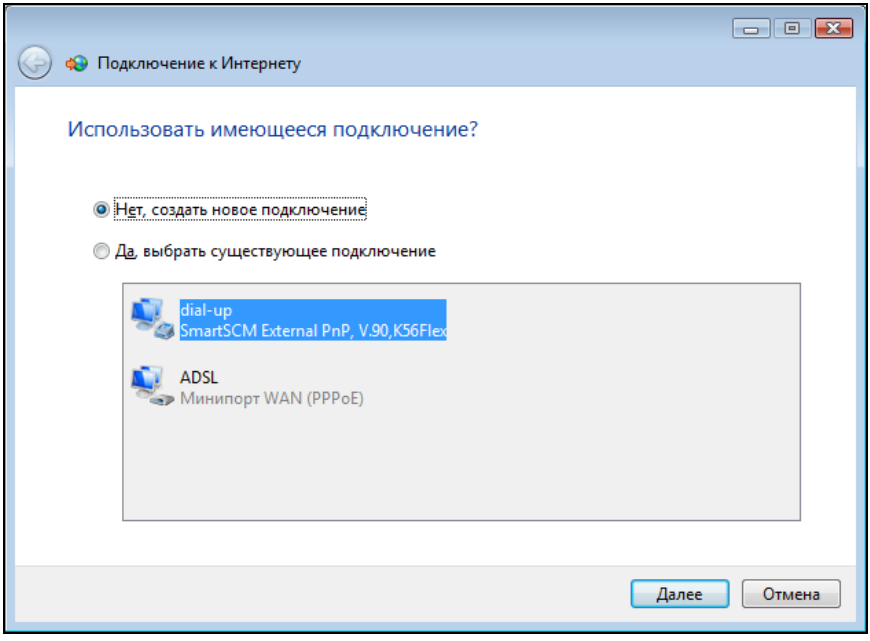


Рис. 8.22. Создание нового подключения

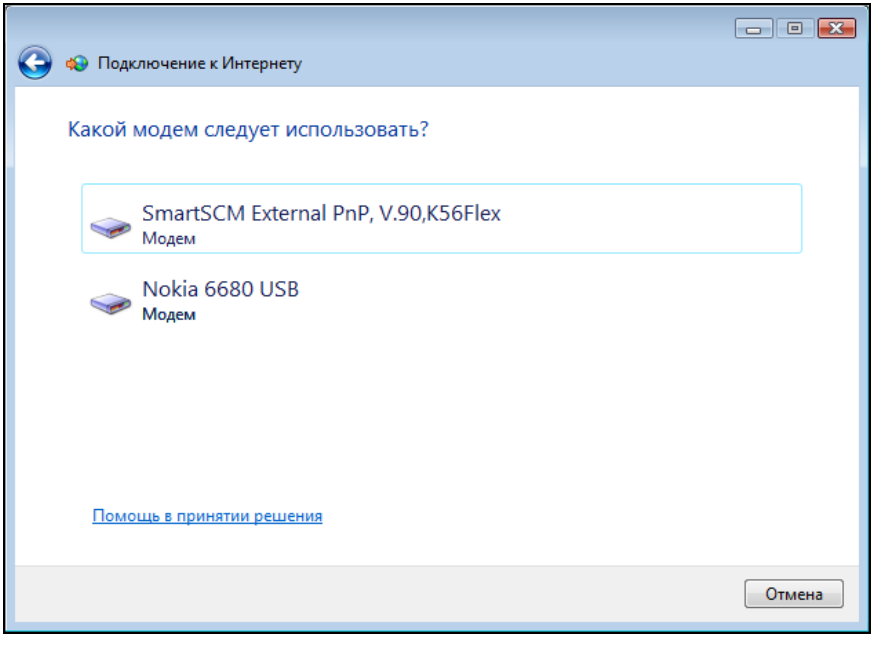


Рис. 8.23. Выбор модема

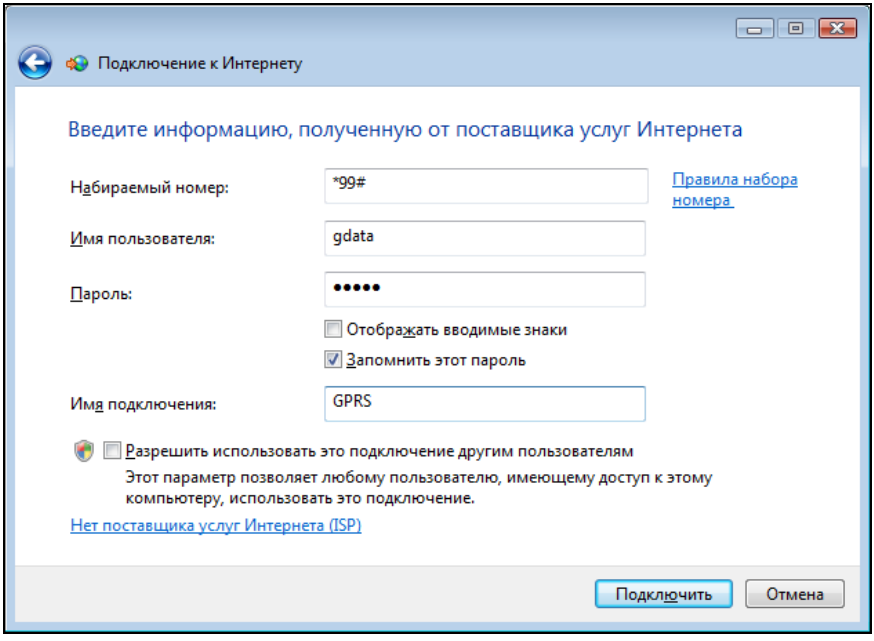


Рис. 8.24. Параметры соединения

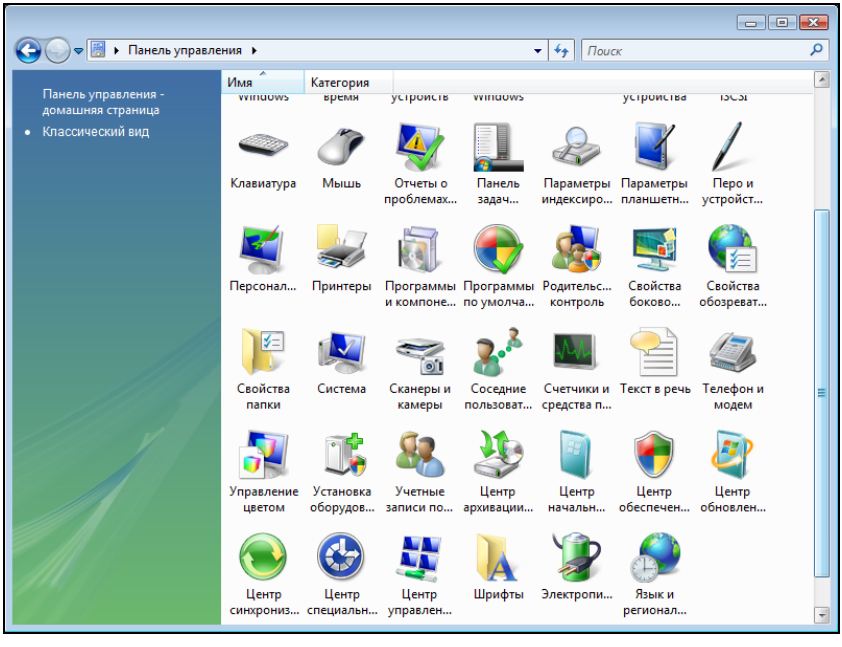


Рис. 8.25. Классический вид Панели управления

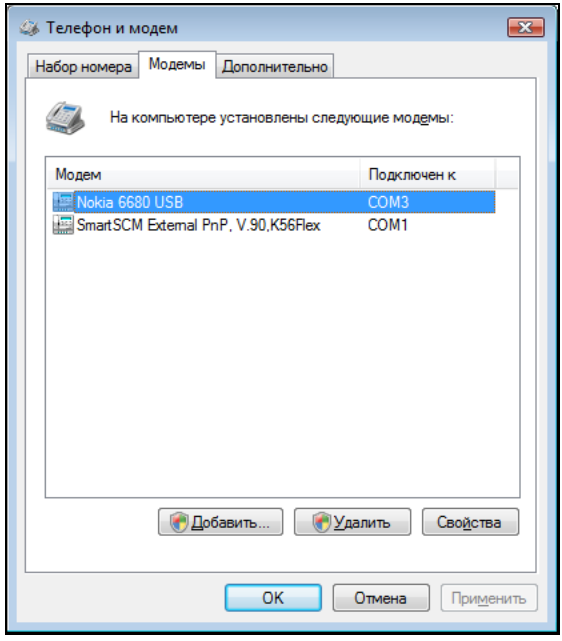


Рис. 8.26. Телефон и модем

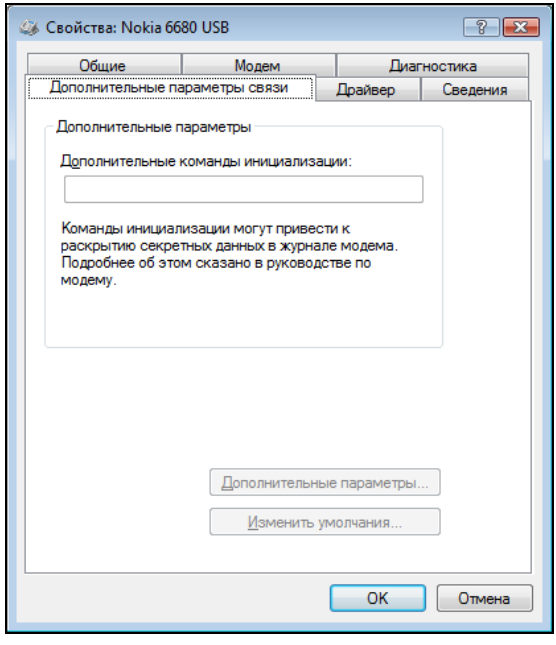


Рис. 8.27. Ввод строки инициализации

Если у вас уже были созданы какие-то интернет-соединения, нужно выбрать опцию **Нет, создать новое подключение**. Windows спросит вас, какое соединение нужно настроить. Следует выбрать **Коммутируемое**, а затем Windows предложит выбрать модем для коммутируемого соединения, если к вашему компьютеру подключено более одного модема (рис. 8.23).

В следующем окне введите номер телефона, имя пользователя, пароль, название соединения (рис. 8.24).

Для завершения создания соединения нужно нажать кнопку **Подключить**, но не спешите — поскольку вы не указали строку инициализации, у вас ничего не выйдет. Откройте Панель управления снова. В левой части ее окна вы увидите ссылку **Классический вид**. Нажмите ее — Панель управления будет переведена в классический вид (рис. 8.25). Запустите апплет **Телефон и модем**.

В окне **Телефон и модем** (рис. 8.26) выберите свой телефон и нажмите кнопку **Свойства**.

В открывшемся окне перейдите на вкладку **Дополнительные параметры связи** (рис. 8.27) и введите строку инициализации *(см. разд. 8.4)*.

Вот теперь в окне **Подключение к Интернету** (см. рис. 8.24) можно нажать кнопку **Подключить**. После пробной попытки установки связи новое соединение будет создано. Воспользоваться им можно через список подключений, вызываемый с помощью команды меню **Пуск | Подключения**.

8.6. Подключение мобильного телефона к ноутбуку по Bluetooth

Практически все современные ноутбуки оснащены Bluetooth-адаптером и практически все современные телефоны поддерживают Bluetooth, поэтому владельцам ноутбуков удобнее использовать именно радиосвязь, а не кабель. Поскольку на всех современных ноутбуках установлена Windows Vista, мы будем рассматривать Bluetooth-подключение именно в этой операционной системе — нужно идти в ногу со временем.

Bluetooth — это технология беспроводного обмена данными, обеспечивающая скорость передачи до 2,1 Мбит/с и радиус действия до 10–100 метров. GPRS-соединение удобно устанавливать по Bluetooth — положили телефон в карман и спокойно работаете в Интернете. Однако помните, что Bluetooth — это все-таки радиосвязь, и она чувствительна ко всякого рода помехам, поэтому Bluetooth-подключение может быть нестабильным.

Итак, приступим к настройке. Активируйте Bluetooth-адаптер. Обычно для этого используется специальная клавиша на передней панели ноутбука (за подробной информацией обратитесь к руководству по ноутбуку). Постоянно держать включенным этот адаптер не рекомендуется, поскольку он энергично "сажает" аккумулятор ноутбука.

Как только адаптер станет активным, в области уведомлений появится пиктограмма с изображением логотипа Bluetooth (рис. 8.28).

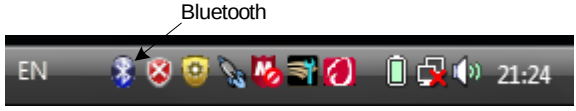


Рис. 8.28. Значок **Bluetooth** в области уведомлений

Щелкните двойным щелчком по значку **Bluetooth**. Вы увидите список Bluetooth-устройств (рис. 8.29). В большинстве случаев (если вы еще не подключали телефон к компьютеру) он будет пуст. На рис. 8.29 видно, что телефон Nokia уже установлен. Сейчас мы выполним установку другого телефона. Для добавления нового телефона нажмите кнопку **Добавить**.

Откроется мастер подключения Bluetooth (рис. 8.30). Включите Bluetooth в вашем телефоне, затем поставьте флажок **Устройство установлено и готово к обнаружению** и нажмите кнопку **Далее**.

Мастер обнаружит новое устройство — выберите его и нажмите **Далее** (рис. 8.31). Следующий шаг — это ввод ключа доступа к устройству (рис. 8.32). Вы можете придумать и ввести свой ключ доступа, а затем, когда компьютер запросит соединение с телефоном, вам нужно будет ввести этот же ключ доступа и в телефоне. При этом имейте в виду, что ключ доступа должен состоять как минимум из 8 цифр.

Можно также позволить компьютеру выбрать код доступа автоматически. В этом случае компьютер сообщит вам назначенный им ключ доступа (рис. 8.33). Этот ключ доступа нужно будет ввести в телефон.

Затем компьютер сообщит, какие COM-порты назначены устройству. Нажмите кнопку **Готово** — устройство готово к использованию (рис. 8.34).

Теперь убедимся, что наше устройство имеется в списке модемов. Откройте Панель управления, затем **Диспетчер устройств** и разверните группу **Модемы** (рис. 8.35). В моем случае установлено два беспроводных модема.

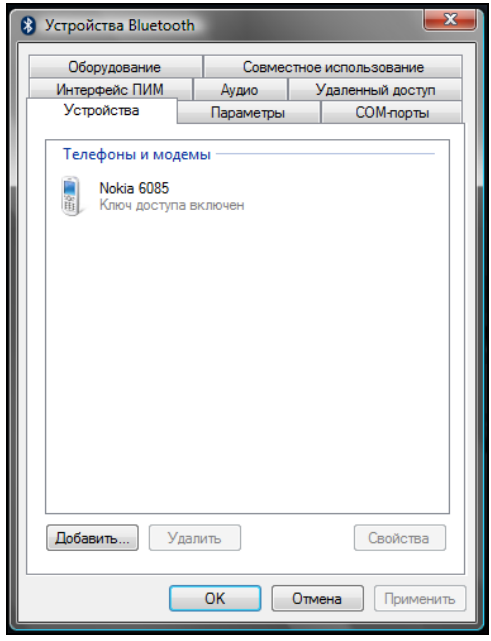


Рис. 8.29. Bluetooth-устройства

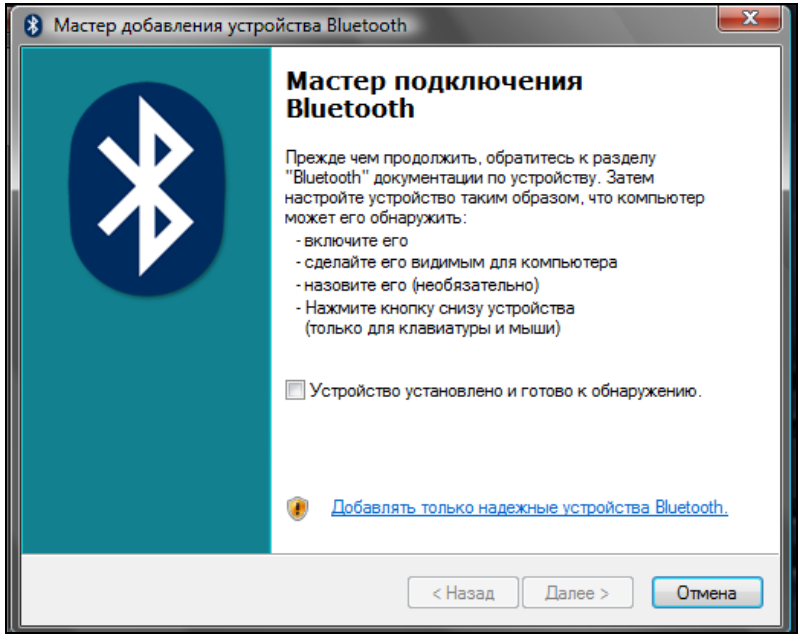


Рис. 8.30. Мастер подключения Bluetooth

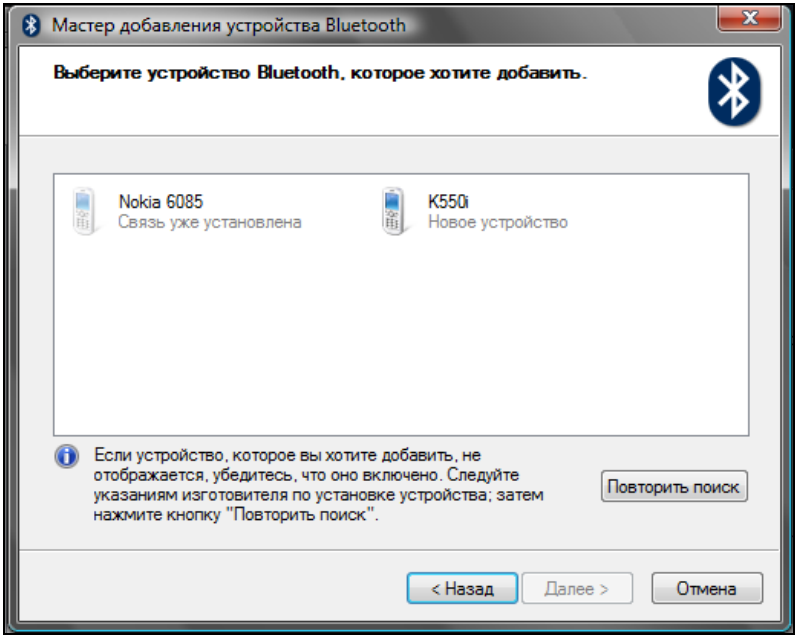


Рис. 8.31. Найдено новое устройство

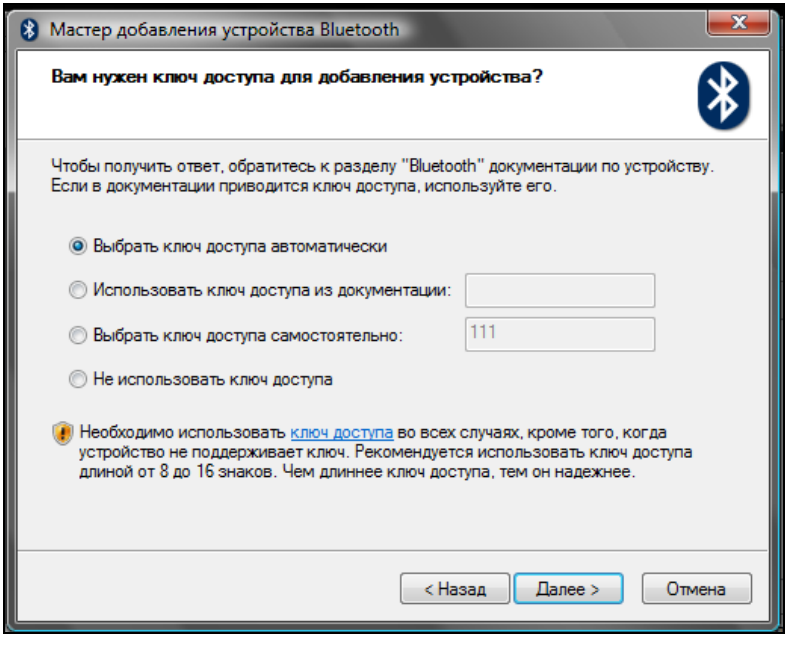


Рис. 8.32. Выбор ключа доступа

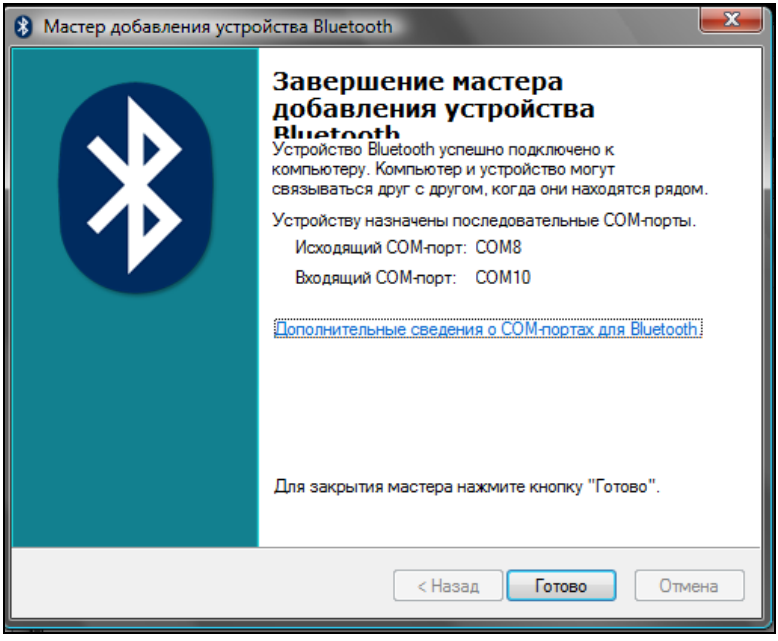


Рис. 8.33. Выбранный компьютером код доступа

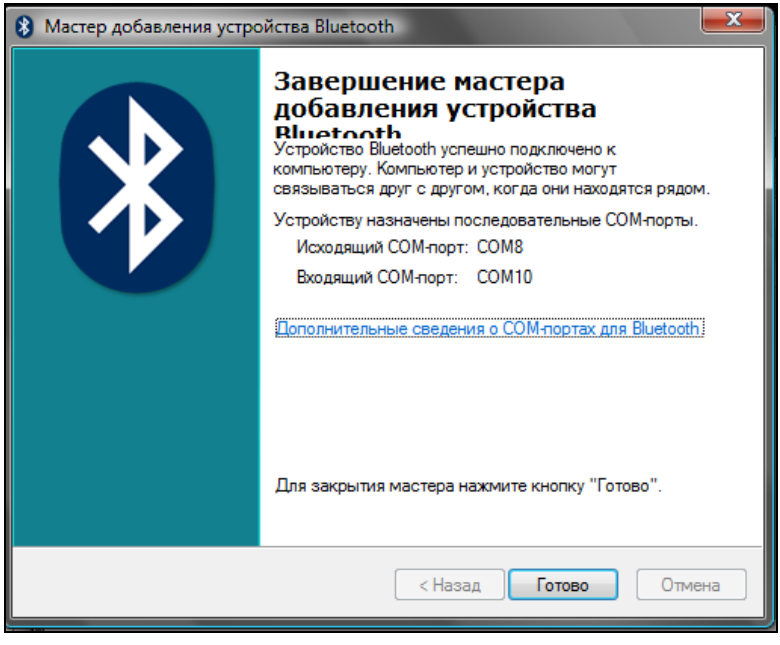


Рис. 8.34. Устройство настроено

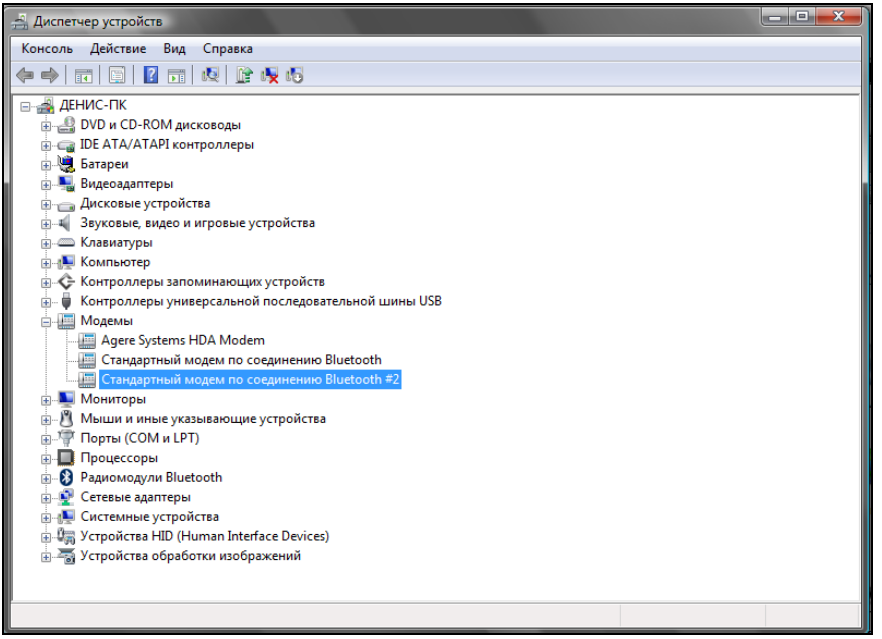


Рис. 8.35. Устройство настроено

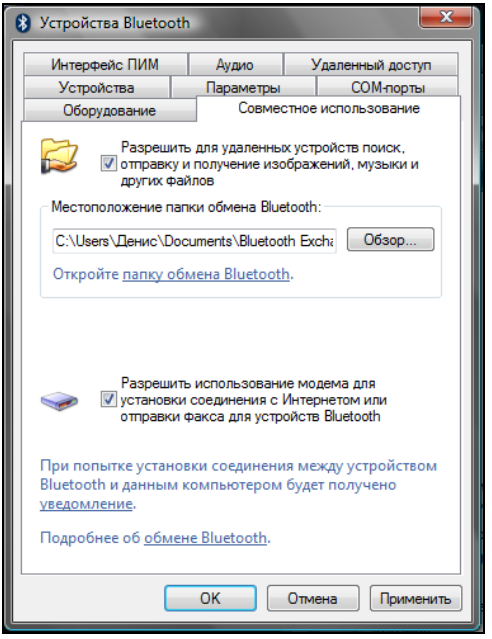


Рис. 8.36. Разрешение использования этого телефона для подключения к Интернету

Но это еще не все. Чтобы использовать только что установленный телефон в качестве модема для интернет-подключения, щелкните на значке **Bluetooth**, выберите только что установленный телефон, перейдите на вкладку **Совместное использование** и включите флажок **Разрешить использование модема для установки соединения с Интернетом…** (рис. 8.36).

Вот теперь можно использовать ваш телефон как модем. Остальная настройка GPRS-соединения ничем не отличается от настройки подключения, описанной ранее — ведь телефон уже установлен как модем.

8.7. Тонкости настройки: подробно о строке инициализации

Представим, что у вас есть два оператора, соединения с которыми вы используете для подключения к Интернету. Дело в том, что тарифы, как и зоны покрытия, операторов отличаются. В дороге вы можете соединяться через одного оператора, поскольку его зона покрытия значительно шире. Дома же или в офисе можно пользоваться услугами второго оператора, поскольку его тарифы дешевле или же его сигнал в данном месте лучше, чем у первого. Если вы отключаетесь от одного оператора и подключаетесь к другому, то вам приходится менять строку инициализации, поскольку и точка доступа у другого оператора иная. Иногда менять строку инициализации приходится несколько раз в день. Рано или поздно, вам это надоест.

Оказывается, можно сформировать универсальную строку инициализации. Давайте рассмотрим типичную строку инициализации:

```
AT+CGDCONT=1,"IP","internet.mts.ru"
```

Здесь: `AT` — обязательная команда, `CGDCONT` указывает номер профиля настроек (в данном случае `1`), `IP` — тип соединения, `internet.mts.ru` — точка доступа.

Теперь рассмотрим другую строку инициализации:

```
AT+CGDCONT=1,"IP","internet.mts.ru"+CGDCONT=2,"IP","internet.beeline.ru"
```

В данном случае мы определили два профиля: один для МТС, другой (с номером 2) — для Beeline. Теперь вам остается создать два соединения. В первом вам нужно использовать номер набора *99***1#, а во втором: *99***2#. Как вы уже догадались, число перед решеткой — это номер профиля соединения.

Часть III

Построение Ethernet-сети

Поскольку "чистые" беспроводные сети встречаются редко, построение сети нужно начать с ее проводной части. В *главе 9* мы сначала спланируем нашу кабельную сеть, а в *главе 10* рассмотрим стандарты и правила построения Ethernet-сети. Нужно отметить, что практически все сказанное в *главе 9* относится к корпоративным сетям, — какое уж тут планирование при построении домашней сети? К какой розетке лучше подключить коммутатор? Или где лучше его расположить, чтобы потратить меньше витой пары? То же самое касается и небольших офисных сетей. А вот когда перед нами задача настроить корпоративную сеть, знаний сетевых стандартов будет недостаточно. Необходимо предварительно спланировать все ваши действия и набросать план сети.

Девятую главу, таким образом, можно считать сугубо теоретической, десятую — теоретико-практической (поскольку в ней будет как теоретическая, так и практическая части), одиннадцатая будет сугубо практической — в ней мы рассмотрим организацию общего доступа к файлам и принтерам.

Глава 9

Планирование сети

9.1. Важность планирования

Вспомним старую русскую пословицу "семь раз отмерь, а один раз отрежь". Она очень точно подходит к нашему случаю. Конечно, бытует мнение, что пока семь раз будете мерить, кто-то уже отрежет. Согласен, но не сейчас. Сейчас вы планируете сеть, вы — главный, и вам никто не мешает. Очень важно продумать все нюансы, связанные с построением сети. Ведь корпоративная сеть — это очень сложная система, состоящая из тысяч различных компонентов. Это в маленькой домашней сети могут быть два-три компьютера, коммутатор, модем и принтер, подключенный к одному из компьютеров (не думаю, что в домашней сети кто-то организует принт-сервер). А в корпоративной сети могут быть самые разнообразные устройства, которые некоторые домашние пользователи даже ни разу в жизни и не видели. Скажем, кто из обычных домашних пользователей видел настоящий *мейнфрейм*, *кластер* или хотя бы обычный *терминал*, подключаемый к мейнфрейму?

Очень важно ориентироваться во всем этом оборудовании. Ведь жизнь не стоит не месте — все развивается с очень большой скоростью, особенно информационные технологии. Модель маршрутизатора, которая была популярна в прошлом году, уже давно такой не является — на ее место пришла более новая, с более совершенными функциями, позволяющими эффективнее использовать всю систему в целом. Поэтому прежде чем закупать оборудование для сети, нужно ознакомиться с возможностями самых последних моделей устройств, а также сравнить устройства других производителей. Вот пример: всю жизнь вы считали, что устройства фирмы AAA (не хочется делать никому никакой рекламы — ни хорошей, ни плохой) — лучшие, но вот всего полгода назад на рынке появилась компания BBB, которая начала производство устройств, которые по всем своим характеристикам превосходят устройства компании AAA. Вы привыкли к компании AAA, поэтому всеми правдами

и неправдами (мол, устройство от BBB еще не проверены временем и т. д.) будете уговаривать себя остановить свой выбор на устройстве от AAA, хотя прекрасно знаете, что устройство от BBB явно превосходит его характеристиками. С одной стороны, вы правы — проверенные временем, надежные устройства обеспечивают безотказную работу сети. А с другой стороны — нет, ведь уже через полгода все будут пользоваться принципиально новыми устройствами BBB, а вы построили свою сеть на устаревшем оборудовании от AAA.

Интернет внес огромные изменения в корпоративную сеть. Сейчас по каналам Интернета можно передать любую информацию: если раньше преимущественно передавался текст, графика и иногда звук, то сейчас видеоконференции он-лайн — это норма. Кроме того, Интернет можно использовать как компонент корпоративной сети — для передачи корпоративной информации по каналам Интернета: это существенно дешевле, чем прокладывать свои линии связи.

9.1.1. Планирование как основа безопасности

При планировании нужно учитывать еще и *безопасность* сети. Да, это нужно делать именно при планировании, а не после того, как сеть уже построена. Поэтому о безопасности — отдельный разговор.

Небольшой пример уже был приведен ранее: использовать проверенные временем решения или применить новые? Это касается не только оборудования, но и программного обеспечения, которое также является компонентом корпоративной сети, причем очень важным компонентом. Весьма желательно найти золотую середину между проверенными временем решениями и новыми разработками.

В предыдущем разделе мы начали говорить о влиянии Интернета на корпоративную сеть. По данным ISC (**www.isc.org**) в январе 2008 года (более новых данных пока нет, поэтому будем считать, что это последние данные) в Сети насчитывалось более 541 миллиона (!) узлов (рис. 9.1). Сейчас их еще больше. Посмотреть отчет ISC можно по адресу: **https://www.isc.org/solutions/survey**.

Для сравнения: в январе 2007 года было 433 миллиона узлов. За год (с 1 января 2007 года по 1 января 2008 года) появилось 108 миллионов узлов, и, хотя данных за 2008 год пока нет, следует ожидать роста примерно до 640 миллионов узлов. Это целая армия потенциальных клиентов вашей компании. И вам жизненно необходимо предоставить им всевозможную рекламную (и не только) информацию о своем бизнесе. Сейчас практически у каждой компании есть собственный Web-сайт. На сайте можно не только ознакомиться с предлагаемым товаром, но и приобрести его. Понятно, что в данном

случае общение с клиентом происходит с помощью Интернета — по электронной почте, ICQ, Skype и т. п. Помимо общения с клиентами, общение с партнерами также происходит по Интернету.

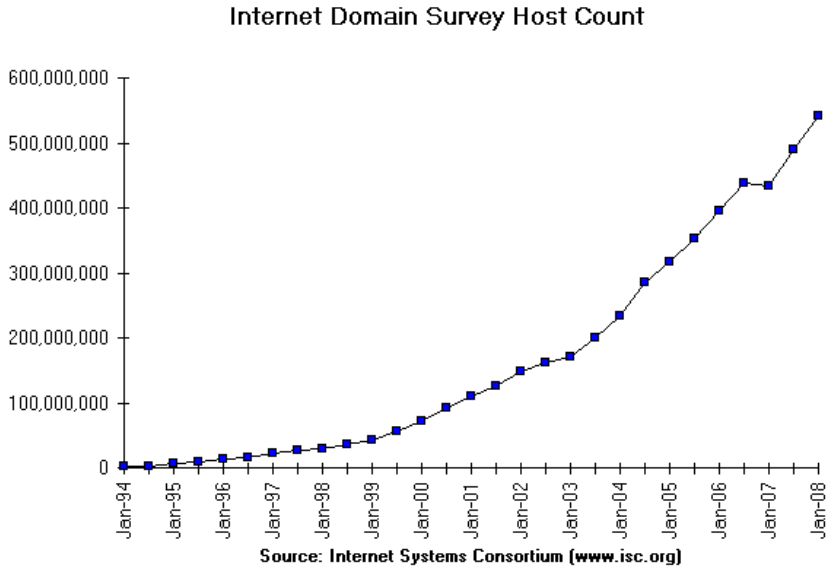


Рис. 9.1. Динамика роста количества узлов (по данным ISC)

Вот теперь мы подошли к самому главному. Ранее считалось, что 80% трафика корпоративной сети будет внутренним, а только 20% — внешним. Сейчас ситуация в корне изменилась. Точные цифры назвать нельзя, потому что они зависят от специфики работы компании: у кого-то соотношение будет 50/50, а у кого-то 20/80, но точно не 80/20. Поэтому возрастает нагрузка на пограничные маршрутизаторы и брандмауэры, которые уже не так эффективно справляются с поставленными задачами. Поэтому, приобретая оборудование или программное обеспечение, нужно думать о будущем и покупать с некоторым запасом, чтобы потом, уже через год-два, не перестраивать всю сеть заново.

Развитие Интернета несет в себе потенциальную угрозу для корпоративной сети — чем больше пользователей, тем потенциально больше желающих взломать вашу сеть. Нужно также подумать и о защите информации, передаваемой по каналам Интернета. На этапе планирования важно решить, какое программное обеспечение будет использоваться в сети. Особое внимание следует уделить программам, с помощью которых пользователи вашей сети

будут "общаться" с внешним миром. Оно должно поддерживать шифрование, как средство безопасной передачи данных. Нужно регулярно следить за обновлением программного обеспечения — ведь в новых версиях не только появляются новые функции, но и устраняются ошибки старых версий.

Как показывает практика, в среднем срок устаревания IT-продуктов (аппаратного и программного обеспечения) находится в районе 3–5 лет. Неужели каждые три года нужно перестраивать всю сеть? Понятно, что так работать нельзя, поскольку на это потребуются большие деньги. А сеть тем временем будет устаревать. Поэтому необходимо следить за основными тенденциями развития мира информационных технологий и постепенно на регулярной основе вносить изменения в существующую сеть — так всегда ваша сеть будет идти в ногу со временем.

9.1.2. Построение транспортной системы корпоративной сети

Всем хочется, чтобы сеть работала быстро. Понятно, что никому не хочется ждать — ни пользователю сети, ни клиенту компании, который обращается к Web-серверу компании. Чтобы сеть работала быстро, нужно продумать ее *транспортную систему*.

Транспортная инфраструктура

Все чаще и чаще возникает необходимость в повышении пропускной способности каналов между клиентами сети и серверами. Причины, думаю, ясны: "средняя" современная рабочая станция по производительности мощнее "среднего" 5-летнего сервера. Мощные компьютеры позволяют эффективно работать с мультимедиа и передавать мультимедиаинформацию по сети и Интернету. Пять лет назад далеко не каждый обычный пользователь мог выкачать из Интернета фильм или посмотреть видео в режиме реального времени. А сейчас Интернет стал дешевле, качественнее, быстрее. Если сеть была построена раньше, понятно, что ее транспортная инфраструктура не выдерживает возросших нагрузок — отсюда и "эффект торможения" сети.

Построение транспортной системы — задача не простая. Сложность заключается в том, что требования к пропускной способности неоднородны для различных подсетей крупной корпоративной сети. Сомневаюсь, что все клиенты будут обмениваться данными с одинаковой интенсивностью с внешними и внутренними серверами, поэтому часть сегментов будет загружена больше, а часть — меньше. Понятно, что с экономической точки зрения нужно предоставлять подсетям ту пропускную способность, которая им требуется.

Магистраль для корпоративной сети

Магистраль — один из самых главных и, следовательно, самых дорогих компонентов сети. Через магистраль проходит большая часть трафика сети, поэтому она влияет на работу всей сети в целом. Решение о выборе магистрали является одним из самых важных при планировании сети.

Кроме протокола, который будет использоваться магистралью, нужно еще учесть структуру самой магистрали, которая (структура) потом будет положена в основу кабельной системы. В некоторых сетях стоимость кабельной системы доходит до 20% от стоимости всей сети — сами понимаете, во что может вылиться неправильное решение. Выбор магистрали — это всегда компромисс между скоростью и стоимостью. Можно выбрать все самое быстродействующее и дорогое, но в некоторых случаях применение такого оборудования не оправдает себя. Все зависит от потребностей пользователей (также не забываем и о завтрашнем дне): может, самое дорогое и не нужно? На структуру длины влияет выбранная технология, поскольку она и только она определяет максимальную длину сегмента, расстояния между рабочими станциями, возможность использования резервных кабелей, конечно, типы самого кабеля и т. п.

Итак, какую технологию выбрать в качестве магистральной? Иногда в качестве магистрали вполне будет достаточно сети Gigabit Ethernet 1000Base-T — на базе витой пары, а остальные подсети будут работать со скоростью 100Мбит/с (Fast Ethernet, 100Base-T) — недорого и сердито.

Но что если нам нужны более высокие скорости? Тогда можно использовать стандарт 10GBASE (скорость передачи 10 Гбит/с), но этот стандарт пока достаточно молод, а оборудование для него — весьма дорогое. С другой стороны, этот стандарт идеально подходит для интеграции с сетями Gigabit Ethernet. А другие технологии, например, ATM, будут еще дороже. Зато ATM обеспечивает максимальную скорость передачи данных в 40 Гбит/с, что идеально подходит для работы с потоковым видео. Повторюсь, выбор магистральной технологии зависит от конкретных задач, которые ставятся перед вашей сетью.

Быстрый и экономичный доступ удаленных пользователей к сети компании

Иногда нужно обеспечить доступ удаленных пользователей к сети компании. Ранее для доступа к корпоративной сети использовались так называемые *dial-in серверы* (серверы входящих звонков). Сейчас такое решение нельзя назвать эффективным. Во-первых, для организации сервера входящих звон-

ков нужна многоканальная телефонная линия и модемный пул, а все это стоит недешево. Во-вторых, сервер входящих звонков рационально использовать, если удаленный абонент находится в пределах города, — междугородние и международные звонки дорогие. Поэтому нужно использовать что-то более доступное.

Намного дешевле, да и проще использовать для доступа к сети возможности Интернета. В этом случае нам поможет *виртуальная частная сеть* (Virtual Private Network, VPN). Администратор настраивает VPN-сервер, который будет предоставлять доступ пользователям к ресурсам корпоративной сети. В качестве "среды" передачи данных будет использоваться Интернет. Найти интернет-кафе с беспроводным доступом (Wi-fi) проще, чем просить кого-то разрешить подключиться к его телефонной линии. Даже если рядом нет точки беспроводного доступа к Интернету, можно подключиться к Интернету с помощью мобильного телефона — сейчас многие операторы сотовой связи существенно снизили тарифы на доступ к Интернету. Для компании же организация VPN-сервера обойдется намного дешевле организации сервера входящих звонков: не нужна ни многоканальная телефонная линия, ни модемный пул.

Помните о Wi-Fi

Если вы планируете использовать Wi-Fi, то о беспроводной сети нужно помнить с самого начала планирования сети. Очень часто о беспроводной сети забывают, а потом пытаются добавить беспроводную часть в уже существующую сеть, что не всегда эффективно. Более эффективно будет заранее спланировать сочетание Wi-Fi-сети с проводной сетью.

9.2. Обеспечение безопасности сети

О безопасности нужно думать еще на этапе планирования сети, особенно, если вы планируете использовать для построения сети только аппаратные решения. Например, для связи удаленных офисов лучше бы сразу приобрести маршрутизаторы с поддержкой VPN, чтобы потом не пришлось "изобретать велосипед" заново.

9.2.1. Защита данных, передаваемых по публичным каналам связи

Сначала нужно определиться, какие данные будут передаваться по Интернету, определить степень их секретности и уже после этого выбрать способ их защиты. В нашем случае нужно защитить: данные, передаваемые удаленными

пользователями, электронную почту, Web-трафик и административный трафик.

Доступ удаленных клиентов будет защищен самим VPN-каналом — при передаче данных по виртуальному каналу используется шифрование. Электронную почту, не содержащую коммерческих тайн, можно не шифровать, а вот при обмене информацией с партнерами желательно использовать шифрование PGP. Коммерческий Web-трафик (номера кредитных карточек, например) целесообразно передавать с использованием защищенного протокола HTTPS, а не обычного HTTP. Административный трафик (например, когда администратор сети из дома получает доступ к серверу) тоже нужно шифровать. Тут все зависит от типа доступа: если по VPN, то все и так уже зашифровано, а если VPN не используется, нужно использовать SSH, но не telnet.

9.2.2. Выдача IP-адресов по рабочим местам

В больших компаниях принято назначать IP-адреса по рабочим местам пользователей. Вот одна из схем:

```
10.<этаж>.<кабинет>.<номер_компьютера>
```

Например, IP-адрес 10.2.207.3 принадлежит компьютеру с номером 3, который находится на втором этаже в комнате 207. Можно придумать и свою схему. К безопасности особого отношения это не имеет, но вам будет удобнее управлять сетью, если IP-адреса назначены не хаотично, а упорядоченно.

9.2.3. Привязка IP-адресов к MAC-адресам

Представим, что в целях экономии трафика вы ограничили определенным пользователям доступ к Интернету. Зачем, например, он бухгалтерам? Поэтому вы решили закрыть доступ к Интернету всему третьему этажу, то есть всем адресам 10.3.*.*. Но среди бухгалтеров нашелся один "продвинутый" пользователь, который додумался изменить свой IP-адрес. В результате он получит доступ к Интернету. Чтобы такого не произошло, нужно выполнить привязку IP-адресов к MAC-адресам сетевых адаптеров. MAC-адрес уникален — в мире нет двух сетевых устройств с одинаковыми MAC-адресами. Если сервер сети обнаружит, что MAC-адрес не соответствует IP-адресу, доступ к сети предоставлен не будет.

Конечно, вам предстоит огромная работа — ведь нужно переписать MAC-адреса всех компьютеров сети. В этом вам поможет программа, позволяющая просканировать сеть и вывести MAC-адреса всех сетевых адаптеров сети. Могу назвать одну из таких программ: TCPNetView. Скачать ее можно по адресу **http://gorlach.etype.net/netview/download.html**.

9.2.4. Антивирусные серверные решения

Вирусы чаще всего попадают в сеть из Интернета, поэтому необходимо обеспечить контроль интернет-трафика (как WWW, так и почтового). Ранее контролировать весь трафик было накладно — уж очень сильно это замедляло работу всей сети, проверялся лишь почтовый трафик собственного SMTP-сервера. Сейчас это возможно. Познакомиться с соответствующими рекомендациями можно в моей книге "Серверное применение Linux. 2 изд." (издательство "БХВ-Петербург", **http://www.bhv.ru/books/book.php?id=184941**).

Также желательно настроить прокси-сервер корпоративной сети так, чтобы он запрещал доступ пользователей к сомнительным ресурсам, которые потенциально могут содержать вирусы. Прокси-сервер Squid в паре со SquidGuard *(см. главу 25)* вполне в состоянии справиться с этой задачей.

9.2.5. Антивирусные клиентские решения

Но антивирус на сервере — это еще не панацея, ведь вирус может проникнуть в компьютер пользователя со сменных носителей. Кто-то может специально или непреднамеренно инфицировать компьютер, открыв зараженный файл с дискеты или компакт-диска. Поэтому не нужно забывать и о клиентских антивирусных решениях. Таких довольно много, поэтому я думаю, что вы уже сделали выбор. Кроме антивируса я бы порекомендовал еще установить брандмауэр на каждую рабочую станцию и средство поиска spyware (шпионских программ). Подробно об этом мы поговорим в *главе 19*.

9.2.6. Необходим ли дежурный администратор?

Практически все компьютеры (кроме серверов) выключены, все пользователи разошлись по домам. В здании осталась только охрана. Спрашивается, зачем нужен дежурный администратор? Оказывается, нужен... Представим, что ночью кто-то решил взломать сеть предприятия. Если дежурного администратора нет, факт взлома будет замечен только утром, а тогда может быть уже поздно. Поэтому на дежурном администраторе экономить не нужно. Конечно, можно выключить серверы на ночь, но это тоже не выход — как, например, пользователи из других стран, где не ночь, а день, получат доступ к вашему Web-серверу? Правильно, никак. Не солидно как-то….

9.3. Человеческий фактор

Человеческий фактор оказывает огромное влияние на безопасность сети. Как говорил один мой знакомый системный администратор: "Даже самая безопасная система не в силах устоять против несанкционированного доступа, если пароль пользователя написан на желтой бумажке, приклеенной к монитору".

9.3.1. Ограничение доступа

Понятно, что на пароль особо надеяться не нужно, даже если вы обойдете все комнаты и лично убедитесь, что пароль не написан маркером на мониторе или клавиатуре. Желательно, кроме назначения пароля, выполнять проверку и IP-адреса (который, в свою очередь, будет привязан к MAC-адресу), то есть разрешать доступ к тому или иному ресурсу корпоративной сети только по IP-адресу.

9.3.2. Как быть с обиженными или уволенными сотрудниками?

Все мы знаем, что такое месть. В ней нет ничего странного — так уж устроен человек... Просто кто-то может перебороть это чувство, а кто-то — нет. Существуют два типа недовольных сотрудников: просто обиженный и обиженный и уволенный. Более опасен первый тип, поскольку второму можно закрыть доступ в сеть по причине его увольнения. Что же делать с первым? Все зависит от его прав доступа. Если администратор правильно распределил права доступа, то этот пользователь сможет повредить только свои данные, за которые он отвечает.

Намного сложнее ситуация, если увольняют одного из администраторов. Администратор — это человек, который знает о сети все, и даже если он не оставил "черный ход" в корпоративную сеть, то его знания могут быть использованы в не очень хороших целях. И даже не им самим, а конкурентами компании. Ведь они только и ждут, когда руководство что-то не поделит с администратором. А потом администратору последует очень интересное предложение, сами знаете какое. Поэтому в данном случае администратором должны заниматься уже не IT-специалисты компании, а служба безопасности.

9.3.3. Принцип "правая рука не знает, что делает левая"

Все мы знакомы с этим принципом. Давайте взглянем на него применительно к предприятию. Предположим, есть отдел. Пусть это будет отдел IT. Есть задача, которую нужно выполнить. Над ней должны работать, скажем, 3 человека. Но работать они должны не вместе, а по отдельности, — то есть цель у всех общая, но каждый должен дойти к ней своим путем. Получается, что в результате будет разработано не одно, а три решения задачи, — вам останется взять оптимальное. Такой способ очень эффективен: ведь если бы эти три человека работали вместе, то появилось бы всего одно решение. Администратору же нужно организовать такой режим доступа, чтобы эти три человека не могли получить доступ к файлам друг друга.

9.3.4. Планирование безопасности серверной комнаты/этажа

Серверное помещение — важнейшее помещение корпоративной сети. Для его защиты желательно установить электронные замки (доступ по паролю или чип-карте), а также систему видеонаблюдения, которая поможет определить время "миграции" сотрудников (ведь кто-то может выйти, а кто-то зайти — все это будет запечатлено с помощью видеокамеры). Иногда не будет лишней и охрана — все зависит от важности охраняемых данных. Помню, на одном из предприятий IT-отдел очень тесно работал со службой безопасности: на территорию предприятия нельзя было занести какой-либо носитель данных, не говоря о том, чтобы его вынести. IT-отдел проверял такие носители в случае, если кто-то пытался принести или вынести какую-либо информацию. А как же ноутбуки? Их вообще запрещалось там использовать. Да, похоже на паранойю, но в том случае безопасность была превыше всего, и введенные меры себя оправдывали. Что побудило предприятие пойти на такие меры? Кража информации, в результате которой предприятию был нанесен огромный экономический ущерб.

Также не следует забывать об элементарных правилах пожарной безопасности — все-таки компьютеров много, поэтому нужно приобрести пару огнетушителей.

9.4. Отдел системного администрирования и безопасности

А теперь опять рассмотрим человеческий фактор, но уже с другой стороны — с точки зрения подбора персонала.

9.4.1. Подбор персонала

Подбор персонала должен выполняться IT-специалистом, а не кадровиком предпенсионного возраста, который ничего не понимает в компьютерах. Это первый аспект. Второй заключается в том, чтобы подбор персонала выполнялся не только субъективно, то есть "по знакомству". Одно дело, если "по знакомству" находят действительно хорошего специалиста, но совсем другое, когда место программиста занимает "специалист", не имеющий элементарных представлений о IT.

В идеале должна быть определенная система тестирования, разработанная IT-специалистом (желательно посторонним, чтобы исключить субъективный фактор). Для компьютера не существует "своих" и "чужих", для него все равны

(при условии, что программа написана не с учетом "знакомых"), поэтому тестирование будет выполняться объективно. Кандидат, набравший большее количество баллов, будет принят на работу. Если времени заниматься разработкой такой системы нет, то можно пригласить постороннего IT-специалиста для подбора персонала.

Дипломы и сертификаты — конечно, хорошо. Хотя бывает так, что у человека нет даже высшего образования, а он является лучшим специалистом, чем дипломированный. Вот для этого и нужна система тестирования при приеме на работу — особенно с учетом особенностей нашей системы образования, когда за определенную сумму диплом приносят чуть ли не на дом. С сертификатами дело обстоит чуть иначе. Онлайн-сертификатам (которые можно получить любому желающему в Интернете) я бы не очень доверял — за "специалиста" пройти тест может кто угодно. А вот сертификаты, выданные крупными компаниями, например, Microsoft, порою говорят даже о большем, нежели дипломы о высшем образовании.

9.4.2. Инструктаж отдела IT

Желательно, чтобы при приеме на работу сотрудник знал не только название своей должности, но и свои права и обязанности. Чтобы каждый раз не рассказывать сотруднику, что он должен делать и какие результаты от него ожидаются, все это оформляется в служебную инструкцию, которую должен изучить сотрудник в первые дни работы. Вся его дальнейшая деятельность должна проходить в рамках инструкции. Что должно быть в инструкции? Прежде всего, общие положения, ожидаемые результаты деятельности данного сотрудника, права и обязанности сотрудника, правила взаимодействия с другими службами предприятия, критерии оценки результатов, ответственность и квалификационные требования. Инструкция должна разрабатываться опытным IT-специалистом, который мог бы не только создать инструкцию, но и обосновать необходимость того или иного пункта инструкции (ведь можно ее и из Интернета позаимствовать, а потом смотреть на нее большими от удивления глазами).

9.4.3. Распределение задач и сфер ответственности

Задачи IT-сотрудников и сферы их ответственности должны быть четко распределены. Кстати, для этого и пишется инструкция, в которой четко должно быть сказано, кто что должен делать и кто за что отвечает.

9.4.4. Контроль работы и иерархия

Обычно иерархия того или иного подразделения изображается в виде организационной или пирамидальной диаграммы. Лично мне больше нравится последняя. На рис. 9.2 изображена пирамидальная диаграмма иерархии IT-отдела.

Рис. 9.2. Пирамидальная диаграмма иерархии IT-отдела

Итак, на пирамиде мы видим: руководство IT-отдела, среднее звено и специалисты. К руководству относят следующие должности: директор департамента информационных технологий (попросту говоря, начальник IT-отдела) и руководитель проекта. Руководитель проекта — должность необязательная. Как правило, такая должность имеется на предприятиях, занимающихся разработкой IT-продуктов.

Директор IT-департамента занимается разработкой и внедрением информационных стратегий и созданием единой информационной структуры, подчиняется он только генеральному директору компании. Руководитель проекта подчиняется директору IT-департамента, но задача у него своя — он руководит отделом, который входит в структуру компании. В больших IT-компаниях может быть несколько IT-отделов, каждый из которых работает в своем направлении, и у каждого IT-отдела есть собственный руководитель проекта.

Теперь переходим к среднему звену. К нему могут относиться следующие должности: IT-менеджер, менеджер автоматизации, менеджер по работе с клиентами. Первый отвечает за бесперебойную работу всех информационных систем компании, второй занимается автоматизацией деятельности компании и ее филиалов, третий, как понятно из названия, работает с клиентами.

К специалистам относят следующие должности: системный администратор, главный программист, программист. В больших компаниях роли системного

администратора и IT-менеджера четко разделены: системный администратор подчиняется IT-менеджеру и выполняет исполнительские обязанности. А в не очень больших компаниях системный администратор частенько выполняет функции IT-менеджера. Главный программист руководит программистами и отвечает за своевременное выполнение проекта.

9.5. Программы для планирования сети

В Интернете можно скачать различные программы для планирования вашей сети. Конечно, они не учитывают всех приведенных в этой главе аспектов, но с их помощью вы хотя бы набросаете схему сети, которая поможет потом при развертывании сети. Могу назвать одну из таких программ: LanFlow (рис. 9.3). Скачать ознакомительную версию программы можно на сайте **www.pacestar.com/lanflow**.

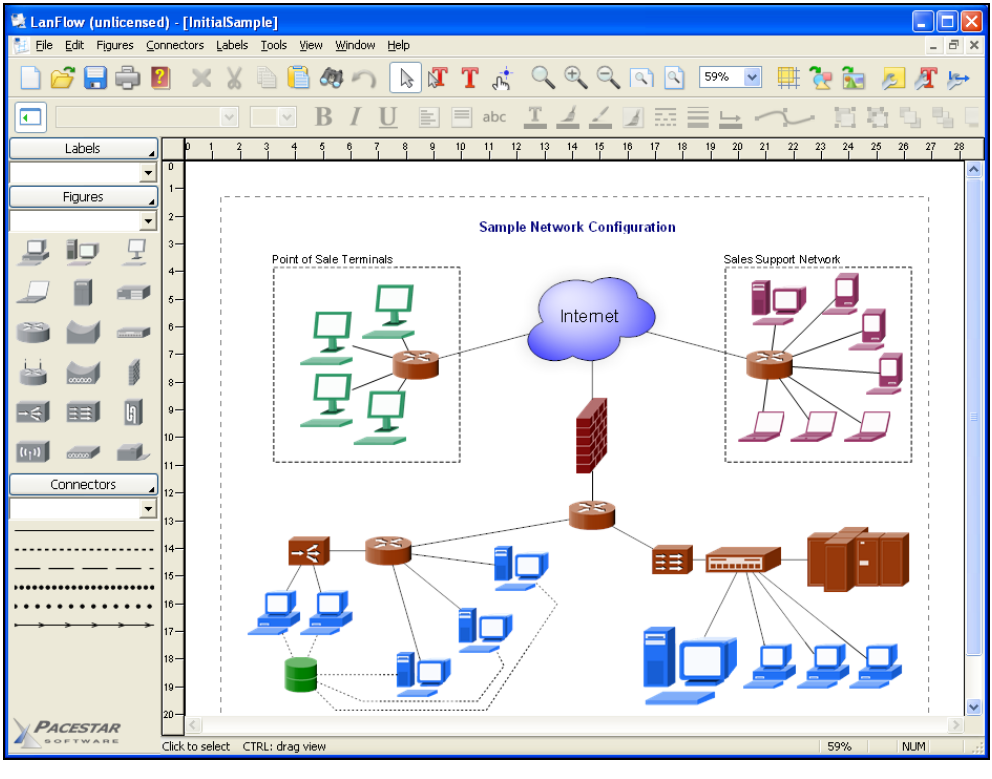


Рис. 9.3. Программа LanFlow

Глава 10

Монтаж Ethernet-сети

10.1. Развитие стандарта Ethernet

В *главе 1*, когда мы знакомились с краткой историей сетей, были рассмотрены основные этапы развития сетей Ethernet, сейчас же настало время поговорить о стандарте Ethernet подробнее.

Технология Ethernet намного "древнее", чем это можно себе представить. Хотя первая Ethernet-сеть была создана в 1975 году, она использует (как на момент создания, так и сейчас) метод доступа CSMA/CD (мы его рассмотрим позже), который был разработан во второй половине 60-х годов прошлого века.

Создателем Ethernet-сети является компания Xerox. В 1980 году эта компания вместе с компаниями DEC и Intel разработали вторую версию стандарта Ethernet, которая называлась DIX (DEC, Intel, Xerox) или Ethernet-II. В то время Ethernet-сети использовали в качестве среды передачи данных только коаксиальный кабель.

Чуть позже был разработан стандарт IEEE 802.3, который практически полностью повторял стандарт Ethernet II. У нового стандарта были лишь небольшие отличия в формате кадров, в нем не было протокола тестирования конфигурации, который существовал в DIX, и новый стандарт выделял два уровня MAC и LLC, которые в DIX были одним целым.

Среди ранних модификаций стандарта Ethernet можно выделить следующие:

- Xerox Ethernet — оригинальный стандарт, предусматривающий скорость передачи данных 3 Мбит/с. Как уже было отмечено, существовали две версии этого стандарта: 1 и 2 (DIX);
- 10BROAD36 — позволял передавать данные на большие расстояния, для чего использовал технологию широкополосной модуляции. Средой передачи данных служил коаксиальный кабель. Стандарт не получил широкого распространения;

- 1BASE5 (второе название StarLAN) — дальний предок стандарта 10Base-T. Скорость передачи данных — 1 Мбит/с. В качестве среды передачи данных использовал витую пару. Не получил большого распространения.

10.1.1. Модификации стандарта Ethernet

После принятия стандарта IEEE 802.3 технология Ethernet продолжала бурно развиваться — скорость передачи данных повысилась до 10 Мбит/с (это еще в стандарте 802.3), а в качестве среды передачи данных использовался не только коаксиальный кабель, но и витая пара, и оптоволоконный кабель. Модификации стандарта Ethernet представлены в табл. 10.1.

Таблица 10.1. *Модификации стандарта Ethernet*

Стандарт	Описание
10Base-5 (IEEE 802.3)	Использовался "толстый" коаксиальный кабель RG-8, именно поэтому данный стандарт иногда называют "толстый Ethernet". Максимальная длина сегмента — 500 метров
10Base-2 (IEEE 802.3a)	Сеть на базе "тонкого коаксиала" (кабель RG-58). Поскольку тонкий коаксиал более гибкий, такую сеть было проще монтировать, чем сеть 10Base-5. Однако максимальная длина сегмента не превышает 200 метров. Этот стандарт прожил долгую жизнь. Помню, встречал сеть на его базе даже в 2002 году (правда, после уже не видел, но уверен, что где-то они до сих пор есть)
StarLAN 10	Первый стандарт, работающий на скорости 10 Мбит/с и использующий витую пару. Послужил прототипом стандарта 10Base-T
10Base-T (IEEE 802.3i)	Среда передачи данных: витая пара 3-й или 5-й категорий. Максимальная длина сегмента такой сети — 100 метров
FOIRL (Fiber-optic inter-repeater link)	Стандарт, использующий для передачи данных оптоволоконный кабель. Послужил прототипом для 10Base-F. Максимальное расстояние передачи данных (без повторителя) — 1 км
10Base-F (IEEE 802.3j)	Основной стандарт, послуживший базой для стандартов 10Base-FL, 10Base-FB, 10Base-FP. Все стандарты используют в качестве среды передачи данных оптоволоконный кабель. Расстояние — до 2 км, скорость передачи данных — 10 Мбит/с

Таблица 10.1 *(окончание)*

Стандарт	Описание
10Base-FL (Fiber Link)	Практически то же самое, что и FOIRL, но длина передачи данных увеличена до 2 км
10Base-FB (Fiber Backbone)	Предназначался для объединения повторителей в магистраль
10Base-FP (Fiber Passive)	Топология "пассивная звезда", которая не предусматривает повторителей. Этот стандарт остался на бумаге — он не был реализован

10.1.2. Стандарты Fast Ethernet (100 Мбит/с)

Настоящий прорыв в развитии Ethernet произошел в 1995 году, когда появилась технология Fast Ethernet, позволяющая передавать данные со скоростью в 10 раз выше обычного Ethernet'а — 100 Мбит/с. С появлением Fast Ethernet коаксиальный кабель ушел в прошлое, новая технология в качестве среды передачи данных использовала только витую пару 5-й категории и оптоволоконный кабель.

Стандарты Fast Ethernet представлены в табл. 10.2.

Таблица 10.2. *Модификации стандарта Fast Ethernet*

Стандарт	Описание
100Base-T	Общее название стандарта для модификаций 100Base-TX, 100Base-T4 и 100Base-T, которые описаны далее. Все эти стандарты используют витую пару, а максимальная длина сегмента составляет 100 метров
100Base-TX (IEEE 802.3u)	Дальнейшее развитие стандарта 10Base-T. Как и в 10Base-T, используется топология "звезда"
100Base-T4	Создан из соображений обратной совместимости. Данный стандарт использует витую пару категории 3. Это значительно упрощает модернизацию сетей 10Base-T, где из соображений экономии использовалась витая пара 3-й категории. Нужно отметить, что этот стандарт сейчас практически не используется
100Base-T2	Еще один вариант на витой паре 3-й категории, сейчас практически не применяется. Отличительная особенность: использует полный дуплекс (то есть один и тот же кабель может *одновременно* использоваться как для приема, так и для передачи данных). Скорость приема/передачи данных (в одном направлении) — 50 Мбит/с

Таблица 10.2 *(окончание)*

Стандарт	Описание
100Base-FX	Использует многомодовое оптоволокно, максимальная длина сегмента в полудуплексе — 400 метров, в полном дуплексе — 2 км
100Base-LX	Используется одномодовое волокно (оборудование на базе одномодового кабеля стоит дороже). Обеспечивает передачу данных на расстояние 15 км в режиме полного дуплекса, длина волны 1310 нм
100Base-LX WDM	То же, что и 100Base-LX, но допускается использование длин волны 1310 нм и 1550 нм. При этом с одной стороны используется передатчик с длиной волны 1310 нм, а с другой — 1550 нм

Что такое дуплекс

В приведенной здесь таблице встретился, возможно, незнакомый вам термин — *дуплекс*. Существуют два режима передачи данных по одному и тому же кабелю: полудуплекс (Half Duplex) и полный дуплекс (Full Duplex). Рассмотрим оба режима на примере обычного телефона. Телефонная связь работает в *полнодуплексном* режиме, поскольку вы можете и говорить, и одновременно слышать своего собеседника, то есть вы можете говорить с ним одновременно. Если бы телефон работал в *полудуплексном* режиме, то когда бы вы говорили, то не слышали бы своего собеседника, поскольку передача идет в одном направлении — отправки. Вам нужно было бы сказать фразу, нажать какую-то кнопку, переключающую аппарат в режим приема информации, и тогда вы бы смогли услышать ответ своего собеседника.

Типы оптоволоконных кабелей

Многомодовый кабель — это кабель, где есть несколько пространственных мод, *одномодовый* — где имеется только одна мода. *Мода* — это тип электромагнитной волны в оптическом кабеле. Оптоволоконные кабели и сети на их основе из-за их дороговизны и сложности монтажа мы не рассматриваем. Интересующиеся могут прочитать о различных типах кабелей и их внутреннем устройстве по адресу: **http://kgg.moldline.net/teaching/cable/cable_media.htm**.

10.1.3. Gigabit Ethernet (1000 Мбит/с)

В 1998 году появилась новая технология Gigabit Ethernet. Прорывом или революцией ее не назовешь. По сути, это количественное улучшение, а не качественное. Ничего нового создано не было: та же среда передачи данных, тот же метод разделения этой самой среды — CSMA/CD. Зато очень легко модернизировать сеть Fast Ethernet в Gigabit Ethernet: достаточно заменить сетевые адаптеры и коммутаторы, кабели трогать не нужно — они останутся

прежними (нужно будет только переобжать концевые коннекторы, но об этом — позже). Модификации Gigabit Ethernet представлены в табл. 10.3.

Таблица 10.3. *Модификации стандарта Gigabit Ethernet*

Стандарт	Описание
1000Base-T (IEEE 802.3ab)	Использует витую пару категорий 5e или 6. В отличие от стандарта 100Base-TX, где используются только 2 пары кабеля (то есть 4 жилы), этот стандарт используется все 4 пары (8 жил), благодаря чему увеличивается скорость передачи данных
1000Base-TX	Разработан Ассоциацией телекоммуникационной промышленности (Telecommunications Industry Association, TIA) в 2001 году. Работает в полном дуплексе, скорость передачи данных в обеих направлениях — 500 Мбит/с. Использует 2 пары (4 жилы) для передачи данных, и 2 — для приема, что упрощает конструкцию приемопередающих устройств, но требует витую пару более высокой категории — 6-й. Зато этот стандарт предполагает более простое оборудование, которое стоит дешевле, чем оборудование для 1000Base-T
1000Base-SX (IEEE 802.z)	Использует многомодовое оптоволокно, длина сегмента — 550 метров
1000Base-LX (IEEE 802.3z)	Дальность передачи данных при использовании многомодового оптоволокна — 550 м, а при использовании одномодового — до 40 км (без повторителей)
1000Base-CX	Подходит для передачи данных на небольшие расстояния (до 25 м) и использует экранированную витую пару (STP). Сейчас этот стандарт не примняется и замен стандартом 1000Base-T
1000Base-LH (Long Haul)	Обеспечивает передачу данных на расстояние до 100 км без повторителей

10.1.4. Наше будущее — 10 Gigabit Ethernet

Относительно недавно был разработан новый стандарт, способный передавать данные со скоростью 10 Гбит/с — 10 Gigabit Ethernet. Этот стандарт пока еще очень молод, и понадобится несколько лет, чтобы понять, какие его спецификации будут востребованы, а какие исчезнут с рынка.

Пока доступны следующие спецификации:

- 10GBase-CX4 — используется для передачи данных на короткие расстояния (до 15 м), применяются медный кабель CX4 и коннекторы InfiniBand. Мне кажется, что этот стандарт не получит особого распространения (как и 1000Base-CX), но поживем — увидим;
- 10GBase-SR — пригоден для передачи данных на небольшие расстояния (от 26 до 82 метров в зависимости от типа кабеля), использует многомодовое оптоволокно;
- 10GBase-LX4 — расстояние передачи данных от 240 до 300 метров по многомодовому оптоволокну или до 10 км по одномодовому оптоволокну;
- 10GBase-LR и 10GBase-ER — используются для передачи данных на расстояния до 10 и 40 км соответственно;
- 10GBase-T — принят в 2006 году (самый молодой стандарт из этого семейства), использует экранированную витую пару, длина сегмента (расстояние передачи данных) — 100 метров.

10.2. Несколько слов о коллизиях...

Чтобы иметь представление о Ethernet-сетях, вам нужно знать, что такое метод доступа CSMA/CD (Carrier-Sense-Multiply-Access with Collision Detection) — метод коллективного доступа с обнаружением несущей (carrier) и коллизий. Этот метод используется во всех сетях с логической топологией "общая шина". Да, с появлением коммутаторов Ethernet-сети преобразились, но метод CSMA/CD служит до сих пор.

Представим себе общую шину — общую среду передачи информации. Ее можно сравнить с гирляндами лампочек на елке — все они подключены к одному проводу. Поскольку кабель общий, одновременно обмениваться информацией могут всего два компьютера. Спрашивается, какая же будет эффективность такой сети, если вся сеть должна ждать, пока два компьютера обмениваются информацией? Однако все происходит иначе. Все мы помним, что перед передачей данные разбиваются на части — пакеты. Общий алгоритм передачи данных таков:

1. Компьютер разбивает информацию на пакеты.
2. Затем он проверяет, не занята ли среда передачи данных.
3. Если среда свободна, компьютер передает один пакет.
4. После передачи пакета компьютер должен подождать 9,6 мкс, а потом начать процесс передачи следующего пакета.

Иногда случается *коллизия* — ситуация, когда два или больше компьютеров пытаются одновременно передать данные. Почему происходят коллизии, ведь компьютер перед отправкой данных проверяет, свободна ли среда передачи данных? Сначала разберемся, как он это делает. Компьютер прослушивает *несущую частоту* (carrier sense — вот откуда взялись две начальные буквы CS в названии метода!). Если несущей частоты (5–10 МГц) нет, то среда свободна. А теперь представим, что компьютер А только начал передавать кадр, а компьютер Б, который находится где-то очень далеко, одновременно начал проверять занятость среды передачи данных. Понятно, что несущая частота еще не "дошла" до компьютера Б, поэтому он тоже начал передачу данных. В результате передаваемые данные смешались — вот вам и коллизия…

Суть метода CSMA/CA в том и заключается, что когда два или большее количество узлов пытаются одновременно передать данные, CSMA/CA "просит" все узлы, кроме одного, прекратить передачу данных. "Счастливчик", которому разрешено передать данные, выбирается случайным образом. Но CSMA/CA может также предоставить приоритет узлу, который пытается передать данные, критические к времени (видео и/или голос).

В современных сетях на базе коммутаторов коллизии возникать, в общем-то, не должны — поскольку к каждому порту коммутатора подключено по одному компьютеру, и коммутатор передает пакет не всем компьютерам, а только тому, кому пакет адресован. Однако и в таких сетях коллизии порой возникают — например, когда сетевой адаптер и порт коммутатора одновременно начинают передавать кадры, решив, что кабель не занят. Правда, такая ситуация может сложиться только в полудуплексном режиме. В полнодуплексном режиме, как мы знаем, разрешена одновременная передача данных в обоих направлениях (прием и передача), поэтому в сети на базе коммутаторов, работающей в полнодуплексном режиме, коллизии не возникают.

