Александр Ватаманюк

Создание и обслуживание сетей в Windows 7

Введение

«Кто владеет информацией, тот владеет миром» – это высказывание наверняка слышали многие из вас. Информация – самое важное и ценное, чем обладает человечество. Она постоянно аккумулируется, заменяет старую, устраняет лишнюю, подтверждает достоверность существующей. Обладая нужной информацией, можно создать практически все и с нуля. Именно поэтому столь важно постоянно иметь доступ к информации: чем больший объем ее будет доступен, тем большую ценность это представляет для человека.

Появление первых компьютеров вызвало бурю радости в научной сфере, поскольку с их помощью можно было проводить уникальные исследования, получая в результате новые технологии. Кроме того, компьютеры позволили автоматизировать множество процессов, что было выгодно как производителям, так и потребителям разнообразнейших товаров.

Появление первых локальных сетей вызвало не меньший шквал эмоций, но теперь радовались те, кто уже успел понять, что такое компьютер и какие преимущества дает его использование. Причина проста: объединение компьютеров в сеть позволило получить самое важное – доступ к информации. Одни просто черпали нужные для себя данные, изучая премудрости наук, другие объединяли свои усилия для исследования чего-то нового.

Сегодня без локальной сети уже не обойтись. Распределенные базы данных, системы бухгалтерского и оперативного учета, дистанционное обучение, удаленный контроль за разнообразными процессами, сетевые игры – все это требует совместной работы многих пользователей, а она возможна, только когда компьютеры соединены в сеть. А ведь еще есть Интернет, без которого уже никто не может обойтись…

Наверняка многие из вас уже задумывались над тем, что было бы неплохо воспользоваться преимуществами локальной сети. Не имеет значения, использовать ее в офисе или дома, соединять два или двадцать компьютеров – удобство локальной сети вы ощутите сразу же.

Книга, которую вы держите в руках, познакомит вас с особенностями локальных сетей и даст достаточно сведений, чтобы можно было воплотить свои задумки в жизнь. Теория и практические советы, приведенные в этой книге, изложены в настолько простой форме, что, только начав читать, вы уже захотите использовать приобретенные знания на

практике. И это будет правильным решением!

Часть 1
Общие сведения о сетях

Глава 1
Сеть: необходимое преимущество?

Вернемся немного назад во времени, лет так на сто.

Потребность в появлении компьютера как средства произведения вычислений зрела давно. Существовавшие примитивные устройства не позволяли производить сложные вычисления, а для того, чтобы исследовать какой-либо сложный процесс или явление, требовались годы труда множества сотрудников. То же касалось информации: тысячи книг хранились в библиотеках и разного рода хранилищах, но получить доступ к ним было очень трудно, а то и вовсе невозможно.

Примерно в это время начали появляться первые счетные машины, позволяющие автоматизировать достаточно сложные вычисления, например решение простейших дифференциальных уравнений.

Этот период стал переломным. Именно тогда человечество вплотную приблизилось к столь важному изобретению, без которого просто невозможно представить современную жизнь. Хотя, конечно, многие прекрасно обходились существующими арифмометрами…

Появление первых компьютеров, которые были еще аналоговыми, произошло практически незаметно для основной массы людей. Кроме того, специфика этих компьютеров позволяла использовать их лишь в производственных целях: для автоматизации достаточно простых процессов.

Однако время и технологии не стояли на месте. Совершались новые открытия, аналоговые устройства превращались в механические, сложность компьютеров росла, как и сфера их применения.

Настоящий компьютерный бум начался в 50-х годах прошлого века, когда появились первые цифровые компьютеры. В то время вся научная общественность массово переходила на использование компьютерной техники, которая открывала перед своими пользователями невиданную вычислительную мощь. Именно это время стало началом новой эры в развитии человечества – эры компьютеризации.

Время шло, компьютеры совершенствовались, появились первые персональные компьютеры, и их распространение уже ничто не могло остановить. Однако оставалось одно «но»: ученые, как и прежде, столкнулись с тем, что мощности одного компьютера, пусть даже очень большого, не хватало для того, чтобы производить действительно сложные вычисления. Было очевидно, что несколько компьютеров смогут сделать больше, чем один, и это стало причиной появления локальной сети. Конечно, сначала это был всего лишь способ объединить главный майнфрейм с рабочей станцией, затем – несколько

рабочих станций с главным компьютером и, наконец, – создать единую сеть из большого количества компьютеров, чтобы использовать общие ресурсы.

Когда же персональные компьютеры подешевели настолько, что стали доступны не только крупным организациям и образовательным учреждениям, но и рядовым пользователям, локальная сеть стала своего рода стандартом.

Локальные сети нашли свое применение в образовании, медицине, промышленности и в других областях жизни человека, где требовались вычислительная мощь и доступ к ресурсам. Когда же появился Интернет, локальная сеть стала просто незаменимой, даже если речь шла о нескольких компьютерах.

А теперь ответьте на простой вопрос: нужны ли нам компьютеры, локальные сети и Интернет как яркий представитель сети? Дают ли они преимущество перед обычным, автономным использованием компьютеров?

Глава 2
Создание сети своими силами

Количество компьютеров растет с каждым днем, и этим уже никого не удивишь. Естественно, отдельно стоящие компьютеры теперь не очень интересны, да и не позволяют удовлетворять все возрастающие потребности. Поэтому стоило только появиться способу соединения компьютеров, как его сразу же стали развивать.

Конечно, первые локальные сети требовали вложения круглых сумм, поскольку необходимое оборудование, расходные материалы и инструменты были достаточно дороги. В связи с этим созданием сетей занимались только организации, у которых были деньги и соответствующая квалификация.

Однако время шло, компьютерные технологии на месте не стояли и постепенно проникали во все организации, от мала до велика. Сегодня, когда прошло уже почти полвека со времени первого объединения компьютеров, локальные сети настолько широко распространились, что теперь любой достаточно грамотный пользователь компьютера может своими руками создать, например, у себя дома простую локальную сеть. А если вооружиться достаточным багажом знаний, то вполне по силам будет самостоятельно создать локальную сеть, например, в офисе, с большим количеством сетевых подключений.

Итак, что же необходимо знать и уметь, чтобы взяться за создание локальной сети? Как и в любом другом деле, требуется всего три вещи: знания, умения и навыки, но можно добавить и четвертую – желание. Раз у вас в руках эта книга, значит, с желанием у вас все в порядке. Остается только определиться, какими знаниями, умениями и навыками необходимо обладать, чтобы осуществить задуманное.

Необходимые знания

Локальная сеть – это не просто провод, привязанный к системному блоку компьютера, и электронная плата, приклеенная скотчем к материнской плате. Естественно, существует теоретическая основа, включающая в себя все правила и особенности функционирования локальных сетей. Именно она четко описывает, какая среда передачи данных, какие сетевые адаптеры и какие программные манипуляции нужны, чтобы соединить хотя бы два компьютера в локальную сеть и организовать обмен данными между ними.

Из наиболее важных аспектов, с которыми необходимо подробно познакомиться, можно отметить следующие.

▪ Основные типы сети. Тип сети определяет функциональность и возможности локальной сети, поэтому его выбор в большинстве случаев очень критичен.

▪ Топология сети. Топология сети описывает способ соединения участников сети и влияет не только на надежность сети, но и на принцип и скорость обмена информацией между участниками.

▪ Модель ISO/OSI. Одно из ключевых понятий, так как содержит описание всего, что происходит в локальной сети: от самой информации до способов ее передачи по существующему каналу связи.

▪ Протоколы передачи данных. Протоколы – «носители» информации, умеющие передавать и принимать данные, учитывая все особенности передающей среды.

▪ Среда и методы передачи данных. Среда передачи данных – любой канал связи, используемый для передачи данных. Выбор среды передачи данных влияет на выбор сетевого стандарта и методов передачи данных, что в результате однозначно определяет скорость и надежность передачи данных.

▪ Сетевые стандарты и спецификации. Сетевой стандарт – набор правил и соглашений, влияющих как на стоимость создания локальной сети, так и на ее возможности.

▪ Сетевое оборудование. Сетевое оборудование – это не что иное, как практическая реализация того, что описывают стандарты. Внешний вид, исполнение и возможности сетевого оборудования напрямую зависят от выбранного сетевого стандарта и среды передачи данных.

▪ Правила проектирования и монтажа сети. Работоспособность и надежность локальной сети во многом зависят от того, насколько грамотным был процесс ее проектирования и монтажа. Если сделать все правильно, то можно обойти многие проблемы, иногда возникающие в процессе эксплуатации сети.

При правильном изложении информации ее восприятие значительно облегчается, а скорость понимания и освоения увеличивается. Мы уверены, что с помощью этой книги вы быстро и легко разберетесь во всех интересующих вас вопросах, что в конечном итоге поможет вам при создании локальной сети. Поэтому не отступайте и не сдавайтесь – и уже через неделю вы сможете приступить к практической реализации полученных знаний.

Необходимые умения и навыки

Теория – теорией, но практические навыки при монтаже сети играют ключевую роль. Особенно это важно, когда речь идет о создании локальной сети с большим количеством подключений, сетевые узлы которой расположены на разных этажах высотного здания или в удаленных друг от друга строениях.

Однако если у вас нет опыта в монтаже сети, то это совсем не означает, что вы не сможете ее создать. Ничто не мешает вам получить необходимые навыки, помогая в создании локальных сетей своим друзьям или в офисе на работе. Подобная практика и есть наиболее оптимальный способ приобретения опыта.

Если же поучаствовать в создании локальных сетей по разным причинам нет возможности, придется пойти сложным путем – вооружиться теоретическими знаниями и на своих ошибках научиться все делать самому: выбирать и обжимать кабель, заниматься монтажом коробов и сетевых розеток, осваивать активное сетевое оборудование, настраивать операционную систему и т. д.

Из наиболее важных аспектов, которые играют роль при монтаже и настройке локальной сети, можно отметить следующие.

▪ Принципы проектирования сети. Сетевыми стандартами и спецификациями достаточно жестко регламентируются разные параметры локальной сети, в частности,

какой длины должны быть сегменты, какое оборудование должно использоваться, каким способом должны соединяться сетевые узлы и т. п. Кроме того, если планируется использовать в качестве среды передачи данных кабель, то существуют определенные ограничения на его прокладку и монтаж, которые также необходимо учитывать.

▪ Правила монтажа кабеля. При монтаже кабельной системы необходимо учитывать некоторые правила. К примеру, любой кабель рассчитан на использование в определенных условиях, поэтому при его монтаже необходимо избегать областей, которые могут отрицательно повлиять на его характеристики. Кроме того, есть правила изгиба кабеля, его обжима в коннекторах и сетевых розетках, монтажа в монтажном шкафу и кросс-панелях и т. д.

▪ Принцип расположения точек доступа. Беспроводная сеть в своей работе использует точки доступа, от правильного расположения которых зависят радиус покрытия, мощность сигнала, скорость передачи данных, безопасность локальной сети и другие параметры.

▪ Сетевое оборудование. Функциональность сетевого оборудования определяет параметры сети, поэтому знание предназначения и принципов функционирования того или иного устройства позволяет сделать локальную сеть максимально надежной и быстрой.

▪ Умение обращаться с инструментами. При создании локальной сети с использованием кабельной системы для работы с кабелем используются специальные инструменты. Знакомство с ними и умение их использовать сделает процесс монтажа локальной сети более простым и качественным.

▪ Особенности настройки операционной системы. Даже если монтаж сети уже завершен, это совсем не означает, что сеть уже работает. Для того чтобы она действительно заработала, необходимо произвести целый ряд настроек: выбрать способ работы сети и установить соответствующее программное обеспечение, настроить операционную систему каждого компьютера, настроить необходимые протоколы передачи данных, создать и настроить общие ресурсы и т. д.

Если вы знакомы со всеми этими аспектами и имеете хотя бы немного опыта монтажа, то вы спокойно можете взяться за создание локальной сети. И пусть сначала она будет небольшой, из нескольких компьютеров, но это позволит вам получить больше опыта и отточить свое мастерство. А уж за созданием достаточно серьезной сети дело не станет, ведь не боги же горшки обжигают!

Глава 3
Основные типы и варианты сетей

Появление компьютерных сетей было вполне ожидаемым шагом в процессе компьютеризации общества. Благодаря этому компьютеры теперь есть почти в каждом доме и в любом офисе, а самое главное – практически в каждый дом пришел Интернет, несущий в себе безграничные источники информации.

Компьютерные сети прошли долгий этап развития, и в результате мы имеем возможность объединить компьютеры как в локальном, так и в глобальном масштабе.

Существует два варианта сетей: локальные и глобальные. Принцип объединения компьютеров и их работы в этих сетях практически идентичен, но масштабы сети накладывают свои ограничения и требования.

Локальная сеть, LAN (Local Area Networks), – сеть, с помощью которой объединяются компьютеры на ограниченной территории. Такой вариант сети встречается в офисах, на

предприятиях, в залах ожидания аэропортов и вокзалов, кафе, ресторанах и т. д. Главное ее предназначение – организация доступа к общим внутренним ресурсам. При этом локальная сеть часто имеет подключение к Интернету, что делает ее частью глобальной сети.

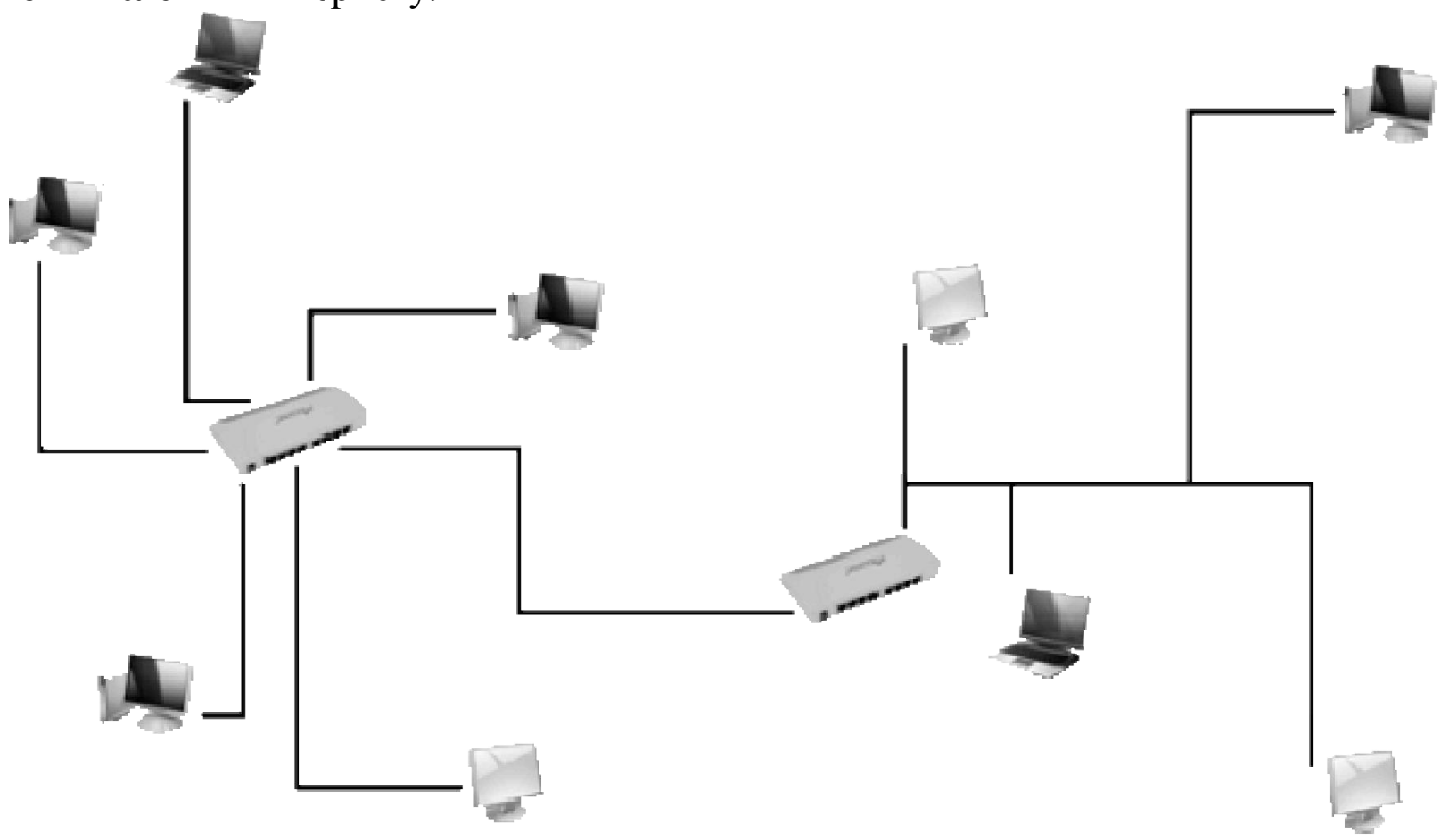
Глобальная сеть, WAN (Wide Area Networks), – сеть, состоящая из множества локальных сетей и отдельно стоящих компьютеров, которые соединяются между собой любым доступным способом. При этом работоспособность всей сети не зависит от работоспособности отдельных ее элементов. Примером открытой глобальной сети является сеть Интернет, которая за свою разветвленную структуру получила название Всемирной паутины.

Однако наиболее важной характеристикой сети является ее тип. Ведь именно от типа зависят возможности сети, ее безопасность, управляемость и, самое главное, условия доступа к важным данным.

Различают два типа сетей: одноранговую сеть и сеть на основе сервера. Каждый из этих типов по-своему выполняет поставленную перед ним задачу и требует разных финансовых затрат, в чем вы сможете убедиться далее.

Одноранговая сеть

Одноранговая сеть (рис. 3.1) хоть и является наиболее простой и дешевой в создании, тем не менее способна обеспечить своим пользователям доступ к нужной информации, в том числе и к Интернету.



Главной особенностью такой сети является то, что каждый участник сети, то есть каждая рабочая станция, имеет одинаковые права и выступает в роли администратора

своего компьютера. Это означает, что только он может контролировать доступ к своему компьютеру, создавать общие ресурсы и определять правила доступа к ним. С одной стороны, такую сеть очень просто создать, но с другой стороны, администрирование такой сети вызывает достаточно много проблем, особенно если в ней насчитывается более 25 узлов.

Одноранговые сети обычно оборудуют в небольших офисах, ресторанах, кафе и залах ожидания, то есть в тех местах, которые без проблем позволяют поддерживать работу сети с небольшим количеством подключений. Однако, хотя это и противоречит всем принципам, одноранговые сети используются и в так называемых домашних сетях, при этом количество подключений может быть очень большим, например 1000 и более компьютеров. Главное объяснение этому факту – хаотичный и наиболее дешевый способ создания локальной сети.

Системному администратору одноранговой сети приходится достаточно сложно, особенно если в сети много участников. К примеру, чтобы ограничить доступ пользователя к тем или иным устройствам, потребуется изменить определенные настройки операционной системы, а сделать это централизованно невозможно: необходимо личное присутствие возле каждого из компьютеров либо использование программ удаленного управления компьютером. Это же касается обновления антивирусных баз, установки обновлений операционной системы и офисных программ и т. д.

Таким образом, использование одноранговых сетей можно считать оправданным только в том случае, если количество узлов достаточно мало и все они расположены на небольшой территории, например в пределах одного или нескольких помещений.

Поддержка одноранговых сетей имеется в любой современной операционной системе семейства Microsoft Windows. Поэтому никакого дополнительного программного обеспечения не требуется, а также нет никаких ограничений в конфигурации используемых компьютеров и установленных на них операционных систем.

ВНИМАНИЕ

Стоит учесть один нюанс: если вы решите организовать доступ к общему ресурсу, то вступит в действие ограничение на 10 одновременных подключений, которое можно «вылечить» только установкой серверной операционной системы.

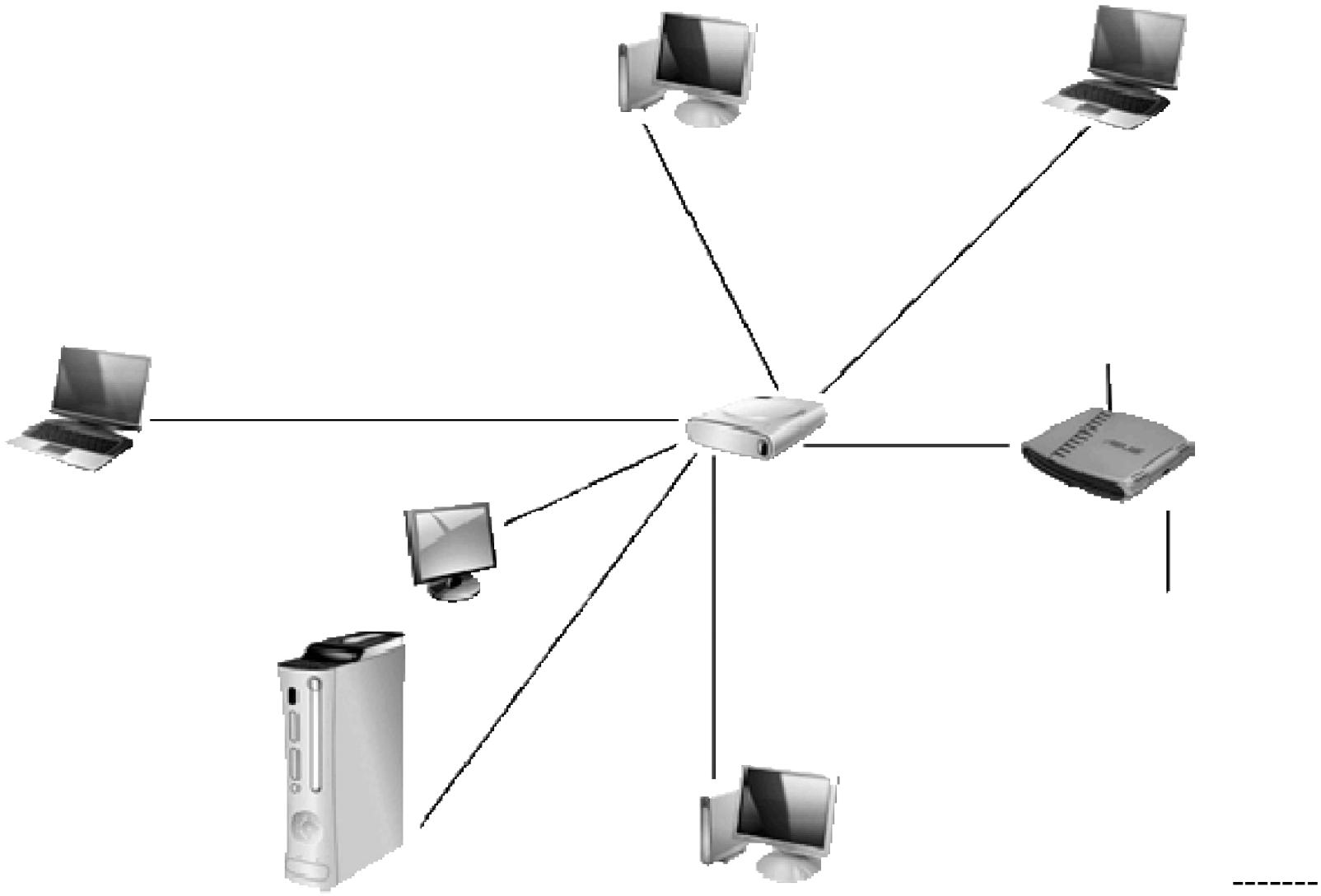
Ниже в табл. 3.1 приведены основные преимущества и недостатки одноранговой сети, на которые обязательно стоит обратить внимание, прежде чем выбрать ее в качестве будущей локальной сети.

Таблица 3.1. Особенности одноранговых сетей

Преимущества сети	**Недостатки сети**
Простая и дешевая в создании	Отсутствие централизованного хранилища ресурсов
Не требует управляющих компьютеров	Отсутствует возможность административного управления пользователями и ресурсами
Работа сети не зависит от работоспособности отдельных узлов	Каждый пользователь должен самостоятельно следить за состоянием программного обеспечения
	За обновление антивирусной и подобных ей баз отвечает пользователь
	Низкий уровень защиты информации

Сеть на основе сервера

Сеть на основе сервера (рис. 3.2), или, как ее еще часто называют, сеть типа «клиент – сервер», – наиболее удобный и востребованный тип сети, основными показателями которого являются высокая скорость передачи данных и высокий уровень безопасности.



Под словом «сервер» следует понимать выделенный компьютер, на котором установлена система управления пользователями и ресурсами сети. Данный компьютер в идеале должен отвечать только за обслуживание сети и не выполнять больше никаких других задач. Этот сервер носит название контроллера домена, и от него зависит работоспособность всей сети. Именно поэтому данный сервер обязательно подключается к системе бесперебойного питания. Мало того, в сети, как правило, присутствует дублирующий сервер, который носит название вторичного контроллера домена: в случае выхода контроллера домена из строя он сразу же начинает выполнять его работу.

Кроме контроллера домена в сети могут использоваться и другие серверы разного назначения, к числу которых относятся следующие.

▪ Файл-сервер. Данный сервер представляет собой хранилище файлов разного типа. На нем, как правило, хранятся файлы пользователей, общие информационные ресурсы, аудио– и видеофайлы общего использования и многое другое. Главное требование к

файловому серверу – надежная дисковая подсистема, которая обеспечит безопасное хранение файлов и доступ к ним в любое время суток. Часто на данном сервере устанавливается архивирующая система, например стример, с помощью которого осуществляется плановое создание архивных данных. Это обеспечивает гарантированное восстановление данных в случае непредвиденных сбоев оборудования.

▪ Сервер базы данных. Подобного типа серверы наиболее востребованы, поскольку позволяют обеспечить доступ к единой базе данных, в качестве которой могут выступать базы данных бухгалтерского и другого типа учета, юридические базы данных и т. д. В качестве сервера базы данных используются мощные компьютеры с большим объемом оперативной памяти и RAID-массивом из быстрых жестких дисков. Очень важно организовать архивирование данных, поскольку от целостности базы данных и доступа к ней зависит работа всего предприятия.

▪ Сервер приложений. Сервер приложений используется в качестве промежуточного звена между сервером базы данных и клиентским компьютером. Это позволяет организовать так называемую трехзвенную, или трехуровневую, архитектуру, с помощью которой программы, требующие обмена с базой данных, могут работать с максимальной скоростью и эффективностью. Кроме того, за счет такой организации увеличивается безопасность доступа к данным и становится легче управлять всем процессом: ведь проще контролировать работу одного компьютера, нежели сотни.

▪ Принт-сервер. Специализированный сервер, позволяющий ускорить процесс печати и контролировать его. Используется в сетях, которым необходим доступ к общему принтеру. Подобного рода сервер управляет очередью печати и обеспечивает доступ к принтеру любому типу клиента, будь то проводное или беспроводное соединение, переносное устройство или мобильный телефон.

▪ Интернет-шлюз. Использование этого сервера вызвано необходимостью доступа пользователей локальной сети в Интернет, а также доступа к ресурсам по протоколам ftp и http. Поскольку данный сервер является «окном» во внешнюю сеть, к нему предъявляется ряд требований, среди которых главные – это безопасность локальных данных и защита от доступа к ним извне. Именно поэтому на данном сервере устанавливают разного рода сетевые фильтры и брандмауэры, позволяющие эффективно фильтровать входящий и исходящий трафик, что делает использование Интернета более безопасным.

▪ Почтовый сервер. Практически каждое серьезное предприятие для общения с внешним миром пользуется корпоративными электронными ящиками. Этот подход вполне оправдан, поскольку позволяет контролировать входящий и исходящий трафик, тем самым блокируя возможность утечки информации. Для того чтобы подобная система обмена информацией была возможной, используется почтовый сервер с соответствующим программным обеспечением. Дополнительно на этот сервер устанавливаются разнообразные антиспамовые фильтры, позволяющие бороться, насколько это возможно, со всевозрастающим объемом рекламных писем, которые и называются спамом.

Кроме упомянутых выше типов серверов могут использоваться и другие, что зависит только от реальных потребностей сети. Подключение новых серверов не вызывает никаких трудностей, поскольку гибкость и возможности сети на основе сервера позволяют сделать это в любой момент.

Для системного администратора сеть на основе сервера будет сложнее в создании и обслуживании, но зато она наиболее управляемая и контролируемая. При помощи управляющего компьютера можно очень легко и эффективно следить за учетными

записями пользователей, а благодаря политике безопасности упрощается контроль над самими компьютерами, что делает данные в сети более защищенными.

На сервер устанавливается серверная операционная система, которая, в отличие от клиентской операционной системы, обладает рядом преимуществ, например поддержкой нескольких процессоров, бóльшего объема оперативной памяти, инструментами администрирования сети и т. д. К таким системам относятся операционные системы Windows 2003 Server, Windows 2008 и т. д.

В табл. 3.2 вы можете увидеть основные недостатки и преимущества сетей на основе выделенного сервера.