10.3. Монтаж сети

10.3.1. Основные компоненты Ethernet-сети

Итак, давайте вспомним основные компоненты сети:

- *сетевые адаптеры* — с этим проблем сейчас нет, поскольку сетевые адаптеры встроены в материнские платы всех настольных компьютеров и ноутбуков;
- *вилки* (концевые коннекторы, разъемы) RJ-45 — ими обжимается витая пара, после чего обжатым кабелем можно соединить компьютер с коммутатором. Поскольку этими вилками кабель обжимается с обеих сторон,

то количество вилок должно в два раза превышать количество компьютеров. Разъемы желательно покупать с запасом (они стоят копейки), поскольку во время обжима разъем легко повредить. На рис. 10.1 приведена схема нумерации контактов вилки RJ-45;

- *кабель "витая пара"* — о выборе витой пары мы поговорим чуть позже;
- *коммутатор* — перед покупкой коммутатора убедитесь, что он содержит достаточное количество портов, необходимое для подключения всех компьютеров вашей сети. Если у вас много компьютеров, скажем больше 24, то имеет смысл купить два коммутатора по 24 порта, чем один на 48 — для локализации трафика и уменьшения нагрузки на коммутатор;
- *инструмент для обжима витой пары* — именно этим инструментом вы будете обжимать витую пару (рис. 10.2).

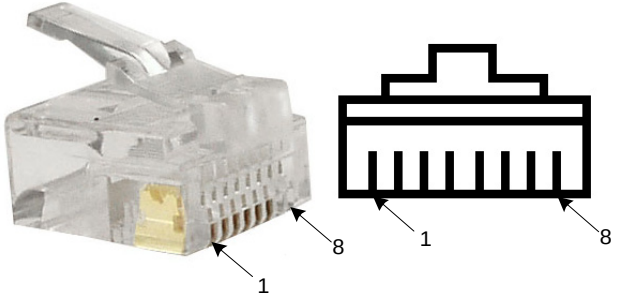


Рис. 10.1. Нумерация контактов вилки RJ-45

Рис. 10.2. Инструмент для обжима витой пары

Примечание

Интересно, что то, что практически все называют разъемом RJ-45, на самом деле называется вилкой 8P8C. Подробно об этом можно прочитать в Википедии: **http://ru.wikipedia.org/wiki/8P8C**.

Совет

Не покупайте дешевый инструмент для обжима витой пары! Помните пословицу о дешевой рыбке и соответствующей ей юшке? Когда-то я решил купить дешевый инструмент — он стоил в три раза дешевле, чем обычно. Да, на вид он был такой же. И вроде RG-45 обжимал. Как оказалось, именно "вроде". Сколько я разъемов испортил! Оказывается, этот инструмент не до конца обжимал разъем — обжимал не все его контакты. А чтобы обжать все контакты, приходилось сжимать разъем сильнее. Чуть-чуть перестарался, и все — разъем треснул. В итоге этот инструмент я выбросил и купил нормальный. Скупой платит дважды.

Если вам нужно построить небольшую сеть (скажем, до 10 компьютеров), тогда можно пойти путем наименьшего сопротивления и купить в компьютерном магазине уже готовые кабели. Они уже будут обжаты, и вам останется только соединить ими компьютеры с коммутатором. Обжатый кабель стоит немного дороже, чем комплект из витой пары необходимой длины и двух разъемов, но учитывая, что компьютеров будет немного, а профессионально заниматься монтажом сети вы не собираетесь, то вы даже сэкономите. Хороший инструмент стоит дороже, чем 5–7 уже обжатых кабелей (в зависимости от длины). Правда, в случае с обжатыми кабелями есть один недостаток: они продаются только фиксированной длины — обычно по 5 или 10 метров, что не всегда удобно.

10.3.2. Подробнее о витой паре

Категории витой пары

Витая пара витой паре — рознь. Существуют различные категории витой пары. Тут все просто: чем выше категория, тем кабель более качественный и дорогой. Витая пара 1–4 категорий уже не используется для построения сетей (хотя для построения сетей и ранее использовалась витая пара только 3 и 4-й категорий, а кабели 1 и 2-й категорий применялись в телефонных сетях).

Для построения современных Ethernet-сетей используется витая пара 5 и 6-й категорий. Пятая категория (CAT5) представляет собой 4-парный кабель (4 пары жил) и служит для построения сетей 100Base-TX. В этих сетях задействованы всего 2 пары (4 провода), при этом достигается скорость передачи данных до 100 Мбит/с.

Более современная модификация пятой категории называется 5E. Сейчас практически вся продаваемая витая пара относится к этой категории. При покупке кабеля обратите внимание на надписи на его внешней оболочке — лучше приобрести витую пару именно CAT5E, чем просто CAT5, поскольку модернизированная версия может использоваться для построения сетей Gigabit Ethernet. Для передачи данных со скоростью 1000 Мбит/с используются все 4 пары.

В июне 2002 года появилась витая пара шестой категории — CAT6. Она стоит дороже, чем витая пара CAT5E. Если вы планируете использовать Gigabit Ethernet, то следует применить витую пару шестой категории — она лучше подходит для передачи данных со скоростью 1000 Мбит/с. К тому же, для скоростей 10 Гбит/с CAT5E не годится вовсе, нужна CAT6. Поэтому если вы в будущем собираетесь модернизировать свою сеть — ваш выбор CAT6.

Кроме 5-й и 6-й есть еще и седьмая категория. Но она пока только анонсирована, и в свободной продаже ее нет. Планируется, что седьмая категория будет использована для построения сетей, работающих со скоростью 100 Гбит/с.

Классификация витой пары по типу защиты

Существуют следующие виды витой пары:

- UTP (Unshielded twisted pair) — защита и экранирование отсутствуют, это самый дешевый вид витой пары и предназначен для использования внутри помещений (конечно, такой кабель можно использовать и снаружи, но в силу своей незащищенности долго он не прослужит);
- FTP (Foiled twisted pair) — есть один общий экран (для всех пар) из фольги. Тип более защищенный, чем UTP;
- STP (Shielded twisted pair) — экранированная витая пара, присутствует один экран для каждой пары;
- S/FTP (Shielded Foiled twisted pair) — почти то же, что и FTP, но присутствует дополнительный внешний экран из медной оплетки;
- S/STP (Screened shielded twisted pair) — похож на STP, но присутствует дополнительный общий внешний экран.

Типы витой пары приведены по мере возрастания защиты и стоимости. Для наружного использования рекомендуется STP. Хотя если позволяют средства, то можно купить и S/STP.

10.3.3. Обжим витой пары

Обжать витую пару — это значит поместить отдельные жилы витой пары в определенной последовательности в вилку RJ-45 и закрепить их в этой последовательности с помощью инструмента.

А вот теперь начинается самое интересное: ключевая фраза здесь "в определенной последовательности". Последовательность расположения жил зависит от:

- стандарта кабеля;
- от того, кабель какого стандарта вы пытаетесь получить.

Существуют два стандарта витой пары: 568A и 568B (маркировка стандарта нанесена на оболочку кабеля). Если не вникать в подробности этих стандартов, то они для нас отличаются порядком обжима отдельных жил витой пары. И вся беда в том, что вам нужно помнить (или держать под рукой) обе схемы обжима. Ведь сегодня вы построили сеть на базе кабеля 568A, а завтра, когда

пришлось подключить дополнительный компьютер, в продаже был только 568B. Мы рассмотрим обе схемы обжима, но чуть позже.

Схема обжима может зависеть не только от стандарта кабеля, но еще и от того, что вы хотите соединить. Ethernet-кабель бывает *прямым*, а бывает — *перекрестным* (его еще называют кроссовер, от англ. cross-over).

- Прямой кабель используется для соединения компьютера с коммутатором и коммутатора с другим коммутатором, и схема обжима прямого кабеля с обеих сторон одинаковая.
- Перекрестный кабель служит для соединения двух компьютеров напрямую, без коммутатора (для организации сети из двух компьютеров) или для соединения некоторых старых коммутаторов/концентраторов, у которых есть порт Uplink. Одна вилка перекрестного кабеля обжимается как и у прямого кабеля, а вторая — перекрестно (с другим порядком расположения жил — чуть позже я поясню, как именно). Поскольку у кроссовера порядок обжима витой пары изменен, его нельзя использовать для подключения компьютера к коммутатору.

Итак, когда мы знаем о стандартах 568A и 568B и о прямом и перекрестном обжиме, самое время приступить к обжиму. Напомню, что схема нумерации контактов вилки RJ-45 приведена на рис. 10.1.

Прямой кабель, Fast/Gigabit Ethernet

В табл. 10.4 приведена схема обжима прямого Ethernet-кабеля стандартов 568A и 568B для сети Fast/Gigabit Ethernet (100/1000 Мбит/с). Напомню, что прямой кабель обжимается одинаково с обеих сторон.

Таблица 10.4. *Прямой Ethernet-кабель (100/1000 Мбит/с)*

Номер контакта	Цвет жилы (для 568A)	Цвет жилы (для 568B)
1	Зелено-белый	Оранжево-белый
2	Зеленый	Оранжевый
3	Оранжево-белый	Зелено-белый
4	Синий	Синий
5	Сине-белый	Сине-белый
6	Оранжевый	Зеленый
7	Коричнево-белый	Коричнево-белый
8	Коричневый	Коричневый

Перекрестный кабель (кроссовер) для соединения 100 Мбит/с

В табл. 10.5 приводится номер контакта и схема обжима для первой стороны и для второй стороны кабеля. Обратите внимание: схема действительна только для кабеля 586B.

Таблица 10.5. *Кроссовер 100 Мбит/с*

Номер контакта	Сторона 1	Сторона 2
1	Оранжево-белый	Зелено-белый
2	Оранжевый	Зеленый
3	Зелено-белый	Оранжево-белый
4	Синий	Синий
5	Сине-белый	Сине-белый
6	Зеленый	Оранжевый
7	Коричнево-белый	Коричнево-белый
8	Коричневый	Коричневый

Перекрестный кабель (кроссовер) для соединения 1000 Мбит/с

В табл. 10.6 приводится схема обжима кроссовера для соединения со скоростью 1000 Мбит/с (Gigabit Ethernet).

Таблица 10.6. *Кроссовер 1000 Мбит/с*

Номер контакта	Сторона 1	Сторона 2
1	Оранжево-белый	Зелено-белый
2	Оранжевый	Зеленый
3	Зелено-белый	Оранжево-белый
4	Синий	Коричнево-белый
5	Сине-белый	Коричневый
6	Зеленый	Оранжевый
7	Коричнево-белый	Синий
8	Коричневый	Сине-белый

Проверка правильности обжима кабеля

Обжимать кабель нужно тщательно, но стараясь не поломать коннекторы. Проверить, правильно ли вы обжали кабель, можно с помощью самого же коммутатора. Подключите один конец кабеля к компьютеру, а другой к коммутатору (коммутатор и компьютер должны быть включены).

Напротив каждого порта коммутатора есть минимум два индикатора: первый (обычно маркируется "Link/ACT") показывает, есть или нет связь, а второй (может маркироваться "Speed", или "100", или "1000" — в зависимости от устройства) — скорость работы порта. Технология Fast Ethernet подразумевает передачу данных со скоростью 100 Мбит/с, но поддерживает и старые устройства, которые могут работать только на 10 Мбит/с. Так вот, второй индикатор загорается только в том случае, если обеспечивается скорость 100 Мбит/с. Если же индикатор не загорается, давайте подумаем, в чем причина. Сетевой адаптер и коммутатор точно поддерживают скорость передачи данных 100 Мбит/с — старые устройства уже давно сняли с продажи, а новые помимо скорости 100 Мбит/с могут даже поддерживать скорость 1000 Мбит/с. Следовательно, дело в кабеле — вы неправильно его обжали (повреждение самого кабеля я исключаю), возможно, плохо обжали какой-нибудь контакт. Попробуйте, не снимая вилку, еще раз обжать ее. Если опять не получится, нужно срезать вилку и обжать кабель заново.

В случае с Gigabit Ethernet все аналогично: если не загорается индикатор "Speed", то кабель обжат неправильно. Если оба индикатора не горят, нужно обжать кабель заново — и так до тех пор, пока не обожмете правильно.

10.4. Ограничения при построении сети

Правильно обжать вилки RJ-45 — это еще не все. Нужно помнить о минимальной и максимальной длине кабеля. Минимальная длина — 1 метр, меньше никак. Максимальная — 100 метров. Что делать, если 100 метров мало? В этом случае нужно использовать несколько коммутаторов: к одному коммутатору вы подключаете близлежащие компьютеры и второй коммутатор. Ко второму коммутатору подключите остальные компьютеры. В итоге максимальное расстояние между двумя максимально удаленными компьютерами получится 210 метров (см. рис. 10.3).

Хочу заметить, что максимальная длина сегмента 100 метров — это только по стандарту, на практике можно "выжать" значительно больше. В зависимости от сетевого адаптера и коммутатора возможна максимальная длина сегмента до 150 метров. Только сами понимаете, никто не гарантирует, что:

- такой сегмент вообще будет работать (в некоторых условиях будет работать, а в некоторых — нет);

Рис. 10.3. Схема простой, но "длинной" сети

- будет достигнута максимальная скорость. Скорее всего, максимум, что получится выжать из такого длинного сегмента, — 10 Мбит/с. При превышении максимального расстояния дальнейшее развитие событий зависит от коммутатора и сетевого адаптера. Как минимум, вы получите потери сигнала в 40% (следовательно, и потерю скорости).

Однако вы должны знать, что такой вариант возможен. Иногда расстояние от одного из компьютеров до коммутатора составляет 105–110 метров. Ради одного компьютера и десяти лишних метров покупать еще один коммутатор не хочется, поэтому можно попробовать работать с превышением максимальной длины. Может и получится, а может — нет...

Если нужно еще большее расстояние, то лучше использовать оптоволоконный кабель — в этом случае максимальное расстояние достигнет 2000 м. Но в этой книге мы не рассматриваем сети на базе оптоволоконного кабеля. Как правило, в домашних и офисных сетях среднего размера вполне можно обойтись витой парой.

В табл. 10.7 вы найдете ограничения для сетей Fast и Gigabit Ethernet.

Таблица 10.7. *Сводная таблица ограничений*

Характеристика	Fast Ethernet	Gigabit Ethernet
Минимальная длина кабеля	1 м	1 м
Максимальное расстояние между компьютером и коммутатором	100 м	100 м для 1000Base-T 25 м для 1000Base-CX
Максимальное расстояние между коммутаторами	90 м	90 м
Максимальный диаметр сети (расстояние между максимально удаленными друг от друга элементами)	210 (250) м	210 (250) м
Максимальное число компьютеров в сети	1024	1024
Витая пара (категория)	5, 5E, 6	5E, 6

А теперь предположим, что нам нужно построить сеть, подобную изображенной на рис. 10.3. То есть у нас есть два сегмента и два коммутатора. Какое может быть максимальное расстояние между коммутаторами? Из табл. 10.7 следует, что 90 метров. Считаем: если максимальное расстояние от компьютера 1 до коммутатора 1 — 100 метров и от компьютера 2 до коммутатора 2 — тоже 100 метров, а максимальный диаметр сети равен 250 метрам, то максимальное расстояние между коммутаторами может быть только 50 метров, а не 90, как указано в таблице. Обратите внимание, что и 250 метров — это теоретическое значение, на практике лучше ориентироваться на 210 метров (с запасом).

Иногда нужно увеличить расстояние между коммутаторами. Например, есть два здания, находящихся на небольшом расстоянии друг от друга. В каждом здании имеется коммутатор, к которому подключаются компьютеры, находящиеся в этом здании. Если длина кабеля между коммутаторами равна 90 метрам (теоретический предел), то максимальное расстояние от каждого коммутатора до конечного компьютера должно быть не более 80 метров: (250 – 90) / 2, см. рис. 10.4. Да и это довольно-таки теоретические построения. Лучше, как было сказано, ориентироваться на максимальную длину сети 210 метров.

Что же касается максимального числа узлов, то его с головой хватит для построения любой домашней и офисной сети среднего размера. Если узлов много, можно использовать несколько 48-портовых коммутаторов, объединенных в стек.

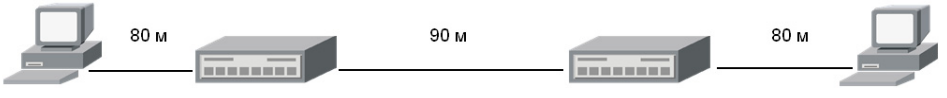


Рис. 10.4. Еще одна конфигурация сети

Глава 11

Общие папки и принтеры сети Microsoft

11.1. Рабочие группы или домен?

Сеть Microsoft может быть *одноранговой* (без выделенного сервера) и с архитектурой *клиент/сервер*. В последнем случае устанавливается отдельный сервер, называемый *первичным контроллером домена* (PDC, Primary Domain Controller). PDC содержит сведения о членах домена, управляет общими ресурсами домена и производит аутентификацию пользователей. Сеть с архитектурой клиент/сервер безопаснее и удобнее в использовании (чего только стоит функция миграции профилей пользователей!), но требует выделенного сервера.

> ***Примечание***
>
> Настройка собственного контроллера домена выходит за рамки этой книги. Если вы заинтересовались подобной тематикой, настоятельно рекомендую прочитать книгу "Windows Server 2008. Настольная книга администратора" (Чекмарев А., "БХВ-Петербург", 2009, **http://www.bhv.ru/books/book.php?id=185321**) или книгу "Знакомство с Windows Server 2008" (Митч Т., "БХВ-Петербург", 2008, **http://www.bhv.ru/books/book.php?id=182988**).

А в этой книге мы поговорим о настройке одноранговой сети на базе рабочих групп. Такая сеть чаще всего используется дома и в небольшом офисе. В офисе среднего размера уже желательно использовать сеть на базе доменов или же немного иначе организовать общие ресурсы (из соображений безопасности), а как это сделать, будет сказано чуть позже.

Обычно в одной сети есть только одна рабочая группа, но вы можете создать несколько рабочих групп и поместить в них неограниченное количество компьютеров. Один компьютер может быть членом только одной рабочей группы.

Недостаток одноранговой сети заключается только в отсутствии централизованного сервера аутентификации. Предположим, что у нас есть 5 пользователей: user1, user2, user3, user4 и user5. Вы хотите пользователям user1, user2

и user3 предоставить доступ к какому-либо каталогу только для чтения, а пользователям user4 и user5 — полный доступ. Соответственно, вам нужно на машине с данным каталогом создать 5 пользователей, назначить каждому его пароль, а затем в свойствах каталога установить необходимые полномочия пользователей. Сложность заключается в том, что пользователей нужно создавать на всех компьютерах сети, где планируется предоставление файлов и принтеров в общий доступ! А если один из пользователей попросит изменить ему пароль, его нужно будет изменять на всех компьютерах сети. А был бы центральный сервер аутентификации, все стало бы намного проще — пользователей пришлось бы создать только на одном компьютере — сервере.

Немного скрасить ситуацию позволяет создание гостевого аккаунта (гостевой учетной записи) — пользователя с именем Гость (guest). Вы можете разрешить использование гостевой учетной записи и применять ее для предоставления доступа только для чтения ко всем общим ресурсам. А для полного доступа придется создавать отдельных пользователей. В любом случае в нашем примере это сокращает количество пользователей с пяти до трех. Ведь нам потребуются только пользователь guest (он заменит пользователей user1, user2, user3) и пользователи user4 и user5.

В небольших сетях, где каждый знает друг друга, такая организация общего доступа весьма приемлема и удобна. Ведь не нужно тратиться на отдельный сервер. Не следует забывать также, что кроме "железа" придется покупать еще и "математику" — программное обеспечение. А операционная система Windows 2008 Server стоит недорого, только если к ней прилагается лицензия на 5 клиентов. Правильно, ради 5 машин никто не будет покупать Windows 2008 Server — вполне можно обойтись рабочей группой. А вот если машин в сети существенно больше, скажем, 30–50, то на покупку ОС придется потратиться. Так что повторюсь: для небольших сетей оптимальным будет использование рабочих групп. Когда "все свои" — пароль, по большому счету, вообще не нужен. Максимум, что даст пароль в такой ситуации, — это защиту данных от несанкционированных пользователей — например, от соседей, которые (намеренно или случайно) подключились к вашей Wi-Fi-сети и получили доступ к вашим общим ресурсам.

С другой стороны, даже если у вас всего двадцать компьютеров, обслуживать сеть на базе рабочих групп станет довольно сложно. В любом случае, я подскажу, как облегчить настройку такой сети, а пока нам нужно задать (изменить) имя рабочей группы.

11.2. Задание имени рабочей группы

11.2.1. В Windows

Задать (изменить) имя рабочей группы довольно просто — в Windows XP откройте Панель управления, щелкните двойным щелчком по значку **Система** (можно также щелкнуть правой кнопкой мыши по значку **Мой компьютер** на рабочем столе и выбрать команду **Свойства**). В Windows Vista намного проще открыть меню **Пуск**, щелкнуть правой кнопкой мыши на пункте меню **Компьютер** и выбрать команду **Свойства**.

В Windows XP откроется окно **Свойства системы** (рис. 11.1). Перейдите на вкладку **Имя компьютера** и нажмите кнопку **Изменить**. В открывшемся окне (рис. 11.2) вы можете изменить имя компьютера и имя рабочей группы компьютера. Имя компьютера должно быть уникальным в пределах рабочей группы, а имя рабочей группы должно быть одинаковым на всех компьютерах группы.

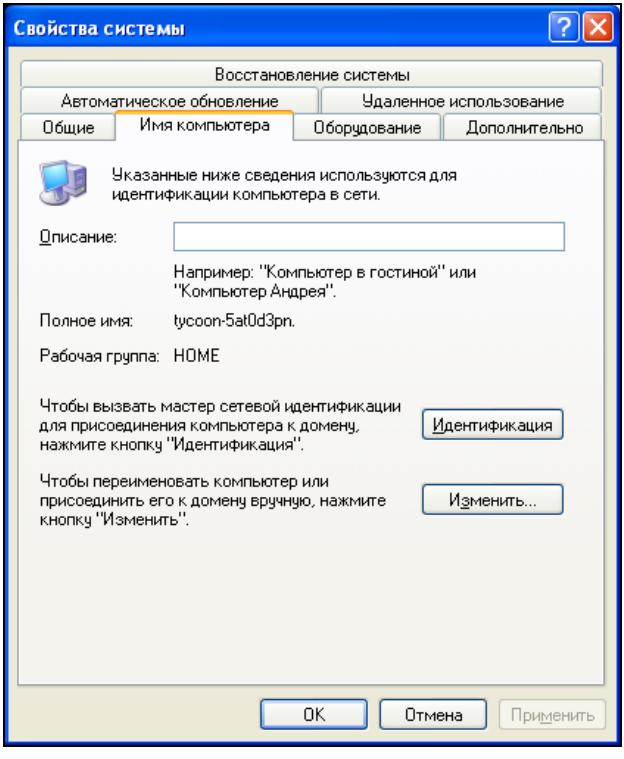


Рис. 11.1. Свойства системы (Windows XP)

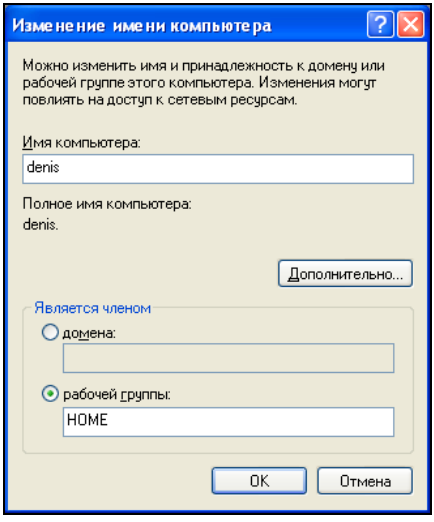


Рис. 11.2. Изменение имени компьютера и рабочей группы

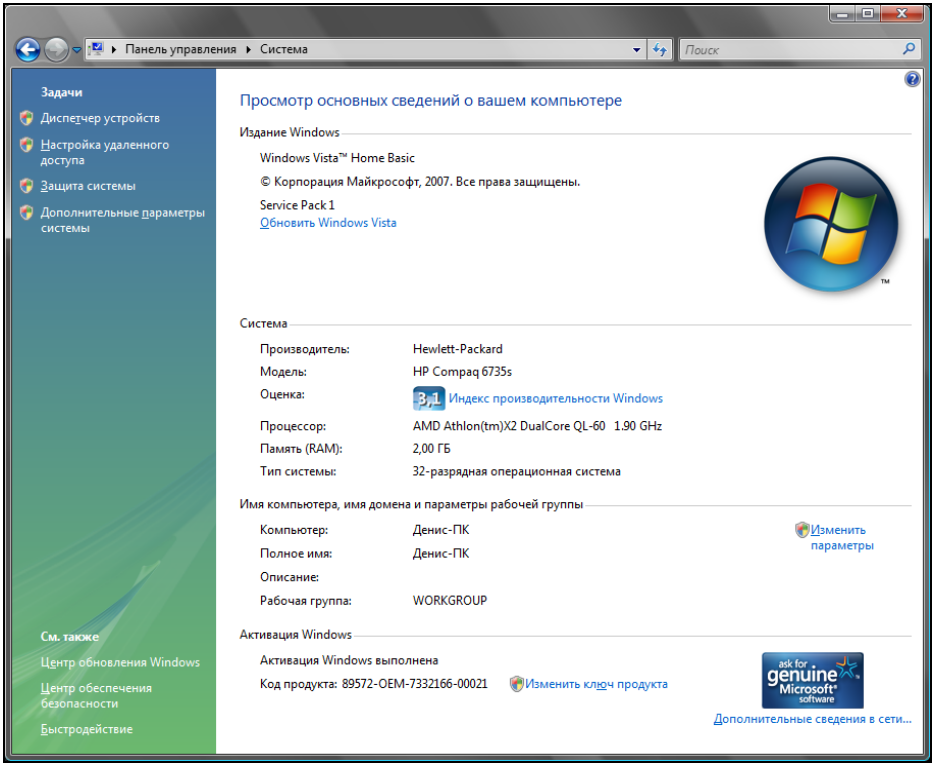


Рис. 11.3. Свойства системы (Windows Vista)

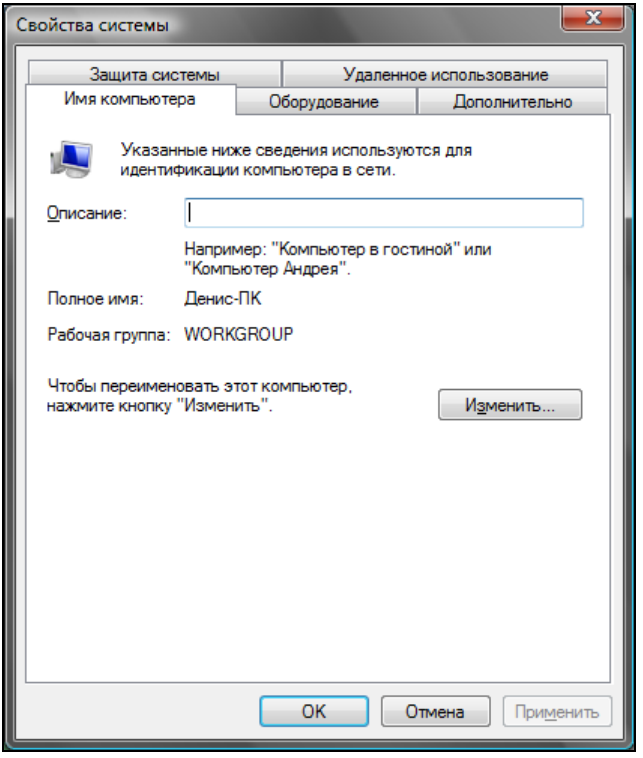


Рис. 11.4. Окно свойств системы в Windows Vista

В Windows Vista откроется окно свойств системы, изображенное на рис. 11.3. Щелкните на ссылке **Изменить параметры**, после чего откроется классическое окно **Свойства системы** (рис. 11.4), подобное изображенному на рис. 11.2. Для изменения имени компьютера и рабочей группы нажмите кнопку **Изменить**.

> ***Примечание***
>
> До сих пор не могу понять Microsoft. Зачем нужно было окно, изображенное на рис. 11.3? Ведь все основные функции осуществляются через окно **Свойства системы** (рис. 11.4), которое практически такое же, как в Windows XP.

11.2.2. В Linux

Учитывая, что в каждом дистрибутиве имеются свои средства конфигурации системы, описывать настройку сети Microsoft в тех или иных дистрибутивах Linux просто нет смысла. Я могу затронуть пять разных дистрибутивов,

а у вас будет шестой, который окажется не описан в этой книге. Поэтому настраивать сеть будем с помощью конфигурационных файлов.

Чтобы Linux-машина смогла получить доступ к сети Microsoft, на ней должен быть установлен пакет samba. Надеюсь, вы знаете, как его установить, потому что описывать установку пакетов в Linux я не буду. В помощь вам могу порекомендовать другую свою книгу "Linux. От новичка к профессионалу" ("БХВ-Петербург", **http://www.bhv.ru/books/book.php?id=184162**).

После установки пакета samba нужно отредактировать файл конфигурации /etc/samba/smb.conf. Пропишите следующие параметры в секции `global`:

```
[global]
workgroup = HOME
comment = Linux
security = share
```

Первый параметр задает имя рабочей группы, второй — это комментарий (описание компьютера), третий — тип безопасности (в сети без выделенного сервера следует установить тип безопасности `share`).

Сохраните файл конфигурации и перезапустите Samba:

```
# /etc/rc.d/init.d/smb restart
```

или

```
# service smb restart
```

Если эти две команды не помогли перезапустить Samba (о перезапуске Samba будет выведено соответствующее сообщение), перезапустите компьютер.

11.3. Предоставление доступа к файлам и папкам в Windows XP

Как оказалось, настройка общего доступа в Windows XP — не совсем простое занятие. Если вы когда-нибудь настраивали общий доступ в Windows 98, а сейчас будете пытаться проделать то же самое в Windows XP, то будете неприятно удивлены — все стало значительно сложнее. С другой стороны, общий доступ в Windows XP теперь намного безопаснее — при правильной настройке, разумеется.

11.3.1. Простой способ — через учетную запись *Гость*

Предоставить общий доступ к папке или диску достаточно просто — щелкните правой кнопкой по значку папки или диска и выберите команду **Свойства**. Перейдите на вкладку **Доступ** (рис. 11.5). В группе **Сетевой совместный**

доступ и безопасность вы можете или запустить **мастера настройки сети** или же просто открыть общий доступ к папке. Если вы еще ничего не настраивали, тогда можете запустить **мастера настройки сети**. А если вы уже задали имя рабочей группы и даже настроили общее соединение с Интернетом, необходимости в мастере нет. Щелкните по ссылке **Если вы понимаете потенциальную опасность…**. В открывшемся окне (рис. 11.6) выберите **Просто включить общий доступ к файлам**.

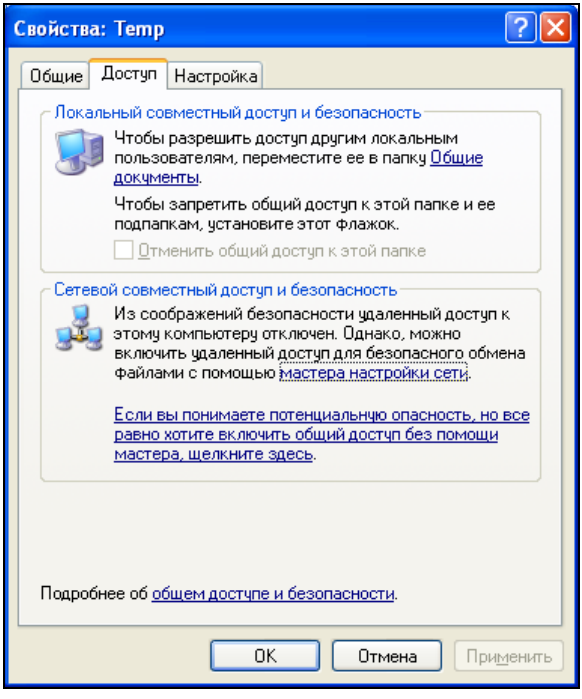


Рис. 11.5. Вкладка **Доступ**

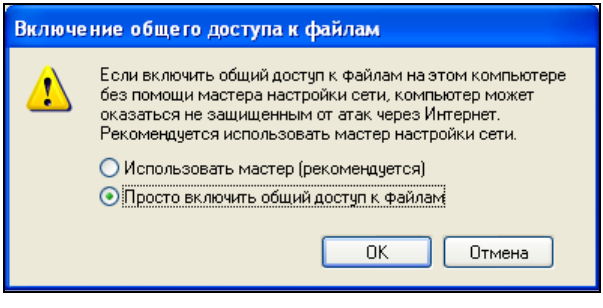


Рис. 11.6. Включение общего доступа к файлам

После этого вкладка **Доступ** окна свойств папки видоизменится (рис. 11.7). Включите параметр **Открыть общий доступ к этой папке**. Можно указать имя общего ресурса и разрешить изменение файлов по сети.

Примечание

Если доступ к файлам был уже включен ранее, то вместо окна, изображенного на рис. 11.5, будет сразу открываться окно, изображенное на рис. 11.7.

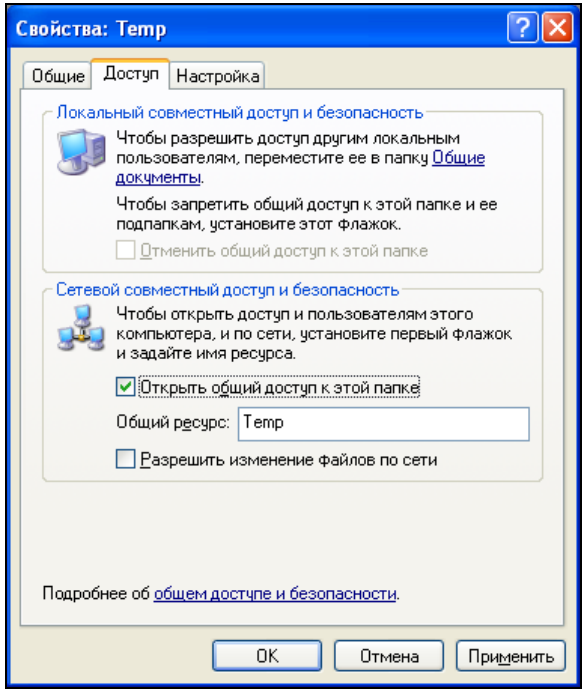


Рис. 11.7. Открыть общий доступ к этой папке

При просмотре файловой системы в Проводнике значки папок и дисков, к которым открыт общий доступ, будут отображаться с рукой, поддерживающей соответствующий значок (рис. 11.8).

Теперь попробуйте на другом компьютере сети открыть **Сетевое окружение** (значок находится на рабочем столе) и просмотреть список доступных сетей. Выберите рабочую группу — вы увидите список относящихся к ней компьютеров (рис. 11.9). Не можете получить доступ к общим ресурсам компьютера (рис. 11.10)? Скорее всего, у вас выключена учетная запись **Гость** (она как раз выключена по умолчанию).

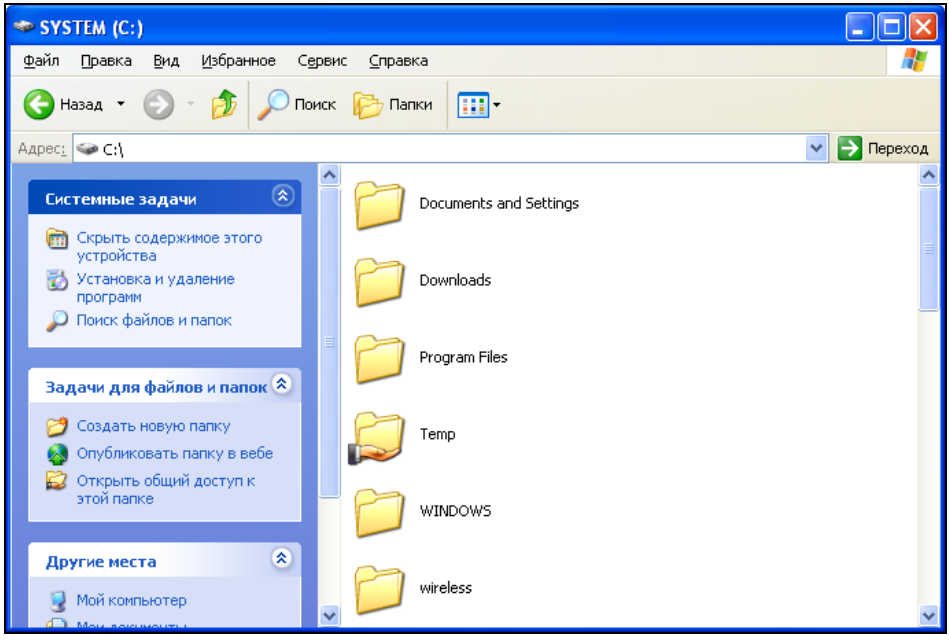


Рис. 11.8. К папке Temp открыт общий доступ

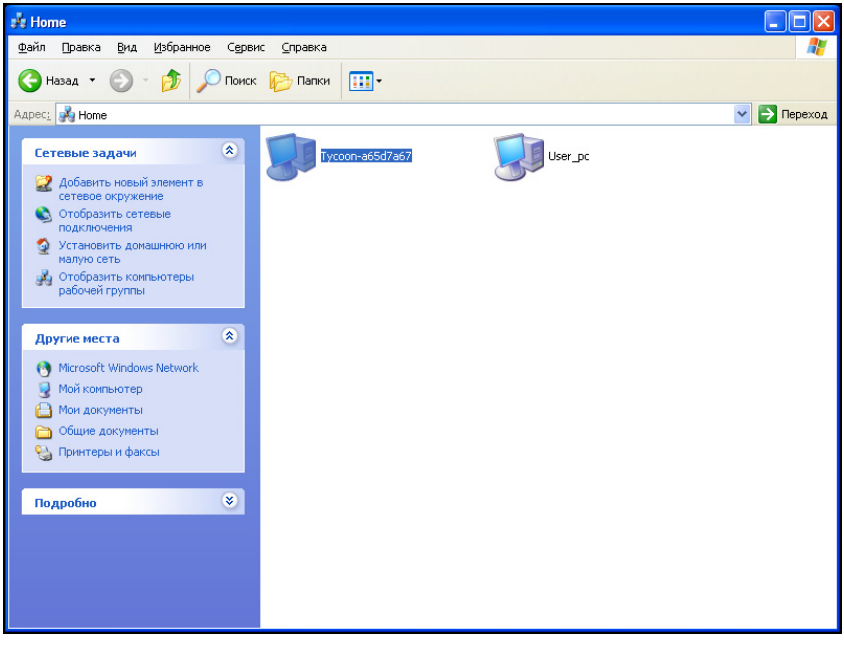


Рис. 11.9. Список компьютеров рабочей группы Home

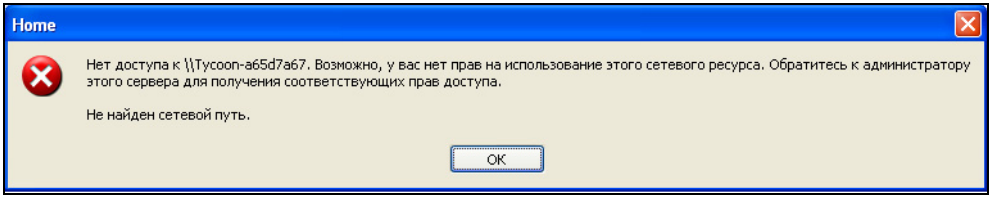


Рис. 11.10. Нет доступа к списку общих ресурсов

Давайте включим гостевую учетную запись:

1. Выполните команду **Пуск | Выполнить**.
2. Введите команду `lusrmgr.msc` и нажмите клавишу <Enter>. Откроется окно **Локальные группы и пользователи**.
3. Перейдите в раздел **Пользователи** и щелкните двойным щелчком по учетной записи **Гость**.
4. В открывшемся окне (рис. 11.11) снимите флажок **Отключить учетную запись**.

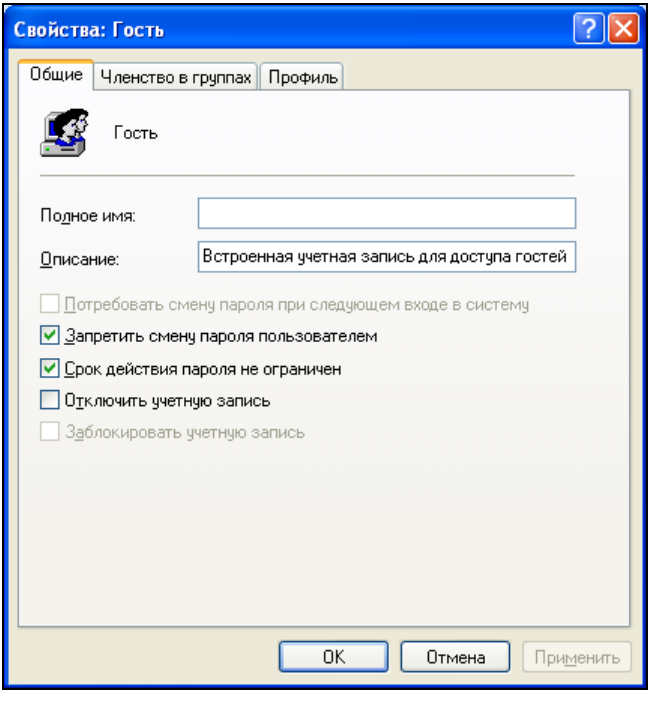


Рис. 11.11. Изменение учетной записи Гость

После этого все должно заработать, и вы сможете войти по сети на общий ресурс (рис. 11.12). Если и после этого не удается получить доступ к общим ресурсам, возможно, на вашем компьютере запущен брандмауэр, блокирующий доступ к компьютеру. В этом случае нужно обратиться к документации брандмауэра.

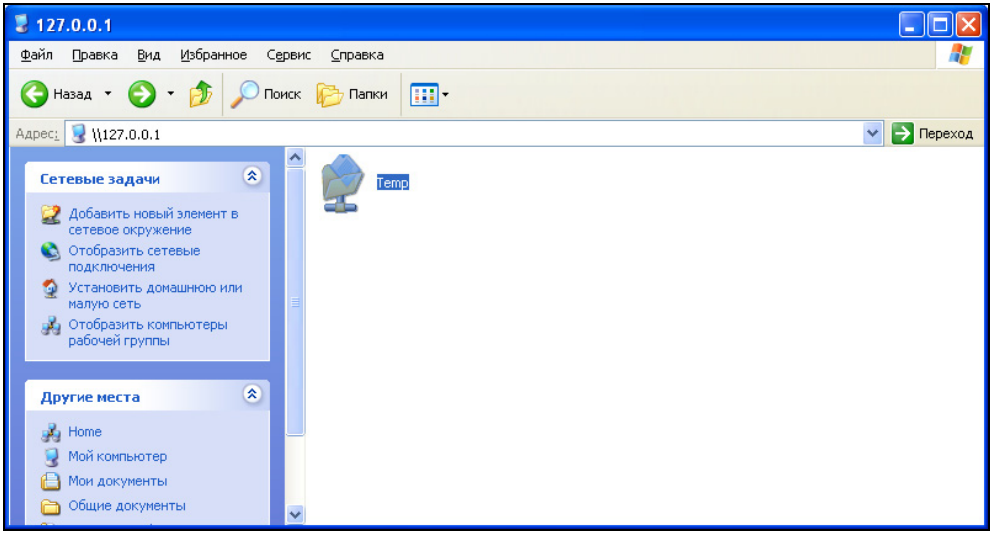


Рис. 11.12. Список общих ресурсов, предоставляемых моим (локальным) компьютером

11.3.2. Сложный способ — по паролю

Рассмотрим, как можно предоставить доступ к ресурсу по паролю. Это очень полезно, если надо некоторым пользователям предоставить к ресурсу полный доступ, а некоторым — ограниченный.

Существуют три способа предоставления общего доступа к файлам и принтерам в Windows XP:

- первый способ заключается в предоставлении его всем желающим — никакого контроля доступа не осуществляется. Этот способ был только что описан *(см. разд. 11.3.1)*. Его можно использовать, если ваша сеть надежно защищена брандмауэром, иначе доступ к вашим файлам и принтерам смогут получить интернет-пользователи!
- второй способ заключается в создании нужного количества учетных записей на вашем компьютере (и на других компьютерах локальной сети). Предположим, в нашей сети есть три компьютера. Для удобства их можно

назвать так: comp1, comp2 и comp3. Имя пользователя не должно совпадать с именем компьютера, поэтому пользователей, работающих за этими компьютерами, можно назвать: user1, user2 и user3. Вы знаете, что пользователь user1 соответствует компьютеру comp1, user2 — компьютеру comp2 и т. д. Если вы хотите разрешить пользователю user1 доступ к папке Video вашего компьютера, а пользователю user3 — доступ к вашему принтеру, вы создаете пользователей с такими именами на своем компьютере, назначаете им пароли, потом сообщаете их соответствующим лицам, которые будут работать за компьютерами. Понятно, что на другом компьютере можно создать пользователей с такими же именами, но пароли можно указать совсем другие. Это неудобно, поскольку возникнет путаница с паролями. Избежать ее никак нельзя, иначе придется устанавливать контроллер домена. Тут уже или комфорт, или экономия — решать вам;

- существует и третий способ — общий пароль. Это приемлемо, если в вашей сети всего 3–5 компьютеров, все они находятся на виду, и вы лично знаете всех пользователей сети. Здесь пароль, по большому счету, вообще не нужен! Однако он может защитить ваши компьютеры от вторжения посторонних пользователей, о чем мы уже говорили чуть ранее. В этом случае нужно поступить так:
  - Активировать на всех компьютерах учетную запись **Гость**.
  - Назначить на всех компьютерах одинаковый пароль для учетной записи **Гость**.

  На мой взгляд — идеальное решение. И сеть от "чужих" можно защитить, и довольно удобно для пользователей сети.

Общий пароль для учетной записи *Гость*

Задать пароль для учетной записи **Гость** очень просто:

1. Выполните команду **Пуск | Выполнить**.
2. Введите команду `lusrmgr.msc` и нажмите клавишу <Enter>. Откроется окно **Локальные группы и пользователи**.
3. Перейдите в раздел **Пользователи** и щелкните на учетной записи **Гость** правой кнопкой мыши.
4. Выберите в открывшемся контекстном меню (рис. 11.13) команду **Задать пароль**.
5. Введите пароль и его подтверждение.

Вот, собственно, и вся настройка.

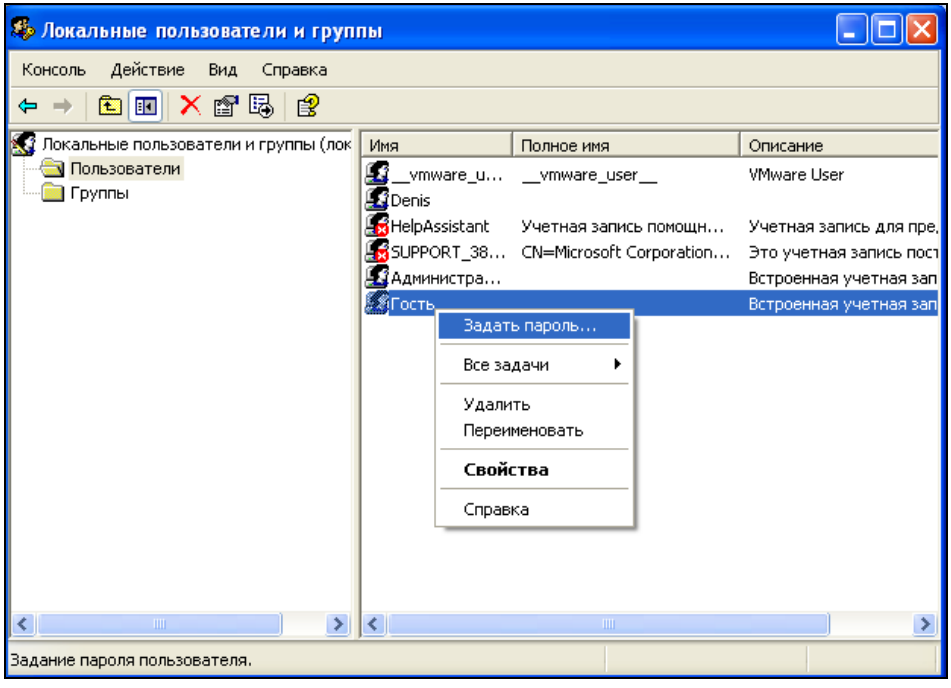


Рис. 11.13. Задание пароля для пользователя Гость

Создание пользователей и разрешение доступа к ресурсам определенным пользователям

Теперь рассмотрим более сложный способ, а именно — создание пользователей и разрешение доступа к ресурсам определенным пользователям. Прежде всего взгляните на рис. 11.7 — вкладка **Доступ** не содержит средств для выбора имен пользователей и разрешения им доступа к ресурсу (вы можете только предоставить доступ к ресурсу и назначить для него имя). Для того чтобы получить доступ к этим средствам — откройте Проводник, выберите команду **Сервис | Свойства папки**, перейдите на вкладку **Вид** и снимите флажок **Использовать простой общий доступ к файлам** (рис. 11.14). После этого вкладка **Доступ** преобразится (рис. 11.15).

Не спешите пока что-либо в ней настраивать. Вернитесь в окно **Локальные пользователи и группы** (см. рис. 11.13). Щелкните правой кнопкой на рабочей области окна и выберите команду **Новый пользователь**. В открывшемся окне (рис. 11.16) введите имя пользователя, его описание (если нужно), пароль, его подтверждение и снимите флажок **Потребовать смену пароля при следующем входе в систему**. Если других пользователей добавлять в систему не нужно, нажмите кнопку **Закрыть** — новый пользователь появится в списке пользователей (рис. 11.17).

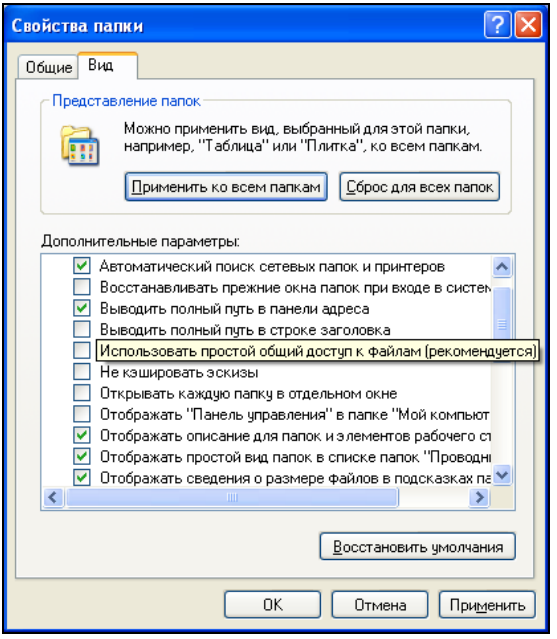


Рис. 11.14. Снимите флажок **Использовать простой общий доступ к файлам**

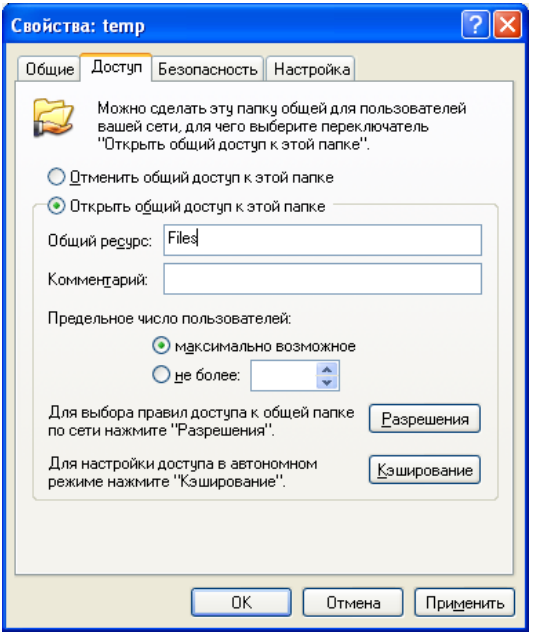


Рис. 11.15. Новая вкладка **Доступ**

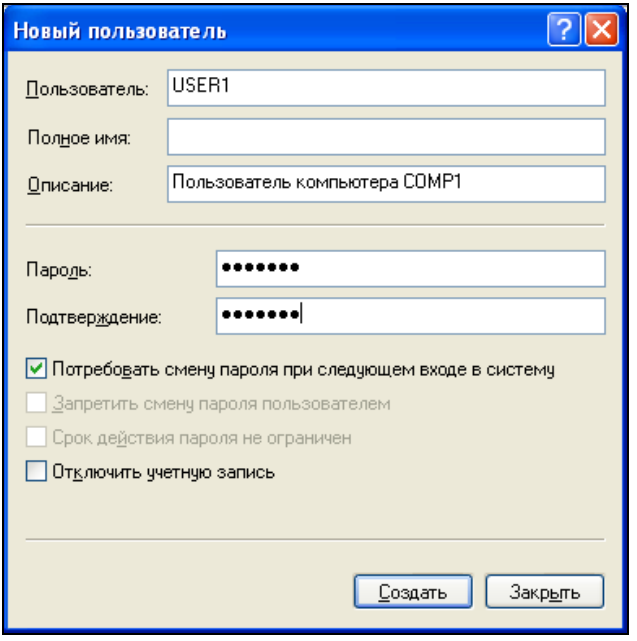


Рис. 11.16. Добавление пользователя

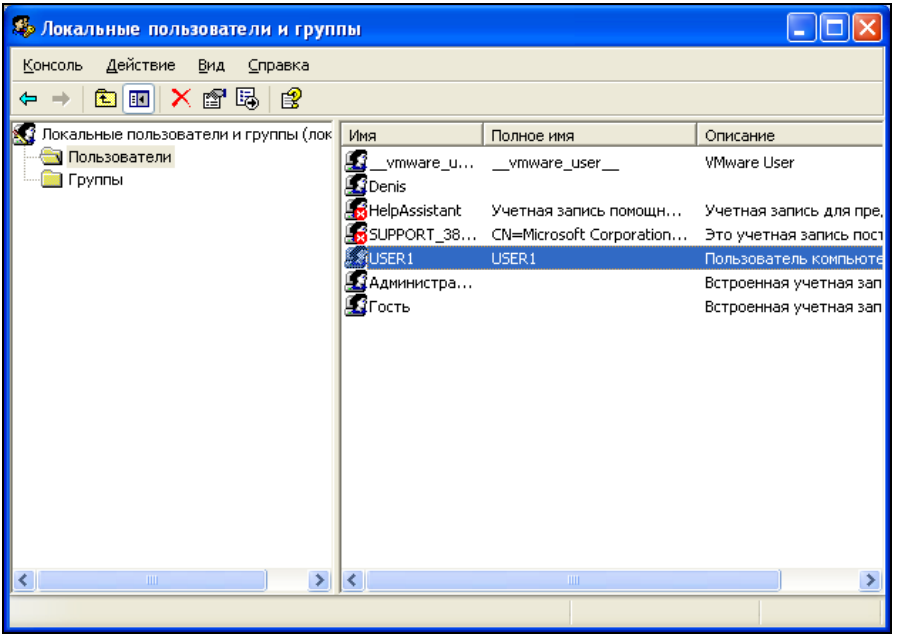


Рис. 11.17. Список пользователей

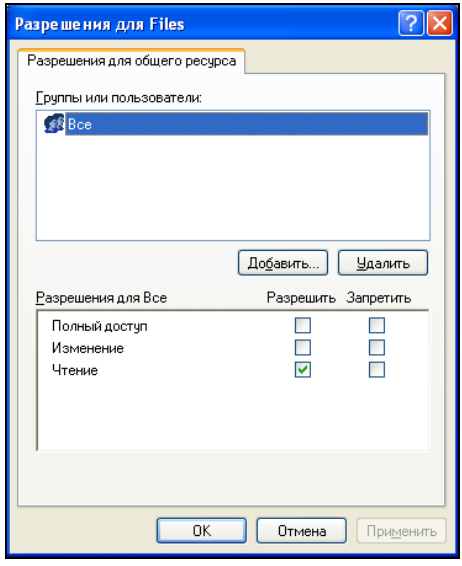


Рис. 11.18. Разрешения для ресурса

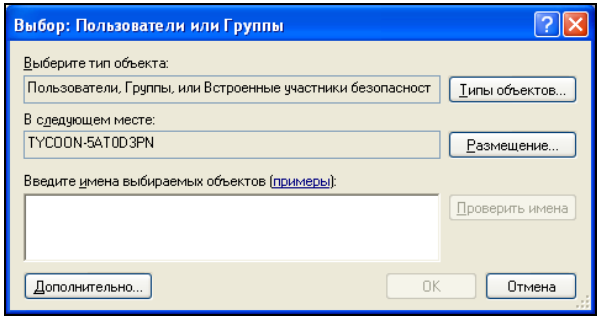


Рис. 11.19. Выбор пользователя или группы

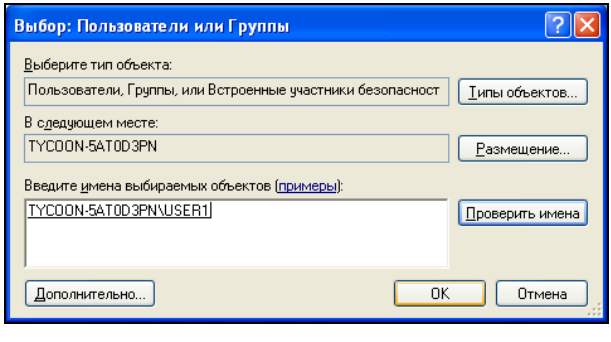


Рис. 11.20. Проверка имени пользователя

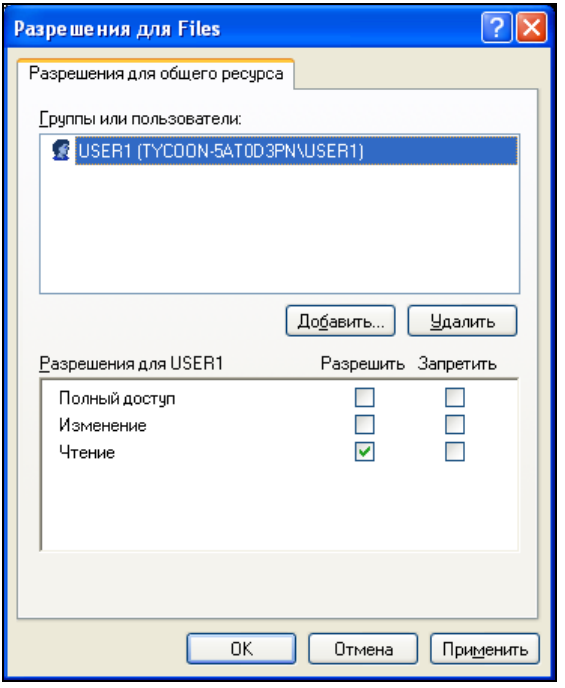


Рис. 11.21. Разрешения для пользователя **USER1**

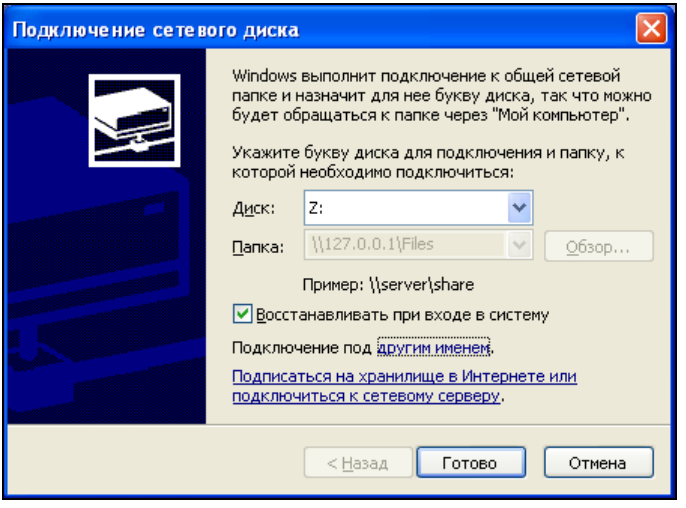


Рис. 11.22. Подключение сетевого диска

Теперь перейдите в окно Проводника, щелкните правой кнопкой мыши по значку ресурса, к которому вы хотите предоставить общий доступ, выберите команду **Свойства** и перейдите на вкладку **Доступ** (см. рис. 11.15). Включите переключатель **Открыть общий доступ к этой папке**, введите имя общего ресурса, комментарий (если нужно), установите предельное число пользователей. Затем нажмите кнопку **Разрешения**. Вы увидите окно **Разрешения для <Имя_ресурса>** (рис. 11.18). Выберите группу **Все** и нажмите кнопку **Удалить**. Затем нажмите кнопку **Добавить** — вы увидите окно, изображенное на рис. 11.19.

Введите имя пользователя (`USER1`) и нажмите кнопку **Проверить имена**. Если вы ввели имя пользователя правильно, перед ним будет добавлено имя компьютера (рис. 11.20). Если это так, нажмите кнопку **OK**, в противном случае попытайтесь еще раз.

Пользователь будет добавлен в список разрешений. После этого вы можете решить, какой тип доступа ему предоставить, например, **Полный доступ** или **Чтение** (рис. 11.21).

Затем нажмите кнопку **OK** — вы вернетесь в окно свойств ресурса, еще раз нажмите кнопку **OK** для сохранения изменений.

Но это еще не все. Перейдите к другому компьютеру сети. Если на него вы не зашли как пользователь USER1, вам будет отказано в доступе к сетевому ресурсу. Но это можно обойти — щелкните на сетевом ресурсе правой кнопкой мыши и выберите команду **Подключить сетевой диск**. В открывшемся окне (рис. 11.22) нажмите ссылку подключения под **другим именем**, а в открывшемся окне введите имя пользователя (желательно вводить его в формате `Компьютер_к_которому_подключаетесь\Имя_пользователя`) и пароль (рис. 11.23).

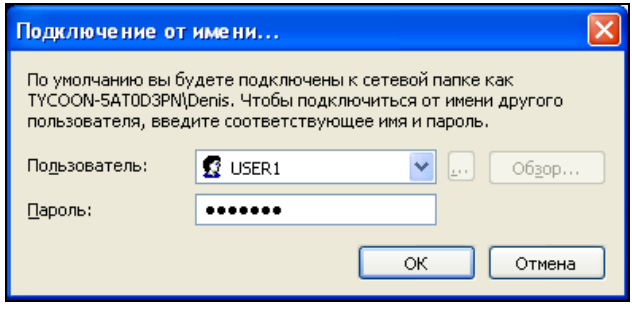


Рис. 11.23. Вход под другим именем

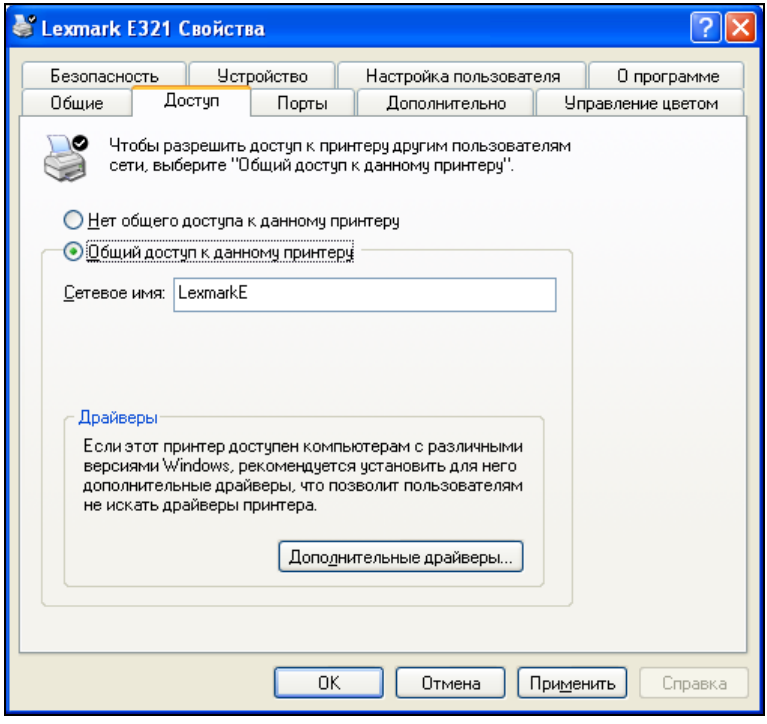


Рис. 11.24. Предоставление общего доступа к принтеру

Предоставить общий доступ к принтеру можно аналогично. Откройте папку **Принтеры и факсы**, щелкните на принтере правой кнопкой мыши, выберите команду **Общий доступ** и включите общий доступ к принтеру (см. рис. 11.24).

11.4. Общий доступ в Windows Vista

Процесс настройки общего доступа в Windows Vista в принципе подобен процессу настройки в Windows XP, но есть и отличия. В Windows XP была папка **Общие документы**, в которую можно было поместить файлы, которые вы хотели предоставить в общий доступ (если не собирались предоставлять доступ к отдельным дискам и папкам). В Vista эта папка называется **Общие**. Но работает она несколько иначе. Общий доступ к файлам из этой папки будет предоставлен, только если для сети установлено **Частное** размещение. Если размещение **Общественное** (рис. 11.25), доступ к файлам из папки **Общие** сетевые пользователи не получат.

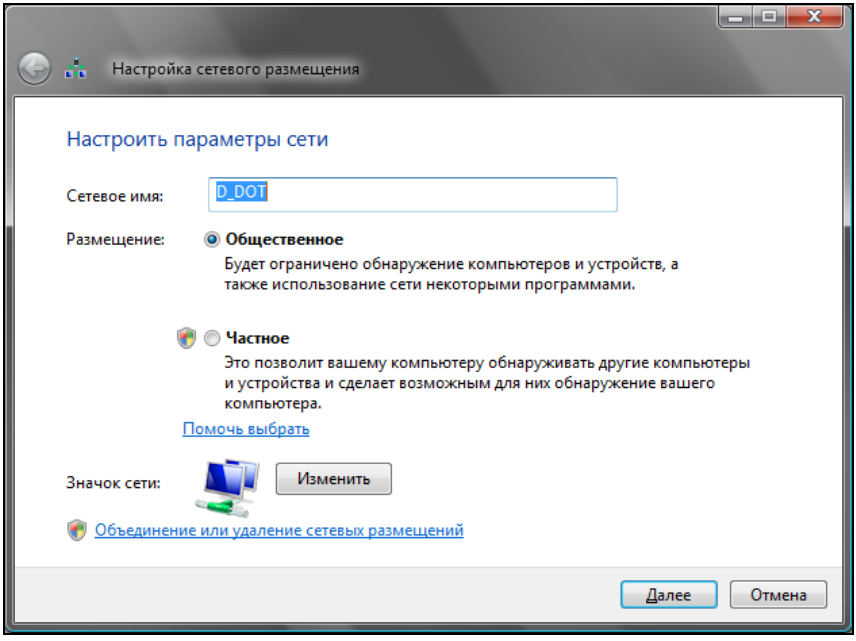


Рис. 11.25. Частное или публичное размещение сети

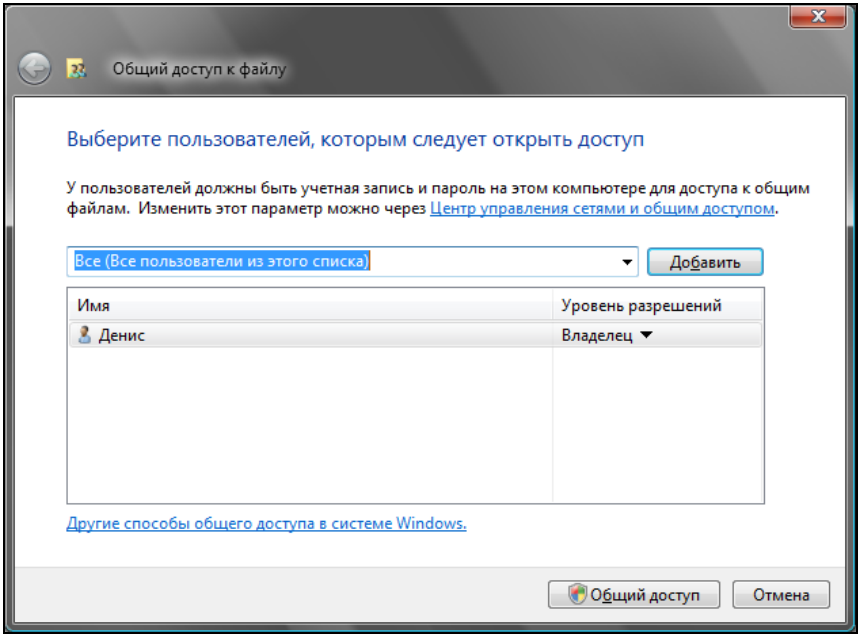


Рис. 11.26. По умолчанию доступ разрешен только пользователю-владельцу

Теперь рассмотрим, как предоставить общий доступ к произвольной папке. Щелкните правой кнопкой мыши на папке и выберите команду **Общий доступ**. В открывшемся окне нужно добавить пользователей, которым разрешен доступ к папке. По умолчанию добавлен только пользователь-владелец (рис. 11.26).

Вы можете добавить или всех пользователей или же какого-то конкретного пользователя. Добавить пользователя можно с помощью утилиты lusrmgr.msc или апплета **Учетные записи пользователей** Панели управления (**Панель управления | Добавление и удаление учетных записей пользователей**). Хотя проще всего добавить пользователя, выбрав из выпадающего списка пользователей опцию **Создать нового пользователя** (рис. 11.27).

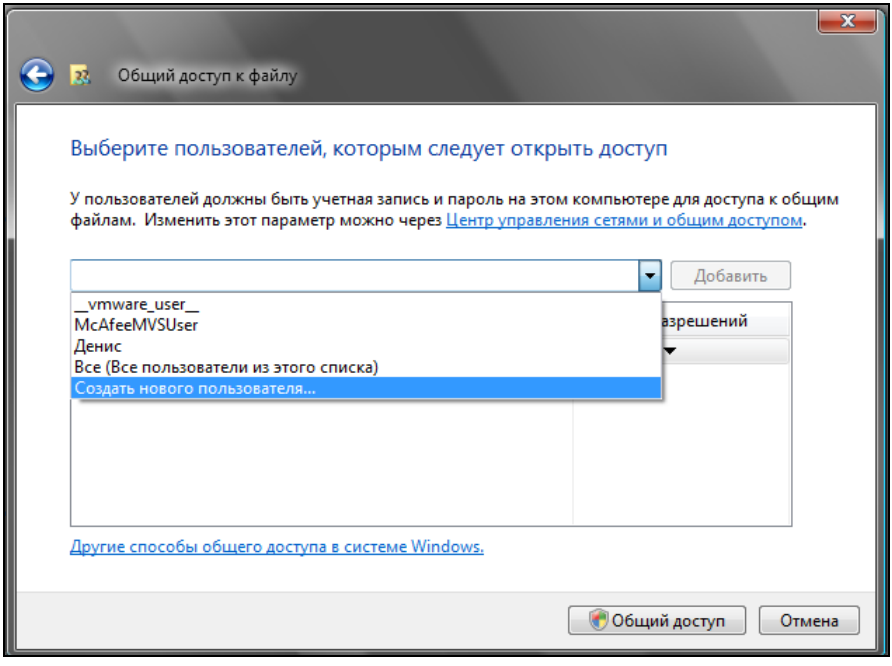


Рис. 11.27. Создать нового пользователя можно при предоставлении общего доступа к папке

Создавая нового пользователя, имейте в виду уровень разрешений, который вы ему предоставляете (рис. 11.28):

- **Читатель** — может только просматривать файлы;
- **Соавтор** — может просматривать файлы, добавлять новые файлы, а также изменять и удалять добавленные им файлы;
- **Совладелец** — может читать, редактировать, добавлять и удалять любые файлы.

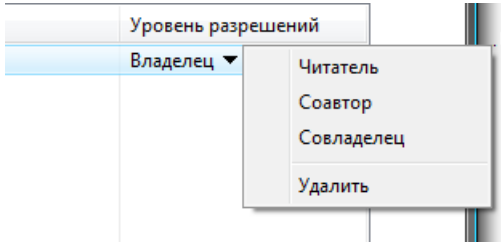


Рис. 11.28. Уровень разрешений

Примечание

Обратите внимание, что в списке уровней разрешений (см. рис. 11.28) помимо всего прочего имеется команда **Удалить**. Она используется для удаления пользователя из списка.

После добавления пользователя, имеющего право доступа к папке, система сообщит, что папка открыта для общего доступа (рис. 11.29). На рис. 11.30 изображен доступ к моему компьютеру с другого компьютера сети.

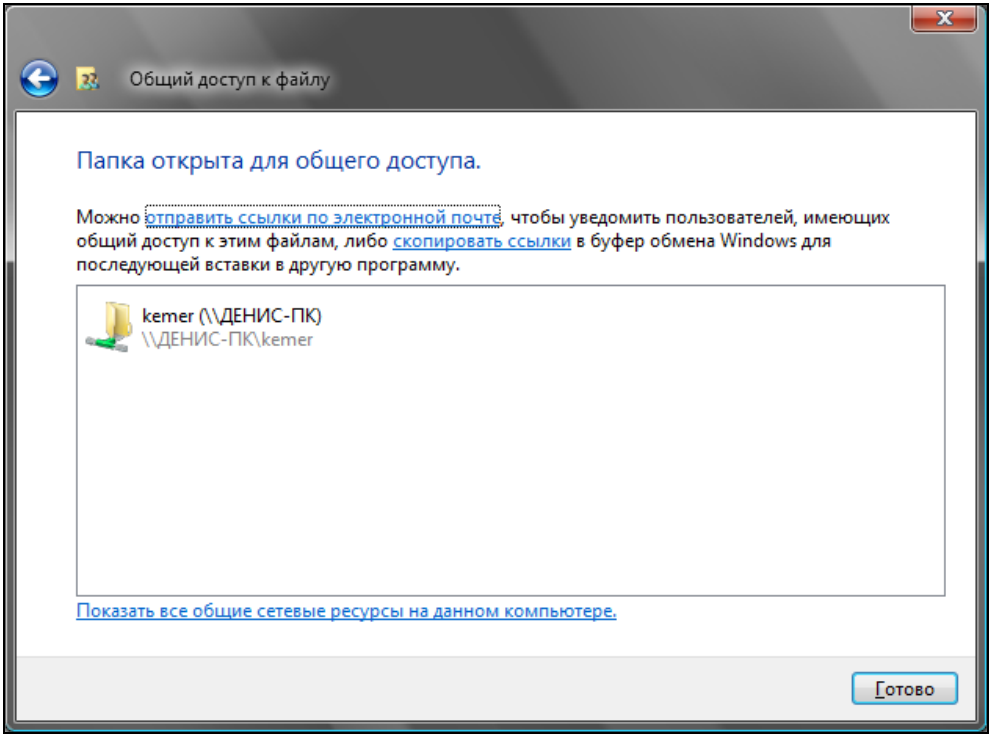


Рис. 11.29. Папка открыта для общего доступа

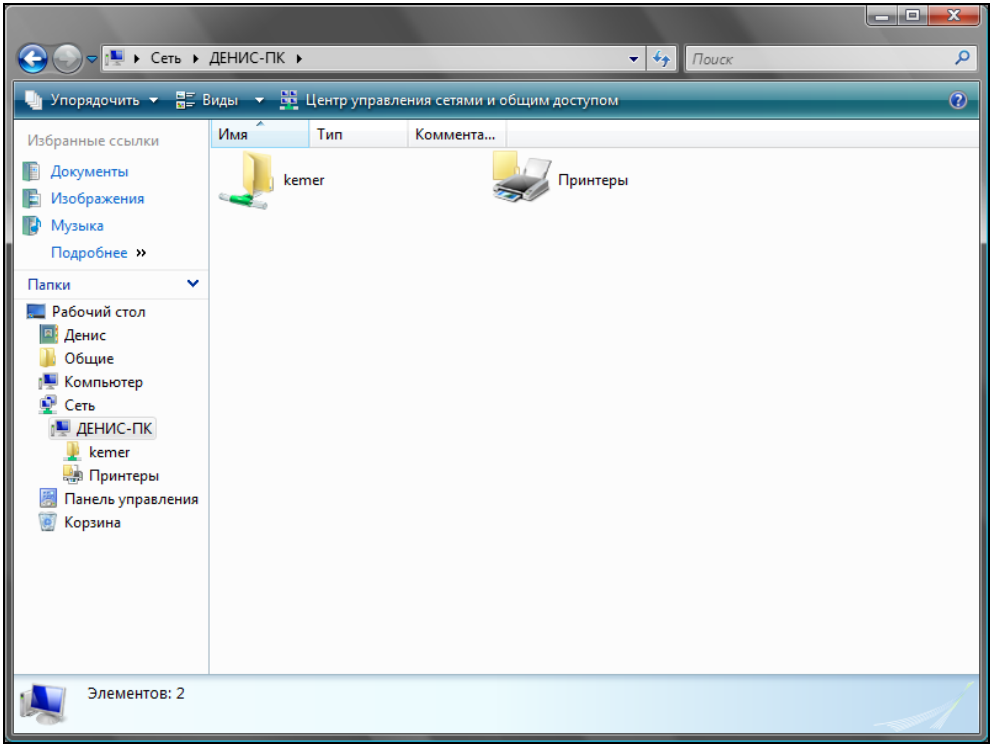


Рис. 11.30. Доступ к компьютеру по сети

11.5. Общий доступ к папкам в Linux

Как уже было отмечено ранее, чтобы Linux-машина смогла получить доступ к сети Microsoft, на ней должен быть установлен пакет samba. После этого можно "прописать" все общие ресурсы в файле /etc/samba/smb.conf. Конечно, этот способ не очень удобен для некоторых пользователей, привыкших к графическому интерфейсу, но зато он самый универсальный.

Рассмотрим описание в файле /etc/samba/smb.conf общего ресурса video. Это наш каталог /mnt/video, к которому разрешен публичный доступ (`public = yes` и `guest ok = yes`) и в который запрещена запись (`writable = no`):

```
[video]
path = /mnt/video
public = yes
guest ok = yes
writable = no
printable = no
```

Подробно об описании общих ресурсов вы узнаете в документации по пакету Samba (она устанавливается вместе с самим пакетом). К счастью, во многих дистрибутивах можно щелкнуть на папке правой кнопкой мыши и выбрать команду **Общий доступ**, после чего откроется окно, позволяющее опубликовать папку в сети, то есть предоставить к ней общий доступ другим пользователям сети (рис. 11.31). Вам нужно включить параметр **Опубликовать эту папку**, ввести имя ресурса, а затем отметить (если нужно) параметры:

- **Разрешать другим пользователям изменять содержимое папки** — к папке будет предоставлен полный доступ;
- **Гостевой доступ** — будет разрешен доступ пользователям, для которых вы не создали учетную запись.

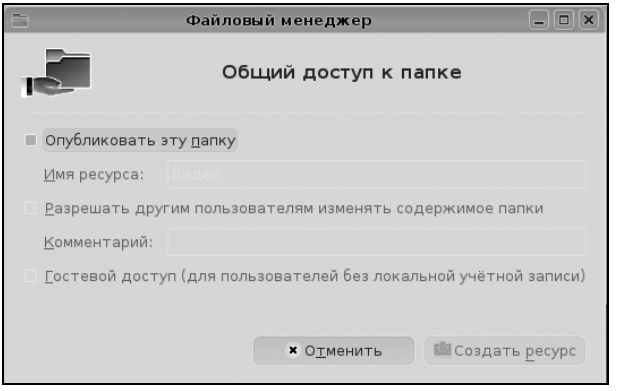


Рис. 11.31. Предоставление общего доступа к папке в Linux

При этом для других Windows-машин наша Linux-машина будет выглядеть обычной рабочей станцией сети Microsoft — они даже не заметят "подмену". О том, как предоставить общий доступ с паролем (как мы это делали в Windows), вы узнаете в документации по Samba.

Отобразить список доступных Windows-сетей можно с помощью команды меню **Переход | Сеть**, хотя команда меню зависит от дистрибутива (в вашем дистрибутиве может быть другая команда для отображения списка сетей).

11.6. А нужен ли общий доступ к ресурсам в сети Microsoft?

Самое интересное, что настройка общего доступа к ресурсам не очень простое занятие даже в Windows. А если на компьютерах вашей сети стоят разные версии Windows (что в большинстве случаев так и есть), то настройка

усложняется из-за небольших нестыковок этих версий: то пароль почему-то не подходит, то вы забыли создать дополнительного пользователя, то что-то не понравилось брандмауэру. Все эти ситуации — не мои домыслы, а практика. Предположим, в вашей сети есть несколько компьютеров, купленных 2–3 года назад. Скорее всего, на них будет установлена или Windows XP, или Windows XP SP2. На компьютерах, купленных год назад, будет установлена Windows Vista (у которой тоже есть несколько версий: Basic, Home и т. д.), на совсем старенькой машине может быть установлена Windows 98 или Windows 2000. Плюс ко всему этому еще и компьютеры, работающие под управлением Linux. Парк получается довольно разношерстный... Даже если вы и настроите всю эту сеть, то потратите достаточно много времени на борьбу с брандмауэрами, пользователями и их правами. В итоге получите потенциально "дырявую" службу.

Спрашивается, а зачем вам нужен общий доступ к ресурсам в сети Microsoft? Большая часть пользователей использует ее для организации совместного доступа к файлам. Например, есть у вас большой раздел с фильмами на одном из компьютеров, вы можете сделать его общим, и тогда остальные пользователи сети смогут посмотреть записанные фильмы. Таким образом, все упирается в совместный доступ к файлам. Мне не нужен совместный доступ к принтеру, поэтому вместо общих сетевых ресурсов я настроил FTP-сервер (FTP, File Transfer Protocol). Здесь полный простор для творчества:

- можно сделать публичный каталог, к которому получат доступ все пользователи сети. Например, каталог с фильмами;
- можно сделать каталог-обменник, куда все пользователи сети смогут закачивать файлы;
- можно предоставить персональный доступ к серверу каждому пользователю сети — на сервере будет домашний каталог для каждого пользователя, где пользователь сможет хранить свои данные.

Преимущества очевидны! В нашей сети появится центральный сервер. Да, он не заменит контроллер домена, но обеспечит дополнительные удобства:

- вам не придется создавать учетные записи пользователей на каждом компьютере — достаточно создать их на сервере;
- в сети Microsoft, если выключен компьютер, предоставляющий ресурс, вам нужно его включить, иначе доступ к ресурсу будет невозможен. В случае с центральным FTP-сервером, развернутым на шлюзе (шлюз предоставляет доступ к Интернету, поэтому он будет включен всегда), эта проблема исчезает;
- более гибкое управление правами пользователей;

- используя персональные каталоги пользователей, можно обеспечить функциональность, подобную перемещению профилей пользователей в сети Microsoft. Пользователь может хранить свои документы на FTP-сервере. Если он перейдет на другой компьютер, то легко сможет получить доступ к своим файлам, хранящимся на FTP-сервере;
- снимается ограничение на максимальное число одновременно использующих ресурс пользователей. Напомню, что в Windows XP/Vista одновременно работать с общим ресурсом могут максимум 10 пользователей. В случае с FTP-сервером количество пользователей не ограничено — лишь бы у сервера хватило оперативной памяти!

> ***Примечание***
>
> Если вы все-таки решили использовать сеть Microsoft, снять ограничение на максимальное число клиентов можно программой SwitchNT. Вы найдете ее в Интернете. Однако помните, что использование этой программы нарушает лицензионное соглашение с Microsoft!

О том, как настроить собственный FTP-сервер в Linux, вы сможете прочитать в моей книге "Серверное применение Linux, 2-е изд." ("БХВ-Петербург", 2009, **http://www.bhv.ru/books/book.php?id=184941**). Настроить FTP-сервер в Windows можно с помощью программы FileZilla Server, скачать которую можно по адресу: **http://filezilla-project.org/download.php?type=server**. Документация на русском языке по этой программе доступна на сайте: **http://help.vth.ru/FileZilla_Server**.

Вообще, если есть желание, можно сэкономить немного денег, настроив первичный контроллер домена сети Microsoft под управлением Windows. О том, как это сделать, написано здесь: **http://www.dkws.org.ua/phpbb2/viewtopic.php?t=3838**.

Глава 12

Совместное подключение к Интернету

12.1. Небольшая домашняя сеть с выходом в Интернет

12.1.1. Основы маршрутизации

У вас дома (или в офисе) есть несколько компьютеров. Один из них подключен к Интернету, но вы хотите, чтобы все члены вашей семьи (или ваши коллеги) могли подключаться к Интернету со своих компьютеров. Согласитесь, не очень удобно работать, когда над головой стоят несколько человек и просят что-то поискать в Интернете, скачать песню или посмотреть прогноз погоды.

В этой главе мы подключим вашу проводную сеть к Интернету. Для доступа к Интернету нам необходим маршрутизатор (router) или шлюз. Сейчас термины "маршрутизатор" и "шлюз" означают практически одно и то же — устройство, предоставляющее доступ к другой сети путем маршрутизации пакетов. Но между маршрутизатором и шлюзом на самом деле есть небольшая разница. *Маршрутизатор* связывает две однотипные сети (например, две локальные сети), а *шлюз* — две сети разного типа (например, локальную и глобальную). Но еще раз замечу: сейчас, говоря "маршрутизатор" или "шлюз", имеют в виду одно и то же устройство.

У маршрутизатора будет всегда два (или больше) сетевых интерфейса. Один сетевой интерфейс маршрутизатор использует для связи с локальной сетью. А второй — для связи с Интернетом (ну, или любой другой сетью, но сейчас мы будем подразумевать, что эта вторая сеть — Интернет). При этом маршрутизатор подключается к коммутатору как любой другой узел сети (рис. 12.1).

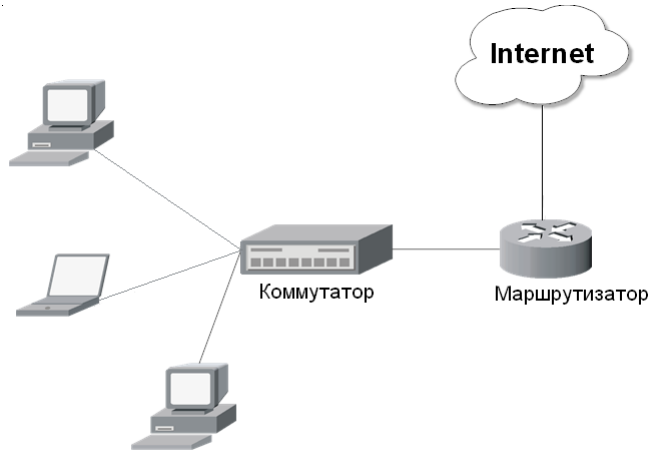


Рис. 12.1. План небольшой сети

Маршрутизация осуществляется следующим образом. Представим, что у нас есть "древняя" сеть, администратор которой понятия не имеет о DHCP-сервере (то есть все сетевые параметры на узлах сети устанавливаются вручную). Администратор установил для всех компьютеров IP-адреса в диапазоне от 192.168.1.2 до 192.168.1.5. Адрес маршрутизатора: 192.168.1.1. Этот адрес и устанавливается в качестве адреса шлюза по умолчанию.

Когда компьютер 192.168.1.2 отправляет данные компьютеру 192.168.1.3, то коммутатор знает, к какому порту подключен компьютер 192.168.1.3, и передает ему эти данные. Но что будет, если компьютеру 192.168.1.2 нужно передать данные компьютеру, находящемуся в другой сети, — скажем, компьютеру с адресом 10.1.1.11? В этом случае пакеты, исходящие от компьютера 192.168.1.2, будут направлены по маршруту по умолчанию, то есть нашему маршрутизатору. Далее вступает в действие маршрутизатор. Если в его настройках "прописан" маршрут к сети 10.1.1.0, то он отправляет пакет в эту сеть по одному из своих интерфейсов. Компьютер 10.1.1.11, получив пакет, отправляет ответ ("данные получены") компьютеру 192.168.1.2. Ответ опять проходит через маршрутизатор, который на этот раз отправляет его в сеть 192.168.1.0.

Как видите, маршрутизатор содержит таблицу маршрутизации, в которой, как минимум, записаны сведения о сети назначения и о сетевом интерфейсе, через который нужно отправлять пакеты в эту сеть. Раньше таблица маршрутизации редактировалась вручную администратором. И от того, как правиль-

но администратор заполнял эту таблицу, зависело, как работала сеть. Сейчас же таблица маршрутизации формируется динамически.

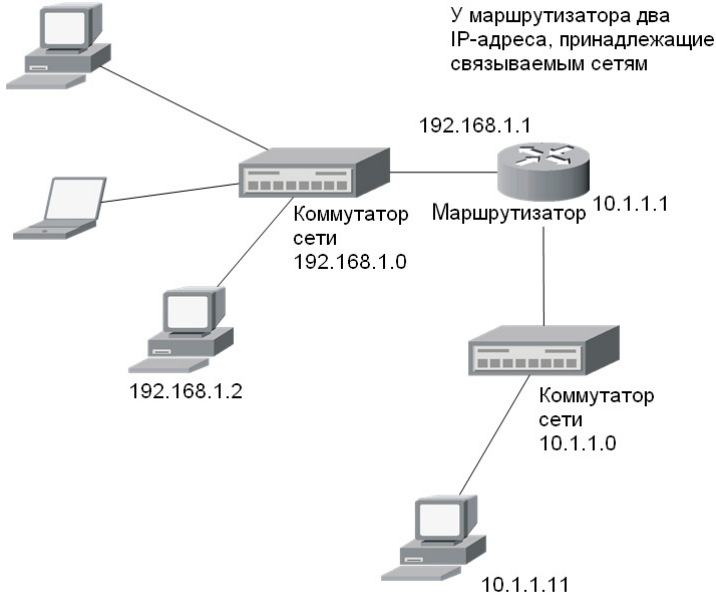


Рис. 12.2. Схема маршрутизации между двумя сетями

12.1.2. Преобразование сетевых адресов (NAT)

А теперь снова посмотрим на рис. 12.1. На нем изображена небольшая сеть с доступом к Интернету. Допустим, узел локальной сети отправляет данные узлу Интернета — например, по адресу 194.67.57.226 (это IP-адрес сайта **www.mail.ru**). Задача маршрутизатора усложняется — он должен выполнить *преобразование сетевых адресов* (NAT, Network Address Translation), иначе даже если он отправит узлу 194.67.57.226 пакет с локальным IP-адресом (например, 192.168.1.2), то любой маршрутизатор, находящийся на пути между нашей локальной сетью и сетью узла-назначения, удалит такой пакет.

Мы уже вкратце рассматривали NAT *(см. разд. 3.4)*, давайте разберемся с этой функцией подробнее. Предположим, у нас есть шлюз и локальная сеть с адресами 192.168.*.*. Реальный IP-адрес (который можно использовать в Интернете) есть только у шлюза, пусть это 193.254.219.1. У всех остальных

компьютеров — локальные адреса, поэтому при всем своем желании они не могут обратиться к интернет-узлам.

У нашего шлюза два сетевых интерфейса. Один из них (пусть к нему подключен ADSL-модем) используется для подключения к Интернету. Его IP-адрес, как уже было сказано, 93.254.219.1. Для подключения к локальной сети используется другой сетевой интерфейс (это сетевая плата) с IP-адресом 192.168.1.1.

Все узлы нашей локальной сети используют в качестве шлюза компьютер с адресом 192.168.1.1. Это означает, что все запросы будут переданы на узел 192.168.1.1. Запросы передаются в виде:

```
Назначение: IP-адрес узла Интернета
Источник: адрес компьютера локальной сети, пусть 192.168.1.10
```

Наш шлюз принимает запрос и перезаписывает его так:

```
Назначение: IP-адрес узла Интернета
Источник: 193.254.219.1
```

Таким образом шлюз подменяет адрес источника, устанавливая в качестве этого адреса свой реальный IP-адрес, поскольку ни один интернет-узел не примет запрос с локального адреса. Получив ответ от узла, он направляет его нашему узлу:

```
Назначение: 192.168.1.10
Источник: IP-адрес узла Интернета
```

Нашему локальному узлу "кажется", что он получил ответ непосредственно от узла Интернета, а на самом деле ответ приходит от шлюза.

Теперь, когда мы разобрались с основами маршрутизации, можно приступить к выбору самого маршрутизатора.

12.2. Аппаратный или программный маршрутизатор?

Маршрутизаторы бывают аппаратными и программными. *Аппаратный* маршрутизатор — это отдельное устройство с несколькими (обычно двумя, хотя у промышленных маршрутизаторов для крупных сетей может быть большее число интерфейсов) сетевыми интерфейсами. *Программный* маршрутизатор — это компьютер с несколькими сетевыми интерфейсами (например, двумя сетевыми платами или модемом и сетевой платой) и соответствующим программным обеспечением — брандмауэром, разрешающим общий доступ к соединению с Интернетом другим компьютерам сети. В программный

маршрутизатор можно превратить практически любой компьютер под управлением Windows XP, Vista или Linux.

Собственно, теперь вы находитесь перед выбором: или немного потратиться и купить аппаратный маршрутизатор, или использовать то, что есть, — обычный компьютер. Во втором случае можно сэкономить деньги: стоимость маршрутизатора во многом зависит от выполняемых им функций. Для дома можно найти недорогой маршрутизатор ценой в несколько тысяч рублей, а вот в крупных сетях используются маршрутизаторы стоимостью несколько тысяч долларов.

Если вы решили использовать в качестве маршрутизатора обычный компьютер, то помните, что для того, чтобы другие компьютеры смогли получить доступ к Интернету, компьютер-маршрутизатор должен быть постоянно включен. А это не всегда удобно, поскольку работающий компьютер создает шум, а аппаратный маршрутизатор бесшумен.

Выбирать — вам: или экономия, или комфорт. Скорее всего, домашние пользователи выберут более экономный вариант. А в офисе лучше использовать аппаратный маршрутизатор. Вы только представьте, что будет, если компьютер-маршрутизатор сломается? Правильно, все минимум на несколько часов останутся без Интернета, что неприемлемо для современной фирмы.

> ***Совет***
>
> О выборе оборудования нужно думать на этапе планирования сети, о чем неоднократно упоминалось в этой книге.

Для небольших офисных сетей выпускаются очень интересные комбинированные устройства. Конкретных моделей приводить не стану, поскольку модельный ряд постоянно обновляется, но в каталоге любого производителя сетевого оборудования (3Com, ZyXEL, Linksys, D-Link и др.) вы найдете модели, по своим функциям напоминающие описанные здесь.

Существуют модели, сочетающие в себе функции коммутатора и ADSL-модема. Правда, количество портов на таких комбинированных устройствах ограничено (4–8 портов), но для малых сетей этого будет вполне достаточно. А есть устройства, сочетающие в себе и маршрутизатор, и точку беспроводного доступа, и коммутатор. Очень удобно — вам нужно добавить только ADSL-модем, и ваша сеть подключена к Интернету. Причем такие устройства практически не нужно настраивать (надо выполнить только базовую настройку), поэтому установка сети не займет много времени.

Набор возможностей современных маршрутизаторов обычно включает и функцию *брандмауэра* (firewall) — межсетевого экрана, выполняющего фильтрацию пакетов. Брандмауэр используется для защиты вашей сети

от вторжения извне (например, от пользователей Интернета, которые хотят обратиться к ресурсам вашей локальной сети). Настройка такого комбинированного маршрутизатора зависит от конкретной модели, но я в нескольких словах опишу ее основные этапы:

1. Подключите маршрутизатор к сети питания.
2. Подключите к нему другие компьютеры. Если у вашего маршрутизатора нет портов для подключения компьютера (то есть это сугубо маршрутизатор без функции коммутатора), то включите коммутатор, подключите к нему маршрутизатор и все компьютеры сети.

   Примечание

   У всех современных маршрутизаторов по умолчанию активна функция DHCP — то есть все компьютеры будут настроены автоматически по протоколу DHCP, и вам не нужно будет изменять параметры каждого компьютера сети.

3. Откройте браузер и обратитесь к маршрутизатору. Обычно его URL будет выглядеть так: `http://IP-адрес:порт`. IP-адрес и порт вы сможете узнать в руководстве по маршрутизатору.
4. В открывшейся панели управления маршрутизатором следует ввести имя пользователя и пароль, указанные в руководстве.
5. Прежде всего, измените пароль администратора (в панели управления для этого будут команды типа **Change password** или **Set password**).
6. Теперь можно приступить к настройке сети:
   - укажите желаемый IP-адрес сети (впрочем, это не обязательно, поскольку маршрутизатор автоматически настраивает все компьютеры сети, и нет никакой разницы, какие IP-адреса он им назначит);
   - укажите имя пользователя и пароль для ADSL-доступа к Интернету (имя пользователя и пароль можно посмотреть в договоре с вашим интернет-провайдером).

     Примечание

     Особое внимание нужно уделить маршрутизаторам с функциями ADSL-модема. У многих провайдеров установлена привязка конкретного пользователя к MAC-адресу его модема. Если вы заменяете свой ADSL-модем на маршрутизатор с функциями ADSL-модема, вам нужно сообщить его MAC-адрес своему провайдеру, иначе доступ к Интернету будет заблокирован.

Далее мы займемся настройкой программного маршрутизатора в операционных системах Windows XP, Vista и Linux.

12.3. Настройка совместного доступа к Интернету

12.3.1. Установка дополнительного сетевого адаптера

При настройке общего доступа мы будем считать, что у вас есть, как минимум, два соединения: соединение по локальной сети и соединение, которое используется для подключения к Интернету (например, модемное соединение). В случае с ADSL у вас должно быть два сетевых адаптера: к одному будет подключаться ADSL-модем, а второй будет использоваться для подключения к локальной сети. Схема сети у нас будет такой, как показано на рис. 12.3.

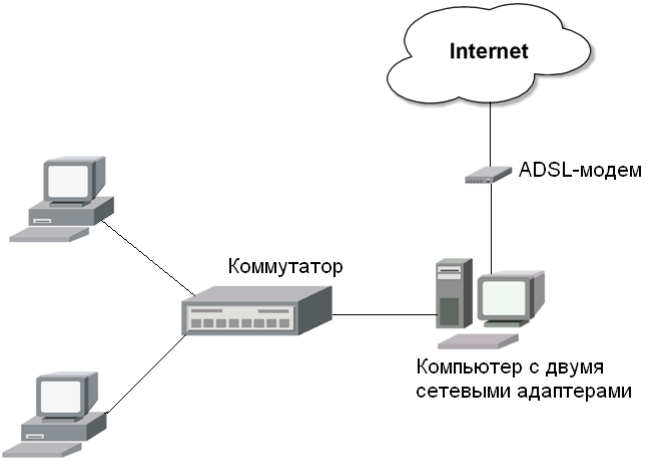


Рис. 12.3. Схема небольшой домашней сети

Перед установкой дополнительного сетевого адаптера отключите питание компьютера (отсоедините кабель питания от сети питания!), откройте крышку системного блока, удалите фальш-панель напротив свободного PCI-слота и установите сетевой адаптер в свободный слот (рис. 12.4).

Убедитесь, что надежно закрепили сетевой адаптер, соберите корпус и включите питание компьютера. Windows обнаружит новый сетевой адаптер (рис. 12.5) и попросит установить для него драйвер (рис. 12.6).

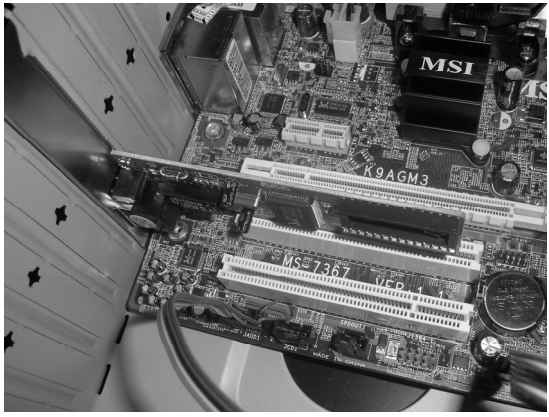


Рис. 12.4. Установленный сетевой адаптер

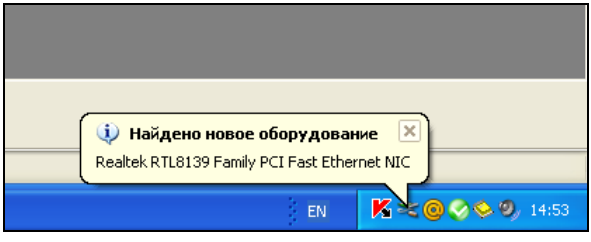


Рис. 12.5. Windows нашла сетевой адаптер

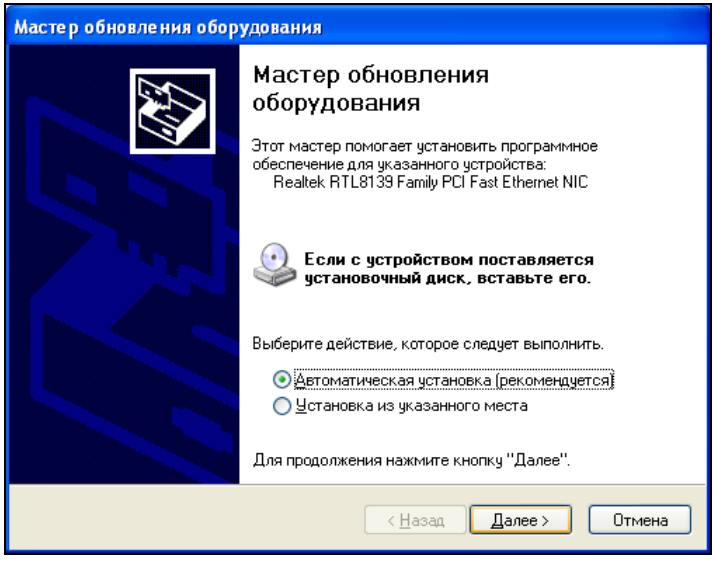


Рис. 12.6. Нужно установить драйвер

Примечание

Иллюстрации 12.5 и 12.6 сделаны в Windows XP. В Windows Vista окна будут выглядеть примерно так же.

Вставьте в дисковод CD/DVD прилагаемый к сетевому адаптеру установочный диск, и Windows сама выполнит все необходимые процедуры по установке драйвера.

Linux не запрашивает драйвер — она его устанавливает по умолчанию (драйверы для большинства сетевых адаптеров входят в состав Linux, поэтому ситуация отсутствия драйвера практически исключена). Чтобы убедиться, что Linux нашла вторую сетевую плату, откройте терминал (обычно для этого используется команда меню **Приложения | Стандартные | Терминал**) и введите команду `ifconfig`. На рис. 12.7 показано, что Linux нашла две сетевые платы: eth0 и eth1. Значит, можно продолжать настройку дальше.

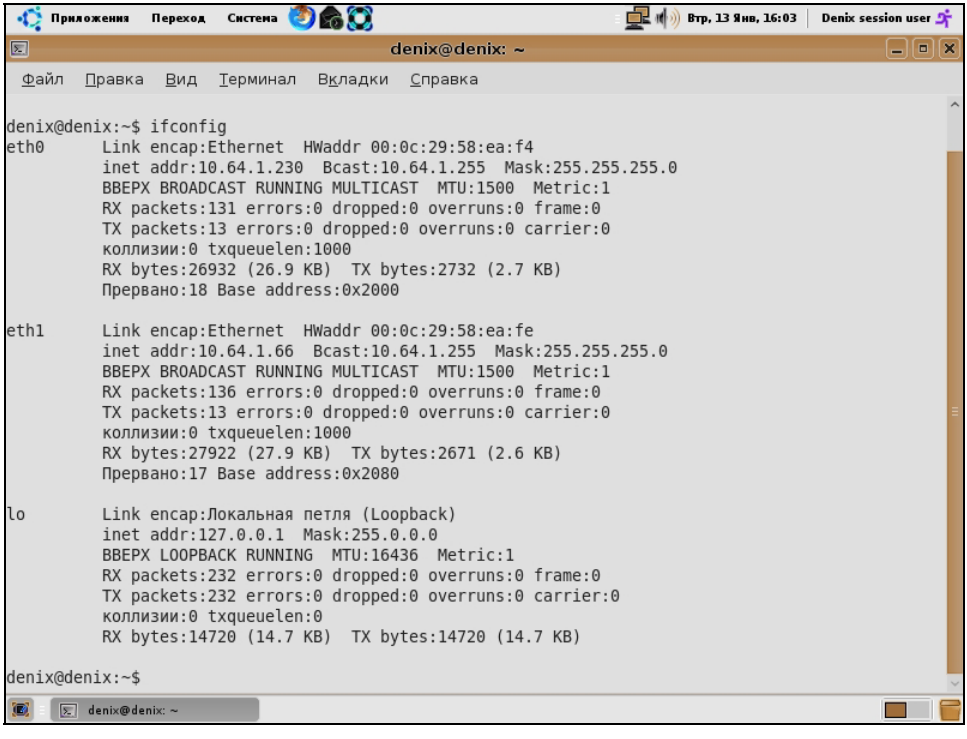


Рис. 12.7. Linux определила два сетевых адаптера

Скорее всего, к одному сетевому адаптеру у вас уже подключен Ethernet-кабель, ведущий к ADSL-модему. Второй сетевой адаптер будет использо-

ваться для подключения этого компьютера к коммутатору, поэтому не забудьте подключить и его! Вот теперь можно приступить к дальнейшей настройке.

12.3.2. Работаем в Windows XP

Откройте окно **Сетевые подключения** (**Пуск | Настройка | Сетевые подключения**). Выберите команду **Установить домашнюю сеть или сеть малого офиса** (рис. 12.8).

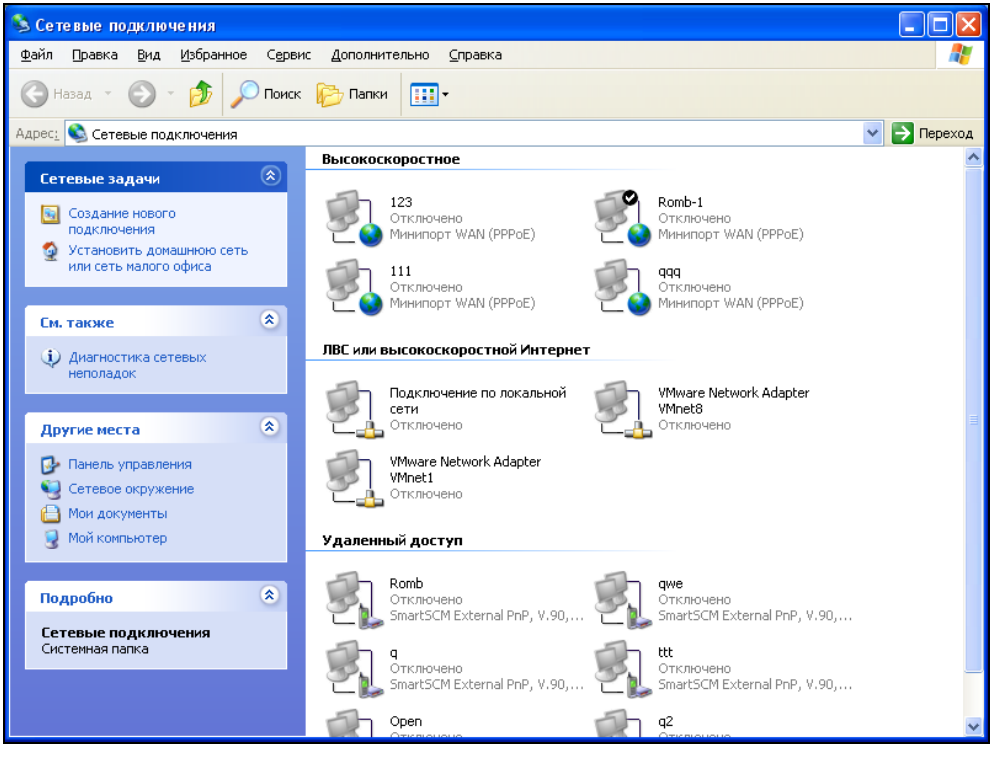


Рис. 12.8. Окно **Сетевые подключения**

Примечание

Если на компьютере установлен брандмауэр, то его нужно отключить перед настройкой общего соединения с Интернетом, а после настройки — включить. Возможно, придется изменить параметры брандмауэра. При настройке своей домашней сети я поступил очень просто: установил брандмауэр, когда уже общее соединение было настроено.

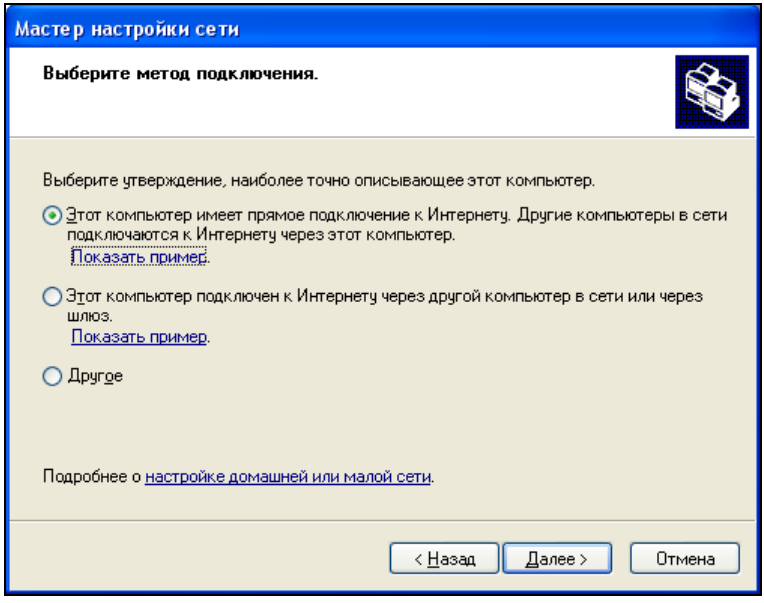


Рис. 12.9. Роль компьютера

Вы увидите окно мастера настройки сети. Два раза нажимаем кнопку **Далее**, затем мастер предложит вам выбрать роль данного компьютера (рис. 12.9). Следует выбрать переключатель **Этот компьютер имеет прямое подключение к Интернету. Другие компьютеры в сети подключаются к Интернету через этот компьютер**.

Затем нужно выбрать соединение, которое используется для подключения к Интернету (рис. 12.10).

Если у вас несколько локальных сетевых соединений (например, в случае использования ADSL-модема), Windows спросит вас (рис. 12.11), хотите ли вы сами указать соединение, которое будет использоваться для связи с компьютерами локальной сети, или предоставите выбор системе. Windows достаточно умна, чтобы распознать кто есть кто, поэтому можете выбрать автоматическую настройку, впрочем, можно выбрать соединение и вручную (рис. 12.12).

Следующие два вопроса мастера настройки сети очень просты: нужно ввести имя своего компьютера и его описание (что, скорее всего, вы сделали при установке системы), а также ввести имя рабочей группы (по умолчанию MSHOME, можете его не изменять). Затем мастер предложит проверить указанные вами параметры — если все правильно, нажмите кнопку **Далее** — начнется настройка сети, после которой потребуется перезагрузить компьютер.

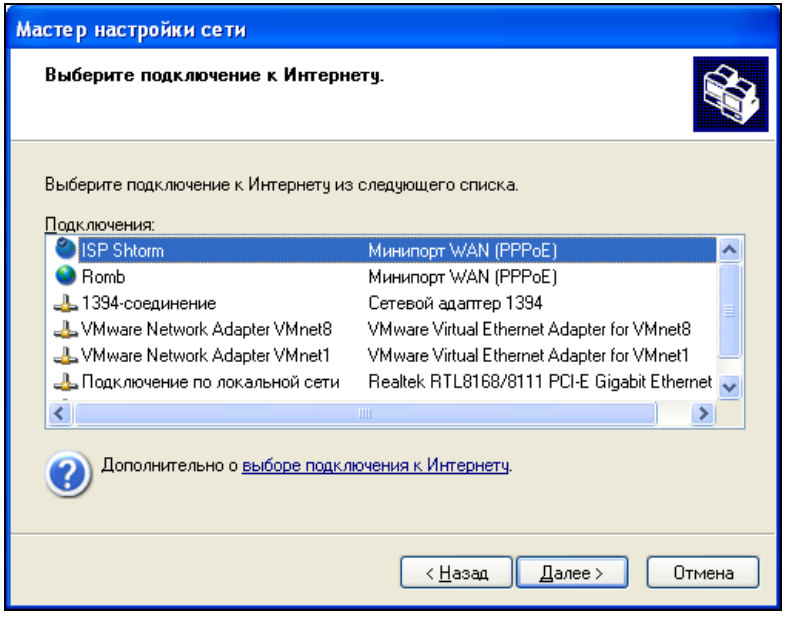


Рис. 12.10. Выбор соединения для подключения к Интернету

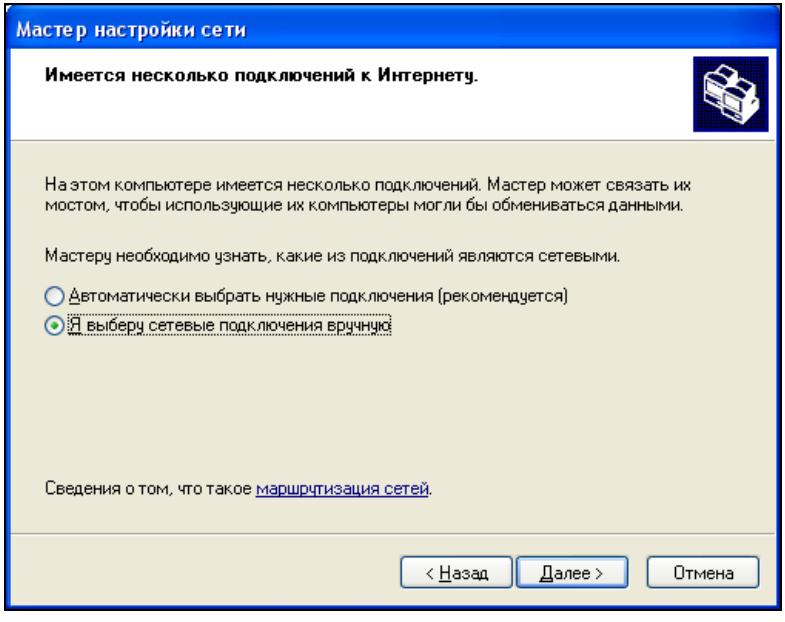


Рис. 12.11. Выбор локального соединения

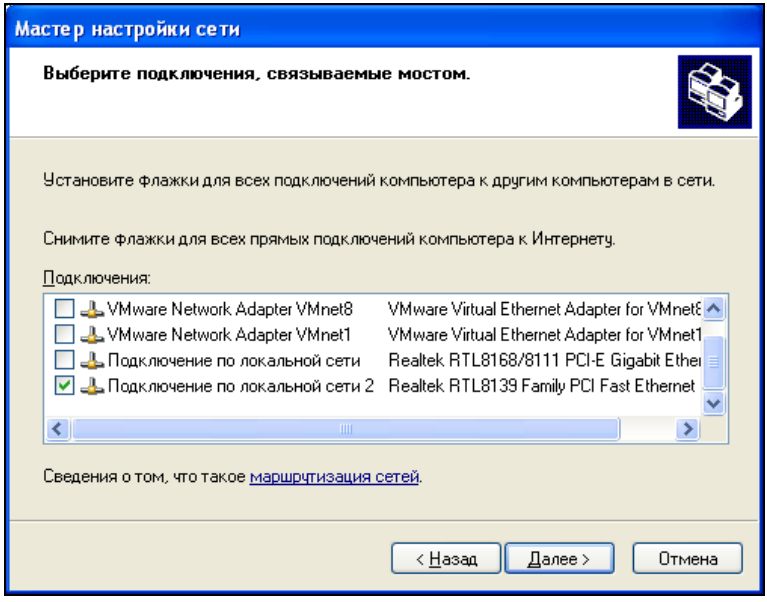


Рис. 12.12. Список соединений

Настройка главного компьютера завершена. Теперь можно приступить к настройке остальных компьютеров сети.

Для *каждого* компьютера локальной сети (кроме главного) нужно установить *одинаковые параметры соединения по локальной сети* следующим образом:

1. Откройте окно **Сетевые подключения**.
2. Щелкните правой кнопкой мыши по локальному соединению и выберите команду **Свойства**.
3. В окне **Подключение по локальной сети – свойства** (рис. 12.13) выберите **Протокол Интернета TCP/IP** и нажмите кнопку **Свойства**.
4. На вкладке **Общие** (рис. 12.14) установите переключатель **Получить IP-адрес автоматически**.
5. Позвоните в службу технической поддержки провайдера и узнайте IP-адреса серверов DNS (их можно также узнать из вашего с ним договора на предоставление услуги доступа в Интернет).
6. Установите параметр **Использовать следующие адреса DNS-серверов** и введите IP-адреса, которые вы только что узнали. Дело в том, что Windows не всегда правильно определяет адреса DNS-серверов, поэтому лучше сразу установить их вручную.

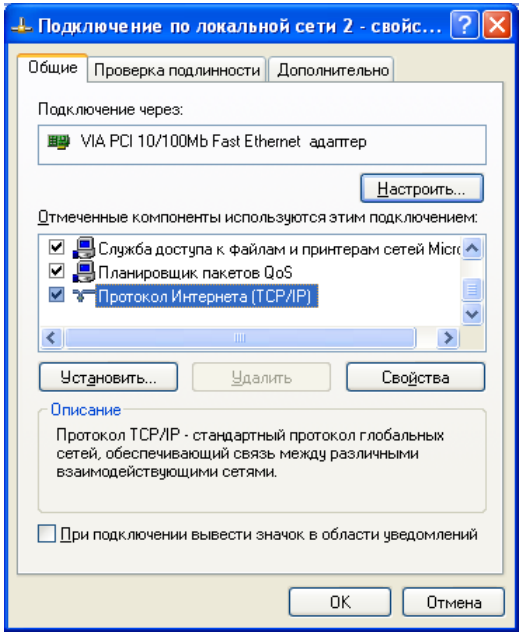


Рис. 12.13. Свойства соединения по локальной сети

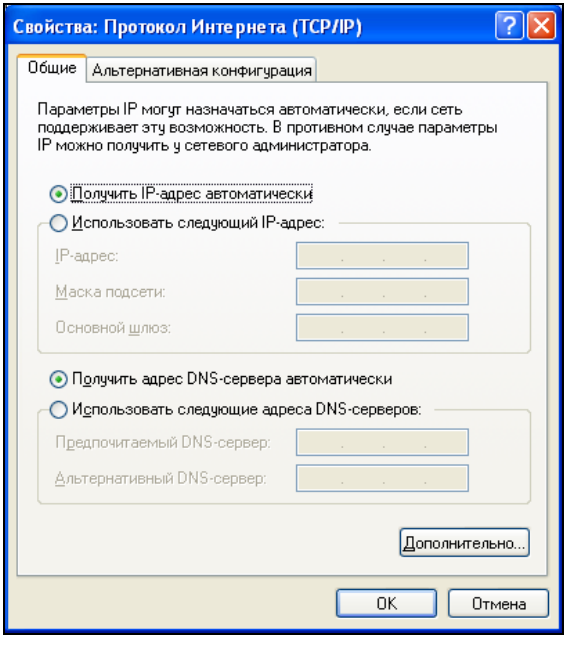


Рис. 12.14. Свойства протокола Интернета

Примечание

Впрочем, можно попробовать оставить опцию **Получить адрес DNS-сервера автоматически** включенной. А вот если начнутся проблемы, то тогда уже заняться поиском и назначением адресов DNS-серверов вручную.

7. Перезагрузите компьютер.
8. Повторите пункты 1–7 для каждого компьютера сети (кроме главного).

После перезагрузки, если все настроено правильно и основное соединение, используемое для подключения к Интернету, запущено, все "второстепенные" настроенные компьютеры локальной сети смогут получить доступ к Интернету.

Примечание

С технической точки зрения на главном компьютере нами были развернуты DHCP-сервер и шлюз. Первый осуществляет автоматическую настройку компьютеров локальной сети (присваивает им IP-адреса и устанавливает другие сетевые параметры), а второй — предоставляет доступ к Интернету.

12.3.3. Работаем в Windows Vista

Принцип действия средства общего доступа к Интернету в Windows Vista такой же, как и в Windows XP, но процесс настройки немного отличается. Откройте Панель управления (рис. 12.15) и запустите **Центр управления сетями и общим доступом**.

В окне центра управления сетями (рис. 12.16) выберите команду **Управление сетевыми подключениями**.

Выберите соединение (рис. 12.17), которое используется для подключения к Интернету (например, модемное), щелкните по нему правой кнопкой мыши и выберите команду **Свойства**.

В открывшемся окне (рис. 12.18) перейдите на вкладку **Доступ** (она будет недоступна, если у компьютера имеется только одно сетевое соединение). Включите параметр **Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера**. При необходимости можете установить следующие параметры:

- **Устанавливать телефонное подключение при попытке доступа к Интернету** — очень удобный параметр. Например, если пользователю вашей домашней сети понадобится Интернет, то ваш компьютер, если соединение разорвано, сам подключится к Интернету без вашего вмешательства. С другой стороны, вы не сможете контролировать время работы пользователей. Поэтому данный параметр нужно использовать, только если у вас неограниченный тарифный план;

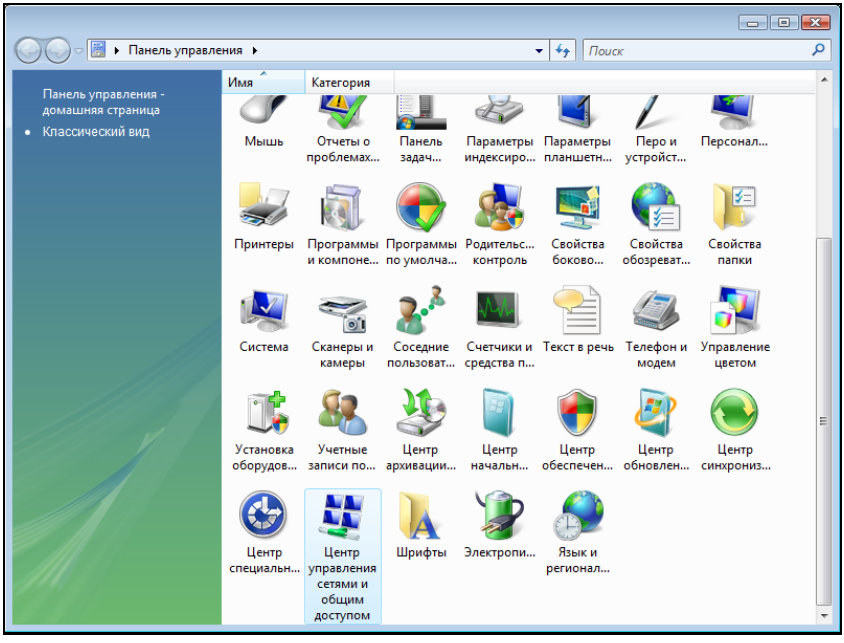


Рис. 12.15. Панель управления

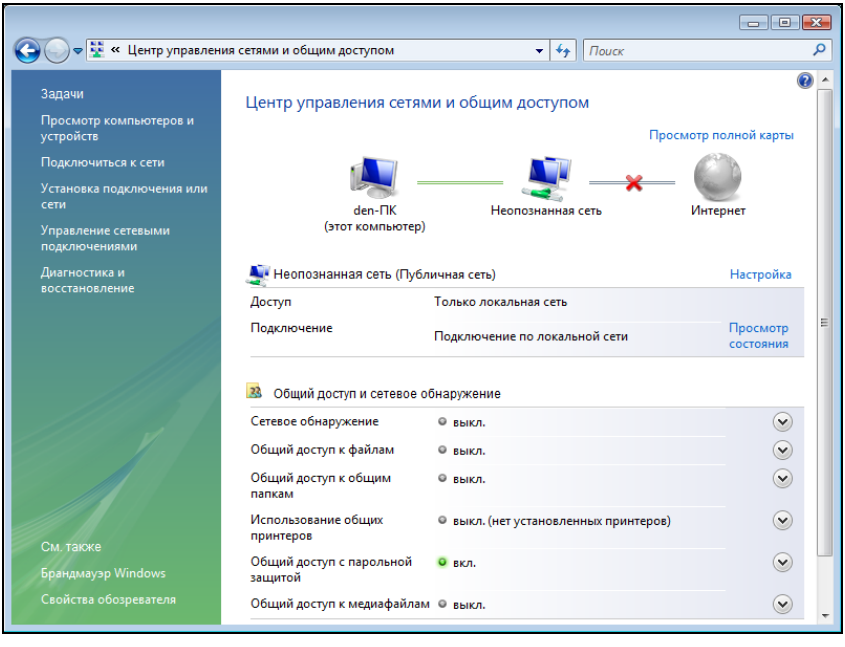


Рис. 12.16. Центр управления сетями и общим доступом

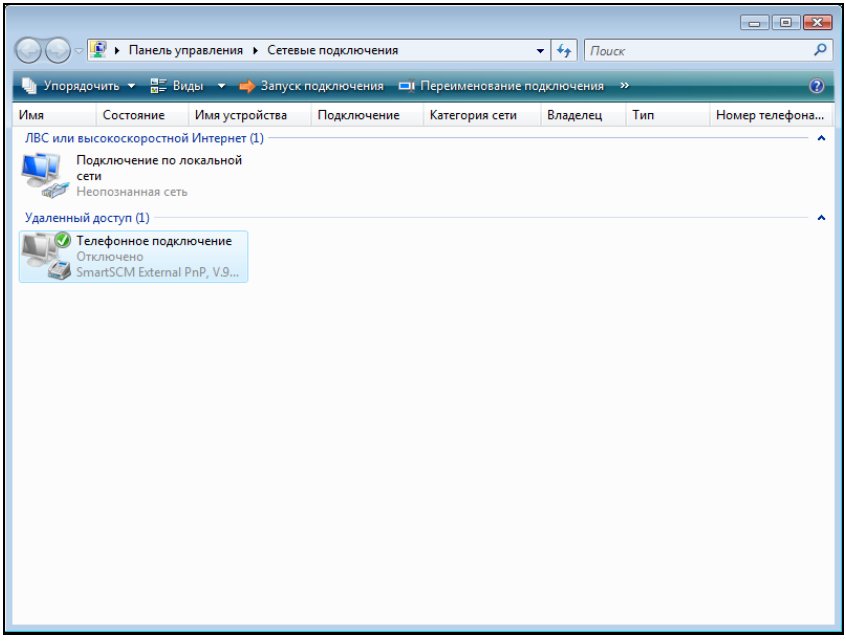


Рис. 12.17. Управление соединениями

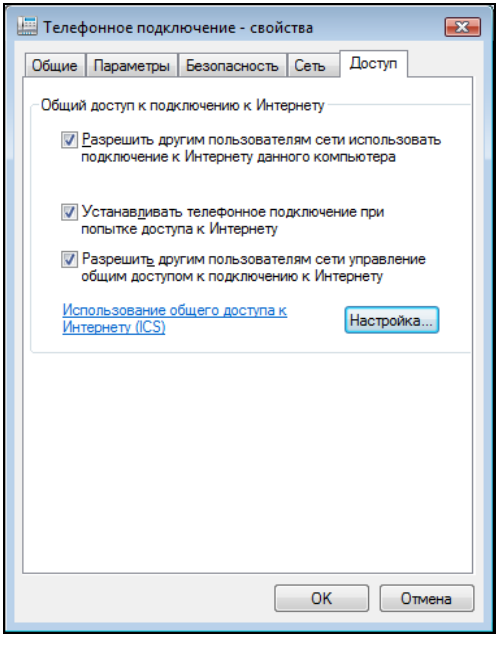


Рис. 12.18. Параметры общего доступа

- **Разрешить другим пользователям сети управление общим доступом к подключению к Интернету**. Этот параметр можно не устанавливать — зачем пользователям сети управлять сетевыми подключениями вашего компьютера? Хотя по умолчанию параметр включен.

Настройка главного компьютера завершена. Желательно перезагрузить компьютер для того, чтобы изменения вступили в силу.

Для *каждого* компьютера локальной сети (кроме главного) нужно установить *одинаковые параметры соединения по локальной сети* следующим образом:

1. Откройте центр управления сетями.
2. Выберите команду **Управление сетевыми подключениями**.
3. Щелкните на локальном соединении правой кнопкой мыши и выберите команду **Свойства**.
4. В открывшемся окне (рис. 12.19) выберите **Протокол Интернета версии 4** и нажмите кнопку **Свойства**.

> ***Примечание***
>
> Протокол Интернета версии 6 пока используется редко, поэтому можете смело отключить его в свойствах подключения по локальной сети.

5. На вкладке **Общие** (рис. 12.20) установите параметр **Получить IP-адрес автоматически**. Что же касается DNS-серверов, то, как и в случае с Windows XP, лучше ввести IP-адреса DNS-серверов явно.

> ***Примечание***
>
> На рис. 12.20 приведены вымышленные IP-адреса серверов DNS.

6. Перезагрузите компьютер.
7. Повторите пункты 1–6 для каждого компьютера сети (кроме главного).

На этом настройка домашней сети завершена. Не забудьте перезагрузить компьютеры.

> ***Совет***
>
> Можно обойтись и без перезагрузки — щелкните по локальному соединению правой кнопкой мыши и выберите команду **Отключить**. Подождите немного, затем опять щелкните по соединению правой кнопкой и выберите команду **Подключить**. Этим вы перезагрузите сетевое соединение и его параметры, что позволяет обойтись без перезагрузки компьютера.

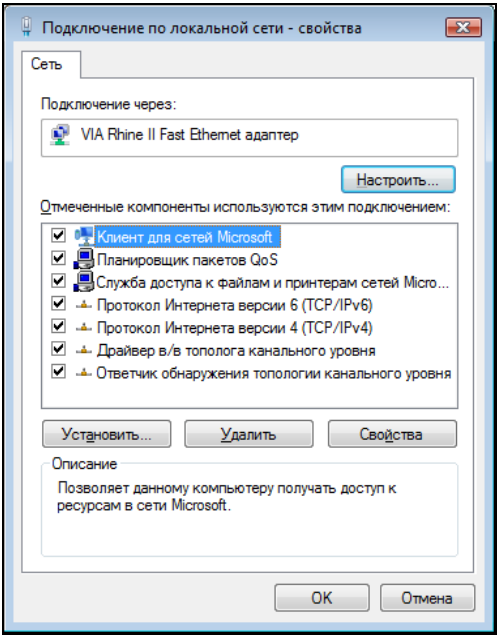


Рис. 12.19. Свойства подключения по локальной сети

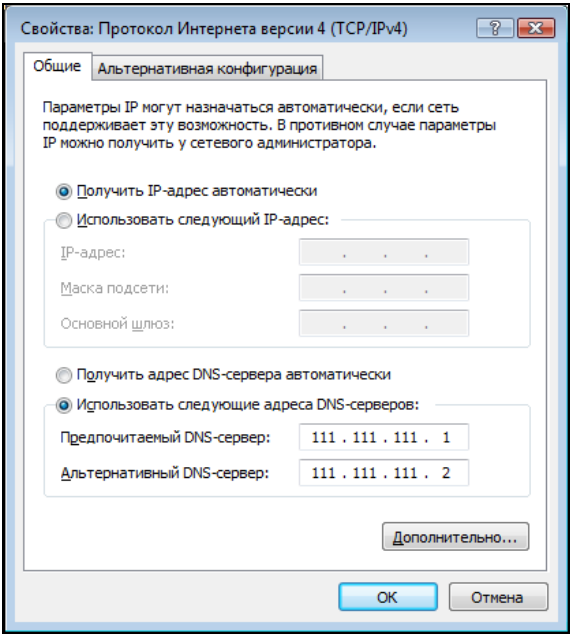


Рис. 12.20. Параметры TCP/IP

Часть IV

Построение беспроводной сети

Четвертая часть книги полностью посвящена построению беспроводной сети. Сначала мы рассмотрим преимущества и недостатки беспроводной сети, разберемся, как данные передаются "по воздуху", познакомимся с основными беспроводными стандартами, а потом перейдем непосредственно к практическому построению сети и решению проблем, возникающих при эксплуатации беспроводных сетей.

Глава 13

Введение в беспроводные сети

13.1. Преимущества и недостатки беспроводной сети

Итак, ваш офис нуждается в сети (пока ни слова о беспроводных сетях). Вы сразу сталкиваетесь с проблемой монтажа сети. Скорее всего, компьютеры вашей сети будут находиться в разных комнатах. Тогда вы предстанете перед выбором: или тянуть витую пару "в обход", или же воспользоваться перфоратором, чтобы сэкономить витую пару и избавиться от проводов на стенах. Даже на монтаж небольшой сети вы можете потратить от нескольких часов до целого дня — все зависит от вашего опыта в этом деле.

Рано или поздно ваша сеть заработает. Но в один прекрасный день к вам в офис придет клиент, которому нужно сбросить некоторые файлы на его ноутбук. Болванок, как обычно, нет, флешка почему-то "глючит" (уж очень много на рынке дешевых флешек, которые выходят из строя спустя несколько месяцев эксплуатации). Вы решаете подключить ноутбук клиента к сети. А у вас есть заранее обжатый Ethernet-кабель? Нет? А есть ли свободные порты на коммутаторе? В общем, опять проблемы.

А теперь представим, что офис — арендуемый (как оно обычно бывает) и нужно переезжать на новое место. Да, придется сворачивать сеть и разворачивать ее в другом помещении. Возможно, придется заново обжать некоторые кабели, а некоторые подготовить заранее, — но не всегда можно угадать с длиной.

Беспроводная сеть — это решение для современного офиса. Ее монтаж осуществляется быстро и без перфоратора, клещей для обжима витой пары и прочих инструментов. Все, что вам нужно, — это правильно выбрать место для точки доступа (позже в этой книге вы узнаете, как это сделать), затем обойти с ноутбуком всю вашу территорию и убедиться, что везде, где нужно,

обеспечивается хорошее качество сигнала. Не потребуется тянуть витую пару и делать дырки в стенах. Ваши клиенты без особых проблем смогут подключиться к сети — не нужно думать ни о наличии свободных портов, ни о запасном Ethernet-кабеле. А демонтаж беспроводной сети заключается в демонтаже только точки доступа. Все просто и относительно дешево.

Однако, "чисто" беспроводная сеть — это что-то из области фантастики. Полностью отказаться от кабелей все же не получится. Во-первых, скорость передачи данных "по воздуху" все еще намного ниже, чем по кабелю: 54 Мбит/с против 1000 Мбит/с (Gigabit Ethernet). Во-вторых, перехватить данные, передаваемые радиоканалом, проще — злоумышленник может находиться даже не внутри вашего здания (если радиоволны проникают наружу), в случае же с кабельной сетью злоумышленник должен находиться в здании, а это сильно усложняет его задачу. Поэтому серверы и другие компьютеры, которым нужен высокоскоростной и безопасный доступ к сети, лучше подключать по кабелю, а все остальные, например, ноутбуки мобильных пользователей — по беспроводной сети.

У беспроводной сети есть и недостатки. О них вы должны узнать прежде, чем начнете эксплуатировать собственную беспроводную сеть. Вот они:

- набор частот и каналов для разных стран может отличаться. Например, во многих европейских странах можно задействовать два дополнительных канала (12 и 13), использование которых запрещено в США. В Японии есть дополнительный — 14-й канал, а во Франции можно использовать всего 4 канала. На территории бывшего СНГ все проще: Wi-Fi-сети пока не требуют регистрации, и можно использовать все 13 каналов;
- довольно высокое энергопотребление: у вашего ноутбука быстрее сядет аккумулятор при работе в беспроводной сети, чем при использовании GPRS-соединения;
- при построении публичной сети вам придется использовать стандарт шифрования WEP (поскольку стандарты шифрования WPA и WPA2 не поддерживаются "древними" адаптерами), а его можно относительно просто взломать даже при правильной настройке сети. Причем для этого не требуется обладать какой-либо квалификацией — программы для взлома WEP легко найти в Интернете;
- радиус действия Wi-Fi-сети ограничен: 30–50 метров в помещении и около 100 метров снаружи. Ослабить уровень сигнала могут стены (все зависит от материала, из которого они построены), зеркала, микроволновки и соседние беспроводные сети;
- в многоквартирных домах, где жильцы разворачивают свои беспроводные сети, может возникнуть проблема интерференции (наложения сигнала);

- неполная совместимость устройств разных производителей или неполное их соответствие стандартам может привести к снижению производительности сети;
- производительность сети может уменьшиться даже во время дождя (для наружных сетей).

Далее мы рассмотрим основные теоретические принципы беспроводной сети.

13.2. Зачем здесь теория?

Можно было бы эту часть книги написать намного проще. Рассказать, для чего используется точка доступа, объяснить, что такое беспроводной адаптер, заявить, что в беспроводной сети беспроводная точка доступа выполняет роль коммутатора (хотя это и не так), и на этом — все! По большому счету (в идеале) для построения беспроводной сети нужно включить точку доступа, установить некоторые основные ее параметры и включить беспроводные клиенты. Сеть будет работать. Но что делать, если начнутся проблемы (а они будут — это я вам гарантирую). Какие именно проблемы? Вот несколько типичных проблем для беспроводной сети:

- некоторые беспроводные сетевые клиенты не могут подключиться к сети — часть беспроводных клиентов отлично работают в вашей сети, а часть попросту не может подключиться. Первое, что приходит на ум — несовместимость беспроводных стандартов: например, точка доступа поддерживает один беспроводной стандарт, а некоторые сетевые клиенты — другой. Вы проверяете поддерживаемые стандарты и к своему удивлению обнаруживаете, что... все оборудование совместимо. В чем же причина? А в том, что по умолчанию одни производители используют одни параметры для своих сетевых адаптеров, а другие — совершенно иные. Поэтому нужно настроить беспроводные сетевые адаптеры. А как это сделать, если вы не знаете, что означает тот или иной параметр? Правильно, никак;
- ваша беспроводная сеть работает отвратительно, качество сигнала слишком низкое, стоит немного отойти от точки доступа с ноутбуком, и соединение сразу обрывается… Но уровень сигнала, отображаемый в программе настройки, — высокий. Вы в замешательстве. Что делать? Причиной такого неудовлетворительного поведения вашей сети является интерференция (наложение) радиосигналов. Вам нужно выяснить источник интерференции. Им может быть какое-то бытовое устройство: например, радиотелефон или микроволновая печь. А может быть, ваши соседи тоже развернули беспроводную сеть, и ваша сеть работает с сетью соседей на одном радиоканале (еще бы — ведь никто не изменял канал по умолчанию!);

- в вашу сеть проникли неавторизированные пользователи... Одно дело, если "гости" попользуются вашим каналом просто для Web-серфинга (да, пропускную способность они немного "посадят", но не это самое страшное), но совсем другое, если ваша сеть будет использоваться в качестве транзитной сети для взлома банка или распространения пиратского программного обеспечения (в том числе вирусов). Оно вам надо? Думаю, нет, поэтому в этой книге отдельное внимание будет уделено безопасности вашей сети.

Перечисленные три проблемы далеко не единственные. По мере чтения этой книги вы узнаете и о других проблемах, характерных для беспроводной сети.

13.3. Основные принципы работы беспроводной сети

Человечество научилось использовать радиоволны для передачи информации еще в 1920-х годах. Конечно, до современных беспроводных сетей тогда еще было далеко, но прорыв был сделан.

> ***Примечание***
>
> На самом деле радио было изобретено в 90-х годах позапрошлого века. В разных странах радио возникло в разные годы, причем разработки велись параллельно, поэтому нельзя сказать, что кто-то является единственным отцом радио. В России радио впервые изобрел А. Попов в 1895 году. В Италии разработчиком радио считается Гульельмо Маркони (1896), в США — Никола Тесла (но тут целая история: он первым запатентовал радио, а кто его первым создал — остается загадкой). Однако первооткрывателем способов передачи и приема электромагнитных волн является немецкий ученый Генрих Герц — он разработал эти способы еще в 1888 году.

Если вы в школе физику изучали, а не "проходили" мимо (в свое время я как раз "прошел" ее мимо, а наверстывать пришлось в институте, но это другая история, которая не имеет к книге никакого отношения), то наверняка помните уравнения Максвелла. Эти уравнения показывают изменение магнитного поля под воздействием электрического, и наоборот — как изменяется электрическое поле под действием магнитного. Когда ток перемещается по проводнику, освобождается часть энергии, которая трансформируется в магнитное поле. В свою очередь, это магнитное поле создает переменное электрическое поле, которое опять создает магнитное поле и т. д., пока самый первый поток не будет прерван.

Так вот, при переходе энергии из электрической в магнитную выделяется электромагнитная энергия или не что иное, как радиоволна. Устройство,

которое порождает радиоволны, называется *радиопередатчиком*, а устройство, принимающее их, — *радиоприемником*.

Чтобы радиоприемник смог получить радиоволны от радиопередатчика, приемник и передатчик должны работать на одной частоте. Что это за частота? Это частота, с которой переменное электромагнитное поле перемещается из передатчика в пространство. Вот почему радиоволны от тех же FM-станций не смешиваются между собой — потому что каждая FM-станция работает на своей частоте.

Радиочастоты, как и другие частоты, выражаются в герцах (Гц). Радиосигналы передаются на частотах, измеряемых обычно в кило-, мега- и гигагерцах (соответственно, кГц, МГц, ГГц).

Для передачи по радио звука (например, музыки или речи) передатчик смешивает аудиосигнал с несущей волной (это пример амплитудной модуляции — AM) или модулирует аудиосигналом частоту в диапазоне низких частот (это частотная модуляция — FM, frequency modulation). Приемник (AM или FM) определяет несущую волну и отделяет аудиосигнал.

Понятно, что если два передатчика будут передавать сигналы на одной частоте, то сигналы перемешаются. Поэтому в каждой стране есть специальные комитеты связи, регулирующие использование радиочастот. Каждая радиостанция должна получить лицензию на вещание на определенной частоте. Однако есть некоторые частоты, зарезервированные для нелицензионного использования, — чтобы работать на таких частотах, не нужна лицензия. Беспроводная компьютерная сеть работает как раз на нелицензированной частоте. Вы только представьте, что бы было, если бы каждому пользователю пришлось выдавать лицензию на использование беспроводной точки доступа? Большинство беспроводных Wi-Fi сетей работают на частоте 2,4 ГГц, некоторые отдельные варианты беспроводных сетей используют другой набор частот — 5 ГГц.

С одной стороны, использование нелицензированных частот — это хорошо, поскольку вы можете начать эксплуатировать свою сеть без всяких разрешений контролирующих органов. С другой стороны, массовость превращает достоинства в недостаток. Если вы собираетесь организовать беспроводную сеть на необитаемом острове, то никаких осложнений не заметите. Но в современных офисных зданиях беспроводные сети могут быть расположены в каждом офисе, что приводит к интерференции сигналов, поскольку радиосигналы с легкостью проникают через стены офисов. Радиус действия беспроводной сети внутри помещения — примерно 35 метров. Но не забывайте, что радиосигналы распространяются сферически. Допустим, ваш офис находится на третьем этаже шестиэтажного здания. Тогда радиосигналы вашей

сети будут доступны не только на третьем этаже, но также на первом, втором, четвертом, пятом и, возможно, шестом. По большому счету, одна беспроводная точка доступа может с легкостью охватить одно относительно небольшое здание (в среднем, один этаж занимает 3 метра в высоту, так что девятиэтажка по высоте — примерно 30 метров). Понятно, если еще кто-то в здании развернет беспроводную сеть (совсем не обязательно, что это будет ваш непосредственный сосед, — другая беспроводная сеть может находиться совсем на другом этаже), радиосигналы могут пересекаться. Чтобы все беспроводные сети работали нормально, администраторам этих сетей нужно собраться и скоординировать используемые радиоканалы. О том, как это сделать, будет сказано чуть позже.