Таблица 3.2. Особенности сетей на основе выделенного сервера

Преимущества сети	Недостатки сети
Высокая скорость и производительность сети	Дорогая в создании и обслуживании
Использование выделенных серверов облегчает работу с ресурсами, упрощает контроль над их использованием	Требуется постоянный системный администратор
Наличие дублирующих систем, позволяющих защитить данные и сделать доступ к ним бесперебойным	Зависимость сети от работоспособности контроллера домена
Централизованные обновления операционной системы и программного обеспечения	
Полный контроль над пользователями сети	
Высокий уровень безопасности данных	
Продвинутые средства мониторинга работоспособности сети	
Легкая расширяемость сети	

Глава 4
Топология: способы объединения компьютеров

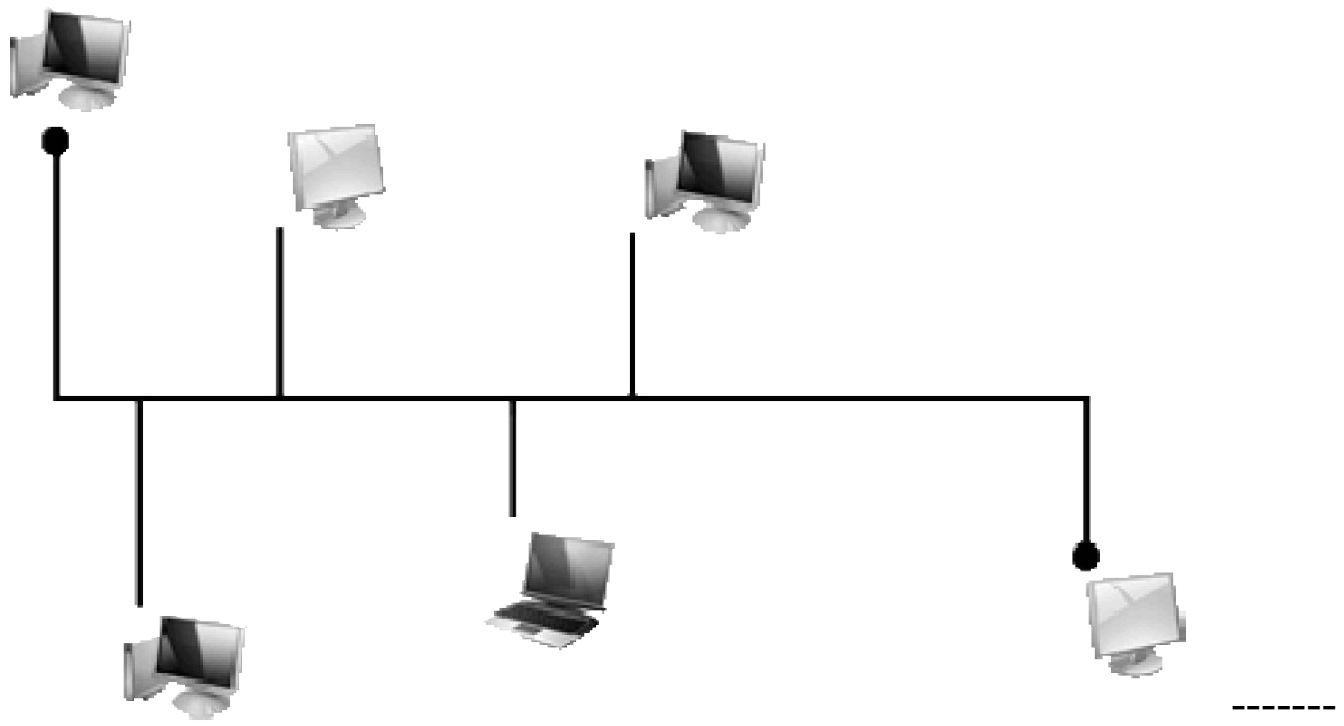
При проектировании и создании сети важную роль играет способ объединения компьютеров и других узлов. От него зависят скорость передачи данных, надежность сети, степень устойчивости к поломкам, возможности администрирования и многое другое. Первым и, пожалуй, самым важным фактором, от которого зависят упомянутые показатели, является топология сети.

Топология сети, или сетевая топология, – это описание схемы сети, включающее в себя способ взаимного расположения компьютеров и способ их объединения, а также правила, связанные с прокладкой кабеля, подключением оборудования, взаимодействием управляющих устройств и т. д.

Существует достаточно много способов объединения компьютеров. К их числу относятся топологии «шина», «звезда», «кольцо», «двойное кольцо», «дерево», «решетка» и др. Наибольшее распространение получили сетевые топологии «шина», «звезда» и «кольцо», поэтому именно они будут рассмотрены в данной книге.

Топология «шина»

Согласно топологии «шина», или, как ее еще часто называют, «общая шина» или «магистраль», все участники сети подключаются к центральному кабелю (рис. 4.1). Для предотвращения дальнейшего распространения и возможного отражения сигнала на концах кабеля устанавливаются специальные заглушки – терминаторы, один из которых обязательно заземляется.



Данные в такой сети передаются сразу всем компьютерам, поэтому задача каждого компьютера – проверить, не ему ли адресовано сообщение. Только компьютер, которому адресовано сообщение, может обработать его. При этом пока данные не будут обработаны, никакие сообщения больше не отправляются. Как только данные обработаны, сигнал об этом поступает в сеть и работа возобновляется.

Достоинство такой сети в том, что создать ее просто и достаточно дешево. При ее построении используется минимальное количество кабеля и не требуется никакого управляющего оборудования: в обмене данными участвуют только сетевые адаптеры компьютеров. В случае если количество компьютеров уже достаточно велико, сеть часто разбивается на сегменты, для соединения которых используются повторители – концентраторы, коммутаторы, мосты и т. п.

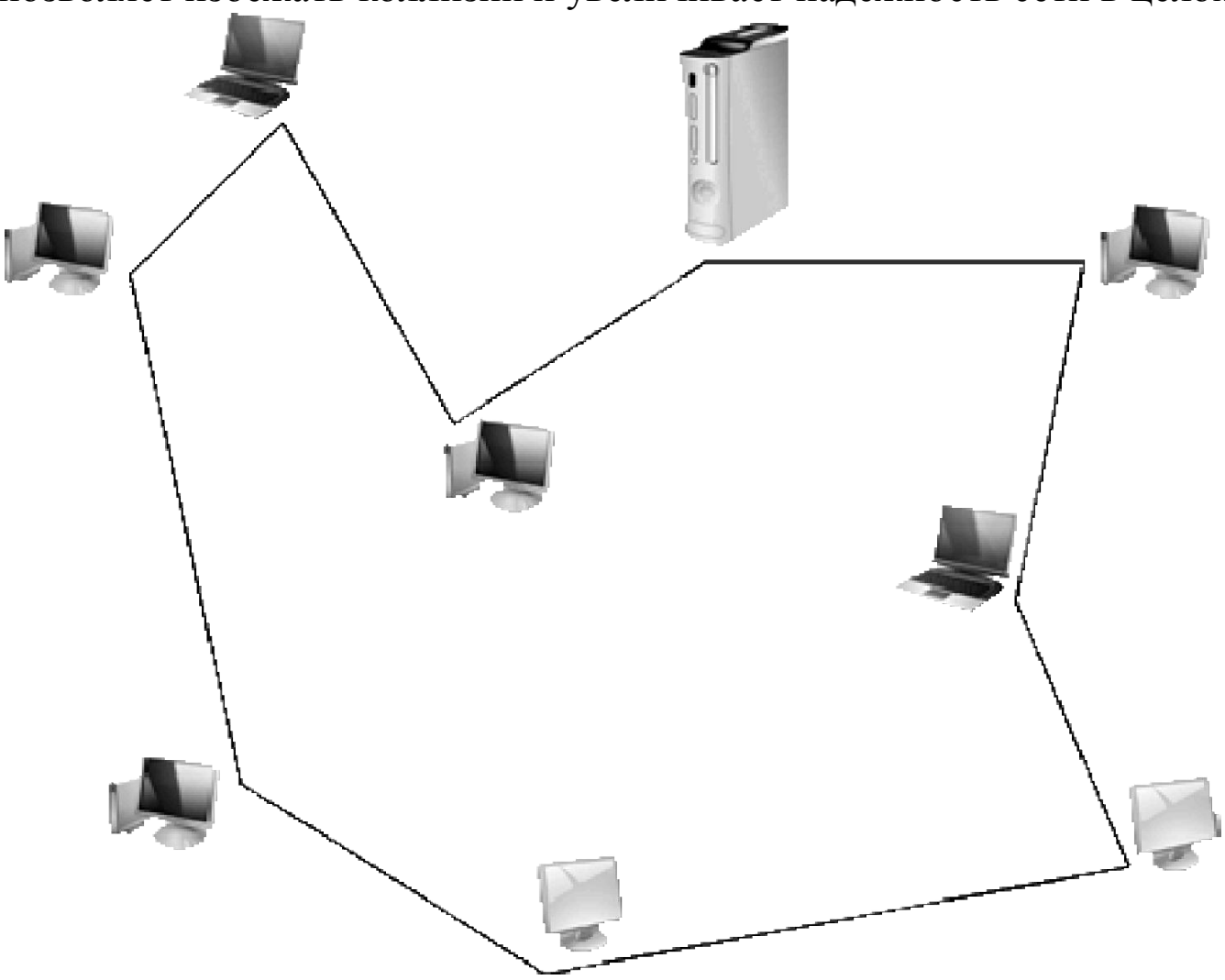
Главный минус сети – прямая зависимость скорости передачи данных от количества подключенных компьютеров: чем больше компьютеров и других устройств, тем ниже скорость передачи данных. Кроме того, обрыв центрального кабеля или нарушение контакта в любом из разъемов парализует работу всей сети, при этом обнаружить причину порой бывает очень сложно.

Топология «кольцо»

Согласно топологии «кольцо» все компьютеры сети подключаются последовательно и образуют своего рода замкнутую кольцевую структуру (рис. 4.2).

Для передачи данных в сети используется маркерная система, то есть в конкретный

момент времени передавать данные может только компьютер, захвативший маркер. При этом данные передаются только следующему по кругу компьютеру (справа налево). Это позволяет избежать коллизий и увеличивает надежность сети в целом.



Когда компьютеру, обладающему маркером, необходимо передать данные, маркер дополняется адресом компьютера, которому эти данные предназначены, и маркерный блок отправляется в сеть по кругу. Каждый компьютер, который лежит на пути следования маркерного блока, считывает из него адрес получателя и сравнивает его со своим адресом: если адреса не совпадают, то компьютер отправляет маркерный блок далее по кругу, предварительно усилив сигнал. Если адреса совпали, то есть отправитель найден, формируется подтверждающий блок, который передается далее по кругу, к отправителю: в дальнейшем данные уже передаются по найденному пути до тех пор, пока они не будут переданы в полном объеме. Как только передача данных заканчивается, маркер освобождается и идет далее по кругу до первого компьютера, который также хочет передавать данные.

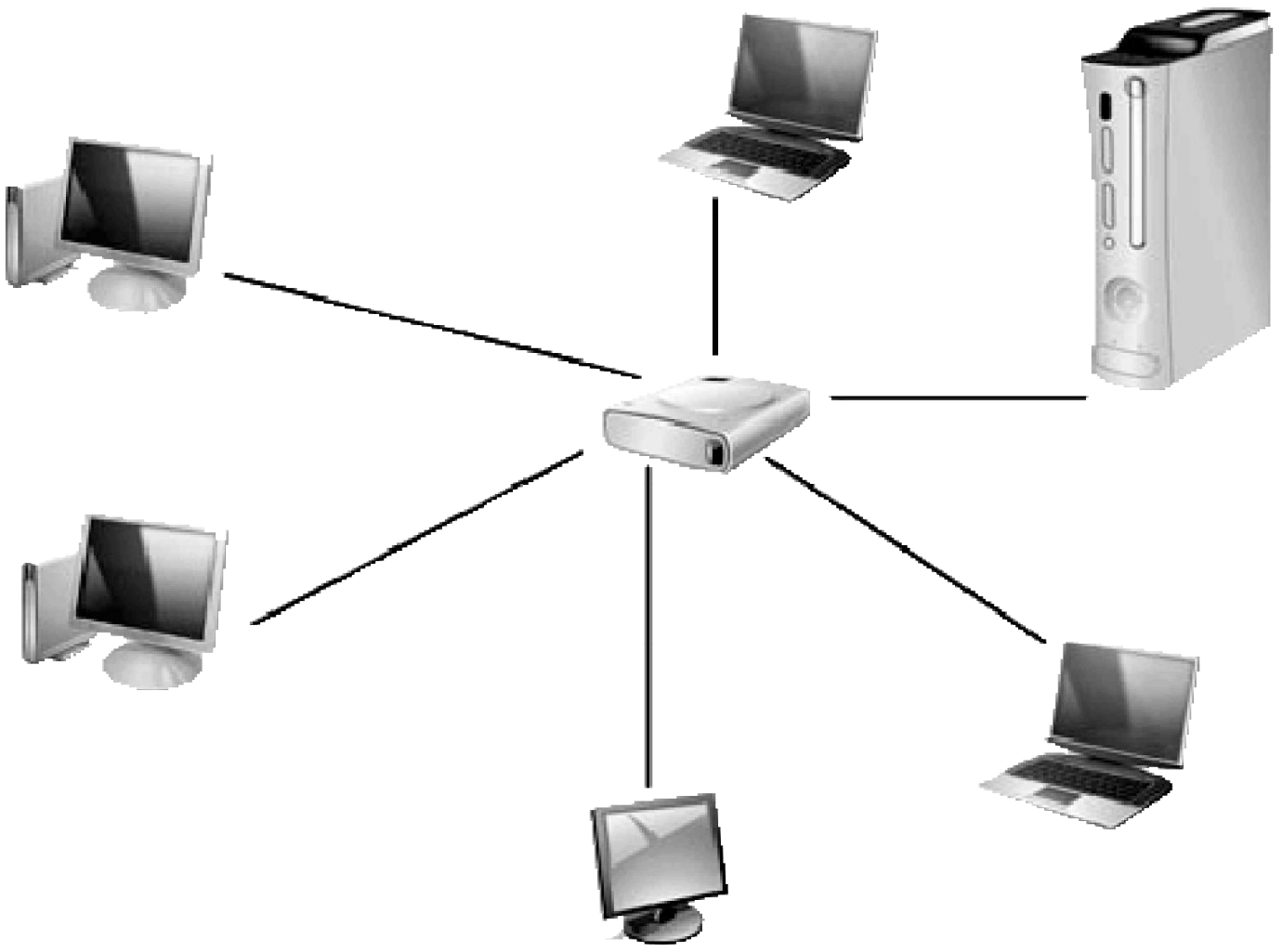
Использование топологии «кольцо» обладает рядом преимуществ. Например, каждый компьютер сети одновременно выступает повторителем, поэтому уменьшение уровня сигнала возможно только между соседними компьютерами, что напрямую зависит от расстояния между ними. Кроме этого, сеть способна справляться с очень большими объемами трафика за счет отсутствия коллизий и центрального управляющего узла.

Существуют, однако, и недостатки. К примеру, подключение нового компьютера требует остановки работы всей сети. Аналогичная ситуация случается, если один из компьютеров выходит из строя: сеть становится неработоспособной. Кроме того, поиск неисправности в такой сети сопряжен с множеством сложностей.

Топология «звезда»

Топология «звезда» на сегодня является наиболее распространенным способом объединения компьютеров в сеть. Согласно этой топологии каждый компьютер или устройство сети подключается к центральному узлу, тем самым образуя сегмент сети (рис. 4.3).

Сегменты сети общаются между собой посредством того же центрального узла либо промежуточного узла, образуя более сложную сеть или входя в состав комбинированной сети.



В качестве центрального узла используется любое активное сетевое устройство с достаточным количеством портов. В самом простом случае в роли центрального узла выступает концентратор, при этом поступившие ему данные пересылаются сразу же всем подключенным к концентратору устройствам. Если на концентратор в один момент времени поступают данные от двух разных отправителей, оба пакета игнорируются.

В случае с более интеллектуальным узлом, например коммутатором, данные одновременно могут передаваться сразу несколькими компьютерами, что значительно увеличивает скорость передачи данных.

Несмотря на то что использование топологии «звезда» самое дорогостоящее (по сравнению с использованием других топологий), надежность сети и высокая скорость передачи данных делают ее применение практически стандартом. Кроме того, принятый уже достаточно давно стандарт ATX подразумевает наличие на материнской плате персонального компьютера интегрированного сетевого адаптера, который изначально «заточен» под работу с этой топологией.

Глава 5
Эталонная модель взаимодействия открытых систем

Теоретической основой функционирования сети является свод правил и стандартов, которые описывают так называемую модель взаимодействия открытых систем (Open System Interconnection, OSI). Основным разработчиком модели является Международная организация по стандартизации (International Organization for Standardization, ISO), поэтому очень часто используется более короткое название – модель ISO/OSI.

Согласно модели ISO/OSI существует семь уровней, пройдя через которые данные от одного компьютера могут быть переданы другому компьютеру, и абсолютно не важно, какая операционная система или оборудование при этом используется и каким образом данные попадают от источника к адресату.

Уровни имеют названия и расположены в следующем порядке: физический, канальный, сетевой, транспортный, сеансовый, уровень представления данных и прикладной уровень. Данные могут передаваться как в указанном, так и в обратном порядке. Так, при передаче данные начинают свое движение с прикладного уровня и доходят до физического уровня, который непосредственно связан со средой передачи данных. Если же данные принимаются, то они проходят путь от физического до прикладного уровня (рис. 5.1).

-

Описанная модель является стандартом для любой среды передачи данных, которых на сегодня используется три: кабель, радиоволны и инфракрасное излучение. Однако, учитывая особенности среды передачи данных, имеются определенные различия в работе физического и канального уровней модели ISO/OSI, в чем вы сможете убедиться далее.

Каждый уровень отвечает только за свою часть подготовки данных к приему или передаче, что в результате позволяет сделать процесс передачи/приема максимально эффективным и, самое главное, независимым от среды передачи данных. Кроме того, что немаловажно, это позволяет забыть о вопросе совместимости оборудования, которое используется для приема и передачи данных.

Как уже было упомянуто выше, модель ISO/OSI состоит из семи уровней, а именно:

- физический — передача и прием электрических сигналов;
- канальный — управление каналом связи и доступом к среде передачи данных;
- сетевой — определение оптимальных маршрутов передачи данных;
- транспортный — контроль целостности и правильности данных в процессе передачи и приема данных;
- сеансовый — создание, сопровождение и поддержание сеанса связи;
- уровень представления — кодирование и шифрование данных с помощью требуемых алгоритмов;
- прикладной — взаимодействие с клиентскими программами.

Данные между разными уровнями модели передаются посредством стандартных интерфейсов и протоколов передачи данных, главная задача которых – обработка полученных данных и приведение их к тому виду, который необходим для работы следующего уровня. Более подробно о разных протоколах передачи данных вы сможете узнать далее.

Физический уровень

Физический уровень (Physical Layer) является самым нижним в модели ISO/OSI. Он работает непосредственно с имеющимся каналом связи. Его главная задача – преобразование поступивших от вышестоящего уровня данных и передача соответствующих им электрических сигналов по каналу связи получателю, а также прием данных от отправителя и их конвертирование согласно существующим таблицам кодирования сигналов с передачей данных вышестоящему уровню.

Прежде чем начать передачу электрических сигналов, алгоритмы физического уровня определяют тип канала связи и его свойства: электротехнические и механические характеристики, величину напряжений, расстояние между отправителем и получателем, скорость передачи данных и т. д., то есть все, что является критичным для передачи данных. Именно на этом этапе определяется, сеть какого типа используется (проводная или беспроводная), а также выясняется топология сети.

Функции физического уровня выполняют сетевые адаптеры на отправителе и получателе, а также повторители сигнала, например концентратор.

Стандартизация на уровне модели ISO/OSI позволяет использовать в сети оборудование разных производителей, не заботясь при этом об их совместимости, что дает возможность сосредоточиться только на процессе передачи и приема данных.

Канальный уровень

Задача канального уровня (Data Link Layer) – обеспечить гарантированную передачу данных через физический канал, параметры и особенности которого уже установлены и «приняты во внимание» на физическом уровне. При этом решаются вопросы физической

адресации, корректности отправленной и полученной информации, контроля возникающих ошибок, управления потоком информации и т. д.

Данные передаются блоками, которые называются кадрами. К каждому кадру добавляется несколько бит информации о типе кадра, а также контрольная сумма, которая сверяется при его получении адресатом. При несовпадении контрольных сумм запрашивается повторная передача кадра и данные синхронизируются.

За работу канального уровня локальных сетей отвечают два подуровня:

- MAC (Medium Access Control) – уровень доступа к разделяемой среде;
- LLC (Logical Link Control) – уровень управления логическим каналом.

Уровень MAC отвечает за получение доступа к общей среде передачи данных, в связи с чем каждый протокол передачи данных имеет соответствующую процедуру доступа. Кроме того, MAC отвечает за согласование режимов работы канального и физического уровней (дуплексный и полудуплексный режим соответственно), буферизацию кадров и т. д.

Уровень LLC использует три разные процедуры, отвечающие за качество доставки данных.

- LLC1 – без установления соединения и без подтверждения доставки. Данная процедура управления каналом позволяет передавать данные с максимальной скоростью, для чего используются датаграммы.
- LLC2 – с установлением соединения и подтверждением доставки. Этот вид управления каналом наиболее надежный. Он позволяет гарантированно доставлять данные и получать подтверждения о доставке. На этом уровне работает система контроля ошибок, которая дает возможность восстанавливать поврежденные блоки данных и упорядочивать их последовательность. Подобная система функционирует благодаря нумерации кадров, что позволяет запрашивать ошибочные кадры и упорядочивать их.
- LLC3 – без установления соединения, но с подтверждением доставки. Данный тип управления каналом достаточно специфичен и часто используется в процессах, которые требуют быстрой передачи данных, но с подтверждением доставки. Как правило, это необходимо для разного рода процессов, происходящих в режиме реального времени, когда временные затраты очень критичны. В этом случае передача следующего кадра осуществляется только после подтверждения доставки предыдущего.

Таким образом, LLC-уровень может передавать данные либо с помощью датаграмм, либо с использованием одной из процедур, уровень качества доставки которой позволяет достичь необходимого компромисса между качеством и скоростью передачи данных.

Канальный уровень может реализовываться как на аппаратном уровне, например с помощью коммутаторов, так и с применением программного обеспечения, допустим, драйвера сетевого адаптера.

Сетевой уровень

Сетевой уровень (Network Layer) – один из важнейших уровней модели взаимодействия открытых систем. Поскольку для построения сети могут использоваться различные технологии, а то и вовсе сеть может состоять из нескольких сегментов с абсолютно разными сетевыми топологиями, чтобы «подружить» эти сегменты, требуется специальный механизм. В качестве такого механизма и выступает сетевой уровень.

Кроме определения физических адресов всех участников сети, данный уровень отвечает за нахождение кратчайших путей доставки данных, то есть умеет выполнять маршрутизацию пакетов. При этом постоянно отслеживается состояние сети и определяются новые маршруты, если возникают «заторы» на пути следования данных. Благодаря маршрутизации данные всегда доставляются с максимальной скоростью.

Сетевой уровень для доставки данных между разными сетевыми сегментами использует

особую адресацию. Так, вместо MAC-адресов применяется пара чисел – номер сети и номер компьютера в этой сети. Использование нумерации позволяет составить точную карту сети независимо от топологии сегментов и определить альтернативные пути передачи данных.

На практике функции сетевого уровня выполняет маршрутизатор.

Транспортный уровень

Транспортный уровень (Transport Layer) служит для организации гарантированной доставки данных, для чего используется уже подготовленный канал связи. При этом отслеживается правильная последовательность передачи и приема пакетов, восстанавливаются потерянные или отсеиваются дублирующие. При необходимости данные фрагментируются (разбиваются на более мелкие пакеты) или дефрагментируются (объединяются в большой пакет), что повышает надежность скорость доставки данных.

На транспортном уровне предусмотрено пять классов сервиса с различными уровнями надежности. Они различаются скоростью, возможностями восстановления данных и т. п. Например, некоторые классы работают без предварительной установки связи и не гарантируют доставку пакетов в правильной их последовательности. В этом случае за выбор маршрута отвечают промежуточные устройства, которые попадаются на пути следования данных. Классы с установкой связи начинают свою работу с установки маршрута и только после того, как маршрут будет определен, начинают последовательную передачу данных.

Благодаря такому подходу всегда можно найти компромисс между скоростью и качеством доставки данных.

Сеансовый уровень

Сеансовый уровень (Session Layer) используется для создания и управления сеансом связи на время, необходимое для передачи данных. Время сеанса зависит лишь от объема информации, которая должна быть передана. Поскольку этот объем может быть существенным, используются разные механизмы, позволяющие контролировать данный процесс.

Для управления сеансом применяется маркер, обладатель которого гарантирует себе право на связь. Кроме того, используются служебные сообщения, с помощью которых, например, стороны могут договариваться о способе передачи данных или сообщать о завершении передачи данных и освобождении маркера.

Чтобы передача данных была успешной, создаются специальные контрольные точки, которые позволяют начать повторную передачу данных практически с того места, на котором произошел непредвиденный обрыв связи. В данном случае работают также механизмы синхронизации данных, определяются права на передачу данных, поддерживается связь в периоды неактивности и т. п.

Уровень представления данных

Уровень представления данных, или представительский уровень (Representation Layer), является своего рода проходным уровнем, основная задача которого – кодирование и декодирование информации в представление, понятное вышестоящему и нижестоящему уровню. С его помощью обеспечивается совместимость компьютерных систем, использующих разные способы представления данных.

Этот уровень удобен тем, что именно на этом этапе выгодно использовать разные алгоритмы сжатия и шифрования данных, преобразование форматов данных, обрабатывать структуры данных, преобразовывать их в битовые потоки и т. д.

Прикладной уровень

Прикладной уровень (Application Layer) – последний «бастион» между пользователем и сетью. Он поддерживает связь пользовательских приложений, то есть программ, с сетевыми сервисами и службами на всех уровнях модели ISO/OSI, обеспечивает передачу служебной информации, синхронизирует взаимодействие прикладных процессов и т. д.

Глава 6
Протоколы передачи данных

Понятие протокола

В предыдущей главе мы познакомились с эталонной моделью, описывающей принцип и правила подготовки, приема и передачи данных через любой канал связи. Каждый из ее семи уровней для выполнения своих функций в подготовке или обработке данных использует стандартные процедуры межуровневого обмена информацией и протоколы передачи данных. Поэтому получается, что модель ISO/OSI является теоретической основой функционирования сети, а сетевые протоколы – это то, что превращает теорию в практику.

Протокол передачи данных – это набор правил и соглашений, которые описывают способ передачи данных между объектами в сети.

Для обслуживания модели взаимодействия открытых систем используется достаточно большое количество сетевых протоколов. Многие из них специфичны и часто выполняют только одно конкретное действие, но делают это быстро и, самое главное, правильно. Существуют также более продвинутые и функциональные протоколы, которые могут совершать определенные действия, выполняя работу сразу нескольких уровней модели. Есть даже целые семейства (стеки) протоколов, которые являются составной частью протоколов с общим названием, например стеки протоколов TCP/IP или IPX/SPX.

ПРИМЕЧАНИЕ

Модель ISO/OSI разрабатывалась тогда, когда уже были разработаны многие протоколы, в частности TCP/IP. Ее главной задачей была стандартизация работы сетей. Однако, когда модель была принята окончательно, оказалось, что она имеет много недостатков. В частности, самым слабым звеном модели стал транспортный уровень. По этой причине существует достаточно много протоколов, которые выполняют работу сразу несколькихуровней, что противоречит самой модели открытых систем.

Различают низкоуровневые и высокоуровневые протоколы.

Низкоуровневые работают на самых нижних уровнях модели ISO/OSI и, как правило, имеют аппаратную реализацию, что позволяет использовать их в таких сетевых устройствах, как концентраторы, мосты, коммутаторы и т. д.

Высокоуровневые протоколы работают на верхних уровнях модели ISO/OSI и обычно реализуются программным путем. Это позволяет создавать любое количество протоколов

разного применения, делая их настолько гибкими, как того требует современная ситуация.

В табл. 6.1 приведены названия некоторых популярных протоколов и их положение в модели взаимодействия открытых систем.

Таблица 6.1.Популярные протоколы модели ISO/OSI

Уровни модели ISO/OSI	Протоколы передачи данных
Физический	X.25, RS-232, EIA-422, RS-485, V.21, ZyX, PEP
Канальный	Ethernet, ATM, PPP, PPTP, Frame Relay, FDDI, Token Ring, SLIP
Сетевой	IPX, IP, ARP, ICMP, DDP
Транспортный	TCP, UDP, SPX, RTCP, RDP, RUDP, RTMP, NBP, ATP
Сеансовый	RPC, SSL, WSP, NetBIOS, ZIP, ADSP
Уровень представления данных	Telnet, FTP, SMTP, SNMP, TDI, XDR, NCP
Прикладной	HTTP, FTP, DHCP, DNS, POP3, SNMP, LDAP, Gopher, SMB, IMAP

Основные протоколы

Как вы уже могли заметить, количество протоколов, обслуживающих модель взаимодействия открытых систем, достаточно велико. Принцип работы части этих протоколов, особенно низкоуровневых, не представляет особого интереса. Но принцип работы и возможности некоторых протоколов, с работой которых приходится сталкиваться каждый день (таких как TCP/IP, UDP, POP3 и т. д.), все же стоит знать.

Стеки протоколов

Выше уже упоминалось, что за организацию работы всех уровней модели ISO/OSI часто отвечают стеки протоколов. Плюсом их использования является то, что все протоколы, входящие в стек, разработаны одним производителем, а значит, они способны работать максимально быстро и эффективно.

За время существования сетей было разработано несколько таких стеков протоколов, среди которых наиболее популярными являются TCP/IP, IPX/SPX, NetBIOS/SMB, Novell NetWare, DECnet и др.

В состав стеков включены протоколы, работающие на разных уровнях модели ISO/OSI, однако обычно выделяют только три типа протоколов: транспортный, сетевой и прикладной.

Преимущество использования стеков протоколов заключается в том, что протоколы, работающие на нижних уровнях, применяют стандартные и давно отлаженные сетевые протоколы, такие как Ethernet, FDDI и т. д. Эти протоколы аппаратно реализованы, поэтому возможно использовать одно и то же оборудование для разных типов сетей и тем самым достигать их совместимости на аппаратном уровне. Что касается высокоуровневых протоколов, то каждый из стеков имеет свои преимущества и недостатки. Часто случается и так, что нет жесткой привязки «один протокол – один уровень», то есть один протокол может работать сразу на двух-трех уровнях.

Привязка

Важным моментом в функционировании сетевого оборудования, в частности сетевого адаптера, является привязка протоколов. На практике она позволяет использовать разные стеки протоколов при обслуживании одного сетевого адаптера. Например, можно одновременно использовать стеки TCP/IP и IPX/SPX: если при попытке установления связи с адресатом с помощью первого стека произошла ошибка, то автоматически происходит переключение на протокол из следующего стека. В этом случае важна очередность привязки, поскольку она влияет на использование того или иного протокола из разных стеков.

Вне зависимости от того, какое количество сетевых адаптеров установлено в компьютере, привязка может осуществляться как по принципу «один к нескольким», так и по принципу «несколько к одному», то есть один стек протоколов может обслуживать сразу несколько сетевых адаптеров или несколько стеков – работу одного адаптера.