Если скоординировать совместное использование сетей не получается или же источником интерференции сигналов является не другая сеть, а некий иной объект, избавиться от которого нельзя, следует понизить мощность радиопередатчика, что снизит и эффект наложения сигналов. Но в этом случае вы можете не охватить всю необходимую территорию. Кстати, по поводу территории. Помните, что радиоволны могут распространяться далеко за пределы вашего здания, и злоумышленнику, чтобы проникнуть в вашу беспроводную сеть, совсем не обязательно находиться на вашей территории — он может сидеть в машине, припаркованной неподалеку. Вот так...

13.4. Расширение спектра

Расширение спектра позволяет повысить эффективность передачи информации через канал с сильными линейными искажениями с помощью модулированных сигналов. Благодаря расширению спектра можно добиться увеличения базы сигнала.

В настоящее время используются три метода расширения спектра:

- FHSS (Frequency Hopping Spread Spectrum, псевдослучайная перестройка рабочей частоты) — несущая частота скачкообразно изменяется по некоторому алгоритму, который известен только приемнику и передатчику. Метод очень просто реализовать, но он не весьма эффективен. Такой метод используется технологией Bluetooth;
- DSSS (Direct Sequence Spread Spectrum, расширение спектра методом прямой последовательности) — более эффективен, чем FHSS, но и более сложен в реализации. Повышает тактовую частоту модуляции, каждому байту передаваемого сообщения ставится в соответствие некоторая достаточно длинная псевдослучайная последовательность;

- OFDM (Orthogonal Frequency Division Multiplexing, мультиплексирование с разделением по ортогональным частотам) — поток данных разбивается на 52 параллельных потока, каждый из которых использует собственную радиочастоту и называется *поднесущей*. Четыре поднесущих содержат данные об остальных 48 потоках. Поскольку сами данные передаются по 48 потокам, а 4 потока используются для передачи служебной информации, реальная максимальная скорость чуть ниже заявленной. Метод OFDM используется в беспроводных сетях;
- CSS (Chirp Spread Spectrum, расширение спектра методом прямой последовательности) — несущая частота перестраивается по линейному закону. Данный метод используется преимущественно в радиолокации.

Современные беспроводные Wi-Fi-стандарты IEEE 802.11a и 802.11g используют метод OFDM. Разница между ними в том, что 802.11a работает на частоте 5 ГГц, а 802.11g — 2,4 ГГц. Есть еще и стандарт 802.11b, работающий на частоте 2,4 ГГц, но использующий метод DSSS.

13.5. Современные беспроводные службы передачи данных

Современными беспроводными службами передачи данных являются: Wi-Fi, WiMAX и сотовые сервисы. На наших просторах WiMAX не очень распространен, хотя это вопрос времени. В этой книге серьезное внимание уделяется только Wi-Fi и сотовым сервисам (впрочем, WiMAX мы тоже вкратце рассмотрим).

13.5.1. Wi-Fi

Институтом инженеров электротехники и электроники (IEEE) разработан набор стандартов для беспроводных сетей — IEEE 802.11. Вот основные стандарты:

- IEEE 802.11 — разработан в 1997 году, охватывает два вида радиопередачи и сети на базе инфракрасных сигналов;
- IEEE 802.11a — охватывает высокоскоростные беспроводные сети;
- IEEE 802.11b — описывает дополнительные спецификации;
- IEEE 802.11g — на этом стандарте основаны практически все современные беспроводные сети.

Скоро будет окончательно утвержден новый стандарт — IEEE 802.11n. Он будет поддерживать скорость передачи данных 480 Мбит/с (текущий

стандарт 802.11g поддерживает всего 54 Мбит/с). Поскольку этот стандарт еще не принят, то мы рассматривать его в книге не будем, а кому интересно, тот всегда сможет прочитать о нем по адресу: **http://ru.wikipedia.org/wiki/IEEE_802.11n**.

> ***Примечание***
>
> Некоторые производители оборудования уже начали выпускать оборудование, поддерживающее предварительную версию стандарта IEEE 802.11n, — так называемые pre-802.11n-устройства. Не советую покупать такие устройства, потому что нет никакой гарантии, что такие "предварительные" устройства будут новый стандарт полностью поддерживать, когда его окончательно утвердят.

Сегодня используется в основном стандарт 802.11g, стандарты 802.11a и 802.11b считаются устаревшими. Правда, устаревшие сетевые адаптеры стандарта 802.11b все еще можно использовать в сетях 802.11g, но из-за одного такого адаптера вся сеть будет вынуждена снизить скорость в лучшем случае до 11 Мбит/с, поэтому рекомендуется использовать оборудование одного стандарта. Конечно, если вы строите публичную сеть (например, сеть для публичной библиотеки, отеля или беспроводную сеть интернет-зала), где будут самые "разношерстные" клиенты, то выбирайте точки доступа стандарта 802.11g, которые будут поддерживать как клиентов 802.11g, так и клиентов с устаревшими адаптерами стандарта 802.11b.

Стандарты 802.11a, b и g — далеко не единственные стандарты семейства IEEE 802.11, остальные стандарты приведены в табл. 13.1.

Таблица 13.1. *Семейство стандартов IEEE 802.11*

Стандарт	Описание
IEEE 802.11	Поддерживались скорости 1 и 2 Мбит/с, частота 2,4 ГГц и сети на инфракрасных сигналах
IEEE 802.11a	Скорость передачи данных — 54 Мбит/с, частота 5 ГГц. Стандарт был утвержден в 1999 году, но первые продукты появились в 2001 г.
IEEE 802.11b	Скорости передачи данных 11 Мбит/с и 5,5 Мбит/с (1999 год)
IEEE 802.11c	Описывает операции с мостами
IEEE 802.11d	Поддерживает международные роуминговые расширения (2001 год)
IEEE 802.11e	Обеспечивает поддержку QoS (качество обслуживания)
IEEE 802.11F	Протокол Inter-Access Point Protocol (2003 год)

Таблица 13.1 *(окончание)*

Стандарт	Описание
IEEE 802.11g	Скорость передачи данных — 54 Мбит/с, частота 2,4 ГГц. Стандарт обратно совместим с 802.11b. Дата утверждения стандарта — 2003 год
IEEE 802.11h	Распределение по спектру 802.11a (5 ГГц) для лучшей совместимости в Европе (2004 год)
IEEE 802.11i	Дополнения, касающиеся безопасности
IEEE 802.11j	Специальные расширения для Японии (2004 год)
IEEE 802.11k	Различные незначительные изменения
IEEE 802.11l	Не используется, зарезервирован
IEEE 802.11m	Различные незначительные изменения
IEEE 802.11n	Планируется скорость передачи данных до 480 Мбит/с, частота 2,4–2,5 или 5 ГГц. Обратная совместимость с 802.11a/b/g. Пока не утвержден
IEEE 802.11o	Не используется, зарезервирован
IEEE 802.11p	Беспроводной доступ для транспортных средств, например, для машин скорой помощи
IEEE 802.11q	Не используется, зарезервирован
IEEE 802.11r	Быстрый роуминг
IEEE 802.11s	Расширенный набор сервисов (ESS) Mesh Networking
IEEE 802.11T	Это не стандарт, а рекомендация относительно проведения тестов и измерений
IEEE 802.11u	Описывает взаимодействие с не-802 сетями (например, с сотовыми сетями)
IEEE 802.11v	Описывает управление беспроводными сетями
IEEE 802.11x	Не используется, зарезервирован
IEEE 802.11w	Описывает защищенные управляющие кадры (Protected Management Frames)

Характеристики стандартов 802.11a/b/g/n приведены в табл. 13.2.

Таблица 13.2. *Характеристики стандартов Wi-Fi*

Стандарт	Частота, ГГц	Реальная скорость передачи, Мбит/с	Максимальная скорость передачи, Мбит/с	Радиус покрытия
802.11b	2,4	5	11	~30 м (внутри) ~100 м (снаружи)
802.11a	5	20	54	~35 м (внутри) ~110 м (снаружи)
802.11g	2,4	20	54	~35 м (внутри) ~110 м (снаружи)
802.11n	2,4	150	480	~70 м (внутри) ~160 м (снаружи)

Примечание

Радиус покрытия во многом зависит от точки доступа. По стандарту он составляет примерно 35 метров внутри помещения и около 100 метров снаружи. Но современные точки доступа позволяют охватывать значительно большую территорию. Например, точка доступа D-LINK DWL-2100AP обладает радиусом действия 100 и 400 метров (соответственно, внутри и снаружи). И это недорогая точка доступа — она относится к средней ценовой категории. А точка доступа ENCORE ENRXWI-SG обладает меньшим радиусом действия (но и стоит дешевле, чем точка доступа от D-Link): 30–50 метров внутри помещения и 50–200 метров снаружи. Однако даже эти значения превышают стандартные.

Множество стандартов удручает? Поэтому гении маркетинга решили назвать все стандарты семейства IEEE 802.11 одним красивым термином — Wi-Fi[1] (кратко и созвучно с Hi-Fi). Кто эти гении? Специалисты группы WECA (Wireless Ethernet Compatibility Alliance, Альянс совместимости беспроводных Ethernet-сетей). WECA проводит тестирование и сертификацию оборудования различных производителей. Если на коробке с Wi-Fi-устройством вы увидели логотип Wi-Fi (рис. 13.1), значит, находящееся в коробке устройство совместимо с другими устройствами с таким же логотипом.

Рис. 13.1. Логотип Wi-Fi

[1] От англ. *Wireless Fidelity* — беспроводная точность.

13.5.2. WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) — еще один вид беспроводных сетей (описан в стандарте IEEE 802.16). Сети Wi-Fi предназначены для покрытия небольшой территории (как уже отмечалось ранее — примерно 35 метров внутри помещения и 100 метров снаружи). А вот сети WiMAX могут покрывать территорию с радиусом 48 км (30 миль).

Максимальная скорость передачи данных по WiMAX-каналу — 70 Мбит/с. У нас WiMAX пока распространен мало. В США WiMAX используется как альтернатива DSL-соединениям. В основном удел WiMAX — это стационарные компьютеры, размещенные в фиксированных местах (в силу особенностей оборудования для WiMAX), хотя сама передача данных осуществляется "по воздуху".

13.5.3. Сотовые сервисы

Наверное, сегодня не найдется ни одного пользователя Интернета, который бы не знал о GPRS (General Packet Radio Service, пакетная радиосвязь общего пользования). GPRS-соединение теоретически способно передавать данные со скоростью 171 Кбит/с, но на практике (поскольку вы не единственный пользователь сотового оператора) выходит около 20–30 Кбит/с. Конечно, по современным меркам такая скорость никуда не годится. Но зато GPRS позволяет пользователю быть более мобильным — ведь Интернет по GPRS есть везде, где есть зона покрытия оператора, и не ограничивается ни расстоянием в 100 метров (Wi-Fi), ни 48 км (WiMAX).

На смену GPRS пришла технология EDGE (Enhanced Data rates for GSM Evolution) — это не что иное, как надстройка над технологией GPRS. EDGE позволяет передавать данные со скоростью 474 Кбит/с, что существенно выше скорости GPRS-соединения. Практическая скорость ограничивается сотовым оператором, но она в любом случае ощутимо выше скорости GPRS-соединения (больше 100 Кбит/с).

Сейчас активно развивается новая технология — 3G. Интересно, что для нее не придумали собственного названия: 3G — это просто "третье поколение" (G, generation) сотовой связи. Помимо всяких "вкусностей", относящихся непосредственно к мобильной связи (вроде видеозвонка), третье поколение поддерживает передачу данных со скоростью до 2,4 Мбит/с, что вполне приемлемо даже по сегодняшним меркам. Скоро будет доступна и 4G, там обещают скорость передачи данных в пределах 100 Мбит/с. Вот только, когда это произойдет, пока не известно, — сейчас даже 3G пока не получил особого распространения. Кстати, GPRS условно относят к сетям 2G, а EDGE — к 2,5G.

13.5.4. Не забудем и о Bluetooth

Bluetooth — это еще один способ беспроводной связи, но он используется преимущественно не для организации сетей, а для соединения различных периферийных устройств — например, для подключения мобильного телефона или КПК к ноутбуку, для подключения гарнитуры free-hand к мобильному телефону, для подключения беспроводной клавиатуры и мыши и т. п. Радиус действия Bluetooth — до 10 метров, а скорость передачи данных — до 700 Кбит/с (в зависимости от класса Bluetooth). Как и беспроводные сети, Bluetooth использует частоту 2,4 ГГц. Другими словами, Bluetooth служит в качестве вспомогательного средства для обмена данными, но для построения сетей не используется. Впрочем, никто не запрещает по Bluetooth подключить ноутбук (нетбук) к стационарному компьютеру и выходить по этой связке в Интернет, лежа на диване. К слову, вы можете связать ноутбук с мобильным телефоном по Bluetooth, но для подключения к Интернету в этом случае будет использоваться GPRS или EDGE (в зависимости от вашего сотового оператора и телефона).

13.6. Принципы работы Wi-Fi

Наша теоретическая глава продолжается. Мы вкратце рассмотрели основные службы беспроводной передачи данных. Поскольку для построения нашей беспроводной сети мы будем использовать Wi-Fi, настало время подробно поговорить об этом сервисе.

13.6.1. Физический и канальный уровни Wi-Fi

Сначала рассмотрим передачу данных на физическом и канальном уровнях OSI-модели. На *физическом* уровне к каждому пакету радиопередатчик добавляет 144-битную преамбулу. Из этих 144 битов 128 битов используются для синхронизации с передатчиком, а оставшиеся 16 битов служат признаком начала кадра. После преамбулы следует 48-битный заголовок. Заголовок содержит служебную информацию: скорость передачи данных, длина передаваемых данных и др.

А теперь вдумайтесь: поскольку скорость задается в заголовке, но сам заголовок следует после преамбулы, то на какой скорости передается преамбула? Преамбула (понятно, и сам заголовок) передаются всегда на постоянной скорости — 1 Мбит/с. После получения заголовка скорость повышается до указанного в заголовке значения. Именно поэтому даже если сеть работает на максимальной скорости (например, 54 Мбит/с), реальная скорость будет ниже, поскольку первые 192 бита каждого кадра передаются со скоростью 1 Мбит/с.

Не кажется ли вам, что 144 бита — это для преамбулы слишком много? 144-битная преамбула использовалась в старых DSSS-системах (802.11b). В новых системах (802.11g) используется короткая преамбула длиной 72 бита. Из них 56 битов отвечают за синхронизацию устройств (передатчика и приемника), а последние 16 битов занимает поле начала кадра (его размер такой же, как и в 144-битной преамбуле).

Новая 72-битная преамбула не совместима с оборудованием 802.11b. Поэтому многие производители 802.11g-оборудования по умолчанию устанавливают 144-битную преамбулу — для обеспечения обратной совместимости с 802.11b. Если вы строите свою собственную (частную) сеть на базе нового оборудования, то в настройках точки доступа можете выбрать короткую преамбулу — ведь все ваше оборудование ее поддерживает. А вот если вы строите публичную сеть, вам нужно обеспечить поддержку старого оборудования, поэтому следует выбрать длинную преамбулу.

Стоит ли переходить на короткую преамбулу, если нет необходимости в поддержке старого оборудования? Конечно! Ведь на обработку преамбулы старого образца требуется 192 мс, а на обработку новой преамбулы — всего 96. Если вы планируете передавать голос и видео в реальном времени (например, общаться через Web-камеру), обязательно установите короткую преамбулу. Если же вы обмениваетесь только обычными данными (документы, ICQ, электронная почта), то преамбула особой роли не играет.

Чуть ранее было сказано, что производители оборудования по умолчанию задают длинную преамбулу. К сожалению, этого правила придерживаются не все производители, и на этапе настройки сети вы можете обнаружить, что точка доступа и часть беспроводных адаптеров настроены на использование короткой преамбулы, а часть — длинной (или наоборот). Если вы работаете с оборудованием одного производителя, то проблем не возникнет. А вот если у вас оборудование разных производителей, то вы можете столкнуться с необходимостью изменения длины преамбулы на точке доступа и/или на сетевых адаптерах.

Самое интересное, что эта проблема теоретически может появиться даже при настройке вашей домашней сети! Предположим, что у вас есть стационарный компьютер и ноутбук. Вы покупаете точку доступа производства компании А, вы покупаете беспроводной адаптер для стационарного компьютера тоже фирмы А, но в ноутбуке установлен сетевой адаптер фирмы Б. Рекомендовал бы сначала выяснить, какой фирмы адаптер установлен в ноутбуке, и покупать все остальное оборудование этой фирмы (но это не всегда возможно), или в случае необходимости изменить длину преамбулы на адаптере ноутбука (это делается с помощью специального программного обеспечения).

Мы рассмотрели физический уровень, теперь переходим к MAC (Media Access Control) уровню. MAC-уровень обычно рассматривается как подмно-

жество *канального* уровня. На этом уровне происходит управление трафиком, передающимся по беспроводной сети. Для предотвращения конфликтов и коллизий используется метод CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance) — множественный доступ с прослушиванием несущей волны и избеганием коллизий. На MAC-уровне также реализованы функции безопасности, определенные стандартом 802.11.

Вспомним суть метода CSMA/CA *(см. разд. 10.2)*. Когда два или большее количество узлов пытаются одновременно передать данные, CSMA/CA "просит" все узлы, кроме одного, прекратить передачу данных. "Счастливчик", которому разрешено передать данные, выбирается случайным образом. Но CSMA/CA может также предоставить приоритет узлу, который пытается передать данные, критические к времени (видео и/или голос).

На MAC-уровне определено два вида аутентификации узла (об этом мы достаточно подробно поговорим позже). Помните, что все узлы сети должны использовать один и тот же способ аутентификации.

Чаще всего клиентами Wi-Fi-сетей выступают мобильные устройства — ноутбуки, КПК. Все эти устройства обычно питаются от встроенного аккумулятора, поэтому на MAC-уровне были предусмотрены средства энергосбережения. Беспроводной сетевой адаптер может работать в одном из двух режимов: в обычном или в энергосберегающем. В первом случае адаптер отправляет и получает данные мгновенно, но всегда потребляет одно и то же количество энергии, даже если ничего не получает и не передает. В таком режим аккумулятор ноутбука разрядится быстрее. В энергосберегающем режиме адаптер находится большую часть времени в режиме простоя и потребляет мало энергии. Периодически он "просыпается" для отправки пакетов, находящихся в его буфере и для получения пакетов от сети, которые до этого времени хранятся в буфере точки доступа. В этом режиме обеспечивается экономия заряда аккумулятора.

13.6.2. Радиочастоты и каналы Wi-Fi

Стандарты 802.11b и 802.11g

Как уже было отмечено, сети 802.11b и 802.11g работают на частоте 2,4 ГГц, но это не значит, что рабочая частота именно 2,400 ГГц, — сеть может использовать диапазон частот 2,400–2,4835 ГГц. Именно в таком диапазоне частот работают Wi-Fi-сети в Европе и США. Исключение составляют Франция, Испания и Япония, где рабочий диапазон частот чуть другой:

- 2,445–2.475 ГГц — в Испании;
- 2,4465–2.4835 ГГц — во Франции;
- 2,471– 2.497 ГГц — в Японии.

Вообще, точные значения частот нам не интересны, поскольку все продаваемое в нашей стране оборудование сертифицировано и использует частоты 2,400–2,4835 ГГц.

Какую именно частоту из диапазона 2,400–2,4835 ГГц будет использовать ваша сеть? Рабочая частота сети определяется радиоканалом, на котором она работает (помните, говорили о каналах чуть ранее). В табл. 13.3 приведено распределение беспроводных каналов.

Таблица 13.3. *Распределение беспроводных каналов (для 802.11b и 802.11g)*

Канал	Частота, ГГц	Канал	Частота, ГГц
1	2,412	8	2,447
2	2,417	9	2,452
3	2,422	10	2,457
4	2,427	11	2,462
5	2,432	12	2.467
6	2,437	13	2,472
7	2,442	14	2,484

В Европе и США используется 13 каналов, в Японии — 14. Опять всю картину портит Франция — она использует всего 4 канала, но поскольку мы к французам не имеем никакого отношения, то и говорить больше о них не будем.

Итак, если ваша сеть работает на первом канале, то рабочей частотой будет 2,412 ГГц, если на третьем, то — 2,422 ГГц.

Помните, мы говорили о интерференции (наложении) радиосигналов двух рядом работающих сетей? По умолчанию беспроводные точки доступа настроены на работу на первом канале. Если рядом (на расстоянии, которое не превышает 35 метров) размещены две точки доступа, работающие на первом канале, то их радиосигналы будут накладываться. Чтобы две сети не мешали друг другу, одну из сетей нужно перенести на другой канал, например, на 5-й. Тогда одна сеть будет работать на частоте 2,412 ГГц, а другая — на 2,432 ГГц.

Дабы полностью исключить интерференцию, нужно, чтобы частоты сетей отличались на 25 МГц, или на 5 каналов. Оптимальная раскладка для трех рядом расположенных сетей: это каналы 1, 6 и 11. Если надо обеспечить совместную работу четырех рядом расположенных сетей, тогда можно использовать каналы 1, 5, 9, 13. В этом случае "расстояние" между ними будет равно четырем каналам — все сети будут ощущать небольшое вмешательство,

но не критичное, и все они смогут работать почти с максимальной производительностью. Если вы хотите полностью исключить интерференцию сигналов четырех сетей, нужно также понизить мощность передатчика каждой точки доступа. Правда, в этом случае охватываемая территория может стать меньше (например, вместо 35 метров покрытия будет охвачено всего 30). Но в большинстве случаев и это не критично. Ведь средняя площадь квартиры или небольшого офиса — примерно 60–65 квадратных метров. Грубо говоря, нам нужно охватить "коробочку" размером 8×8 м. Даже если вы понизите мощность передатчика так, что он будет охватывать радиус в 20 метров, этого будет достаточно, чтобы охватить все помещение.

Стандарт 802.11a

Стандарт 802.11a использует диапазон частот 5,00–5,34 ГГц. Каналы для этого стандарта "шириной" в 20 МГц (а не в 25, как в случае с 802.11g). Распределение каналов для этого стандарта приведено в табл. 13.4.

Таблица 13.4. *Распределение беспроводных каналов для 802.11a*

Канал	Частота, ГГц	Канал	Частота, ГГц
34	5,17	46	5,23
36	5,18	48	5,24
38	5,19	52	5,26
40	5,20	56	5,28
42	5,21	60	5,30
44	5,22	64	5,32

В Европе используются каналы 36, 40, 44 и 48. Остальные каналы задействованы в неевропейских странах — например, каналы 34, 38, 42 и 46 заняты под Японию. В США используются "европейские" каналы плюс каналы 52, 56, 60 и 64.

13.6.3. Режимы работы сети

Обычно беспроводная сеть является *централизованной*, или, как ее еще называют, *инфраструктурной* (рис. 13.2). Центральным устройством выступает точка доступа. На рис. 13.2 показано, что ноутбуки для подключения к беспроводной сети используют встроенные адаптеры, а стационарные компьютеры — внешние. В *главе 14*, когда мы будем выбирать оборудование для нашей сети, вы узнаете, почему для стационарных компьютеров лучше подходят внешние адаптеры.

Рис. 13.2. Централизованная сеть

Но при желании можно организовать одноранговую беспроводную сеть без центрального устройства. Такие сети называется *ad hoc-сетями*. Сетевые адаптеры компьютеров переводятся в режим ad hoc и обмениваются данными напрямую, без участия точки доступа. Такой режим полезен, когда есть два компьютера (например, два ноутбука), но рядом нет никакой точки доступа, а передать данные нужно. В такой сети максимальная скорость передачи данных составляет всего 1 Мбит/с, но для обмена данными между всего двумя узлами этого вполне достаточно.

Напоследок рассмотрим несколько терминов, которые вы можете встретить при чтении документации по беспроводным сетям (например, при чтении руководства по точке доступа):

- BSS (Basic Service Set) — обычная беспроводная сеть с одной точкой доступа;
- ESS (Extended Service Set) — беспроводная сеть с двумя или больше точками доступа;
- IBSS (Independent Basic Service Set) — одноранговая беспроводная сеть без точки доступа.

В следующей главе будет больше практики — мы поговорим о выборе оборудования для нашей беспроводной сети.

Глава 14

Выбор оборудования для беспроводной сети

14.1. Основные сетевые устройства беспроводной сети

Для построения беспроводной сети нам понадобится одна *точка доступа* (в англ. терминологии wireless access point) и несколько *беспроводных сетевых адаптеров* (в англ. терм. wireless adapter) — по количеству *стационарных* компьютеров. Напомню, что точка доступа выполняет роль центрального устройства сети. Попросту говоря, это тот же коммутатор, но для беспроводной сети. Такое сравнение сугубо ассоциативное, просто чтобы у вас сформировалось представление о функциях точки доступа.

Если вы планируете построить довольно большую беспроводную сеть, то вам понадобится несколько точек доступа. Просчитать зону покрытия относительно просто: в помещении радиус действия точки доступа составляет примерно 35 метров, снаружи — примерно 100 метров. Обычно радиосигналы точки доступа распространяются с одинаковой мощностью по всем направлениям, поскольку точки доступа по умолчанию оснащаются всенаправленными антеннами. Если нужно обеспечить покрытие сети только в одном направлении, то понадобится направленная антенна. В этом случае вы можете охватить примерно 70 метров внутри помещения и около 200 метров (иногда даже больше) — снаружи.

В помещениях, в плане близких к квадрату, лучше всего использовать всенаправленную антенну (рис. 14.1). Угол распространения радиосигнала направленной антенны составляет 45 градусов (рис. 14.2), это тоже нужно учитывать при построении сети. Хотя бывают антенны с другим углом апертуры, но об этом мы поговорим в следующей главе, когда будем планировать свою сеть.

Забегая вперед (вообще-то об этом нужно говорить при планировании сети, но ведь оборудование выбирается сейчас!), скажу, что бывают не очень приятные ситуации, связанные с расположением стационарных компьютеров.

Такая ситуация изображена на рис. 14.3. Вы установили точку доступа, которая охватывает практически всю необходимую территорию, но вне зоны покрытия остался один стационарный компьютер. С такими компьютерами всегда сложнее — ведь ноутбук можно легко перенести на другое место, а вот проделать то же самое со стационарным компьютером не всегда просто.

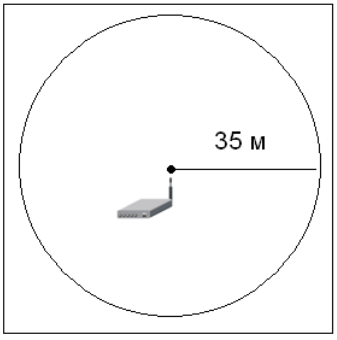


Рис. 14.1. Зона покрытия при использовании всенаправленной антенны

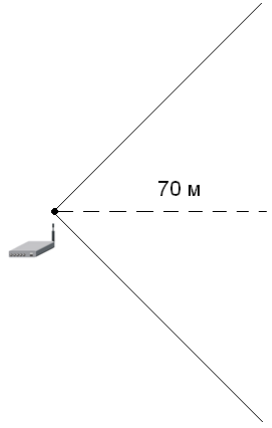


Рис. 14.2. Зона покрытия сети при использовании направленной антенны

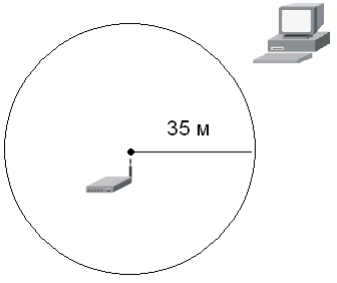


Рис. 14.3. Один компьютер остался вне зоны сети

Что делать? Покупать вторую точку доступа? Но это нерационально — ведь компьютер всего один. В этом случае поможет беспроводной сетевой адаптер с возможностью подключения внешней антенны. Такой сетевой адаптер подключается к тому самому неохваченному компьютеру, а к нему, в свою очередь, подключается направленная антенна, которая и направляется в сторону точки доступа. Все — проблема решена.

Что же касается беспроводных сетевых адаптеров, то вам нужно купить их столько, сколько у вас стационарных компьютеров. Как правило, все современные ноутбуки оснащены беспроводными адаптерами 802.11g, поэтому покупать беспроводные адаптеры для ноутбуков необходимости нет.

Итак, теперь мы знаем, что понадобится для нашей сети: пока одна точка доступа и несколько беспроводных сетевых адаптеров. Возможно, понадобятся направленные антенны для удаленных от точки доступа компьютеров. Нам осталось только выбрать точку доступа и сетевые адаптеры. Начнем с сетевых адаптеров.

14.2. Выбор сетевых адаптеров

Выбор беспроводного адаптера — дело тонкое. Принцип "пришел, увидел, купил" здесь не работает. При выборе беспроводного адаптера вам нужно учитывать следующее:

- форм-фактор сетевого адаптера;
- поддерживаемые беспроводные стандарты;
- тип антенны;
- совместимость с операционной системой компьютера.

14.2.1. Форм-фактор

Wi-Fi-адаптеры выполняются в следующих вариантах:

- *внешние адаптеры* — такие адаптеры, как правило, подключаются к компьютеру по USB. Это самый удобный вид адаптеров: их легко установить и отключить и легко в случае необходимости подключить к другому компьютеру;
- *внутренние адаптеры* — обычно такие адаптеры выполняются в виде PCI-карт расширения (рис. 14.4). Они стоят дешевле, чем внешние адаптеры, но тут вы столкнетесь с определенными неудобствами. Во-первых, при самостоятельной установке возможна потеря гарантии на системный блок, поэтому если ваш системный блок еще на гарантии, устанавливать такой адаптер можно только в сервисном центре. Во-вторых, в случае, если понадобится перенести адаптер на другой компьютер, придется разбирать их оба: компьютер, на котором установлен адаптер, и компьютер, на который нужно его установить. Решать вам — стоит ли экономия таких неудобств?
- *PC-Card* (старое название PCMCIA) — такие адаптеры подходят для ноутбуков (рис. 14.5). Если у вас старенький ноутбук, где нет беспроводного

адаптера или же установлен устаревший беспроводный адаптер (802.11b), то вы можете модернизировать такой ноутбук путем установки адаптера 802.11g, выполненного в виде PC-Card;

- *адаптеры для КПК* — перед покупкой такого адаптера нужно убедиться, что он подойдет для вашего КПК, поскольку разъемы для подключения таких адаптеров могут быть различны для КПК разных производителей.

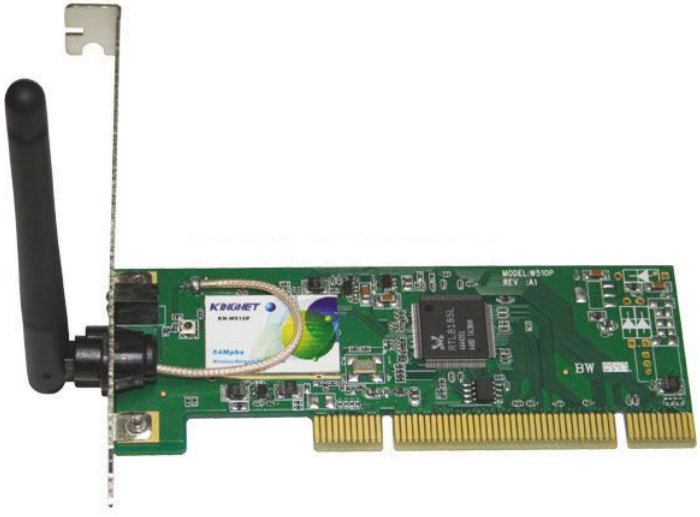


Рис. 14.4. Беспроводной адаптер, выполненный в виде PCI-карты расширения

Рис. 14.5. Беспроводной адаптер производства ZyXEL для ноутбука (вид сверху и снизу)

Понятно, что самыми универсальными являются внешние USB-адаптеры. При желании такой адаптер можно легко подключить к любому стационарному компьютеру и даже к ноутбуку. USB-разъемы сейчас есть даже на не самых "свежих" компьютерах, поэтому проблем с подключением такого адаптера не возникнет. USB-адаптер легко подключить, отключить и перенести на другой компьютер. Одним словом — это лучший выбор.

Однако USB-адаптеры бывают двух типов: мини и полноразмерные. Мини-адаптеры напоминают флешку — и по размерам и по внешнему виду (рис. 14.6). Обычно у такого адаптера встроенная антенна, поэтому не нужно ожидать от него уверенного качества приема на "пограничной" территории. Однако, учитывая компактность, такой адаптер можно порекомендовать пользователям ноутбуков — ведь с ноутбуком гораздо проще перейти в зону уверенного приема, чем со стационарным компьютером. Мини-адаптеры также можно установить и на стационарные компьютеры, но только если они находятся поближе к точке доступа.

Для стационарных компьютеров можно порекомендовать USB-адаптеры, подключаемые к компьютеру по USB-кабелю. Некоторые из них внешне чем-то напоминают небольшую точку доступа (коробочка с одной или двумя антеннами), некоторые обладают стильным дизайном (рис. 14.7). Но преимущество такого адаптера отнюдь не в дизайне. Дело в том, что такой адаптер не жестко прикреплен к компьютеру. Вы можете его свободно перемещать в пределах длины кабеля. Иногда, переместив адаптер всего на несколько сантиметров, можно добиться существенного улучшения приема.

Рис. 14.6. Мини USB-адаптер

Рис. 14.7. Адаптер, подключаемый к компьютеру по USB-кабелю

14.2.2. Поддерживаемые беспроводные стандарты

Современный стандарт один — 802.11g. Поэтому все адаптеры и точки доступа должны поддерживать этот стандарт. Покупать устройства, поддерживающие предварительную версию стандарта 802.11n, не стоит. Поскольку

этот стандарт еще окончательно не утвержден, то и не известно, как будут работать купленные устройства в настоящей 802.11n-сети. Да и не ясно, как будут работать "pre-n"-устройства в сети 802.11g.

14.2.3. Тип антенны

У мини-USB адаптеров и адаптеров, выполненных в формате PC-Card, антенна часто встроенная. Если вы покупаете адаптер для ноутбука, в этом нет ничего страшного, даже, наоборот, удобно — вы можете свободно перемещаться с ноутбуком, не боясь повредить антенну. А вот для стационарных компьютеров желательно покупать адаптеры с внешними антеннами. Кстати, выпускаются и мини-адаптеры с внешними антеннами (рис. 14.8). Такие адаптеры одновременно и компактны, и обеспечивают надежный прием радиосигналов.

Рис. 14.8. Адаптер с внешней антенной

Желательно, чтобы была возможность подключения к адаптеру еще одной антенны. Помните, чуть ранее была рассмотрена ситуация, когда для уверенного приема сигнала пришлось подключить направленную антенну. Ведь по умолчанию антенны беспроводных адаптеров всенаправленные, то есть обеспечивают прием/передачу сигналов по всем направлениям с одинаковой мощностью. А если нужно будет усилить сигнал в определенном направлении, то понадобится дополнительная направленная антенна. Поэтому разъем для такой антенны должен быть. Особенно это касается адаптеров, которые будут установлены на компьютерах, достаточно удаленных от точки доступа (30–35 метров).

14.2.4. Совместимость с операционной системой компьютера

Перед покупкой адаптера нужно убедиться, что он совместим с вашей операционной системой. Например, на коробке может быть написано "Works with Windows Vista", или "Supported by Windows Vista", или "Designed for Windows Vista".

Такой адаптер, понятное дело, будет превосходно работать в Windows Vista. Но что делать, если у вас Windows XP или Linux. Некоторые производители оборудования, спроектированного для Vista, даже не предоставляют драйверы для этого оборудования — в Vista необходимый драйвер уже есть, а для других операционных систем драйвер недоступен не то что в комплекте с адаптером, но и на сайте производителя.

Итак, вам нужно узнать, есть ли в комплекте поставки драйвер для вашей операционной системы. Если его нет, тогда стоит попытаться найти драйвер на сайте производителя сетевого адаптера. Кроме сайта производителя, драйвер для беспроводного адаптера можно поискать еще на следующих сайтах:

- **http://www.windrivers.com**;
- **http://www.driverzone.com**;
- **http://www.driverguide.com**.

Современные дистрибутивы Linux поддерживают много беспроводных адаптеров, но никто не даст гарантию, что ваш дистрибутив будет поддерживать именно тот адаптер. Поэтому перед покупкой адаптера пройдитесь по форумам и поищите, настраивал ли кто-то такой адаптер в Linux? Заодно найдете и процедуру настройки.

Если вас терзают сомнения по поводу поддержки того или иного устройства операционной системой, лучше выбрать адаптер другого производителя, который будет гарантированно работать на вашем компьютере.

14.2.5. Комбинированные адаптеры

Некоторые производители выпускают комбинированные адаптеры. Такие адаптеры сочетают в себе функциональность Wi-Fi и Bluetooth. Предложение довольно заманчивое: ведь они стоят немного дороже обычных Wi-Fi-адаптеров и дешевле двух отдельных адаптеров: Wi-Fi и Bluetooth. Покупать такой адаптер или нет — решать вам. Если вам нужен Bluetooth, тогда такой адаптер — хорошее приобретение. А если Bluetooth не нужен, не вижу смысла платить больше.

14.3. Установка беспроводного адаптера

USB-адаптер достаточно просто подключить к компьютеру, после чего система обнаружит его и установит драйверы. В случае с PCI-устройством обязательно выключите питание компьютера и отсоедините кабель питания от сети напряжения. Затем откройте крышку системного блока, установите адаптер в свободный слот и соберите корпус. Подключать PCI-адаптер при включенном компьютере нельзя!

Некоторые ноутбуки позволяют модернизировать беспроводной адаптер. Тогда нужно покупать не USB-адаптер, а внутренний адаптер, предназначенный именно для вашего ноутбука. Правда, устанавливать такие адаптеры лучше в сервисном центре, особенно, если вы не знаете, как это сделать. На рис. 14.9 изображено днище ноутбука HP Compaq: крышка слева позволяет "добраться" до жесткого диска ноутбука, а крышка справа — до беспроводного адаптера.

Рис. 14.9. Нижняя панель ноутбука HP Compaq

14.4. Выбор точки доступа

При выборе точки доступа нужно учитывать следующие факторы:

- поддерживаемые точкой доступа стандарты;
- область применения точки доступа (внутреннее или наружное);
- радиус покрытия;
- тип антенны, наличие разъема для подключения внешней антенны;
- алгоритм шифрования;
- дополнительные функции.

Типичная точка доступа изображена на рис. 14.10.

Рис. 14.10. Точка доступа

14.4.1. Поддерживаемые точкой доступа стандарты

Современные точки доступа поддерживают стандарты 802.11b и 802.11g. Иногда встречаются комбинированные точки доступа, поддерживающие стандарты 802.11a и 802.11g. Но такие точки доступа — редкость, и их стоимость существенно превышает стоимость обычных точек доступа стандарта 802.11g. Необходимость в таких точках доступа может быть только, если вы настраиваете публичную сеть и хотите, чтобы к ней могли подключиться клиенты с адаптерами всех типов.

14.4.2. Область применения и радиус действия точки доступа

Для многих точек доступа указывается область внутреннего и наружного радиуса действия. Однако это не означает, что данная точка доступа может эксплуатироваться за пределами помещения. Значение наружного радиуса действия можно использовать только в ознакомительных целях для оценки мощности передатчика точки доступа. Если в характеристиках точки доступа, например, указано: "Радиус покрытия: внутри помещения: 30 ~ 50 м, на открытом пространстве: 50 ~ 200 м", то это означает, что в обычном помещении радиус действия составит от 30 до 50 метров в зависимости от материала стен и наличия в окружающей среде радиопомех. Но гарантировано, что вы получите радиус в 30 метров. А вот если в этом помещении убрать все стены и исключить радиопомехи, то точка доступа сможет охватить радиус в 200 метров.

Точки доступа для наружного размещения (в наименовании таких точек доступа обычно указывается "outdoor") стоят обычно в несколько раз дороже, чем обычные. Это связано с особым корпусом точки доступа, который защищает ее от воздействия окружающей среды: дождя, мороза, влажности. Обычная точка доступа может работать при температуре от 0 до 55 градусов. Наружная точка доступа (рис. 14.11) может работать и при отрицательных температурах. Обычная точка доступа, скорее всего, не выживет даже после дождя, а наружную от погодных условий защищает корпус.

Рис. 14.11. Наружная точка доступа

Зачем нужны наружные точки доступа? В Америке они обычно используются для построения так называемых *кампусных сетей* — сетей, которые развернуты на территории университетского городка (кампуса), причем такие сети обеспечивают доступ как внутри помещения, так и снаружи. Студентам некоторых отечественных вузов приходится только мечтать об Интернете в общежитиях, не говоря уже об Интернете за его пределами...

Другое дело, если у вас частный дом, и вы хотите, чтобы Интернет был и во дворе. Довольно удобно летом сидеть в беседке и работать в Интернете. А почему бы и нет? Сказано — сделано. Но в этом случае можно немного сэкономить. Разместите обычную ("внутреннюю") точку доступа ближе к наружной стене дома. Если использовать некоторые модели с повышенным радиусом действия, то вы получите охват даже внутри помещения порядка 100 метров. А этого вполне хватит, чтобы охватить и дом, и двор.

14.4.3. Антенна точки доступа

Практически у всех точек доступа антенны внешние, и в некоторых случаях "на борту" точки доступа имеются даже две антенны (такие точки доступа

обеспечивают наилучший прием, поэтому лучше отдать предпочтение подобным моделям). Вы можете изменять угол наклона каждой антенны для обеспечения наилучшего покрытия.

Забегая вперед, подскажу: если вы планируете разместить точку доступа на столе, то антенны нужно направить вверх, а если вам хочется разместить точку доступа под потолком, тогда антенны нужно направить вниз. Так будет обеспечен наилучший прием сигналов.

Желательно также, чтобы у точки доступа была возможность подключения дополнительной антенны. Мало ли что может понадобиться.

14.4.4. Алгоритм шифрования

Существуют два алгоритма шифрования данных, передаваемых по беспроводной сети: WEP (Wired Equivalent Privacy) и WPA (Wi-Fi Protected Access). Алгоритм WEP по своей надежности напоминает швейцарский сыр (или решето). В Интернете имеется масса программ для взлома WEP-защиты, так что взломать сеть, использующую WEP, может даже школьник. Ради справедливости нужно отметить, что и WPA не панацея, но этот метод шифрования намного надежнее, чем WEP, поэтому следует покупать точку доступа, которая поддерживает WPA.

Впрочем, WPA поддерживают практически все современные точки доступа, поэтому сейчас можно было бы и не упоминать об алгоритмах шифрования. Но я физически не могу ознакомиться со всеми моделями всех производителей. Может, где-то есть ультрапростые и ультрадешевые точки доступа, которые не поддерживают WPA, а вы присмотрели именно такое устройство из-за его дешевизны.

14.4.5. Дополнительные функции

Перед покупкой точки доступа очень важно ознакомиться с ее дополнительными возможностями. Как минимум, у каждой точки доступа должен быть порт для подключения к коммутатору проводной Ethernet-сети. Схема сети в этом случае будет такой, как показано на рис. 14.12.

Некоторые точки доступа сочетают в себе функции коммутатора. Правда, портов совсем немного (обычно 4 или 8), но для небольших домашних и офисных сетей — это решение. Тогда схема сети будет значительно проще (рис. 14.13).

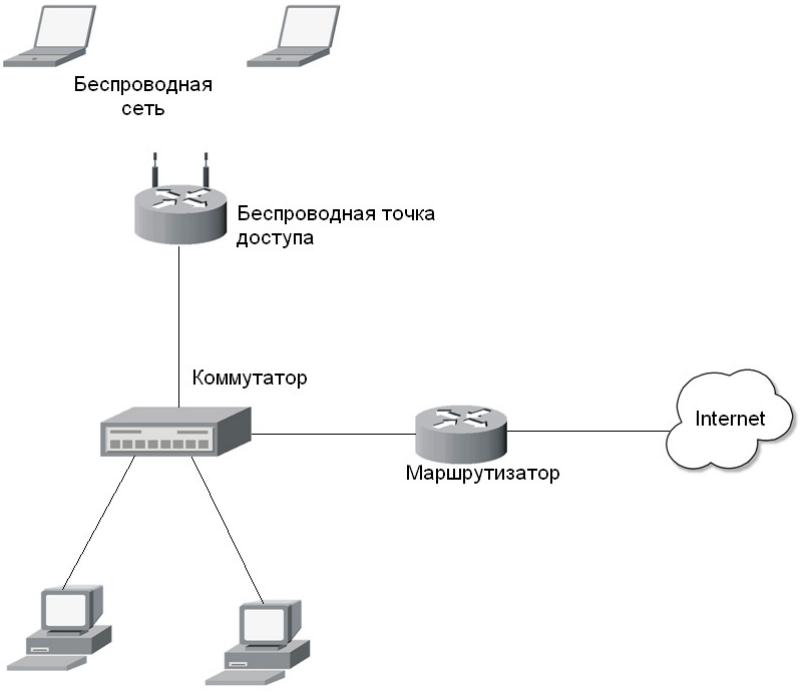


Рис. 14.12. Схема сети с обычной точкой доступа

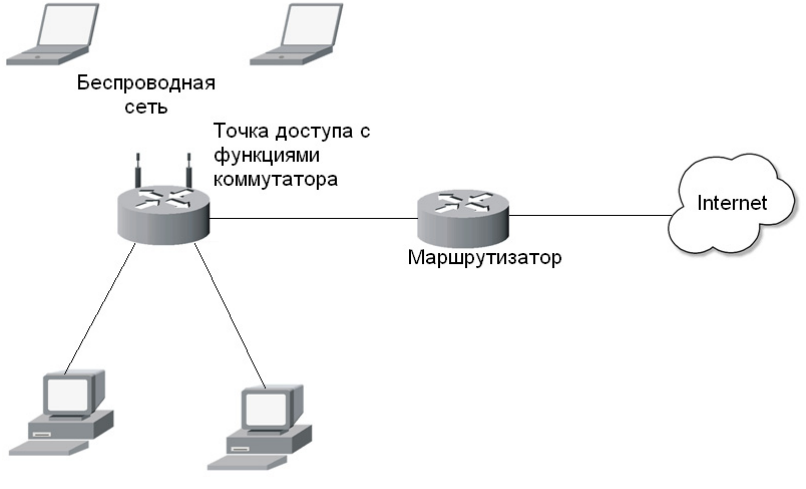


Рис. 14.13. Небольшое упрощение схемы сети

Но обратите внимание: у нас маршрутизатор все еще выступает в виде отдельного устройства. Это может быть аппаратное устройство, к которому подключается DSL-модем, или же компьютер, к которому мы подключили DSL-модем и установили специальное программное обеспечение, выполняющее функции шлюза. Но можно сделать нашу сеть еще проще. Имеются точки доступа с функциями и маршрутизатора, и брандмауэра. В этом случае мы получаем одно единое устройство, которое будет полностью обслуживать нашу сеть (рис. 14.14).

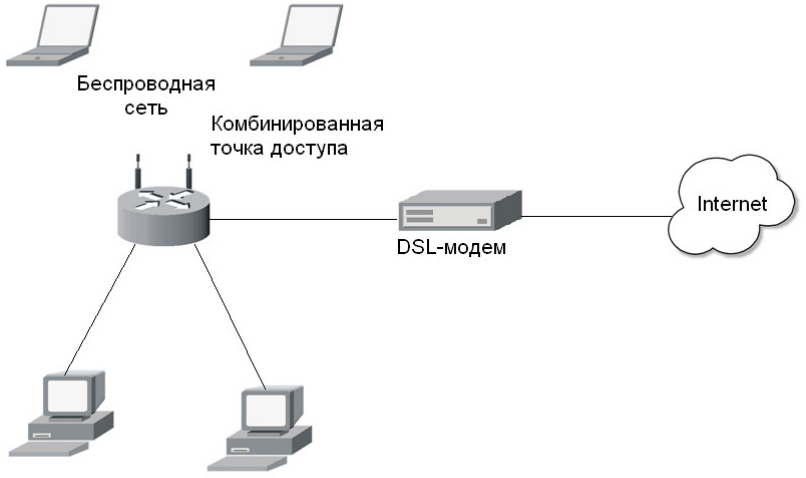


Рис. 14.14. Упрощение схемы сети с помощью комбинированной точки доступа

Теперь, когда вы знаете все нюансы выбора точки доступа, можете отправляться в магазин (конечно же, в интернет-магазин — там дешевле) за покупкой. Конкретные модели описывать я не стану, поскольку модельный ряд, как и цены, периодически обновляются.

14.4.6. Загадочный стандарт 802.11g+

На коробках точек доступа некоторых производителей (например, Encore) красуется надпись "802.11g+". При этом производитель гарантирует скорость в 100, 108 и даже 125 Мбит/с, о чем указано на коробке.

Знайте, что в природе стандарта 802.11g+ как такового не существует. То, что некоторые производители называют 802.11g+ или SuperG, является

расширением стандарта 802.11g. Но беда в том, что все производители по-разному реализуют данное расширение, и нет никакой гарантии, что, скажем, адаптер 802.11g от Intel будет работать с точкой доступа, например, Encore, на скорости 108 Мбит/с.

Мне удалось протестировать подобную комбинацию: на моем ноутбуке (HP) установлен адаптер Broadcom 802.11g. Когда я подключался к точке доступа Encore, на коробке которой красовалась надпись 108 Мбит/с, то реальная скорость была всего 54 Мбит/с.

Если вы хотите получить максимальную скорость, то нужно купить адаптеры этого же производителя или совместимые с ним. Другими словами, при покупке точки доступа "стандарта" 802.11g+ лучше не рассчитывать на максимальную скорость порядка 100 Мбит/с, но 54 Мбит/с вы получите в любом случае.

Глава 15

Настройка беспроводной сети

15.1. Выбор расположения точки доступа

Настройка точки доступа — не очень сложный процесс. Обычно программа конфигурации позволяет установить основные параметры, что займет 5–10 минут, и после этого ваша сеть готова к работе. Но вот *как* она будет работать, напрямую зависит от размещения точки доступа. Если у вас небольшое, квадратное (или около того) в плане помещение, площадью примерно 60 кв. метров, то лучше всего разместить точку доступа в центре этого помещения. С учетом материала стен, наличия радиопомех и некоторых бытовых приборов (напр., микроволновок) можно рассчитывать на радиус действия точки доступа порядка 35 метров. Некоторые точки доступа в зависимости от мощности передатчика и типа антенны могут охватывать куда большие расстояния: от 45 до 100 метров. При наружном размещении точки можно рассчитывать на минимальный радиус действия 60 метров, максимальный — 300 метров (табл. 15.1).

Таблица 15.1. *Радиус действия точки доступа с всенаправленной антенной*

Использование точки доступа	Минимальный радиус, м	Максимальный радиус, м
Внутри помещения	35	100
За пределами помещения	60	300

Примечание

В этой книге мы уже не раз обращались к теме радиуса действия точек доступа (напр., в *главе 14*), причем приводимые цифры могли от раздела к разделу несколько отличаться в ту или иную сторону. Тут надо понимать, что никакой абсолютной конкретики в этом вопросе быть не может, и минимальные/максимальные величины сильно подвержены колебаниям в зависимости от значительного количества условий.

При планировании размещения точки доступа я бы рекомендовал ориентироваться на минимальный радиус действия, поскольку максимальный зависит от слишком многих факторов, включая модель точки доступа, наличие помех, материал стен и даже время года! Так, если вы разворачиваете беспроводную сеть во дворе (то есть за пределами помещения), то зимой радиус действия будет больше, чем летом. Дополнительные помехи создает листва — зимой ее просто нет. Поэтому при построении наружных сетей старайтесь установить внешние антенны выше крон деревьев. Во всяком случае, всегда нужно помнить об эффекте листвы при планировании наружной сети.

Если вам требуется охватить большое помещение, протяженностью, скажем, в 70–80 метров, лучше не рассчитывать, что одна точка доступа обеспечит всю зону покрытия, — в этом случае следует разместить две точки доступа. Но разместить их нужно правильно. На рис. 15.1 приведены варианты не совсем правильного расположения точек доступа в прямоугольном помещении. На рис. 5.1, *а* они расположены слишком близко к граничным стенам помещения, поэтому охватывают соседнюю территорию, а в центре помещения образуется огромная "мертвая" зона, где нет беспроводной связи.

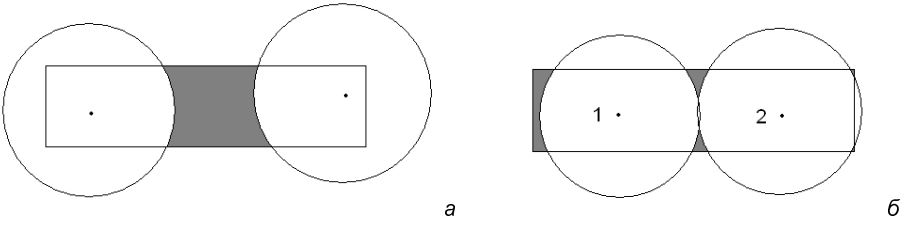


Рис. 15.1. Неправильное расположение точек доступа:
а — "мертвая" зона в центре помещения;
б — в центре сигнал слабый, слева — "мертвая" зона

На рис. 15.1, *б* точки доступа расположены намного лучше, но тоже не идеально. Здесь они смещены ближе к центру помещения. Поскольку помещение узкое, мощность передатчиков немного снижена — чтобы зона покрытия чуть меньше (по сравнению с расположением точек доступа на рис. 15.1, *а*) выходила за пределы помещения. Слева наблюдается небольшая "мертвая" зона, а в центре помещения — слабый сигнал. Чтобы избавиться от этих недостатков, нужно точку доступа 1 сдвинуть на пару метров влево. Точку доступа 2 тоже нужно сдвинуть немного влево, но при этом не перестараться, иначе справа появится такая же "мертвая" зона, как была до этого слева. Если важно покрытие именно в центре помещения, то обе точки доступа следует сдвинуть ближе к центру помещения. Понятно, что реальная конфигурация

помещения может быть намного сложнее, и вполне вероятно, что вам понадобится даже три точки доступа, чтобы полностью покрыть всю территорию.

Не нужно забывать и о другом факторе — возможности одной точки доступа не безграничны. Предположим, что у нас есть идеально квадратное помещение размером 30×30 метров. Проблем с покрытием не будет — охватить такое помещение с легкостью сможет одна точка доступа. Но одна точка доступа сможет обслужить примерно 20–30 клиентов. После этого ее производительность начнет снижаться. Другими словами, пользователи будут жаловаться, что сеть медленно работает. Поэтому на загруженных участках, где предполагается одновременная работа более 20 клиентов, лучше установить несколько точек доступа из расчета 20–30 клиентов на одну точку доступа.

> ***Примечание***
>
> При выборе места расположения точки доступа не нужно забывать и об электрических розетках — ведь точки доступа надо подключить к сети напряжения. Если нет желания тянуть огромную "переноску" или делать еще одну розетку, можно выбрать точку доступа, которая получает питание по Ethernet-кабелю (технология PoE — Power over Ethernet).

15.2. Схемы сети

Итак, у нас есть план зоны покрытия сети. Теперь осталось решить, как наша беспроводная сеть будет связываться с проводной сетью. Классический вариант схемы сети изображен на рис. 15.2 — беспроводная точка доступа подключается к коммутатору локальной сети, к этому же коммутатору подключаются проводные клиенты. К коммутатору также подключен шлюз — это может быть как обычный компьютер с двумя сетевыми интерфейсами, так и аппаратный маршрутизатор. Стена на схеме символизирует брандмауэр. На обычном компьютере развернуть брандмауэр достаточно просто, а маршрутизаторы обычно оснащаются встроенными брандмауэрами. Шлюз обеспечивает доступ к WAN: обычно это Интернет.

Для домашней или небольшой офисной сети больше всего подходит (из соображений экономии) несколько иная схема, изображенная на рис. 15.3. Центральным устройством сети является интернет-центр, осуществляющий функции точки доступа, коммутатора, маршрутизатора и даже DSL-модема. Преимущества этой схемы очевидны: дешевизна и простота настройки. Вам надо будет настроить всего одно устройство, и ваша сеть будет работать. Центральное устройство стоит относительно недорого — порядка 2–4 тыс. рублей. Но недостатки, к сожалению, тоже очевидны:

- *плохая масштабируемость сети* — обычно такая комбинированная точка доступа позволяет подключить 4 (максимум 8) проводных клиента. Если

стационарных компьютеров больше, придется или оснащать их беспроводными адаптерами, или же отказаться от использования такой схемы сети. Нужно также не забывать о максимальной нагрузке на точку доступа: 20–30 клиентов. Поэтому такая схема идеально подойдет, как уже было сказано, для домашней и небольшой офисной сети, но никак не для предприятия среднего размера, где более уместной будет первая (классическая) схема;

- *слабая защита сети* — не всегда такие точки доступа оснащаются брандмауэром, а если он и есть, то его функциональность оставляет желать лучшего. Поэтому, скорее всего, в сети придется установить отдельный брандмауэр (о выборе брандмауэра и антивируса мы поговорим в *главе 19*).

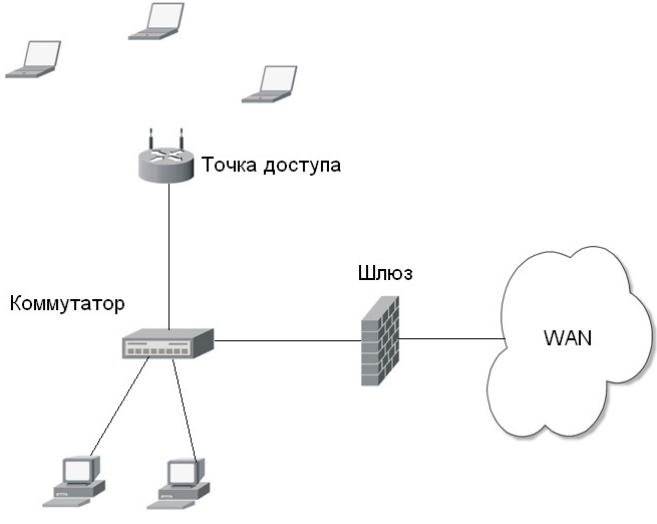


Рис. 15.2. Классическая схема соединения беспроводной и проводной сетей

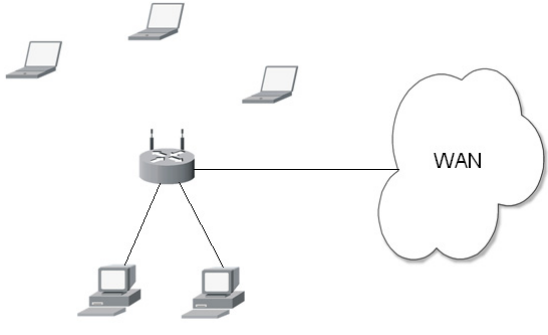


Рис. 15.3. Схема домашней сети

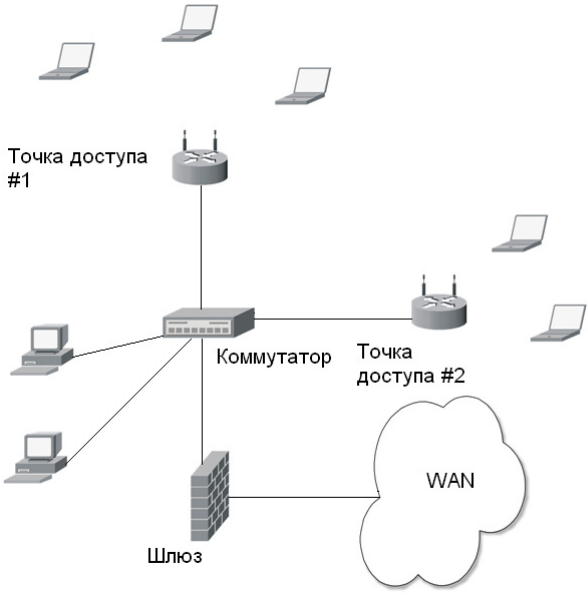


Рис. 15.4. Схема сети с несколькими точками доступа

Если у вас несколько точек доступа, то схема сети будет выглядеть, как показано на рис. 15.4. Все точки доступа подключаются к коммутатору сети, к нему же подключаются проводные клиенты и шлюз.

15.3. Точка доступа с точки зрения протокола TCP/IP

Теперь настало время поговорить о том, как точка доступа подключается к коммутатору. Ранее было сказано, что точку доступа можно рассматривать в качестве коммутатора для беспроводных клиентов. Это не совсем так. Точка доступа — это как бы коммутатор и одновременно шлюз для беспроводных клиентов. Через точку доступа они получают доступ в локальную сеть. Для локальной сети точка доступа выглядит как отдельный "компьютер"-шлюз со своим IP-адресом.

На каждой точке доступа по умолчанию развернут DHCP-сервер, который может конфликтовать с DHCP-сервером, запущенным на шлюзе сети (см. рис. 15.2). Также нужно помнить, что DHCP-сервер точки доступа может "раздавать" IP-адреса, которые не принадлежат вашей сети. Например, адрес вашей кабельной сети — 192.168.1.0, а точка доступа может "раздавать"

IP-адреса из подсети 192.168.7.0. IP-адрес точки доступа постоянный — например, 192.168.7.252 (его можно узнать из руководства по точке доступа). Получается, что если вы сразу подключите точку доступа к коммутатору (см. рис. 15.2), то возникнут две проблемы:

- конфликт DHCP-серверов — поскольку DHCP-сервер на шлюзе ничего не знает о DHCP-сервере на точке доступа. Два DHCP-сервера будут раздавать клиентам адреса из совершенно разных подсетей;
- к коммутатору будут подключены клиенты с IP-адресами, относящимися к разным подсетям.

Поэтому перед подключением точки доступа к коммутатору кабельной сети нужно зайти в программу управления точкой доступа и установить следующие параметры:

- IP-адрес точки доступа — он должен принадлежать нашей сети;
- диапазон IP-адресов, которые будет раздавать DHCP-сервер точки доступа.

Какой DHCP-сервер использовать: на точке доступа или на шлюзе? Проще отключить DHCP-сервер шлюза, а DHCP-сервер точки доступа будет обслуживать как беспроводных, так и проводных клиентов. Ничего страшного в этом нет.

Даже на самых дешевых точках доступа можно выполнить привязку к MAC-адресу (при этом определенному клиенту будет постоянно присваиваться один и тот же IP-адрес). Иногда такую политику назначения IP-адресов используют из соображений безопасности.

Можно вообще отказаться от использования DHCP-серверов, назначив IP-адреса каждому узлу вручную, но такая схема назначения IP-адресов подойдет только для домашней сети, где вы можете получить физический доступ к каждому клиенту. Для публичных сетей такая схема совершенно не подходит — прописывать вручную IP-адреса неудобно, да и нужно как-то контролировать, какой IP-адрес занят, а какой — свободен.

15.4. Физическая установка точки доступа

Вообще, при физической установке точки доступа нужно руководствоваться инструкцией, к ней прилагаемой (ведь все точки доступа — разные). Но иногда такие инструкции оставляют желать лучшего (или же попросту нет инструкции на русском языке).

Основные действия по установке точки доступа следующие:

1. Вскройте упаковку точки доступа и, если нужно, соберите ее — например, подключите антенны, смонтируйте подставку для точки доступа, если она есть в комплекте.

2. Установите точку доступа в заранее выбранное место. Вы уже, надеюсь, определились с местом, где она должна быть установлена?
3. Антенны установите под углом 90 градусов к корпусу. Если точка доступа расположена на столе или на полке, тогда антенны (или антенну, если она одна) нужно направить вверх. Если же точка доступа расположена под потолком, то антенны следует направить вниз.
4. Подключите кабель питания. Если ваша точка доступа поддерживает PoE (электропитание по кабелю локальной сети), тогда подключите к ней Ethernet-кабель.
5. Подключите Ethernet-кабель к ближайшему коммутатору, маршрутизатору или к другой точке доступа — все зависит от схемы вашей сети.
6. Включите точку доступа.

Вот некоторые дополнительные правила правильного размещения точки доступа:

- размещайте ее на ровной горизонтальной поверхности. Если вы крепите точку доступа к стене, то нужно смонтировать ее горизонтально, а не вертикально;
- не загораживайте вентиляционные отверстия точки доступа во избежание ее перегрева;
- желательно подключать точку доступа через стабилизатор напряжения или ИБП (источник бесперебойного питания) для уменьшения риска ее повреждения при скачках напряжения и разрядах молнии.

> ***Внимание!***
>
> После физической установки точки доступа можно приступить к ее настройке. Однако тут есть один нюанс. Предположим, вы используете точку доступа, поддерживающую технологию PoE, и там, где вы собираетесь ее устанавливать, нет свободной электророзетки. Другими словами, чтобы точка доступа смогла получить питание, вы сразу подключаете ее к Ethernet-кабелю, ведущему в вашу сеть. Не нужно этого делать! Ведь запустится DHCP-сервер точки доступа, что может привести к возникновению коллизий с основным DHCP-сервером сети. Сначала нужно запитать точку доступа от обычной розетки, подключиться к ней по Wi-Fi с любого ноутбука, настроить ее, а только потом уже подключать точку доступа к существующей сети.

15.5. Практическая настройка беспроводной сети

15.5.1. Точка доступа D-Link DSL-2640U

Рассмотрим построение реальной беспроводной сети на базе точки доступа D-Link DSL-2640U. Почему я остановил свой выбор на D-Link, не спраши-

вайте — выбора как такового не было. Да и не худшая это модель. И, вообще, нельзя сказать, что D-Link — это плохо, а ZyXEL — хорошо. Нужно говорить о конкретных моделях. Среди моделей ZyXEL тоже встречаются не совсем удачные, а некоторые D-Link по своим функциям не уступают устройствам от ZyXEL, но при этом стоят ощутимо дешевле.

Полный комплект DSL-2640U изображен на рис. 15.5. Что сразу бросается в глаза — это четыре порта для организации локальной сети (то есть точка доступа поддерживает функции коммутатора), телефонный разъем RJ-11 (точка доступа выполняет функции DSL-модема). В комплекте также был DSL-сплиттер, кабель Ethernet (RJ-45) и два телефонных кабеля RJ-11 — мелочь, а приятно. Другими словами, все, что нужно для установки этой точки доступа, поставляется в комплекте с ней, и больше ничего не нужно покупать.

Рис. 15.5. Точка доступа DSL-2640U: *а* — вид спереди; *б* — вид сзади; *в* — комплект поставки

Внимание!

На задней панели этой точки доступа (впрочем, как и других устройств от D-Link), имеется загадочный порт Console и кнопка Reset. Порт Console предназначен только для сервисного персонала D-Link, а вот с кнопкой Reset нужно быть предельно осторожным! Это не перезагрузка точки доступа, как можно подумать сразу (сначала я так и подумал!), — это кнопка сброса всех настроек. То есть после нажатия этой кнопки все параметры будут сброшены к заводским значениям. Для настроенной точки доступа нажатие этой кнопки означает, что придется ее настраивать сначала.

Как выяснилось из руководства, точка доступа, помимо своих собственных функций, выполняет также функции ADSL-модема, коммутатора, маршрутизатора и брандмауэра. Брандмауэр тоже непростой. Кроме фильтрации пакетов (это стандартная функция брандмауэра), он умеет выполнять фильтрацию по MAC-адресу и содержит средства защиты от DoS-атак (атаки на отказ).

Вот другие особенности этой точки доступа:

- рабочая частота 2,4–2,484 ГГц;
- индикаторы на передней панели:
  - Power — индикатор питания;
  - Status — индикатор статуса;
  - DSL — индикатор DSL-соединения;
  - WLAN — индикатор беспроводной локальной сети (Wireless LAN);
  - четыре индикатора LAN — сигнализируют о том, что к конкретному порту подключен компьютер;
- поддержка протоколов виртуальных частных сетей: IPSec, PPTP, L2TP;
- поддержка протоколов PPPoA, PPPoE, UPnP, DNS Relay, DDNS, IGMP, SNTP;
- максимальная скорость передачи 54 Мбит/с;
- поддержка беспроводных стандартов IEEE 802.11g и 802.11b;
- поддержка схем обеспечения безопасности беспроводной передачи WPA2, WPA, TKIP, AES, WEP-кодирование с 64- или 128-битным ключом;
- поддержка QoS (Quality of Service);
- поддержка NAT;
- собственный DHCP-сервер;
- поддержка WDS (Wireless Distribution System) — форма организации взаимодействия между точками доступа;
- управление по Web-интерфейсу и протоколу SNMP (Simple Network Management Protocol);
- четыре порта Fast Ethernet (10/100 Мбит/с);
- один ADSL-порт RJ-11;
- одна съемная внешняя антенна.

С учетом набора функций, эта модель довольно неплохо подойдет как для домашнего использования, так и для небольшой офисной сети.

15.5.2. Предварительная настройка

Итак, начнем настройку нашей сети. Первым делом установите точку доступа в предназначенное ей место *(см. разд. 15.4)*. Затем подключите ADSL-сплиттер (он входит в комплект поставки) к телефонной линии. Подключите к ADSL-сплиттеру телефон и точку доступа с помощью обычного телефонного кабеля (тоже входит в комплект поставки).

Затем подключите к точке доступа все стационарные компьютеры с помощью обычного Ethernet-кабеля. Поскольку эта модель поддерживает только Fast Ethernet, можно обойтись витой парой 5-й категории (не 5E и не 6-й). О том, как самостоятельно обжать витую пару, рассказано в *главе 10*.

Практически все готово — можно приступать к настройке точки доступа. Первый доступ к ней лучше производить со стационарного компьютера или ноутбука, подключенного к точке доступа с помощью Ethernet-кабеля (он входит в состав поставки). При этом компьютер должен быть настроен на автоматическое получение IP-адреса (по умолчанию оно так и есть).

Откройте браузер и подключитесь к узлу 192.168.1.1 (по умолчанию у точки доступа именно такой IP-адрес), набрав в адресной строке: `http://192.168.1.1`. Вы увидите окно, подобное изображенному на рис. 15.6. Имя пользователя по умолчанию: `admin`, пароль: `admin` — введите их и нажмите кнопку **OK**.

> ***Примечание***
>
> На рис. 15.6 вы видите другой IP-адрес — это потому, что я подключался к реальной и уже настроенной сети и не хотелось для создания иллюстрации изменять IP-адрес точки доступа.

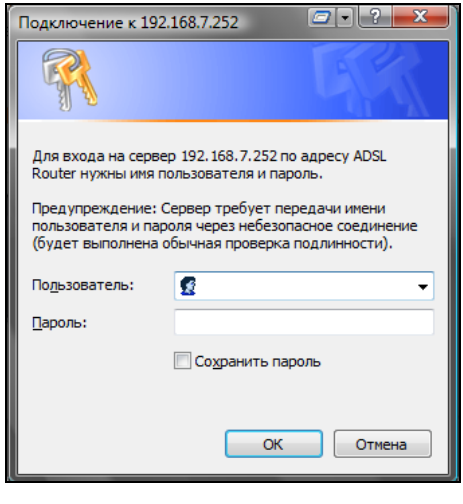


Рис. 15.6. Окно входа в программу управления точкой доступа

Прежде всего зайдите на вкладку **Home** (рис. 15.7) и на левой панели окна нажмите кнопку **Wizard**. Убедитесь, что параметр **DSL Auto-connect** включен, и нажмите кнопку **Next**.

Примечание

Мастер настройки точки доступа позволяет за несколько минут настроить точку доступа, в чем мы сейчас и убедимся. Но все иллюстрации мастера приводить я не стану. Пользователям D-Link они мало помогут — ведь на CD имеется руководство на русском языке, а пользователям других точек доступа иллюстрации программы настройки D-Link будут вообще бесполезны. Однако не нужно думать, что этот материал помещен в книгу зря. Этапы настройки и название конфигурационных параметров сходны для точек доступа всех производителей. Зная примерное название опции, вы сможете настроить точку доступа другого производителя "по образу и подобию". Настраивая D-Link, я буду комментировать процесс настройки и, кроме всего прочего, описывать опции, которым уделено мало внимания в руководстве пользователя.