TCP/IP

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol) на сегодня является наиболее распространенным и универсальным. Он работает в локальных сетях любых масштабов. Кроме того, это единственный из протоколов, который позволяет работать в глобальной сети Интернет.

Протокол был создан в далеких 70-х годах прошлого века управлением Министерства обороны США. Именно с его подачи началась разработка универсального протокола, который позволил бы соединить любые два компьютера, как бы далеко друг от друга они ни находились. Конечно, они преследовали собственную цель – обеспечить постоянную связь с центром управления, даже если все вокруг будет разрушено в результате военных действий. Так была образована глобальная сеть ARPAnet, которую министерство активно использовало в своих целях.

Толчком к дальнейшему усовершенствованию и широкому распространению стека TCP/IP стал тот факт, что его поддержка была реализована в компьютерах с операционной системой UNIX. В результате популярность TCP/IP возросла.

В данный стек входит достаточно много протоколов, работающих на различных уровнях, но свое название он получил благодаря двум из них – TCP и IP.

TCP (Transmission Control Protocol) – транспортный протокол, предназначенный для управлением передачей данных в сетях, использующих стек TCP/IP. IP (Internet Protocol) – протокол сетевого уровня, предназначенный для доставки данных в составной сети с использованием одного из транспортных протоколов, например TCP или UDP.

Нижний уровень стека TCP/IP использует стандартные протоколы передачи данных, что делает возможным его применение в сетях с использованием любых сетевых технологий и на компьютерах с любой операционной системой.

Изначально протокол TCP/IP разрабатывался для применения в глобальных сетях, именно поэтому он является максимально гибким. В частности, благодаря способности «дробления» пакетов данные доходят до адресата вне зависимости от качества канала связи. Кроме того, благодаря наличию IP-протокола становится возможной передача данных между сегментами сети с разной топологией и способом передачи данных.

Недостатком TCP/IP-протокола является сложность администрирования сети. Для нормального функционирования сети требуется наличие дополнительных серверов, например DNS, DHCP и т. д., поддержание работы которых и занимает большую часть времени системного администратора. Тем не менее, как говорится, результат налицо.

IPX/SPX

Стек протоколов IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) является разработкой и собственностью компании Novell. Он был разработан для нужд операционной системы Novell NetWare, которая еще недавно занимала одну из лидирующих позиций среди серверных операционных систем.

Протоколы IPX и SPX работают на сетевом и транспортном уровнях модели ISO/OSI соответственно, поэтому отлично дополняют друг друга. Протокол IPX может передавать данные с помощью датаграмм, используя для этого информацию о маршрутизации в сети. Однако для того, чтобы передать данные по найденному маршруту, необходимо сначала установить соединение между отправителем и получателем. Этим и занимается протокол SPX или любой другой транспортный протокол, работающий в паре с IPX.

К сожалению, стек протоколов IPX/SPX изначально ориентирован на обслуживание сетей с небольшим количеством компьютеров, поэтому его использование в больших сетях, особенно на низкоскоростных линиях связи, крайне неэффективно.

NetBIOS/SMB

Достаточно популярный стек протоколов, разработкой которого занимались компании IBM и Microsoft соответственно, ориентированный на использование в продуктах этих компаний. Как и у TCP/IP, на физическом и канальном уровне стека NetBIOS/SMB работают стандартные протоколы, такие как Ethernet, Token Ring и др., что делает возможным его использование в паре с любым активным сетевым оборудованием. На верхних же уровнях работают протоколы NetBIOS (Network Basic Input/Output System) и SMB (Server Message Block).

Протокол NetBIOS был разработан в середине 80-х годов прошлого века, но вскоре был заменен на более функциональный протокол NetBEUI (NetBIOS Extended User Interface), позволяющий организовать очень эффективный обмен информацией в сетях, состоящих не более чем из 200 компьютеров.

Для обмена данными между компьютерами используются логические имена, присваиваемые компьютерам динамически при их подключении к сети. При этом таблица имен распространяется на каждый компьютер сети. Поддерживается также работа с групповыми именами, что позволяет передавать данные сразу нескольким компьютерам.

Главные плюсы протокола NetBEUI – скорость работы и очень скромные требования к ресурсам. Если требуется организовать быстрый обмен данными в небольшой сети, состоящей из одного сегмента, – лучшего протокола не найти. Кроме того, для доставки сообщений соединение не обязательно должно быть установлено: в случае отсутствия соединения протокол использует датаграммный метод, когда сообщение снабжается адресом получателя и отправителя и «пускается в путь», переходя от одного компьютера к другому.

Однако NetBEUI обладает и существенным недостатком: он полностью лишен понятия о маршрутизации пакетов, поэтому его использование в сложных составных сетях не имеет смысла.

Что касается протокола SMB (Server Message Block), то с его помощью организуется работа сети на трех высших уровнях – сеансовом, уровне представления и прикладном уровне. Именно при его использовании становится возможным доступ к файлам, принтерам и другим ресурсам сети. Данный протокол несколько раз совершенствовался (вышло три его версии), что позволило применять его даже в таких современных операционных системах, как Microsoft Windows Vista и Windows 7. Кроме того, протокол SMB универсален и может работать в паре практически с любым транспортным

протоколом, например TCP и SPX.

HTTP

Пожалуй, самый востребованный из протоколов, с которым ежедневно работают десятки миллионов пользователей Интернета по всем миру.

Протокол HTTP (HyperText Transfer Protocol) разрабатывался специально для получения и передачи данных по Интернету. Он работает по технологии «клиент – сервер», которая подразумевает, что есть клиенты, запрашивающие информацию, и есть сервер, который эти запросы обрабатывает и отсылает ответ. Примером работы данного протокола является просмотр веб-страницы в браузере: в этом случае браузер выполняет роль клиента, а компьютер, на котором находится вебстраница, – роль сервера.

HTTP работает на уровне приложений. Это означает, что данный протокол должен пользоваться услугами транспортного протокола, в качестве которого по умолчанию выступает протокол TCP.

Первая версия протокола HTTP была разработана еще в начале 90-х годов прошлого века и на то время полностью удовлетворяла пользователей своими возможностями. Но со временем, когда в Интернет пришла графика и динамика, возможностей протокола перестало хватать и он постепенно начал изменяться в лучшую сторону.

В своей работе протокол использует понятие URI (Uniform Resource Identifier) – уникального идентификатора ресурса, в качестве которого обычно выступает адрес веб-страницы, файла или любого другого логического объекта. При этом URI поддерживает работу с параметрами, что позволяет расширять функциональность протокола. Так, используя параметры, можно указать, в каком формате и кодировке вы хотите получить ответ от сервера. Это в свою очередь позволяет передавать с помощью HTTP не только текстовые документы, но и любые двоичные данные.

Основным недостатком протокола HTTP является избыточный объем текстовой информации, необходимой для того, чтобы клиент мог правильно отобразить полученный от сервера ответ. При большом объеме содержимого веб-страницы это может создавать излишне большой трафик, что уменьшает скорость отображения полезного содержимого. Кроме того, протокол полностью лишен каких-либо механизмов сохранения состояния, что делает невозможной навигацию по веб-страницам посредством одного лишь HTTP-протокола. Для устранения этого неудобства можно использовать вместе с HTTP сторонние протоколы или же работать с браузером, имеющим продвинутые методы обработки HTTP-запросов.

FTP

Протокол FTP (File Transfer Protocol) является «родным братом» протокола HTTP, только в отличие от последнего он работает не с текстовыми или двоичными данными, а с файлами.

Этот протокол – один из старейших: он появился еще в начале 70-х годов прошлого века. Как и HTTP, он работает на прикладном уровне и в качестве транспортного протокола использует TCP-протокол. Его основная задача – передача файлов между FTP-сервером и клиентским приложением.

FTP-протокол представляет собой набор команд, которые описывают правила подключения и обмена данными. При этом команды и непосредственно данные передаются с использованием различных портов. В качестве стандартных портов используются порты 21 и 20: первый – для передачи данных, второй – для передачи команд. Кроме того, порты могут выбираться динамически, что делает этот протокол

очень универсальным.

Размер файлов, передаваемых с помощью FTP-протокола, не лимитируется. Предусмотрен также механизм докачки файла, если в процессе передачи произошел обрыв связи.

Главным недостатком FTP-протокола является отсутствие механизмов шифрования данных, что делает возможным перехват и анализ трафика с дальнейшим определением данных авторизации пользователя на FTP-сервере. Чтобы избежать перехвата столь важных данных, параллельно используется протокол SSL, с помощью которого данные шифруются.

POP3 и SMTP

Использование электронной почты для обмена сообщениями уже давно является альтернативой обычной почте. Электронная почта гораздо эффективнее и, что самое главное, быстрее. Ее использование стало возможным благодаря протоколам POP3 (Post Office Protocol Version 3) и SMTP (Simple Mail Transfer Protocol).

Протокол POP3 работает на прикладном уровне и применяется для получения электронных сообщений из почтового ящика на почтовом сервере. При этом он использует один из портов и транспортный протокол TCP.

Сеанс связи с почтовым сервером разбит на три этапа: авторизация, транзакция и обновление. Авторизация пользователя происходит при соединении с почтовым сервером, для чего может использоваться любой почтовый клиент, поддерживающий работу с протоколом POP3. На этапе транзакции клиент запрашивает у сервера выполнение необходимого действия, например получения информации о количестве сообщений, получения самих сообщений либо их удаления. Процесс обновления предназначен для выполнения запроса клиента. После окончания обновления сеанс связи завершается до поступления следующего запроса на соединение.

При прохождении этапа авторизации может использоваться любой из существующих протоколов шифрования, например SSL или TLS, что делает процесс получения электронной корреспонденции более защищенным.

Протокол POP3 позволяет только получать электронные сообщения, а для их отправки приходится использовать другой протокол, в качестве которого чаще всего выступаеет SMTP, точнее, его усовершенствованная версия – ESMTP (Extended SMTP).

Как и POP3, протокол SMTP работает на прикладном уровне, поэтому ему необходимы услуги транспортного протокола, в роли которого выступает протокол TCP. При этом отправка электронных сообщений также происходит с использованием одного из портов, например 25-го.

IMAP

IMAP (Interactive Mail Access Protocol) – еще один почтовый протокол, созданный на основе протокола POP3. В новом протоколе были учтены все недостатки и добавлено большое количество новых востребованных функций.

Наиболее полезной среди них является возможность частичного скачивания сообщений, анализируя содержимое которых можно эффективно настраивать фильтры, сортирующие письма или отсеивающие спам.

Еще одна немаловажная функция – механизм оптимизации использования каналов, по которым передаются сообщения. Поскольку практически всегда скорость каналов оставляет желать лучшего, наличие такой функции существенно облегчает жизнь пользователя. Имеется также возможность передачи сообщений небольшими частями, что

очень удобно, когда размер письма большой, например 5-10 Мбайт.

SLIP

Протокол передачи данных SLIP (Serial Line Internet Protocol) создан специально для организации постоянного подключения к Интернету с использованием имеющейся телефонной линии и обычного модема. Из-за высокой стоимости этот тип подключения могут позволить себе немногие пользователи. Как правило, такое подключение создается в организациях, имеющих сервер, на котором находится веб-страница организации и другие ресурсы (база данных, файлы).

Данный протокол работает вместе с протоколом TCP/IP и находится на более низком уровне. Перед тем как информация с модема поступит на обработку TCP/IP-протоколу, ее предварительно обрабатывает SLIP-протокол. Выполнив все необходимые действия, он создает другой пакет и передает его TCP/IP.

PPP

Протокол PPP (Point-to-Point Protocol) выполняет ту же работу, что и описанный выше SLIP. Однако он лучше осуществляет эти функции, так как обладает дополнительными возможностями. Кроме того, в отличие от SLIP, PPP может взаимодействовать не только с TCP/IP, но и с протоколами IPX/SPX, NetBIOS, DHCP, которые широко используются в локальных сетях.

Протокол PPP более распространен также благодаря использованию его на интернет-серверах с установленной серверной операционной системой семейства Windows NT (SLIP применяют для соединения с серверами, работающими в операционной системе UNIX).

Frame Relay

Frame Relay – еще один протокол, предназначенный для передачи данных по телефонной линии. Помимо высокой надежности он обладает расширенной функциональностью. Так, поскольку передаваемые данные часто имеют формат видео, аудио или содержат электронную информацию, есть возможность выбора приоритетности передаваемого содержимого.

Еще одна особенность протокола Frame Relay – его скорость, которая достигает 45 Мбит/с.

AppleTalk

Стек протоколов AppleTalk является собственностью компании Apple Computer. Он был разработан для установки связи между компьютерами Macintosh.

Как и TCP/IP, AppleTalk представляет собой набор протоколов, каждый из которых отвечает за работу определенного уровня модели ISO/OSI.

В отличие от протоколов TCP/IP и IPX/SPX, стек протоколов AppleTalk использует собственную реализацию физического и канального уровней, а не протоколы модели ISO/OSI.

Рассмотрим некоторые протоколы стека AppleTalk.

▪ DDP (Datagram Delivery Protocol) – отвечает за работу сетевого уровня. Его основное

предназначение – организация и обслуживание процесса передачи данных без предварительной установки связи между компьютерами.

▪ RTMP (Routing Table Maintenance Protocol) – работает с маршрутными таблицами AppleTalk. Любая такая таблица содержит информацию о каждом сегменте, куда возможна доставка сообщений. Таблица состоит из номеров маршрутизаторов (порта), которые могут доставить сообщение к выбранному компьютеру, количества маршрутизаторов, параметров выбранных сегментов сети (скорости, загруженности и т. п.).

▪ NBP (Name Binding Protocol) – отвечает за адресацию, которая сводится к привязке логического имени компьютера к физическому адресу в сети. Кроме процесса привязки имени, он отвечает за регистрацию, подтверждение, стирание и поиск этого имени.

▪ ZIP (Zone Information Protocol) – работает в паре с протоколом NBP, помогая ему производить поиск имени в рабочих группах, или зонах. Для этого он использует информацию ближайшего маршрутизатора, который создает запрос по всей сети, где могут находиться входящие в заданную рабочую группу компьютеры.

▪ ATP (AppleTalk Transaction Protocol) – один из протоколов транспортного уровня, который отвечает за транзакции. Транзакция — это набор из запроса, ответа на этот запрос и идентификационного номера, который присваивается данному набору. Примером транзакции может быть сообщение о доставке данных от одного компьютера другому. Кроме того, ATP умеет делать разбивку больших пакетов на более мелкие с последующей их сборкой после подтверждения о приеме или доставке.

▪ ADSP (AppleTalk Data Stream Protocol) – протокол, аналогичный ATP. Он отвечает за доставку пакетов. Однако в данном случае осуществляется не одна транзакция, а гарантированная доставка, которая может повлечь за собой несколько транзакций. Кроме того, протокол гарантирует, что данные при доставке не будут утеряны или продублированы.

Глава 7
Варианты среды передачи данных

Ключевым моментом в функционировании локальной сети является среда передачи данных, то есть канал, по которому компьютеры могут обмениваться информацией. От среды передачи данных зависят многие параметры сети, в частности:

▪ топология сети;
▪ используемое оборудование;
▪ стоимость создания;
▪ физическая надежность;
▪ скорость передачи данных;
▪ безопасность сети;
▪ возможности администрирования сети;
▪ возможность модернизации.

Этот список можно продолжить, но ясно одно: среда передачи данных однозначно определяет как возможности сети, так и возможности ее модернизации. В данной главе мы рассмотрим основные использующиеся в настоящее время среды передачи данных.

Коаксиальный кабель

Первой средой для объединения компьютеров в сеть с целью обмена информацией был коаксиальный кабель (Coaxial Cable). Сети с использованием коаксиального кабеля появились еще в начале 70-х годов прошлого века. На то время он считался идеальным вариантом для передачи данных. Скорости тогда были не столь высоки, как сегодня, и коаксиальный кабель полностью удовлетворял существующие потребности. Сетевое оборудование для работы с коаксиальным кабелем, согласно существующим сетевым стандартам, позволяет передавать данные со скоростью до 10 Мбит/с, что даже сегодня в некоторых случаях является вполне достаточной скоростью.

Различают тонкий и толстый коаксиальные кабели. Несмотря на то что толстый коаксиальный кабель появился раньше, его технические характеристики (скорость, дальность связи и т. п.) существенно лучше, нежели у тонкого коаксиального кабеля, который появился после дальнейшего усовершенствования проводных сетевых стандартов.

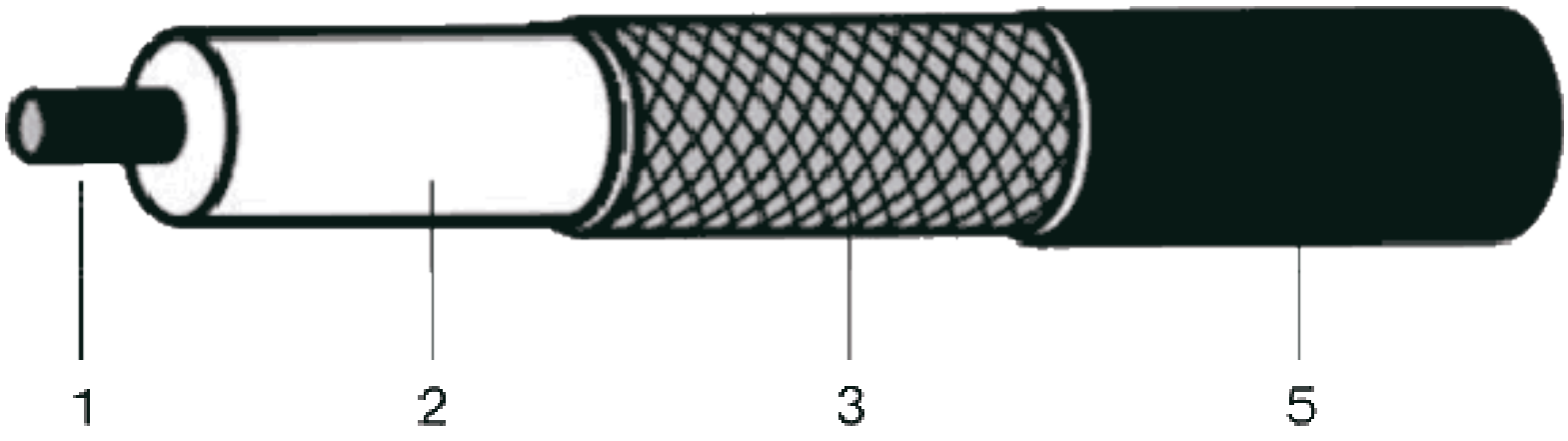
Толстый и тонкий кабели внешне различаются только толщиной, хотя иногда могут быть и другие различия (рис. 7.1).

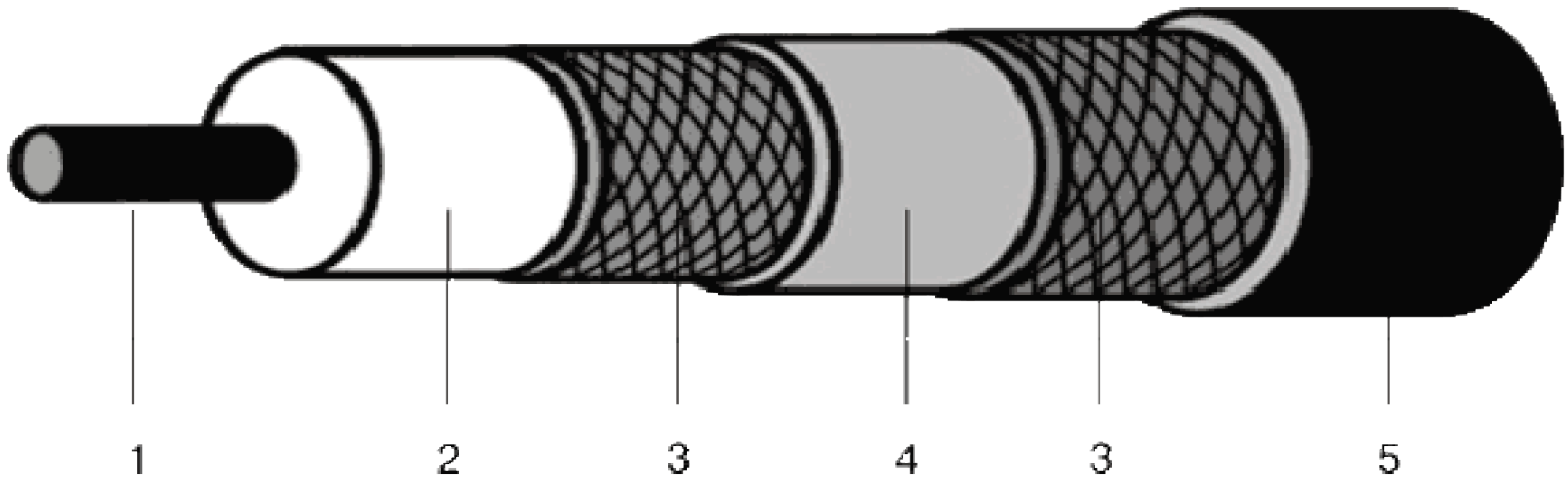
Например, когда требуется прокладка кабеля снаружи здания, часто используется кабель с усилительным тросом, который выглядит как отдельная жила в отдельной оболочке.

Однако основные различия между этими типами кабелей заключаются в их строении:

могут присутствовать дополнительные оплетки, диэлектрики, экраны из фольги и т. д.

Типичное строение самой простой реализации тонкого и толстого коаксиального кабеля показано на рис. 7.2 и 7.3.





Рассмотрим элементы коаксиального кабеля, показанные на рисунке.

1. Центральный проводник (Center Conductor). Представляет собой металлический стержень, цельный или состоящий из нескольких проводников. В качестве металла, как правило, выступает медь или сплав с медью, например сплав меди с карбоном, омедненная сталь или омедненный алюминий. Толщина проводника обычно находится в пределах 1–2 мм.

2. Диэлектрик (Dielectric). Служит для надежного разделения и изолирования центрального проводника и оплетки, которая используется для передачи сигнала. Диэлектрик может изготавливаться из различных материалов, например из полиэтилена, фторопласта, пенополиуретана, поливинилхлорида, тефлона и т. д.

3. Оплетка (Braid). Является одним из носителей, который участвует в передаче сигнала. Кроме того, она играет роль заземления и защитного экрана от электромагнитных шумов и наводок. Как правило, оплетка сделана из медной или алюминиевой проволоки. Когда требуется увеличить помехозащищенность системы, может использоваться кабель с двойной и даже четверной оплеткой.

4. Изолирующая пленка (Foil). Выступает обычно в роли дополнительного экрана. В качестве материала используется алюминиевая фольга.

5. Внешняя оболочка (Outer Jacket). Используется для защиты кабеля от воздействия внешней среды. Оболочка, как правило, имеет ультрафиолетовую защиту и защиту от возгорания, для чего используется материал с соответствующими свойствами, например поливинилхлорид, пластик, резина и т. д.

Волновое сопротивление коаксиального кабеля, используемого для передачи данных в локальных сетях, составляет 50 Ом. При этом толщина тонкого коаксиального кабеля – примерно 0,5–0,6 см, а толстого – 1–1,3 см.

Существует определенная маркировка (категория) кабелей, которая позволяет различать их характеристики. Например, кабель с волновым сопротивлением 50 Ом имеет маркировку R-8 [1 - RG (от англ. Radio Grade) – волновод.], RG-11 и RG-58. Различают также подкатегории кабелей, например RG-58/U (одножильный проводник) или RG-58A/U (многожильный проводник).

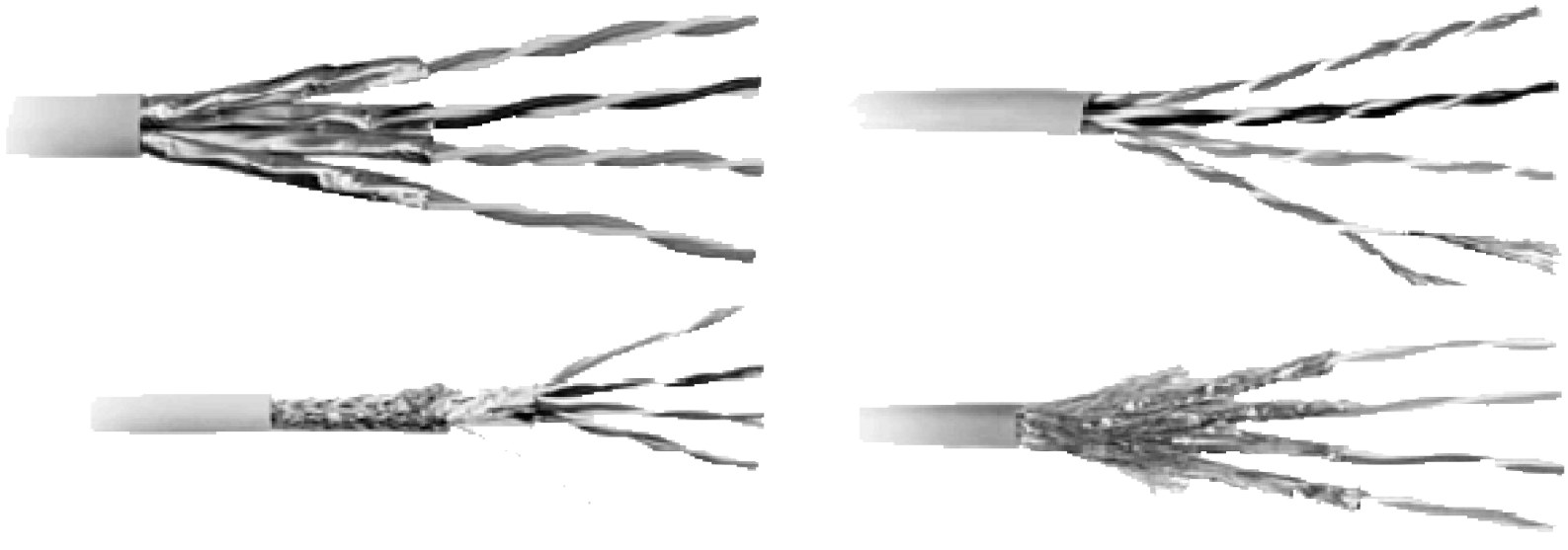
Наибольшее распространение получил тонкий коаксиальный кабель, поскольку он более гибкий и его легче прокладывать. Тем не менее, если требуется увеличить длину центральной кабельной магистрали, то используется толстый коаксиальный кабель. Иногда тонкий и толстый кабели применяются одновременно: тонким кабелем соединяют близкорасположенные компьютеры, а толстым – компьютеры на большом удалении или разные сегменты сети.

Кабель «витая пара»

На сегодняшний день кабель «витая пара» (Twisted Pair) получил наибольшее распространение благодаря своим скоростным характеристикам и удобству прокладки. Его появление было вполне прогнозируемым, поскольку использование коаксиального кабеля накладывает ограничение на топологию сети, что в свою очередь отражается на скорости передачи данных и, самое главное, возможности ее модернизации, то есть использования более современного сетевого стандарта.

Свое название он получил благодаря особенности внутреннего исполнения: внутри кабеля может находиться от одной до двадцати пяти пар проводников, скрученных между собой и имеющих определенную цветовую раскраску.

Внешний вид кабеля «витая пара» зависит от того, какое количество проводников находится внутри него, какого типа оплетки используются для экранирования кабеля и пар, а также от наличия дополнительного заземляющего проводника (рис. 7.4).



Различают экранированный (Shielded) и неэкранированный (Unshielded) кабели. Кроме того, существует много различных вариантов исполнения кабеля, среди которых наибольшее распространение получили UTP (Unshielded Twisted Pair, неэкранированная витая пара), F/UTP (Foiled Unshielded Twisted Pair, фольгированная неэкранированная витая пара), STP (Shielded Twisted Pair, экранированная витая пара), S/FTP (Screened Foiled Twisted Pair, фольгированная экранированная витая пара), SF/UTP (Screened Foiled Unshielded Twisted Pair, фольгированная неэкранированная витая пара) и др. Есть также несколько вариантов кабеля с многожильными проводниками.

Кабели различают и по категориям: чем выше категория, тем лучшими характеристиками (в том числе и скоростными) обладает кабель. В настоящее время существует семь категорий кабеля «витая пара», используемых для организации работы локальной сети. Например, кабель пятой категории позволяет передавать данные со скоростью 100 Мбит/с, а кабель шестой категории и выше обеспечивает скорость передачи данных не менее 1 Гбит/с. Кабель же седьмой категории теоретически способен передавать данные со скоростью 100 Гбит/с.

Кабель «витая пара» является самым популярным способом подключения компьютеров в домашних сетях. Стоимость кабеля достаточно низкая, а скорость передачи данных при этом находится на очень высоком уровне. Длины сегмента кабеля в 100 м хватает, чтобы подключить компьютер в квартире, просто свесив кабель с крыши и подведя его к окну. Именно такой способ подключения является самым простым и распространенным в домашних сетях.