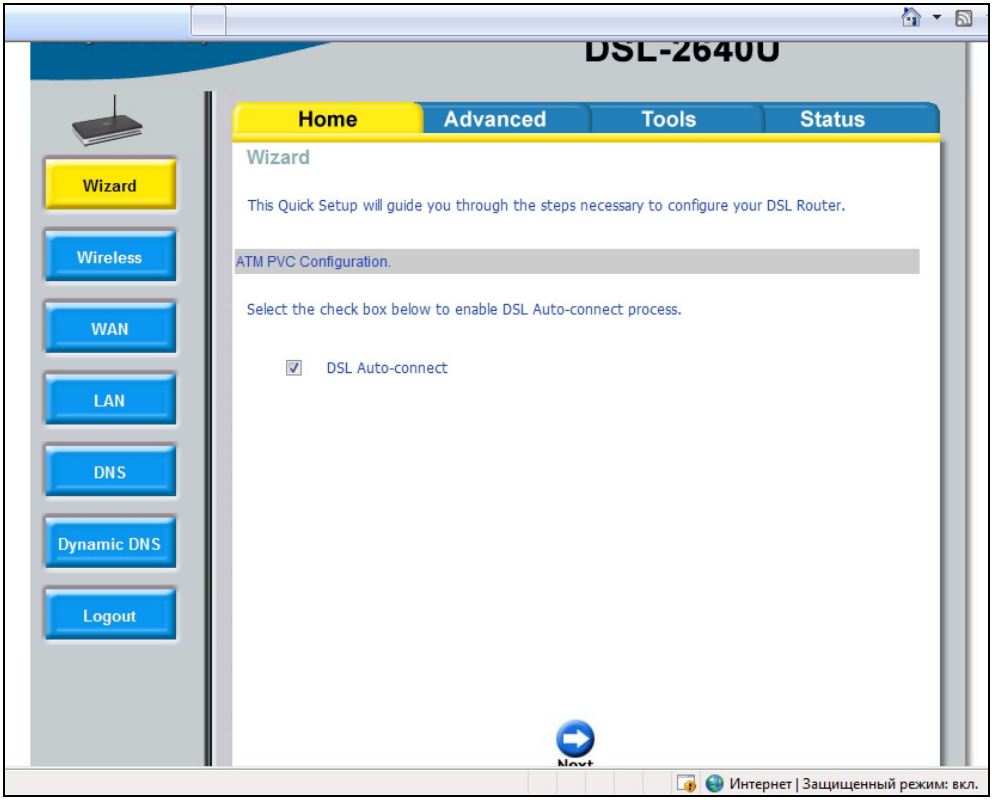


Рис. 15.7. Программа настройки точки доступа

Первым делом мастер попросит выбрать тип соединения (**Connection type**). По умолчанию выбран тип **PPPoA** (PPP over ATM), но отечественные провайдеры чаще используют другой тип соединения — **PPPoE** (PPP over Ethernet), его и нужно выбрать. Впрочем, не помешает заглянуть в договор со своим провайдером и уточнить тип соединения.

Следующий шаг — это ввод имени пользователя (**PPP username**) и его пароля (**PPP Password**). Для экономии трафика (если у вас не безлимитное соединение или соединение с почасовой оплатой) можно выбрать опцию **Dial on demand**. В этом случае соединение с Интернетом будет установлено, только если один из клиентов сети обратится к Интернету. В противном случае соединение будет установлено при включении точки доступа.

Опция **Keep Alive** разрешает поддерживать соединение с провайдером, даже если оно долгое время не использовалось. Если опции **Dial on demand** и **Keep Alive** включены, точка доступа поведет себя следующим образом: соединение с провайдером будет установлено не при запуске точки доступа, а при первом обращении к Интернету одного из клиентов. После этого соединение не будет разорвано, пока не выключат точку доступа или пока не произойдет разрыв соединения со стороны провайдера. Такая схема очень удобна для домашней сети, поскольку дома Интернет нужен не всегда. Если у вас не безлимитка, а тариф с почасовой оплатой, то при запуске точки доступа лучше не устанавливать соединение. Например, вы просто хотите скачать файл с другого компьютера локальной сети. Включаете точку доступа, она "поднимает" интернет-соединение, а вам потом придется платить за фактически не использованное время доступа к Интернету. Так что пусть точка доступа соединяется с провайдером только тогда, когда вам, действительно, понадобится Интернет. Если вы уж совсем экономны, то можно выключить параметр **Keep Alive** — при длительном простое точка доступа отключится от Интернета.

Опция **Use static IP Address** позволяет установить статический IP-адрес для вашего интернет-соединения. Обычно в этом нет необходимости, поскольку IP-адрес динамически назначается DHCP-сервером провайдера. С другой стороны, если провайдер назначает IP-адреса статически (эта услуга провайдера, как правило, платная), такая возможность иногда будет довольно полезной.

Иногда нужно указать шлюз по умолчанию (этот факт можно уточнить в службе поддержки провайдера). Для этого включите параметры **Use the following default gateway** и **Use IP Address**. Опция **Use IP Address** позволяет задать IP-адрес шлюза.

На следующем шаге можно (и нужно!!!) включить NAT и брандмауэр. Включите параметры **Enable NAT** и **Enable Firewall** и нажмите **Next**.

Далее установите следующие параметры:

- **IP Address** — IP-адрес точки доступа (по умолчанию 192.168.1.1), в принципе можно не изменять, если у вас нет существующей Ethernet-сети, к которой вы подключаете точку доступа. Если такая сеть есть, надо ввести свободный IP-адрес, принадлежащий этой сети. В любом случае из соображений безопасности (об этом мы поговорим в *главе 17*) рекомендуется изменить IP-адрес точки доступа на какое-либо значение, отличное от установленного по умолчанию. IP-адрес точки доступа не должен принадлежать диапазону динамических IP-адресов, которые будут "раздаваться" DHCP-сервером (см. далее);
- **Subnet Mask** — маску подсети (по умолчанию 255.255.255.0) при настройке новой сети можно не изменять. Если вы подключаете точку доступа к существующей сети, нужно указать ее маску;
- **Disable DHCP** — позволяет отключить DHCP-сервер. Этот параметр нужно установить, если вы планируете использование отдельного DHCP-сервера (вы должны знать, как настроить такой сервер!);
- **Enable DHCP** — включить DHCP-сервер. Здесь же можно установить его параметры:
  - **Start IP Address** — начальный IP-адрес диапазона IP-адресов, из которого DHCP-сервер будет назначать адреса (по умолчанию 192.168.1.2). Если вы настраиваете новую сеть, это значение можно не изменять. А при подключении точки доступа к существующей сети вы должны знать, какой диапазон IP-адресов у вас занят, а какой — свободен;
  - **End IP Address** — конечный IP-адрес диапазона IP-адресов;
  - **Leased Time** — время аренды IP-адреса в часах (значение по умолчанию — 24 часа). Через 24 часа DHCP-сервер назначит всем клиентам, работающим 24 часа подряд, новые IP-адреса.

СОВЕТ

Как уже здесь несколько раз отмечалось, если вы настраиваете новую сеть, то можно оставить все параметры по умолчанию. Однако из соображений безопасности ряд параметров рекомендуется изменить — например, назначить точке доступа другой IP-адрес, скажем, 192.168.1.99. А диапазон IP-адресов DHCP-сервера установить так: 192.168.1.1 — 192.168.1.98. Вам мало 98 адресов? Не забывайте, что эта точка доступа может обслужить одновременно всего 30 беспроводных клиентов и 4 проводных. Как мне кажется, 98 адресов должно хватить с головой.

Следующий шаг в настройке точки доступа — это установка параметров беспроводной сети:

- параметр **Enable Wireless** позволяет включить функции беспроводной точки доступа. В принципе, вы можете использовать точку доступа в качестве маршрутизатора для проводных клиентов и отказаться от использования беспроводного доступа к сети, если он вам в данное время не нужен. Для этого нужно выключить параметр **Enable Wireless**. Но поскольку мы сейчас настраиваем именно беспроводную сеть, то отключение этого параметра выглядело бы странным;
- параметр **SSID** задает имя (идентификатор) беспроводной сети. Измените SSID, установленный по умолчанию! SSID не должен содержать вашего адреса, номера вашего офиса или квартиры, названия вашей компании. SSID A75SN привлечет внимание злоумышленника меньше, чем VaBank-Network.

Вот и все! Теперь программа выведет установленные вами параметры. Если они верны, нажмите кнопку **Save/Reboot** для перезагрузки точки доступа с заданными параметрами.

Впрочем, это была только предварительная настройка! Представим, что нам нужно изменить какие-то параметры точки доступа, но мастера запускать не хочется. К тому же, программа конфигурации позволяет установить дополнительные параметры, которые были скрыты мастером для упрощения процесса настройки.

15.5.3. Настройка дополнительных параметров

Для изменения параметров беспроводной сети нужно перейти в раздел **Home** и нажать кнопку **Wireless** (рис. 15.8). Здесь можно включить/выключить беспроводные функции — параметр **Enable Wireless** (см. ранее). Можно также включить параметр **Hide Access Point** — после этого точка доступа прекратит широковещание своего SSID и станет скрытой.

> ***Примечание***
>
> Такой способ позволяет скрыть сеть от злоумышленников-дилетантов, которые бродят в поисках "Интернета на шару", — ведь для подключения к скрытой сети нужно знать ее SSID. Однако профессионалы-злоумышленники все равно смогут обнаружить присутствие вашей сети. Дело в том, что при передаче данных между беспроводными клиентами сети передается также и SSID сети. Достаточно перехватить один пакет, и враг будет знать название сети.

В этом окне программы настройки можно изменить и сам SSID сети. Чтобы принять сделанные изменения, нажмите кнопку **Apply**.

Рис. 15.8. Беспроводные параметры точки доступа

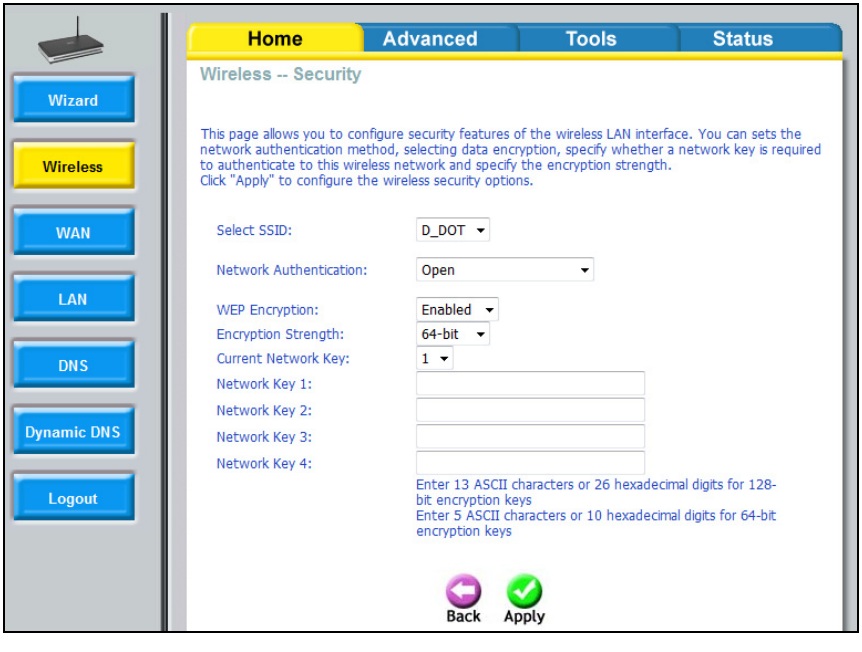


Рис. 15.9. Параметры безопасности

Затем нажмите кнопку **Security** (см. рис. 15.8). В открывшемся окне (рис. 15.9) вы сможете установить параметры безопасности вашей точки доступа. Параметр **Network Authentication** задает тип аутентификации и может принимать следующие параметры:

- **Open** — открытая аутентификация, любой пользователь может получить доступ к такой сети. WEP-шифрование отключено;
- **Shared** — включено WEP-шифрование. С помощью параметра **Encryption Strength** можно выбрать длину ключа: 64 или 128 битов;
- **802.1X** — используется только с RADIUS-сервером (Remote Authentication in Dial-In User Service), в книге мы не рассматриваем такой вариант;
- **WPA** (Wi-Fi Protected Access) — данный вид аутентификации также требует наличия RADIUS-сервера, поэтому для домашних пользователей и пользователей небольших офисных сетей совсем не интересен;
- **WPA-PSK** (Wi-Fi Protected Access — Pre-Shared-Key) — а вот этот тип WPA-шифрования подходит для домашних пользователей. Используется надежное TKIP-шифрование и управление ключами с помощью протокола WPA. Отличие от WPA заключается в том, что пароль вводится вручную в программе настройки, а не проверяется RADIUS-сервером;
- **WPA2** — улучшенная версия WPA. Вместо протокола TKIP используется более современный стандарт шифрования AES (Advanced Encryption Standard). Работает совместно с RADIUS-сервером аутентификации;
- **WPA2-PSK** — то же, что и WPA-PSK, но вместо TKIP-шифрования используется более надежное AES-шифрование. Самый надежный способ шифрования. Недостаток один — некоторые старые клиенты ничего не знают не только об AES, но и о WPA2. Такой тип шифрования подойдет для вашей частной сети, где вы используете современное оборудование, но этот способ нельзя применять для публичной сети (например, сети библиотеки, отеля и т. д.), поскольку тогда некоторые клиенты не смогут подключиться к вашей сети;
- **Mixed WPA2/WPA** — поддерживаются оба типа шифрования: TKIP и AES. Используется RADIUS;
- **Mixed WPA2/WPA-PSK** — самый универсальный способ аутентификации. Во-первых, не нужен RADIUS-сервер, и пароль можно ввести вручную. Во-вторых, поддерживаются оба тип шифрования: TKIP и AES, что расширяет круг потенциальных клиентов сети.

Что выбрать? Для домашней сети выбираем самую надежную защиту — **WPA2-PSK**. Для открытой (публичной) сети лучше выбрать **Shared** — в этом случае будет использоваться WEP-шифрование. Конечно, оно дырявое,

как швейцарский сыр, но все же лучше, чем ничего. Зато к сети сможет подключиться любой желающий. Если у вас совсем уж публичная сеть, и доступ нужно предоставлять абсолютно всем желающим без всяких паролей — выбирайте **Open**. Для офисной сети лучше выбрать **Mixed WPA2/WPA-PSK**. Я не сомневаюсь, что все ваше оборудование самое современное и будет поддерживать WPA2 и AES, но в ваш офис могут прийти клиенты с устаревшими ноутбуками, которые поддерживают только обычный WPA.

Далее вы можете указать четыре ключа (пароля): **Network Key…**. Для большей безопасности длина пароля должна быть 13 или 26 символов. Параметр **Current Network Key** позволяет выбрать текущий ключ. Очень удобно — можно сразу ввести 4 пароля, а потом выбрать один из них.

Изменить параметры DHCP-сервера можно в разделе **Home**, нажав кнопку **LAN** (рис. 15.10). Здесь же можно изменить IP-адрес точки доступа и маску подсети.

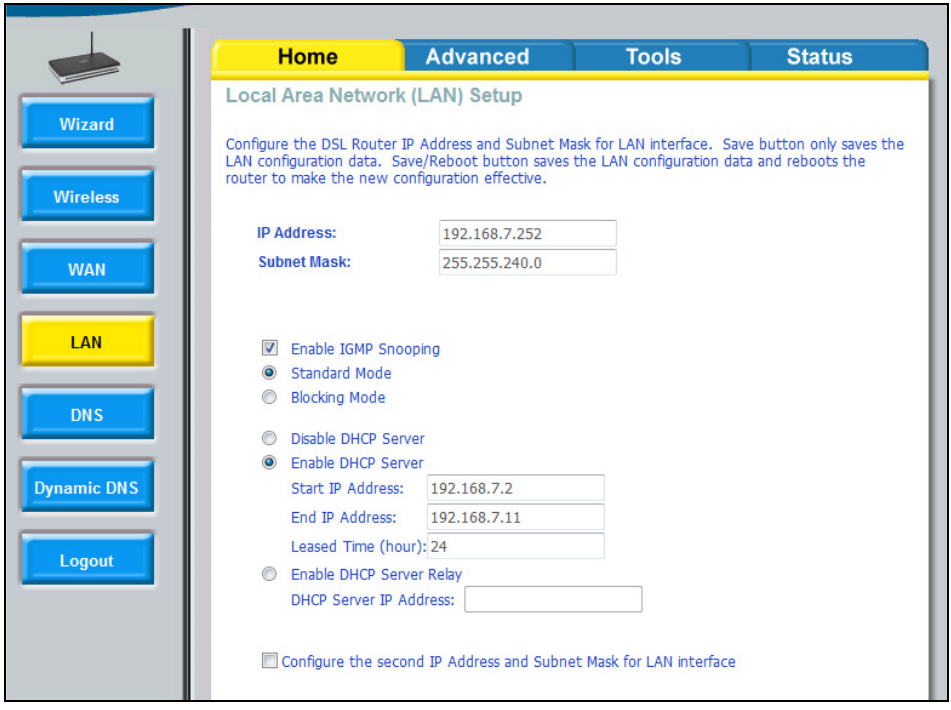


Рис. 15.10. Сетевые параметры точки доступа

Для изменения параметров DNS нажмите кнопку **DNS** (рис. 15.11). Вы можете указать два DNS-сервера: первичный и вторичный. Обычно DNS-серверы выделяются провайдером и назначаются автоматически при установке DSL-

соединения. Но иногда имена серверов нужно указать вручную, например, когда вы развернули собственные DNS-серверы, о чем мы поговорим в последней части этой книги.

Рис. 15.11. Параметры DNS

Теперь перейдите на вкладку **Status**. Кнопка **Device Info** отображает сводную информацию о точке доступа (рис. 15.12), а кнопка **DHCP Clients** (рис. 15.13) — информацию о текущих клиентах сети (о компьютерах, которые в данный момент подключены к сети). Нужно отметить, что информация, отображаемая в этом разделе, предоставляется не в реальном времени, а с определенной задержкой. Например, компьютер с именем **denix** (см. рис. 15.13) на момент создания снимка экрана был выключен! Но выключение произошло примерно минуту назад, поэтому точка доступа еще не успела обновить информацию.

В заключение раздела о настройке точки доступа расссмотрим, как можно с помощью этой точки доступа организовать классическую схему сети (см. рис. 15.2). Зайдите на вкладку **Advanced**, нажмите кнопку **Routing**, затем кнопку **Default Gateway**. Выключите параметр **Enable Automatic Assigned Default Gateway** и введите адрес шлюза в поле **Use Default Gateway IP Address**.

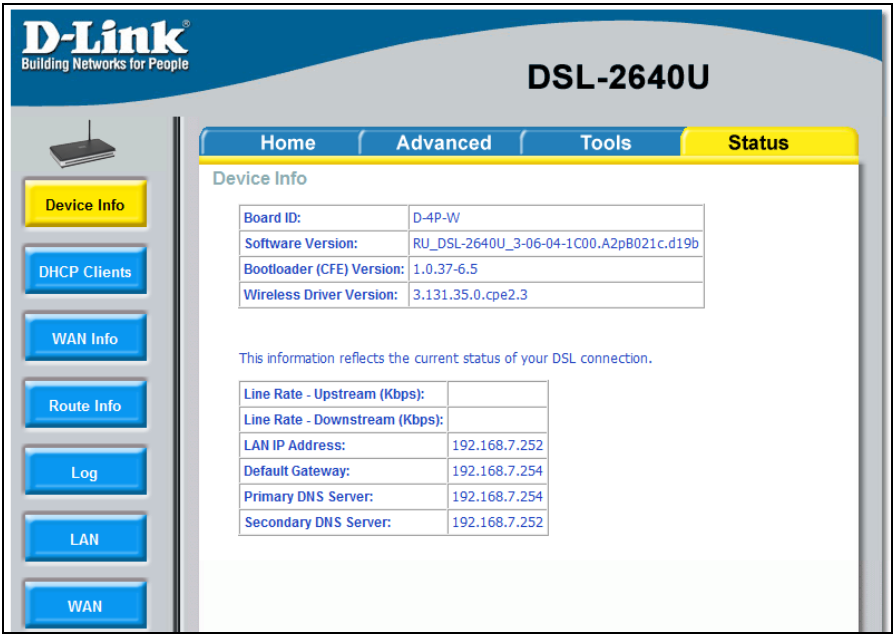


Рис. 15.12. Информация о точке доступа

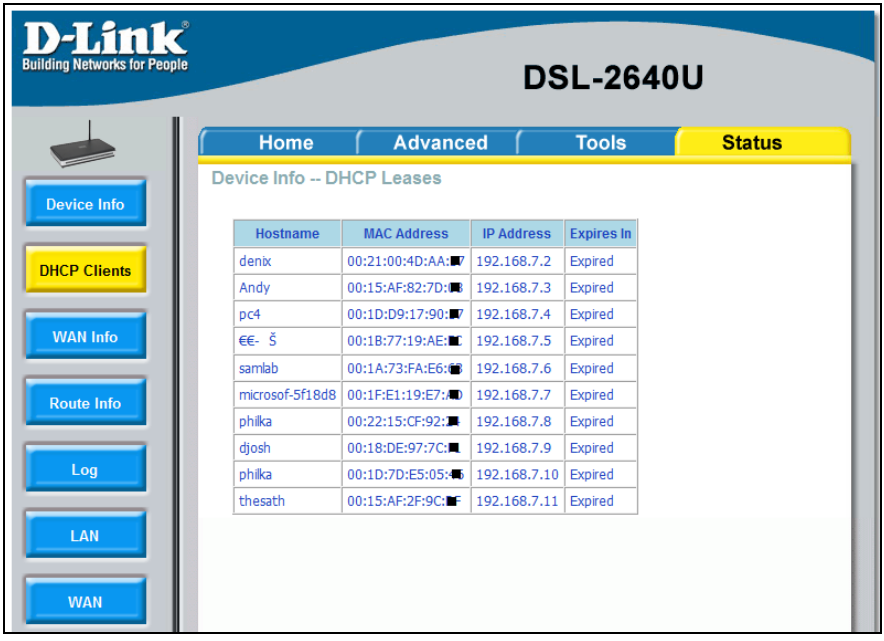


Рис. 15.13. Активные компьютеры

На этом настройку нашей сети можно считать завершенной. Но глава на этом не заканчивается. Далее вы узнаете, как бороться с проблемами интерференции и много еще чего интересного.

15.6. Проблемы интерференции

Если вы — единственный владелец беспроводной сети в радиусе 50–70 метров и рядом нет устройств, работающих на частоте 2,4 ГГц (например, беспроводных телефонов, радиоуправляемых игрушек), то можно сказать с уверенностью, что проблемы интерференции вам не страшны. Но, как показывает практика, сейчас в каждом многоэтажном доме есть несколько беспроводных сетей. Следовательно, проблемы интерференции — это более чем реально. *Интерференция* (наложение) радиосигналов приводит к снижению производительности сети. Если наложение сигналов очень сильное, ваша беспроводная сеть вообще не будет работать — радиосигналы, отправленные беспроводными адаптерами, не дойдут до получателя.

Вокруг вас достаточно много источников интерференции. Это и микроволновка, и некоторые беспроводные телефоны, и радиоуправляемые игрушки. Но все эти источники — не проблема. Их легко обнаружить, следовательно, легко устранить проблему, просто выключив устройство-источник интерференции.

Просмотрите список доступных сетей. В нем может оказаться сеть вашего соседа. Посмотрите в свойствах сети номер канала, на котором она работает. Чтобы максимально исключить интерференцию, вы должны перевести свою сеть на канал, номер которого отличается от номера другой сети на 5 единиц. Например, если сеть соседа работает на канале 11, то вам нужно перевести свою сеть на канал 6.

Бывает иная ситуация. Сосед свою сеть скрыл, но она-то работает, и наложение сигналов все равно происходит. В этом случае попробуйте просто установить другой номер канала. Экспериментируйте. По умолчанию многие точки доступа используют или номер 1, или номер 11. Попробуйте установить номер канала 5 или 6. Можно, конечно, обойти ближайших соседей и узнать, используют ли они беспроводную сеть, и на каком канале она работает.

Изменить номер канала можно в настройках точки доступа. В случае с D-Link перейдите на вкладку **Advanced** и нажмите кнопку **Wireless**. Номер канала точки доступа задается параметром **Channel**, а параметр **Preamble type** позволяет изменить тип преамбулы *(см. разд. 13.6.1)*: **long** (длинная) и **short** (короткая). Напомню, длинная преамбула более универсальна (ее будут поддерживать как современные, так и "древние" клиенты), но короткая позволяет повысить производительность сети.

Снизить интерференцию можно также путем перемещения вашей точки доступа. Иногда стоит перенести точку доступа на метр в сторону, и результат будет довольно ощутим. Также помогает использование направленных антенн — они позволяют существенно сократить область пересечения сигналов двух сетей.

15.7. Большая сеть: несколько точек доступа

Вы можете установить несколько точек доступа в одной сети. Чтобы все точки доступа были частью одной сети, нужно установить на каждой из точек доступа одинаковый SSID, а до этого — чтобы они не мешали друг другу — надо перевести каждую точку доступа на свой канал. Чтобы максимально исключить интерференцию, "расстояние" между точками доступа должно быть не менее 5 каналов — например, можно взять каналы 1, 6 и 11. Такая схема идеально подходит для сети из трех точек доступа, области покрытия которых пересекаются.

Пользователь при выходе из области покрытия одной точки доступа будет плавно перенесен в область действия другой точки доступа — при условии, что ее сигнал сильнее. Чтобы не происходило обрыва соединения, напомню — SSID всех точек доступа одной сети должен быть одинаков.

15.8. Наружные антенны

Если вы планируете расширить свою сеть за пределы помещения, вам нужно задуматься о покупке наружной антенны. На максимальную дистанцию между точкой доступа и клиентом сети влияют следующие факторы:

- мощность передатчика;
- чувствительность антенны;
- высота антенны;
- наличие помех;
- кабель.

С мощностью передатчика и чувствительностью антенны все ясно — чем выше мощность и чувствительность, тем больше расстояние, на которое можно передать данные. К слову, для преодоления расстояния в 300 метров (например, когда нужно соединить беспроводной сетью два удаленных здания) следует использовать направленные антенны с чувствительностью 6 dBi.

Расстояние зависит также и от высоты антенны. Так, для передачи радиосигнала на 1,6 км средняя высота антенны должна быть 4 метра. Для передачи

сигнала на расстояние 4,8 км нужно поднять антенну на высоту 8,1 метра. Не следует забывать и о том, что между антеннами должна быть прямая видимость. А на высоте 4 метра прямую видимость получить довольно сложно — прохождению радиосигнала будут мешать кроны деревьев и различные здания.

Радиоволна в процессе распространения в пространстве принимает форму как бы эллипсоида вращения с максимальным радиусом в его центре (рис. 15.14). Этот эллипсоид называется *зоной Френеля*. Ослабить сигнал могут искусственные (здания) и естественные (деревья, холмы) преграды, которые попадают в зону Френеля. Рассчитать зону Френеля можно по формуле, представленной на странице **www.intuit.ru/department/network/wifi/12/3.html**. Если вручную считать не хочется, можно использовать калькулятор зоны Френеля: **http://www.nporapira.ru/ext2.doc64.html**.

Рис. 15.14. Зона Френеля

Надо также иметь в виду и затухание сигнала в кабеле. Ведь кабель, по которому сигнал передается от передатчика к антенне и от антенны к приемнику — не идеальная среда передачи данных. Каждый метр кабеля отбирает немного мощности сигнала. Следовательно, снижается максимальное расстояние. Чтобы снизить затухание сигнала в кабеле, старайтесь минимизировать его длину. Лучше проложить более длинный Ethernet-кабель от точки доступа к коммутатору, чем более длинный кабель от точки доступа к антенне.

Глава 16

Решение проблем, возникающих при эксплуатации беспроводной сети

16.1. Компьютер не определяет беспроводной сетевой адаптер

Сразу после того, как вы подключите беспроводной адаптер (USB или PC-Card), Windows должна его определить. Если драйвер беспроводного адаптера еще не устанавливался, то вы увидите окно мастера нового оборудования, позволяющего установить драйвер. Если же драйверы установлены, Windows сразу начнет поиск беспроводных сетей.

Иногда при первом подключении устройства оно не определяется. В этом случае нужно извлечь устройство и попытаться установить его снова. USB-адаптер можно попытаться подключить к другому USB-порту.

Если же Windows не может установить устройство, хотя "видит" его, это означает, что она не может найти подходящий драйвер. Самую новую версию драйвера можно скачать с сайта производителя адаптера.

После установки драйвера откройте **Диспетчер устройств** (рис. 16.1), чтобы убедиться, что драйвер установлен корректно (у названия устройства не должно быть желтого треугольника с восклицательным знаком).

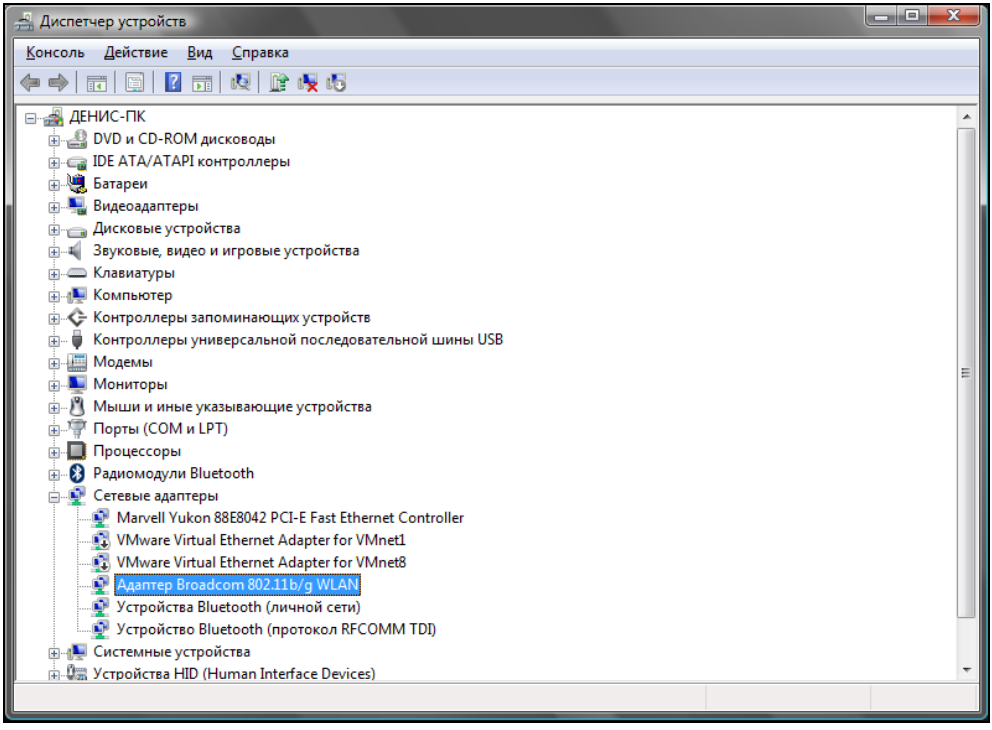


Рис. 16.1. Диспетчер устройств: драйвер беспроводного адаптера установлен корректно

16.2. Изменение длины преамбулы, номера канала и мощности передатчика беспроводной сети

Как мы уже знаем *(см. разд. 13.6.1)*, существуют два вида преамбулы: длинная (144 бита) и короткая (72 бита). Короткая преамбула более современная, но иногда при совместной работе различных устройств наблюдаются нестыковки преамбул, — ваш адаптер настроен на использование короткой преамбулы, а публичная сеть для совместимости со старыми адаптерами использует длинную преамбулу. К тому же, не у всех адаптеров есть функция автоматического выбора длины преамбулы. Поэтому вид преамбулы иногда приходится изменять. Для изменения вида преамбулы выполните следующие действия:

1. Откройте **Диспетчер устройств**.
2. Найдите в списке устройств ваш сетевой адаптер.

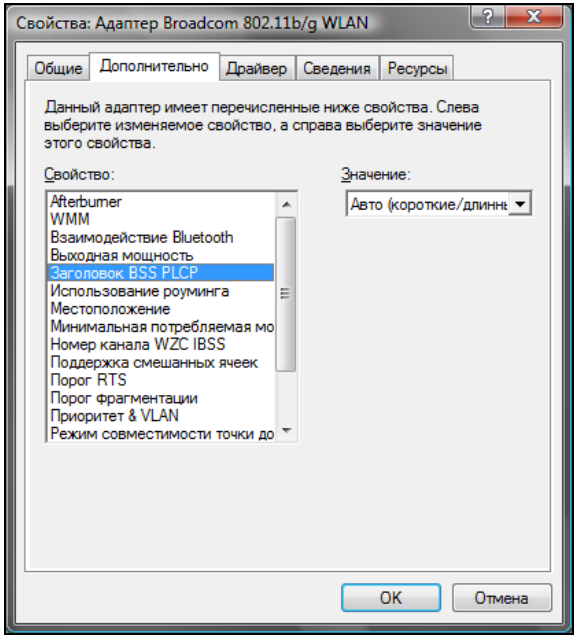


Рис. 16.2. Изменение длины преамбулы

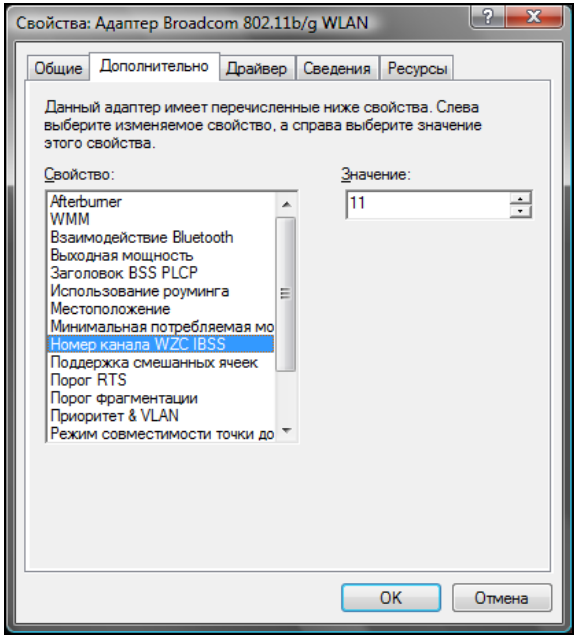


Рис. 16.3. Изменение номера радиоканала

3. Щелкните по нему правой кнопкой мыши и выберите команду **Свойства**.
4. В открывшемся окне перейдите на вкладку **Дополнительно** (рис. 16.2) и выберите свойство **Заголовок BSS PLCP** — это и есть длина преамбулы. Некоторые адаптеры поддерживают режим **Авто**. А некоторым нужно явно указать тип преамбулы: длинная или короткая.

Номер радиоканала можно изменить на той же вкладке с помощью свойства **Номер канала WZC IBSS** (рис. 16.3), а мощность передатчика — с помощью свойства **Выходная мощность**.

16.3. Проблемы с присоединением к публичной сети

У вас возникли проблемы с присоединением к публичной сети? Вы все делаете правильно, но почему-то соединение не устанавливается, хотя при правильной настройке точки доступа все должно устанавливаться автоматически. Возможно, есть какая-то несовместимость между вашим беспроводным адаптером и точкой доступа или же последняя "криво" настроена. Проверьте следующие настройки:

- правильно ли установлен SSID сети. Если широковещание SSID отключено, SSID нужно вводить вручную, и при вводе символов вы могли ошибиться;
- включено шифрование или выключено? Может, ваш адаптер не поддерживает самое современное шифрование WPA2, которое поддерживается современными точками доступа…
- возможно, включен фильтр MAC-адресов, а ваш адаптер не включен в этот список. Тут нужно обратиться к администратору;
- совпадает ли имя рабочей группы с SSID?
- правильно ли установлена длина преамбулы *(см. разд. 16.2)*?
- правильно ли выбран номер канала *(см. разд. 16.2)*?

В некоторых случаях имя рабочей группы должно совпадать с именем SSID *(см. четвертый пункт списка)*. Тут все зависит от того, как администратор настроил сеть. Для изменения имени рабочей группы в Windows XP откройте апплет **Система** из Панели управления, перейдите на вкладку **Имя компьютера** и нажмите кнопку **Изменить**. В Windows Vista изменение рабочей группы производится аналогично: **Панель управления | Система**, кнопка **Изменить параметры**.

16.4. Беспроводной клиент "не видит" локальную сеть

Вы можете подключиться к Интернету, но не можете получить доступ к ресурсам локальной сети? Возможно, дело в брандмауэре, предотвращающем несанкционированный доступ к вашему компьютеру. А заодно этот брандмауэр может блокировать доступ к локальной сети или же блокировать доступ только к вашему компьютеру — тогда другие компьютеры локальной сети не смогут использовать ресурсы вашего компьютера. Одним словом, наиболее вероятная причина — это неправильная настройка брандмауэра, и начать решение проблемы нужно с изучения документации по установленному брандмауэру. По умолчанию (если нет сторонних брандмауэров) все должно работать.

16.5. Есть доступ к локальной сети, но нет доступа к Интернету

Обратная ситуация — есть доступ к компьютерам локальной сети, но нет доступа к Интернету. Наиболее вероятная причина — это или посторонний брандмауэр, или же нужно просто заново инициализировать протокол IP.

Нажмите комбинацию клавиш <Win>+<R> и введите команду `cmd`. Откроется командная строка, введите в нее последовательно две команды:

```
ipconfig /release
ipconfig /renew
```

16.6. Компьютер самопроизвольно разрывает соединение — как его восстановить

Иногда беспроводное соединение может просто исчезнуть. Такое случается не часто, но случается. Причина может быть совершенно непредсказуемой — это или сильная интерференция, или зависание точки доступа, или другая кратковременная проблема. Намного проще восстановить соединение, чем тратить часы на поиск проблемы.

В Windows XP, чтобы восстановить соединение, щелкните правой кнопкой мыши на значке соединения и выберите команду **Исправить**.

В Windows Vista откройте **Центр управления сетями и общим доступом** (см. рис. 4.20) и щелкните на ссылке **Диагностика и восстановление**. Даже

если в открывшемся окне появится сообщение, что ошибок не обнаружено (см. рис. 4.23), нажмите кнопку **Выполнить сброс сетевого адаптера**.

Если команда исправления/сброса сетевого адаптера не помогла, извлеките беспроводной адаптер (или выключите его, если у вас ноутбук) и подключите (включите, если у вас ноутбук) к компьютеру снова через 10–15 секунд. Иногда помогает перезагрузка всего компьютера — это уже особенность Windows.

16.7. Низкое качество сигнала или слабый сигнал

Нужно различать два разных понятия: *слабый* сигнал и сигнал *плохого качества*. Уровень сигнала может быть высоким (сигнал сильный), а качество сигнала — низкое. Например, вы находитесь в нескольких метрах от точки доступа, уровень сигнала высокий, а качество — всего 50% или даже ниже. Причина, скорее всего, в интерференции радиосигналов. В *главе 15* пояснено, как бороться с этой напастью, — перевести беспроводную сеть на другой радиоканал.

Теперь рассмотрим другую ситуацию — слабый сигнал. Слабый сигнал говорит о большом расстоянии между беспроводным клиентом и точкой доступа или же о наличии существенных преград на пути следования радиосигналов. Проблемы может решить использование внешней направленной антенны, подключенной к беспроводному адаптеру удаленного компьютера. Антенну беспроводного адаптера нужно направить на антенну точки доступа. Также нужно убедиться, что мощность передатчика беспроводного адаптера равна 100% *(см. разд. 16.2)*.

16.8. Сеть работает медленно

Снижение производительности беспроводной сети может быть вызвано:

- интерференцией радиосигналов — поблизости кто-то развернул еще одну беспроводную сеть, работающую на одном канале с вашей, или же разница между номерами каналов невелика — например, ваша сеть работает на канале 1, а соседняя — на канале 3. О том, как бороться с интерференцией, рассказано в *главе 15*;
- ростом числа пользователей — если одновременно в вашей беспроводной сети работает более 20 клиентов, может наблюдаться существенное снижение производительности. Тут поможет только установка еще одной точки доступа. Помните, что точки доступа одной сети должны работать на разных каналах, иначе их радиосигналы будут накладываться;

- в вашей сети появился адаптер старого типа. Как известно, сеть 802.11g обратно совместима с адаптерами 802.11b. Но если в вашей сети есть хотя бы один старый адаптер (802.11b), вся сеть будет работать на скорости всего 11 Мбит/с, но не 54 Мбит/с.

Вообще, снижение скорости — это довольно субъективное ощущение. Предположим, вы используете беспроводную сеть для подключения нескольких ноутбуков к Интернету. Скорость интернет-соединения — 1 Мбит/с. По нынешним меркам — довольно неплохо, хотя сейчас никого не удивишь скоростью и в 10 Мбит/с. Но сейчас не об этом. Так вот, скорость вашего интернет-соединения — всего 1 Мбит/с. Даже если скорость работы вашей беспроводной сети упадет до 11 Мбит/с (например, если в сети появился старый адаптер 802.11b), то вы не заметите разницы! Интернет от этого не будет работать медленнее. Равно, как и быстрее, — даже если бы ваша сеть работала на скорости 54 Мбит/с.

А вот если вы развернули локальную сеть для доступа к общим ресурсам ваших беспроводных клиентов, тогда снижение скорости примерно в 5 раз (с 54 Мбит/с до 11 Мбит/с) сразу станет заметно — ведь большие файлы будут копироваться в 5 раз медленнее!

16.9. Беспроводной сети вообще нет...

Беспроводная сеть "упала"? Хотя всего несколько минут назад все прекрасно работало. Скорее всего, беспроводная точка доступа перегружена — такое иногда случается. Или же что-то случилось с вашим интернет-соединением. А может, что-то случилось с питанием точки доступа?

Итак, проверьте следующее:

- горит ли индикатор Power — это означает, что с питанием все в порядке;
- горит/мерцает ли индикатор WLAN (у вас он может называться иначе) — это признак того, что "по воздуху" передаются данные. Если этот индикатор не горит (или горит желтым светом), это означает зависание точки доступа. Выключите и включите ее снова;
- горит ли индикатор WAN (ADSL). Если он не горит, что-то случилось с интернет-соединением. Можно попробовать перезагрузить точку доступа. Если и это не поможет, пора звонить в службу поддержки провайдера.

Часть V

Защита сети

Пятая части книги посвящена безопасности вашей сети. Мы рассмотрим обеспечение безопасности средствами как точки доступа, так и VPN, поговорим о выборе брандмауэра и антивируса, защите маршрутизатора, а также познакомимся с дополнительными утилитами, позволяющими обнаружить вирусы в Windows.

Глава 17

Защита беспроводной сети

17.1. Беспроводные сети небезопасны

Настраивая и используя Wi-Fi-сеть, помните, что беспроводные сети небезопасны. Я бы никогда не порекомендовал использовать Wi-Fi-сеть для объединения компьютеров, хранящих конфиденциальную информацию, потеря или кража которой может стать причиной крупных финансовых проблем. Точно так же — не следует через Wi-Fi-сеть выполнять операции, связанные с электронным банкингом. А публичные сети, развернутые в аэропортах и гостиницах, — это, вообще, отдельная тема для разговора. Если вы часто путешествуете и не можете обойтись без чтения своей электронной почты, то во избежание перехвата вашего пароля к электронному ящику, лучше на время путешествия завести отдельный ящик и перенаправить на него почту с основного ящика. Даже если у вас похитят пароль от временного ящика, никто не будет знать пароль вашего основного e-mail. То же самое касается и мессенджеров: ICQ, Jabber, Skype — на время путешествия лучше обзавестись временными учетными записями.

Самое неприятное, что инструкции по взлому беспроводной сети доступны в Интернете всем желающим, а учитывая наличие программ, делающих за злоумышленника всю рутинную работу, для взлома беспроводной сети не нужно обладать какой-то особой квалификацией — взломать беспроводную сеть порой под силу даже школьнику или студенту-первокурснику.

Безопасность беспроводной сети можно сравнить с безопасностью автомобиля. При желании можно угнать даже автомобиль, оснащенный самой современной спутниковой сигнализацией. Но тут уже решать вам: или установить современную хорошую сигнализацию, которая пресечет 90% попыток угона, или даже не закрывать двери своего автомобиля — зачем, ведь все равно сопрут?! Не знаю, как вы, но я сторонник первого способа — хорошей охранной системы. В этой главе мы попытаемся защитить, правда, не автомобиль, а свою беспроводную сеть.

При правильной настройке сети можно отсечь до 90% попыток взлома. Оставшиеся 10% — тоже много, но если злоумышленник не будет точно знать, что в вашей сети есть что-то интересное, что потом можно или выгодно продать, или использовать против вас, тогда он выберет другую сеть, которую ему будет взломать намного проще. Обычно беспроводные сети взламываются с целью получения бесплатного доступа к Интернету. Зачем тратить время и взламывать вашу, хорошо защищенную сеть, если рядом есть соседская сеть, практически доступная всем?

Прежде чем приступить к рассмотрению конкретных способов защиты вашей сети, давайте еще раз вспомним, почему беспроводные сети не безопасны. Все дело в том, что данные передаются "по воздуху", следовательно, перехватить их намного проще, чем данные, передаваемые по кабелю. В среднем, радиус действия беспроводной сети — 45 метров, и сигналы сети без особых проблем выйдут за пределы квартиры или офиса. А за пределами вашей территории намного сложнее контролировать злоумышленников. Поэтому в ваших интересах сделать свою сеть неинтересной для взломщика.

17.2. Десять шагов к безопасной беспроводной сети

17.2.1. Изменение параметров по умолчанию

Нужно обязательно изменить стандартные пароль администратора и идентификатор SSID, задающий имя сети. Пароли администратора и идентификаторы SSID в большинстве случаев свободно доступны в Интернете для большинства моделей беспроводного оборудования. А это означает, что злоумышленнику достаточно выяснить модель вашей беспроводной точки доступа, чтобы получить к ней доступ, предварительно узнав стандартные SSID и пароль администратора.

При изменении SSID помните, что новый SSID не должен содержать название вашей компании, адрес, вашу фамилию, номер телефона и прочую общедоступную информацию. Отнеситесь к SSID как к паролю — используйте символы разного регистра и цифры.

Также не забудьте изменить IP-адрес точки доступа! По умолчанию IP-адрес многих точек доступа одинаков и известен всем — 192.168.1.1. Можно изменить его, например, на 192.168.1.211. Ведь для проникновения в панель управления точки доступа, злоумышленнику нужно знать ее IP-адрес. Изменив стандартный IP-адрес, вы доставите злоумышленнику больше неудобств.

17.2.2. Отключение широковещания SSID

Многие точки доступа по умолчанию транслируют всем свой SSID. Поэтому к вашей точке доступа может подключиться любой нежелательный гость, даже непреднамеренно, — человек просто запустит поиск сети и найдет вашу точку доступа.

С другой стороны, отключение широковещания недопустимо для публичной сети. На то она и публичная, чтобы ее смогли найти пользователи.

17.2.3. Используйте WPA или WPA2

Протоколы WPA (Wi-Fi Protected Access), WPA2 и WEP (Wired Equivalent Privacy) обеспечивают защиту и шифрование данных, передаваемых беспроводной точкой доступа и беспроводным клиентом. Предпочтительнее использовать WPA2, но если этот протокол не поддерживается, следует использовать WPA. Взломать защиту WEP можно с помощью ряда стандартных инструментов, а это значит, что взлом WEP — весьма обычная процедура. Шифрование WEP заметно хуже, чем WPA, но это лучше, чем вообще ничего.

> ***Примечание***
>
> По адресу **http://www.thg.ru/network/20050806/index.html** вы найдете пошаговую инструкцию взлома протокола WEP.

На смену WEP пришел протокол WPA. Для управления ключом и шифрования в WPA применяются несколько алгоритмов, в их числе TKIP (Temporal Key Integrity Protocol) и AES (Advanced Encryption Standard). Для использования WPA необходимо, чтобы все клиенты были совместимы с этим протоколом (не говоря уже о точке доступа). Впрочем, все современные точки доступа поддерживают WPA.

При шифровании данных, которые передаются между точкой доступа и беспроводным клиентом, протоколы WPA и WEP используют специальный ключ (пароль). Завладев ключом, злоумышленник сможет не только установить соединение с беспроводной точкой доступа, но и расшифровать данные, передающиеся между клиентами беспроводной точки доступа.

Если используется протокол WEP, то ключ приходится вводить вручную. Это существенный недостаток, поскольку пользователи вводят ключ всего лишь раз, а затем им его менять лень. Протокол WPA периодически сам меняет ключ, причем делает он это автоматически. Даже если злоумышленник каким-нибудь образом узнает ключ, то он будет действовать только до момента изменения ключа беспроводной точкой доступа. Во многих точках доступа ключи меняются один раз в час.

17.2.4. Фильтрация MAC-адресов

Вы можете указать список MAC-адресов адаптеров компьютеров, которые смогут получить доступ к вашей точке доступа (рис. 17.1). Нужно отметить, что фильтрация MAC-адресов не обеспечивает надежной защиты, а служит просто дополнительным барьером. Опытный злоумышленник всегда сможет перехватить MAC-адреса и подменить свой адрес одним из разрешенных адресов. Зато фильтрация MAC-адресов эффективно срабатывает против дилетантов. Это как сигнализация в автомобиле: какая бы она ни была хорошая, опытный злоумышленник обойдет ее, а вот дилетанты и близко к машине не подойдут.

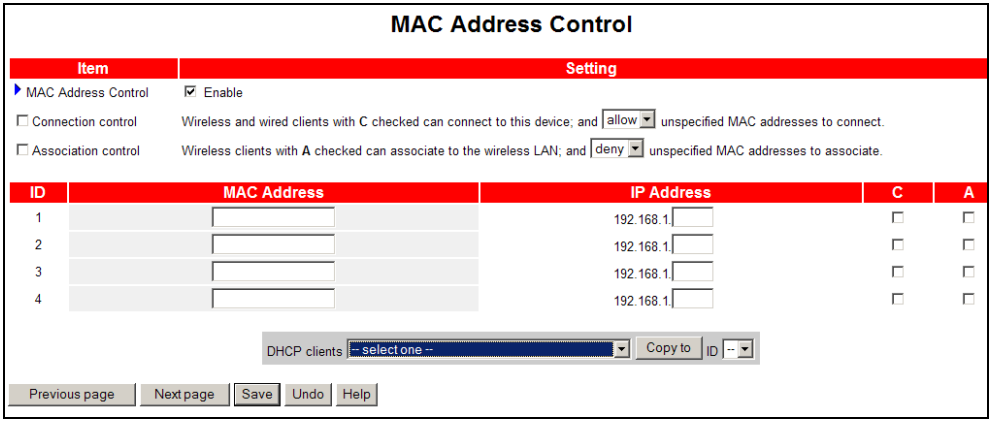


Рис. 17.1. Фильтрация по MAC-адресам

Вы немного удивлены, что MAC-адрес можно перехватить и изменить? Перехват MAC-адреса сетевых адаптеров, работающих в беспроводной сети, возможен, если злоумышленник находится в радиусе действия сети. Поскольку пакеты передаются "по воздуху", перехватить их с помощью специальной программы, например, с помощью NetStumbler, — вообще не проблема. Что же касается изменения MAC-адреса, то это — довольно-таки тривиальная задача для квалифицированного пользователя. А в Linux вообще есть штатные средства для изменения MAC-адреса.

Примечание

Как изменять MAC-адрес, я показывать не буду даже в общеобразовательных целях. Мало ли к кому в руки попадет эта книга, а вот вы, как администратор, должны знать, что подделать MAC-адрес можно, поэтому фильтрация по MAC-адресам — это не панацея, а всего лишь дополнительный барьер.

17.2.5. Обновление прошивки оборудования

Как уже было отмечено, все современные версии точек доступа поддерживают протокол шифрования WPA. Устаревшие версии поддерживают только WEP. Иногда с помощью обновления прошивки удается добавить точке доступа поддержку WPA. Удается, но не всегда — далеко не все производители точек доступа выпускают прошивки для своих устаревших моделей.

Но даже если у вас самая современная точка доступа, все равно рекомендуется зайти на сайт производителя — вдруг обнаружится свежая версия прошивки. Дело в том, что в новой версии прошивки могут быть устранены ошибки, имеющиеся в ее текущей версии, а также добавлены новые методы шифрования. Одним словом, обновление прошивки — дело полезное.

Выполнить прошивку можно в сервисном центре — это одно из самых правильных решений. Если сервисный центр находится далеко или нет возможности на долгое время отключить беспроводную сеть, тогда инструкции по перепрошивке точки доступа можно скачать с сайта ее производителя. Там же можно скачать и новую версию прошивки.

17.2.6. Использование аутентификации

Протоколы WPA и WPA2 значительно лучше, чем WEP, но и они все же уязвимы. Да, взлом WPA/WPA2 довольно сложен, но все же возможен — в Интернете можно найти пошаговые инструкции взлома всех применяемых протоколов шифрования.

Что же делать? Единственный выход — это использование *аутентификации* (рис. 17.2). Аутентификация требует от клиента регистрации в сети и может производиться с помощью сертификатов или с помощью паролей, которые проверяются на сервере аутентификации. Протоколы WEP, WPA и WPA2 поддерживают несколько типов аутентификации EAP (Extensible Authentication Protocol).

> ***Примечание***
>
> О взаимодействии протоколов шифрования WPA и WPA2 с протоколом аутентификации EAP можно прочитать по адресу **http://blogs.zdnet.com/Ou/?p=67**. Протоколы WPA и EAP и защита сети с их помощью подробно рассмотрена по адресу **http://www.ixbt.com/comm/prac-wpa-eap.shtml**.

Настройка сервера аутентификации может быть довольно сложной задачей. Тот, кто хотя бы раз настраивал RADIUS (Remote Authentication Dial-In User Service), знает, о чем я говорю. Если настраивать RADIUS не хочется, тогда можно воспользоваться альтернативными серверами доступа, например,

WSC Guard (**http://www.wirelesssecuritycorp.com/wsc/public/WirelessGuard.do**). Но данное решение далеко не бесплатно — почти 5 долларов за каждого пользователя. При желании в Интернете можно найти и бесплатные серверы доступа, более простые в настройке, чем RADIUS. Некоторые из них не всегда подходят для организаций, поскольку позволяют аутентифицировать небольшое количество пользователей.

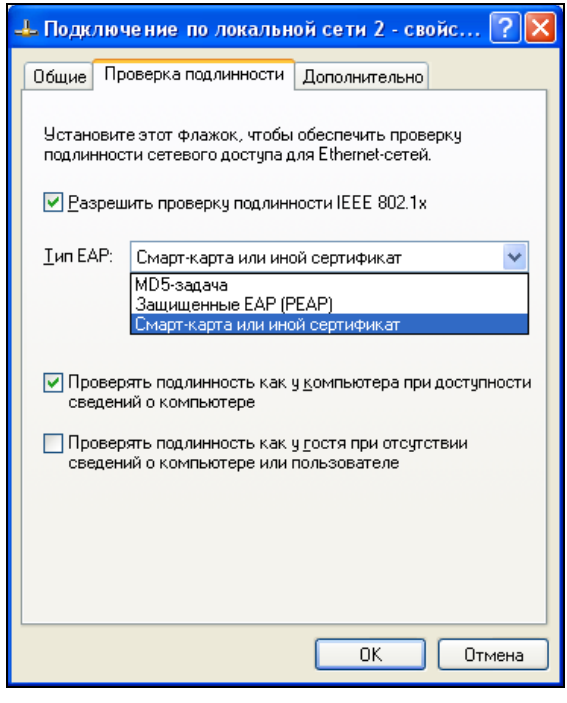


Рис. 17.2. Настройка аутентификации в Windows XP

На помощь администратору приходят методы аутентификации, не требующие сервера аутентификации: WPA-PSK и WPA2-PSK. Вам нужно только установить секретный ключ в настройках точки доступа, и она сама будет выполнять функции как бы сервера аутентификации. RADIUS-сервер будет полезен в достаточно крупных сетях, где нужно аутентифицировать не только беспроводных, но и остальных клиентов сети, — например, клиентов, подключаемых по VPN, поэтому целесообразно аутентификацию проводить через один сервер.

Помните, что WPA и WPA2 тоже можно взломать, но сделать это существенно сложнее, чем в случае с WEP. А если вы будете еще время от времени

изменять секретные ключи (скажем, хотя бы раз в месяц), то ваша сеть будет оставаться неприступной долгое время. Потом или злоумышленник потеряет к ней интерес, или все-таки взломает ее.

17.2.7. Понижение мощности передачи

Некоторые точки доступа дают возможность понизить мощность передачи, что позволяет снизить число как преднамеренных, так и случайных, несанкционированных подключений к точке доступа. Понизив мощность передачи, можно добиться того, что точка доступа будет доступна только в пределах офиса вашей компании. Вообще-то, использование мощной направленной антенны, позволяющей обнаружить даже самый слабый сигнал, сведет на нет все ваши старания, но, во всяком случае, вы оградите себя от случайных подключений к вашей точке доступа.

После понижения мощности передачи, запустите на вашем ноутбуке программу мониторинга уровня сигнала (подойдет NetStumbler: **http://www.netstumbler.com/**) и исследуйте уровень сигнала в разных частях вашего помещения. Если у граничных стен сигнал слабый, можно его еще понизить так, чтобы возле границ вашей территории сигнала вообще не было. Однако после этого нужно произвести повторное исследование уровня сигнала, чтобы убедиться, что беспроводная сеть есть там, где она должна быть.

Если у вас частный дом или отдельно стоящее офисное здание, выйдите из него и обойдите с ноутбуком здание вокруг — сигнала за его пределами быть не должно. Только так вы можете быть уверены, что никто случайно не подключится к вашей сети. Намеренное подключение с использованием направленных антенн, сигнал которых может проникать даже через стены вашего здания, исключать все же не стоит. Поэтому не нужно думать, что если вы понизили до минимума мощность передатчика точки доступа, то к вашей сети никто не сможет подключиться, и можно игнорировать остальные правила безопасности!

17.2.8. Отключайте точку доступа, когда вы не работаете

Вы работаете ночью? Нет? Тогда выключайте точку доступа, когда вы не работаете. Можно настроить автоматическое выключение, а можно выключать все самому — так вы на 100% будете уверены, что никто не проникнет в вашу сеть. Заодно и сэкономите электроэнергию. К тому же отключение точки доступа имеет и третье преимущество (первое — безопасность, второе — экономия). Точки доступа, особенно наружные и без громоотвода, желательно

выключать во время грозы, иначе разряд молнии может вывести из строя точку доступа и оборудование, к которому она подключена, например, коммутатор. Днем вы сразу заметите грозу и успеете выключить точку доступа. А вот ночью отключить ее может не получиться — дома вы будете спать и вряд ли о ней вспомните. Если же точка доступа установлена в офисе, то — тем более, вы не поедете в грозу на работу, чтобы ее выключить.

17.2.9. Защита портов управления

Интерфейсы управления беспроводной сети не должны быть доступны по беспроводной сети — все управление беспроводной сетью должно осуществляться только по внутренней (кабельной) сети. Также доступ к портам управления следует разрешить только одной-двум конкретным станциям — зачем разрешать доступ к портам управления всем компьютерам сети? Некоторые точки доступа позволяют ограничить доступ к панели управления по MAC-адресу. Введите один-два MAC-адреса: например, MAC-адрес беспроводного адаптера вашего ноутбука и MAC-адрес обычного сетевого адаптера стационарного компьютера, за которым вы чаще всего работаете.

17.2.10. Защита от внешних угроз. Общая защита сети

Помните, что антивирусы и брандмауэры никто не отменял даже в случае с беспроводной связью. Желательно установить не один общий брандмауэр/антивирус — на сервере, но и установить клиентские брандмауэры и антивирусы для защиты каждого компьютера сети в отдельности. Но только после установки не забудьте настроить их должным образом *(см. главу 19)*, а то толку от них не будет.

17.3. Дополнительная защита сети

Понятно, что описанные здесь 10 шагов можно рассматривать как базовую защиту точки доступа. Вот какие еще меры можно использовать для дополнительной защиты сети:

- чаще меняйте ключи для доступа к сети — хотя бы раз в месяц. Ключ не должен состоять только из цифр. Используйте буквы разного регистра и цифры, вот пример хорошего ключа: WoERs1815dtr2011 — только не нужно применять именно его, чтобы другой читатель этой книги не смог взломать вашу сеть ;-)

- если вы используете общий доступ к сетевым ресурсам, обязательно ограничьте его только определенными пользователями и задайте сложные пароли;
- установите антивирусы и брандмауэры *(см. главу 19)* на компьютеры вашей сети;
- включите брандмауэр на точке доступа или шлюзе, запретив доступ извне к вашей сети.

Есть еще один очень эффективный способ обезопасить вашу сеть — это использование виртуальных частных сетей (VPN). О том, как использовать VPN, мы поговорим в следующей главе.

Глава 18

Виртуальные частные сети

18.1. Предназначение VPN

Как уже было отмечено в *главе 17*, безопасность Wi-Fi-сетей оставляет желать лучшего. Скрасить ситуацию поможет *виртуальная частная сеть* (Virtual Private Network, VPN) — только с ее помощью можно обеспечить должный уровень безопасности в беспроводной сети. VPN также используют не только для дополнительного шифрования данных, но и для соединения в одно целое двух разных сетей, находящихся в различных частях страны или даже в разных странах.

Рассмотрим два сценария использования VPN.

18.1.1. Сценарий 1

Предположим, что пользователям нашей организации нужно обращаться к ресурсам корпоративной сети, когда они находятся за ее пределами, например, в другом городе. Первое, что приходит в голову, — это настроить *сервер удаленного доступа* (Remote Access Server, RAS или dial-in сервер). Пользователь с помощью модема "дозванивается" до сервера удаленного доступа, сервер аутентифицирует пользователя, после чего последний подключается к сети предприятия и работает в ней как обычно (разве что скорость передачи данных будет значительно ниже).

Но использование RAS — затея довольно дорогая и неудобная. Во-первых, нужно организовать модемный пул, а это недешево и накладно: нужна или многоканальная линия, или же несколько телефонных линий (ведь необходимо обеспечить одновременную работу нескольких пользователей). Во-вторых, нужно оплачивать междугородние и даже международные звонки пользователей (для удобства самих пользователей желательно организовать callback-режим). В-третьих, далеко не всегда у отдаленного пользователя есть возможность подключиться к телефонной сети.

Выходом из такой ситуации является использование виртуальной частной сети. В этом случае данные будут передаваться по каналам Интернета, что существенно упрощает и удешевляет задачу. Доступ к Интернету есть везде, пользователи сами смогут выбирать провайдера и способ (соответственно, и скорость) подключения к Интернету. Понятно, чтобы оградить себя от перехвата информации, данные при передаче через VPN шифруются.

18.1.2. Сценарий 2

Нам нужно соединить два филиала (подразделения) одной компании. Филиалы могут находиться как в разных зданиях, так и в разных городах. Если подразделения находятся в пределах прямой видимости, соединить их в одну сеть можно с помощью Wi-Fi-соединения (если только устроит скорость передачи данных — на 54 Мбит/с рассчитывать не приходится, скорее при "дальнобойных" соединениях придется обойтись скоростью до 11 Мбит/с). Есть и еще одна небольшая проблема — данные будут передаваться по воздуху, поэтому они окажутся легко доступны злоумышленникам.

Чтобы предотвратить хищение данных, нужно (в дополнение к методам WEP/WPA/WPA2) использовать виртуальную частную сеть. VPN создаст виртуальный тоннель для передачи данных между двумя точками доступа (они должны поддерживать VPN), при этом данные будут передаваться в зашифрованном виде.

Если же подразделения компании находятся в другой части города или в другом городе, их тоже можно соединить с помощью VPN, которая будет защищать данные, передаваемые по незащищенному интернет-соединению. Использование VPN обойдется намного дешевле, чем организация собственных каналов передачи данных и поддержание их в надлежащем состоянии.

18.1.3. Преимущества VPN

Вот основные преимущества VPN:

- не нужно никакое дополнительное оборудование (модемный пул) и какие-либо дополнительные ресурсы (например, многоканальная телефонная линия). Все, что требуется иметь, — это подключение к Интернету, а поскольку нет сейчас такого предприятия, которое не было бы подключено к Интернету, будем считать, что все необходимое для организации VPN уже есть;
- безопасность передачи данных;

- возможность как соединения филиалов компании, так и подключения отдельных пользователей к корпоративной сети. При этом мобильные пользователи могут заходить в Интернет с помощью GPRS, что делает подключение к VPN максимально гибким — пользователю не придется искать свободную телефонную розетку;
- дешевизна доступа к Интернету, следовательно, дешевизна использования VPN. Можно забыть о международных звонках и callback — пользователь подключается к местному провайдеру, платит копейки за доступ к Интернету и пользуется всеми ресурсами VPN.

Чтобы вы понимали, как работает VPN, вспомним модель OSI *(см. главу 3)*. VPN работает на сетевом уровне этой модели, поэтому VPN функционирует "поверх" любого протокола, передающего данные на нижнем уровне. VPN никак не зависит от физического уровня — вы можете физически передавать данные как по воздуху (Wi-Fi-соединение), так и по кабелю (Ethernet).

После подключения к локальной сети через VPN-сервер пользователь сможет использовать все ее ресурсы без ограничений — так, как если бы он непосредственно находился в этой сети. Конечно, скорость соединения будет ограничена физически. Если пользователь подключился к VPN через медленное GPRS-соединение, понятно, что скорости в 100 Мбит/с, которую получают остальные пользователи локальной сети, ему не видать.

Типичная реализация VPN представлена на рис. 18.1. Удаленный клиент подключается по незащищенному каналу (НК) к VPN-маршрутизатору нашей сети, после успешной аутентификации клиент подключается к нашей локальной сети. Такой способ называется соединением "клиент-сеть".

Иногда нужно защитить нашу кабельную сеть от беспроводной сети, к которой может подключиться любой желающий. Так вот — подключиться-то он сможет, но вряд ли пройдет аутентификацию на нашем VPN-сервере. В данном случае схема сети будет выглядеть, как показано на рис. 18.2. Как вы уже догадались, это один из вариантов соединения "клиент-сеть", только с уточнением — как именно будет подключаться наш клиент (по Wi-Fi).

Еще один вариант использования VPN, как было сказано ранее, заключается в связывании двух проводных сетей, находящихся в разных частях города, страны или мира в единое целое с использованием каналов Интернета. Схема сети изображена на рис. 18.3. Сети двух филиалов связываются в единое целое с помощью VPN-тоннеля, организованного "поверх" интернет-каналов. Такой способ называется соединением "сеть-сеть".

Рис. 18.1. VPN-сеть

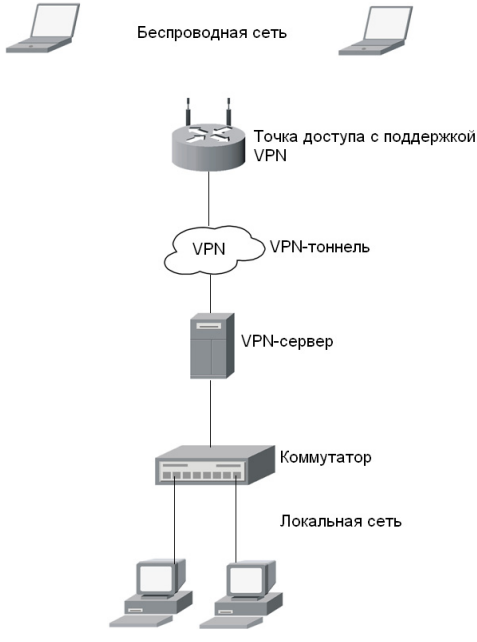


Рис. 18.2. VPN-тоннель защищает проводную сеть от пользователей беспроводной сети

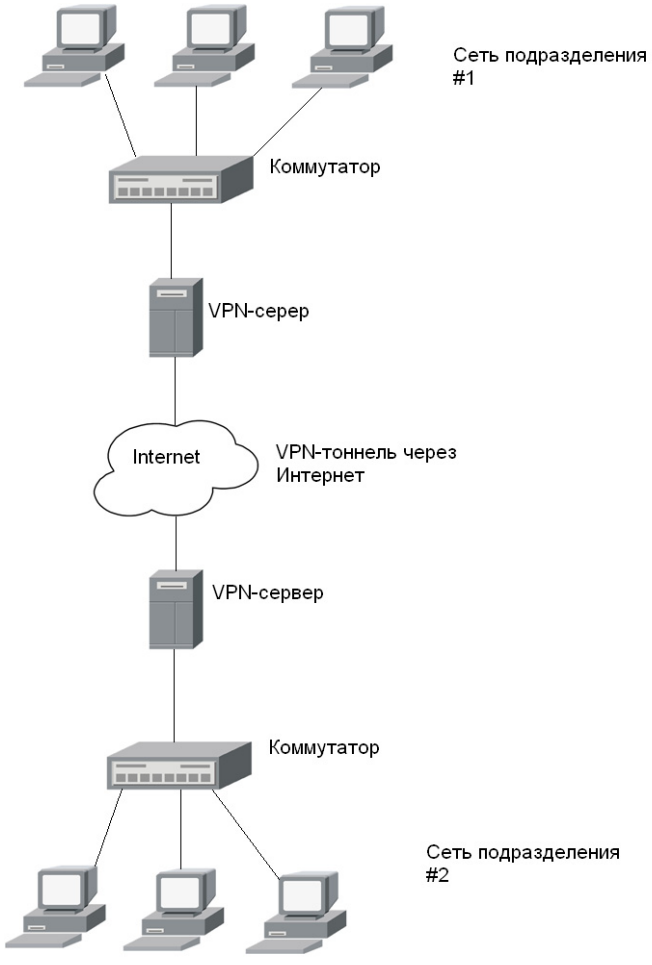


Рис. 18.3. VPN-тоннель связывает в единое целое две сети и защищает передаваемые данные

18.2. VPN-протоколы, VPN-серверы

Для организации VPN-тоннеля может использоваться один из следующих протоколов: PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol) и IPSec (IP Security). Протоколы PPTP и L2TP могут передавать данные по сетям IP, IPX и NetBEUI, а IPSec ограничен только IP-сетями. Понятно, что VPN-клиенты и VPN-сервер должны использовать один и тот же протокол.

У всех протоколов есть свои достоинства и недостатки, но разница между ними больше теоретическая, нежели практическая. Иногда выбор протокола полностью зависит от оборудования. Например, если ваши маршрутизаторы поддерживают только протокол PPTP, то вам придется использовать именно его. Если вы настраиваете программный VPN-сервер, то выбор протокола зависит от операционной системы: в Windows Server 2003/2008 вы будете использовать протоколы IPSec или L2TP, в Windows NT 4.0 или 2000 Server — PPTP или L2TP, в UNIX/Linux — IPSec или PPTP. Далее в этой главе будет рассмотрен процесс настройки VPN-серверов на базе Linux, а о настройке серверов под управлением Windows вы можете прочитать тут: **http://technet.microsoft.com/en-us/network/bb545442.aspx**.

Как вы уже поняли, VPN-сервер может быть *аппаратным* (отдельное устройство с поддержкой VPN) или *программным* — компьютер с установленной серверной операционной системой и соответствующим программным обеспечением. Аппаратные VPN-серверы (обычно это маршрутизаторы или точки доступа с поддержкой VPN) производят многие производители, в том числе Cisco, NETGEAR, TRENDnet. На сайте **http://www.vpnc.org** вы можете найти список сертифицированных устройств (устройств, которые успешно прошли испытания консорциума Virtual Private Network Consortium).

Далее мы рассмотрим практическую настройку VPN-сети на базе серверов под управлением Linux. Напомню, что VPN не зависит от физического способа передачи данных, поэтому для VPN-сети все равно, как подключится клиент к серверу — по Wi-Fi или через Интернет.

18.3. Необходимое программное обеспечение

Для организации соединений типа "сеть-сеть", то есть для связи двух сетей одной компании в одну виртуальную частную сеть, используется протокол IpSec. В Linux его реализации называется OpenS/WAN (**http://www.openswan.org**). OpenS/WAN — это потомок самой популярной Linux-реализации IpSec — FreeS/WAN (**http://www.freeswan.org**). Проект OpenS/WAN более современный и поддерживает ядра Linux 2.4 и 2.6, в то время как FreeS/WAN поддерживает только старые ядра (2.2 и 2.4).