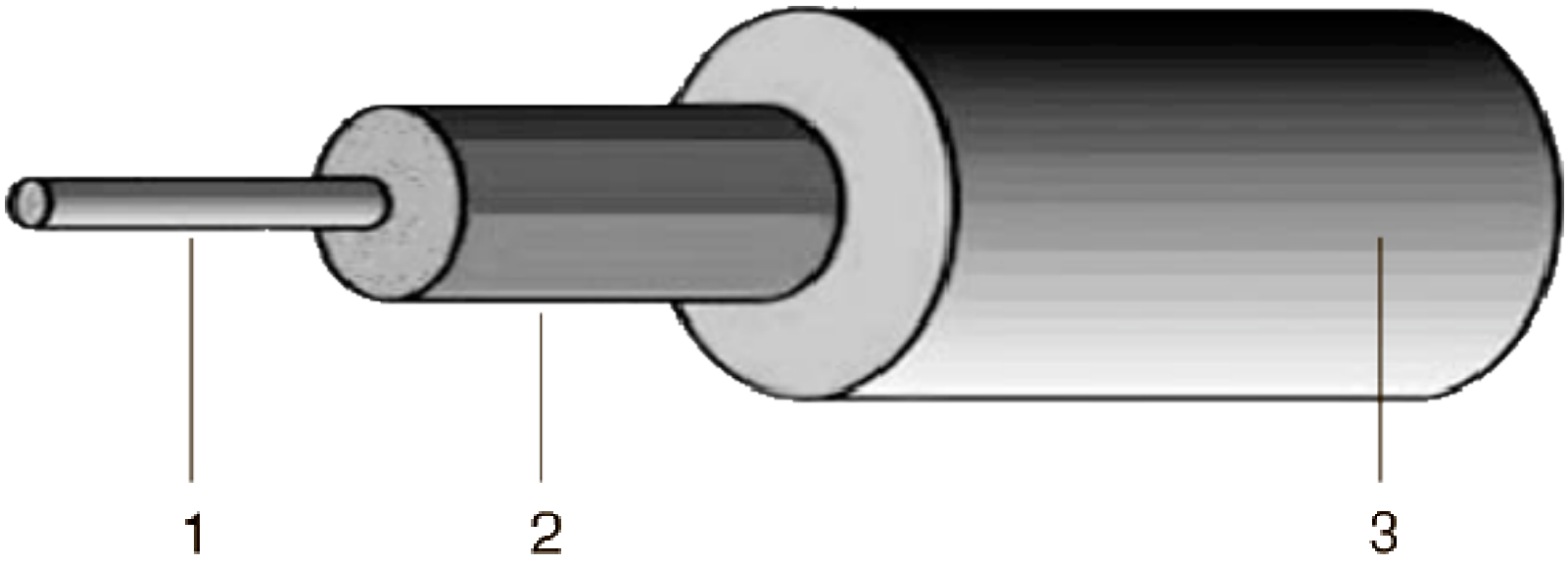
Оптоволоконный кабель

Еще один вариант кабеля для передачи данных в сетях – оптоволоконный (Fiber Optic). Благодаря своим характеристикам именно оптоволоконный кабель имеет наибольшие шансы остаться в лидерах.

Его главным отличием от существующих вариантов кабеля является способ передачи электрических сигналов: для этого используется свет. Это означает, что оптоволоконный кабель не подвержен влиянию электромеханических наводок, а сигнал ослабевает гораздо меньше. Как результат – высокая скорость передачи данных на большие расстояния.

Оптоволоконные кабели отличаются конструкцией, точнее, диаметром сердцевины, то есть самого оптоволокна. Существует два варианта оптоволокна, которые и определяют характеристики кабеля. Так, различают одномодовое (SM, Single Mode) и многомодовое, или мультимодовое (MM, Multi Mode), волокно.

Упрощенная схема оптоволоконного кабеля показана на рис. 7.5.



Основная деталь оптоволоконного кабеля – оптоволокно, или, как его еще называют, световод (1), по которому непосредственно и передается световой сигнал. Чтобы сигнал не уходил из световода, вокруг последнего располагается отражающая оболочка (2) толщиной 125 мкм и, наконец, оболочка (3), которая защищает кабель от внешних воздействий, например влаги или солнечных лучей.

Обычно оптоволоконный кабель снабжается дополнительными уровнями прочности: применяются разного рода лаковые покрытия, дополнительные оболочки (буферы), усилительные тросы и т. д. Кроме того, широкое распространение получили кабели с несколькими световодами, которые позволяют значительно увеличить пропускную способность кабеля.

Преимущества и недостатки одномодового и многомодового оптоволокна понять достаточно легко. По световоду передаются световые сигналы с длиной волны в диапазоне 0,85-1,3 мкм. Многомодовое волокно в зависимости от типа имеет толщину световода 50 или 62,5 мкм, в то время как у одномодового волокна данный показатель составляет примерно 7–9 мкм. Если представить себе, как будет распространяться свет в подобных «коридорах», то становится ясно, что чем уже «коридор», тем меньше отражений будет испытывать данный сигнал, а значит, меньшими будут искажения и затухание сигнала. Конечно, такое теоретическое изложение принципа распространения сигнала в кабеле далеко от идеального, но и его вполне достаточно, чтобы сделать однозначный вывод: одномодовый кабель гораздо практичнее и лучше. Об этом же свидетельствует практика: скорость передачи сигнала в простейшем одномодовом кабеле может достигать 2,5 Гбит/с при длине сегмента 20 и более километров.

К сожалению, распространению оптоволоконного кабеля мешают некоторые факторы, основными из которых являются дороговизна кабеля и обслуживающей его аппаратуры, а также необходимость в соответствующей подготовке при работе с кабелем.

Телефонная проводка

Телефонный кабель, а точнее, телефонная линия, уже давно используется, например, для подключения удаленного компьютера к существующей сети, другому компьютеру или Интернету. Для этого существует достаточно большое количество протоколов и технологий, например Frame Relay, ADSL и т. д.

Не так давно появилась технология, которая дает возможность использовать существующую аналоговую или цифровую телефонную линию для объединения компьютеров в локальную сеть. Речь идет о стандартах HomePNA, оборудование которых позволяет объединить в локальную сеть достаточно большое количество компьютеров и обеспечить при этом хорошую скорость передачи данных.

Плюсы такой сети очевидны: низкая стоимость создания, применение уже существующего канала связи, возможность развертывания сети там, где другой способ связи по разным причинам невозможен.

Телефонная линия часто используется для подключения компьютеров к домашней локальной сети. В этом случае к щитку на лестничной площадке или в любое другое удобное место подводится кабель «витая пара» и устанавливается специальный конвертер с Ethernet на HomePNA, соединяющий «витую пару» с телефонным кабелем, заходящим в квартиру. В результате разводка квартиры превращается в отдельную локальную сеть, подключение к которой осуществляется с помощью адаптеров HomePNA.

Электропроводка

Идеи использования электропроводки в качестве канала связи для передачи данных существовали уже достаточно давно. Причина очень проста: электрическим кабелем буквально опутаны все места обитания человека, поэтому вполне логично было бы использовать его для решения еще одной задачи. Однако воплотить эту мечту в жизнь мешал недостаток знаний и соответствующих технологий.

Все изменилось с того момента, когда десять лет назад была создана организация HomePlug Powerline Alliance. Ее стараниями на свет появился первый стандарт HomePlug, который и позволил осуществить мечту. Конечно, он не может составить серьезную конкуренцию другим способам связи, но в случае, когда никакой другой способ создания локальной сети не подходит, это возможный выход из ситуации.

Удобно то, что для использования электрического кабеля в качестве среды передачи данных он не обязательно должен быть однородным! Именно так: передача данных будет возможна даже в случае, когда электрический кабель представляет собой скрутку кабелей из разных материалов различного сечения и разной длины.

Поскольку электропроводка для своих прямых целей применяет диапазон частот 50–60 Гц, то для передачи данных используется другая частота, которая не является помехой для работы электрических устройств, а именно диапазон частот 4-20 МГц.

Радиоволны

Пожалуй, самая интересная и перспективная среда передачи данных – это радиоволны. Возможности этой среды практически неограниченны, о чем свидетельствует множество разнообразнейших способов ее использования: спутниковое телевидение, радиовещание, мобильная связь и многое другое. Тяжело даже представить себе, сколько различных радиоволн окружают нас!

Использование радиоволн в качестве среды передачи данных в локальных сетях практикуется уже очень давно и, что самое главное, очень успешно.

Существует достаточно много беспроводных технологий, которые позволяют это сделать, например Wi-Fi, WiMAX, Bluetooth и т. д. Каждая из них имеет свои особенности

и ограничения, но тем не менее отлично справляется с поставленной перед ними задачей.

Любая технология передачи данных использует определенный диапазон радиочастот, который строго регламентирован стандартами. Существуют даже государственные структуры по контролю над применением этих частот. Например, беспроводная сеть, построенная по стандарту IEEE 802.11 (Wi-Fi), использует в своей работе диапазон частот 2400–2483,5 МГц, а беспроводная сеть стандарта WiMAX – диапазон частот 2300–2400 МГц.

Популярность беспроводных сетей обусловлена одним очень серьезным преимуществом – мобильностью клиентов: никакая другая среда передачи данных не может похвастаться такими возможностями. Однако беспроводные сети более чувствительны к разного рода препятствиям и помехам распространению сигнала, что часто становится серьезным ограничением в их использовании.

Применение «радиоэфира» достаточно часто практикуется для подключения компьютеров к домашней локальной сети. Существуют даже домашние сети, которые подразумевают только такой способ подключения.

Однако есть и существенный недостаток использования беспроводного оборудования, особенно в условиях открытого пространства, то есть на улице. Как показала практика, беспроводное оборудование, а точнее, беспроводные точки доступа, очень чувствительно к грозам и молниям, которые часто выводят оборудование из строя, даже несмотря на наличие грозозащиты. Именно поэтому зачастую все же выбирают проводное соединение компьютеров, пусть даже и более дорогое.

Инфракрасное излучение

Инфракрасное излучение используется в качестве среды передачи данных уже достаточно давно. Эту среду можно сравнить со средой радиоволн, поскольку они обе используют невидимые глазу волны, только работают по-разному.

Данная технология развивалась достаточно быстро, поскольку ее перспективы были очевидны. Это же подтверждала и скорость передачи данных, теоретический показатель которой доходил до 100 Мбит/с. Однако зависимость распространения сигнала от наличия препятствий ограничивала широкое распространение этого способа связи. По этой причине свое основное применение технология передачи данных посредством инфракрасных волн нашла в устройствах удаленного управления объектами, например телевизионным приемником, магнитофоном, гаражными воротами и т. д. Тем не менее подобные технологии могут использоваться и в локальных сетях, например для соединения двух рядом расположенных компьютеров или компьютера с периферией.

Глава 8
Коротко о сетевых стандартах

Функционирование локальной сети обеспечивается разнообразными стандартами, в частности моделью взаимодействия открытых систем. Кроме того, на основе модели ISO/OSI создано множество стандартов, которые используются для передачи данных в локальной сети с достаточной по современным меркам скоростью и безопасностью.

На сегодняшний день существует достаточно много технологий построения локальной сети. Однако независимо от того, какие топологии, каналы связи и методы передачи данных используются, все они реализованы и описаны в так называемых сетевых стандартах. Таким образом, стандарт – это набор правил и соглашений, используемых при создании локальной сети и организации передачи данных с применением определенной

топологии, оборудования, протоколов и т. д.

Логично, что сами по себе эти стандарты не появляются: они – результат слаженной работы множества организаций, которые, принимая во внимание современные требования и возможности, разрабатывают все необходимые правила, использование которых в результате позволяет создать сеть с необходимыми параметрами. К числу таких организаций относятся уже упомянутая международная организация по стандартизации, международная комиссия по электротехнике (International Electrotechnical Commision, IEC), международный союз электросвязи (International Telecommunications Union, ITU), институт инженеров электротехники и радиоэлектроники (Institute of Electrical and Electronic Engineers, IEEE), ассоциация производителей компьютеров и оргтехники (Computer and Business Equipment Manufacturers Association, CBEMA), американский национальный институт стандартов (American National Standards Institute, ANSI) и др. Каждая из этих организаций проводит практические исследования и вносит в создаваемые стандарты необходимые коррективы.

Существует достаточно большое количество сетевых стандартов, касающихся абсолютно всех аспектов работы сети. Однако если разработка стандартов относится к определенному типу сети, то имеется четкое разделение на уровне комитетов. При этом в состав комитета входят организации, непосредственно связанные с разрабатываемыми стандартами, то есть те, которые действительно понимают, что они делают и что от них зависит.

Что касается локальных компьютерных сетей, то за разработку сетевых стандартов отвечает комитет 802 по стандартизации локальных сетей, который в 1980 году был сформирован под эгидой IEEE (институт инженеров электротехники и радиоэлектроники). Именно поэтому все стандарты, разрабатываемые этим комитетом, в своем названии содержат IEEE 802.

В составе комитета 802 находится большое количество подкомитетов, каждый из которых работает по своему направлению и отвечает за стандартизацию разных типов сети и создание отчетов, описывающих разные процессы, которые возникают при передаче данных. Например, за разработку стандартов для сети с кабельной системой отвечает комитет IEEE 802.3, с использованием радиоэфира – комитет IEEE 802.11 и т. д.

Наиболее известными подкомитетами являются следующие.

▪ IEEE 802.1. Данный подкомитет занимается разработкой стандартов межсетевого взаимодействия и управления сетевыми устройствами. Он разрабатывает стандарты по управлению локальной сетью, принципам и логике работы активного сетевого оборудования, безопасности протоколов MAC-уровня и т. д.

▪ IEEE 802.2. Этот подкомитет разрабатывает стандарты для протоколов канального уровня, осуществляющих логическое управление средой передачи данных.

▪ IEEE 802.3. Работа данного подкомитета представляет особый интерес в рамках данной книги, поскольку именно он занимается разработкой стандартов для проводных сетей стандарта Ethernet, которые для доступа к среде передачи данных используют метод множественного доступа с контролем несущей частоты и обнаружением коллизий CSMA/CD. Данный комитет разработал более 30 стандартов, бóльшая часть которых находит свое применение в современных локальных сетях.

▪ IEEE 802.4. Этот комитет разрабатывает стандарты для локальных сетей, которые используют маркерный метод доступа к передающей сети и топологию «шина».

▪ IEEE 802.5. Данный комитет разрабатывает правила и спецификации для локальных сетей, которые в качестве метода доступа к среде передачи данных используют метод маркера и в основе которых лежит топология «кольцо».

▪ IEEE 802.6. Стандарты данного комитета описывают принципы и правила функционирования сетей городского масштаба (MAN).

▪ IEEE 802.11. Этот комитет разрабатывает стандарты и правила функционирования устройств в беспроводных локальных сетях, которые работают с частотами 2,4, 3,6 и

5 ГГц.

▪ IEEE 802.15. Данный комитет разрабатывает стандарты для персональных беспроводных сетей, использующих такие технологии передачи данных, как ZigBee, Bluetooth и т. д.

▪ IEEE 802.16. Внимание этого комитета сосредоточено на стандартизации функционирования локальных сетей (WiMAX) с использованием беспроводной связи в широком диапазоне частот (2-66 ГГц).

Глава 9
Активное и пассивное сетевое оборудование

Локальная сеть, независимо от применяемой топологии, сетевого стандарта и типа, использует различное сетевое оборудование, которое, согласно существующим стандартам, правилам и соглашениям, может передавать и принимать данные. Тип оборудования, его технические характеристики и его количество зависят от многих факторов, основными из которых являются:

▪ топология сети;
▪ тип среды передачи данных;
▪ используемый сетевой стандарт;
▪ количество узлов в сети;
▪ потребности пользователей;
▪ уровень безопасности работы с данными.

В данной главе рассмотрим основные элементы сетевого оборудования.

Активное оборудование

Оборудование, которое непосредственно участвует в процессе передачи данных путем аппаратной обработки сигнала, называется активным. К нему относятся сетевой адаптер, концентратор, коммутатор и т. д.

Сетевой «проводной» адаптер

Сетевой адаптер, или сетевая карта, – это ключевое оборудование, которое используется в качестве посредника между компьютером и средой передачи данных. Без сетевого адаптера невозможен обмен информацией в принципе.

Сетевой адаптер вне зависимости от того, для работы в сетях какого типа он предназначен, служит для обработки данных, поступающих ему от компьютера или по каналу передачи данных. В режиме передачи он преобразовывает поступившие от компьютера данные в электрический сигнал и отправляет его по каналу, используемому для передачи данных. В режиме получения данных он выполняет обратное действие: преобразовывает электрические сигналы в двоичные данные и передает их протоколам верхнего уровня.

Главное различие сетевых адаптеров (не учитывая способ приема и передачи данных) – вариант исполнения. Существует три варианта.

▪ Плата для установки в слот расширения. Представляет собой плату, содержащую необходимую аппаратную начинку, которую можно установить в свободный слот расширения материнской платы. До появления ATX-стандарта этот вариант сетевого

адаптера был наиболее распространенным и дешевым. Так, материнская плата, даже бюджетный ее вариант, всегда имеет в своем составе свободный слот, предназначенный для установки устройства любого типа. Как правило, это слот типа PCI или PCI Express (в персональных компьютерах) или PCMCIA-слот (в ноутбуках или других переносных устройствах).

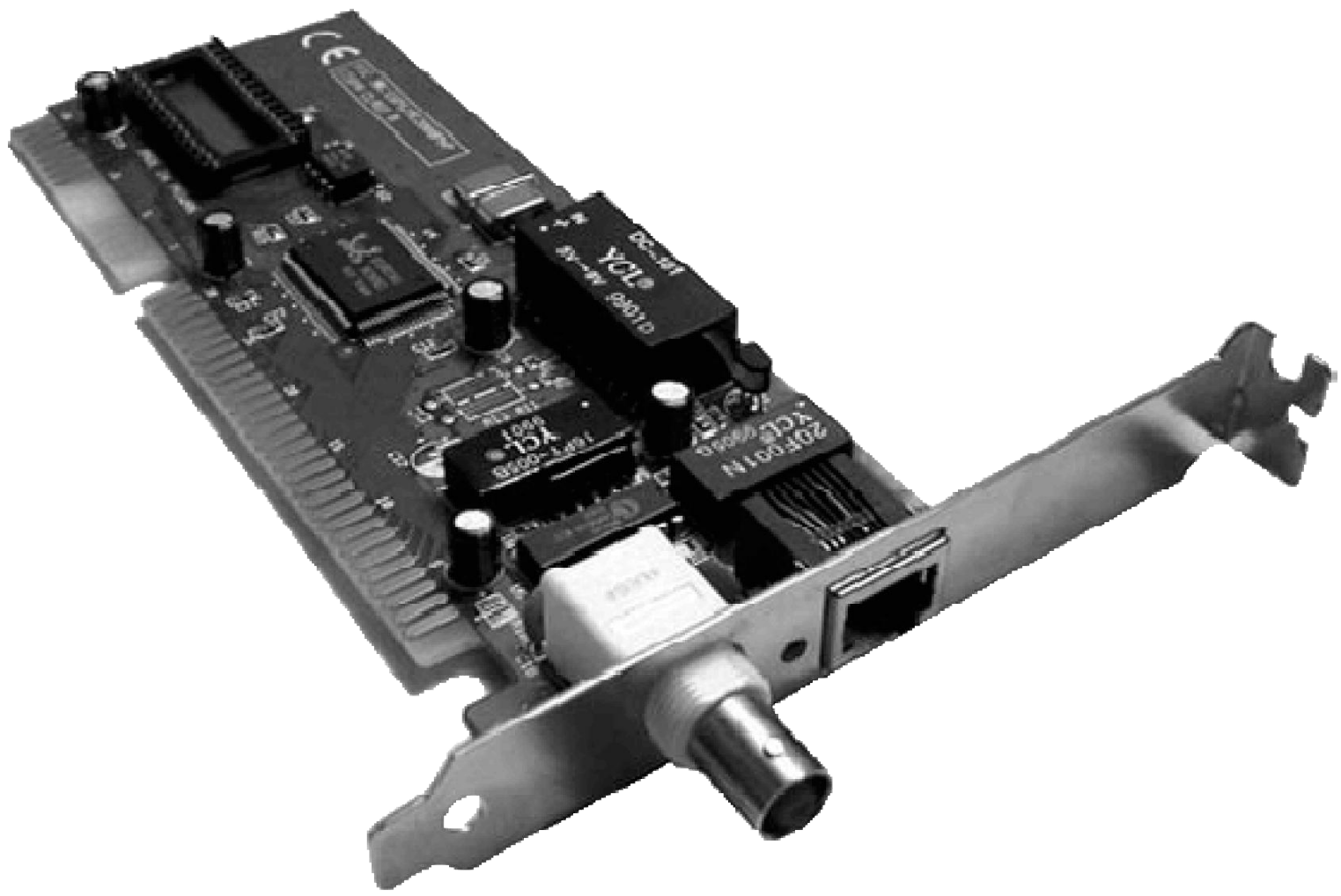
▪ Внешний USB-адаптер. Использование USB-адаптеров для расширения функциональности компьютера уже давно стало одним из самых распространенных способов. Не являются исключением и сетевые адаптеры. Мало того, часто USB-порт становится единственным способом подключения дополнительных устройств. В некоторых случаях для подключения адаптера используется удлинительный USB-шнур.

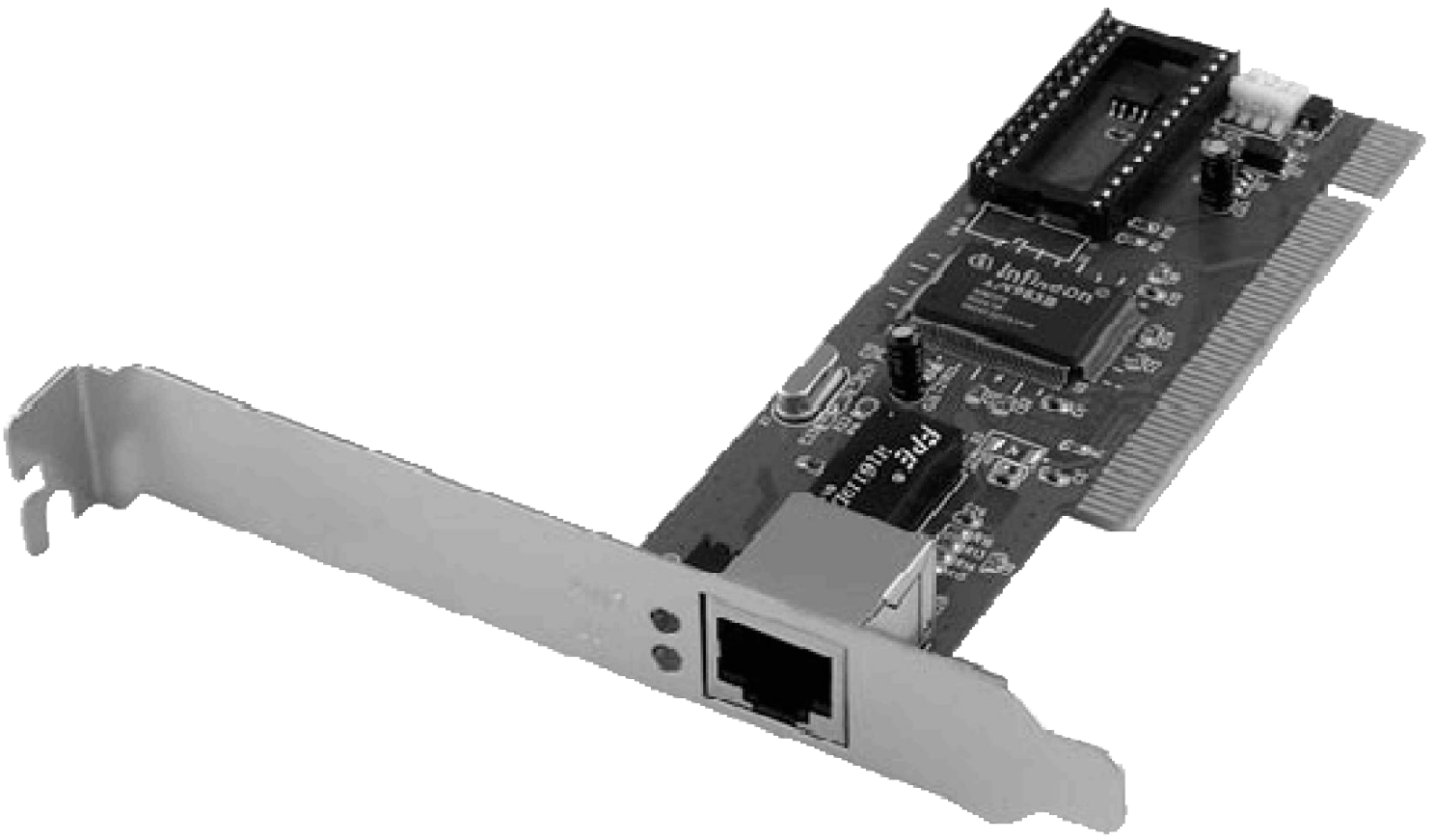
▪ Интегрированный адаптер. Данный вариант сетевого адаптера получил, пожалуй, наибольшее распространение. Причиной тому стал ATX-стандарт материнских плат, который предусматривает использование интегрированных решений, в частности – сетевого адаптера стандарта 100Base-TX или ему подобного. Правда, иногда встречаются материнские платы, которые дополнительно содержат интегрированный беспроводной контроллер стандарта IEEE 802.11b или IEEE 802.11g.

Кроме варианта исполнения, сетевые адаптеры отличаются поддержкой того или иного сетевого стандарта. Так, сетевой стандарт 10Base-2, 10Base-5 или 10Base-T подразумевает использование порта с BNC-коннектором. В свое время, когда наступил переломный момент, появились сетевые адаптеры, содержащие как BNC-, так и RJ-45-разъем. Внешний вид такого адаптера показан на рис. 9.1.

Сетевой стандарт 100Base-TX или 1000Base-T подразумевает использование адаптера с портом RJ-45. Внешний вид такого адаптера в виде платы расширения показан на рис. 9.2, а в USB-варианте – на рис. 9.3.

Несколько иначе выглядят сетевые адаптеры, предназначенные для работы со стандартами HomePNA (рис. 9.4) и HomePlug (рис. 9.5).






TRENDnet
TU2-CY100

Отредактировал и опубликовал на сайте : PRESSI (HERSON)

У адаптеров HomePNA и HomePlug кроме порта, с помощью которого они подключаются к среде передачи данных, присутствует порт RJ-45. Используя RJ-45-порт, адаптер присоединяется к Ethernet-адаптеру на материнской плате и уже через него передает данные, которые поступают через «родной» канал связи.

Особняком стоят адаптеры, предназначенные для установки в переносные компьютеры. Как правило, подобного рода компьютеры изначально снабжаются максимальным количеством устройств для разного вида связи. Однако если сетевой адаптер нужного типа все же отсутствует, всегда можно воспользоваться PCMCIA-разъемом (рис. 9.6), который предназначен именно для таких случаев.

Сетевой беспроводной адаптер

Несмотря на то что беспроводная сеть в качестве среды передачи данных использует радиоволны, принцип работы беспроводного адаптера похож на принцип работы проводного аналога. Единственное, что их может различать, – присутствие антенны.

Количество антенн беспроводного оборудования, в том числе и сетевого адаптера,

зависит от сетевого стандарта. Так, для адаптеров сетевых стандартов IEEE 802.11a, IEEE 802.11b и IEEE 802.11g нормальным считается наличие одной антенны (рис. 9.7).

Что касается беспроводных адаптеров стандарта IEEE 802.11n, то особенности их функционирования подразумевают наличие двух, а иногда и трех антенн (рис. 9.8).

Бóльшая часть беспроводных адаптеров позволяет использовать антенны с разным уровнем усиления, поэтому стандартные антенны, идущие в комплекте с сетевым адаптером, можно заменять антеннами с бóльшим коэффициентом усиления. В этом случае антенна имеет специальное крепление, позволяющее ее открутить и установить на ее место другую.

Концентратор

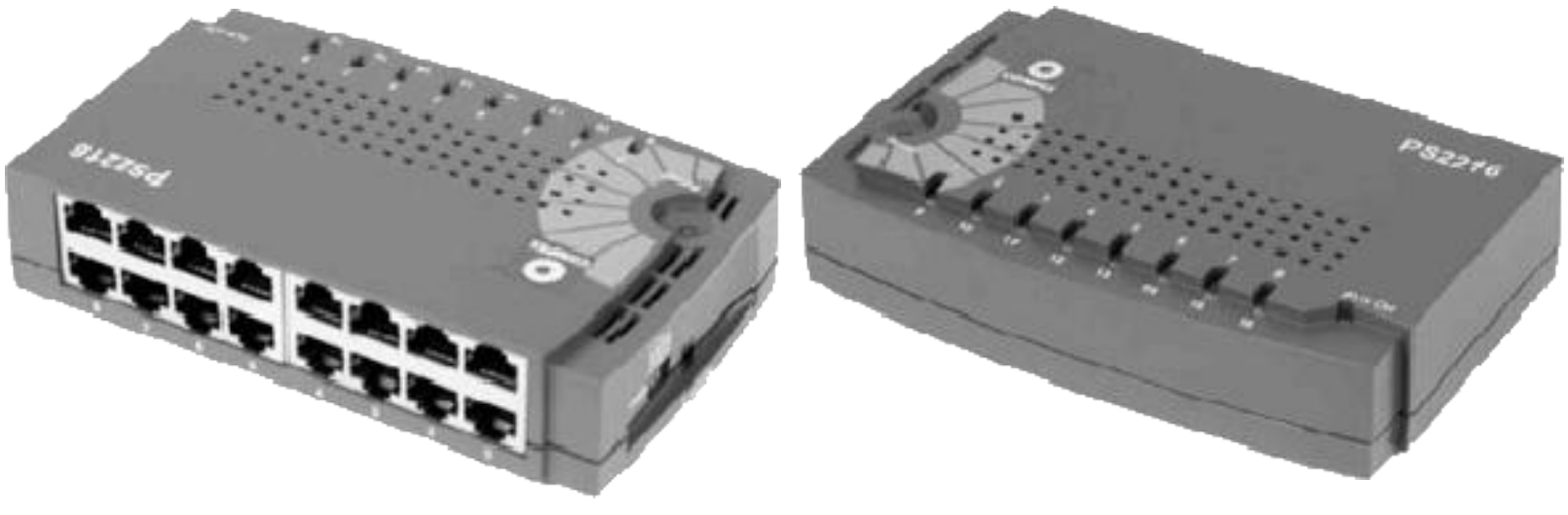
Концентратор (хаб, репитер, повторитель) – один из вариантов активного центрального управляющего узла, который необходим для соединения компьютеров в сеть при использовании топологии «звезда». Его можно также применять в качестве усилителя сигнала для увеличения максимальной длины сегментов сети.

Концентратор использует протоколы, работающие на физическом уровне модели взаимодействия открытых систем, что позволяет использовать его в локальных сетях, построенных с применением любых технологий. Он считается одним из простейших устройств.

Главная задача концентратора – трансляция поступившего по одному из портов сигнала на все остальные порты. При этом для него не имеет значения, какого типа данные передаются и кому: в любом случае они транслируются сразу на все порты, что увеличивает трафик в сети, уменьшая тем самым полезную скорость. В связи с этим использование концентратора как центрального устройства оправданно лишь в небольших

сетях. В сетях с количеством подключений более 10 вместо концентратора используют более интеллектуальное устройство, например коммутатор.

Концентратор представляет собой электронное устройство, для подключения к которому используется определенное парное количество портов, редко превышающее 24 (рис. 9.9).



На передней панели коммутатора обычно находятся светодиоды, отображающие активность портов (если индикатор светится или мигает, значит, через этот порт идет обмен данных с подключенным к нему компьютером).

В последнее время встречаются только концентраторы, предназначенные для использования с кабелем «витая пара», то есть содержащие порты RJ-45. Однако существуют также концентраторы, которые в дополнение к портам RJ-45 имеют один порт с BNC-коннектором, что позволяет подключать к концентратору коаксиальный сегмент сети, тем самым создавая сеть комбинированной топологии.

Можно встретить и так называемые стоечные концентраторы, корпус которых подразумевает их установку в монтажный шкаф. В этом случае порты для подключения кабеля могут располагаться как на передней, так и на задней панели концентратора.

Мост

Сетевой мост – это активное устройство, которое используется для объединения в единую сеть разнородных сегментов сети, часто с разной топологией. Его также можно использовать в качестве повторителя для увеличения длины сегментов локальной сети и увеличения количества подключений.

В отличие от коммутатора, мост является более интеллектуальным устройством. Применяя аппаратную реализацию разных алгоритмов, мост позволяет фильтровать и разделять трафик. Это дает возможность сэкономить на трафике в сети, а также увеличить скорость доставки пакетов с данными компьютерам в нужном сегменте сети.

Мост имеет небольшой размер и содержит минимальное количество портов: как правило, не более 2–3 портов RJ-45 (рис. 9.10).

В последнее время мост как отдельное оборудование используется достаточно редко, поскольку практически любой коммутатор может выполнять аналогичные функции.

Коммутатор

Коммутатор (свитч) – основное устройство активного типа, применяемое в качестве центрального узла для подключения компьютеров в сетях, основанных на топологии «звезда». Ближайшим к нему по функциональности (но не по «интеллекту») устройством является концентратор, который еще не так давно из-за меньшей стоимости получил широкое распространение.

Большей, чем у концентратора, функциональностью коммутатор обязан протоколам, работающим на канальном уровне. Они позволяют избежать использования лишнего трафика, когда необходимо передать данные от отправителя конкретному компьютеру, не затрагивая при этом остальные компьютеры. За счет этого достигается высокая скорость передачи данных, поэтому использовать коммутатор более выгодно, чем концентратор.

Коммутатор представляет собой достаточно интеллектуальное устройство, которое способно обучаться. Он использует MAC-адреса устройств, причем эти адреса коммутатор запоминает. Например, когда компьютер передает данные другому компьютеру, коммутатор запоминает MAC-адрес отправителя и отправляет данные сразу на все порты, то есть работает как концентратор. Однако это происходит только на первых порах. Как только коммутатор сможет определить MAC-адреса каждого из подключенных к его портам компьютеров, данные сразу же будут отправляться на конкретный порт, тем самым уменьшая время доставки, а значит, увеличивая скорость передачи данных.

Внешне коммутатор выглядит как коробка с определенным количеством портов (как правило, не более 48) RJ-45 (рис. 9.11).

Как и в случае с концентраторами, часто можно встретить стоечные коммутаторы, предназначенные для установки в монтажный шкаф. При этом стоечные коммутаторы обычно можно соединять, для чего используется либо отдельный RJ-45-порт на задней панели, либо один из свободных портов на передней панели.

Еще одним плюсом коммутаторов является возможность управления, в связи с чем различают управляемые и неуправляемые коммутаторы.

Управляемые коммутаторы кроме набора портов RJ-45 содержат еще один порт, с помощью которого их можно подключить к компьютеру и производить настройку. Кроме того, часто управление коммутатором осуществляется с помощью веб-интерфейса через любой браузер, для чего коммутатору присваивается статический IP-адрес (при необходимости его можно изменять).

Маршрутизатор

Маршрутизатор (роутер) – еще один представитель активного оборудования, который играет роль центрального узла в случае использования топологии «звезда» или комбинированной топологии. По своим возможностям он является наиболее «интеллектуальным» и может делать все, что выполняют концентратор, мост и коммутатор вместе взятые. Кроме того, он имеет еще свой «багаж» возможностей: использование обновляемых таблиц маршрутизации, поддержка виртуальных сетей, работа с разнородными сегментами сети, внутренний брандмауэр и многое другое. Как результат – быстрая и эффективная работа локальной сети без лишних задержек и коллизий.

Протоколы, реализованные в аппаратной части маршрутизатора, позволяют ему работать на сетевом уровне модели взаимодействия открытых систем, а значит – получать доступ практически к любому типу служебной информации, которым оперируют сетевые устройства. В результате таблицы маршрутизации, которые используются для передачи данных между компьютерами, не только всегда актуальны, но и содержат данные об альтернативных маршрутах движения.

Как правило, применяются только управляемые маршрутизаторы, для чего может использоваться либо веб-интерфейс с доступом по определенному IP-адресу, либо один из портов на маршрутизаторе.

Внешний вид маршрутизатора мало чем отличается от коммутатора и концентратора,

поэтому их часто путают (рис. 9.12).

Как правило, маршрутизатор содержит от 16 до 64 портов и обязательно поддерживает возможность установки в стойку монтажного шкафа.

Точка доступа

Точка доступа (Access Point) – представитель активного типа устройств, необходимых для объединения компьютеров в беспроводную сеть. Ее аналогом является проводной коммутатор, а в отдельных случаях и маршрутизатор.

Точка доступа в силу особенностей беспроводной среды передачи данных является достаточно интеллектуальным устройством и часто позволяет осуществлять дополнительное управление локальной сетью. Например, в современных точках доступа имеется аппаратная реализация DNS– и DHCP-серверов, что позволяет создавать структурированные локальные сети, представляющие собой упрощенный вариант доменной структуры. Кроме того, точка доступа одновременно является брандмауэром, способным фильтровать и блокировать пакеты, а также, что самое главное, содержит информацию, необходимую для авторизации подключаемых компьютеров.

Как уже упоминалось ранее, точка доступа использует идентификатор сети, а также подразумевает применение одного или нескольких работающих в паре алгоритмов безопасности и шифрования. В связи с этим, чтобы иметь возможность настраивать эти параметры, точка доступа имеет в своем составе как минимум один порт RJ-45, посредством которого она подключается к сетевому адаптеру компьютера. Далее, применяя веб-интерфейс или программное обеспечение, идущее в комплекте с точкой

доступа, пользователь может настраивать необходимые параметры ее работы.

Внешний вид точки доступа зависит от некоторых факторов.

▪ Наличия дополнительных портов RJ-45. С помощью точки доступа можно объединить беспроводную сеть с проводными сегментами сети, для чего используются порты RJ-45 стандарта 100Base-TX или подобного. Количество этих портов может быть разным, но обычно их не более четырех.

▪ Количества и мощности антенн. Различные сетевые стандарты требуют использования разного количества антенн, поэтому на точке доступа их будет столько, сколько предусмотрено стандартом (рис. 9.13).

Однако часто встречаются точки доступа, которые содержат дополнительную антенну, что позволяет расширить зону покрытия сети за счет более сильного сигнала. Кроме того, некоторые точки доступа имеют возможность подключать внешнюю антенну, для чего оборудуются соответствующим гнездом, либо антенну с большим коэффициентом усиления вместо стандартной.

▪ Средств индикации. На передней панели точки доступа расположены светодиоды, которые сигнализируют о переходе точки доступа в тот или иной режим работы, а также отображают активность дополнительных портов. Количество средств индикации напрямую зависит от функциональных возможностей точки доступа и от количества

дополнительных портов на задней панели.

▪ Типа исполнения. Поскольку беспроводная сеть может организовываться как в закрытом помещении, так и на открытом воздухе, корпус точки доступа должен быть готов к этому. Поэтому офисные точки доступа отличаются от точек доступа для внешнего использования. Как минимум отличаются вид и материал корпуса, но могут быть и другие отличия: в наличии портов и креплений для грозозащиты, портов для подключения внешней антенны, питания и т. п.

Модем

Модем используется для соединения двух удаленных точек, например компьютеров или сегментов сети. Однако чаще всего он используется для подключения компьютера к Интернету.

Слово «модем» является сокращением от слов «модулятор» и «демодулятор», что подразумевает наличие в составе устройства соответствующей аппаратной начинки, которая выполняет модуляцию и демодуляцию сигнала.

Модем имеет цифровой интерфейс связи с компьютером (цифроаналоговые и аналого-цифровые преобразования) и аналоговый интерфейс для связи с телефонной линией. Он состоит из процессора, памяти, аналоговой части, ответственной за сопряжение модема с телефонной сетью, и контроллера, который всем управляет.

У стандартного аналого-цифрового модема (рис. 9.14) обмен информацией происходит по обычной телефонной линии в диапазоне частот 300-3400 Гц.

Преобразование аналогового сигнала осуществляется достаточно просто: его

характеристики измеряются с определенной частотой и записываются в цифровой форме по определенному алгоритму. Преобразование цифровой информации идет в обратной последовательности.

Главное различие модемов – вариант их исполнения. Бывают внешние и внутренние модемы. Внутренние, как правило, выполнены в виде платы расширения, которая вставляется в свободный слот компьютера. В персональном компьютере это слот PCI или PCI Express, в переносных устройствах – слот PCMCIA.

В зависимости от типа модема и среды передачи данных различается скорость их передачи. Скорость обычного цифроаналогового модема, работающего с телефонной аналоговой линией, равна 33,6-56 Кбит/с.

Широкое распространение получили ADSL-модемы (рис. 9.15), которые используются для организации скоростного подключения к Интернету.

Скорость передачи данных у таких модемов обычно находится в пределах 1–8 Мбит/с, но теоретически может быть и более 20 Мбит/с.

Модемы бывают как проводными, так и беспроводными. При этом внешний (беспроводной) модем кроме телефонного разъема RJ-11 часто снабжается одним или несколькими портами RJ-45, получая при этом возможность выполнять функции концентратора. Чаще всего внешние модемы подключаются к компьютеру через сетевой адаптер, но встречаются также модемы с USB-подключением.

Антенна

В беспроводной сети антенна имеет большое значение, поскольку именно она является связующим звеном между данными и средой передачи данных. Хорошая антенна позволяет сети работать с максимальной отдачей, достигая при этом своих теоретических пределов дальности распространения сигнала и скорости передачи данных.

Антенны бывают всенаправленные (рис. 9.16) и узконаправленные (рис. 9.17), а также различаются вариантом их использования: внутри здания или на открытом воздухе.

Узконаправленная антенна позволяет увеличить дальность связи, что используют, когда необходимо соединить два удаленных сегмента беспроводной сети. Всенаправленная антенна распространяет сигнал вокруг себя, что дает возможность другим устройствам, установленным рядом, взаимодействовать друг с другом. По умолчанию именно всенаправленная антенна идет в комплекте с точкой доступа или беспроводным адаптером.

Одной из самых важных технических характеристик антенны является коэффициент усиления сигнала. К примеру, использование антенны с бóльшим коэффициентом усиления позволяет получить более высокий уровень сигнала и, соответственно, увеличить радиус сети. Это становится крайне важным, особенно когда компьютеры находятся на значительном удалении от точки доступа.

Пассивное оборудование

Оборудование, которое присутствует при передаче данных, но не принимает в этом непосредственного участия, называется пассивным. Сюда относятся монтажные шкафы, распределительные панели, сетевые розетки, кабель, коннекторы и т. д. К этой группе можно отнести также инструменты, которые используются при создании локальной сети.

Монтажный шкаф

Локальная сеть с большим количеством компьютеров редко обходится без монтажного шкафа, который позволяет собрать в одном месте все или почти все центральные органы управления сетью. В нем обычно располагают бóльшую часть активного оборудования сети (коммутаторы, маршрутизаторы, модемы) и часть пассивного оборудования (кросс-панели, кросс-кабели и т. п.).

В зависимости от размера шкафа и варианта его исполнения в него можно устанавливать также серверы стоечного типа, блоки бесперебойного питания, KVM-переключатели (для вывода изображения с нескольких компьютеров на один монитор, а также для использования только одной клавиатуры и мыши) и т. д.

Существуют разные варианты монтажных шкафов, различающиеся двумя основными показателями – типом исполнения (напольный или подвесной) и габаритами. Кроме того, различия могут быть в конструкции шкафа, наличии охлаждающей системы, способе подвода кабелей и т. д.

Размеры шкафа и вариант его исполнения подбираются исходя из количества компьютеров в сети и количества оборудования, которое планируется установить в шкаф. Если в сети 30–40 компьютеров, то вполне достаточным будет использовать подвесной шкаф (рис. 9.18).

Если же в сети насчитывается большее количество компьютеров или решено использовать серверы стоечного типа, то стоит остановить свой выбор на напольном варианте. Размеры шкафа должны не только позволить поместить туда все необходимое оборудование, но и дать возможность установить его в серверной или другой комнате, обеспечив к нему свободный доступ (рис. 9.19).

Чтобы дать доступ к оборудованию и кабельной системе, монтажный шкаф оборудуется как минимум одной дверкой из стекла. Это вполне оправданное решение, поскольку позволяет вести постоянный визуальный контроль оборудования, а также обеспечивает оптимальный температурный режим внутри шкафа.

Кросс-панель

Кросс-панель является неотъемлемым атрибутом любой большой локальной сети, которая использует монтажные шкафы. Кросс-панели бывают только стандартных размеров, которые зависят от параметров самого монтажного шкафа.

Основное предназначение кросс-панели – обеспечить удобный монтаж кабеля в контактных площадках разъемов с последующим соединением этих разъемов с портами на активном сетевом оборудовании.

Внешний вид кросс-панели зависит от количества и типа портов, которые располагаются на ее передней панели, а также от ее габаритов. Как правило, на кросс-панели не бывает менее 16 портов, что связано со стандартными размерами стоек в монтажном шкафу.

Количество кросс-панелей подбирается исходя из нужд, то есть в зависимости от количества компьютеров локальной сети и другого оборудования, которому нужно подключение к порту на кросс-панели. Как правило, стандартная кросс-панель содержит от 24 до 48 портов, которые могут располагаться как в один, так и в несколько рядов (рис. 9.20).

Чтобы облегчить монтаж кабеля и создание необходимой проектной документации, каждый порт на кросс-панели пронумерован. Кроме того, рядом с портом обычно находится специальный участок, на котором маркером можно сделать любую полезную короткую запись.

На задней части кросс-панели находится система разводки портов, то есть непосредственно контактные площадки портов, которые используются для зажима проводников кабеля или монтажа оптоволоконных жил. Каждый порт снабжается фиксирующим устройством или скобами, позволяющими закрепить кабель, который идет к конкретному порту. Существует также общая система фиксирования, предназначенная для того, чтобы закрепить сразу все кабели, исключая тем самым возможность потери контакта.

Сетевой кабель

Если в беспроводной сети для передачи данных используется радиоэфир, то создание проводной сети требует применения кабелей разного типа. Как уже говорилось выше, основными типами кабелей являются «витая пара», коаксиальный и оптоволоконный.

Каждый тип кабеля имеет свои характеристики и особенности использования. Основными отличительными параметрами являются:

- диаметр проводников;
- диаметр проводника с изоляцией;
- количество проводников (или пар проводников);
- наличие экрана вокруг проводника (проводников);
- диаметр кабеля;
- диапазон температур, при котором качественные показатели находятся в норме;
- минимальный радиус изгиба, который допускается при прокладке кабеля;
- максимально допустимые наводки в кабеле;
- волновое сопротивление кабеля;
- максимальное затухание сигнала в кабеле.

Это только малая часть того, что различает разные типы кабелей. Более детально о строении кабеля и его особенностях было рассказано ранее, в гл. 7.

Патч-корд, кросс-корд

Патч-корд и кросс-корд – это кабели небольшой длины с обжатыми коннекторами, которые используются для различных целей. Они являются частью сети, построенной с применением кабеля «витая пара» (рис. 9.21).

Патч-корд, в отличие от кросс-корда, сделан из более мягкого кабеля и применяется для подключения компьютеров и другого сетевого оборудования к сетевым розеткам или непосредственно к портам на активном оборудовании. Длина кабеля, согласно существующим стандартам, не должна превышать 5 м, однако на практике часто используют кабель длиной до 10 м.

Что касается кросс-корда, то он имеет гораздо меньшую длину (как правило, не более 1 м) и используется в монтажном шкафу для соединения портов кросс-панели с портами на активном оборудовании или для соединения активного оборудования между собой.

Коннекторы

Кабель, используемый для создания проводных вариантов сети, не представляет никакой ценности без коннекторов. Именно они завершают его целостность и позволяют использовать его по назначению – для передачи данных между отправителем и получателем. С помощью коннекторов кабель подключается к нужному разъему на оборудовании – как активном, так и пассивном.

Тип коннектора описывают сетевые стандарты, и достаточно часто они несовместимы друг с другом. Например, локальные сети с использованием коаксиального кабеля требуют применения коннекторов BNC-типа, с использованием кабеля «витая пара» – коннектора RJ-45, стандарта HomePNA – коннекторов RJ-11 и RJ-45 и т. д.

Коннекторы BNC-типа. Коннекторы BNC-типа (Bayonet Neill Concelman) используются при построении сети с использованием коаксиального кабеля. Существует несколько коннекторов BNC-типа, которые различаются своим назначением.

- BNC-коннектор. Применяется для обжима концов коаксиального кабеля (рис. 9.22).

С помощью такого коннектора кабель подключается к сетевой карте, порту на сетевом оборудовании и к другим коннекторам типа BNC, например T– или I-коннектору.

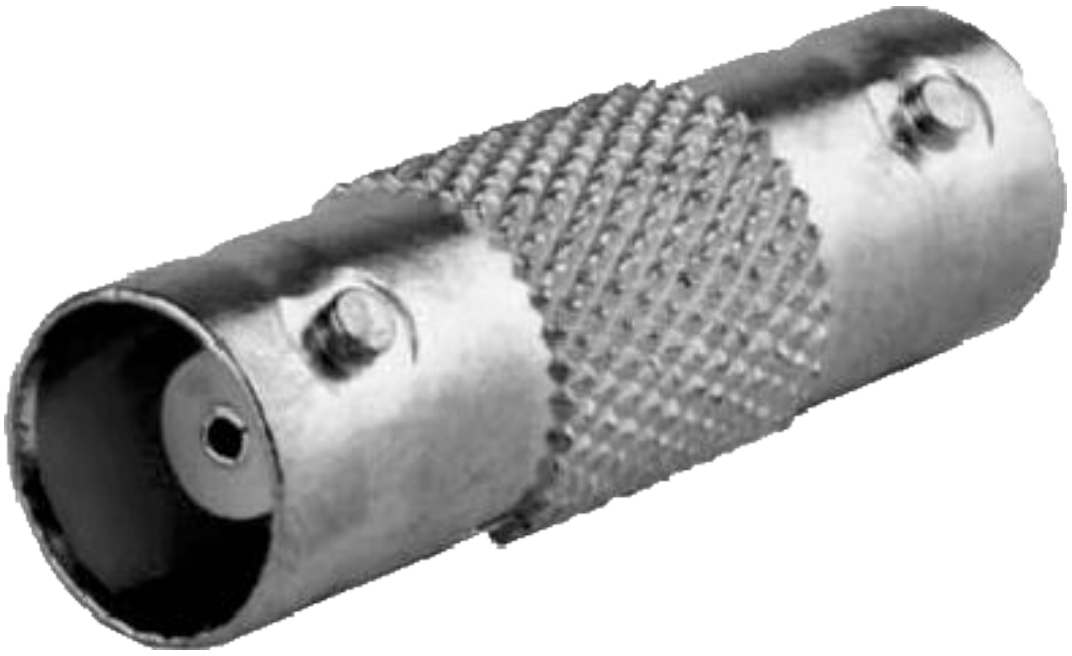
Существуют и более старые варианты исполнения BNC-коннектора, например накручивающиеся или коннекторы для пайки, однако в силу разных особенностей сегодня они уже не встречаются.

▪ T-коннектор. Данный тип коннекторов используется для соединения основной кабельной магистрали с сетевой картой компьютера или другого сетевого оборудования в сети, построенной с применением коаксиального кабеля и топологии «шина».

Внешне T-коннектор (рис. 9.23) похож на обычный BNC-коннектор, но имеет отводы для врезки в центральную магистраль.

Т-коннектор всегда используется в паре с BNC-коннектором (продлевает сегмент кабеля) или терминатором (закрывает сегмент).

▪ I-коннектор. Этот тип коннектора (рис. 9.24), который часто называют барел-коннектором, используется для соединения сегментов кабеля без применения активного оборудования.



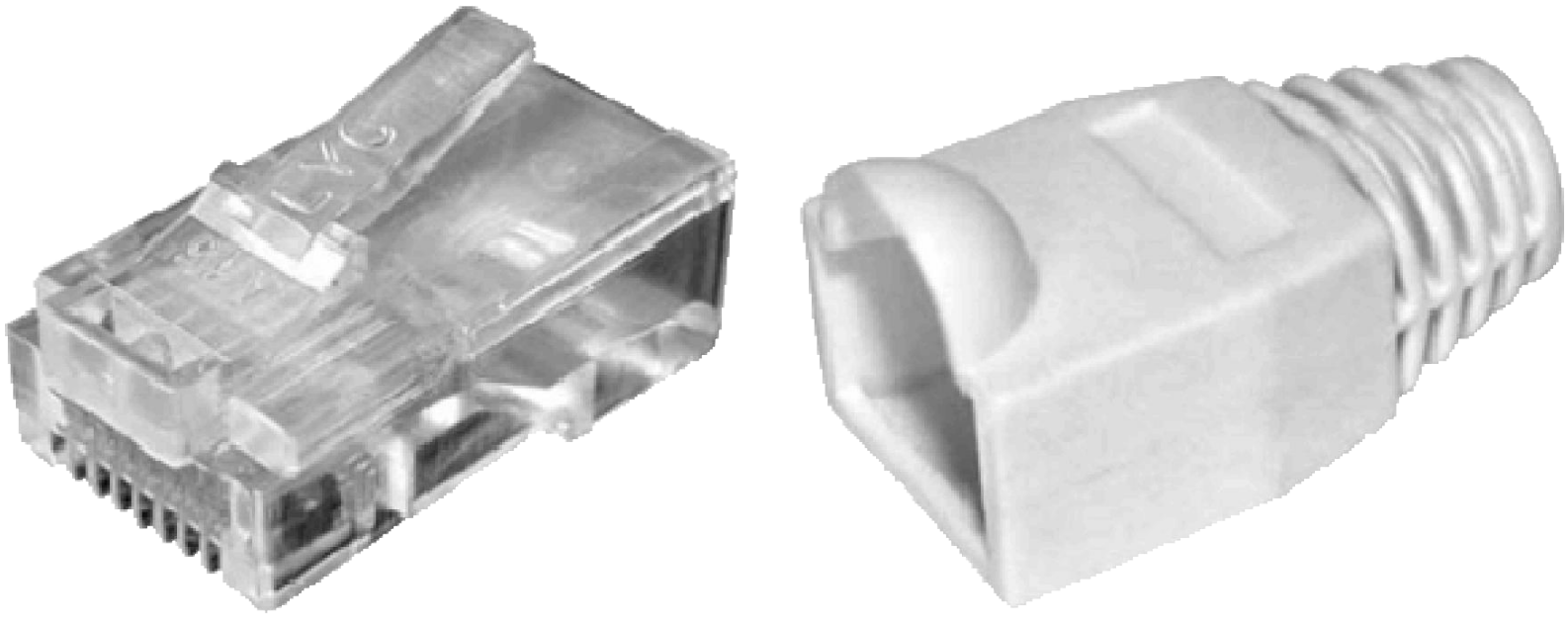
Подобное достаточно часто происходит, когда случается разрыв центральной магистрали либо ее отростка или когда необходимо удлинить кабель.

▪ Терминатор (рис. 9.25) представляет собой заглушку, которая должна препятствовать появлению отбитого сигнала.

Такой коннектор устанавливается на обоих концах магистрали, при этом один из терминаторов обязательно заземляется. Если его не установить, то сигнал, поступая в никуда, может привести не только к задержкам неопределенной длительности, но и к выходу сети из строя.

Коннектор RJ-45. Коннектор RJ-45 используется для обжима кабеля «витая пара», который применяется для создания локальных сетей, например стандарта 100BaseTX. Внешне этот коннектор похож на RJ-11, используемый для обжима телефонного кабеля, только шире его и содержит больше контактных групп.

Внешний вид коннектора может иметь небольшие различия, касающиеся материала изготовления основы или составных частей коннектора, что зависит от сетевого стандарта, однако это не приводит к изменению габаритов и конструкции. Внешний вид такого коннектора показан на рис. 9.26.



Особенностью коннектора RJ-45 является его ограниченный срок службы, что связано с особенностями конструкции и материала, из которого сделан коннектор. К примеру, для фиксации коннектора в разъеме используется пластиковый фиксатор; если он сломается, то обеспечить хороший контакт уже будет невозможно. Как результат – нестабильная работа сегмента и частое «пропадание» сети.

ПРИМЕЧАНИЕ

Как правило, стандартный срок службы фиксатора на коннекторе RJ-45 составляет 2000 подключений.

В паре с коннектором RJ-45, как правило, идет защитный колпачок из мягкого материала, например обрезиненного пластика, который надевается на коннектор и часть кабеля, скрывая и защищая тем самым наиболее уязвимую часть – место обжима. Однако это не обязательная мера, поэтому очень часто, особенно в небольших локальных сетях

офисного или домашнего масштаба, в целях экономии денежных средств защитный колпачок не используется.

Розетка RJ-45

Розетка RJ-45, как и все розетки, предназначена для обеспечения контакта между носителем и потребителем, в нашем случае – между кабельной системой и компьютером или другим сетевым устройством. При этом подразумевается, что речь идет о локальной сети, использующей один из стандартов на основе кабеля «витая пара».

Применение сетевых розеток делает кабельную систему более устойчивой к разного рода неприятностям в виде обрывов кабеля, пропадания контактов в соединениях и т. п. Розетки применяются при необходимости. Их выбор критичен только для локальных сетей с большим количеством подключений. Подобные сети, как правило, оборудованы в больших организациях, которые могут себе позволить сделать все по правилам, в том числе и использовать розетки. В небольших сетях и уж тем более в домашней сети чаще всего использование розеток игнорируется. В этом случае компьютеры или другие устройства подключаются напрямую к портам на оборудовании.

На внешний вид сетевой розетки оказывают влияние следующие параметры.

▪ Категория розетки. Как и кабель, сетевая розетка также может быть разных категорий: чем выше категория, тем лучше качество розетки, выше уровень безопасности, лучше способ обжима проводников кабеля и т. д. Например, розетка низкой категории часто использует систему крепления проводников с помощью шурупов, в то время как розетка высокой категории использует для этого монтажную контактную площадку.

▪ Тип розетки и способ ее крепления. Встречаются розетки с внутренним и внешним способами монтажа. Внутренний способ подразумевает монтаж розетки в монтажной коробке, для которой в стене делается специальное отверстие. При внешнем монтаже розетку крепят шурупами прямо на стену, встраивают ее в сетевой короб или просто приклеивают к гладкой поверхности с помощью двухстороннего скотча.

▪ Наличие дополнительных разъемов. Часто на розетке присутствуют дополнительные разъемы, например RJ-45 или RJ-11, что делает ее более универсальной: одну и ту же конструкцию можно использовать для обслуживания нескольких устройств, например компьютера и телефона.

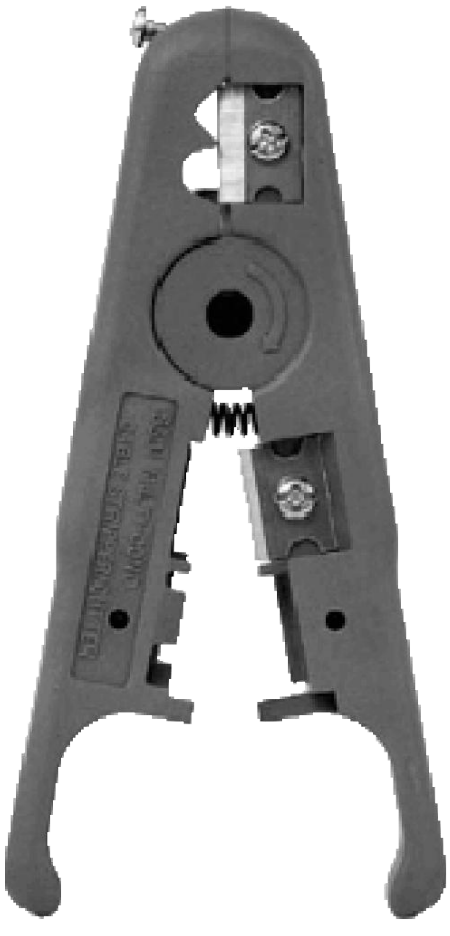
Внешний вид розетки, предназначенной для крепления на стене, показан на рис. 9.27.

Инструменты для работы с кабелем

Без специальных инструментов очень сложно произвести качественный обжим коннектора на кабеле или зажим проводников кабеля в контактной площадке. Результатом может стать не только низкое качество выполнения такой работы, но и возможная неработоспособность всей сети [2 - Это является особенностью сетей, построенных с применением топологии «шина»: обрыв или плохой контакт в любом из коннекторов приводит к неработоспособности всей сети. Если с помощью коаксиального кабеля к коммутатору подключается отдельный сегмент сети, неработоспособным будет только этот сегмент.] или отдельного ее сегмента.

Коннекторы на коаксиальном кабеле и кабеле «витая пара» различаются по конструкции, поэтому для их обжима используются разные инструменты.

Как правило, для работы с коаксиальным кабелем и BNC-коннектором применяются два инструмента: первый используется для обрезки и зачистки кабеля (рис. 9.28), второй – для обжима коннектора (рис. 9.29).



С помощью первого инструмента кабель обрезается так, что он сразу готов к обжиму, то есть обрезается внешняя изоляция и диэлектрик, под которым находится центральный проводник. Для точной глубины обрезки на инструменте есть специальный механизм регулировки: отдельно для изоляции и диэлектрика.

После того как кабель обрезан, производят обжим коннектора, предварительно собранного в правильной последовательности.

Что касается инструмента для работы с кабелем «витая пара», то он имеет несколько иную конструкцию и более универсален: резак и обжимной механизм объединены в одном инструменте.