Для подключения удаленных пользователей к корпоративной сети используется протокол PPTP (Point to Point Tunneling Protocol). Настройку этого протокола мы также рассмотрим в этой главе.

18.4. Настройка соединения "сеть-сеть"

18.4.1. Установка OpenS/WAN

По адресу **http://www.openswan.org/download/binaries/** вы найдете уже откомпилированные пакеты OpenS/WAN для дистрибутивов Fedora, Mandriva, Mandrake, OpenWRT, RHEL, openSUSE.

Перед установкой пакетов, возможно, понадобится перекомпиляция ядра. Вам нужно включить опции `PF_KEY`, `AH`, `ESP` и все опции в группе `CryptoAPI`.

> ***Примечание***
>
> Мы рассматриваем установку OpenS/WAN 2.4.*x* в систему с ядром 2.6.*x*.

18.4.2. Немного терминологии

Предположим, что нам нужно связать два офиса компании. Один расположен в Москве, другой — во Владивостоке. Посмотрите на рис. 18.4: Москва находится на западе (слева), Владивосток — на востоке (справа), поэтому московскую сеть мы будем называть *left*, а сеть Владивостока — *right*. Это не принципиально, но так принято.

Рис. 18.4. Пример VPN-сети

Понятно, что VPN-маршрутизатор будет выходить в Интернет через какой-то обычный маршрутизатор. В терминологии VPN маршрутизатор, через который подключается к Интернету левый VPN-маршрутизатор, называется *leftnexthop* (соответственно правый — *rightnexthop*).

18.4.3. Генерирование ключей

Перед настройкой OpenS/WAN нужно сгенерировать ключи на обоих VPN-маршрутизаторах. Для этого на каждом VPN-маршрутизаторе введите команду:

```
# ipsec newhostkey
```

Просмотреть ключ можно с помощью одной из команд:

```
# ipsec showhostkey --left
# ipsec showhostkey --right
```

18.4.4. Конфигурационный файл

OpenS/WAN использует один основной файл конфигурации: /etc/ipsec/ipsec.conf. Этот файл состоит из трех разделов: общие настройки (`config setup`), настройки по умолчанию (`conn %default`) и настройки соединения (`conn <название соединения>`). Понятно, что последних разделов может быть несколько, поскольку каждый такой раздел задает параметры конкретного соединения.

Рассмотрим пример раздела, содержащий общие настройки (листинг 18.1).

Листинг 18.1. Общие настройки

```
config setup
        # указывает интерфейсы, которые будут использоваться для
        # VPN-соединений
        interfaces=%defaultroute

        # управляют протоколированием KLIPS (Kernel IP Security) и
        # демоном Pluto
        klipsdebug=none
        plutodebug=none

        # Эти параметры лучше не изменять
        plutoload=%search
        plutostart=%search
```

Примечание

Табуляция перед именем директивы (именно директивы, а не раздела файла конфигурации) обязательна! Иначе при обработке конфигурационного файла будет выведено сообщение об ошибке: **... has wrong number of fields ...**.

Обратите внимание на параметр `interfaces`. В большинстве случаев подойдет значение `%defaultroute`, но можно указать имя интерфейса явно, например:

```
interfaces="ipsec0=ppp1"
```

Теперь рассмотрим раздел с настройками по умолчанию. Такой раздел вообще не обязателен, но если он есть, то обычно в нем указываются две директивы: `authby` и `keyingtries`. Первая задает метод аутентификации, а вторая — количество попыток установки соединения (по умолчанию 0, то есть соединение будет устанавливаться бесконечно, пока не будет установлено). Пример раздела приведен в листинге 18.2.

Листинг 18.2. Пример раздела настроек по умолчанию

```
conn %default

      authby=rsasig
      keyingtries=3
```

Основным разделом конфигурационного файла является раздел, описывающий настройки (параметры) VPN-соединения. Для написания этого раздела нам нужно обратиться к рис. 18.1.

В конфигурационном файле обоих VPN-маршрутизаторов нужно указать сведения, приведенные в табл. 18.1.

Таблица 18.1. *Параметры VPN-соединения типа "сеть-сеть"*

Директива	Назначение
`left`	IP-адрес левого VPN-маршрутизатора (вместо него можно указать значение `%defaultroute`). В нашем случае это 192.168.1.1
`leftsubnet`	IP-адрес левой сети. В нашем случае это 192.168.1.0/24
`leftnexthop`	IP-адрес левого маршрутизатора (можно указать значение `%defaultroute`)
`leftrsasigkey`	Ключ левого маршрутизатора (можно узнать с помощью команды `ipsec showhostkey --left`)
`leftid`	Идентификатор левой сети. Например, `@moscow.firma.ru` Можно в разделе `config setup` указать опцию `uniqueids=yes`. Это избавит вас от указания идентификаторов сети

Таблица 18.1 *(окончание)*

Директива	Назначение
`right`	IP-адрес правого VPN-маршрутизатора (вместо него можно указать значение `%defaultroute`). В нашем случае это 192.168.2.1
`rightsubnet`	IP-адрес правой сети (192.168.2.0/24)
`rightnexthop`	IP-адрес правого маршрутизатора (можно указать значение `%defaultroute`)
`rightrsasigkey`	Ключ правого маршрутизатора (можно узнать с помощью команды `ipsec showhostkey --right`)
`rightid`	Идентификатор правой сети. Например, `@vladivostok.firma.ru`
`leftfirewall`	Если левая сторона защищена брандмауэром, то нужно установить значение `yes` для этой директивы
`auto`	Управляет автоматической установкой соединений. Если указать `auto=start`, соединение будет автоматически установлено. Чтобы директива auto работала, нужно в `config setup` указать `plutostart=%search`

Пример раздела параметров соединения приведен в листинге 18.3.

Листинг 18.3. Пример раздела параметров VPN-соединения

```
conn my_vpn
       left=192.168.1.1
       leftsubnet=192.168.1.0/24
       leftnexthop=10.0.0.1
       leftrsasigkey= 0sAQtyjh9345...
       leftid=@moscow.firma.ru

       right=192.168.2.1
       rightsubnet=192.168.2.0/24
       rightnexthop=10.1.0.1
       rightrsasigkey=0sAQ65jh92...
       rightid=@vladivostok.firma.ru

       auto=start
```

Полная версия файла ipsec.conf представлена в листинге 18.4.

Листинг 18.4. Пример файла ipsec.conf

```
config setup
       # указывает интерфейсы, которые будут использоваться для
       # VPN-соединений
       interfaces=%defaultroute

       # управляют протоколированием KLIPS (Kernel IP Security) и
       # демоном Pluto
       klipsdebug=none
       plutodebug=none

       # Эти параметры лучше не изменять
       plutoload=%search
       plutostart=%search

conn %default

       authby=rsasig
       keyingtries=3

conn my_vpn
       left=192.168.1.1
       leftsubnet=192.168.1.0/24
       leftnexthop=10.0.0.1
       leftrsasigkey= 0sAQtyjh9345...
       leftid=@moscow.firma.ru

       right=192.168.2.1
       rightsubnet=192.168.2.0/24
       rightnexthop=10.1.0.1
       rightrsasigkey=0sAQ65jh92...
       rightid=@vladivostok.firma.ru

       auto=start
```

18.4.5. Установка VPN-соединения

Для запуска демона OpenS/WAN нужно выполнить команду:

```
ipsec start
```

При этом будут запущены все соединения, для которых вы указали `auto=start`. Команду `ipsec start` нужно выполнить на обеих сторонах.

Проверить, запущено ли соединение, можно с помощью команды:

```
ipsec look
```

18.4.6. Настройка утилиты *iptables*

Для работы IpSec нужно должным образом настроить утилиту `iptables`, а именно: разрешить порт 500, который используется для обмена сертификатами и ключами:

```
iptables -A INPUT -i eth0 -p udp -s $IP --sport 500 --dport 500 -j ACCEPT
iptables -A OUTPUT -o eth0 -p udp -d $IP --sport 500 --dport 500 -j
ACCEPT

iptables -A INPUT -i eth0 -p 50 -s $IP -j ACCEPT
iptables -A OUTPUT -o eth0 -p 50 -d $IP -j ACCEPT

iptables -A INPUT -i eth0 -p 51 -s $IP -j ACCEPT
iptables -A OUTPUT -o eth0 -p 51 -d $IP -j ACCEPT

iptables -A FORWARD -p all -s 192.168.2.0/24 -d 192.168.1.0/24 -j ACCEPT
iptables -A FORWARD -p all -s 192.168.1.0/24 -d 192.168.2.0/24 -j ACCEPT
```

В нашем случае:

- `$IP` — это IP-адрес шлюза на противоположной стороне, то есть: 192.168.2.1 для левой стороны и 192.168.1.1 для правой стороны;
- `eth0` — это внешний интерфейс сети;
- `ipsec0` — это VPN-интерфейс.

18.5. Настройка соединения "клиент-сеть"

В этом разделе мы рассмотрим настройку соединения "клиент-сеть", когда нужно обеспечить подключение отдельного пользователя к локальной сети. Для настройки соединения такого типа используется протокол PPTP.

Нам понадобятся следующие пакеты:

- pptpd или pptp-server — PPTP-сервер;
- pptp-linux, pptp-client, pptp-adsl — PPTP-клиент.

Названия пакетов зависят от дистрибутива и могут немного различаться. Найти указанные пакеты можно с помощью сайтов **http://rpmfind.net** (если у вас Red Hat-совместимый дистрибутив) или **http://packages.ubuntu.com** (если у вас Ubuntu или Debian).

Еще нам понадобится пакет ppp, но в большинстве случаев он устанавливается по умолчанию, поэтому вам нужно только проверить его наличие в вашей системе.

> ***Примечание***
>
> Необходимо отметить, что VPN-сервер в современных дистрибутивах настраивается на порядок проще, чем в дистрибутивах, основанных на ядре 2.4. Ведь в старых дистрибутивах вам нужно было добавить поддержку MPPE (патч) для ppp и ядра, а новых дистрибутивах, основанных на ядре 2.6, всего этого делать не нужно. Не нужно даже перекомпилировать ядро, поскольку в большинстве случаев расширение MPEE включено по умолчанию. Почему в большинстве случаев? Откуда же я знаю, какой у вас дистрибутив? Может, он у вас какой-то экзотический, разработчики которого посчитали, что MPPE вам не нужен, и отключили его.

18.5.1. Редактирование конфигурационных файлов

После установки пакета ppptd (или pptp-server) можно отредактировать его конфигурационный файл /etc/pptpd.conf (листинг 18.5).

Листинг 18.5. Конфигурационный файл /etc/pptpd.conf

```
speed 115200
option /etc/ppp/options.vpn
debug
localip 192.168.1.1
remoteip 192.168.1.12-22
```

Думаю, назначение всех опций файла понятно и без моих комментариев. Конечно, IP-адрес этого сервера (`localip`) и IP-адреса VPN-клиентов вам нужно изменить. В этом примере предполагается, что может быть максимум 10 VPN-клиентов, которым будут назначены IP-адреса из диапазона 192.168.1.12–192.168.1.22. Кроме того, чтобы основной конфигурационный файл был компактнее, дополнительные опции вынесены в файл /etc/ppp/options.vpn.

Теперь отредактируем файл /etc/ppp/options.vpn (понятно, его еще нужно создать, листинг 18.6).

Листинг 18.6. Конфигурационный файл /etc/ppp/options.vpn

```
ipparam PoPToP

lock

mtu 1490
mru 1490

ms-dns 192.168.1.1
name server.com
proxyarp
auth

refuse-pap
refuse-chap
refuse-chapms
require-mschap-v2

ipcp-accept-local
ipcp-accept-remote
lcp-echo-failure 30
lcp-echo-interval 5
deflate 0
+mppe-128
```

Этот конфигурационный файл немного сложнее, чем предыдущий. Если разбираться в деталях не очень хочется, просто измените IP-адрес DNS-сервера (опция `ms-dns`) и имя узла (опция `name`). В некоторых версиях ppp вместо опций `refuse-pap`, `refuse-chap`, `refuse-chapms`, `require-mschap-v2` следует использовать опции (соответственно):

```
-pap
-chap
-chapms
+chapms-v2
```

Эти опции управляют аутентификацией VPN-пользователя. Мы используем протокол аутентификации MS CHAP v2, как самый безопасный.

Практически все настроено. Проверьте еще раз, чтобы в файле /etc/ppp/options.vpn присутствовала опция:

```
lock
```

Имена VPN-пользователей можно определить в файле /etc/ppp/chap-secrets. Формат этого файла такой:

```
имя сервер.домен пароль IP
```

Вот небольшой пример:

```
vpn1 server.com "" *
```

Здесь: `vpn1` — имя пользователя, `server.com` — имя нашего VPN-сервера. Пароль мы указали пустой — это означает, что пароль будет браться из /etc/shadow. IP-адрес мы тоже не указывали — VPN-пользователь сможет аутентифицироваться с любого IP. Пользователь `vpn1` должен существовать в системе (добавить пользователя можно командой `adduser`).

Вот сейчас все готово. Для запуска PPTP-сервера используется команда:

```
service pptpd start (или /etc/init.d/pptpd start)
```

Не забудьте разрешить на брандмауэре прохождение пакетов на 47 порт (ведь наверняка в вашей сети есть брандмауэр).

18.5.2. Настройка Linux-клиента

В этом разделе мы рассмотрим настройку клиента, работающего под управлением Windows. Понятно, что на VPN-сервере не обязательно устанавливать PPTP-клиент.

1. Для установки VPN-клиента нужно установить пакет pptp-linux или pptp-client. После установки запустите сценарий `pptp-command`. Сценарий отобразит меню из четырех пунктов, нужно выбрать пункт **3.) setup** (рис. 18.5).
2. Вы увидите еще одно меню, в котором нужно выбрать пункт **1.) Manage CHAP secrets** (рис. 18.5), после чего выбрать команду **Add a New CHAP secret**. Сценарий попросит ввести вас имя локальной машины, имя удаленной машины (вводить необязательно), имя пользователя и пароль.
3. Затем вы вернетесь в меню настройки. Нужно будет выбрать пункт **4.) Add a New PPTP Tunnel**, а затем команду **Other**. Вам надо ввести следующую информацию: имя и IP-адрес VPN-сервера, а также параметры маршрутизации.
4. После этого надо выбрать пункт меню **6.) Configure resolv.conf** и указать IP-адреса DNS-серверов.

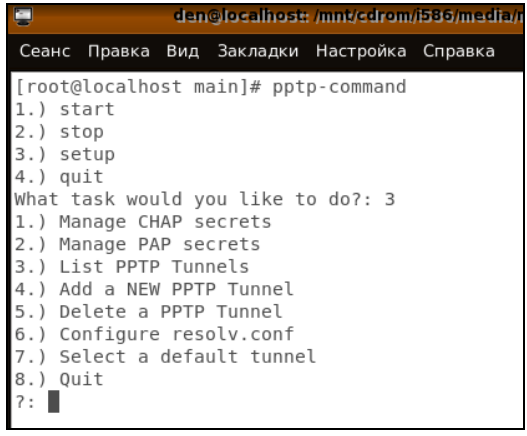


Рис. 18.5. Сценарий pptp-command

5. Настройка почти закончена. Осталось в уже хорошо знакомом нам меню выбрать пункт **7.) Select a default tunnel**, позволяющий выбрать тоннель по умолчанию. Выберите тоннель, который только что создали.
6. Для подключения к VPN нужно опять запустить сценарий `pptp-command` и выбрать команду **1.) start**. Понятно, что перед этим вы должны подключиться к Интернету.

18.5.3. Настройка Windows-клиента

Настройка VPN-подключения в Windows 2000/XP намного проще. Во-первых, вам не нужно устанавливать VPN-клиент — он уже входит в состав Windows и установлен по умолчанию. Во-вторых, интерфейс мастера новых подключений в Windows дружелюбнее и привычнее интерфейса сценария `pptp-command` (хотя кому как).

Чтобы создать VPN-подключение, выполните команду меню **Пуск | Настройка | Сетевые подключения | Создание нового подключения**. В окне мастера новых подключений выберите **Подключить к сети на рабочем месте** (рис. 18.6). Затем выберите **Подключение к виртуальной частной сети** (рис. 18.7).

Перед подключением к VPN нужно установить соединение с Интернетом, поэтому мастер новых подключений предложит вам выбрать соединение с Интернетом, которое будет установлено перед подключением к VPN (рис. 18.8).

Теперь вам останется лишь ввести параметры подключения: имя VPN-сервера (рис. 18.9), имя пользователя и пароль. Вместо имени VPN-сервера можно ввести его IP-адрес.

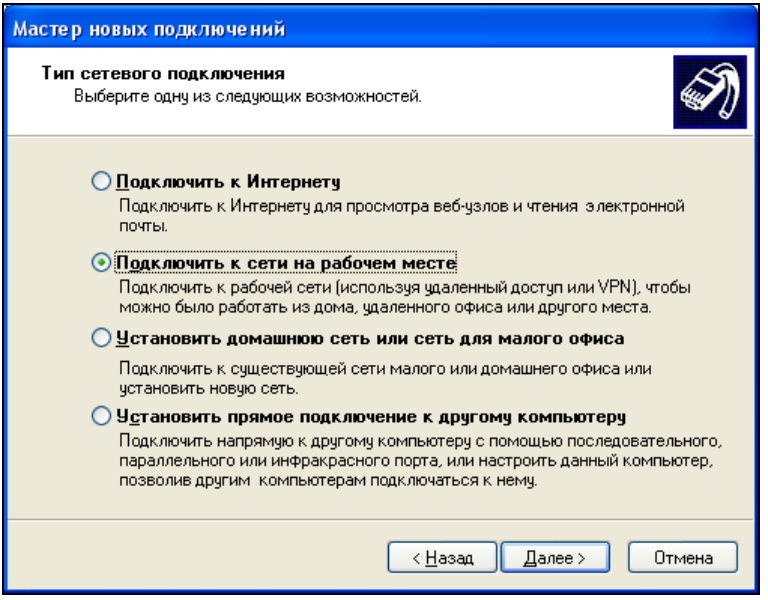


Рис. 18.6. Мастер новых подключений

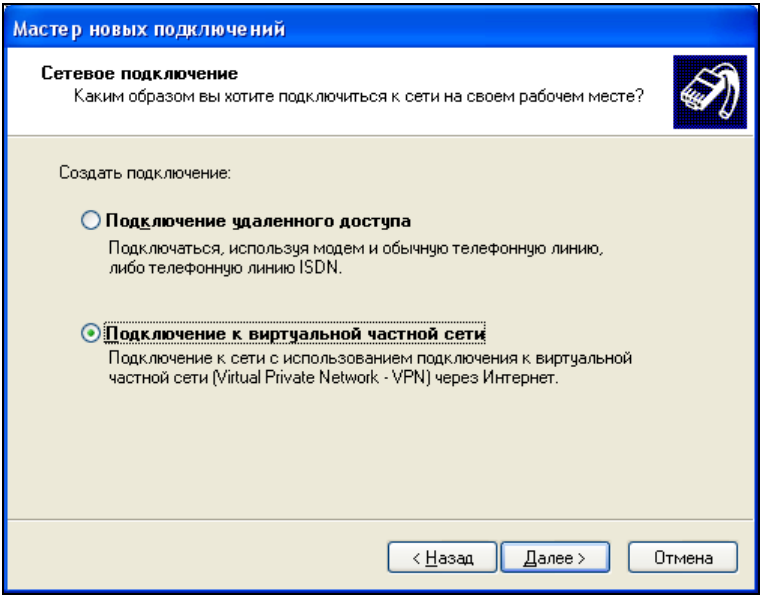


Рис. 18.7. Подключение к VPN

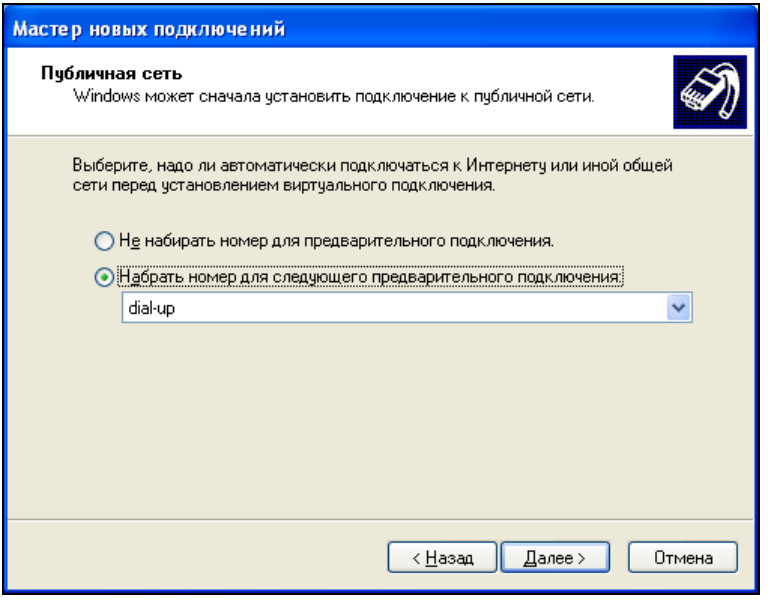


Рис. 18.8. Выбор подключения к Интернету

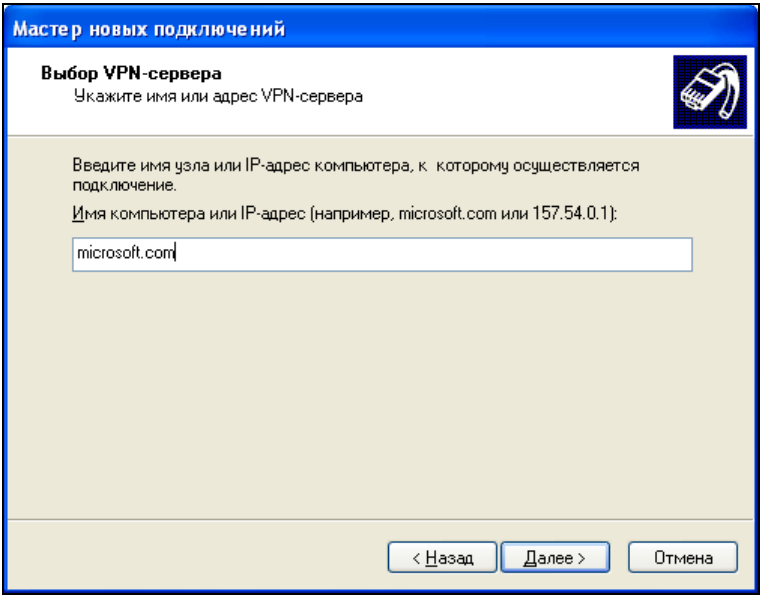


Рис. 18.9. Ввод имени VPN-сервера

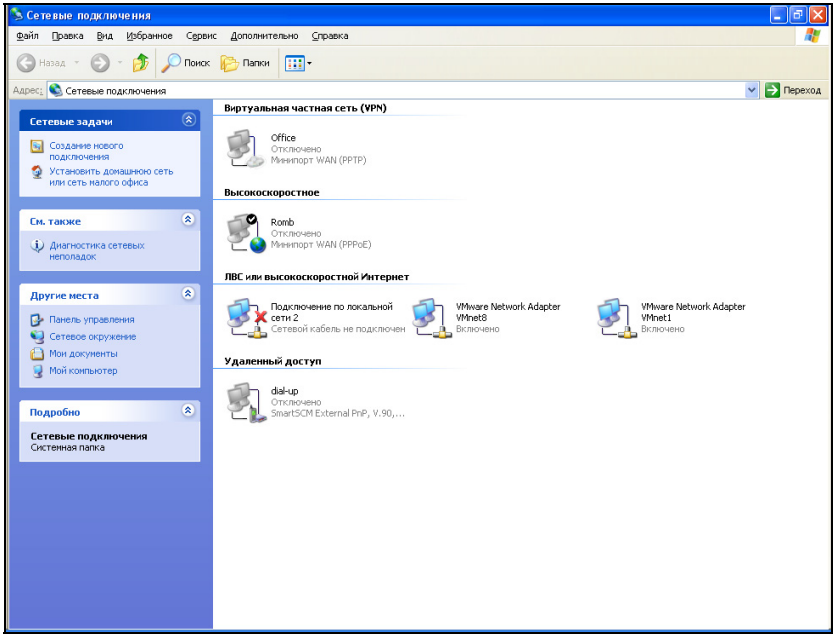


Рис. 18.10. Сетевые подключения

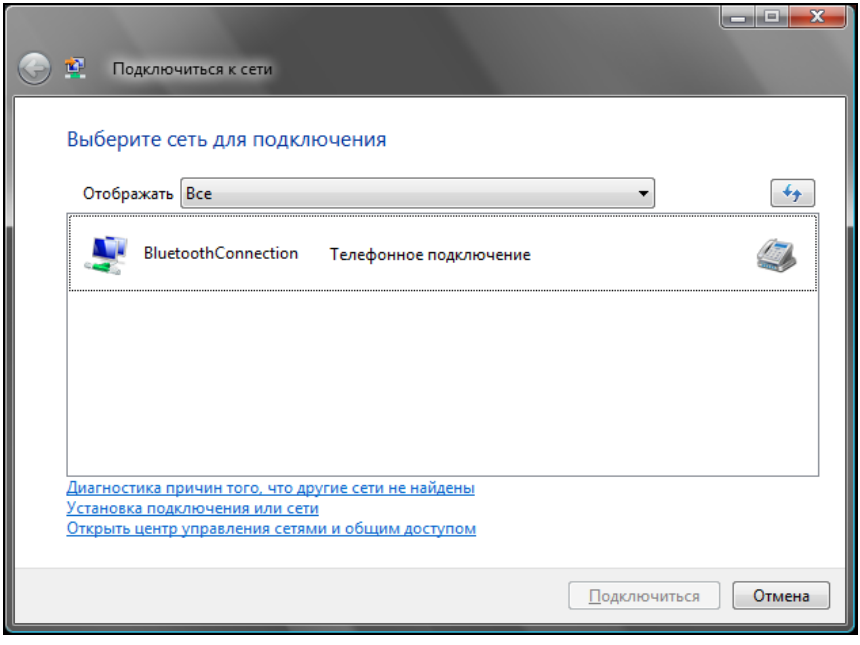


Рис. 18.11. Подключиться к сети

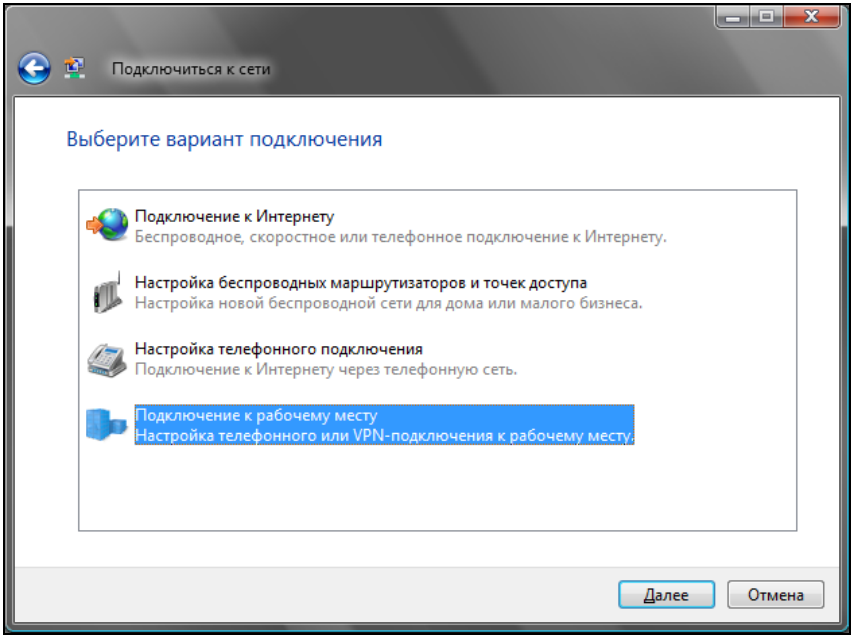


Рис. 18.12. Выбор варианта подключения

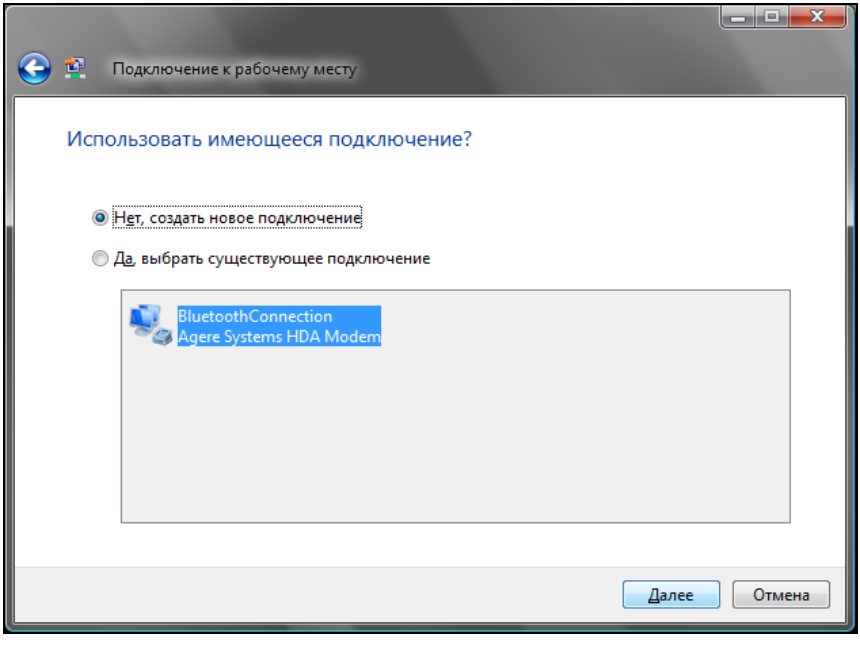


Рис. 18.13. Выбор интернет-соединения

После создания VPN-подключения его можно запустить из системной папки **Сетевые подключения** (рис. 18.10).

В Windows Vista VPN-подключение создается аналогично. Выберите команду **Пуск | Подключение**. В открывшемся окне (рис. 18.11) перейдите по ссылке **Установка подключения или сети**.

В открывшемся окне выберите **Подключение к рабочему месту** (рис. 18.12).

Далее процесс настройки ничем не отличается от процесса настройки в Windows XP: нужно выбрать интернет-соединение (рис. 18.13), ввести имя VPN-сервера и т. д.

Глава 19

Антивирусы и брандмауэры

19.1. Windows — под прицелом

Windows — очень уязвимая операционная система. Не нужно думать, что я говорю это просто так. Буквально неделю назад моя система подхватила очередной "троян". И это при работающем брандмауэре и антивирусе! Брандмауэр Outpost Firewall 3 и антивирус NOD32. Согласен, что брандмауэр весьма "древний", а NOD32 — далеко не лучший антивирус. Именно это и стало причиной инфицирования системы. Справедливости ради надо отметить, что NOD32 чуть позже обнаружил и удалил вирус, но не полностью. Остался backdoor[1], позволяющий злоумышленнику проникать в мою систему. Более того, после инфицирования компьютера брандмауэр уже больше не запускался.

Что я сделал? Установил новую версию брандмауэра — Outpost Security Suite Pro 2009. Но и это не помогло (хорошо, хоть есть условно-бесплатные версии программ, позволяющие ознакомиться с ними до покупки). Компьютер продолжал зависать, очевидно, пытаясь получить инструкции от злоумышленника (очевидно, что-то шло не так, отсюда и частые зависания). Мне это надоело, и так как не было ни желания разбираться с вирусом, ни переустанавливать Windows, я полностью мигрировал в Linux и провел там полтора месяца.

Разница сказалась заметна сразу. Мне не нужно было больше думать ни о брандмауэрах, ни об антивирусах, я просто работал и ни о чем не беспокоился. Все стало замечательно.

---

[1] Backdoor (букв. перевод с англ. — задняя дверь) — средство, позволяющее злоумышленнику проникать в систему без согласия пользователя и выполнять необходимые ему действия. Какими будут эти действия (рассылка спама или тотальный контроль над вашим рабочим столом), зависит от backdoor и желаний самого злоумышленника.

Примечание редактора относительно Linux

Ну, да, только постоянно и по любому поводу приходится "мусолить" конфигурационные файлы... То это устройство без плясок с бубном не работает (типа LPT-сканера), то — то (типа Web-камеры), то драйвера нужного нет, то он есть, да для другого дистрибутива (суперсовет в форумах — смените дистрибутив), то половина окна по-русски — половина "по-нерусски", одна морока все время подлаживать систему... А уж совместимость приложений — того же Writer с Word — только теоретически и до тех пор, пока не начнешь работать по-настоящему: нам как-то принесли книжный каталог (в табличке JPG-обложки + аннотации, и так 300 стр.) из-под Writer — куда и как съехали и покорежились при открытии в Word все картиночки, до сих пор вся редакция за сердце держится... Все это для тех, кто любит ковыряться в системе ради самого ковыряния, либо запустить Linux-сервер и отойти от него навсегда. А для нормальной работы в инете, офисе, с текстом, с графикой, с верстkой и т. п. лучше "виндов" пока ничего нет... А если что-то уж очень заест — я за 20 минут солью акронисом "чистую" систему со всеми нужными приложениями взамен "упавшей" — и работаю дальше... Прошу прощения за крик души — не верю я в Linux, пробовал, ставил, даже работать пытался, но не было удовлетворения, кустарщина это, однако (ИМХО, разумеется)...

Мой ответ на примечание

Не знаю, стоит или нет включать эти примечания в книгу, но наверняка читателям будут интересны две разные точки зрения. Да, у Linux есть проблемы. Да, иногда самого бесит неполная русификация некоторых дистрибутивов. Взять ту же Fedora 10 — 10-я (!) версия, а некоторые окошки до сих пор на английском. Хоть английским и владеем, но в Windows-то, если она "русская", никаких англоязычных окошек! Что же касается принтеров, сканеров и Web-камер, то в последних версиях дистрибутивов с этим все намного лучше, чем два года назад. А вот OpenOffice меня не радует, особенно, если в нем открываешь документ, содержащий макросы. Они до сих пор интерпретируются неправильно. Открою вам огромный секрет. Книги по Linux создаются в Windows. Вот так... Да, саму книгу пишу в OpenOffice/Linux, а потом приходится перезагружаться в Windows, чтобы отформатировать книгу в соответствии с шаблонами издательства, содержащими простейшие макрокоманды. OpenOffice, к сожалению, работать с ними отказывается. Вот и выходит, что проще мне одному перезагрузить компьютер, чем заново "изобретать велосипед" (под этим я подразумеваю приложение для набора текста, которое бы одинаково работало в любой ОС) и переводить издательство на использование этого "велика". С другой стороны, существуют эмуляторы wine и cedega, позволяющие в Linux запускать Windows-приложения и даже Windows-игры. Так, можно запустить MS Office, QIP, The Bat! и AutoCAD в Linux под управлением эмулятора. Но, спрашивается — зачем тогда Linux, если половина приложений будут работать в эмуляторе? Есть по крайней мере две причины перейти на Linux. Во-первых, она бесплатна — если вопрос о лицензионном программном обеспечении для вас актуален, есть возможность сэкономить. Во-вторых, с точки зрения безопасности Linux на голову выше Windows. О вирусах, по крайней мере, на данный момент, можно забыть. Понятно, что как энтузиаст и фанат Linux, я буду отстаивать эту ОС. И не только на словах — я реально попытался сделать ее лучше. На сайте **denix.dkws.org.ua** вы найдете русифицированную версию

> Ubuntu (будьте уверены, что все окошки — на русском языке) с уже установленными кодеками и OpenOffice 3.0 Pro от "Инфра-Ресурс". Обратите внимание — текущие версии дистрибутивов включают пока OpenOffice 2.4. Версия 3.0 Pro лучше, чем 2.4, но с макросами она все равно работать не умеет. К сожалению... Так что какую ОС выбирать, — решать только вам.

Вирусов для Linux очень мало, а те, которые есть, не могут причинить системе серьезного вреда. Поэтому если у вас нет особых программ, которые не запускаются даже в Windows-эмуляторе, рекомендую перейти на Linux (офисные пакеты, программы для работы в Интернете — все это есть в любом дистрибутиве).

Вообще, полученный на прошлой неделе вирус, — это далеко не первый и, если продолжать работать в Windows, далеко не последний. Если во времена DOS и Windows 95 преимущественно были распространены загрузочные и стелз-вирусы, то в эру быстрого Интернета "размножились" сетевые черви. Вирусы больше не шифруют загрузочные секторы или отдельные файлы, не заражают исполнимые файлы, они поражают сетевые службы Windows. Современный вирус — это не один файл, а совокупность файлов. Одна часть файлов используется для "десантирования" на компьютер-жертву. Как правило, эта часть вируса очень маленькая — чтобы вирус мог поражать даже компьютеры, имеющие медленное соединение с Интернетом. Далее эта часть вируса постепенно, байт за байтом, выкачивает основную часть вируса из Интернета. Как только эта часть вируса загружена, вирус начинает свои деструктивные действия. Чем занимаются сетевые черви? Довольно часто они используются для:

- сбора паролей и другой конфиденциальной информации — поскольку сетевые черви маскируются под сетевые службы Windows, получить доступ к передаваемому трафику им очень легко;
- рассылки спама — ваш компьютер будет отправлять спам, а вы об этом даже не будете знать. В итоге в "черный список" почтового сервера внесут ваш компьютер, а не компьютер злоумышленника;
- атаки других компьютеров — вы только представьте: под контролем злоумышленника тысячи инфицированных компьютеров. Он может отдать команду одновременно всем компьютерам просто подключиться к определенному серверу или завалить удаленный сервер ICMP-пакетами. Понятно, что сервер не выдержит такого напора и "упадет" на несколько минут (иногда даже на несколько часов). Такой вариант называется *распределенной атакой на отказ* (DDoS);
- предоставления доступа злоумышленнику к вашему компьютеру — тут комментировать особо нечего. Оно вам нужно?

- взлома других компьютеров — злоумышленник может использовать ваш компьютер для взлома серверов, например, Министерства обороны. В итоге спецотдел постучит в двери к вам, а не к нему;
- других незаконных действий.

Написать вирус не очень сложно. Тем более, что в Интернете находится достаточно много узлов, где можно скачать исходный код самых популярных вирусов. Именно этим и объясняется огромное количество вирусов для Windows. Любой "моральный урод", чтобы удовлетворить свои амбиции, может стать вирусописателем. И для этого ему не нужны какие-то особо глубокие знания. Все, что надо — это азы программирования и умение использовать компилятор. Хотя можно и без этого. Особо продвинутые вирусописатели еще десять лет назад придумали "вирусные лаборатории", позволяющие изменять параметры поддерживаемых ими вирусов. Вы можете взять за основу базовый вирус, изменить условия его срабатывания (например, каждую пятницу вместо каждой среды), заменить название вируса и основных исполнимых файлов, и все — новый клон готов.

К счастью, именно поэтому с вирусами относительно просто бороться. Помню, на моем компьютере "поселился" один из вариантов вируса WinProxy. Работать было практически невозможно, а антивирус (у меня тогда был антивирус Касперского) в нормальном режиме работы Windows ничего поделать не мог, а в безопасном даже не запускался. Пришлось перезагрузиться в безопасный режим и использовать другие утилиты (AVZ и CureIt от DrWeb). Сначала они тоже не хотели запускаться — как оказалось, вирус блокировал запуск этих утилит по имени их файлов. После переименования исполнимых файлов утилит они запуститься смогли.

> **Совет**
>
> Возьмите себе это на заметку. Если у вас не получается запустить антивирус, переименуйте его исполнимый файл в какую-либо абракадабру (например, в aaaa11.exe) и запустите его. В большинстве случаев это сработает.

Тогда AVZ помог опознать основные файлы вируса, но удалить их не мог — после удаления они сразу же появлялись снова. Но мне удалось обмануть этот вирус. Как выяснилось, он проверял наличие файла karina.dat. Если его не оказывалось на месте, вирус из какого-то скрытого процесса восстанавливал свои файлы. В самом файле karina.dat помимо всего прочего содержался вредоносный код какой-то части вируса. Я открыл этот файл и стер его содержимое, заполнив файл единичками. Потом с помощью AVZ удалил другие части вируса (кроме файла karina.dat). Затем перезагрузился в обычный режим, после чего выслушал *N* сообщений об ошибках — система пыталась загрузить DLL из … karina.dat, а так как это был уже обычный текстовый

файл, у нее ничего не получилось. Вот и славно. Как оказалось, основной код вируса как раз и был в этом файле. Мне осталось только прогнать систему через антивирус Касперского, который окончательно подчистил ее, и почистить реестр, удалив все ссылки на karina.dat.

Как видите, нужно использовать несколько утилит для проверки вашей системы. Лечить компьютер лучше в безопасном режиме. Некоторые вирусы не запускаются в безопасном режиме, что позволяет легко вычистить их файлы и удалить. В нормальном же режиме они перехватывают системные вызовы, возвращающие содержимое файловой системы, и скрывают свое присутствие. Вообще, путем перехвата системных вызовов достаточно легко скрыть пребывание того или иного процесса в системе (как самого процесса, так и его исполнимых файлов).

Итак, давайте сформулируем стратегию защиты вашего компьютера:

- обязательно установите брандмауэр — чуть позже мы поговорим о выборе брандмауэра;
- установите антивирус — некоторые решения, например, Internet Security 2009 от Касперского, сочетают в себе функции как брандмауэра, так и антивируса, но я предпочитаю использовать решения различных разработчиков, а не слепо доверять какому-то одному;
- скачайте дополнительные утилиты — лучше всего себя зарекомендовали утилиты AVZ и CureIt. Они могут запускаться без установки на компьютер и работать в безопасном режиме. Дабы исключить их поражение вирусом, запишите эти утилиты на компакт-диск и для проверки компьютера запускайте их с диска. Только не забывайте их регулярно обновлять — скажем, раз в месяц. Толку от таких утилит полугодичной давности будет мало.

Из связки антивирус-брандмауэр первым нужно устанавливать антивирус. После его установки обязательно проверьте всю систему. Затем установите брандмауэр — тогда он автоматически создаст правила для уже установленного антивируса. Если вы сначала установите брандмауэр, а потом — антивирус, никто не может гарантировать, что правила брандмауэра для антивируса будут прописаны корректно (впрочем, это зависит от брандмауэра).

Дополнительные утилиты действительно можно хранить на компакт-диске. С сайта **http://www.freedrweb.com/livecd/** вы вообще можете скачать загрузочный диск (Live CD). После загрузки с этого диска вы сможете проверить все жесткие диски вашего компьютера. Такая проверка будет самой эффективной, поскольку вирусы при загрузке компьютера с Live CD находятся в неактивном состоянии и не могут скрыть себя от антивируса. Более подробно мы поговорим о такой проверке позже *(см. разд. 19.4.3)*. А сейчас самое время поговорить о выборе антивируса.

19.2. Выбор антивируса

Какой антивирус выбрать? Наверное, лучший антивирус, который у меня был, — это *антивирус Касперского*. Если вирусы я и "хватал", то когда этот антивирус "спал" (то есть я его или вообще не устанавливал или отключал). С сайта **http://kaspersky.ru/** можно скачать пробную 30-дневную версию этого антивируса (KAV, Антивирус Касперского 2009). Можете убедиться, что на протяжении этих 30 дней вирусы вам точно не будут страшны. Потом придется или купить его (980 рублей) или удалить… На этом же сайте можно скачать и пробную версию KIS, Kaspersky Internet Security 2009 — этот продукт сочетает в себе функции брандмауэра и антивируса. Если вы выбрали KIS, брандмауэр можете уже не устанавливать. KIS 2009 стоит дороже: 1600 рублей. Сравнительную таблицу продуктов KAV и KIS можно найти по адресу: **http://www.kaspersky.ru/compare_NEW**.

Сейчас у меня установлен *NOD32* (**www.eset.com**). Это тоже коммерческий антивирус. Именно "под его руководством" в моей системе поселился троян на прошлой неделе. Когда у меня был KAV, такого при работающем антивирусе не случалось. NOD32 я же вообще не выгружал — а вот так получилось. Учитывая, что цена NOD32 примерно такая же, как и KIS, лучше выбрать KAV (еще и деньги сэкономите) или KIS (будет брандмауэр впридачу).

В Интернете можно частенько услышать, что KAV "пожирает" системные ресурсы. Скажем так, это особо не ощущается, если у вас современный компьютер и достаточно оперативной памяти. Конечно, NOD32 будет "полегче", и компьютер при нем загружается быстрее. Но вам же нужен антивирус для защиты системы, а не просто для того, "чтобы было"? Поэтому следует выбирать лучшее, а не идти на компромиссы.

Антивирус McAfee вообще меня не порадовал. Этот антивирус был на моем ноутбуке предустановлен. Понятно, что от подарков не отказываются, поэтому сначала я его оставил, тем более, что в комплекте был не только антивирус, но и брандмауэр от McAfee. Но когда этот антивирус не справился с простейшим вирусом (распространяющемся на Flash-дисках), который я смог удалить самостоятельно, переведя файловый менеджер в режим отображения скрытых файлов, McAfee был с моего ноутбука "снесен". На его место пришел NOD32. Учитывая, что мой ноутбук редко бывает в Интернете, NO32 — не самое плохое решение. А вот скорость загрузки ноутбука стала намного выше. Субъективно, но мне показалось, что McAfee требует ресурсов еще больше, чем даже KAV.

Что же касается функциональности, то все эти антивирусы (KAV, McAfee и NOD32) предоставляют примерно одинаковый набор функций и могут про-

верять файловую систему, интернет-соединения, почту, обеспечивают защиту от вредоносных и шпионских программ и т. п. Но вот эффективность защиты от того или иного вируса у каждой программы — разная.

DrWeb — хороший антивирус, но я предпочитаю использовать утилиту CureIt (подробнее о ней см. в *разд. 19.4.2*), созданную на его базе. Эта утилита не умеет проверять файлы "на лету" (по мере их открытия программами), не проверяет интернет-соединения, но зато хорошо выполняет функцию файлового антивируса-сканера. Она сканирует все файлы жесткого диска, находит и удаляет вирусы. Чуть позже мы рассмотрим эту утилиту подробнее. В некоторых случаях только она помогала искоренить вирусы из моей системы.

Не хочется платить за безопасность? Тогда можно попробовать использовать *бесплатные антивирусы*, например, Avast или ClamAV для Windows. У меня когда-то были установлены оба эти антивируса. Честно говоря, эффективность если не нулевая, то близкая к нулю. Если выбирать между двумя этими антивирусами, то советую обратить внимание на Avast. ClamAV можно установить на UNIX/Linux-сервере для проверки почты и файлов в файловом обменнике. Много вирусов он не найдет, но если найдет хоть что-то, значит, мы не зря его установили.

Еще могу порекомендовать очень хороший антивирус *AVZ* (**www.z-oleg.com**). Использовать его в качестве полноценного антивируса трудно. Да, в нем есть функция AVZGuard, защищающая систему от незаконных действий, но под незаконными действиями воспринимается практически любое изменение настроек системы, поэтому работать при включенном AVZGuard просто невозможно. Эту утилиту следует использовать, когда есть подозрение на заражение вирусом. Вот тогда AVZ обязательно поможет. Даже если AVZ не найдет вирус "в лоб", он содержит набор диагностических средств, позволяющих проанализировать положение вещей и этот вирус вычислить. К тому же AVZ сообщает о небезопасных настройках системы, что также позволяет повысить ее безопасность (подробнее об антивирусе AVZ см. в *разд. 19.4.1*).

Если хотите немного развлечься, можете прочитать юмористическое сравнение различных антивирусов на моем сайте: **http://www.dkws.org.ua/phpbb2/viewtopic.php?t=3679**. Нужно отметить, что в каждой шутке есть "доля шутки", поэтому в некоторых моментах данное сравнение весьма объективно отображает ситуацию на рынке антивирусов.

19.3. Выбор брандмауэра

Бастион (он же брандмауэр, он же firewall) — это пакетный фильтр, позволяющий защитить ваш компьютер от действия вредоносных программ, сетевых червей, нежелательного трафика и всевозможных атак.

Разберемся, как работает бастион. Данные по сети передаются частями, которые называются *пакетами*. Каждый пакет состоит из двух основных частей — области заголовков и области данных. Первая область содержит служебную информацию — IP-адрес отправителя пакета, IP-адрес получателя пакета, порт отправителя и получателя и др. Вторая область содержит передаваемые данные — часть электронного письма, часть файла, часть голосового сообщения и т. д. Брандмауэр (привыкайте к разным названиям) перехватывает все сетевые пакеты и сопоставляет область заголовка (иногда и область данных) набору правил. *Набор правил* обычно задается администратором системы. Например, вы можете запретить обращение к определенному узлу. Это может понадобиться, чтобы другие пользователи (ваши дети) не смогли получить доступ к нежелательным узлам.

Брандмауэры обычно устанавливаются на так называемых *граничных компьютерах* — компьютерах, предоставляющих доступ к Интернету другим пользователям сети. Существуют также аппаратные брандмауэры — специальные устройства, которые выполняют маршрутизацию и фильтрацию пакетов. Скорее всего, такой брандмауэр установлен у вашего провайдера или же встроен в маршрутизатор, предоставляющий локальным компьютерам доступ к Интернету. Но, как показывает практика, рабочие станции требуют дополнительной защиты, поскольку администратор сети не может проконтролировать все компьютеры сети (особенно это сложно сделать с сетью провайдера — ведь для максимальной защиты нужно пройтись по всем клиентам и защитить каждый компьютер). Поэтому весьма желательно установить локальный брандмауэр. Такой бастион будет защищать наш и только наш компьютер. К тому же локальные бастионы часто оснащаются дополнительными приятными функциями: детектором атак, средством для поиска шпионских программ и др.

19.3.1. Брандмауэр для Windows

Одним из лучших брандмауэров для Windows, которые я использовал, является Outpost Security Suite Pro 2009. Вот основные его преимущества:

- защита от кражи личной информации — Outpost не позволит вредоносным программам передать данные с вашего компьютера;
- защита от сетевых атак — брандмауэр предотвращает любые попытки проникновения злоумышленника на ваш компьютер;
- защита от шпионских программ — шпионские программы мгновенно удаляются с компьютера;
- автоматическое обновление конфигурации для лучшей защиты — начиная с четвертой версии брандмауэр умеет автоматически обновлять свою кон-

фигурацию через систему ImproveNet, благодаря чему ваша защита всегда будет соответствовать последним требованиям безопасности.

Помните, что Outpost Security Suite Pro нельзя использовать с другими подобными программами. Например, вы не сможете одновременно использовать Outpost Security Suite Pro и Kaspersky Internet Security.

Скачать программу можно по адресу: **http://www.agnitum.ru/**.

Обратите внимание на версию программы: существуют версии для обычных процессоров (32-битных) и для 64-битных. При этом помните, что нужно ориентироваться не на разрядность процессора, а на разрядность операционной системы. У вас может быть 64-разрядный процессор, но 32-разрядная версия Windows. В этом случае вам нужно скачать 32-разрядную версию программы.

Нужно отметить, что программа не бесплатна. Вы можете скачать бесплатную 30-дневную версию. По истечении этого срока нужно или удалить программу или приобрести ее.

Установка программы довольно проста. Во время установки мастер настройки попросит вас выбрать способ создания новой конфигурации. Нужно выбрать **Автоматическая настройка**. Минимум вашего вмешательства (нужно только нажать кнопку **Далее**), и конфигурация будет создана. После установки нужно будет перезагрузить компьютер. Брандмауэр будет запускаться автоматически — при загрузке системы.

Брандмауэр желательно устанавливать после установки всех сетевых программ, которые вы планируете использовать. Тогда при автоматическом создании конфигурации Outpost определит ваши сетевые программы (а он "знает" очень много таких программ) и в процессе работы будет задавать меньше вопросов, поскольку при создании конфигурации будут созданы правила для большинства программ. Но это не означает, что нельзя будет создать правило для сетевых программ, которые были установлены после установки бастиона. Если вы установили какую-нибудь программу после установки брандмауэра, и брандмауэр работает в режиме обучения, он сообщит, что некая программа пытается получить сетевой доступ.

Основное окно программы изображено на рис. 19.1. В левой части отображено основное меню программы:

- **Брандмауэр** — содержит команды управления брандмауэром. Вы можете просмотреть активные сетевые соединения (рис. 19.2) и открытые порты (рис. 19.3). Непосредственно в разделе **Брандмауэр** можно просмотреть сведения об атаках на ваш компьютер (рис. 19.4).
- **Локальная безопасность** — содержит список программ, которым разрешен доступ к Интернету и список активных в данный момент процессов;

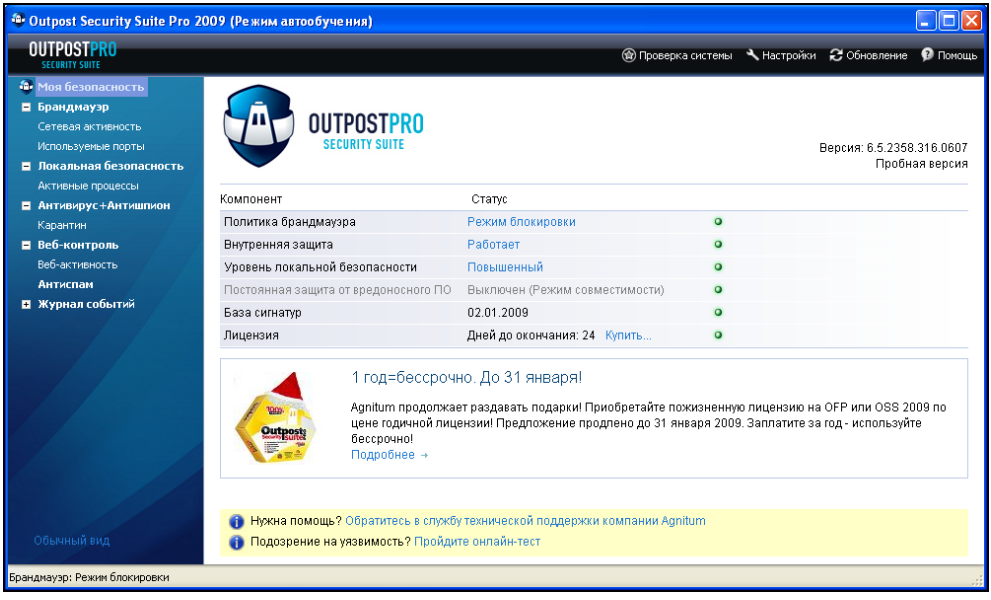


Рис. 19.1. Основное окно **Outpost Security Suite Pro**

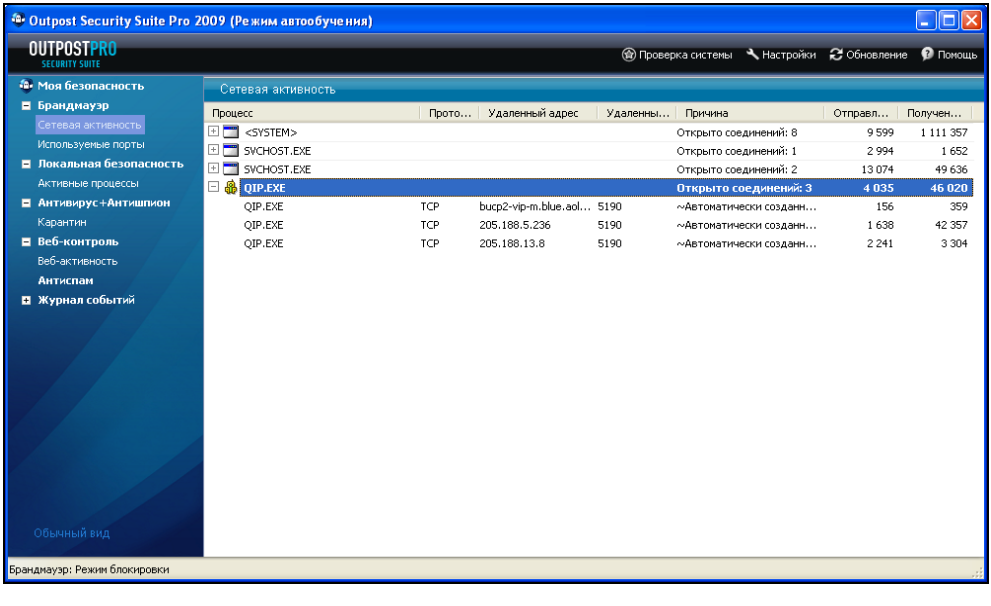


Рис. 19.2. Активные сетевые соединения

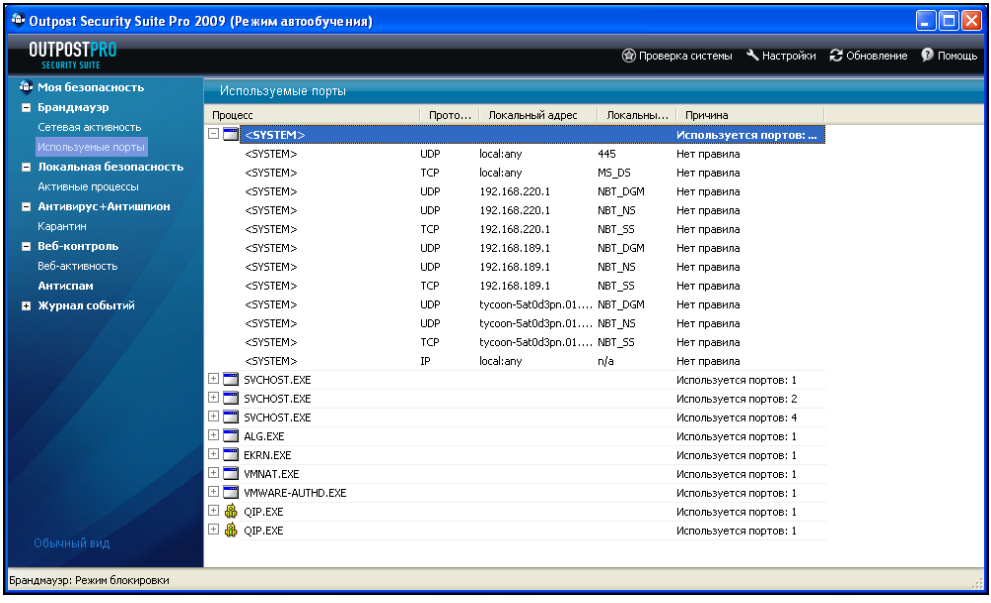


Рис. 19.3. Открытые порты

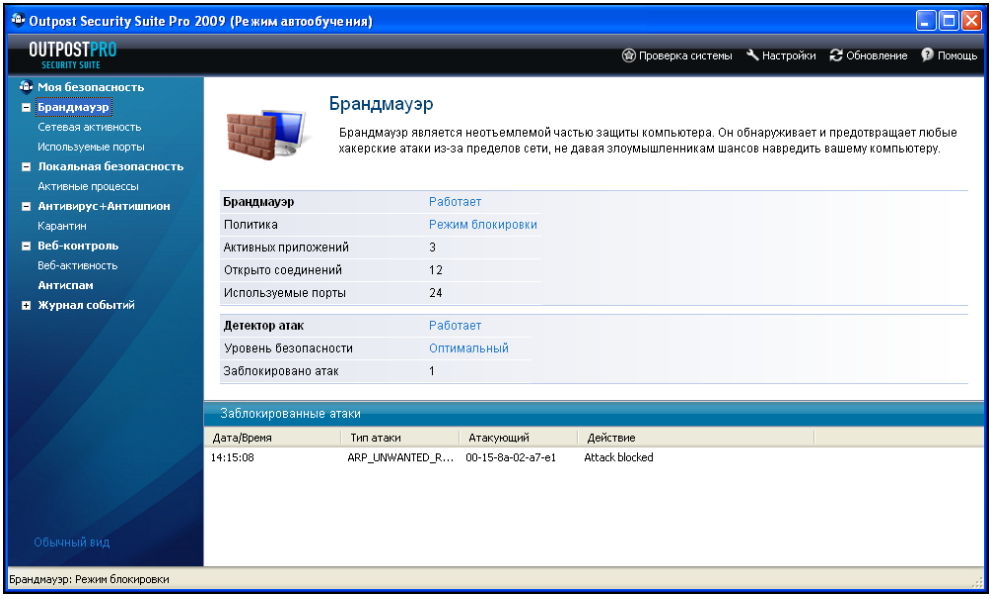


Рис. 19.4. Брандмауэр определил атаку и заблокировал атакующего

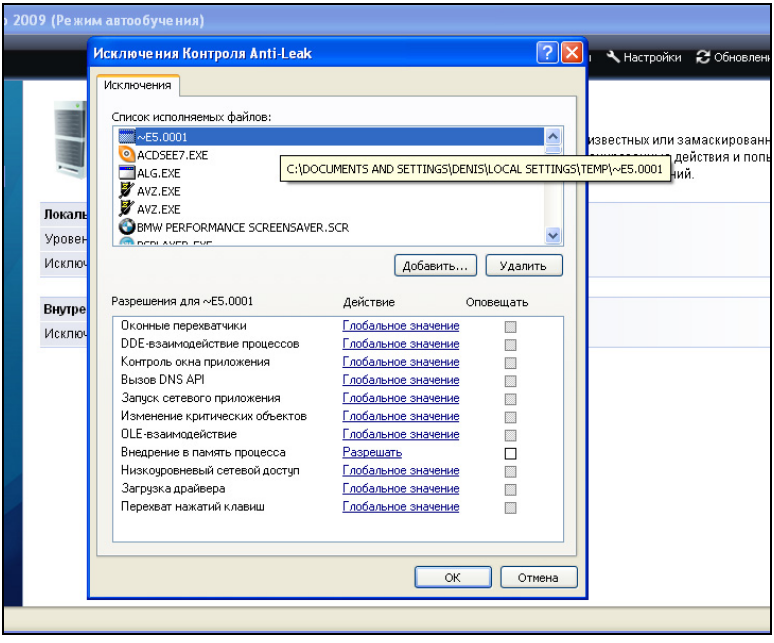


Рис. 19.5. Список программ, которым разрешен доступ к Интернету. Неопознанная программа

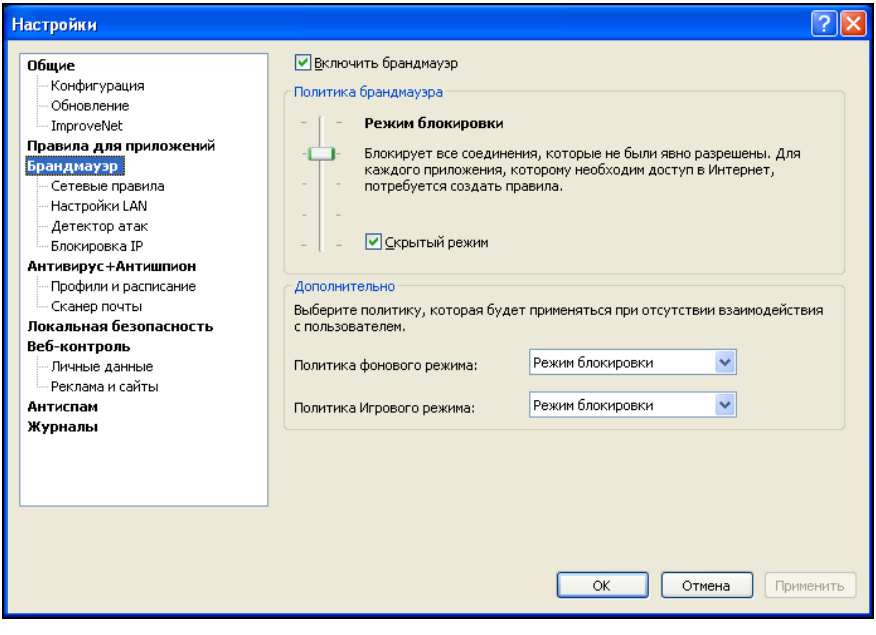


Рис. 19.6. Изменение политики брандмауэра

- **Антивирус + Антишпион** — здесь вы можете запустить проверку системы на наличие вредоносных программ и просмотреть карантин (объекты, которые встроенный антивирус посчитал вредоносными). Только не забывайте время от времени обновлять вашу базу сигнатур вредоносных объектов (кнопка **Обновление** в верхней части окна);
- **Веб-контроль** — контроль за вашими HTTP-соединениями;
- **Антиспам** — настройки спам-фильтров;
- **Журнал событий** — в журналах вы найдете полный отчет о работе того или иного модуля брандмауэра. Просто откройте нужный вам журнал и просмотрите его.

Нужно отметить, что брандмауэр далеко не всегда распознает вредоносную программу в режиме обучения. Перейдите в раздел **Локальная безопасность** и нажмите кнопку **Список**. Вы увидите список программ, которым антивирус автоматически разрешил доступ к Интернету. В моем списке оказался … вирус. Как видно из рис. 19.5, брандмауэр разрешил доступ неизвестной программе, запускающейся из временного каталога. Поэтому лучше всего обучать брандмауэр так:

- после установки брандмауэра он по умолчанию будет работать в режиме обучения. Долго работать в этом режиме не нужно. Запустите все ваши программы, которым вы хотите разрешить доступ к Интернету: браузеры, почтовые клиенты, ICQ, FTP-клиенты, Skype и т. д.;
- затем перейдите в раздел **Брандмауэр** и выберите политику **Режим блокировки** (рис. 19.6).

Брандмауэр Outpost Security Suite Pro — очень неплохой выбор, но иногда не хочется платить. Что делать? Можно использовать *бесплатный брандмауэр*. Бесплатный не всегда означает плохой. Могу порекомендовать персональный брандмауэр Comodo Firewall, который очень хорошо зарекомендовал себя на другом моем компьютере. Скачать бесплатную версию Comodo Internet Security можно по адресу: **http://www.personalfirewall.comodo.com/**.

Comodo также обеспечивает надежную защиту вашего компьютера и, ко всему прочему, обеспечивает еще и контроль реестра Windows. Очень хороший брандмауэр. Правда, иногда он надоедает своими предупреждениями и запросами, зато безопасность — на высоте.

19.3.2. Брандмауэр для Linux

В Linux часто используется брандмауэр iptables, и в других моих книгах рассматривался именно этот брандмауэр. В этой книге мы изменим традиции и рассмотрим программу Firestarter (сайт разработчиков: **www.fs-security.com**).

Благодаря наличию графического интерфейса Firestarter прост в настройке, поэтому его может использовать не только администратор сети, но и пользователь обычного домашнего компьютера, постоянно подключенного к Интернету.

Для установки введите в терминале (**Приложения | Стандартные | Терминал**) следующие команды:

```
sudo apt-get install firestarter (Ubuntu, Debian)
sudo yum install firestarter (Fedora)
```

Если ваш дистрибутив Linux не использует программу `apt-get` для установки пакетов, установите пакет firestarter, используя менеджер пакетов вашего дистрибутива.

Для запуска Firestarter введите команду `firestarter` (с привилегиями root). При первом ее запуске будет открыт мастер быстрой настройки (рис. 19.7).

Прежде всего мастер предложит выбрать сетевой интерфейс, подключенный к Интернету (рис. 19.8) — в нашем случае это ppp0. Имейте в виду: если неправильно выбрать сетевой интерфейс, брандмауэр будет работать неправильно и блокировать все соединения.

Если вы настраиваете шлюз (а не просто устанавливаете брандмауэр на локальном компьютере), на следующем шаге настройки (рис. 19.9) включите режим **Enable Internet connection sharing**. Что же касается DHCP-сервера (параметр **Enable DHCP for local network**), то управление DHCP-сервером станет возможным, только если у вас до установки Firestarter уже установлен DHCP-сервер.

В следующем окне (рис. 19.10) установите флажок **Start firewall now** и нажмите кнопку **Сохранить**.

Итак, базовая настройка брандмауэра выполнена. Изменить эту настройку можно, нажав кнопку **Preferences** на панели инструментов брандмауэра (рис. 19.11). Если вам опять понадобится запустить мастера настройки, выполните команду меню **Firewall | Run Wizard**.

Теперь приступим к редактированию правил. Перейдите на вкладку **Policy** (рис. 19.12). Поле **Editing** позволяет выбрать, какую политику вы хотите редактировать:

- **Inbond traffic policy** — политика входящего трафика. По умолчанию запрещены все входящие запросы. Если на вашем компьютере установлены серверы WWW и FTP и вы хотите, чтобы они были доступны извне, тогда вам нужно нажать кнопку **Add Rule** и открыть порты 80 и 21 соответственно;

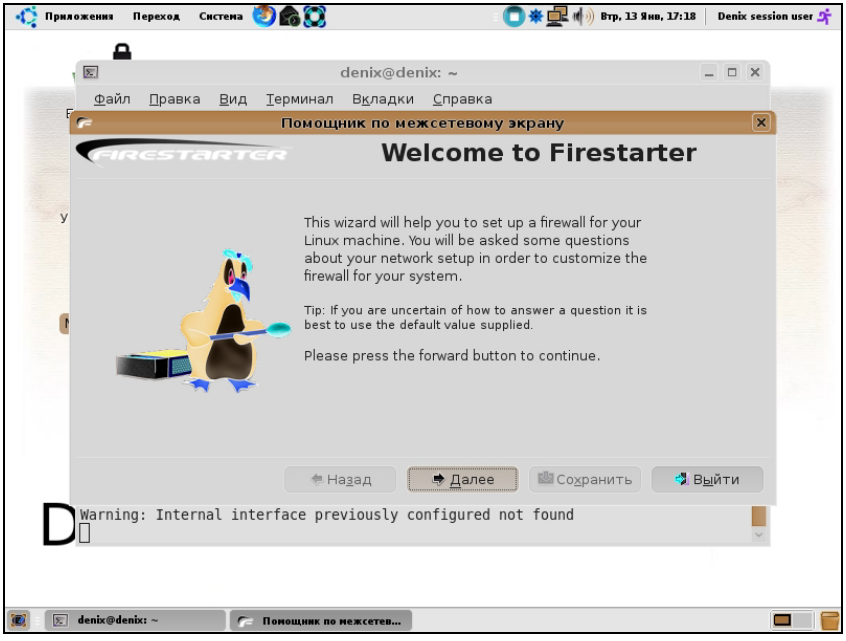


Рис. 19.7. Мастер настройки Firestarter

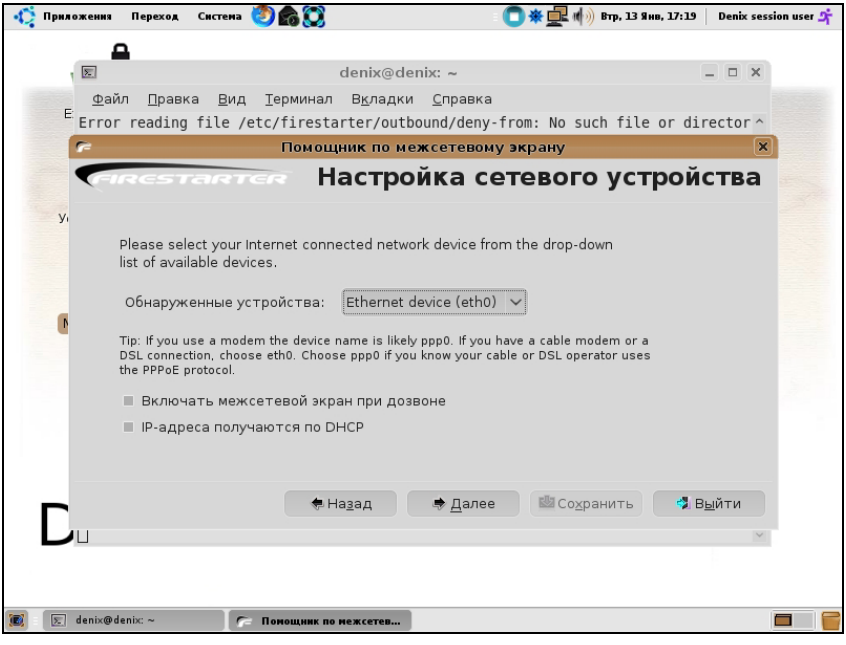


Рис. 19.8. Выбор сетевого интерфейса

Рис. 19.9. Настройка шлюза

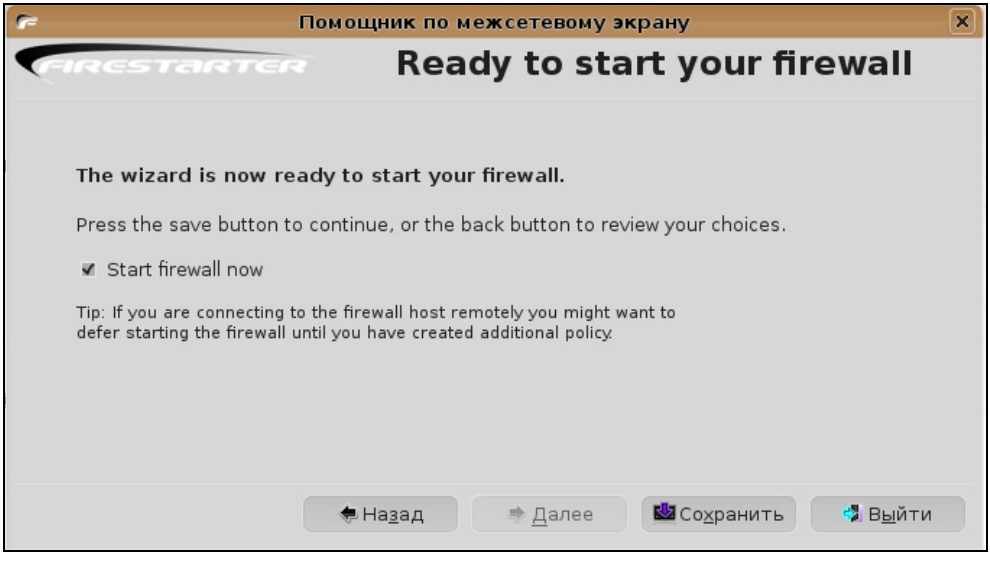


Рис. 19.10. Запустить брандмауэр

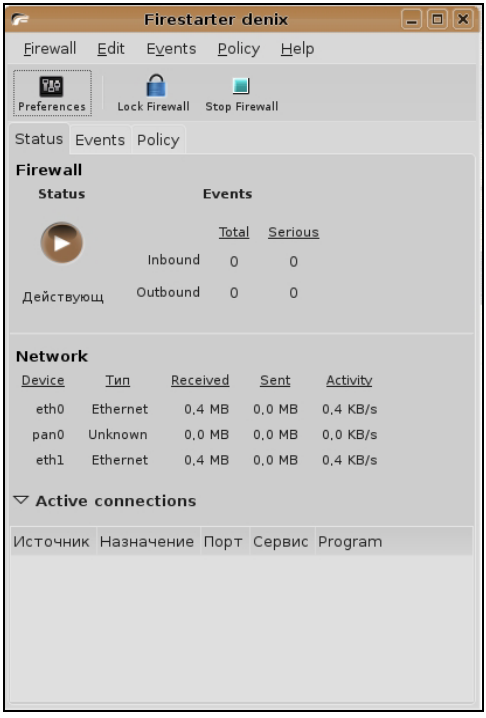


Рис. 19.11. Главное окно Firestarter

Рис. 19.12. Редактирование политик

- **Outbond traffic policy** — политика исходящего трафика. По умолчанию пользователям сети разрешается подключаться ко всем узлам Интернета, кроме тех, которые вы внесли в "черный" список. Такая политика называется **Permissive**. Вы можете использовать другую политику, при которой будет запрещен доступ ко всем узлам, кроме тех, которые описаны в "белом" списке. Такая политика называется **Restrictive**. Формировать вручную черный список удобнее, чем белый, поэтому обычно используется политика **Permissive**.