Внешний вид инструмента зависит от его функциональности. К примеру, некоторые инструменты позволяют производить также обжим коннекторов RJ-11, для чего на них сделано специальное отверстие (рис. 9.30).

Для монтажа сетевых розеток или зажима проводников на кросс-панели используется специальный нож-вставка (рис. 9.31).

Внешний вид ножа-вставки также может быть разным. Это зависит от производителя и дополнительных возможностей инструмента.

Отредактировал и опубликовал на сайте : PRESSI (HERSON)

Часть 2
Проводные сети

Глава 10
Проводные стандарты

Разработкой правил функционирования локальных сетей стандарта Ethernet с кабельной средой передачи данных занимается комитет IEEE 802.3. За время своего существования он выпустил в свет достаточно много стандартов. Наиболее известными среди них являются стандарты 10Base-5, 10Base-2, 10Base-T, 100Base-TX, 1000Base-X. Особенности этих и некоторых других стандартов будут рассмотрены в данной главе.

10Base-5, 10Base-2

Данные стандарты описывают принцип функционирования сети с применением топологии «шина» и коаксиального кабеля в качестве среды передачи данных. Именно с появлением стандарта 10Base-5 локальные сети стали набирать популярность.

Стандарт 10Base-5 был принят в начале 80-х годов прошлого века. Он описывает правила функционирования локальных сетей и устройств, которые для передачи данных используют коаксиальный кабель, точнее, его толстый вариант, то есть кабель толщиной примерно 1 см. В связи с этим данный стандарт получил название толстый Ethernet.

Наиболее важными правилами функционирования локальной сети стандарта 10Base-5 являются следующие:

- в качестве среды передачи данных используется толстый коаксиальный кабель, длина которого не должна превышать 500 м для одного сегмента;
- на обоих концах магистрали устанавливаются терминаторы – устройства, устраняющие эффект отображенного (искаженного) сигнала;
- для подключения компьютера к центральной магистрали используется трансивер, при этом количество трансиверов, а соответственно, и сетевых подключений в одном сегменте не должно превышать 100 станций;
- максимальная протяженность центральной магистрали – 2500 м с учетом использования максимум 5 сегментов. Для соединения сегментов применяются специальные устройства, усиливающие сигнал, – репитеры, количество которых не должно превышать 4;
- минимальное расстояние между трансиверами – 2,5 м;
- длина кабеля от трансивера до сетевой карты станции не должна превышать 50 м.

При соблюдении всех этих правил теоретическая скорость передачи данных в локальной сети должна составлять 10 Мбит/с.

Спустя несколько лет комитет 802.3 разработал еще один сетевой стандарт – 10Base-2, который также предполагал использование коаксиального кабеля, но его тонкого варианта. Соответственно, он получил название тонкий Ethernet. Поскольку в качестве среды передачи данных использовался тонкий коаксиальный кабель, создание сети стало более легким: толщина кабеля позволяла выбрать оптимальный маршрут его прокладки. Кроме того, при подключении компьютера отпала надобность в трансивере. Однако при всех этих преимуществах максимальная длина сегмента существенно уменьшилась и

составила около 200 м.

Изменения коснулись и других требований:

▪ для передачи данных используется тонкий коаксиальный кабель, длина сегмента которого не должна превышать 185 м;

▪ в сети может быть не более 5 сегментов, при этом общая протяженность центральной магистрали составляет 925 м;

▪ минимальное расстояние между станциями – 0,5 м;

▪ возможно использование не более 4 репитеров;

▪ количество подключений в одном сегменте не может превышать 30.

Главным недостатком локальной сети с использованием коаксиального кабеля является то, что в случае его обрыва вся сеть перестает функционировать. При этом определить место «аварии» достаточно сложно, поскольку причиной может стать как обрыв самой центральной магистрали, так и микрообрыв в одном из соединительных коннекторов, с помощью которых подключаются рабочие станции. С другой стороны, большая протяженность сегмента является безусловным плюсом, поскольку это позволяет соединить между собой удаленные точки.

Впрочем, время использования этих стандартов уже прошло. Конструкция и характеристики коаксиального кабеля позволяют передавать данные на скорости не более 10 Мбит/с, а ее в большинстве случаев уже не хватает для работы с современными объемами данных.

10Base-T

Топология «шина» была первой из использовавшихся топологий в локальных сетях. Она применялась достаточно долго, почти целое десятилетие. Однако наступил момент, когда эта сетевая топология, по крайней мере с использованием коаксиального кабеля, перестала удовлетворять растущим требованиям скорости передачи данных и надежности сети. При значительном увеличении количества рабочих станций ощутимо падала скорость передачи данных, что сводило на нет главное достоинство подобных сетей – малые затраты на их создание. Кроме того, сыграла свою роль низкая надежность сети в плане обеспечения ее физической целостности.

По этим причинам комитет 802.3 начал работу над созданием нового стандарта, использующего более современные технологии. В результате в 1990 году появился 10Base-T. Он стал первым стандартом, использующим сетевую топологию «звезда» и новый физический носитель – неэкранированный кабель «витая пара» с двумя парами проводников. Пожалуй, именно это событие стало важнейшим этапом в развитии локальных сетей.

Использование топологии «звезда» сделало локальные сети более гибкими и легко расширяемыми, а также повысило их безопасность и отказоустойчивость.

Стандарт 10Base-T подразумевает выполнение следующих требований:

▪ для передачи данных используется кабель «витая пара» с двумя парами неэкранированных проводников, причем одна пара проводников применяется для передачи данных, а вторая – для их приема;

▪ длина кабеля, используемого для подключения рабочей станции, не должна превышать 100 м;

▪ для увеличения длины сегмента сети может применяться не более 4 репитеров, при этом расстояние между двумя самыми крайними рабочими станциями при использовании кабеля «витая пара» не должно превышать 500 м;

▪ все рабочие станции подключаются к центральному управляющему устройству, в качестве которого могут применяться концентратор, коммутатор и т. д.;

▪ максимальное количество подключений – 1024.

Использование этого стандарта позволяет достичь скорости передачи данных 10 Мбит/с, однако главной особенностью локальных сетей с применением топологии «звезда» является то, что скорость передачи данных не зависит от количества подключенных участников.

При использовании этого стандарта сеть стала еще более гибкой, поскольку максимальную длину сегмента можно легко увеличить, используя, например, толстый коаксиальный кабель. Это позволяет создавать разные удаленные сегменты и объединять их в одну локальную сеть с общими ресурсами.

10Base-F

Для повышения эффективности работы локальных сетей в начале 90-х годов прошлого века комитет 802.3 разработал еще один сетевой стандарт – 10Base-F. Как и предыдущий стандарт, 10Base-F подразумевает использование сетевой топологии «звезда». Однако он имеет одно значительное отличие от 10Base-T: в качестве среды передачи данных используется оптоволоконный кабель.

Несмотря на то что скорость передачи данных осталась прежней (10 Мбит/с), увеличилась максимальная протяженность сети. Кроме того, учитывая помехозащищенность такого кабеля, локальную сеть можно создать даже в условиях неблагоприятной окружающей среды.

Стандарт 10Base-F подразумевает выполнение следующих условий:

- для передачи данных используется оптоволоконный кабель с различным сечением световода: как одномодовый, так и многомодовый;
- длина сегмента многомодового кабеля не должна превышать 1000 м, а одномодового – 5000 м;
- для увеличения диаметра сети может использоваться не более 4 репитеров;
- все рабочие станции подключаются к центральному управляющему устройству, в качестве которого могут использоваться концентратор, коммутатор и т. д.;
- максимальное количество подключений – 1024.

Подобные впечатляющие показатели возможной длины сегментов стали доступны благодаря иному принципу передачи сигнала и малому уровню его затухания в оптическом волокне. Это свойство часто используют для того, чтобы увеличить максимальную длину сегментов сети, а также для подключения удаленных сегментов сети с другими топологиями и стандартами.

100Base-TX

Дальнейшее развитие сетевых стандартов происходило уже «по накатанной»: главный упор делался на улучшение качественных показателей. Современные требования по скорости передачи данных заставляли комитет по стандартизации функционирования локальных сетей создавать стандарты, которые бы удовлетворяли эти запросы. Одним из таких стандартов, получившим очень широкое распространение, стал 100Base-TX, принятый в 1995 году. Именно он является первым среди стандартов, получивших общее название Fast Ethernet.

Данный стандарт используется в сетях, построенных по топологии «звезда» и в качестве физической среды использующих кабель «витая пара» UTP не ниже пятой категории. Это позволяет оборудованию работать как в полудуплексном (передача данных одновременно только в одну сторону), так и дуплексном режимах. При этом дуплексный режим обеспечивает максимально возможную для стандарта скорость передачи данных – 100 Мбит/с.

Стандарт 100Base-TX требует выполнения следующих условий:

▪ для передачи данных используется кабель «витая пара» пятой категории;

▪ длина кабеля «витая пара» для подключения рабочей станции не должна превышать 100 м;

▪ для увеличения диаметра сети может применяться не более 2 репитеров (концентраторов, коммутаторов и т. д.), при этом максимальная длина сегмента составляет 205 м;

▪ длина кабеля между репитерами не должна превышать 5 м;

▪ все рабочие станции подключаются к центральному управляющему устройству, в качестве которого могут использоваться концентратор, коммутатор и т. д.;

▪ максимальное количество подключений – 1024.

На широкое распространение 100Base-TX повлияла стандартизация материнских плат (ATX), которая сделала наличие сетевого адаптера на материнской плате обязательным. Мало того, именно этот факт часто становится решающим при выборе топологии и сетевого стандарта будущей сети.

100Base-T4

Этот стандарт относится к серии 100-мегабитных. Он также подразумевает использование топологии «звезда» и кабеля «витая пара» (UTP). Однако, в отличие от 100Base-TX, данный стандарт может использовать кабель ниже пятой категории, что делает его очень удобным. К примеру, пользователи локальной сети стандарта 10Base-T, в которой применяется кабель «витая пара» третьей категории, могут получить скорость передачи данных 100 Мбит/с, как только заменят старое оборудование на оборудование стандарта 100Base-T4 и произведут обжим коннекторов по новым правилам.

Для применения стандарта 100Base-T4 должны выполняться следующие условия:

▪ для передачи данных используется кабель «витая пара» 3-й, 4-й и 5-й категорий;

▪ длина кабеля «витая пара», применяемого для подключения рабочей станции, не должна превышать 100 м;

▪ для увеличения радиуса сети может использоваться не более 2 репитеров, при этом максимальная длина сегмента составляет 205 м;

▪ общее количество сегментов – не более 3;

▪ длина кабеля между репитерами не должна превышать 5 м;

▪ все рабочие станции подключаются к центральному управляющему устройству, в качестве которого могут применяться концентратор, коммутатор и т. д.;

▪ максимальное количество подключений – 1024.

Главным минусом стандарта 100Base-T4 является работа только в полудуплексном режиме, поэтому данный стандарт сегодня используется достаточно редко.

100Base-FX

Стандарт 100Base-FX, принятый в середине 90-х годов прошлого века, стал логическим продолжением стандартов серии 100Base. Он применяется в сетях с топологией «звезда» и использует многомодовый оптоволоконный кабель. На то время, когда разница в стоимости между многомодовым и одномодовым кабелями была значительной, появление данного стандарта произвело настоящий фурор.

Благодаря свойствам оптоволоконного кабеля длина сегмента ограничена лишь уровнем затухания сигнала и мощностью используемых передатчиков, что позволяет добиться скорости передачи данных 100 Мбит/с на достаточно больших расстояниях.

Стандарт 100Base-FX предусматривает соблюдение следующих правил

функционирования сети:

▪ для передачи данных используется многомодовый оптоволоконный кабель;

▪ максимальное расстояние между коммутатором и рабочей станцией или между двумя коммутаторами не должно превышать 412 м в полудуплексном режиме и 2000 м в дуплексном режиме;

▪ все рабочие станции подключаются к центральному управляющему устройству, в роли которого могут выступать концентратор, коммутатор и т. д.;

▪ максимальное количество подключений – 1024.

Особенностью стандарта 100Base-FX является возможность использования очень длинных сегментов кабеля. Даже самые новые сетевые стандарты не могут похвастаться такими показателями с применением многомодового кабеля. Однако сегодня, когда стоимость одномодового кабеля значительно снизилась, использовать многомодовый кабель не имеет особого смысла.

1000Base-LX, 1000Base-CX, 1000Base-LH, 1000Base-SX

Появление стандартов, поддерживающих скорость передачи данных 1 Гбит/с, было лишь делом времени. И вот это случилось: в 1998 году комитет принял стандарт 1000Base-X, объединивший в себе сразу 4 гигабитных стандарта: 1000Base-LX, 1000Base-CX, 1000Base-LH и 1000Base-SX.

При использовании данных стандартов с кабелем «витая пара» возникают определенные проблемы, связанные со слишком сильными наводками между соседними парами проводников, что не позволяет передавать данные на большой скорости, ограничиваясь только четырьмя парами проводников. Что же касается оптоволоконной среды, то ее возможности еще не раскрыты до конца, поэтому именно она представляет наибольший интерес.

Все эти стандарты, кроме 1000Base-CX, подразумевают использование оптоволоконного кабеля в качестве среды передачи данных. При этом в зависимости от стандарта максимальная длина сегмента составляет от 500 (1000Base-SX, многомодовый кабель) до 10 000 м (1000Base-LH, одномодовый кабель).

1000Base-T

1000Base-T – полноценный гигабитный стандарт, который используется в сетях, построенных с применением топологии «звезда» и кабеля «витая пара» выше пятой категории. Поскольку именно эта топология и среда передачи данных получили наибольшее распространение, не удивителен тот факт, что 1000Base-T приходит на смену интегрированному в материнскую плату сетевому контроллеру стандарта 100Base-TX. Это позволяет легко создать гигабитную сеть практически без финансовых вложений даже у себя дома, соединив свои домашние компьютеры.

При передаче данных используются все четыре пары проводников, при этом передача данных ведется на более высокой частоте. Это дает некоторый запас в величине уровня сигнала, что используется для коррекции возникающих ошибок.

Стандарт 1000Base-T требует выполнения следующих условий:

▪ для передачи данных используется неэкранированный кабель «витая пара» 5-й, 6-й и 7-й категорий;

▪ длина кабеля «витая пара», применяемого для подключения рабочей станции, не должна превышать 100 м;

▪ для увеличения радиуса сети может использоваться не более 2 репитеров, при этом

максимальная длина сегмента составляет 205 м;

▪ все рабочие станции подключаются к центральному управляющему устройству, в качестве которого могут применяться концентратор, коммутатор и т. д.;

▪ максимальное количество подключений – 1024.

Переход со стандарта 100Base-TX на 1000Base-T требует только замены оборудования, поскольку очень часто при построении сети используется кабель категории 5e или 6. А это означает, что, изначально правильно запланировав создание сети, вы легко сможете перейти на более высокую скорость передачи данных.

Глава 11
Экзотика: технологии HomePNA и HomePlug

Кроме чисто сетевых способов, которые используются уже достаточно давно, существуют и некоторые, можно сказать, экзотические методы создания сети. Среди них – построение сети с применением стандартов HomePNA и HomePlug.

HomePNA

История появления стандарта HomePNA достаточно проста. Мысль использовать повсеместно проведенную телефонную проводку для создания дешевого способа передачи данных возникла уже давно. Не хватало только знаний и технологий, чтобы это сделать. Кроме того, пугал сам факт использования телефонной проводки в качестве среды передачи данных, ведь ее характеристики могут изменяться, а топология при этом становится все более запутанной. В таких условиях возможность создания более или менее подходящего способа передачи данных была очень сомнительной. Но рано или поздно такой способ должен был быть найден, что вскоре и случилось.

В 1996 году некоторые телекоммуникационные компании, такие как AT&T, 2Wire, Motorola, CopperGate, Scientific Atlanta, K-micro и др., объединились в альянс, получивший название HomePNA (Home Phoneline Networking Alliance). Задачей альянса было продвижение технологий домашних сетей, построенных с применением телефонной проводки или коаксиального кабеля. При этом альянс лишь создает спецификации стандартов, а их стандартизацией занимается международный союз телекоммуникаций ITU (International Telecommunication Union) – известная в телекоммуникационных кругах организация.

Стоит отметить, что HomePNA изначально была ориентирована на обслуживание небольшого количества подключений, что заметно по некоторым ее характеристикам. Именно этот факт и определил возможные сферы ее использования: домашние сети, небольшие офисы, рестораны и кафе и т. п.

Технология HomePNA нашла широкое применение в домашних сетях. Ее часто используют в качестве «последней мили», когда к квартире подводится Ethernet-кабель, устанавливается конвертер Ethernet в HomePNA, а для подключения компьютеров в квартире используется сетевой адаптер HomePNA. Удобство этого способа подключения заключается в том, что подобным образом к одному Ethernet-кабелю можно подключить все компьютеры, находящиеся в квартире.

Существует несколько спецификаций HomePNA, которые мы и рассмотрим ниже.

HomePNA 1.0

Спецификация HomePNA 1.0 была разработана компанией Tut Systems в 1998 году, то есть два года спустя после образования альянса ITU.

Данная спецификация подразумевает использование топологии «звезда» и выполнение следующих правил:

- используется топология «звезда», требующая применение коммутатора;
- в качестве среды передачи данных используется обычная телефонная проводка с двумя проводниками;
- для передачи данных используется диапазон частот 4,5–9,5 МГц, что не мешает работать остальным устройствам, подключенным к линии, например модемам, факсам и т. п.;
- максимальная скорость передачи данных составляет 1 Мбит/с, при этом каждая подключенная точка получает ее в полном объеме;
- возможна работа 25 точек;
- максимальная длина сегмента – 150 м (на практике может быть более 300 м, это зависит только от качества кабеля).

Перспективность спецификации HomePNA 1.0 заставила многих поверить в ее будущее. Тем более что сразу после принятия этого стандарта появилась информация о том, что следующий стандарт будет иметь скорость передачи данных на порядок выше и качество связи при этом будет на очень высоком уровне.

Однако спецификация HomePNA не нашла столь широкого распространения, как ожидалось. Причина кроется в необходимости использования коммутатора для соединения компьютеров в сеть. Это делает ее создание более дорогим и усложняет процесс монтажа сети.

HomePNA 2.0

Можно смело утверждать, что адекватно воспринимать HomePNA как альтернативу существующим сетевым стандартам для построения локальной сети начали именно с появлением данной спецификации в 1999 году. Разработчиком спецификации считается компания Epigram.

Данная спецификация имеет несколько радикальных отличий от версии 1.0, которые сделали ее очень популярной среди «сетевиков».

Основные нововведения HomePNA 2.0:

- используется топология «шина»;
- в качестве среды передачи данных применяется телефонная проводка или коаксиальный кабель. Практика показала, что можно использовать также кабель «витая пара» 5-й категории, радиопроводку и любой кабель, даже не с медными проводниками;
- максимальная скорость передачи данных составляет 10 Мбит/с, при этом скорость передачи данных меняется в зависимости от длины сегмента и качества кабеля и делится между всеми участниками сети;
- поддерживается работа 32 точек;
- максимальная длина сегмента – 350 м (на практике может быть и более 1000 м, что зависит от типа кабеля и установленной аппаратуры);
- для передачи данных используется диапазон частот 4-21 МГц.

Как показала практика, данный стандарт получился очень гибким и функциональным. Особенно впечатляет длина сегмента сети, которая, по результатам некоторых исследований, может превышать 1500 м при использовании специального оборудования.

HomePNA 3.0

Появление спецификации HomePNA 3.0 было встречено с особой радостью: согласно спецификации, скорость передачи данных значительно возросла и составляет 128 Мбит/с. Этот показатель выглядит очень неплохо, особенно если учесть, что для организации локальной сети не нужно ломать стены или проводить дополнительную кабельную систему.

Спецификация 3.0 была принята в 2005 году, ее создателем принято считать Broadcom and Coppergate Communications.

Главными особенностями спецификации HomePNA 3.0 являются следующие:

- в качестве среды передачи данных используется телефонная проводка или коаксиальный кабель;
- максимальная скорость передачи данных составляет 128 Мбит/с;
- максимальная длина сегмента – 350 м;
- поддерживается работа 32 устройств;
- для передачи данных используется диапазон частот 4-36 МГц.

HomePNA 3.1

На сегодняшний день спецификация HomePNA 3.1 является последней и наиболее перспективной. В ней заявлены высокая скорость передачи данных и поддержка работы большего, по сравнению с предыдущими стандартами, количества устройств.

Спецификация HomePNA 3.1 была разработана в 2007 году компанией CopperGate Communications.

Основными показателями спецификации 3.0 являются:

- в качестве среды передачи данных используется телефонная проводка или коаксиальный кабель, применяемый для передачи цифрового сигнала, например спутникового телевидения;
- максимальная скорость передачи данных – 320 Мбит/с;
- максимальная длина сегмента составляет 350 м при использовании телефонной проводки и 600 м – для коаксиального кабеля;
- поддерживается работа 64 устройств;
- для передачи данных используется диапазон частот 4-65 МГц;
- скорость и схема применения частотных каналов автоматически адаптируются в зависимости от зашумленности канала;
- обратная совместимость с оборудованием предыдущих спецификаций;
- невысокая стоимость оборудования.

Как видно, новая спецификация HomePNA вполне заслуживает пристального внимания, тем более что для создания сети не требуется дополнительного оборудования – вполне достаточно любого HomePNA-адаптера.

HomePlug

Выше мы рассмотрели один из экзотических способов объединения компьютеров в локальную сеть, построенную на основе телефонной проводки. Казалось бы, какой помощник из телефонной проводки, если даже телефон иногда отказывается на ней работать? Но оказалось, что все не так плохо, а при определенных условиях очень даже хорошо!

Ниже мы опишем еще одну технологию создания локальной сети, которая по экзотичности даже превосходит предыдущую. Речь пойдет об электрической проводке. Да, именно о той проводке, по которой передается ток переменного напряжения! Казалось бы, передача данных и передача электричества – вещи несовместимые. Но факт остается фактом: большое количество локальных сетей разного размера работают именно по электрической проводке.

Не секрет, что кабель, по которому передается электричество, проложен практически везде, где только может находиться человек. Мало того, к дому, зданию или другому сооружению часто подходит не один, а несколько электрических кабелей, что связано с использованием нескольких электрических фаз или дополнительных линий питания. Поэтому нет ничего странного в том, что о применении этого кабеля для передачи данных задумывались уже давно. Ведь если бы это стало возможным, то создание сети свелось бы к простому подключению «вилки к розетке».

В марте 2000 года был сформирован альянс HomePlug Powerline Alliance, в состав которого вошли многие крупнейшие телекоммуникационные организации, такие как Siemens, Nortel, Motorola и др. Сегодня количество организаций, входящих в альянс HomePlug Powerline Alliance, превышает сотню.

За основу создания новой спецификации были взяты разработки PLC (PowerLine Communication) и DPL (Digital PowerLine), которые велись ранее, в том числе и в России. За десять лет работы и исследований альянс может похвастаться достойным результатом – технологией, позволяющей передавать данные со скоростью 200 Мбит/с по казалось бы безнадежному каналу.

В своей работе оборудование стандарта HomePlug использует диапазон частот 4,5-21 МГц, разделенный на 84 канала. При передаче данных пакеты разбиваются на более мелкие части, и каждая из них передается по отдельному каналу, за счет чего достигается высокая скорость передачи данных. Дойдя до пункта назначения, все части собираются, образуя исходный пакет данных.

Преимущества стандартов HomePlug вполне очевидны: купил адаптер, вставил его в розетку, подключил кабелем к сетевому адаптеру компьютера – и ты в сети. Однако имеются и отрицательные стороны: например необходимость подключения всех адаптеров локальной сети к одной электрической фазе. К ним также относится основной недостаток топологии «шина» – скорость делится между всеми устройствами сети.

HomePlug 1.0

Первая «электрическая» спецификация стандарта HomePlug была разработана и принята уже через год после создания альянса – в середине 2001 года.

Данная спецификация описывает следующие правила функционирования локальной сети:

- в качестве сетевой топологии используется «шина»;
- максимальная скорость передачи данных составляет 14 Мбит/с;
- максимальная длина сегмента составляет 100 м (на практике расстояние может составлять более 1000 м, но при этом уменьшается скорость передачи данных);
- допускается применение репитеров, что позволяет увеличить длину сегмента до 10 000 м;
- используются адаптивные механизмы изменения частоты или отключения определенных каналов при обнаружении сильных помех;
- для шифрования данных используется метод DES с 56-битным ключом шифрования.

Как видите, технические характеристики спецификации HomePlug 1.0 достаточно привлекательны: для подключения к сети достаточно приобрести PowerLine-адаптер, вставить его в розетку и подключить кабелем к Ethernet-адаптеру стандарта 100Base-TX

или ему подобного.

Через некоторое время появилась неофициальная версия HomePlug 1.0 с пометкой Turbo, технические характеристики которой повторяли характеристики HomePlug 1.0 с единственным, но значительным отличием: скорость передачи данных была увеличена до 85 Мбит/с. Этот факт, без преувеличения, стал «путевкой в жизнь» для HomePlug как стандарта для небольших локальных сетей.

HomePlug AV

Принятие в 2005 году спецификации HomePlug AV [3 - Аббревиатура AV указывает на то, что спецификация ориентирована на работу с аудио-и видеосодержимым в режиме реального времени.] стало знаменательным событием, поскольку позволило использовать этот стандарт для работы с большими потоками информации, например видеопотоком в HD-качестве (HDTV). Если проанализировать данную спецификацию детально, то можно заметить, что при ее разработке были пересмотрены большинство подходов, которые применялись при разработке спецификаций HomePlug 1.0 и HomePlug 1.0 Turbo.

Спецификация HomePlug AV имеет следующие возможности:

- максимальная скорость передачи данных составляет 200 Мбит/с;
- передача данных ведется в диапазоне частот 2-28 МГц;
- для шифрования данных используется технология AES со 128-битным ключом шифрования.

Возможности этой спецификации HomePlug позволяют создать сеть в небольшом офисе или дома. Скорости такой сети с запасом хватит для выполнения любых задач вплоть до изначального предназначения спецификации – передачи аудио-и видеосодержимого высокого разрешения.

Глава 12
Особенности проектирования сети

Проектирование сети – очень важный и ответственный этап. От него зависят все технические возможности будущей сети, наиболее критичными из которых являются:

- стоимость создания сети;
- скорость передачи данных;
- количество подключаемых узлов;
- количество активного и пассивного сетевого оборудования;
- простота подключения и обслуживания компьютеров;
- устойчивость к повреждениям и неисправностям и сложность их устранения;
- безопасность работы;
- сложность администрирования сети;
- возможности модернизации сети;
- возможность подключения и поддержки сегментов с другой топологией и способом передачи данных.

Именно поэтому к проектированию сети необходимо отнестись очень тщательно. Торопиться не стоит: неудачный выбор не всегда можно легко поправить, особенно когда дело касается достаточно большой сети…

Потребности – стоимость

Проектирование сети в различных случаях происходит по-разному. Если речь идет о создании локальной сети для большой организации, то все заботы об этом ложатся на фирму-подрядчика, которая занимается созданием локальных сетей на профессиональном уровне и гарантирует отличный результат. Что касается создания локальной сети в пределах небольшой организации, офиса или дома, то задача выбора и проектирования сети ложится на плечи одного-двух человек. В офисах или организациях этим, как правило, занимается штатный программист или системный администратор, а в домашних условиях, естественно, сам хозяин или его друзья. Соответственно, денежные затраты на проектирование сети зависят от задействованных для этого процесса сил.

Очень часто, особенно когда дело касается создания небольшой офисной или домашней сети, процесс проектирования сети опускается, что имеет вполне разумные причины: максимальная экономия средств и использование уже имеющегося оборудования. Например, если в материнской плате каждого компьютера есть интегрированный сетевой адаптер 100Base-TX, то остается только сделать несколько отрезков кабеля нужной длины, купить простенький коммутатор – и сеть готова.

Если же речь идет о создании достаточно большой локальной сети, то ее проектирование происходит обычно в следующем порядке.

1. Определяется количество будущих участников сети. Оно влияет на выбор сетевого стандарта и количество оборудования, необходимого для подключения и организации работы локальной сети.
2. Собираются и анализируются данные о потребностях пользователей. Необходимость выполнения тех или иных задач определяет достаточную скорость передачи данных, а значит, влияет на выбор сетевого стандарта и, соответственно, оборудования.
3. Выбирается сетевой стандарт, который по скоростным характеристикам удовлетворит все потребности и в то же время позволит производить расширение и модернизацию сети.
4. Создается проект будущей сети и определяются количество и тип оборудования. Чем точнее будет составлен проект, тем точнее можно будет подсчитать количество необходимого оборудования. На данном этапе особое внимание следует обратить на пассивное оборудование, так как именно оно влияет на качество, скорость и полноту выполнения работ.

Поскольку данная книга ориентирована на начинающих пользователей, рассматривать процесс проектирования очень сложной сети не имеет смысла, поэтому лишь кратко остановимся на основных моментах.

Итак, прежде всего вам нужно будет определиться по следующим пунктам:

- количество подключаемых компьютеров и других устройств;
- имеющиеся сетевые адаптеры;
- реальная потребность пользователей в скорости передачи данных;
- потребности в администрировании сети;
- будущий сетевой стандарт;
- качество построения сети.

Анализ этих данных позволит вам узнать самое важное – приблизительную стоимость создания сети. Финансовые затраты в основном зависят:

- от количества подключаемых компьютеров и наличия в них сетевых адаптеров;
- количества оборудования и расходных материалов, которые придется дополнительно приобрести;
- стоимости выполнения работ, если для этого привлекаются сторонние люди или организации.

Выбор сетевого стандарта

Выбор сетевого стандарта очень важен, когда планируется создание локальной сети с подключением разнородных сегментов или требуется создать сеть с минимальным количеством выполняемых работ. Например, если нужно создать сеть в офисе или дома и не хочется при этом портить интерьер лишними проводами и коробками, то всегда можно выбрать вариант без проводов или с минимальным их количеством.

В табл. 12.1 приведены основные показатели разных сетевых стандартов. Проанализируйте их еще раз, чтобы определиться с выбором.

Таблица 12.1.Сравнение основных сетевых стандартов

Сетевой стандарт	Среда передачи данных	Скорость передачи данных, Мбит/с	Максимальное количество подключений	Максимальная дальность связи, м
10Base-5	Коаксиальный кабель	10	500	2500
10Base-2	Коаксиальный кабель	10	150	925
10Base-T	«Витая пара»	10	1024	500
10Base-F	Оптоволокно	10	1024	5000
100Base-TX	«Витая пара»	100	1024	205
100Base-T4	«Витая пара»	100	1024	205
100Base-FX	Оптоволокно	100	1024	2000
1000Base-T	«Витая пара»	1000	1024	205
HomePNA 3.1	Телефонная проводка, коаксиальный кабель	320	64	600
HomePlug AV	Электропроводка	200	64	300

Как показывает практика, в большинстве случаев выбор останавливают на одном из современных проводных вариантов, например 100Base-TX или 1000Base-T. Причина этого выбора очень проста и не раз уже упоминалась ранее: любая современная материнская плата уже содержит в своем составе сетевой адаптер стандарта 100Base-TX или 1000Base-T, что позволяет сэкономить на покупке сетевых адаптеров и сосредоточить свое внимание на выборе активного оборудования и расходных материалов.

В последнее время, когда речь идет о локальных сетях в пределах небольшого помещения (офиса, квартиры и т. п.), часто используют один из беспроводных сетевых стандартов, которые позволяют вообще отказаться от каких-либо кабелей.

Конечно, находят свое применение и спецификации HomePNA и HomePlug. Но к ним в основном обращаются только в тех случаях, когда никакое другое решение не подходит.

Проектирование сети

После того как определены потребности сети, известно количество компьютеров и других устройств и, самое главное, выбран сетевой стандарт, можно переходить к последнему, но не менее важному этапу – подготовке проекта.

Проект локальной сети представляет собой чертеж, отражающий расположение рабочих мест и других объектов на плане помещения (комнаты), в котором будет создаваться сеть. При этом чем точнее будет чертеж, тем точнее можно будет рассчитать необходимое количество расходных материалов.

Такое точное проектирование необходимо, как правило, только в случае создания большой сети. Если же вы планируете провести сеть у себя дома или в офисе и особенно если у вас еще нет такого опыта, то необходимости в проекте нет. Однако полезно будет узнать некоторые принципы его создания.

Основная задача проекта – показать, как и где будет проходить кабель, а также будет расположено активное оборудование, включая компьютеры. Это позволяет с достаточно большой точностью рассчитать количество кабеля, розеток, коробов и других расходных материалов.

Основу проекта составляет топология сети, поскольку от нее зависят количество кабельных магистралей и правила их прокладки. Например, в случае использования топологии «шина» кабельная магистраль будет состоять из одного кабеля и небольших отводов. Если же будет использоваться топология «звезда», количество кабельных сегментов зависит от количества подключаемых компьютеров.

Чтобы было понятнее, рассмотрим в качестве примера способы создания проекта для случаев использования коаксиального кабеля и кабеля «витая пара».

Коаксиальный кабель

Как вы уже знаете, коаксиальный кабель применяется для создания сети с топологией «шина» или сегмента с топологией «шина», который может подключаться к сети с другой топологией.

Использование коаксиального кабеля в качестве среды передачи данных делает проектирование сети достаточно простым. Такая сеть подразумевает использование одной центральной магистрали, от которой к компьютерам или другим устройствам делается отвод. По этой причине главный вопрос, который необходимо решить, – где можно проложить центральный кабель, чтобы это оказалось оптимальным для подключения компьютеров и потребовало меньших затрат кабеля.

Существует два подхода к прокладыванию центральной магистрали:

- использовать для подключения компьютеров отводы небольшой длины, что предусмотрено стандартами;
- применить для подключения компьютера петлю из центральной магистрали.

Первый вариант более практичный, поскольку в этом случае центральная магистраль жестко фиксируется с помощью скоб или в коробе. В определенных местах магистрали врезается Т-коннектор, который в дальнейшем служит местом подключения отвода к точке.

Второй вариант подразумевает риск обрыва центральной магистрали, а это происходит достаточно часто, например когда производят перестановку компьютера, не отключив предварительно кабель.

Если планируется подключение компьютеров в небольшом помещении, то лучше воспользоваться вторым способом: зафиксировать центральную магистраль по всей длине и сделать петлю с некоторым запасом, чтобы предусмотреть возможность перемещения компьютеров.

Еще один важный вопрос – расположение центральной магистрали. В идеале кабель должен размещаться так, чтобы исключить возможность его повреждения или обрыва, электромагнитных наводок, тепло– и гидровлияния и т. п., то есть необходимо обеспечить максимально комфортные условия. Конечно, идеала добиться тяжело, ведь у каждого помещения свои особенности проектировки и расположения всевозможных кабелей. Тем не менее можно найти место, которое максимально удовлетворяет этим условиям.

Как показала практика, проводить кабель, в том числе и коаксиальный, очень удобно рядом с плинтусом или на небольшом удалении от него. В таком размещении можно выделить следующие положительные стороны:

▪ как правило, отсутствует проводка других кабелей, за исключением перпендикулярного канала, идущего вниз или вверх к розеткам, который очень просто обойти;

▪ ничего не мешает фиксации кабеля: как с помощью скоб, так и с использованием специальных коробов;

▪ минимальное влияние влажности, особенно если кабель будет находиться в коробе.

Если требуется выполнить проводку в нескольких помещениях, разделенных перегородкой, то в ней проделывают сквозные отверстия либо используют уже существующие. Места таких отверстий выбираются исходя из особенностей проводки кабеля или оптимального пути его расположения. Поэтому прежде всего необходимо проанализировать расположение компьютеров в комнате и возможность их перестановки. После этого и выбирается место для межкомнатных отверстий, например, параллельно дальней или ближней от входа стене в районе плинтуса.

Когда все нюансы учтены, можно переходить непосредственно к составлению проекта на бумаге.

Сначала на рисунок наносится центральная магистраль, затем обозначаются отверстия в стене и точки подключения рабочих мест. Затем проставляются размеры сегментов кабеля, чтобы в дальнейшем можно было узнать общую протяженность сети. В конце ставятся условные обозначения компьютеров с пометками об их важности, а также их нумерация. Она пригодится, когда необходимо будет произвести IP-адресацию компьютеров.

Кабель «витая пара»

Кабель «витая пара» стал самой популярной средой передачи данных в локальных сетях. Этому есть логичное объяснение: современные стандарты, основанные на использовании этого кабеля, позволяют получить локальную сеть с техническими характеристиками, которые полностью удовлетворяют современным потребностям. К тому же такая сеть легко расширяется без ущерба для скорости передачи данных.

Проектирование сети с применением кабеля «витая пара» имеет некоторые особенности, связанные со спецификой топологии «звезда». Эта топология требует подключать каждый компьютер отдельным сегментом кабеля, а затем все сегменты подключаются к центральному управляющему устройству. Подобные нюансы необходимо заранее предусмотреть при проектировании сети.

Упрощенная схема проектирования может быть следующей.

1. Выбираем место расположения центрального устройства или монтажного шкафа.

2. Отмечаем местоположение компьютеров и других устройств, требующих отдельного подключения, то есть и отдельного сегмента.

3. Определяем оптимальный путь прокладывания кабельных сегментов.

Когда речь идет о создании локальной сети в большом офисе, задачу проектирования часто облегчает наличие комнаты, которая отводится под компьютерные коммуникации. В этом случае такая комната автоматически превращается в центральный узел, от которого будут расходиться все сегменты кабеля.

Для небольшого офиса использование монтажного шкафа является неоправданным, поскольку его стоимость может быть равной стоимости монтажа всей сети. Поэтому часто центральное устройство располагается в любом подходящем для этого месте.

Для большой сети использование монтажного шкафа является обязательным, поскольку это значительно упрощает монтаж активных устройств и дальнейший контроль над ними.

Что касается использования таких расходных материалов, как монтажные коробы и сетевые розетки, то опять же все упирается в «размах» сети. Использование этих элементов всегда приветствуется, но на практике они используются только в офисах, чтобы не портить интерьер комнат висящими проводами. В домашних условиях использование этих атрибутов сети не практикуется по понятным причинам.

После того как все нюансы приняты во внимание, можно переходить к созданию бумажного проекта. Принципы его составления не отличаются от принципов проектирования с использованием коаксиального кабеля (см. выше).

Глава 13
Строим сеть: коаксиальный кабель

Сеть, использующая коаксиальный кабель для передачи данных, является одним из самых старых и простых вариантов сети. Для ее создания, как уже было упомянуто ранее, используется сетевой коаксиальный кабель с волновым сопротивлением 50 Ом. Кабель может быть различного диаметра, который определяется выбранным сетевым стандартом.

Использование коаксиального кабеля означает использование топологии «шина». При этом все компьютеры подключаются к общей магистрали, отводы от которой создаются с помощью специального разъема – Т-коннектора.

Если проводить аналогию с сетью, использующей кабель «витая пара», то Т-коннектор играет ту же роль, что и сетевая розетка. И к первому, и ко второй присоединяются отрезки кабеля, соединяющие сетевые карты компьютеров с главным сетевым кабелем или центральным устройством. Каждый такой кабель обжимается с двух сторон коннектором BNC-типа.

Сеть, построенная с применением коаксиального кабеля, сегодня встречается редко. Причинами этого являются низкая скорость сети (10 Мбит/с) и отсутствие необходимого сетевого оборудования. Однако она отлично прижилась на различных предприятиях, особенности процессов которых не требуют высокой скорости обмена данными и, самое главное, использования современного оборудования.

Правила прокладки кабеля

Использование коаксиального кабеля для монтажа сети имеет достаточно много особенностей, обусловленных спецификацией сетевого стандарта. Например, чтобы подключить рабочее место к коаксиальному кабелю, необходимо разделить центральную магистраль на две части и установить специальный отвод, к которому и подключается компьютер. Наличие подобных отводов уменьшает надежность кабеля, и чем больше их будет, тем ниже будет физическая устойчивость к обрыву. Все это требует соблюдения соответствующих правил и принципов прокладки и монтажа кабеля. В противном случае качественная и бесперебойная работа локальной сети не гарантируется.

Итак, при прокладке кабеля старайтесь придерживаться следующих правил. Это позволит обезопасить вашу сеть от выхода из строя и предотвратить возникновение сбоев.

1. Обдуманно выбирайте место прокладки кабеля. Не забывайте, что главным элементом сети на основе коаксиального кабеля является ее носитель – сам кабель. Если произойдет обрыв центрального кабеля, то вся сеть перестанет функционировать. По этой причине кабель должен быть проложен в месте, которое гарантирует его максимальную защиту. Если вы не выбрали место прокладки кабеля на этапе проектирования, то самое время

сделать это сейчас.

2. Не допускайте сильного натяжения кабеля. Кабельная магистраль локальной сети не является цельной структурой, а состоит из цепи последовательно соединенных отрезков кабеля, поэтому любое натяжение кабеля может негативно сказаться на работоспособности сети. Наиболее критичными участками, конечно же, являются места соединения кабеля с коннекторами.

ВНИМАНИЕ

Нарушение целостности контактов или обрыв кабеля приводит к нестабильной работе сети или полному выходу ее из строя. Обнаружить проблемное место в этом случае может быть очень сложно.

Не забудьте о необходимости обеспечить целостность, если вам придется прокладывать кабель между двумя домами или на открытом пространстве. В этом случае в качестве основы используйте толстую стальную проволоку. Когда проволока будет натянута и закреплена между стенами домов или другими объектами, можно закрепить на ней коаксиальный кабель с помощью стальных или жестяных хомутиков. Это простое приспособление защитит кабельную систему от обрыва, который может произойти, например, при сильном ветре.

3. Избегайте создания лишних петель кабеля. Каждая лишняя петля кабеля не только уменьшает полезную длину сегмента, но и создает электрические наводки, особенно если лишний кабель проложен хаотично или сложен петлями. Если нет возможности избавиться от петли, просто натянув центральный кабель, то можно использовать следующий подход.

1. Обрежьте кабель ближе к началу образования петли.
2. Используя обжимной инструмент, закрепите на конце кабеля BNC-коннектор.
3. Обрежьте кабель ближе к концу петли таким образом, чтобы конец кабеля доставал до BNC-коннектора и оставалось еще примерно 15–20 см.
4. С помощью обжимного инструмента закрепите на конце кабеля BNC-коннектор.
5. Для соединения двух BNC-коннекторов используйте I-коннектор.

В результате вы не только уберете лишнюю петлю кабеля, но и оставите возможность через некоторое время заменить I-коннектор на T-коннектор и подключить еще одно рабочее место.

4. Следите за изгибами кабеля. Прокладку кабеля часто осложняют участки, которые требуют обхода препятствий и соответственных изгибов кабеля. Поэтому, если есть необходимость в изгибе, обязательно придерживайтесь следующего правила: минимальный изгиб равен 10 радиусам кабеля.

Это означает, что если вы используете толстый коаксиальный кабель, диаметр которого примерно 1 см, то минимальный изгиб кабеля должен быть не менее 10 см. Если же применяете тонкий коаксиальный кабель, диаметр которого примерно 0,5 см, то изгиб должен быть не менее 5 см.

Несоблюдение этого простого правила часто приводит к тому, что кабель повреждается на участках изгиба, а это делает его дальнейшее использование невозможным.

5. Избегайте прокладки кабеля возле проводов электропитания и электрощитов.

Электрическая проводка – мощнейший источник электрических наводок, которые создают помехи для нормального прохождения сигнала по любому кабелю, в том числе и по коаксиальному. По этой причине если на пути следования кабеля встречается длинный участок электропроводки, то лучше обойти его, проложив кабель ниже или выше этого участка. Этим вы, конечно, увеличите общую длину кабельной магистрали, зато избавитесь от электрических наводок, которые могут повлиять на работоспособность сети.

6. Избегайте прокладки кабеля возле отопительных конструкций. Аналогично

электропроводке нагрев кабеля также вносит изменения в среду передачи данных. Изменение сопротивления центрального проводника коаксиального кабеля может привести к нестабильной работе сети. Поэтому старайтесь не прокладывать кабель рядом с батареями отопления. Если обойти опасный участок невозможно, используйте пластиковый короб, который позволит защитить кабель от воздействия высокой температуры.

7. Используйте специальные пластиковые коробы и трубы. Данное правило особенно актуально, если кабель нужно проложить под землей или на открытом воздухе.

Как известно, в земле вещества разлагаются, и хотя скорость разложения кабеля небольшая, однако в определенных условиях (постоянная влажность земли, ее минеральный и химический состав и т. д.) она может значительно ускориться.

Негативно влияет внешняя окружающая среда и на кабель, проведенный на открытом воздухе. Постоянная смена погоды, дождь и солнце, налипание снега и мороз значительно сокращают срок службы кабельной системы.

Таким образом, чтобы максимально уменьшить вред, наносимый кабелю внешней средой, желательно использовать дополнительную защиту – специальные пластиковые коробы или трубы.

Крепление коробов

Если решено использовать пластиковые коробы для прокладки кабеля, то, прежде чем приступать к обработке кабеля, их необходимо закрепить.

Сечение короба зависит от диаметра и количества кабелей, которые будут в нем скрыты. Даже если количество разных кабелей (сетевой, телефонный, сигнализирующий и т. д.) на разных участках локальной сети неодинаково, не стоит особенно переживать по этому поводу: существуют переходники всевозможных размеров, позволяющие соединять коробы разного сечения.

Крепление короба зависит от его сечения и от того, куда он будет крепиться. Как правило, для крепления используются шурупы определенного размера (подбираются исходя из сечения короба). Если же внутреннее сечение короба небольшое и он должен крепиться к гладкой стене, не покрытой составом на основе песка, часто используется двухсторонний скотч. Но если структура покрытия стены другая, то без шурупов уже не обойтись.

Крепление шурупами, конечно, наиболее предпочтительно, поскольку обеспечивает более плотный контакт со стеной. Это в свою очередь дает возможность открыть уже закрытый короб, чтобы провести дополнительный вид кабеля.

Чтобы обеспечить хорошее крепление, шурупы должны располагаться на расстоянии не более 50 см друг от друга. Если же особенности стены не позволяют осуществить нормальное прокладывание короба, частота размещения шурупов может увеличиваться, что только улучшит качество крепления.

Короб представляет собой составную конструкцию. При этом для крепления используется только одна из частей – нижняя. На ней присутствует замок, с помощью которого внешняя часть короба фиксируется на нижней части.

Стандартная длина короба обычно не превышает 4 м, что связано со сложностью его транспортировки. Поэтому если вам потребуется короб длиной более 4 м, то придется компоновать его из нескольких частей. Этого не стоит бояться, поскольку место соединения коробов можно скрыть с помощью внешней части, которая подбирается таким образом, чтобы соединять два соседних короба. В результате весь короб выглядит цельным.

Подготовка кабеля

Для прокладывания сети используется коаксиальный кабель с волновым сопротивлением 50 Ом. Внешне он неотличим от обычного телевизионного кабеля, однако путать их нельзя: телевизионный кабель имеет волновое сопротивление 75 Ом и при его использовании сеть функционировать не будет.

Как вы уже знаете, для прокладки сети стандарта 10Base-2 применяется тонкий коаксиальный кабель. Однако это совсем не означает, что вы не можете использовать толстый коаксиальный кабель. Часто на практике для соединения двух отдаленных сегментов сети применяется именно толстый коаксиальный кабель, поскольку его длина в этом случае может быть большей.

Теперь можно приступать к работе. Вспомним принципы построения сети на основе коаксиального кабеля.

▪ Центральная магистраль кабеля с обоих концов требует использования специальных коннекторов – терминаторов, которые используются для предотвращения дальнейшего распространения и возможного эффекта отбитого сигнала. При этом один из терминаторов обязательно должен быть заземлен.

▪ Для подключения рабочего места к центральной магистрали применяется специальный коннектор (Т-коннектор), имеющий отвод для подключения к разъему на сетевой карте компьютера. Для установки Т-коннектора центральный кабель разрезают и обжимают BNC-коннекторами, которые обеспечивают целостность центрального кабеля и дают возможность подключить компьютер к сети.

▪ Если произошло разрушение центральной магистрали, например ее физический обрыв, для восстановления целостности кабельной системы применяются два BNC-коннектора и I-коннектор: коннекторы обжимаются и соединяются с помощью I-коннектора.

Как уже упоминалось ранее, существует два подхода в прокладке кабеля.

▪ Сначала прокладывается вся центральная магистраль, а затем подключается каждое рабочее место.

▪ Центральная магистраль формируется путем последовательного подключения рабочих мест.

По нескольким причинам второй подход в прокладке кабеля более предпочтителен, поэтому рассмотрим его более детально.

Основная ваша задача – подготовить отрезки кабеля необходимой длины и обжать их коннекторами. При подготовке кабеля необходимо придерживаться правил прокладки кабеля, которые однозначно влияют на его длину.

Подготовку отрезков кабеля необходимо производить, начиная с самого дальнего компьютера.

Отмерьте отрезок кабеля от этого компьютера до соседнего с учетом всех особенностей пути или ориентируясь на закрепленный заранее короб, затем обрежьте его. Для этого воспользуйтесь обрезным инструментом (рис. 13.1) или обычными ножницами.

Далее необходимо обжать кабель, и на этом создание кабеля для подключения одного рабочего места заканчивается.

Многие предпочитают сразу же зафиксировать кабель в коробе или с помощью скоб. Делать этого не стоит, поскольку, закрепив кабель, вы не сможете регулировать его длину, если это понадобится.

После того как произведен обжим кабеля, можно приступать к подготовке следующего отрезка по описанной выше схеме.

Подготовив нужное количество отрезков кабеля рассчитанной длины, продолжите дальнейшую подготовку.

Монтаж разъемов BNC

После подготовки отрезка кабеля можно переходить к обжиму BNC-коннекторов.

Различают три вида BNC-коннекторов, каждый из которых имеет свои преимущества и недостатки.

▪ Обжимные коннекторы. Данный тип наиболее распространен. Основные преимущества обжимных коннекторов – обеспечение надежного контакта и легкость обжима. Недостаток – одноразовость: в случае обрыва провода требуется новый коннектор, поскольку старый из-за полученных при обжиме деформаций применять уже невозможно. Для обжима такого типа коннекторов используется специальный обжимной инструмент. При некоторой сноровке можно применять и обычные плоскогубцы, но качество обжима в таком случае оставляет желать лучшего.

▪ Накручивающиеся коннекторы. Такие коннекторы обеспечивают простоту монтажа, так как для этого не нужны дополнительные инструменты. Однако они очень чувствительны к натяжению кабеля, из-за чего происходит нарушение контакта и, как следствие, нарушается работоспособность локальной сети.

▪ Коннекторы под пайку. Для установки коннектора требуются паяльник и припой. Недостатком является сложность, требующая опыта проведения паяльных работ. Нарушение контакта в случае плохой пропайки контактов приводит к постоянным сбоям сети, а само место пропадания контакта найти очень трудно.

Как уже было упомянуто, сегодня в основном используются только обжимные коннекторы. Алгоритм обжима такого BNC-коннектора следующий.

1. Обрезать конец кабеля, используя обрезной инструмент.
2. Надеть на кабель обжимную трубку и центральный сердечник из латуни и обжать сердечник.
3. Надеть корпус коннектора и зафиксировать его под внешней изоляцией кабеля.
4. Используя инструмент, обжать коннектор.

Теперь рассмотрим каждый пункт подробнее.

Обрезка кабеля

Подготовка кабеля заключается в его правильной обрезке и зачистке центрального проводника и экранирующей оплетки.

Обрезать кабель старайтесь аккуратно, чтобы обрез получился ровным – это избавит вас от повторного обрезания и, как следствие, уменьшения длины сегмента.

Далее необходимо снять внешнюю изоляцию и диэлектрик на центральном проводнике, для чего используется обрезной инструмент. Для этого откройте инструмент (нажав на среднюю часть, вы поднимете верхнюю, освободив отверстие, в которое нужно вставить кабель) и вставьте в него конец кабеля. Делайте это с таким расчетом, чтобы с правой стороны инструмента торчал кусок кабеля длиной 2–4 мм. После этого выполните два-три поворота по часовой стрелке вокруг оси кабеля.

Затем движением инструмента вправо снимите обрезанную часть внешней оболочки. В результате должно быть снято примерно 25 мм внешней оболочки и до 10 мм диэлектрика вместе с окружающим его экраном (рис. 13.2).

Если с первого раза не получилось, повторите процесс, но не забывайте, что каждая неудачная обрезка уменьшает длину сегмента.

Обжим сердечника

После того как кабель обрезан, можно приступить к работе с коннектором. Начать нужно с установки трубки и обжима сердечника.

Прежде всего необходимо надеть обжимную трубку – основной компонент коннектора, который и позволяет обжать его, то есть надежно зафиксировать на кабеле.

Далее переходим к сердечнику. Ваша задача – определить необходимую длину центрального проводника и, надев на него сердечник, обжать его.

Прежде чем обжать сердечник, необходимо надеть его на центральный проводник и «примерить» коннектор. Это делается для того, чтобы добиться оптимальной длины выступа сердечника из коннектора. Если сердечник будет выступать недостаточно, качество контакта с Т-коннектором будет плохим, что может стать причиной неработоспособности сети, причем обнаружить источник проблемы будет крайне тяжело.

Если после «примерки» вы визуально определили, что центральный проводник слишком длинный, то его необходимо укоротить при помощи резака или ножниц. Если же сердечник выступает недостаточно, нужно укоротить длину диэлектрика либо повторно обрезать кабель.

После того как оптимальная длина центрального проводника подобрана, необходимо обжать сердечник, для чего используется обжимной инструмент. Обратите внимание, что на обжимной части инструмента имеется специальный вырез, в который необходимо установить кабель с сердечником. Убедившись в том, что центральный проводник вставлен в сердечник до упора, произведите обжим (рис. 13.3).

Для этого сожмите ручки инструмента до щелчка, который будет свидетельствовать о том, что обжим произведен и инструмент вернулся в прежнее состояние. В противном случае ручки инструмента останутся сведенными и вытянуть кабель не получится.

После того как обжим завершен, проконтролируйте качество работы. Если есть малейшее подозрение, что обжим произведен плохо, обязательно повторите процесс.

Обжим коннектора

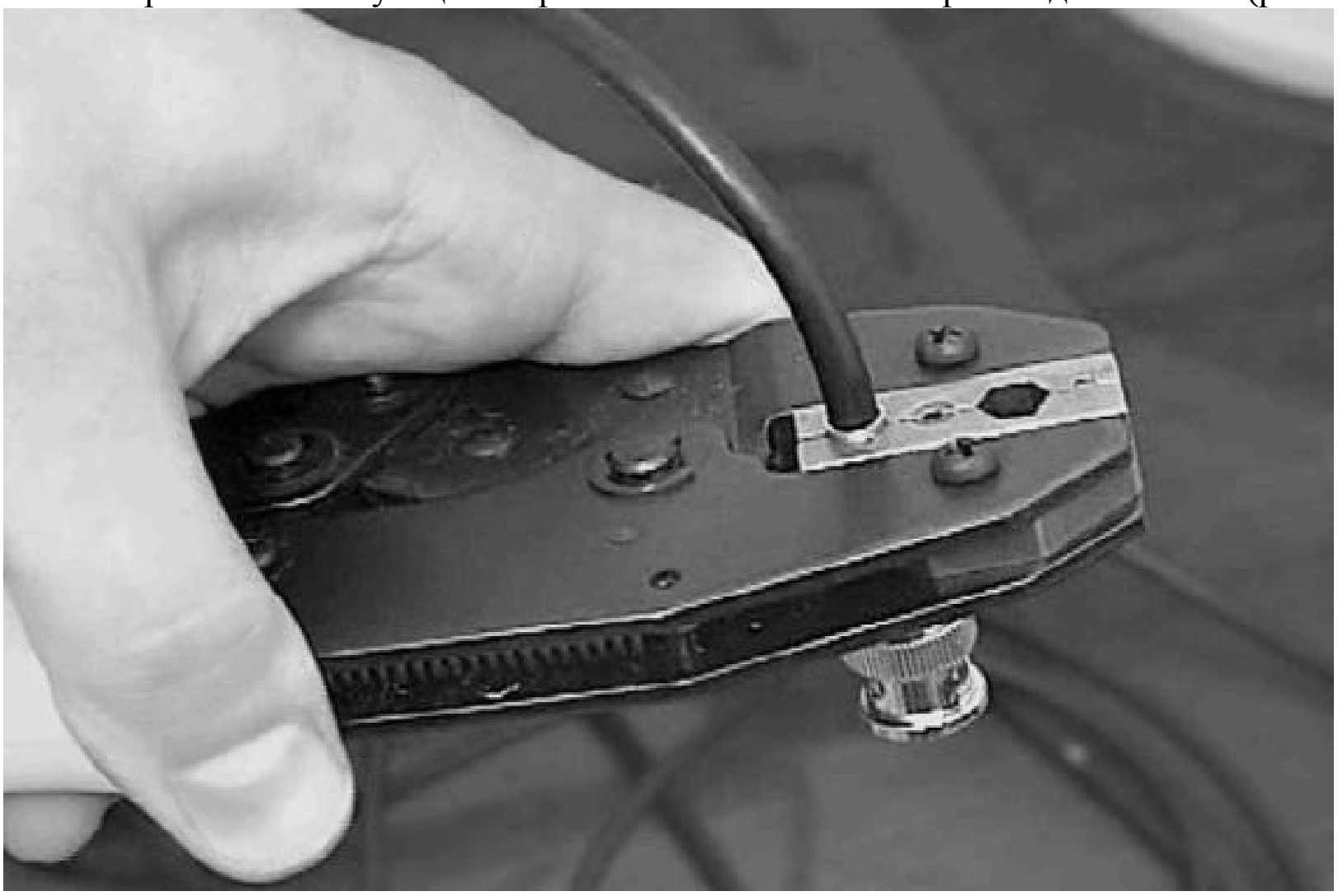
После обжима сердечника аккуратно расплетите экранирующую оплетку и наденьте корпус коннектора таким образом, чтобы конец корпуса оказался под оплеткой.

При этом есть один нюанс, который обязательно нужно проконтролировать. На качество обжима коннектора сильно влияет толщина используемого кабеля. Если кабель слишком тонкий, то, чтобы получить более качественный обжим, может потребоваться задвинуть выступающую часть коннектора под внешнюю изоляцию. Определить, требуются ли такие меры, достаточно просто: установите обжимную трубку на ее «законное» место и проследите за тем, насколько легко это происходит. Если очень легко, то кабель слишком тонкий, а значит, необходимо выполнить описанные выше действия.

После того как коннектор установлен на место, равномерно распределите экранирующую оплетку по всей поверхности торца корпуса разъема. Затем наденьте обжимную трубку до упора на торец корпуса таким образом, чтобы она накрыла медный

экран.

Осталось только произвести обжим. Для этого возьмите в руки инструмент, установите коннектор в соответствующий вырез и сильным сжатием произведите обжим (рис. 13.4).



Как и в случае с обжимом сердечника, процесс обжима коннектора должен завершиться щелчком, который возвращает инструмент в рабочее положение.

Затем описанным способом необходимо произвести обжим второго конца кабеля, чтобы завершить подготовку сегмента.

Подключение коннекторов

Когда обжим кабеля закончен, необходимо подключить коннекторы. Это позволяет не только завершить подключение конкретного рабочего места, но и привести в порядок центральный кабель, то есть убрать его излишки.

Подключение коннекторов не вызывает никаких проблем и позволяет лишний раз проконтролировать качество обжима кабеля. При выявлении некачественной работы лучше сразу повторить обжим, чем после подключения компьютеров лихорадочно искать причину нестабильной работы сети.

На готовый отрезок кабеля необходимо установить Т-коннектор, с помощью которого и будет производиться подключение рабочего места. Конструкция Т-коннектора предполагает только один способ подключения, поэтому ошибиться невозможно.

Если речь идет о крайнем отрезке кабеля, то есть отрезке, с помощью которого подключается крайнее рабочее место, то, согласно стандартам, дополнительно требуется подключить терминатор. Конструкция терминатора также очень проста, что исключает возможность неправильного его подключения.

Когда монтаж сети будет закончен, прежде чем подключать рабочие места, необходимо будет заземлить один из терминаторов. Если этого не сделать, работа сети может оказаться под угрозой, о чем свидетельствуют примеры выгорания сетевого оборудования (выходят из строя компоненты входного тракта).