Вот еще некоторые номера портов:

- 22 — SSH;
- 23 — telnet;
- 25 — SMTP (отправка почты);
- 53 — DNS;
- 110 — POP3 (получение почты).

Какие узлы нужно внести в черный список? Информационно-развлекательные, сайты, содержащие материалы эротического и порнографического характера, чаты и т. д. Все это позволит сэкономить много трафика, да и сотрудники будут заниматься работой, а не просмотром возбуждающих картинок.

19.4. Использование программ AVZ и CureIt

19.4.1. Антивирус AVZ

Бесплатный антивирус AVZ (рис. 19.13), как уже отмечалось, можно скачать с сайта **www.z-oleg.com**. Антивирус не нуждается в установке. Просто распакуйте его в любой каталог на жестком диске и запустите. Сразу после этого выполните команду **Файл | Обновление баз** для обновления антивируса. После этого можно нажать кнопку **Пуск** для сканирования системы.

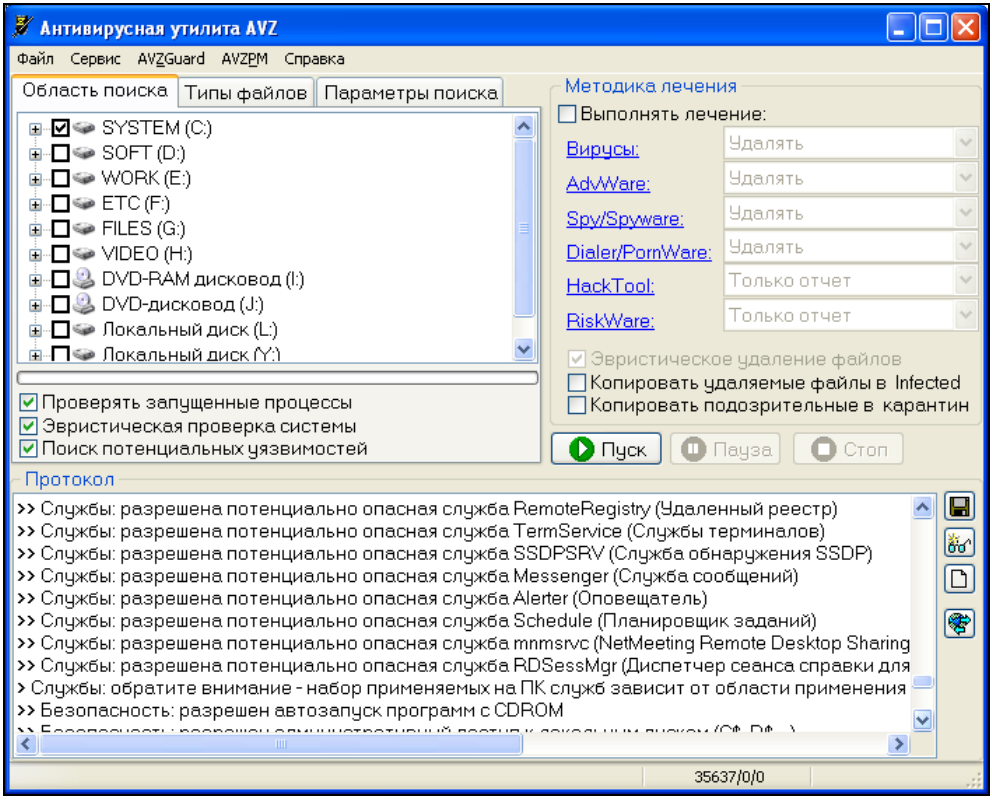


Рис. 19.13. Антивирус AVZ

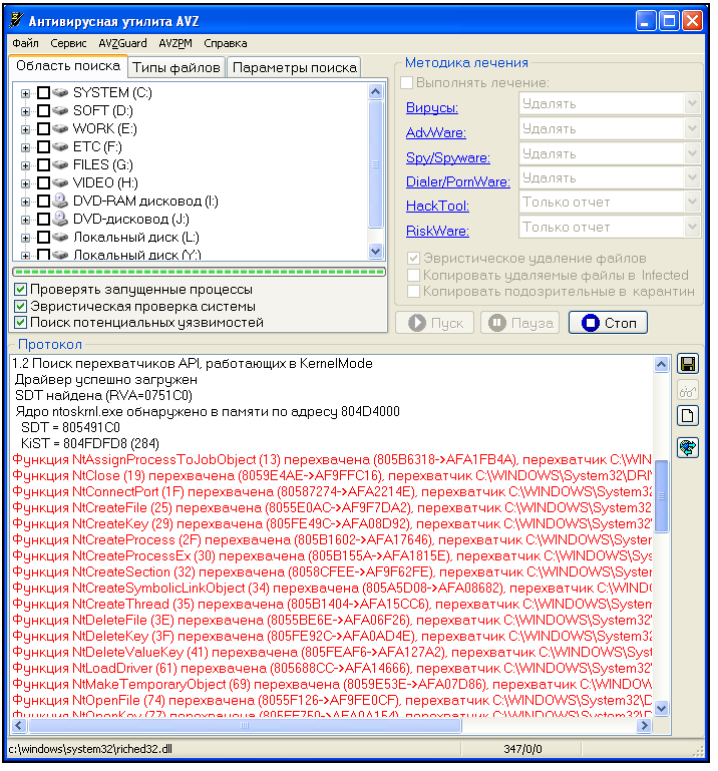
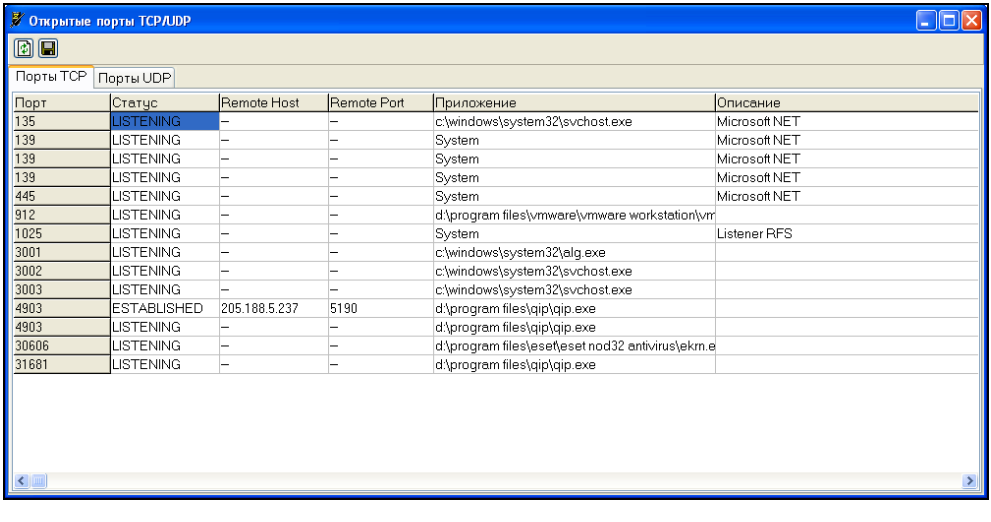


Рис. 19.14. Не всегда перехват функций означает инфицирование компьютера



Порт	Статус	Remote Host	Remote Port	Приложение	Описание
135	LISTENING	–	–	c:\windows\system32\svchost.exe	Microsoft NET
139	LISTENING	–	–	System	Microsoft NET
139	LISTENING	–	–	System	Microsoft NET
139	LISTENING	–	–	System	Microsoft NET
445	LISTENING	–	–	System	Microsoft NET
912	LISTENING	–	–	d:\program files\vmware\vmware workstation\vm	
1025	LISTENING	–	–	System	Listener RFS
3001	LISTENING	–	–	c:\windows\system32\alg.exe	
3002	LISTENING	–	–	c:\windows\system32\svchost.exe	
3003	LISTENING	–	–	c:\windows\system32\svchost.exe	
4903	ESTABLISHED	205.188.5.237	5190	d:\program files\qip\qip.exe	
4903	LISTENING	–	–	d:\program files\qip\qip.exe	
30606	LISTENING	–	–	d:\program files\eset\eset nod32 antivirus\ekrn.e	
31681	LISTENING	–	–	d:\program files\qip\qip.exe	

Рис. 19.15. Список открытых портов

Антивирус не только проверяет вашу систему, но и сообщает о потенциально опасных настройках. Ради эксперимента я запустил потенциально опасные службы Windows — антивирус обнаружил это и вывел соответствующее предупреждение (рис. 19.14).

Антивирус также сообщает о перехвате системных вызовов. Обычно такое поведение характерно вирусам, но в данном случае "перехватчиком" оказался драйвер SandBox.sys, являющийся частью брандмауэра Outpost.

Вычислить сетевого червя можно с помощью команды **Сервис | Открытые порты TCP/UDP** (рис. 19.15). Если найдутся подозрительные открытые порты, они будут выделены красным.

Обратите внимание: открыты порты 135 и 139. Это **Служба доступа к файлам и принтерам Microsoft**. У меня DSL-доступ к Интернету, а для DSL-соединения эта служба недоступна, зато по умолчанию она активна для соединения по локальной сети. Далеко не всегда нужна эта потенциально опасная служба (особенно, если у вас одиночный компьютер без локальной сети). Откройте список сетевых подключений, щелкните правой кнопкой мыши на вашем локальном соединении, выберите команду **Свойства** и отключите службу доступа к файлам и принтерам (рис. 19.16).

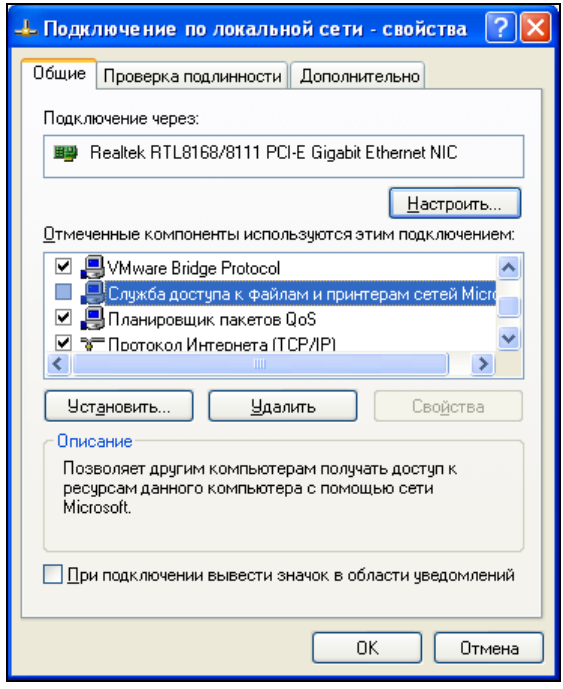


Рис. 19.16. Отключение службы доступа к файлам и принтерам

19.4.2. Утилита CureIt

Утилиту CureIt можно скачать с сайта **http://www.freedrweb.com**. Она очень проста в использовании — просто запустите ее и нажмите кнопку **Пуск**. Если ваш компьютер вообще не "дышит", попробуйте скачать DrWeb LiveCD, загрузиться с него и проверить систему с его помощью. LiveCD и документация на русском языке к нему доступны по следующему адресу: **ftp://ftp.drweb.com/pub/drweb/livecd/**.

19.4.3. Создание и использование проверочных компакт-дисков

Вообще, пока с вашим компьютером все нормально, скачайте упомянутый в предыдущем разделе LiveCD и запишите его на болванку. Для записи LiveCD в Nero нужно выбрать команду **Рекордер | Прожечь образ**. Затем укажите на скачанный образ и подождите завершения операции. Обратите внимание: для прожига нужен диск CD-R, а не DVD-R.

Программу AVZ также желательно записать на компакт-диск, но перед записью переименуйте файл avz.exe — дайте ему другое имя, например, a11a.exe, чтобы вирусы, блокирующие запуск программ по имени, не смогли заблокировать антивирус. Только не забывайте регулярно обновлять ваши антивирусные диски: диск с CureIt и диск с AVZ, иначе толку от них не будет.

19.5. Отключение потенциально опасных служб

Выполните команду **Пуск | Выполнить**, введите команду `services.msc` и нажмите клавишу <Enter>. Откроется окно **Службы**, в котором содержится список служб Windows. Вам нужно отключить следующие службы:

- Удаленный реестр;
- Службы терминалов;
- Служба обнаружения SSDP;
- Служба сообщений;
- Оповещатель;
- Планировщик заданий;
- NetMeeting Remote Desktop Sharing;
- Диспетчер сеанса справки для удаленного рабочего стола.

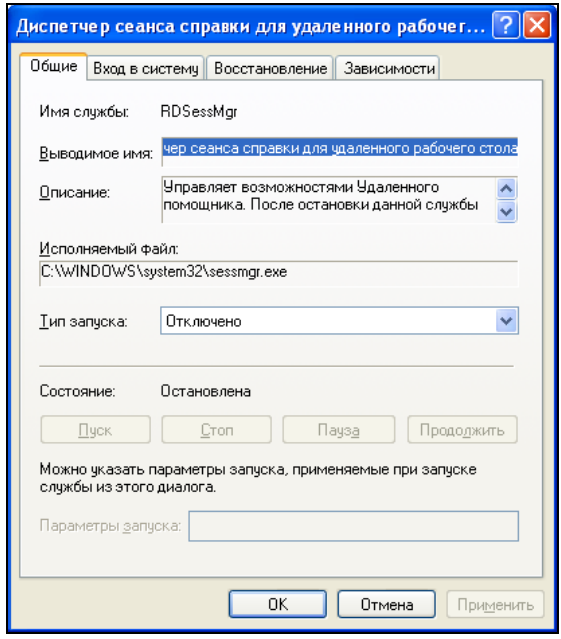


Рис. 19.17. Отключение службы

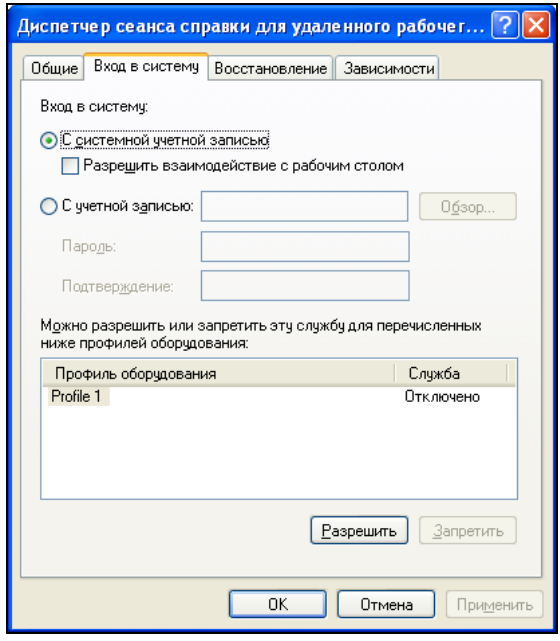


Рис. 19.18. Запрещение входа в систему службы

Все эти службы содержат уязвимости, которые могут использоваться вирусами для вторжения в вашу систему.

Для отключения службы выполните на ней двойной щелчок, нажмите кнопку **Стоп** (если она запущена), затем выберите тип запуска **Отключено** (рис. 19.17). После этого перейдите на вкладку **Вход в систему** и нажмите кнопку **Запретить** (рис. 19.18).

После отключения всех опасных служб щелкните правой кнопкой мыши на пиктограмме **Мой компьютер** и выберите команду **Свойства**. Перейдите на вкладку **Удаленное использование** и снимите оба флажка (рис. 19.19).

Вот теперь можно считать вашу Windows защищенной.

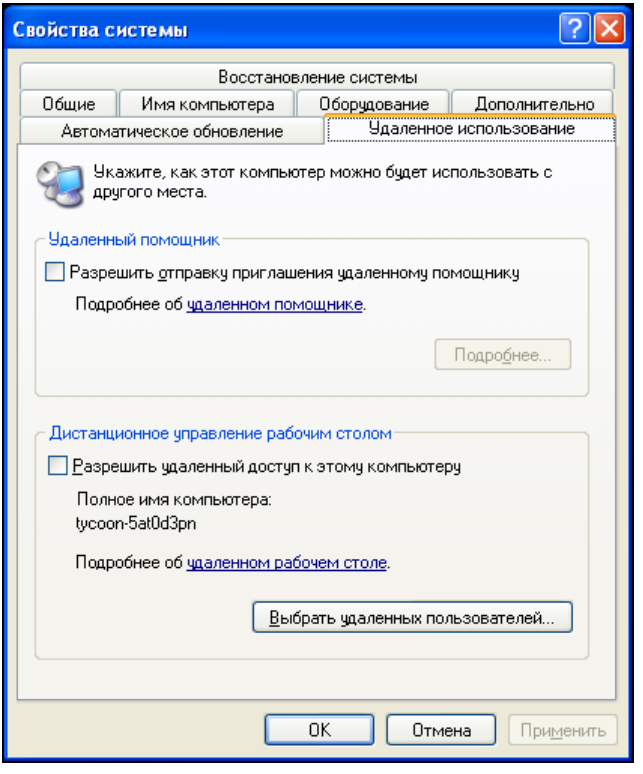


Рис. 19.19. Отключение удаленного помощника и удаленного доступа к вашему компьютеру

Глава 20

Защита маршрутизатора

Откройте любое пособие по сетевой безопасности. В большинстве случаев огромное внимание уделяется защите брандмауэров, но практически ничего не сказано о защите маршрутизатора, а ведь именно это устройство обеспечивает маршрутизацию пакетов, и сбои в работе маршрутизатора могут парализовать работу всей сети. Но почему-то о маршрутизаторе забывают, рассматривая защиту отдельных служб сервера и конфигурирование брандмауэра. В этой главе мы поговорим о защите обычного управляемого маршрутизатора. По возможности, я не буду привязываться к конкретному бренду и конкретной модели, но некоторые пояснения сделаю на примере Cisco IOS, поскольку, что ни говори, маршрутизаторы CISCO являются одними из самых распространенных на наших просторах.

20.1. О маршрутизаторе

Маршрутизатор, как и следует из его названия, обеспечивает маршрутизацию пакетов — это его основная задача. Но современные роутеры совсем не похожи на первые маршрутизаторы. Да, маршрутизацию пакетов никто не отменял, но многие современные маршрутизаторы имеют также функции организации *фильтрации пакетов* (то есть маршрутизатор выполняет роль брандмауэра), для организации VPN-шлюзов и много других функций, полезных и не очень. По сути, современный маршрутизатор — это специальный компьютер, управляемый собственной операционной системой. Многие "встроенные" операционные системы отчасти похожи на UNIX. Но почему-то администрирование и настройку UNIX-серверов все рассматривают, а о роутерах забывают. Сегодня мы попробуем применить принципы защиты UNIX-сервера к обычному маршрутизатору. Что из этого получится — судить вам.

Некоторые сверхдорогие маршрутизаторы оснащаются специальными функциями защиты от атак (например, существует специальная версия IOS — Firewall Feature Set, в которой реализованы функции *системы обнаружения вторжений* (IDS, Intrusion Detection Systems). Рассматривать здесь такие устройства смысла нет — если вам нужны функции IDS, купите такой маршрутизатор и настройте его так, как описано в документации.

Настройку маршрутизатора мы рассмотрим на примере управляемого маршрутизатора среднего класса и сконцентрируем свое внимание на защите самого маршрутизатора, а не узлов, которые находятся за ним.

20.2. Установка пароля

Любой управляемый маршрутизатор позволяет установить пароль для доступа к консоли управления. По умолчанию пароль или вообще отсутствует, или же используется стандартный пароль, который стандартно и "взламывается". Точнее, тут и взламывать нечего: злоумышленнику просто нужно знать модель вашего маршрутизатора, а пароль можно найти в Интернете, — после этого доступ к маршрутизатору ему гарантирован. Поэтому не забываем установить хороший пароль. Напомню, что в пароль не следует включать личные данные или их фрагменты (например, год своего рождения), а также общедоступные сведения о компании (название, аббревиатуру), он должен состоять не менее, чем из восьми символов разного регистра, желательно также использовать не только буквы, но и цифры.

Некоторые маршрутизаторы позволяют установить пароль длиной до 80 символов. Не стоит пользоваться этой возможностью. Такой пароль вы никогда не запомните, поэтому где-нибудь его сохраните — следовательно, этот пароль можно будет найти на вашем компьютере.

20.3. Ограничение доступа по сети

Получить доступ к консоли управляемого маршрутизатора можно локально (подключившись к AUX[1]) или же по сети. Для такого подключения обычно используется протокол Telnet или SSH. При сетевом доступе нужно ограничить узлы, с которых разрешен доступ к консоли управления маршрутизатором. Все управляемые маршрутизаторы позволяют сделать это.

Если есть выбор между Telnet и SSH, то лучше выбрать SSH, поскольку Telnet передает информацию (в том числе и пароли) по сети в открытом виде, что нежелательно.

[1] AUX — сокращение от Auxilary. Так называется порт, используемый для управления маршрутизатором.

20.4. Только локальный доступ

Наверное, самый надежный способ ограничения доступа — это запрещение сетевого доступа. В этом случае доступ к маршрутизатору будет возможен только локально, с помощью AUX. То есть злоумышленнику, чтобы изменить параметры маршрутизатора, придется физически подойти к нему и подключиться к AUX. А сделать это ему следует максимально затруднить. Если же маршрутизатор размещен в отдаленной части помещения, целесообразно также установить скрытую видеокамеру, чтобы знать, кто и когда подходил к маршрутизатору.

20.5. Защита SNMP

Для управления маршрутизаторами очень часто применяется *простой протокол управления сетью* (SNMP, Simple Network Management Protocol). Из соображений безопасности лучше вообще отключить SNMP, но если он вам нужен, убедитесь, что используется более защищенная, третья версия (SNMPv3). В более ранних версиях (SNMPv1, SNMPv2) авторизация и защита данных не предусмотрены.

И если вы все-таки не отключаете SNMP, то примите максимальные меры по обеспечению безопасности, а именно:

- придумайте трудно подбираемое имя community;
- MIB (Management Information Base) должна работать в режиме "только чтение";
- ограничьте SNMP-доступ несколькими узлами (желательно одним — вашим).

20.6. Ведение журналов

Наверняка в вашей компании найдется хотя бы одна машина под управлением UNIX (Linux). Так вот, в составе UNIX имеется *демон протоколирования* — syslogd, который можно настроить на протоколирование событий маршрутизатора. Для большей надежности рекомендуется запустить syslogd, настроенный на протоколирование событий маршрутизатора, на нескольких UNIX-машинах. Дело в том, что syslogd использует протокол UDP (а не TCP), который не гарантирует доставку пакетов, поэтому и нужно запускать несколько демонов протоколирования (если один не запротоколирует, то у второго точно все получится). Протоколировать нужно не все события,

а только те, которые затрагивают сетевую безопасность, например, попытки неудачной авторизации по ACL (спискам доступа).

Желательно также использовать протокол NTP (Network Time Protocol) для синхронизации времени, что существенно помогает при анализе протоколов (чтобы на разных машинах не было разницы во времени).

20.7. Отключение ненужных сервисов

Отключите все сервисы, которые вы не используете (например, finger, BOOTP, ARP Proxy). Ведь каждый такой сервис может стать "дырой" в системе безопасности маршрутизатора.

20.8. Ограничение протокола ICMP

Некоторые DoS-атаки (DoS, от Denial of Service, отказ в обслуживании) используют протокол ICMP (Internet Control Message Protocol — межсетевой протокол управляющих сообщений) в качестве основного инструмента атаки, поэтому желательно ограничить использование этого протокола, разрешив только пакеты определенных типов. В первую очередь, нужно ограничить пакеты PMTU (Path MTU discovery), пакеты с сообщением "packet-too-big". Что делать с другими типами ICMP-сообщений, зависит от вашей политики безопасности.

20.9. Отключение потенциально опасных опций

К потенциально опасным опциям маршрутизаторов относятся **IP source route** и **IP unreachables**.

- В первом случае (**IP source route**) злоумышленник может определить путь, по которому будет передаваться пакет. После этого он может послать пакет source routed на "узел-жертву", который находится за маршрутизатором, и тем самым изменить маршрутизацию атакуемой сети.
- Во втором случае (**IP unreachables**), если пакет отброшен в соответствии со списком доступа (ACL), злоумышленник получит ICMP-пакет (тип 3, код 13), на основании чего сможет сделать вывод, что маршрутизатор защищен с помощью ACL, а это нежелательно. Чем меньше информации о нашем маршрутизаторе, тем меньше вероятность взлома. Поэтому опцию **IP unreachables** следует отключить.

Для отключений опций **IP source route** и **IP unreachables** на маршрутизаторах Cisco нужно ввести IOS-команды:

```
no ip source-route
no ip unreachables
```

20.10. Anti-spoofing и защита от DoS-атак

IP-spoofing — это неавторизированный доступ к компьютеру (серверу) путем подделки IP-адреса. Например, вы разрешили доступ к своему маршрутизатору узлу с определенным адресом, а злоумышленник может подделать этот адрес с целью получения доступа. Для защиты от этого нужно использовать *антиспуфинг*, основная идея которого заключается в том, что никто из внешней сети не имеет право отправлять пакеты, содержащие в поле адреса источника какой-нибудь адрес из вашей подсети. Для фильтрации таких пакетов следует использовать списки доступа, желательно также зафиксировать попытку подделки IP-адреса в журнале.

Защита от DoS-атак заслуживает отдельного разговора. Здесь мы не будем комплексно рассматривать такую защиту, а поговорим только о двух самых распространенных DoS-атаках.

- Первая из них называется SYN flood. Она происходит, когда злоумышленник отправляет на открытый порт много SYN-пакетов с недостижимым адресом источника. Атакуемый маршрутизатор должен ответить пакетом `<SYN, ACK>`, но ведь узел, указанный в качестве источника, недоступен, поэтому трехступенчатая схема установления TCP-соединения не завершается. Учитывая, что таких SYN-пакетов очень много, лимит на количество открытых соединений очень быстро превышается, и жертва отказывается принимать запросы на установление соединения от обычных пользователей сети.

  Руководство по защите маршрутизаторов Cisco от SYN-атак можно найти по адресу: **http://cio.cisco.com/warp/public/707/4.html**.

- Вторая атака (она называется Land) заключается в том, что злоумышленник посылает пакет с одинаковыми портами и IP-адресами источника и получателя. Такие пакеты вызывают исключения во многих маршрутизаторах.

  Информацию о Land-атаке можно найти по адресу: **http://www.cisco.com/warp/public/770/land-pub.shtml**.

20.11. Отключение CDP

CDP (Cisco Discovery Protocol) — протокол, работающий на всем оборудовании Cisco, он используется для управления сетями. Протокол CDP позволяет оповестить другие устройства Cisco о присутствии в сети того или иного устройства от Cisco — другими словами, устройства Cisco с помощью этого протокола находят друг друга.

Используя CDP, можно получить информацию об устройстве, его конфигурации, низкоуровневых протоколах, а также о соседних машрутизаторах. Помните основной принцип защиты любой информационной системы — минимум информации. Чем больше информации вы предоставите злоумышленнику о своей сети, тем быстрее он ее взломает. Поэтому CDP нужно отключить. Для этого используется следующая IOS-команда:

```
no cdp run
```

20.12. Вместо заключения

Мы рассмотрели основные этапы защиты маршрутизатора. Вам остается лишь настроить ваш маршрутизатор, следуя приведенным здесь рекомендациям.

Часть VI

PowerLine — Интернет "из розетки"

Шестая часть книги посвящена еще одной "почти беспроводной" технологии — PLC (Power Line Communications). Еще семь лет назад никто и не думал, что Интернет можно получать "из розетки", а пять лет назад, когда на рынке появились первые коммерческие версии PLC-адаптеров, никто не верил, что эта технология приживется. А получилось так, что она не только прижилась, но и развивается. Скорость передачи данных на современных PLC-устройствах достигает 200 Мбит/с.

Глава 21

Обзор технологии Power Line Communication

21.1. Почти беспроводная технология

На что только не пойдут, чтобы не прокладывать кабели! Беспроводные сети были придуманы именно по этой причине. Воистину, лень — двигатель прогресса. В этой главе мы поговорим еще об одной почти беспроводной технологии — PLC (Power Line Communications). Это очень интересная технология, позволяющая передавать данные по электросети 220 В. Почему PLC я назвал *почти беспроводной* (или *псевдобеспроводной* — вот еще одно красивое название), наверное, вы уже догадались. Да, информация передается по силовым кабелям, но вам не нужно их прокладывать — электропроводка проложена строителями еще до вас.

PLC-сеть выглядит так — к компьютеру подключается PLC-адаптер, который, в свою очередь, подключается к электросети напряжением 220 В. Никаких монтажных работ, никакой витой пары, никаких проблем с интерференцией сигнала. Конечно, свои особенности у этой технологии есть, но о них мы поговорим позже. Скорость передачи данных в PLC-сети, как уже отмечалось, может достигать 200 Мбит/с. В любом случае PLC-сети можно рассматривать в качестве достойной альтернативы Ethernet-сетям и Wi-Fi.

Основное преимущество PLC-сетей — простота монтажа. Собственно, никакого монтажа и не нужно: подключаете адаптеры к компьютерам и к электросети. Сколько компьютеров, столько и адаптеров — потом все они оказываются в одной сети. Максимальное число узлов в PLC-сети — 64. Радиус действия каждого адаптера — 300 метров, что легко позволяет организовать домашнюю сеть и играть со своими соседями в Counter-Strike.

Технология PLC успешно используется в Европе и Америке, у нас пока PLC-сети не очень распространены, но постепенно набирают популярность.

21.2. Технология PLC и ее стандарты

Технология PLC — относительно молодая технология, известная как "Интернет из розетки". Как уже было сказано, с ее помощью можно легко и быстро создать сеть внутри дома или внутри квартиры. Технология эта основана на частотном разделении сигнала, когда поток данных разбивается на несколько низкоскоростных потоков, передающихся каждый на своей отдельной частоте. Реально используются 84 поднесущие частоты в диапазоне 4–20 МГц. Затем все эти потоки объединяются в один сигнал.

PLC-устройства отправляют и принимают сигнал по силовым линиям, но это никак не отражается на работе других электрических устройств, подключенных к этой же сети питания, — во время работы сети лампочки мигать не будут, а телевизор будет показывать картинку без помех.

PLC предусматривает два режима передачи данных:

- BPL (Broadband over Power Lines) — широкополосная передача по линиям электропередачи. Скорость передачи данных более 1 Мбит/с;
- NPL (Narrowband over Power Lines) — узкополосная передача по линиям электропередачи.

При передаче данных по бытовой электросети могут возникать большие затухания сигнала на определенных частотах, что приводит к потере данных. Для решения этой проблемы был разработан *метод динамического включения и выключения передачи сигнала* (в англ. литературе он называется Dynamically turning off and on data-carrying signals). Заключается он в следующем. PLC-устройство осуществляет постоянный мониторинг канала передачи данных с целью выявления затухания. В случае обнаружения затухания на какой-то частоте, временно прекращается использование этой частоты до тех пор, пока не будет восстановлено нормальное значение затухания.

Как уже было отмечено ранее, PLC-устройства никак не влияют на работу бытовой электроники. Наоборот, мощные бытовые приборы (например, проточные бойлеры, холодильники, пылесосы) являются причиной импульсных помех (до 1 микросекунды).

Первые PLC-устройства не отличались особой шустростью. Но с появлением технологии ею заинтересовались крупнейшие производители телекоммуникационного оборудования. Эти производители объединились в альянс HomePlug Powerline Alliance. В итоге, 26 июня 2001 года появился стандарт HomePlug 1.0, определяющий спецификации передачи данных по силовым

линиям со скоростью 14 Мбит/с. В настоящее время приняты и используются следующие стандарты:

- HomePlug Turbo — максимальная скорость передачи данных 85 Мбит/с;
- HomePlug AV — максимальная скорость передачи данных 200 Мбит/с.

В настоящее время все PLC-устройства соответствуют одному из этих стандартов. Более дешевые — HomePlug Turbo, более дорогие — HomePlug AV.

21.3. PLC и Wi-Fi

А что же Wi-Fi-сети? Ведь для их организации тоже не нужны провода. Но, оказывается, PLC-сети в чем-то лучше сетей Wi-Fi. PLC-сети превосходят сети Wi-Fi по скорости передачи данных и по радиусу действия. Скорость передачи данных PLC-сети составляет 129–200 Мбит/с. Сеть 802.11g может обеспечить всего 54 Мбит/с, а сеть 802.11n — 100 Мбит/с. Радиус действия внутри помещения тоже впечатляет: 300 метров против максимум 100 метров в сети Wi-Fi.

Взгляните на данные табл. 21.1, и вы поймете, что PLC-сеть является серьезным конкурентом, по крайней мере, Wi-Fi-сетям.

Таблица 21.1. *Сравнительные характеристики сетевых технологий*

Технология	Скорость передачи данных, Мбит/с	Длина сегмента или радиус действия внутри помещения для Wi-Fi, м
Fast Ethernet	100	100
Gigabit Ethernet	1000	100
IEEE 802.11g	54	35–100
IEEE 802.11n	100–300	35–100
PLC	129–200	300

Однако технология PLC все-таки имеет некоторые ограничения по области применения. Ее удел — это только домашние сети. Предположим, вам нужно построить домашнюю сеть, чтобы все желающие жители многоэтажки смогли обмениваться данными и играть в сетевые игры. В этом случае, возможно, PLC-сеть будет идеальным решением. Не требуется тянуть кабели, не надо устанавливать оборудование (коммутаторы и точки доступа), которое могут попросту украсть. Все, что нужно, — это приобрести PLC-адаптеры по количеству клиентов в сети. Учитывая, что в одном корпусе многоэтажки

примерно 108–144 квартиры (9 этажей, 4 квартиры на этаже и 3–4 подъезда), то PLC-сеть может охватить весь корпус. Ограничение на количество клиентов нам здесь не помеха — далеко не всем захочется подключаться к вашей сети, и не у всех есть компьютеры. Поэтому в 64 узла вы должны "вписаться".

Другое дело — офисное здание. В среднем офисном здании от 180 офисов (20 офисов на этаж, 9 этажей). Интернет сейчас нужен практически всем, поэтому можно ожидать, что подключать придется почти все офисы, а это минимум 180 клиентов. PLC-сеть выдерживает нагрузку только в 64 клиента. Wi-Fi-сеть тоже не справится с такой нагрузкой. Так что в этом случае альтернативы Ethernet-сетям нет.

Если же рассматривать альтернативные технологии (PLC и Wi-Fi) для подключения дополнительных узлов — скажем, клиентов вашей фирмы, которые "заглянули в гости", тогда уже лучше выбрать технологию Wi-Fi. Сейчас большинство ноутбуков оснащено Wi-Fi-адаптерами, а не PLC, — ожидать, что клиент "нагрянет" со стационарным компьютером, да еще и со своим PLC-адаптером, не приходится.

21.4. Преимущества и недостатки PLC-сетей

А теперь рассмотрим преимущества и недостатки PLC-сетей более подробно. По сравнению с Ethernet и другими проводными сетями у PLC-сетей есть следующие преимущества:

- не нужно сверлить стены и опорные конструкции для прокладки кабеля;
- простота настройки и использования;
- скорость монтажа.

По сравнению с Wi-Fi:

- более стабильная связь;
- выше скорость передачи данных (если сравнивать с 802.11g, ведь 802.11n еще не принят);
- практически не требует настроек;
- выше безопасность передаваемых данных;
- на качество сигнала не влияет материал и толщина стен;
- подходит для передачи Multicast-трафика (IPTV).

Но, как у любой другой технологии, у PLC есть и недостатки. Вот их перечень:

- заявленная пропускная способность делится между всеми ее участниками. Это значит, что если в сети имеются 4 устройства, которые попарно обмениваются данными, то максимальная скорость передачи данных для каждой пары устройств составит примерно 100 Мбит/с (а не 200 Мбит/с);
- PLC-адаптеры не работают через сетевые фильтры и ИБП, поэтому для подключения адаптера нужна свободная розетка;
- на качество связи влияют мощные бытовые приборы, дешевые энергосберегающие лампы, импульсные блоки питания и зарядные устройства. Но при этом снижение скорости составляет не более 10%;
- PLC-устройства нарушают радиоприем на средних и коротких волнах.

А теперь подумаем, нужны ли нам PLC-устройства и в каких областях применения их преимущества наиболее наглядны. С одной стороны, их использование очень удобно для домашних пользователей. С другой — некоторые недостатки в ряде ситуаций могут свести на нет все преимущества этих сетей. Пусть у пользователя рядом с компьютером имеется одна простая розетка. К ней подключается "пилот" или ИБП, а через него — компьютер. Поскольку PLC-адаптер не будет работать через фильтр питания или ИБП, то пользователю нужно или устанавливать двойную розетку, или тянуть удлинитель порой через всю комнату от другой розетки (ну или тянуть через всю комнату Ethernet-кабель от PLC-адаптера к компьютеру). Одним словом, вся разрекламированная простота монтажа сводится к установке еще одной розетки[1], а это создает определенные неудобства. Так, не каждый пользователь, в надежде на простоту установки и настройки купивший PLC-адаптеры для соединения в сеть двух компьютеров, находящихся в разных комнатах, сам сможет заменить розетку или обжать витую пару (а для обжатия витой пары еще потребуется специальный инструмент). Тут созревает вопрос: не проще ли сразу было соединить напрямую эти два компьютера, сэкономить кучу денег и при этом получить скорость соединения 1 000 Мбит/с, а не всего 200 Мбит/с!

Таким образом, вполне доказано, что применение PLC-технологии для малых внутриквартирных сетей, очевидно, смысла не имеет. А вот рассмотренный ранее случай охвата частной сетью многоэтажного здания вполне имеет право на существовование.

Второй недостаток, существенный для обычных домашних пользователей, — это помехи, которые вносят PLC-устройства в радиоприем на средних и коротких волнах. А что если вы любите слушать радио? Понимаю, что есть онлайн-радио, но обычные приемники пока никто не отменял!

[1] Впрочем, можно ведь и обычным "тройником" воспользоваться.

21.5. Стоит ли использовать PLC?

Итак, вы познакомились со всеми преимуществами и недостатками PLC-сети. Осталось решить, стоит ли устанавливать такую сеть дома? Ответить на этот вопрос поможет математика — самая точная наука.

Как уже отмечено, удел PLC — домашняя сеть. Вот давайте просчитаем стоимость такой сети для конкретного домашнего пользователя. Представим, что у нас есть два стационарных компьютера и один ноутбук. PLC-адаптер ZyXEL PLA400 EE стоит примерно 2 968 рублей (это средняя цена в интернет-магазинах). И не нужно думать, что если производитель ZyXEL — то это дорого. PLC-адаптеры других производителей в среднем стоят те же 3 000 рублей (плюс-минус). Зато ZyXEL входит в состав альянса HomePlug Powerline Alliance и выпускает гарантированно качественные продукты.

Для построения нашей сети потребуются три PLC-адаптера, итого имеем:

$$3 \times 2\,968 = 8\,904 \text{ рублей.}$$

Чтобы сеть получилась дешевле, в качестве маршрутизатора будет выступать один из наших компьютеров, поэтому максимум, что нам еще нужно, — дополнительный сетевой адаптер. К счастью, он стоит совсем недорого — примерно 200 рублей. Таким образом, наша сеть обойдется нам в 9 100 рублей.

Теперь посчитаем стоимость Wi-Fi-сети. Средняя точка доступа стоит от 2 000 до 3 600 рублей в зависимости от ее функций и производителя. Чтобы все было честно, возьмем точку доступа ZyXEL P660HTW2, которая стоит 3600 рублей, но сочетает в себе функции точки доступа и коммутатора. Ноутбук будет подключаться "по воздуху", а стационарные компьютеры — по Ethernet. Заложим в расчет 20 метров кабеля (по 10 метров на один компьютер) — стандартные 10-метровые кабели продаются уже обжатыми, поэтому ни вилки, ни инструмент для обжима нам не понадобятся. Один такой кабель стоит 150 рублей (максимум) — итого 300 рублей на кабели. Вроде бы все. В качестве маршрутизатора тоже выступит наша точка доступа. Таким образом, общая стоимость спроектированной Wi-Fi-сети — 3 900 рублей. Если же вы захотите подключать стационарные компьютеры тоже "по воздуху", то вам понадобятся еще 2 беспроводных адаптера по 1 200 рублей каждый. В итоге выйдет: 3 600 + 1 200 + 1 200 = 6 000 рублей. Но никак не 9 100!

Получается, беспроводная сеть дешевле. А если есть желание сэкономить еще больше, тогда выбирайте Ethernet-сеть. Обычный 5-портовый неуправляемый коммутатор стоит около 500 рублей. К этой сумме нужно доба-

вить стоимость трех Ethernet-кабелей: 450 рублей (3 кабеля по 150 рублей), итого: 950 рублей. Правда, придется потратить некоторое время на монтаж кабеля.

Что ж, при наличии желания, времени и определенных навыков самым дешевым вариантом остается пока Ethernet-сеть. Wi-Fi-более удобен, но и более дорог. Удобство PLC-сети для внутриквартирной сети под вопросом, а по стоимости она явно превосходит и Wi-Fi, и Ethernet. Нужна она или нет — решать только вам. Я свой выбор сделал в пользу Wi-Fi. Но в любом случае мы в следующей главе рассмотрим создание PLC-сети.

Глава 22

Построение PLC-сети

22.1. Обзор PLC-адаптеров от ZyXEL

В *главе 21* было показано, что с точки зрения экономии лучше выбрать Ethernet-сеть, а с точки зрения комфорта — сеть Wi-Fi, которая является оптимальной по соотношению цена/комфорт. А вот комфорт технологии PLC для внутриквартирной сети под вопросом (как уже отмечалось, для PLC-адаптера нужна отдельная свободная розетка, которой, как всегда, нет), да и цена высока даже для Wi-Fi-сети. Единственное преимущество PLC-сети — скорость передачи информации: в идеальных условиях можно получить до 200 Мбит/с. Идеальные условия: это всего 2 адаптера в PLC-сети и отсутствие помех от крупной бытовой техники.

Но посмотрим на PLC-сеть под другим углом. В предыдущей главе мы подсчитали стоимость сети из трех адаптеров примерно по 3 000 рублей каждый. Общая стоимость сети получилась порядка 9 000 рублей. Но это только в том случае, если вы сами будете покупать все три адаптера. Если же вы хотите быстренько организовать сеть, чтобы играть с соседями по дому в сетевые игры, то вам придется заплатить всего 3 000 рублей — только за свой личный адаптер (остальные каждый игрок купит себе сам). А если повезет, то можно найти такой адаптер и чуть дешевле — около 2 500 рублей. Выходит, не так уж и дорого. Зато не придется прокладывать кабель или искать источники интерференции и разбираться, почему два компьютера могут подключиться к точке доступа, а у третьего — проблемы с соединением. Максимум, что, возможно, придется сделать — это превратить одинарную розетку в двойную, к которой вы подключите PLC-адаптер, а дальше в действие вступает Ethernet-кабель, который соединит ваш компьютер с PLC-адаптером.

Напомню, что дальность распространения сигнала по электропроводке — 300 метров. До соседней квартиры и даже дальше — достанет, а вот до следующего дома — нет. Понятно, что для организации собственной внутриквартирной сети этого тоже вполне достаточно.

Сейчас мы исследуем линейку продуктов HomePlug AV от ZyXEL. Почему именно ZyXEL? Мне так показалось целесообразнее — ведь оборудование D-Link было рассмотрено при построении беспроводной сети, а о настройке коммутаторов Cisco мы поговорим в *главе 27*. Не хочется привязываться к конкретному производителю, но и охватить всех производителей в одной книге тоже невозможно.

Продукты серии HomePlug AV используют чипсет INT6000/6300 компании Intellon (**www.intellon.com**), которая специализируется на разработке чипов для PLC-адаптеров. Особенность этого чипа — отличная помехоустойчивость. Даже в проблемных условиях чип обеспечит минимальную скорость соединения 40 Мбит/с. Поэтому устройства HomePlug AV можно считать альтернативной прямому Ethernet-соединению для приема IP-телевидения в произвольной точке дома. Беспроводные сети для этого использовать нельзя, поскольку на данный момент стандартами 802.11* не предусмотрена передача широковещательного видеоконтента IPTV.

Средняя скорость передачи, обеспечиваемая устройствами HomePlug AV: 80–100 Мбит/с. Основные характеристики PLC-сети на базе устройств HomePlug AV приведены в табл. 22.1.

Таблица 22.1. *Основные характеристики PLC-сети на базе устройств HomePlug AV*

Характеристика	Значение
Максимальная скорость передачи данных	200 Мбит/с
Средняя скорость передачи данных	80–100 Мбит/с
Минимальная скорость передачи данных	40 Мбит/с
Дальность передачи данных	300 метров
Максимальное число клиентов	64
Шифрование передаваемых данных	AES, 128 бит

К сожалению, оборудование HomePlug AV несовместимо с устройствами HomePlug 1.0 (скорость 14 Мбит/с) и HomePlug Turbo (85 Мбит/с). Однако к одной и той же среде передачи данных (то есть к электропроводке) такие адаптеры могут подключаться для передачи данных между собой. Другими словами, нужно купить не просто PLC-адаптер, а именно адаптер из серии HomePlug AV. Поэтому, когда надумаете с соседом строить свою сеть, оборудование надо покупать вместе.

Вот еще одна забавная деталь: для PLC-адаптеров не нужны драйверы, и, вообще, им все равно, какая операционная система установлена на вашем

компьютере. У вас может быть Windows Vista, а у соседа Windows XP или Linux — вы сможете обмениваться данными. Дело в том, что совокупность электропроводки и PLC-адаптеров, подключенных к ней, можно рассматривать как коммутатор Ethernet-сети. Представьте, что вы подключаетесь не к PLC-сети, а к обычному коммутатору. Вот поэтому для PLC не важно, какая ОС будет у вас установлена — главное, чтобы ОС поддерживала вашу сетевую карту.

Однако для запуска утилиты мониторинга адаптера нужна ОС Windows XP или Vista, но это уже, как говорится, нюансы. PLC-сеть прекрасно работает и без запуска таковой утилиты.

В серию HomePlug AV входят следующие устройства (напомню, производитель — ZyXEL):

- PLA400 — PLC-адаптер с одним портом Ethernet;
- PLA470 — PLC-адаптер с 4-портовым коммутатором Ethernet;
- P660HWP — интернет-центр для подключения по ADSL2+ с точкой доступа Wi-Fi 802.11g, 4-портовым коммутатором и адаптером HomePlug AV;
- NBG318S — интернет-центр для выделенных линий Ethernet с точкой доступа Wi-Fi 802.11g, 4-портовым коммутатором Ethernet и адаптером HomePlug AV;
- DMA1100P — сетевой медиаплеер с подключением по Ethernet и проводке.

Далее мы рассмотрим все эти устройства подробнее.

22.1.1. Адаптер PLA400

Адаптер PLA400 — самое простое (и самое дешевое) устройство в линейке HomePlug AV. Он позволяет подключить к сети всего один компьютер. Сам адаптер подключается в свободную розетку, а с компьютером соединяется посредством Ethernet-кабеля. На корпусе адаптера PLA400 имеется переключатель, позволяющий выбрать тип Ethernet-кабеля: обычный или кроссовер (с перекрестным обжимом). Как видите, все для удобства пользователя. Схема сети может быть примерно такой, как показано на рис. 22.1.

В этой сети имеются три сетевых устройства: компьютер, ноутбук и маршрутизатор. Все устройства объединяются в сеть с помощью адаптеров PLA400. Технология PLC, как отмечалось ранее, — это просто расширение сети Ethernet, поэтому сеть не нуждается больше в дополнительной настройке. IP-адреса (и другие сетевые настройки) в данном случае будут присваиваться автоматически DHCP-сервером, запущенным на маршрутизаторе.

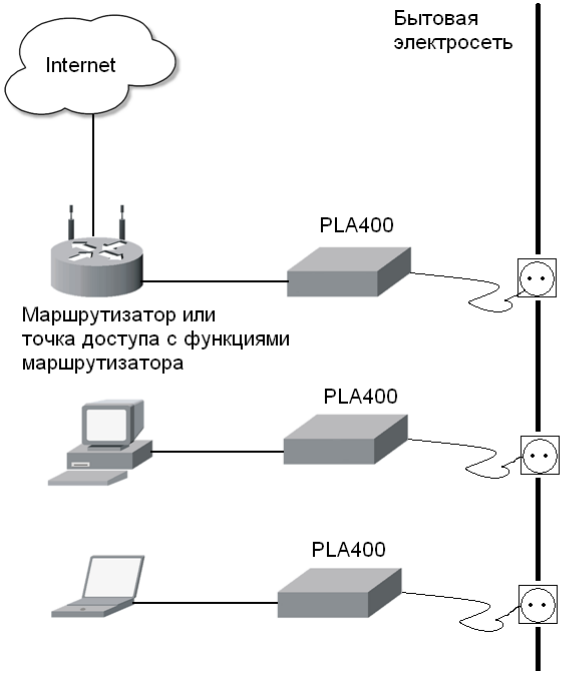


Рис. 22.1. Схема сети на базе адаптеров PLA400

Схема, приведенная на рис. 22.1, не показывает всех имеющихся возможностей. К PLC-сети можно еще подключить ресивер IPTV (он соединяется с PLC-адаптером и с телевизором) — тогда вы сможете принимать IP-телевидение. Главное, чтобы был оператор, вещающий IPTV в вашем доме по PLC-сети. А еще к PLC-адаптеру можно подключить сетевой принтер, и он будет работать так, как если бы он был подключен к обычной Ethernet-сети.

22.1.2. Адаптер PLA470

Адаптер PLA470 обладает четырехпортовым Ethernet-коммутатором, поэтому его можно использовать для подключения к PLC-сети до четырех компьютеров, находящихся в одной квартире. Данный адаптер стоит дороже, чем PLA400, но возможность подключения сразу нескольких компьютеров в итоге экономит ваши деньги. Средняя стоимость данного адаптера (на момент написания этих строк) в интернет-магазинах — 3 700 рублей. Как видите, не так уж и дорого. Схема сети с использованием этого адаптера представлена на рис. 22.2.

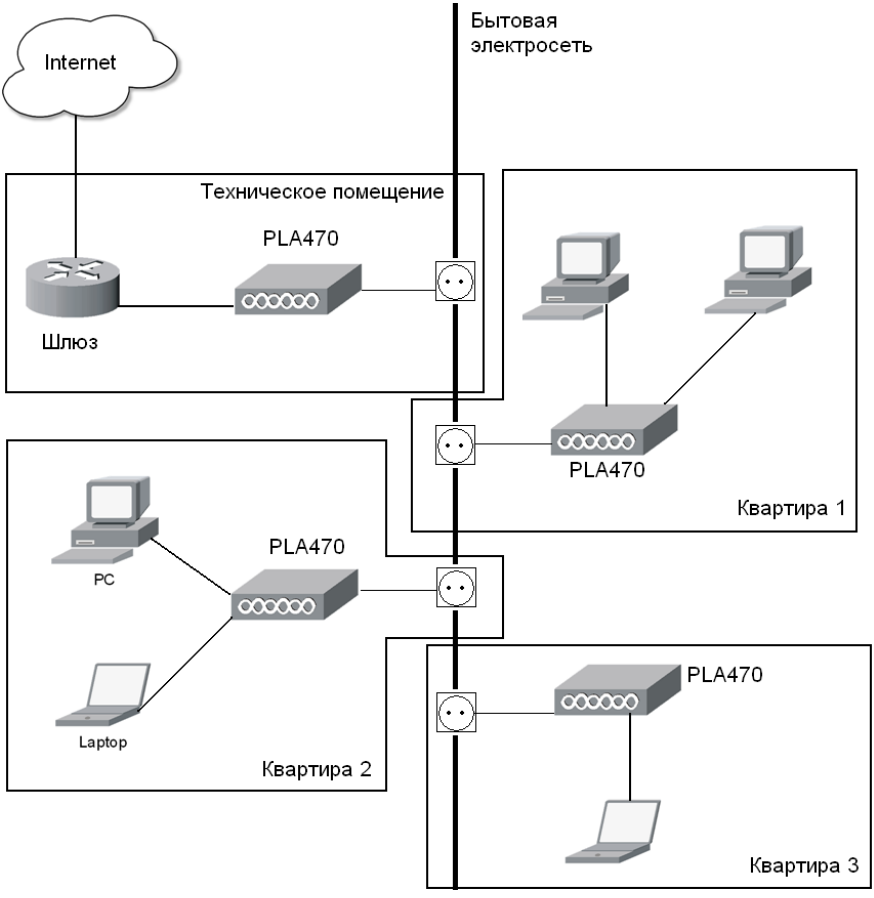


Рис. 22.2. Схема сети на базе адаптеров PLA470: удобный способ подключения к сети через одну розетку нескольких компьютеров

22.1.3. Интернет-центры P660HWP и NBG318S

Интернет-центры P660HWP и NBG318S — это устройства, построенные по принципу "все в одном". Купив, например, P660HWP, вы сразу обеспечиваете свою сеть ADSL-модемом, коммутатором, точкой доступа и PLC-адаптером. Беспроводные клиенты смогут подключаться к сети по Wi-Fi, проводные — по Ethernet (в P660HWP встроен коммутатор на четыре Ethernet-порта), а PLC-клиенты смогут подключаться к сети по электропроводке, как показано на рис. 22.3.

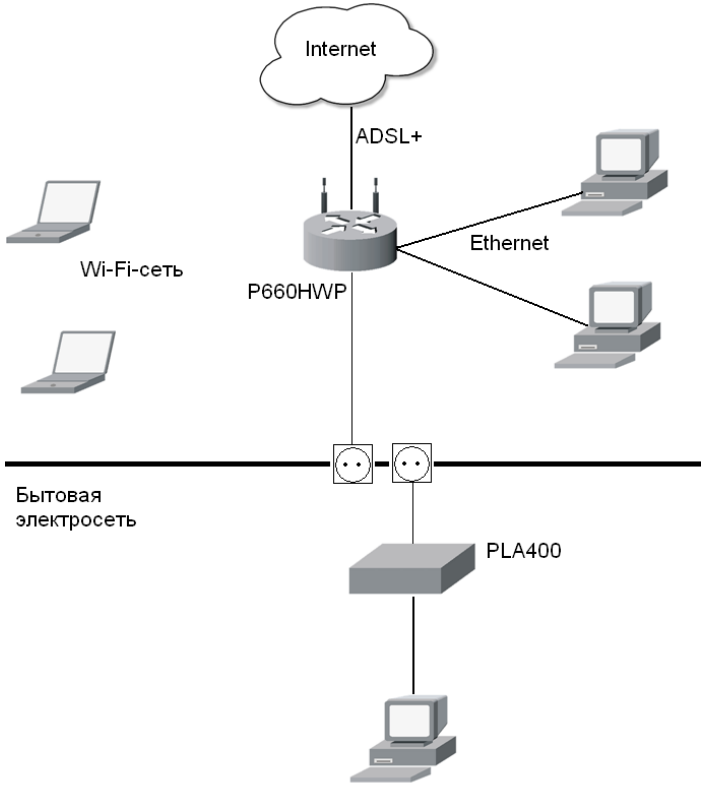


Рис. 22.3. Схема сети с применением интернет-центра

22.1.4. Устройство DMA1100P

Устройство DMA1100P — это сетевой мультимедиапроигрыватель. Его можно подключить к телевизору: как к обычному, так и поддерживающему стандарт High Definition. Если телевизора нет, то к DMA1100P можно подключить монитор по интерфейсу HDMI (жаль, что далеко не все мониторы поддерживают этот стандарт).

У DMA1100P (рис. 22.4) имеются разъемы Ethernet и USB. К USB-разъему можно подключить накопитель с фильмами, музыкой и картинками. Проигрыватель поддерживает следующие видео- и аудиоформаты: MPEG-1, MPEG-2, MPEG-4, AVI, WMV 9, DVD-Audio, AAC-LC, WMA9. Картинки могут быть в форматах TIFF, PNG, GIF, BMP, JPEG. В комплект проигрывателя входит пульт дистанционного управления.

Рис. 22.4. Проигрыватель DMA1100P

Позвольте мне высказать свое, сугубо субъективное, мнение относительно этого устройства. С одной стороны, оно подойдет желающим оснастить свою квартиру по последнему слову техники, но, с другой стороны, ничего примечательного в нем нет. Стоит это чудо почти 9 000 рублей. Теперь давайте подумаем, какие преимущества мы получим, купив его. Это устройство можно подключить к Ethernet-сети (как с помощью Ethernet-кабеля, так и с помощью технологии PLC). Конечно, это преимущество. Можно подключить его к сети и закачать на него фильм прямо с вашего основного компьютера. Но куда закачивать? Встроенного жесткого диска-то нет! Поэтому придется потратиться на внешний USB-диск (такой, который подключается к ноутбукам). Ведь от флешки, даже на 8 Гбайт, толку мало. А за внешний жесткий диск придется отдать еще несколько тысяч честно заработанных рублей. Выходит, стоимость устройства окажется уже не 9 000 рублей, а больше. Ладно, забудем о жестком диске. Может, он у вас уже есть, и вы готовы делить его с ноутбуком. Пусть. Двигаемся дальше. Устройство поддерживает формат MPEG-4. Но все мы знаем, что это только "обертка". А внутри может быть фильм, сжатый одним из кодеков. Кодеки же имеют свойство обновляться. Я уже и забыл, какова текущая версия DivX! На компьютере все легко и просто — установил новый кодек и забыл о нем до выхода следующей версии. Тут все намного сложнее. Придется перепрошивать устройство в сервисном центре. Хотя можно его перепрошить или нет, точно я вам не скажу. Устройство относительно молодое — на нашем рынке оно появилось весной прошлого года. А звонить в сервисный центр ZyXEL мне не с руки.

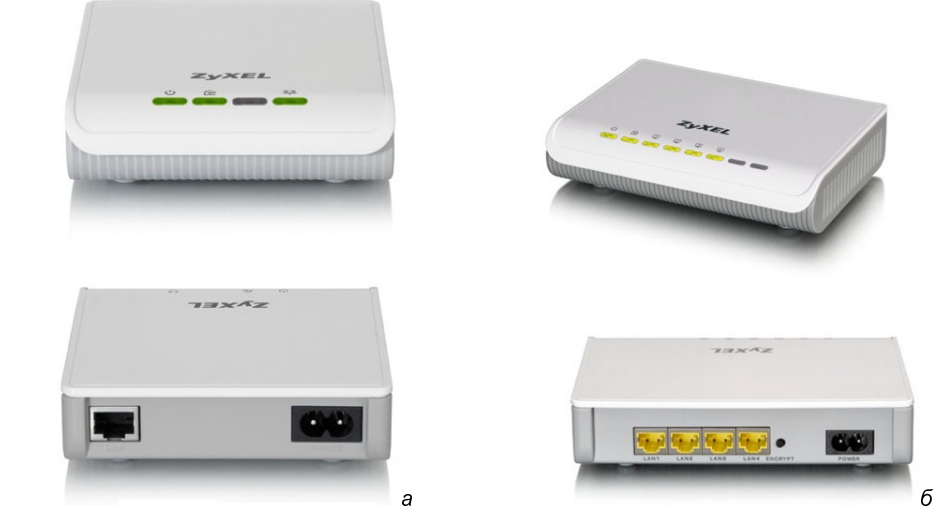
Как альтернативу этому проигрывателю я вижу недорогой б/у ноутбук с разъемом S-Video (или более дорогой — с разъемом HDMI, если ваш телевизор поддерживает этот формат). В итоге мы получим то же компактное устройство, но уже со встроенным жестким диском (то есть экономия на жестком диске — налицо). Ноутбук, как правило, можно подключить не только к Ethernet, но и к Wi-Fi-сети. Некоторые особо "нафаршированные" модели оснащаются инфракрасным портом и пультом ДУ. Чем не домашний кинотеатр? К тому же никаких проблем с обновлением кодеков — установил и забыл.

Другими словами, особой необходимости в таком устройстве я не вижу. Даже если вы не хотите тратиться на покупку ноутбука, можно купить обычный DVD-проигрыватель с поддержкой USB. Такие проигрыватели сейчас стоят намного дешевле, чем два года назад. И уж намного дешевле (примерно в 5–6 раз), чем DMA1100P. А флешку или USB-диск, я думаю, можно без особого труда перенести в другую комнату, где установлен телевизор с DVD-проигрывателем. Ведь все равно нужно идти туда для просмотра фильма.

Кстати, все это было сказано на фоне замены моего DVD-проигрывателя (который покупался всего 2 года назад и стоил совсем недешево) обычным ноутбуком. Теперь мне уже все равно, в каком формате записан фильм, — я его скачиваю из внутренней сети, подключаю ноутбук к телевизору и просто смотрю кино.

22.2. Подключение и настройка PLC-сети

Адаптеры PLA400 и 470 изображены на рис. 22.5. Как видите, PLA400 (рис. 22.5, *а*) оснащен всего одним Ethernet-портом, а PLA470 (рис. 22.5, *б*), как уже отмечалось, — четырехпортовым коммутатором.



а *б*

Рис. 22.5. Адаптеры PLA400 (*а*) и 470 (*б*)

Примечание

У адаптера PLA400 есть одна занимательная особенность. На его передней панели имеются четыре индикатора. Первый (если смотреть слева направо) — это индика-

тор питания, второй — индикатор наличия соединения с другим PLC-адаптером, четвертый — индикатор установки логического соединения, то есть он свидетельствует о наличии подключения к маршрутизатору, компьютеру или ресиверу IPTV. А как же третий? А третий не используется. Зачем он нужен — для меня загадка. Он даже не подписан.

Итак, приступим к подключению. Подключите адаптер к компьютеру с помощью Ethernet-кабеля. Если у вас адаптер PLA470, тогда подключите все ваши компьютеры к его портам. Затем подключите адаптер к свободной розетке. Напомню, розетка должна быть свободной. Нельзя подключать адаптер через фильтр "пилот" или источник бесперебойного питания. Нам осталось включить питание адаптера!

Если вы таким же образом подключили к сети маршрутизатор, то он по протоколу DHCP автоматически настроит все ваши узлы. Больше ничего настраивать не нужно (разве что кроме самого маршрутизатора) — вы можете подключиться к Интернету.

А вот если в вашей сети всего два компьютера: ваш и соседский, и вы хотите поиграть в какую-то игрушку, то можно настроить сеть вручную. Настройка Ethernet-соединения была подробно рассмотрена в *главе 5*. Напомню, что вы должны рассматривать PLC-сеть как обычную Ethernet-сеть, только вместо коммутаторов у вас PLC-адаптеры. Первому компьютеру нужно задать следующие параметры в настройках Ethernet-соединения:

- IP-адрес: 192.168.1.1;
- Маска подсети: 255.255.255.0;
- Шлюз по умолчанию: 0.0.0.0.

На втором компьютере параметры будут такими же, но нужно установить IP-адрес: 192.168.1.2.

А теперь поговорим о безопасности нашей сети. Похоже, что к нашей сети может подключиться кто угодно. Да, это так — пока вы не измените секретный ключ для доступа к сети. Изменить секретный ключ можно с помощью утилиты настройки адаптеров (рис. 22.6), которая поставляется на компакт-диске вместе с адаптером. Утилита локализована, весь ее интерфейс на русском языке — особых проблем с ее использованием вы не испытаете: просто впишите **Сетевой ключ** и нажмите кнопку **Сохранить**. Теперь передаваемые вами данные защищены от прослушивания алгоритмом AES с 128-битным ключом.

Жаль, что эта утилита не работает с другими операционными системами, кроме Windows XP и Vista.

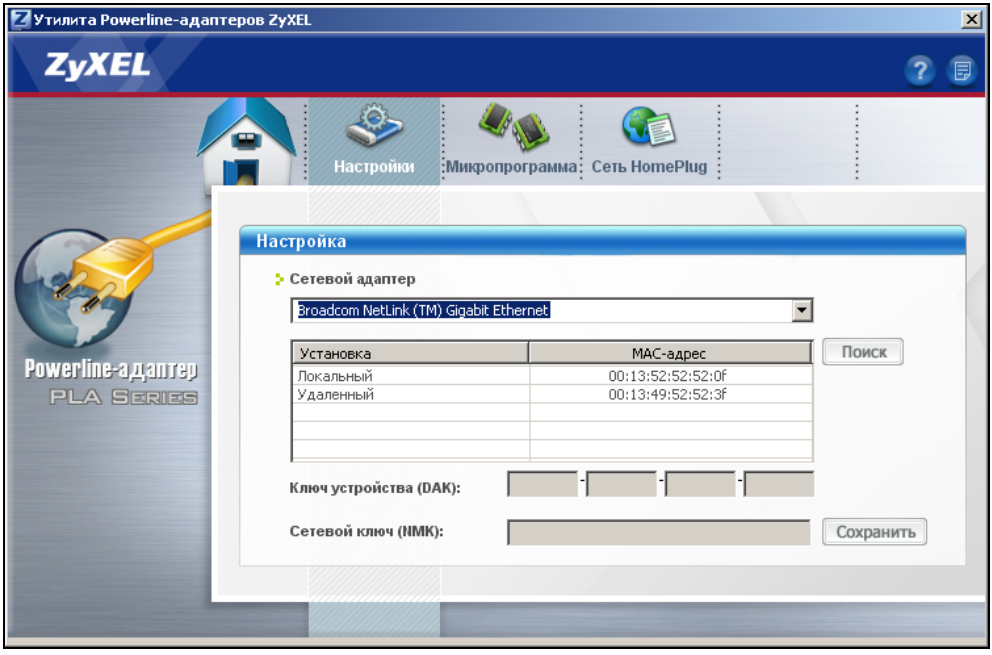


Рис. 22.6. Утилита настройки PLC-адаптеров ZyXEL

На этом все: мы рассмотрели выбор PLC-адаптера, ознакомились с возможными схемами подключения, настроили сеть и установили сетевой ключ. Осталось только приступить к использованию сети.

Часть VII

Повышение производительности сети

В седьмой части книги мы разберемся, как повысить производительность сети. Как известно, повышение производительности сети заключается не только в аппаратных решениях. Мы поговорим и о программной оптимизации сети, в частности об установке некоторых серверов, позволяющих повысить производительность сети. Мы рассмотрим модернизацию сети, настройку прокси-сервера, настройку кэширующего DNS-сервера и собственного DHCP-сервера, а также виртуальные локальные сети (VLAN). Все это в совокупности позволит не только повысить производительность сети, но и сэкономить трафик.

Глава 23

Факторы повышения производительности сети

23.1. Модернизация старой сети

Стоит или нет модернизировать вашу сеть, зависит от используемой в данный момент технологии и от ваших задач. Однозначно нужно модернизировать старые сети 10Base — их пропускной способности сегодня уже недостаточно. Ведь это только на бумаге ее скорость 10 Мбит/с, а на практике выходит около 5–6 Мбит/с.

23.1.1. Сети 10Base на коаксиальном кабеле

Если сеть достаточно старая, то она практически не подлежит модернизации. Рассмотрим сети на коаксиальном кабеле: 10Base-5 и 10Base-2. Что нужно, чтобы модернизировать такие сети до уровня Fast или Gigabit Ethernet? Коммутатор и витая пара. Но не надо забывать, что понадобятся еще и соответствующие сетевые адаптеры. Сетевой адаптер можно купить сейчас только для шины PCI, а на старых компьютерах, которые покупались, когда сети 10Base были оптимальными, таковой может и не оказаться. Сетевых адаптеров Fast Ethernet (не говоря уже о Gigabit Ethernet) для устаревшей шины ISA в природе не существует — эта шина не поддерживает скорость передачи 100 Мбит/с. Выход очевиден: вам придется приобрести не только новое сетевое оборудование, но и новые компьютеры.

23.1.2. Сети 10Base на витой паре

Теперь переходим к следующей технологии — 10Base, но на витой паре. Тут немного проще. Во-первых, существенного увеличения производительности можно добиться, заменив концентратор (хаб) на коммутатор. Да, его порты будут работать на скорости 10 Мбит/с, но, тем не менее, за счет замены центрального устройства на коммутатор прирост производительности произойдет.

Конечно, новые компьютеры, подключенные к коммутатору такой сети, будут работать на скорости 100 Мбит/с. Но тут появляется проблема несбалансированности сети: часть портов коммутатора будет работать на скорости 10 Мбит/с, а часть — на скорости 100 Мбит/с. Впрочем, на эту проблему можно посмотреть и с другой стороны. Если ваша сеть организована на витой паре, скорее всего, все компьютеры оснащены шиной PCI. Поэтому не составит труда установить в них новые адаптеры, поддерживающие технологию Fast Ethernet. А вот переходить с 10Base сразу на 1000Base не рекомендуется — старые компьютеры не справятся с такой производительностью сети — то есть, деньги вы потратите (в том числе и на более дорогую витую пару категории 6), а толку особого не получите.

Если в свое время при прокладке сети не экономили и использовали витую пару 5-й категории, то вы можете "отделаться" только заменой центрального устройства и сетевых адаптеров. А вот если использовалась витая пара 3-й категории, то придется заново прокладывать кабели. Для Fast Ethernet рекомендуется использовать витую пару категории 5E, что позволит со временем перейти на Gigabit Ethernet.

> ***Примечание***
>
> Напомню — витая пара категории 5E может использоваться и в сетях Fast Ethernet, и в сетях Gigabit Ethernet. А витая пара категории 6 — только в сетях Gigabit Ethernet.

Если не хочется заново тянуть кабель, можно оснастить все компьютеры беспроводными сетевыми адаптерами и установить одну или несколько точек доступа. Переход с сети 10Base на Wi-Fi-сеть стандарта 802.11g тоже сможет повысить производительность. Как уже было сказано ранее, на практике реальная скорость передачи данных по сети 10Base не превышает 5–6 Мбит/с. При переходе на 802.11g вы гарантированно получите 30 Мбит/с, что в 5–6 раз быстрее (максимальная скорость по стандарту 802.11g — 54 Мбит/с). Однако напомню, что для установки беспроводного сетевого адаптера нужна шина PCI (не думаю также, что на "древних" компьютерах, не имеющих шины PCI, вы найдете шину USB 1.1, чтобы подключить USB-адаптеры Wi-Fi).

23.1.3. Сети Fast Ethernet

Перейти с Fast Ethernet на Gigabit Ethernet иногда очень просто, а иногда — нет. Если сеть строилась год, максимум два года назад (2007–2008 гг.), то можно предположить, что:

- использовалась витая пара категории 5E — вам не нужно будет заново прокладывать кабель;

- встроенные сетевые адаптеры материнских плат поддерживают Gigabit Ethernet (на материнских платах, изготовленных в конце 2007 года, с вероятностью 90% будет установлен такой сетевой адаптер. В 2008 году практически все встроенные адаптеры поддерживали Gigabit Ethernet).

В этом случае, как вы уже догадались, нужно заменить только центральные устройства (если их несколько) — коммутаторы. И все — вы счастливый обладатель сети Gigabit Ethernet. А вот если при прокладке кабеля экономили и использовали витую пару категории 5, тогда кабель придется прокладывать заново. В этом случае уже лучше взять витую пару категории 6. Проблем с заменой сетевых адаптеров не будет — нужно только отключить в BIOS компьютеров встроенные сетевые адаптеры и установить новые адаптеры, поддерживающие Gigabit Ethernet.

Если компьютеров много и нет никакого желания выкладываться на замену сетевых адаптеров, то нужно проследить, чтобы все центральные устройства (если их не одно, а несколько) были коммутаторами, а не концентраторами (сети Fast Ethernet на базе концентраторов — не редкость). Бюджетное решение, но и прирост производительности будет налицо. Можно еще заменить магистральные коммутаторы (связывающие две подсети между собой) на коммутаторы Gigabit Ethernet. Но в этом случае производительность сети повысится, если имеет место интенсивный обмен информацией между двумя подсетями. Если же трафик в основном локализирован (то есть компьютеры обмениваются информацией, как правило, в пределах своей подсети), то особого прироста не будет.

В крупных сетях повысить производительность можно, используя технологию виртуальных локальных сетей (VLAN), которая позволяет локализировать трафик. Эту технологию мы рассмотрим в *главе 27*.

23.2. Служба QoS

Служба QoS (Quality of Service — качество обслуживания) предназначена для резервирования пропускной способности сети. Не спорю, в больших сетях QoS — довольно полезная служба, но в сетях среднего размера (не говоря уже о небольших домашних сетях) она не только бесполезна, но и вредна. Ведь по умолчанию (даже если QoS отключена, или значение резервирования не задано) QoS забирает 20% пропускной способности сети, которую вы бы могли использовать.

Изменить настройки QoS в Windows XP можно так:

1. Выполните команду **Пуск | Выполнить**.
2. Введите команду `gpedit.msc` и нажмите клавишу <Enter>.

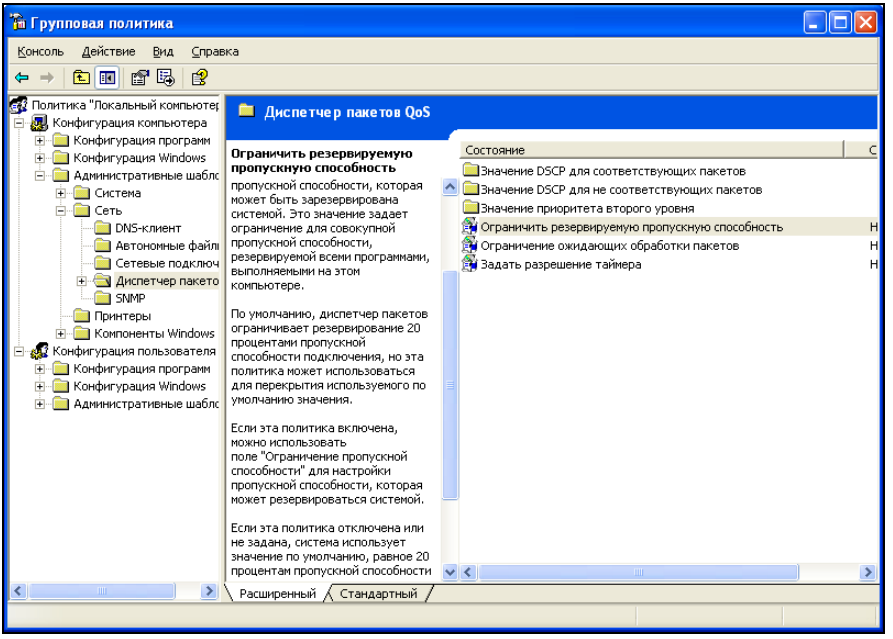


Рис. 23.1. Редактор групповых политик

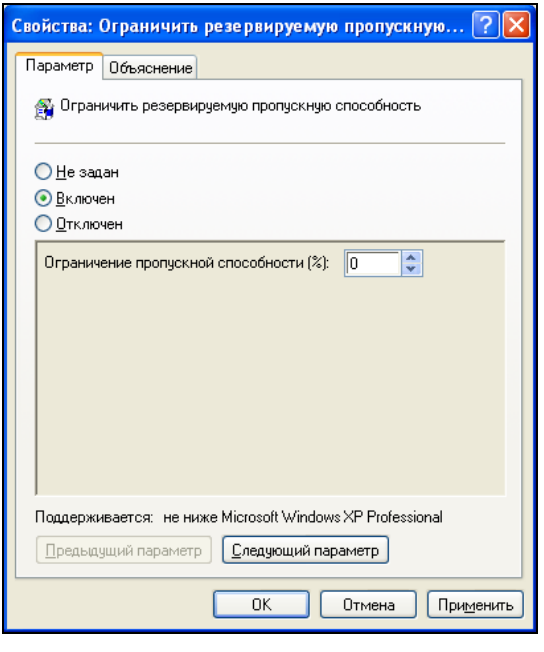


Рис. 23.2. Ограничение резервируемой пропускной способности

3. Откройте политику **Конфигурация компьютера | Административные шаблоны | Сеть** (рис. 23.1).
4. Щелкните двойным щелчком по свойству **Ограничить резервируемую пропускную способность**.
5. В открывшемся окне (рис. 23.2) выберите **Включен** и установите **0** в качестве значения параметра резервирования.

В Windows Vista Home Basic и Premium оснастки gpedit.msc, к сожалению, нет. В более "продвинутых" версиях Vista задание резервируемой пропускной способности выполняется так же, как и в Windows XP.

23.3. Оптимизация сети с помощью реестра Windows

23.3.1. Повышение производительности локальной сети

Обычно Windows самостоятельно сканирует сеть на наличие сетевых принтеров и назначенных заданий планировщика (Scheduled Tasks). Если отключить поиск сетевых принтеров и заданий планировщика, то можно повысить производительность локальной сети, а именно — скорость доступа к компьютерам в сети.

Перейдите в раздел HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\ RemoteComputer\NameSpace. В нем вы найдете два подраздела:

- {2227A280-3AEA-1069-A2DE-08002B30309D};
- {D6277990-4C6A-11CF-8D87-00AA0060F5BF}.

Удаление первого раздела отключит поиск сетевых принтеров, а второго — поиск заданий планировщика.

23.3.2. Повышение производительности Интернета

На производительность интернет-соединения непосредственное влияние оказывает размер передаваемого блока данных. Максимальный размер пакета задает параметр MTU (Maximum Transmit Unit). По умолчанию Windows использует размер MTU, равный 1 500 байт. Это значение не очень хорошо подходит для DSL-соединений, линий T1, кабельных модемов, локальной сети и совсем не подходит для обычных модемных соединений (в *разд. 7.2.3* этому факту дано весьма подробное пояснение).

Вот корректные значения MTU в зависимости от способа соединения:

- ADSL, RadioEthernet (PPPoE) — 1452;
- обычный модем — 576.

Для задания MTU перейдите в раздел HKLM\SYSTEM\CurrentControlSet\Services\ Tcpip\Parameters и создайте параметр REG_DWORD MTU. Установите требуемое значение (1452 или 576). Будьте внимательны: не забудьте переключить редактор реестра в десятичную систему счисления (рис. 23.3).

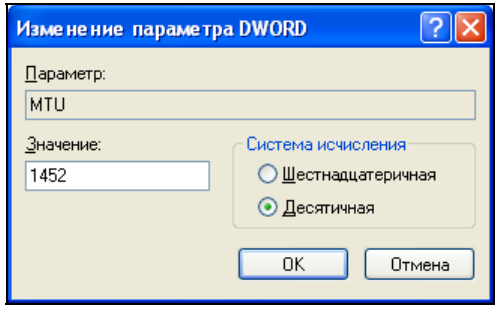


Рис. 23.3. Установка значения MTU

Если у вас не PPPoE и не обычный модем, вы можете заставить Windows автоматически вычислить значение MTU. Для этого в разделе HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters создайте параметр REG_DWORD EnablePMTUDiscovery и присвойте ему значение 1. Если соединение начнет работать медленнее, вы всегда можете удалить этот параметр.

Для высокоскоростных сетей с большой пропускной способностью можно включить поддержку TCP-окон размером больше 64 Кбайт. Для этого в разделе HKLM\SYSTEM\ CurrentControlSet\Services\Tcpip\Parameters создайте параметр REG_DWORD Tcp1323Opts и установите для него значение 1.

> ***Примечание***
>
> Чтобы указанные параметры вступили в силу, нужно перезагрузить компьютер.

23.4. Кэширующие серверы: DNS и прокси

Еще один способ повысить производительность сети — это установить собственные кэширующие серверы DNS и прокси. Разберемся, что нам это даст. Предположим, нам нужно обратиться к узлу **sales.corp.some_domain.ru**. Чтобы подключиться к этому узлу, системе нужно знать его IP-адрес. Сначала

система ищет этот адрес в локальном кэше. Если она его там не находит, то обращается к DNS-серверу. Как правило, это DNS-сервер провайдера. Но DNS-сервер тоже ничего не знает об этом компьютере. Тогда он обращается к DNS-серверу домена **ru**. Тот, в свою очередь, обращается к DNS-серверу домена **some_domain.ru**. Этот сервер должен знать все о своих поддоменах и узлах и, по идее, должен возвратить IP-адрес узла **sales** из поддомена **corp**. Иногда требуется еще одно обращение — к DNS-серверу поддомена **sales** (все зависит от того, как там устроена сеть). На такой рекурсивный запрос нужно много времени. Мы можем установить собственный кэширующий DNS-сервер и настроить все компьютеры на использование этого локального DNS-сервера. В итоге первое обращение к узлу **sales.corp.some_domain.ru** будет выполнено так: локальный кэш, кэш нашего локального сервера DNS, DNS-сервер провайдера, а дальше все, как и в предыдущем случае. Однако если какой-то другой узел нашей сети обратится к узлу **sales.corp.some_domain.ru**, то он уже получит ответ из кэша нашего локального сервера, что существенно уменьшает время обработки запроса! Мы не только повышаем производительность, но и экономим трафик по маршруту "мы — провайдер".

Кэширующий прокси-сервер, можно сказать, работает так же, но кэширует не IP-адреса узлов сети, а целые странички. Например, кто-то из нашей сети обратился к сайту **some_domain.ru**. Сначала будет выполнено обращение к этому узлу и получена его страничка. Но все последующие узлы нашей сети будут получать копию этой странички из кэша прокси-сервера. Заметьте, ответ будет приходить по локальной сети, а это скорость 100–1000 Мбит/с, а не 1–2 Мбит/с, как в случае с интернет-соединением.

Таким образом, прокси-сервер повышает производительность сети и экономит наш трафик. К тому же у него есть еще одна очень полезная функция: он позволяет блокировать узлы с "плохим" контентом: содержащие вирусы, порнографию и т. п. Также прокси можно использовать для вырезания баннеров. Видите, сколько преимуществ вы получите, потратив час на настройку прокси! В следующих главах мы настроим собственные DNS и прокси-сервер.

Глава 24

DNS-сервер

24.1. Еще раз о том, что такое DNS

Система доменных имен (DNS, Domain Name System) используется для преобразования IP-адресов в доменные имена и обратно. Компьютеру намного удобнее работать с числами, человеку же проще запомнить символьное имя узла, чем его IP-адрес.

Система DNS имеет древовидную иерархическую структуру (рис. 24.1). Список корневых серверов DNS хранится на каждом DNS-сервере (позже мы узнаем, где именно и как его обновлять). На рис. 24.1 изображен корень системы DNS, домены первого уровня (**ru**, **com**, **org**) и домен второго уровня (**firma**). Доменов первого уровня (их еще называют TLD, Top Level Domains) довольно много: **com**, **biz**, **org**, **info**, **gov**, **net**, **ws**, домены стран (**ru**, **ua**, **uk**, ...) и т. д. Понятно, что доменов второго уровня еще больше, не говоря уже о доменах третьего уровня и последующих.

Доменное имя компьютера имеет следующий формат:

```
[имя_компьютера].[домен_N]. ... [домен.TLD]
```

Например, **ftp.sales.firma.ru**

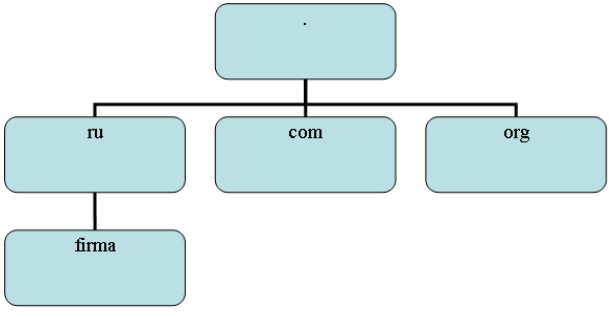


Рис. 24.1. Иерархическая структура DNS

При запросе к DNS-серверу доменное имя обрабатывается в доменном порядке. Сначала наш DNS-сервер посылает запрос к DNS-серверу домена **ru** — знает ли он что-нибудь о домене **firma**? DNS-сервер домена **ru**, если домен **firma** найден, сообщает нашему DNS-серверу IP-адрес сервера DNS домена **firma**. Потом наш DNS-сервер (наш собственный сервер имен или сервер имен провайдера) обращается к серверу имен домена **firma.ru** за адресом DNS-сервера домена **sales**. Получив IP-адрес домена **sales.firma.ru**, мы можем к нему обратиться, чтобы получить IP-адрес компьютера с именем **ftp.sales.firma.ru** (очевидно, это FTP-сервер отдела продаж какой-нибудь фирмы).

Приведенная схема разрешения доменного имени называется *рекурсивной*, а наш запрос — *рекурсивным запросом*. Конечно, саму схему я немного упростил, но общий смысл должен быть понятен. Понятно также, что такой запрос занимает довольно много времени и ресурсов, поэтому целесообразно настроить *кэширующий сервер DNS*, даже если у вас нет собственного домена. Всю "грязную" работу (то есть рекурсивные запросы) будут делать серверы DNS-провайдера, а наш сервер будет только кэшировать результаты запросов — так можно повысить скорость разрешения доменных имен и, следовательно, ускорить работу Интернета в целом. Поэтому кэширующий сервер можно установить не только на шлюзе, но и на домашнем компьютере, где он также будет с успехом выполнять свою функцию.

Настройку сервера DNS мы начнем именно с кэширующего сервера DNS. Во-первых, он настраивается проще, чем полноценный сервер DNS, зато в процессе его настройки мы познакомимся с основными конфигурационными файлами, и при настройке полноценного DNS-сервера нам будет проще. Во-вторых, не всегда есть необходимость настраивать полноценный DNS-сервер. У вас может быть локальная сеть с выходом в Интернет, но у нее не обязательно должен быть свой собственный домен.

> ***Примечание***
>
> Настройку кэширующего сервера мы будем производить только в Linux. На мой взгляд, данная операционная система больше подходит для использования в качестве интернет-сервера, чем Windows.

24.2. Кэширующий сервер DNS

Что же такое кэширующий сервер DNS? Наверняка все мы знакомы с так называемыми "ускорителями" Интернета (их также называют еще "оптимизаторами" Интернета) — программами, якобы помогающими сделать Интернет намного быстрее. Как правило, это Windows-программы, которые распро-

страняются в Интернете за определенную плату. Иногда их даже можно скачать бесплатно. В первом случае (если программа распространяется за деньги) "ускоритель" Интернета ничего вообще не делает. Он запускается, пользователь устанавливает параметры, но на самом деле никакого ускорения не происходит. Просто кто-то таким не очень честным образом зарабатывает деньги. Во втором случае (когда программа распространяется бесплатно) также не наблюдается никакого ускорения, а наоборот, фиксируется падение скорости и повышенный расход трафика. Почему? Да потому что "оптимизаторы" Интернета в большинстве случаев являются вирусами-троянами. Пользователи добровольно устанавливают программу, которая потом передаст секретную информацию (например, ключи от электронного кошелька) злоумышленнику. Помните, что бесплатный сыр — только в мышеловке.

Linux же позволяет организовать настоящий "ускоритель" Интернета. Впрочем, не нужно ожидать, что ваш Интернет будет работать на 70, а то и на все 100% быстрее, как это обещают оптимизаторы-вирусы. Ускорение будет заключаться в установке кэширующего сервера DNS. Установка DNS-сервера позволяет:

- сократить время разрешения доменных имен, поскольку в нашей сети будет свой DNS-сервер — ответы на запросы о разрешении доменных имен станут приходить от локального сервера, а не от загруженного DNS-сервера провайдера;
- немного сэкономить интернет-трафик, поскольку локальный трафик провайдером не учитывается, чего не скажешь о трафике между вами (вашей сетью) и Интернетом.

Итак, кэширующий DNS-сервер — дело нужное, поэтому не будем терять время и приступим к настройке. Установите пакет bind. Обратите внимание, что пакет называется bind (Berkley Internet Nameserver Deamon), а сам сервер — named.

После установки пакета bind нужно отредактировать файл /etc/bind/named.conf — это основной файл конфигурации named (листинг 24.1).

Листинг 24.1. Файл конфигурации /etc/bind/named.conf

```
options {
        directory "/etc/bind/ ";
};

controls {};

zone "." in {
```

```
        type hint;
        file "db.root";
};
zone "0.0.127.in-addr.arpa" in {
        type master;
        file "db.127";
};
zone "localhost" {
        type master;
        file "db.local";
};
zone "255.in-addr.arpa" {
        type master;
        file "db.255";
};

include "/etc/bind/named.conf.local";
```

Небольшие комментарии:

- основной каталог — `/etc/bind`;
- пустой блок `controls {}` нужен для того, чтобы named не обращал внимания на отсутствие ключа `rndc.key`, который нужен для программы удаленного управления сервером rndc. Правда, это не вполне корректно, поскольку для останова сервера нужно будет использовать команду `killall named`, но для нас это не существенно, поскольку мы не будем часто его останавливать;
- зона `"."` не поддерживается нашим сервером, тип `hint` (подсказка) означает, что в файле db.root находится подсказка о том, где "искать" корневые серверы DNS;
- зоны `localhost` и `0.0.127.in-addr.arpa` — это локальные зоны, описанные в файлах db.local и db.127.

В каталоге /etc/bind должны находиться файлы db*. Все эти файлы создаются при установке пакета, поэтому вам не придется создавать их вручную.

Последняя строка файла конфигурации — это директива `include`, подключающая файл /etc/bind/named.conf.local. В нем принято описывать зоны, которые будет обслуживать наш DNS-сервер. Вообще-то, собственные зоны вы можете описать в файле named.conf — особой разницы нет. Но если ваш DNS-сервер описывает много зон или одну большую зону (где много компьютеров),

тогда целесообразно вынести описание этих зон в файл named.conf.local — вам так будет удобнее настраивать DNS-сервер.

Теперь запустим named:

```
# service named start
```

Проверим, работает ли он:

```
# ps -ax | grep named
```

Команда выводит список процессов с именем named — ваш named должен быть в списке.

На всякий случай, проверим журнал — возможно, сервер запущен с какими-то предупреждениями:

```
# tail /var/log/messages
```

Aug 8 9:58:16 ppt named[3140]: starting BIND 9.2.3

Aug 8 9:58:16 ppt named[3140]: using 1 CPU

Aug 8 9:58:16 ppt named[3140]: loading configuration from '/etc/named.conf'

Aug 8 9:58:16 ppt named[3140]: listening on IPv4 interface lo, 127.0.0.1#53

Aug 8 9:58:16 ppt named[3140]: listening on IPv4 interface eth0, 192.168.0.1#53

Aug 8 9:58:16 ppt named[3140]: zone 0.0.127.in-addr.arpa/IN: loaded serial 1997022700

Aug 8 9:58:16 ppt named[3140]: running

Все работает, но мы еще не сделали самого главного. Нам ведь нужно заставить сервер провайдера собирать для нас всю необходимую информацию. Фактически работает он, а не наш сервер. Для этого в блок `options` добавьте следующие строки:

```
forward first;
       forwarders {
         # все запросы будут переадресованы к DNS-серверу
         # провайдера 192.168.99.1
         # если с этим сервером что-то случится, то локальный сервер
         # попробует найти ответ в своем кэше или обратится к другим
         # DNS-серверам, которые указываются в /etc/resolv.conf
              192.168.99.1;
       };
```

Параметр `forwarders` задает заключенный в фигурные скобки список IP-адресов, соответствующих DNS-серверам, которым наш DNS-сервер будет

переадресовывать запросы, вместо того, чтобы отвечать на них самому. IP-адреса перечисляются через точку с запятой.

Параметр `forward` может принимать одно из двух следующих значений:

- `only` — наш DNS-сервер никогда не должен предпринимать попыток обработать запрос самостоятельно;
- `first` — наш сервер должен пытаться сам обработать запрос, если указанные далее параметром `forwarders` серверы DNS не были найдены.

Использование параметра `forward` лишено смысла без использования параметра `forwarders`.

Теперь осталось в файле /etc/resolv.conf прописать IP-адрес собственного сервера DNS. То же самое нужно сделать на всех остальных компьютерах сети:

```
domain firma.ru
# IP адрес либо 127.0.0.1
nameserver 127.0.0.1
# или IP-адрес DNS-сервера — для остальных компьютеров сети
nameserver 10.0.0.1
```

Протестировать настройки можно с помощью программы nslookup:

```
# nslookup yandex.ru
```

Server: localhost.firma.ru

Address: 127.0.0.1

Non-authoritative answer:

Name: yandex.ru

Address: 213.180.216.200

Если вы получили подобный ответ, то это означает, что наш сервер работает нормально.

24.3. Полноценный DNS-сервер

Теперь можно перейти к настройке полноценного сервера DNS, если, конечно, он вам нужен. Первым делом надо настроить удаленное управление сервером, а именно: настроить секцию `controls`, которую мы оставили пустой в предыдущем примере. Выполните команду:

```
# /usr/sbin/rndc-confgen > rndc.conf
```

Откройте файл rndc.conf в любом текстовом редакторе. Нам нужно выделить и скопировать две директивы — `key` и `controls`:

```
key "rndc-key" {
      algorithm hmac-md5;
      secret "ключ";
};
controls {
# разрешаем "удаленное" управление только с локального компьютера
      inet 127.0.0.1 port 953
              allow { 127.0.0.1; } keys { "rndc-key"; };
};
```

Скопированный блок текста нужно вставить в файл named.conf (в самое начало). Понятно, что из него нужно удалить пустую директиву `controls`.

При настройке кэширующего сервера DNS мы в его конфигурационном файле описали две зоны: корневую и локальную. Теперь нам нужно описать две зоны: прямого и обратного преобразования, которые и будут обслуживать наш домен. Добавьте в файл конфигурации named.conf строки:

```
zone "firma.ru"  {
       type master;
       file "firma.ru";
       notify no;
};

zone "1.0.0.10.in-addr.arpa" {
       type master;
       file "10.0.0.1";
       notify yes;
}
```

Файл firma.ru (он должен находиться в каталоге, заданном директивой `directory`) используется для прямого преобразования, то есть для преобразования доменных имен в IP-адреса. В листинге 24.2 представлен пример этого файла.

Листинг 24.2. Пример файла прямого преобразования

```
@       IN      SOA     server.firma.ru.      hostmaster.firma.ru. (
              20040603        ; серийный номер (можно узнать в файлах с
                              примерами)
              3600             ; обновление каждый час
```

```
                3600          ; повтор каждый час
                3600000; время хранения информации 1000 часов
                3600          ; TTL записи
)
        IN NS          server.firma.ru.
        IN A           10.0.0.1
        IN MX          100    server.firma.ru.
www     IN CNAME       server.firma.ru.
ftp     IN CNAME       server.firma.ru.
mail    IN CNAME       server.firma.ru.
c2      IN A           10.0.0.2
c3      IN A           10.0.0.2
localhost.     IN A    127.0.0.1
```

Разберемся, что означают записи этого файла:

- первым делом, обратите внимание на то, что в конце каждого доменного имени ставится точка — это для того, чтобы сервер не приписывал имя домена (`firma.ru`) к доменному имени. Если лень писать имя домена, тогда можно просто указывать имя компьютера (`server` вместо `server.firma.ru`), но тогда не нужно ставить точку в конце доменного имени;
- запись `IN SOA` описывает начало полномочий (Start Of Authority, SOA). Первое имя после SOA — это имя данного компьютера (на котором запущен DNS-сервер). В нашем случае это `server.firma.ru`. Затем следует e-mail администратора сервера, но поскольку символ @ зарезервирован, то вместо него используется точка. Остальные элементы записи SOA прокомментированы в листинге;
- запись `NS` задает имя сервера доменных имен, а запись `IN A` — его IP-адрес;
- запись `MX` используется для задания почтового сервера. Как мы видим, в роли почтового сервера используется все тот же наш `server.firma.ru`. `100` — это приоритет почтового сервера. Приоритет используется, если указано два (или более почтовых сервера). Чем меньше число, тем выше приоритет:

  ```
  IN MX       100   mail1
  IN MX       150   mail2
  ```

- запись `CNAME` используется для определения канонических имен, то есть псевдонимов. Как мы видим, к нашему серверу `server.firma.com` можно обратиться по следующим именам: `www.firma.ru`, `ftp.firma.ru`, `mail.firma.ru`;

- далее описаны два компьютера — `c2.firma.ru` (мы не ставили точку после `c2`, поэтому `firma.ru` сервер допишет автоматически) и `c3.firma.ru`, с IP-адресами `10.0.0.2` и `10.0.0.3` соответственно;
- последняя запись — это определение имени `localhost`, желательно не забыть о нем.

Теперь пора приступить к рассмотрению файла обратного соответствия, который представлен в листинге 24.3. Напомню, что этот файл используется для преобразования IP-адресов в доменные имена.

Листинг 24.3. Пример файла обратного преобразования

```
@       IN      SOA     server.firma.ru.      hostmaster.firma.ru. (
                20040603        ; серийный номер (можно узнать в файлах с
                                примерами)
                3600            ; обновление каждый час
                3600            ; повтор каждый час
                3600000; время хранения информации 1000 часов
                3600            ; TTL записи
)
@       IN      NS      server.firma.ru
1       IN      PTR     server.firmaru
2       IN      PTR     c2.firma.ru
3       IN      PTR     c3.firma.ru
```

В этом файле, если вы успели заметить, можно полностью не указывать IP-адрес, но нужно полностью указывать доменное имя (точки в конце доменного имени не нужны). Если же вам хочется указать IP-адрес полностью, тогда следует указывать его в обратном порядке, например:

```
2.0.0.10        IN      PTR     c2.firma.ru
```

Вот, практически, и все. Можно в целях защиты сервера добавить в блок `options` (конфигурационный файл named.conf) директиву `allow-query`:

```
allow-query {
10.0.0.0/24;
localhost;
}
```

Полный файл конфигурации полноценного DNS-сервера для домена **firma.ru** представлен в листинге 24.4.

Листинг 24.4. Полная версия файла конфигурации named.conf

```
key "rndc-key" {
      algorithm hmac-md5;
      secret "ключ";
};
controls {
      inet 127.0.0.1 port 953
              allow { 127.0.0.1; } keys { "rndc-key"; };
};

options {
              directory "/etc/bind";

allow-query {
10.0.0.0/24;
localhost;
}

};

zone "." in {
        type hint;
        file "db.root";
};
zone "0.0.127.in-addr.arpa" in {
        type master;
        file "db.127";
};
zone "localhost" {
        type master;
        file "db.local";
};
zone "255.in-addr.arpa" {
        type master;
        file "db.255";
};

zone "firma.ru"  {
```

```
        type master;
        file "firma.ru";
        notify no;
};

zone "1.0.0.10.in-addr.arpa" {
        type master;
        file "10.0.0.1";
        notify yes;
}
```

После настройки сервер нужно перезапустить:

```
# service named restart
```

24.4. Вторичный DNS-сервер

В идеале для поддержки домена должно быть выделено два сервера — первичный и вторичный. Вторичный используется для подстраховки, если вдруг с первичным что-то случится (например, банальная перезагрузка администратором).

Вторичный сервер DNS описывается аналогично первичному, но несколько иначе описывается зона домена:

```
zone "firma.ru"  {
        type slave;
        file "firma.ru";
        masters { 10.0.0.1; };
};
```

Как видим, устанавливается тип сервера — подчиненный (`slave`), а в блоке `masters` описываются первичные серверы (у нас он один).

В файл конфигурации первичного сервера нужно добавить директиву `allow-transfer`, в которой следует указать DNS-серверы, которым разрешен трансфер зоны, то есть все вторичные серверы:

```
options {
...
allow-transfer { 10.0.0.2; };
}
```

Глава 25

Прокси-сервер Squid

25.1. Зачем нужен прокси-сервер в локальной сети?

С помощью прокси-сервера Squid можно очень эффективно управлять ресурсами своей сети — например, кэшировать трафик (HTTP), "обрезать" баннеры, указывать, какие файлы можно скачивать пользователям, а какие — нет, задавать максимальный объем передаваемого объекта и даже ограничивать пропускную способность пользователей определенного класса.

Основная функция прокси-сервера — это кэширование трафика. Если в сети используется прокси-сервер, можно сократить кэш браузеров клиентов практически до нуля — он уже не будет нужен, поскольку кэширование станет выполнять прокси-сервер. Тем более, что он выполняет кэширование всех клиентов сети, и уже запрошенные ранее страницы оказываются доступными другим пользователям. Это означает, что если кто-то зашел на сайт **firma.ru**, то у всех остальных пользователей сети этот сайт будет открываться практически мгновенно, потому что его уже кэшировали.

Даже если у вас всего один компьютер, все равно имеет смысл использовать Squid, хотя бы для того, чтобы "обрезать" баннеры — так можно сэкономить на трафике, да и страницы начнут открываться быстрее — загружать многочисленные баннеры не придется.

Squid не сложен в настройке — во всяком случае, не сложнее Samba и подобных сетевых сервисов. Установите пакет squid. После установки пакета у вас в системе появится новый сервис — squid. Его основной конфигурационный файл — /etc/squid/squid.conf.

25.2. Базовая настройка Squid

Приступим к редактированию основного конфигурационного файла /etc/squid/squid.conf (листинг 25.1).

Листинг 25.1. Файл /etc/squid/squid.conf

```
# Порт для прослушивания запросов клиентов.
# Задается в формате http_port <порт> или http_port <узел>:<порт>.
# Последний случай подходит, если SQUID запущен на машине с #несколькими
сетевыми интерфейсами
http_port 192.168.0.1:3128

# Адрес прокси провайдера, нужно согласовать с провайдером
# cach_peer proxy.your_isp.com

# Объем оперативной памяти в байтах, который будет использоваться
# прокси-сервером (85 Мбайт).
#Не устанавливайте более трети физического объема ОЗУ,
# если данная машина должна использоваться еще для чего-либо.
# Можно задать в мегабайтах, но тогда между числом и MB обязательно
# должен быть пробел: cache_mem 85 MB
cache_mem 87040

# Здесь будет размещен кэш.
# Первое число — это размер кэша в мегабайтах. Не устанавливайте
# кэш на весь раздел. Если нужно, чтобы он занимал весь раздел,
# отнимите от размера раздела 20% и укажите это значение.
# Например, если раздел 1024 Мбайт, то для кэша — только 820 Мбайт.
# Второе — количество каталогов первого уровня.
# Третье — количество каталогов второго уровня.
cache_dir /usr/local/squid 1024 16 256

# Максимальный размер кэшируемого объекта.
# Если размер объекта превышает указанный здесь, то объект не будет
# сохранен на диске.
# maximum_object_size 4096 KB

# Хосты, с которых разрешен доступ к прокси
acl allowed_hosts src 192.168.1.0/255.255.255.0
acl localhost src127.0.0.1/255.255.255.255
```

```
# разрешенные порты:
acl allow_ports port 80    # http
acl allow_ports port 21    # ftp
# SSL-порты
acl SSL_ports port 443 563

# Запрещаем все порты, кроме указанных в allow_ports
http_access deny !allow_ports

# Запрещаем метод CONNECT для всех портов, кроме указанных в
# acl SSL_ports:
http_access deny CONNECT !SSL_ports

# Запретим доступ всем, кроме тех, кому можно
http_access allow localhost
http_access allow allowed_hosts
http_access allow SSL_ports
http_access deny all

# Пропишем пользователей, которым разрешено пользоваться squid
# (ppt, admin):
ident_lookup on
acl allowed_users ppt admin
http_access allow allowed_users
http_access deny all
```

Базовый конфигурационный файл с успехом выполняет только функцию кэширования, а в следующем разделе мы поговорим о более тонкой настройке Squid.

25.3. Практические примеры настройки

25.3.1. Управление доступом

Управление доступом осуществляется с помощью *списков управления доступом* — ACL (Access Control List).

Разберемся, как работать с ACL. Создадим список AllowedPorts:

```
acl AllowedPorts port 80 8080 3128
```

Имя списка — `AllowedPorts`, тип списка — `port`. Далее мы можем использовать этот список в `http_access` для разрешения/запрещения указанных портов:

```
http_access allow AllowedPorts     # разрешение портов
http_access deny AllowedPorts      # запрещение портов
```

Кроме типа `port` часто используются следующие типы списков:

- `proto` — протокол (HTTP или FTP);
- `method` — метод передачи данных (GET или POST);
- `src` — IP-адреса (или диапазоны адресов) клиентов;
- `dst` — IP-адреса/URL сайтов, к которым обращаются клиенты.

Вы также можете создать список узлов, которым разрешен доступ к прокси:

```
acl allowed_hosts src "/etc/squid/allowed-hosts.txt"
```

Сам файл /etc/squid/allowed-hosts.txt будет выглядеть так:

```
# den
192.168.0.2/255.255.255.255
# admin
192.168.0.3/255.255.255.255
```

Отдельный файл использовать удобнее — чтобы не "засорять" основной конфигурационный файл. Обратите внимание: права доступа к файлу allowed-hosts.txt должны быть такие же, как и к файлу squid.conf.

25.3.2. Создание "черного" списка URL

Теперь попробуем создать "черный" список URL:

```
acl blacklist url_regex adult
http_access deny blaklist
http_access allow all
```

Этот список не пропускает URL, содержащие слово `adult`. По аналогии можно было бы создать отдельный файл и записать в него все "плохие" URL (но это довольно накладно, проще использовать регулярные выражения).

25.3.3. Отказ от баннеров

С помощью ACL можно отказаться и от баннеров — принцип тот же. Для этого добавьте в файл конфигурации следующие ACL:

```
acl banners urlpath_regex "/etc/squid/banners.txt"
http_access deny banners
```

В файл banners.txt нужно внести URL баннерных сетей, например,

```
^http://www.clickhere.ru
^http://banner.kiev.ua
...
```

Создание этого файла пусть будет вашим домашним заданием — все равно все баннерные сети в книге не приведешь.

25.4. Управление прокси-сервером

Для запуска, перезапуска и остановки прокси-сервера нужно использовать следующие команды:

```
# service squid start
# service squid restart
# service squid stop
```

25.5. Настройка клиентов

Все браузеры на компьютерах вашей сети нужно настроить на использование порта 3128 (именно этот порт мы установили в конфигурационном файле). На рис. 25.1 изображена настройка браузера Opera.

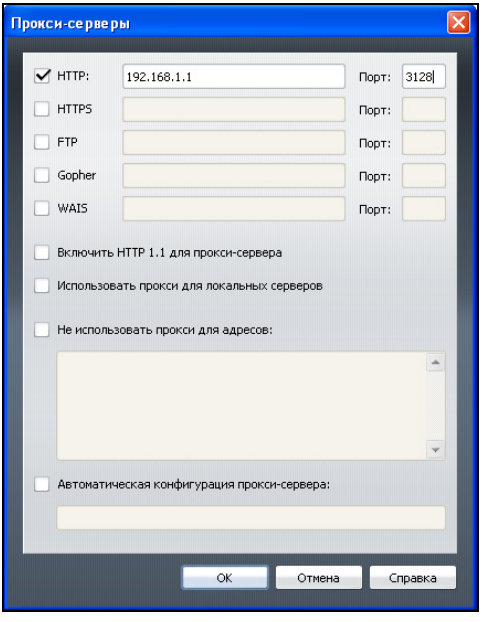


Рис. 25.1. Настройка клиента

25.6. Прозрачный прокси-сервер

С прокси-сервером часто связаны две проблемы. Первая заключается в том, что для работы через прокси-сервер нужно настраивать всех клиентов. Если сеть большая, скажем, 100 компьютеров, можете себе представить, сколько это займет времени — ведь нужно будет подойти к каждому из них. Даже если на настройку одного компьютера потребуется 5 минут, то на все уйдет 500 минут — целый рабочий день. Но настройкой одного браузера может дело и не обойтись — ведь у пользователей могут быть и другие интернет-программы, работающие с WWW/FTP, которые также надо будет настраивать.

Проблема настройки — не самая страшная. Понятно, что если в сети организации 100 или более компьютеров, то и администратор будет не один. А вдвоем-втроем можно настроить все 100 компьютеров за 2–3 часа.

Вторая проблема — более серьезная. Представим, что в сети у нас есть "продвинутые" пользователи (а они таки есть), которые знают, для чего используется прокси-сервер. Они могут запросто изменить настройки, и вместо работы через прокси использовать прямое соединение с Интернетом, т. е. будут работать в обход Squid. Вы так старались, создавая список "черных" URL (преимущественно это сайты для взрослых и всевозможные чаты/форумы), а они с помощью пары щелчков мышью сведут все ваши старания к нулю.

Обе проблемы можно решить, если настроить *прозрачный прокси-сервер*: пользователи даже не будут подозревать, что он есть. Во-первых, это решит проблемы с настройкой — вам не нужно настраивать браузеры пользователей, потому что все HTTP-запросы будут автоматически поступать на этот прокси-сервер. Во-вторых, прозрачный прокси обеспечит принудительное кэширование информации и, соответственно, принудительный контроль за страницами, которые посещают пользователи.

Для настройки прозрачного прокси вам нужно изменить как конфигурационный файл самого прокси-сервера, так и правила брандмауэра iptables:

```
iptables -t nat --new-chain TransProxy
# только порт 80 (HTTP) и 443 (SSL, https) — остальные обрабатывать не # будем
iptables -t nat -A PREROUTING -p tcp --dport 80 -j TransProxy
iptables -t nat -A PREROUTING -p tcp --dport 443 -j TransProxy
iptables -t nat -A TransProxy -d 127.0.0.1/8 -j ACCEPT
# укажите IP-адрес своей сети
iptables -t nat -A TransProxy -d 192.168.1.0/24 -j ACCEPT
# все запросы перенаправляются на прокси-сервер 192.168.1.1, порт 3128
iptables -t nat -A TransProxy -p TCP -j DNAT --to 192.168.1.1:3128
```

Теперь займемся настройкой Squid. В конфигурационный файл squid.conf добавьте следующие директивы:

```
# серверу назначается реальный IP-адрес, его и нужно указать
tcp_outgoing_address ваш_реальный_IP
httpd_accel_host virtual
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

Забегая вперед, скажу, что iptables обычно устанавливается на шлюзе — компьютере, который предоставляет доступ к Интернету других компьютеров сети. На этом же компьютере должен быть установлен и Squid.

25.7. Расширение squidGuard

Чуть ранее были приведены примеры создания "черных" списков, ограничивающих доступ к сайтам с запрещенным контентом. Но пока вы сформируете базу "черных" списков, пройдет время. Для автоматизации этого процесса вы можете применить расширение squidGuard, использующее уже готовые "черные" списки, сформированные большим сообществом пользователей и тщательно проверенные разработчиками squidGuard. Расширение squidGuard не только сэкономит трафик, но и эффективно защитит вашу сеть от запрещенного контента.

"Черный" список squidGuard обновляется постоянно. Скачать его можно с сайта **http://www.squidguard.org/**. Там же вы найдете альтернативные "черные" списки. В базу squidGuard внесены самые известные сайты с запрещенным контентом, а именно: насилие, порнография, наркотики, азартные игры и т. д.

Для установки squidGuard достаточно установить одноименный пакет. После установки "черный" список узлов будет помещен в каталог /usr/share/squidGuard-1-3-0/db (версия squidGuard у вас может быть иная). В некоторых дистрибутивах (или если вы устанавливаете squidGuard из исходных кодов) база будет помещена в каталог /usr/local/squidGuard/db.

Чтобы база данных была самой актуальной, скачайте последнюю ее версию по адресу: **http://www.squidguard.org/blacklists.html**. Вы скачаете файл blacklist.tar.gz. Распакуйте его в каталог /usr/share/squidGuard-1-3-0/db или в /usr/local/squidGuard/db:

```
cp blacklist.tar.gz /usr/local/squidGuard/db
gzip -d blacklist.tar.gz
tar xfv blacklist.tar
```

После этого нужно немного подредактировать файл конфигурации squidGuard. Скопируйте файл /etc/squid/squidGuard.conf.sample в файл /etc/squid/squidGuard.conf и откройте его в текстовом редакторе. Весь файл редактировать не нужно, полный листинг этого файла тоже приводить не стану — он слишком длинный.

Первым делом нужно указать путь к базе и к журналам:

```
dbhome /usr/local/squidGuard/db
logdir /var/log/squidGuard
```

Теперь опишем разрешенное время работы:

```
# s = Вс, m = Пн, t =Вт, w = Ср, h = Чт, f = Пт, a = Сб

time workhours {
        weekly m 08:00-12:00 13:00-19:00
        weekly t 08:00-11:00 12:00-19:00
        weekly w 08:00-12:00 12:00-18:00
        weekly h 08:00-13:00 13:00-18:00
        weekly f 08:00-12:00 13:30-18:00
        weekly a 11:20-14:00
        weekly s 11:32-14:00
}
```

Опишем две зоны. К первой будут относиться наши пользователи, а ко второй — администраторы сети. Пользователи, не относящиеся к первым двум группам, вообще не будут иметь доступа к Интернету.

```
src users {
ip 192.168.1.5-192.168.1.200
}

src admins {
ip 192.168.1.1-192.168.1.4
}
```

Опишем также списки доступа, определяющие, кому и к каким узлам разрешен доступ. Администраторам разрешаем доступ ко всем узлам, кроме рекламных баннеров, а вот пользователям запрещаем доступ по максимуму.

```
acl {
  admins {

    pass !advertising all
```

```
# запрещенные запросы перенаправляем на следующий адрес
    redirect http://server.ru/error.html
  }

  users {
    pass !adult !audio-video !forums !hacking !redirector !warez !ads
!aggressive
         !drugs !gambling !publicite !violence !banneddestination !adver-
tising all

    redirect http://server.ru/error.html
  }

# остальным пользователям доступ к Интернету запрещен (pass none)
  default {
    pass none
    redirect http://server.ru/error.html
  }
}
```

Почти все. Осталось только "прописать" расширение squidGuard в конфигурационном файле Squid. Откройте файл /etc/squid/squid.conf и добавьте в него следующие строки:

```
redirector_bypass on
redirect_program /usr/local/squidGuard/bin/squidGuard
redirect_children 1
```

Сохраните файл и перезапустите Squid:

```
# service squid restart
```

Теперь выполните следующую команду:

```
tac /var/log/squidGuard/squidGuard.log | less
```

Вы должны увидеть сообщение о том, что squidGuard запущен (**started**) и готов к обработке запросов (**ready for requests**). Если вы увидели эти заветные строки, значит, все сделано правильно.

Глава 26

DHCP-сервер для вашей сети

26.1. Протокол динамической конфигурации узла

Протокол *динамической конфигурации узла* (DHCP, Dynamic Host Configuration Protocol) используется для автоматической настройки узлов сети. С помощью DHCP компьютер, подключенный к сети, в которой есть DHCP-сервер, может получить IP-адрес, маску подсети, IP-адрес шлюза, адреса серверов DNS и другие сетевые параметры.

Особенно удобно использовать DHCP в средних и больших сетях. Вы только представьте, что у вас есть, скажем, 20 компьютеров. Если каждому компьютеру назначать IP-адрес статически, то вам придется к каждому компьютеру подойти и прописать в его настройках этот IP-адрес. Заодно вам нужно будет ввести IP-адрес сети, IP-адрес шлюза и адреса серверов DNS. Понятно, что эту процедуру надо выполнить однократно — при настройке сети. Но если через некоторое время конфигурация сети изменится (например, вы поменяете провайдера), и понадобится изменить IP-адреса DNS-серверов, то вам придется все повторить заново: подойти к каждому компьютеру и прописать DNS-серверы.

Функции DHCP-сервера часто включаются в состав встроенного программного обеспечения точки доступа и маршрутизатора. Но иногда полезно настроить собственный сервер. Например, когда приходится обслуживать сразу несколько подсетей или когда программное обеспечение маршрутизатора не позволяет задать определенные опции.

Если же потратить полчаса на настройку DHCP-сервера, то управлять конфигурацией сети можно будет централизованно. Стоит вам изменить IP-адрес DNS-сервера в конфигурационном файле DHCP-сервера — на остальных компьютерах сети новые IP-адреса DNS-серверов "пропишутся" автоматически. Удобно? Я тоже так думаю.

Настройку DHCP-сервера будем рассматривать в ОС Linux. Для установки DHCP-сервера вам достаточно установить пакет dhcp. DHCP-клиенты входят в состав Linux и Windows, поэтому их устанавливать отдельно не нужно.

26.2. Конфигурационный файл DHCP-сервера

Конфигурационный файл DHCP-сервера называется /etc/dhcpd.conf. Пример этого файла вы можете найти в каталоге /usr/share/doc/dhcp-<версия>/dhcpd.conf.sample.

Сделаем по поводу этого конфигурационного файла два замечания:

- директивы файла не чувствительны к регистру символов — вы можете написать как `option`, так и `OPTION`, но принято писать строчными буквами;
- комментарии начинаются с символа решетки `#`.

В начало файла конфигурации нужно поместить одну из директив:

```
ddns-update-style ad-hoc;
```

или

```
ddns-update-style interim;
```

Разберемся, что они означают. Сейчас существуют две схемы обновления DNS: непосредственное обновление (ah-doc) и предварительное взаимодействие DHCP-DNS (interim). Вторая схема пока не утверждена комитетом по техническому развитию Интернета, но уже успешно реализуется, и разработчики DHCP рекомендуют использовать именно ее. Тут выбирать вам: или использовать старую схему взаимодействия (первая директива), или выбрать более перспективную (вторая директива).

По сути, весь конфигурационный файл DHCP-сервера будет состоять из директивы `ddns-update-style` и блочной директивы `section`, описывающей вашу сеть.

Рассмотрим пример объявления сети 192.168.1.0 (листинг 26.1).

Листинг 26.1. Описание сети 192.168.1.0

```
subnet 192.168.1.0 netmask 255.255.255.0 {
# шлюз по умолчанию
        option routers                  192.168.1.1;
# маска сети — этот параметр будет передан всем компьютерам сети
        option subnet-mask              255.255.255.0;
```

```
# наш домен
        option domain-name              "example.ru";
# IP-адрес сервера DNS
        option domain-name-servers       192.168.1.1;

# диапазон IP-адресов: компьютерам нашей сети будут присваиваться
# IP-адреса из этого диапазона
range 192.168.1.10 192.168.1.100;
}
```

Если сеть большая и в ней есть несколько подсетей, то все подсети (директива `subnet`) должны быть описаны в одной директиве `shared-network`. При этом все общие для подсетей параметры: описание маршрутизаторов, DNS-серверов, доменное имя — выносятся за пределы директив `subnet` (листинг 26.2).

Листинг 26.2. Большая сеть и ее подсети

```
shared-network имя_нашей_сети {
# описываем глобальные для всех подсетей параметры

# домен
    option domain-name                      "example.ru";
# серверы DNS
    option domain-name-servers              ns1.isp.com, ns2.isp.com;
# шлюз по умолчанию
    option routers                  192.168.0.1;

# описываем подсети 192.168.1.0 и 192.168.2.0

    subnet 192.168.1.0 netmask 255.255.252.0 {
        range 192.168.1.10 192.168.1.254;
    }
    subnet 192.168.2.0 netmask 255.255.252.0 {
        range 192.168.2.10 192.168.2.254;
    }
}
# конец директивы shared-network
```

26.3. База данных аренды

DHCP-сервер назначает IP-адрес компьютеру не на все время, а только на некоторое, называемое *временем аренды*. По истечении данного времени компьютеру будет назначен другой IP-адрес.

Время аренды регулируется директивами `default-leased-time` и `max-leased-time`, но изменять значения этих директив не имеет смысла, поскольку значения по умолчанию вполне приемлемы.

База данных аренды, то есть информация, кому и какой IP-адрес был назначен, находится в файле /var/lib/dhcp/dhcpd.leases. В этом файле содержится следующая информация: уникальный MAC-адрес сетевого адаптера компьютера (аппаратный адрес), назначенный IP-адрес, дата и время окончания аренды и др.

Базу данных аренды нельзя редактировать вручную, ее можно только просматривать.

26.4. Полный листинг конфигурационного файла

Окончательный вариант конфигурационного файла для подсети 192.168.1.0 представлен в листинге 26.3.

Листинг 26.3. Окончательный вариант конфигурационного файла DHCP-сервера

```
# схема взаимодействия с DNS
ddns-update-style ad-hoc;

subnet 192.168.1.0 netmask 255.255.255.0 {

# шлюз по умолчанию
        option routers                  192.168.1.1;
# маска сети — этот параметр будет передан всем компьютерам сети
        option subnet-mask              255.255.255.0;
# наш домен
        option domain-name              "example.ru";
# IP-адрес сервера DNS
```

```
        option domain-name-servers       192.168.1.1;

# диапазон IP-адресов: компьютерам нашей сети будут присваиваться
# IP-адреса из этого диапазона
range 192.168.1.10 192.168.1.100;
}
```

26.5. Управление сервером DHCP

Для запуска, перезапуска и останова сервера можно использовать команду `service`:

```
service dhcpd start
service dhcpd restart
service dhcpd stop
```

26.6. Настройка клиентов

Все клиенты вашей сети (разумеется, кроме серверов сети, у которых должны быть постоянные IP-адреса) должны быть настроены на автоматическое получение IP-адреса и IP-адресов DNS-серверов.

Глава 27

Виртуальная локальная сеть

27.1. Виртуальность

В Интернете я нашел довольно интересное толкование слова "виртуальный": такой, который может или должен проявиться, возникнуть и т. п. при определенных условиях, возможный. То есть виртуальный объект как бы есть, но в то же время его и нет. Взять бы тот же виртуальный компьютер (развернутый в эмуляторе типа VMware) — он вроде бы и есть, даже ОС можно на нем запустить, но физически его не существует. То же самое происходит с виртуальной локальной сетью.

Виртуальная локальная сеть (VLAN, Virtual Local Area Network) — группа устройств, взаимодействующая напрямую на канальном уровне, при этом на физическом уровне все эти устройства подключены к разным коммутаторам. Устройства, находящиеся в разных виртуальных сетях, невидимы друг для друга на канальном уровне, даже если они подключены к одному и тому же коммутатору, а взаимодействие между устройствами осуществляется только на сетевом или других, более высоких, уровнях.

Виртуальные локальные сети используются для создания логической топологии сети, которая никак не зависит от ее физической топологии.

27.2. Зачем нужны виртуальные сети?

Все виртуальное, оказывается, находит в реальном мире вполне конкретное применение. Виртуальная локальная сеть — это не какой-нибудь эмулятор или игрушка для админа, а вполне реальный инструмент построения современной сети.

- Во-первых, VLAN позволяет гибко компоновать устройства по группам. Например, можно с легкостью объединить устройства, находящиеся

в разных местах, в одну сеть или же разделить устройства одной сети на разные виртуальные подсети.

- Во-вторых, виртуальная локальная сеть может уменьшить количество широковещательного трафика в сети. С помощью VLAN можно разбить коммутатор на несколько широковещательных доменов и отправить широковещательное сообщение только одной группе устройств (одной виртуальной сети).
- В-третьих, VLAN позволяет повысить безопасность и управляемость сети. VLAN активно используются для борьбы с ARP-спуфингом[1] и существенно упрощают применение политик и правил безопасности. С помощью виртуальных сетей можно применять правила к целым подсетям, а не к каждому устройству.

27.3. Метим трафик

Когда компьютер передает данные, он ничего не подозревает ни о своей принадлежности к какой-либо виртуальной сети, ни о существовании VLAN. Он просто передает информацию. А вот всем остальным занимается коммутатор, который "знает", что компьютер, подключенный к тому или иному порту, принадлежит той или иной виртуальной сети.

Что делать, если на порт приходит трафик разных VLAN? Как его различить? Для этого используется *маркировка кадров*. Маркировка позволяет идентифицировать трафик, то есть установить, к какой виртуальной сети он принадлежит.

Существуют различные варианты маркировки кадров. Иногда производители оборудования, в частности, Cisco, разрабатывают собственные протоколы маркировки кадров. Но чаще используется стандарт IEEE 802.1Q. В этом случае во внутрь кадра помещается специальная метка — тег, которая передает информацию о принадлежности трафика к определенной VLAN.

Размер этой метки всего 4 байта, она состоит из следующих полей:

- TPID (Tag Protocol Identifier) — идентификатор протокола маркировки. Идентифицирует протокол, использующийся для маркировки кадра. Идентификатор протокола 802.1Q — 0x8100. Размер этого поля равен 16 битам;
- Priority — задает приоритет передаваемого трафика. Используется стандартом IEEE 802.1p. Размер — 3 бита;

[1] ARP-спуфинг — один из методов взлома сетей.

- CFI (Canonical Format Indicator) — индикатор канонического формата. Проще говоря, задает формат MAC-адреса: 1 — канонический, 0 — не канонический. Размер поля — всего 1 бит;
- VID (VLAN Identifier) — задает индикатор виртуальной сети. Указывает, к какой виртуальной сети принадлежит кадр. Размер — 12 битов.

Маркер вставляется перед полем `Тип протокола` — понятное дело, после этого пересчитывается контрольная сумма, поскольку кадр уже изменился (рис. 27.1).

Рис. 27.1. Исходный и измененный кадр

27.4. Порты и VLAN

Обратимся к портам коммутатора и виртуальным сетям. Порты коммутатора, которые поддерживают виртуальную сеть, можно разделить на две группы: маркированные порты (в терминологии Cisco — это транковые порты, англ. trunk ports) и немаркированные порты (порты доступа, access ports).

- *Маркированные порты* нужны, чтобы через один порт можно было передавать и получать трафик от нескольких виртуальных сетей. При этом виртуальных сетей может быть несколько, а порт — всего один. Как уже было указано ранее, информация о принадлежности трафика той или иной виртуальной сети указывается в специальном поле кадра. Без этого поля коммутатор не сможет различить трафик от разных сетей.
- *Немаркированные порты* (порты доступа) используются для передачи немаркированного трафика. Порт доступа может быть только в одной виртуальной сети. Порт может быть маркированным в нескольких VLAN и одновременно являться портом доступа в какой-то другой одной виртуальной сети. Если порт является портом доступа для какой-то виртуальной сети, то эта сеть называется *родной* для этого порта (native VLAN).

Когда на порт доступа приходит маркированный трафик, то он обычно должен удаляться, но это происходит не всегда — все зависит от настроек ком-

мутатора. По умолчанию все порты коммутатора считаются портами доступа для сети VLAN 1. В процессе настройки администратор может изменить тип порта на маркированный и определить принадлежность портов к разным VLAN.

Порты коммутатора могут привязываться к определенной виртуальной сети статически или динамически. В первом случае администратор вручную определяет, какой порт будет принадлежать к какой VLAN. При динамическом назначении узлов принадлежность порта к той или иной виртуальной сети определяется коммутатором. Процедура назначения портом описана в стандарте 802.1X. Этот стандарт предусматривает аутентификацию пользователя на RADIUS-сервере для получения доступа к порту.

27.5. Практика настройки VLAN на коммутаторах Cisco

Думаю, всем уже ясно, что VLAN — штука полезная, и хочется все настроить на практике. Чтобы не "изобретать колесо заново", будем использовать примерно такую топологию сети, какая описана в документации Cisco, но с небольшими усовершенствованиями.

Итак, у нас есть два коммутатора: switch1 и switch2. К каждому из коммутаторов подключено по две виртуальные сети. Для подключения к коммутаторам компьютеры виртуальной локальной сети используют порты доступа (fa0/N), а для связи между коммутаторами служит транковый (маркированный) порт (рис. 27.2).

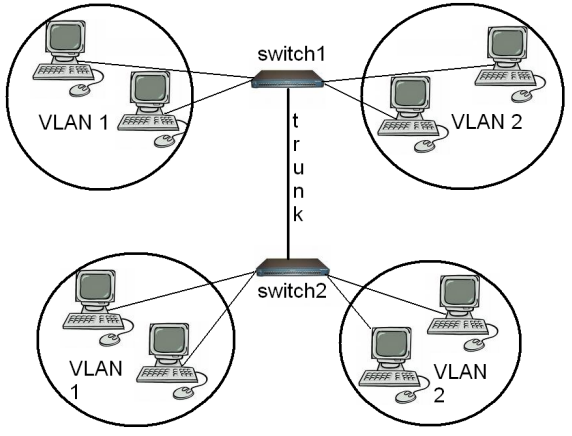


Рис. 27.2. Топология сети

Ранние версии коммутаторов Cisco поддерживали прориетарный протокол ISL (Inter Switch Link), сейчас этот протокол упразднен и вместо него используется 802.1Q.

Итак, приступим к настройке коммутатора. Как уже было отмечено, по умолчанию все порты коммутатора принадлежат к VLAN 1. Чтобы создать вторую виртуальную сеть (VLAN 2) и присвоить ей имя, используются следующие команды Cisco:

```
switch1(config)# vlan 2
switch1(config-vlan)# name myvlan
```

Далее нужно назначить порты к той или иной сети. Назначим порты fa0/3 и fa0/4 к виртуальной сети VLAN 2:

```
switch1(config)# interface fa0/3
switch1(config-if)# switchport mode access
switch1(config-if)# switchport access vlan 2

switch1(config)# interface fa0/4
switch1(config-if)# switchport mode access
switch1(config-if)# switchport access vlan 2
```

Первая команда выбирает интерфейс, вторая задает режим порта: `access`. Третья назначает порт виртуальной сети VLAN 2.

Понятно, что если портов много, то по одному "прописывать" их неудобно. Гораздо проще указать диапазон портов. Например, следующие команды добавляют порты с fa0/5 по fa0/9 в VLAN 2:

```
switch1(config)# interface range fa0/5 - 9
switch1(config-if-range)# switchport mode access
switch1(config-if-range)# switchport access vlan 2
```

Просмотреть информацию о назначенных портах и созданных виртуальных сетях можно с помощью команды:

```
# show vlan brief
```

Вывод команды будет выглядеть так:

```
VLAN  Name                Status    Ports
----- ----------------- --------- -------------------------------
1    default              active  Fa0/1, Fa0/2, Fa0/10, Fa0/11,
                                  Fa0/12, Fa0/13, Fa0/14, Fa0/15,
                                  Fa0/16, Fa0/17, Fa0/18, Fa0/19,
                                  Fa0/20, Fa0/21, Fa0/22, Fa0/23,
```

```
                                    Fa0/24
2    mylan                  active  Fa0/3, Fa0/4, Fa0/5, Fa0/6,
                                    Fa0/7, Fa0/8, Fa0/9
```

Теперь настало время создать транковый порт. Делается это командами:

```
switch1(config)# interface fa0/24
switch1(config-if)# switchport encapsulation dot1q
switch1(config-if)# switchport mode trunk
```

Можно задать "родной" режим — при этом трафик сети VLAN 2, передаваемый через транковый порт, будет немаркированным, а весь немаркированный трафик, попавший на транковый интерфейс, будет промаркирован, как принадлежащий VLAN 2 (по умолчанию он воспринимается как трафик VLAN 1):

```
switch1(config-if)# switchport trunk native vlan 2
```

Просмотреть информацию о транковом порте можно с помощью одной из двух команд:

```
switch1# show interface fa0/24 trunk
switch1# show interface fa0/24 switchport
```

Вот конфигурация для нашего первого коммутатора switch 1:

```
!
interface fa0/3
switchport mode access
switch1(config-if)# switchport access vlan 2

!
switch1(config)# interface fa0/4
switch1(config-if)# switchport mode access
switch1(config-if)# switchport access vlan 2

!
switch1(config)# interface fa0/24
switch1(config-if)# switchport encapsulation dot1q
switch1(config-if)# switchport mode trunk
```

Настройки для коммутатора switch2 выполняются аналогичным образом.

Теперь представим, что в нашей сети появился маршрутизатор, он же роутер. Топология сети будет немного изменена (рис. 27.3).

Первым делом нам нужно включить маршрутизацию на коммутаторе switch1:

```
switch1(config)#ip routing
```

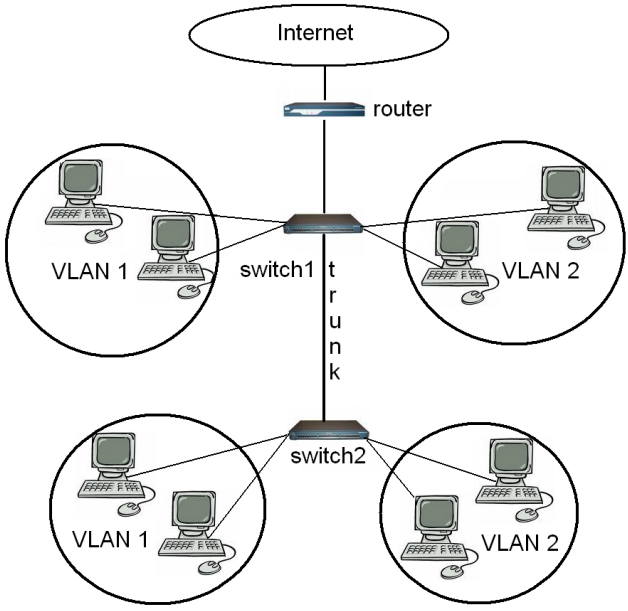


Рис. 27.3. Новая топология сети

После этого следует указать IP-адрес маршрутизатора (192.168.1.1) — этот адрес будет шлюзом по умолчанию для компьютеров первой виртуальной сети (VLAN 1, или default):

```
switch1(config)#interface default
switch1(config-if)#ip address 192.168.1.1 255.255.255.0
switch1(config-if)#no shutdown
```

Аналогично можно задать:

```
switch1(config)#interface vlan2
switch1(config-if)#ip address 192.168.1.1 255.255.255.0
switch1(config-if)#no shutdown
```

Теперь настроим интерфейс fa0/20, который соединен с маршрутизатором. Трафик, который не предназначен нашим виртуальным сетям, должен перенаправляться на маршрутизатор, а он уже сам пусть разбирается, что с ним делать. Вот необходимые команды конфигурации:

```
switch1(config)#interface fa0/20
switch1(config-if)#no switchport
switch1(config-if)#ip address 192.168.1.1 255.255.255.0
switch1(config-if)#no shutdown
```

Осталось еще прописать сам маршрут

```
switch1(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Рассмотрим окончательную конфигурацию коммутатора switch1:

```
!
ip routing
!
interface fa0/3
switchport mode access
switchport access vlan 2
!
interface fa0/4
switchport mode access
switchport access vlan 2
!
interface fa0/24
switchport encapsulation dot1q
switchport mode trunk
!
interface default
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface vlan2
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface fa0/20
no switchport
ip address 192.168.1.1 255.255.255.0
no shutdown
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

27.6. Другие производители оборудования

Понятно, что Cisco — далеко не единственный производитель сетевого оборудования. Учитывая, что оборудование от Cisco стоит недешево, желающие сэкономить наверняка будут искать более дешевые аналоги. Один из таких аналогов — это оборудование от D-Link. Простенькое, иногда зависает (ничего личного — говорю как есть), но зато ощутимо дешевле.

Обратите внимание, что далеко не все оборудование от D-Link поддерживает виртуальные локальные сети. Подробнее об этом можно прочитать вот на этой страничке: **http://www.dlink.ru/technology/vlan.php**.

Перечислять здесь все необходимые модели не вижу смысла — есть ссылка, да и на сайте представителя D-Link информация об оборудовании периодически обновляется.

О настройке VLAN на коммутаторах D-Link можно прочитать вот на этой страничке: **http://xgu.ru/wiki/VLAN_в_D-LINK** или в руководстве пользователя.

27.7. Настройка VLAN в Linux

А теперь поговорим о настройке виртуальных сетей в ОС Linux. Этот раздел статьи понадобится, если вы надумали построить программный маршрутизатор между двумя VLAN на базе Linux или хотите обеспечить присутствие одного и того же сервера в нескольких VLAN: такой себе Фигаро — тут и Фигаро — там.

Первым делом надо добавить модуль 802.1Q, обеспечивающий маркировку кадров:

```
# modprobe 8021q
```

Модуль не найден? Тогда следует перекомпилировать ядро, включив поддержку этого модуля. Вот заветные команды:

```
# cd /usr/src/linux
# make menuconfig
# make modules
# make modules_install
```

Модуль включается в разделе `Network options / 802.1Q VLAN Support`.

После перекомпиляции ядра перезагружаем систему и снова вводим команду:

```
# modprobe 8021q
```

Модуль должен быть загружен. Затем надо выключить сетевой интерфейс и "поднять" его, но уже без IP-адреса:

```
# /sbin/ifconfig eth0 down
# /sbin/ifconfig eth0 0.0.0.0 up
```

Теперь укажем, к какому интерфейсу подключена которая из виртуальных сетей. Для этого используется команда `vconfig` (пакет vlan или vconfig — название пакета, содержащего программу vconfig, зависит от дистрибутива). Формат вызова команды такой:

```
# /sbin/vconfig add интерфейс VLAN_ID
```

Например:

```
# /sbin/vconfig add eth0 1
# /sbin/vconfig add eth0 2
```

В данном случае мы связали VLAN 1 и VLAN 2 с одним сетевым интерфейсом — eth0. Далее нужно указать IP-адрес и сетевую маску для каждого интерфейса:

```
# /sbin/ifconfig eth0.1 192.168.1.x netmask 255.255.255.0 up
# /sbin/ifconfig eth0.2 192.168.2.x netmask 255.255.255.0 up
```

Можно задать маршрут по умолчанию (если необходимо):

```
# /sbin/route add default gw 192.168.1.x
```

Получить исчерпывающую информацию о "виртуальных" интерфейсах можно через псевдофайловую систему /proc:

```
cat /proc/net/vlan/eth0.N
```

Например:

```
cat /proc/net/vlan/eth0.1
```

Это еще не все. VLAN мы, вроде бы, настроили, но при перезагрузке потеряем все настройки. Чтобы этого не случилось, нужно прописать модуль 802.1Q в файле /etc/modules.conf, а настройки VLAN — в файле /etc/network/interfaces, например:

```
auto myvlan
iface myvlan inet static
        address 192.168.1.1
        netmask 255.255.255.0
        vlan_raw_device eth0
```

Можно также создать сценарий и добавить его вызов в сценарии автозапуска системы — это уже как кому больше нравится.

27.8. VLAN в Windows: миф или реальность?

Windows не обладает встроенной поддержкой VLAN, однако ее можно добавить, установив специальные драйверы. Вот они:

- Intel Advanced Networking Suite (iANS);
- 3com DynamicAccess;
- Broadcom Advanced Server Program (BASP).

Все эти драйверы вы без проблем найдете в Интернете, как и документацию, в которой будет рассказано, что с ними дальше делать. Однако вряд ли вам придется настраивать VLAN в Windows, поскольку правильнее и проще

использовать или уже готовые устройства с поддержкой VLAN или же отдельный Linux-сервер. Если же вам интересно, то можете прочитать FAQ по драйверам от Broadcom, где также будут рассмотрены вопросы по BASP (Broadcom Advanced Server Program): **http://www.broadcom.com/support/ethernet_nic/faq_drivers.php**.

27.9. Где применяется VLAN?

Хорошо, настраивать VLAN мы научились. Но где они реально применяются? В последнее время виртуальные локальные сети активно внедряются крупными провайдерами домашних сетей. Поскольку число сервисов (например, данные, VoIP, IPTV) постоянно растет, провайдеры выбирают коммутаторы, которые поддерживают более 1024 статических VLAN (стандарт 802.1Q). Для соединения сетей офисов через сеть провайдера используется механизм Double VLAN (Q-in-Q), что позволяет эффективнее использовать идентификаторы виртуальных сетей (VLAN ID) в крупных сетях. О том, что такое Double VLAN, вы можете прочитать по адресу: **http://www.dlink.ru/technical/faq_hub_switch_86.php**. Там же можно найти примеры настройки Double-VLAN.

27.10. Вместо заключения

Понятно, что этот материал полностью не охватывает все секреты настройки VLAN, но, надеюсь, общее впечатление у вас сформировалось. Дополнительную информацию можно получить по следующим ссылкам:

- **http://ru.wikipedia.org/wiki/VLAN** — общая информация о VLAN;
- **http://www1.bstu.by/wiki/index.php?title=VLAN_802.1Q** — стандарт 802.1Q;
- **http://people.freebsd.org/~arved/vlan/vlan_en.html** — о настройке VLAN в FreeBSD (FreeBSD VLAN mini HowTo);
- **http://www.opennet.ru/tips/info/1381.shtml** — ссылка посвящена двойной инкапсуляции Q-in-Q, позволяющей создавать дважды маркированный трафик.

Заключение

Заключение будет традиционно кратким — как в большинстве моих книг. И не потому, что краткость — сестра таланта, я просто не вижу особого смысла писать огромный и не содержащий конкретики текст, который прочитает один читатель из ста.

Здесь же разрешите выразить вам свою благодарность за покупку именно моей книги. В случае если у вас возникнут какие-либо вопросы, замечания или просто пожелания, вы всегда можете найти меня на форуме моего сайта: **www.dkws.org.ua** (зеркала **dkws.net** и **dkws.org**). Обещаю оказать посильную помощь всем, кто ко мне обратится.

Предметный указатель