Фиксация коробов

Фиксация коробов – завершающий этап монтажа локальной сети. На этом этапе вам предстоит подобрать нужную длину внешней части короба, предусмотрев участки для подключения отводов к рабочим местам.

Как обычно, начать работу следует с самой дальней точки.

Конец кабеля, равный примерно 50 см, необходимо оставить торчащим из крайней точки короба, чтобы в дальнейшем можно было использовать его для подключения новых сегментов сети. Далее, измерив нужную длину крышки с расчетом, чтобы из короба осталась торчать петля необходимой длины или Т-коннектор с небольшим запасом кабеля, следует отрезать необходимую часть.

После этого нужно поместить коаксиальный кабель (и другие типы кабелей, если это было предусмотрено сечением короба) в короб и установить крышку на место, добившись срабатывания замка. Подобным образом необходимо поступить со всеми остальными прямолинейными участками сети.

Переходники и уголки используются в местах, где нужно обойти препятствия. При этом кабель на участках изгиба должен быть натянут в меньшей степени, чем на остальных участках сети (не забывайте о минимальном радиусе изгиба!).

Глава 14
Строим сеть: «витая пара»

Сеть, построенная с применением кабеля «витая пара», – самый распространенный тип сети, используемый как для малых, так и для больших локальных сетей. Особенно популярен он для организации сети в домашних условиях, поскольку наличие на материнской плате интегрированного сетевого адаптера часто позволяет свести создание такой сети только к обжиму кабеля нужной длины.

Основными причинами популярности локальной сети с использованием этого типа кабеля стали высокая скорость передачи данных и уже упоминавшийся стандарт ATX, который подразумевает наличие сетевого адаптера на материнской плате. Причем стандартом предусмотрено присутствие сетевого адаптера именно одного из стандартов, использующих кабель «витая пара», например 100Base-TX и даже 1000Base-T.

Правила прокладки кабеля

Чтобы сеть работала без сбоев, при прокладке кабеля нужно придерживаться простых правил.

▪ Правильно выберите место прокладки кабеля. Старайтесь исключить ситуации, когда

на кабель можно случайно наступить, ведь он при этом может деформироваться, перетереться и даже оборваться, что приведет к выходу из строя целого сегмента сети. На кабель также нельзя ставить тяжелые предметы.

▪ Исключите натяжение кабеля. Излишнее натяжение может привести к обрыву кабеля возле коннектора, что также выведет из строя сегмент сети. Кроме того, перепрыгивать через натянутый шнур не понравится ни вам самим, ни уж точно вашему шефу. Это же правило относится и к случаю, когда нужно проложить кабель между двумя домами. Используйте для этого стальной трос, прикрепив к нему на одинаковом расстоянии друг от друга хомуты, которыми будет удерживаться кабель.

▪ Исключите скопление кабеля. Чрезмерное скопление кабеля в одном месте, например сложенный кругами лишний отрезок кабеля, может вызвать в нем электрические наводки и стать причиной появления коллизий.

▪ Соблюдайте правила изгиба кабеля. Рано или поздно при прокладке кабеля наступает момент, когда нужно придать кабелю изгиб. Это частое явление, поскольку в любом помещении есть участки, которые необходимо обходить. В этом случае следует помнить, что радиус изгиба кабеля «витая пара» должен быть не менее 4–5 см.

▪ Избегайте прокладки кабеля возле электрощитов. Электролинии и электрощиты способствуют возникновению электрических наводок в кабеле, что приводит к появлению коллизий.

▪ Не прокладывайте кабель возле отопительных элементов. Батарея центрального отопления и другие теплогенерирующие приборы отрицательно влияют на кабель. Излишний нагрев может вызвать изменения в сопротивлении кабеля, из-за чего также могут возникнуть коллизии. Если нет возможности обойти препятствие или это связано с рядом проблем, используйте дополнительные средства защиты кабеля, например пластиковый короб.

Соблюдая эти простые правила, можно начинать построение сети. Прежде всего, подготовьте кабель, затем произведите обжим коннекторов. После этого можно подключать их к сетевым картам, подсоединяя кабель непосредственно к разъемам на сетевых картах или используя для этого сетевые розетки.

Прокладка и монтаж коробов

Использование пластиковых коробов – вынужденная мера, однако она позволяет сделать локальную сеть более защищенной. Причиной тому является требование стандарта: каждое рабочее место подключается отдельным кабелем. А это означает, что без коробов вы получите неконтролируемое скопление кабеля, которое явно не улучшит дизайн помещения.

Если планируется создание сети с небольшим количеством рабочих мест, использование коробов часто игнорируют и применяют другой способ фиксации кабелей. Еще реже используются коробы в домашних условиях, когда требуется соединить близко расположенные домашние компьютеры.

ПРИМЕЧАНИЕ

Многие пользователи, запланировавшие появление локальной сети в домашних условиях, прокладывают кабель на этапе ремонта помещений, вместе с телефонным и электрическим кабелями.

Если принято решение об использовании коробов, то их прокладка должна осуществляться согласно созданному проекту сети, иначе стоимость сети может превысить ожидаемую.

Как уже упоминалось, создание большой локальной сети принято доверять

профессионалам, и это вполне оправданно. У подобных организаций есть не только соответствующий опыт, но и, самое главное, специальное оборудование, с помощью которого можно обследовать будущую магистраль на наличие разного рода проводки.

При работе же в небольшом офисе вполне можно обойтись собственными силами, не прибегая даже к соответствующему оборудованию.

В отличие от сети с применением коаксиального кабеля, сеть с кабелем «витая пара» при своем монтаже часто требует использования коробов с разным внутренним сечением: коробы с большим сечением применяются при монтаже ближе к центральному управляющему узлу, коробы с меньшим сечением – в непосредственной близости от компьютеров. При этом чем дальше вы будете отходить от центрального узла, тем меньше по сечению будут использоваться коробы, что вполне объясняется особенностями топологии «звезда».

При креплении коробов к стене практически всегда используются шурупы. Это обусловливается весом короба и его сечением. Чем больше короб, тем плотнее должны располагаться шурупы или же должны использоваться шурупы большего размера.

Прежде чем приступить к монтажу коробов, необходимо определить, короб какого сечения должен находиться на каждом участке сети. Если такой анализ был проведен на этапе проектирования, то можно воспользоваться этими данными, в противном случае необходимо выполнить такой анализ сейчас.

К сожалению, стандартная длина короба ограничена, поэтому для получения нужной длины придется использовать несколько отрезков короба. В местах изгибов крепление коробов необходимо производить более тщательно и аккуратно, применяя для этого больше шурупов, чем обычно.

При стыковке коробов разного сечения следует учитывать строение переходника, чтобы потом можно было легко захлопнуть крышку на замке короба. Если этого вовремя не сделать, то потом нужно будет обрезать уже закрепленный короб, что связано с рядом неудобств.

Прокладка кабеля

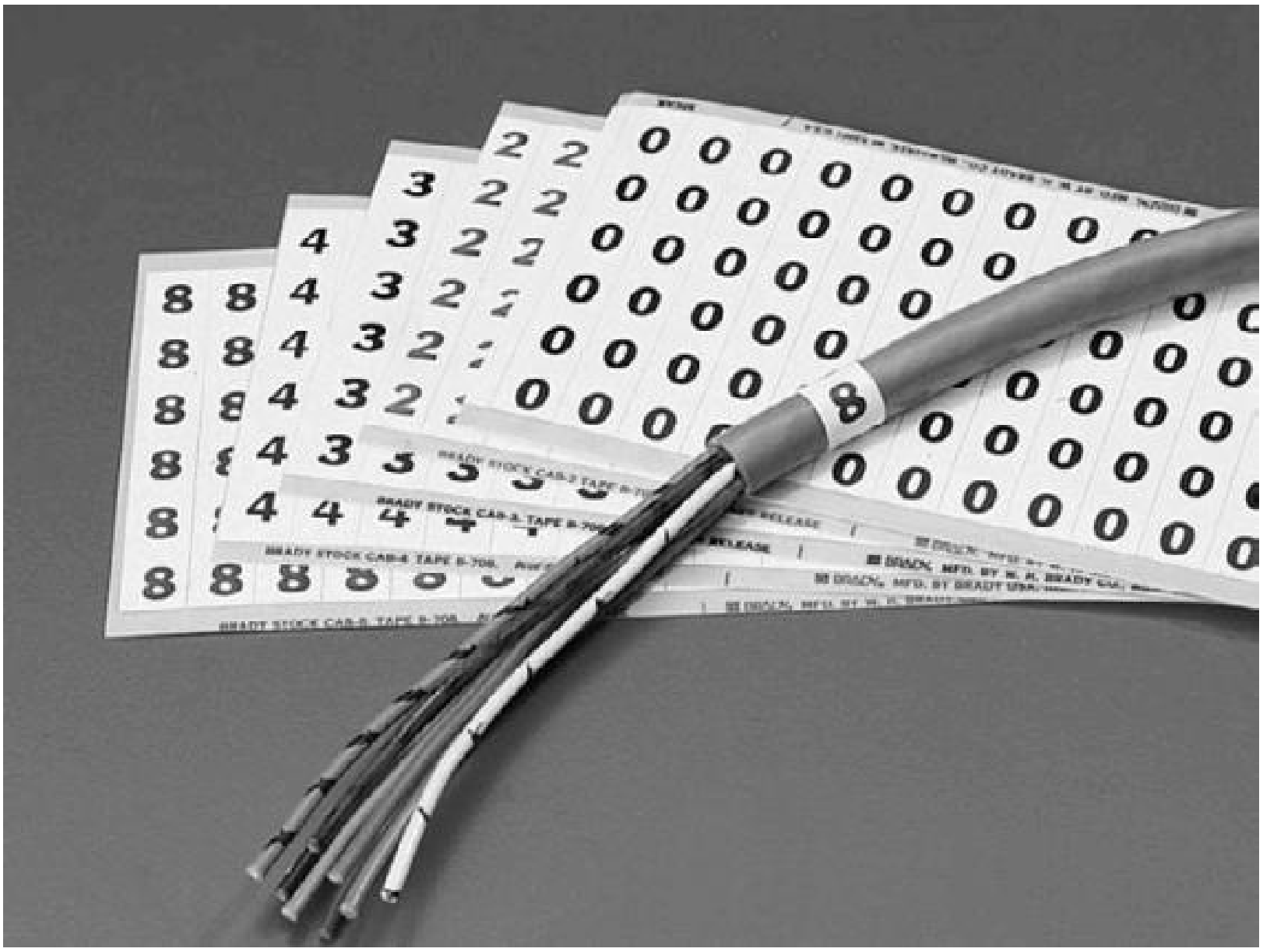
В отличие от монтажа коаксиальной сети, когда кабель можно прокладывать к определенному рабочему месту, переходя от одного места к другому, монтаж кабеля «витая пара» часто подразумевает использование иного подхода. Если речь идет о монтаже большой локальной сети, то прокладка кабеля к отдельному рабочему месту часто сопряжена с рядом проблем. Эти проблемы создаются межкомнатными переходами и отверстиями, сквозь которые бывает тяжело протянуть нужное количество кабелей. По этой причине очень часто протягиваются все сегменты кабеля сразу, что, конечно, увеличивает расход кабеля.

Если же дело касается небольших офисных или домашних сетей, когда стоимость критична, то можно выбрать и другие способы прокладки кабеля, в том числе и прокладку одиночных кабельных сегментов.

В любом случае принцип прокладки кабеля сводится к тому, чтобы его протянуть от центрального узла до конечного с учетом всех особенностей пути или расположения коробов. При этом следует позаботиться о создании некоторого запаса кабеля, который потом можно легко устранить в районе центрального узла. Запас кабеля пригодится для монтажа сетевых розеток или для процесса обжима коннекторов.

При прокладке кабеля, чтобы не перепутать сегменты местами, желательно использовать систему обозначений. Для этого к обоим концам кабеля крепятся маркеры с номером рабочего места или розетки (если они используются).

Чтобы сэкономить деньги, в качестве маркера можно использовать небольшой отрезок бумаги с записью, закрепленный с помощью скотча.

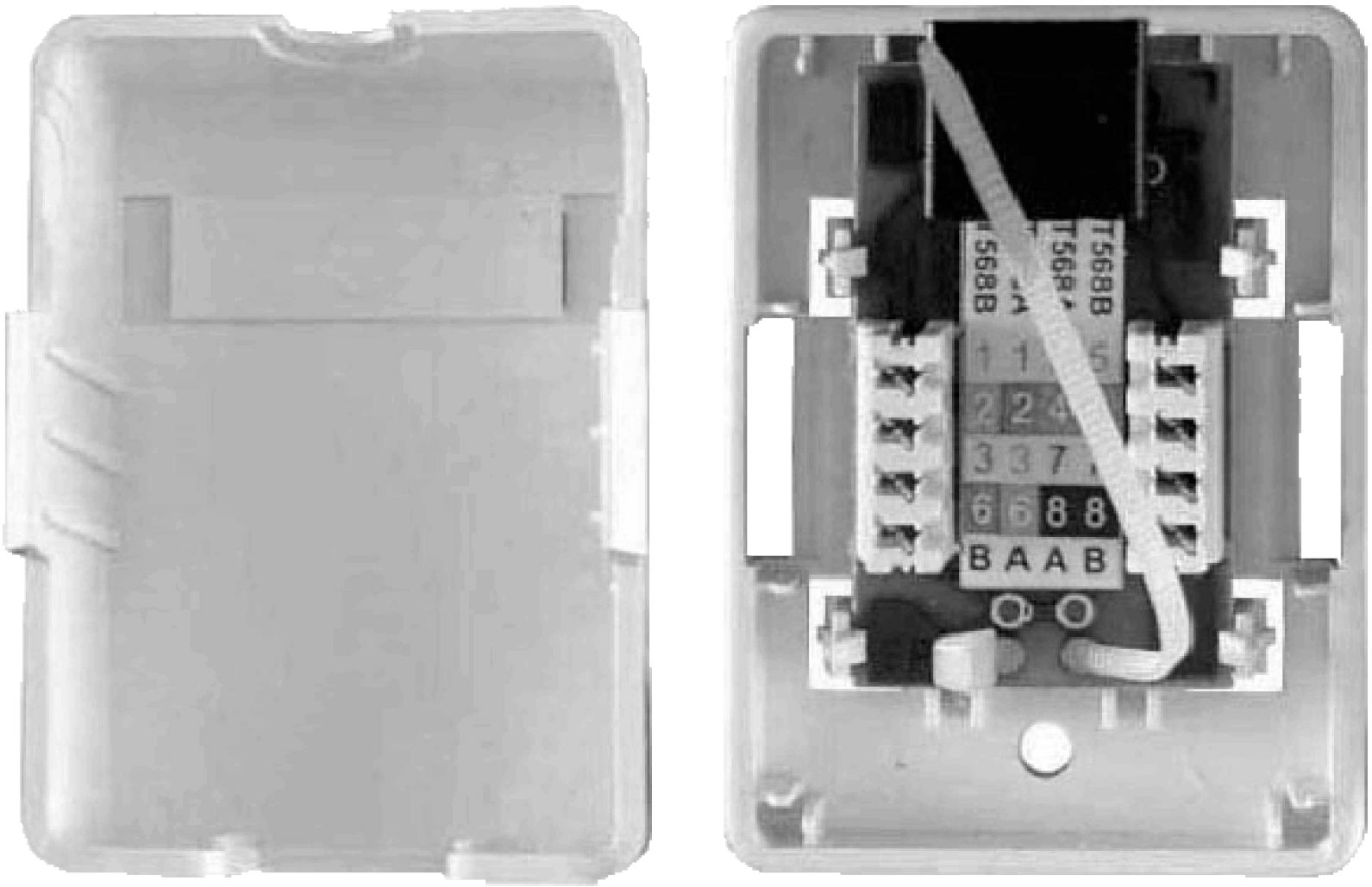


Монтаж сетевых розеток

Как уже упоминалось ранее, использование сетевых розеток практикуется в основном при создании большой локальной сети. Однако это совсем не означает, что их нельзя использовать и в небольших офисах. Что касается хаотичной сети, например домашней, то от сетевых розеток отказываются вообще.

Сетевые розетки бывают разной категории, а соответственно, различаются конструкцией и сложностью. На практике, если речь не идет о государственных организациях с серьезными требованиями безопасности при работе с информацией, применяются сетевые розетки невысокой стоимости.

Для примера рассмотрим монтаж сетевой розетки, которая требует крепления на стене с помощью шурупа или двухстороннего скотча. Такая розетка состоит из трех частей: основы, крышки и платы с контактной группой (рис. 14.2).



При работе с этой розеткой можно придерживаться такой последовательности действий.

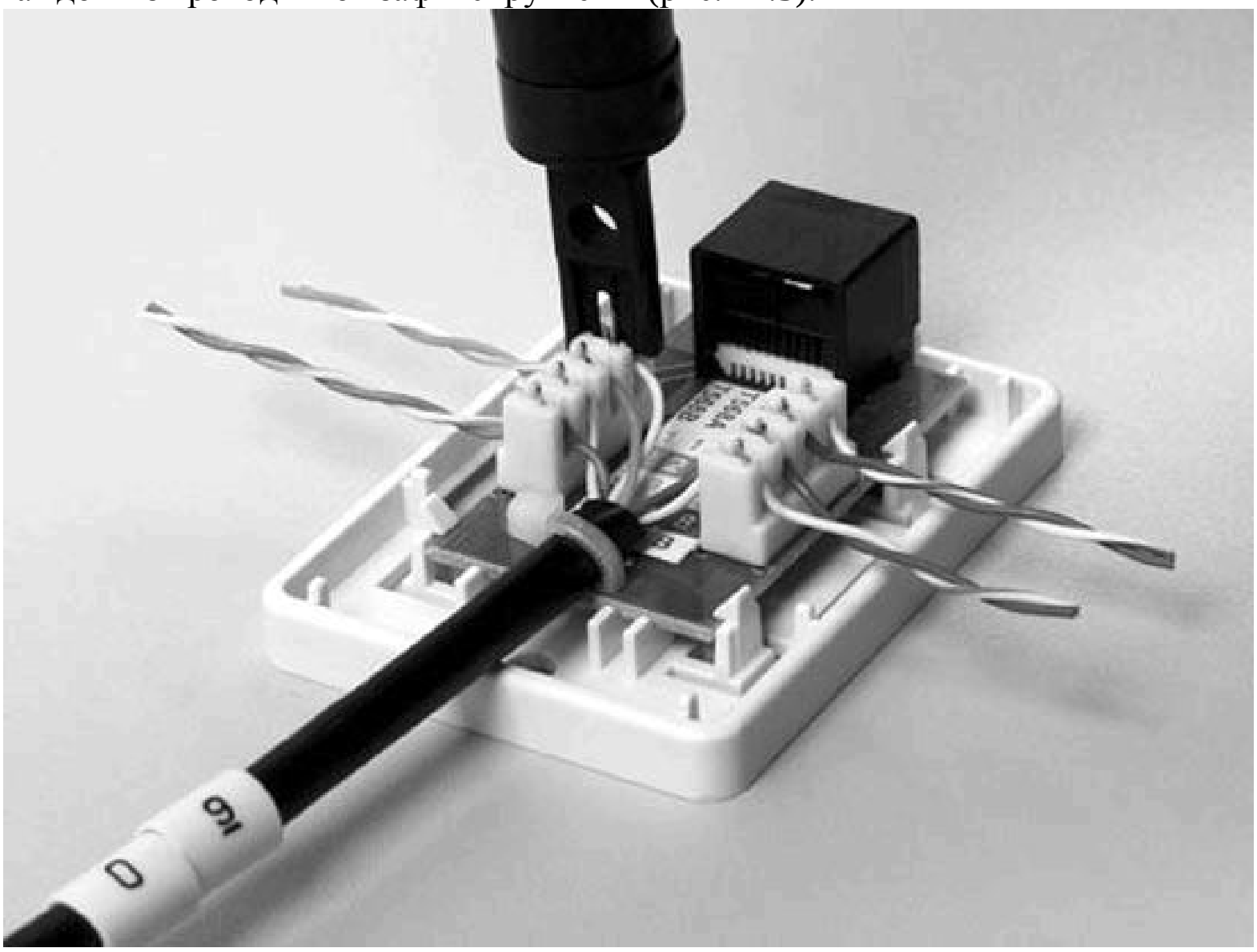
1. Разобрать розетку на составные части, чтобы отделить основу розетки.
2. Зафиксировать основу в том месте, где должна располагаться розетка.
3. Выполнить зажим проводников на контактной группе платы.
4. Закрепить плату на основе, используя для этого предусмотренный способ.
5. Закрыть розетку крышкой.

Как правило, розетка использует систему замков, поэтому, чтобы ее разобрать, инструменты не нужны: просто определите месторасположение замков и раскройте их. Далее все зависит от строения розетки: если крепление платы подразумевает использование винтов, необходимо использовать отвертку, чтобы открутить плату.

Плата с контактной площадкой представляет особый интерес. Как правило, рядом с контактной площадкой имеется схема зажима проводников согласно существующим стандартам, например T568A (более подробно об этом читайте далее). Ваша задача – проверить правильность нанесенной схемы, поскольку очень часто она содержит ошибки (особенно дешевые розетки). Это очень важный момент, поскольку для функционирования локальной сети с использованием кабеля «витая пара» должна применяться одинаковая схема обжима проводников на всех участках сети: центральном узле, сетевых розетках, патч-кордах и т. д.

Система фиксации проводников в контактной площадке подразумевает использование такой системы, когда оба проводника одной пары расположены в смежных контактах. Это сделано не зря, поскольку стандарты жестко регламентируют длину, на которую можно расплетать пары (не более 12,5 мм). По этой причине при фиксации проводников также следует придерживаться данного подхода: расплетайте проводники на минимальную длину.

Для зажима проводников в розетках используется специальный нож-вставка, о котором уже упоминалось ранее. Установив проводники в своих контактах, нажатием ножа на каждом из проводников зафиксируйте их (рис. 14.3).



После визуального контроля качества фиксации проводников лишние концы проводников нужно откусить кусачками.

Для фиксации кабеля в розетке могут применяться разные методы, одним из которых является использование монтажной стяжки. Затянув стяжку до упора, обрежьте лишний конец стяжки и закройте розетку крышкой.

Монтаж кросс-панели

Кросс-панель, как и сетевая розетка, представляет собой лишь удобное средство для подключения кабеля независимо от того, зачем этот кабель используется. В данном случае кабель применяется для соединения порта на кросс-панели с портом на центральном управляющем узле, например коммутаторе.

Кросс-панель для монтажа кабеля «витая пара» также использует контактные площадки, количество которых зависит от количества портов на кросс-панели. Принцип работы с контактной площадкой практически повторяет принцип работы с сетевой розеткой. Отличие может касаться только внешнего вида и размера контактной площадки, а также способа фиксации кабеля.

При обжиме проводников не забывайте о том, что схема подключения проводников должна повторять схему обжима, которая применяется для сетевых розеток и коннекторов.

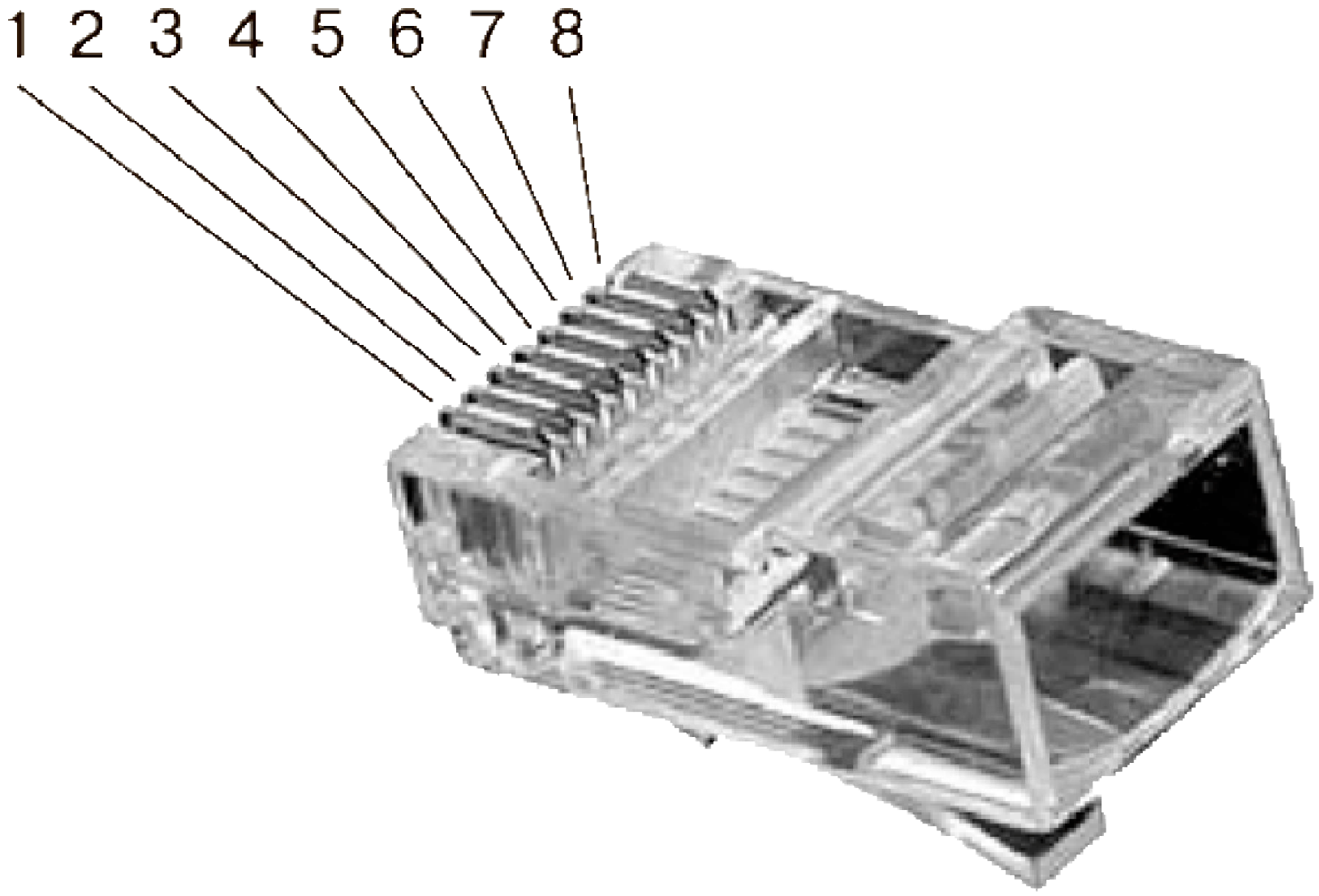
Детально описывать зажим проводников не имеет смысла, поскольку он аналогичен процессу зажима проводников в сетевой розетке. Единственное, на что нужно обратить внимание, – аккуратность выполнения работ: после зажима проводников очередного кабеля обязательно фиксируйте его на плате контакта. После того как все порты на кросс-панели обжаты, вся кабельная система фиксируется с помощью предусмотренного для этого механизма, который находится в задней части кросс-панели.

Обжим кабеля

В зависимости от размера локальной сети и подхода к ее созданию обжим кабеля может быть как последним этапом в монтаже локальной сети, так и вообще единственным. Так, если локальная сеть создается с минимумом затрат, то обжим отрезков кабеля нужной длины – это все, что в этом случае требуется выполнить для создания сети. Если же речь идет о достаточно большой локальной сети, то в первую очередь происходит установка монтажного шкафа, монтаж коробов, сетевых розеток и кросс-панели и лишь потом – обжим кабеля.

Стоит сказать, что необходимость обжима кабеля возникает лишь при создании небольшой офисной сети или сети в домашних условиях. Сеть большого размера подразумевает использование готовых патч-кордов и кросс-кордов, приобретаемых вместе с остальным оборудованием. Тем не менее необходимо знать принцип обжима и приобрести такой полезный опыт, поскольку рано или поздно дело потребует создания кабеля для подключения нужного оборудования. По этой причине рассмотрим данный процесс более детально на примере создания патч-корда.

Для обжима кабеля «витая пара» используются коннекторы RJ-45, чего требуют сетевые стандарты. Нумерация контактов в коннекторе производится так, как показано на рис. 14.4.



Существует определенное правило, которое необходимо выполнять при обжиме кабеля: следует соблюдать особый принцип подключения проводников, причем, как уже было сказано, данный принцип должен соблюдаться на всех этапах проведения работ.

На практике используются две схемы обжима или зажима проводников (табл. 14.1).

Таблица 14.1.Расположение проводников согласно схемам T568A и T568B

Номер контакта	Размещение согласно T568A	Размещение согласно T568B
1	Бело-зеленый	Бело-оранжевый
2	Зеленый	Оранжевый
3	Бело-оранжевый	Бело-зеленый
4	Синий	Синий
5	Бело-синий	Бело-синий
6	Оранжевый	Зеленый
7	Бело-коричневый	Бело-коричневый
8	Коричневый	Коричневый

Принципиального различия между этими схемами нет, поэтому можно выбрать ту, которая вам больше нравится, и ее придерживаться.

При обжиме кабеля можно следовать такому алгоритму действий.

1. Наденьте на конец кабеля изоляционный колпачок, развернув его таким образом, чтобы широкий конец колпачка смотрел в сторону обрабатываемого конца кабеля (рис. 14.5).

2. Аккуратно обрежьте конец кабеля, воспользовавшись резаком обжимного инструмента или обычными ножницами. Снимите с кабеля внешнюю изоляцию длиной примерно 20 мм, не повредив при этом проводники. Это можно сделать резцами обжимного инструмента или ножом.

3. Отделив пары проводников друг от друга, расплетите и выровняйте их, немного вытянув из внешней изоляции. Далее возьмите конец кабеля в руку и зажмите его между большим и указательным пальцами рабочей руки, как показано на рис. 14.6, и расположите проводники согласно одному из стандартов, например T568A.

4. Обрежьте концы проводников так, чтобы их оставшаяся длина не превышала 12 мм.

5. Возьмите в другую руку коннектор RJ-45 и поверните его таким образом, чтобы окошко разъема находилось перед вами, а пластмассовая защелка – внизу коннектора.

6. Медленно и аккуратно вставьте концы проводников в окошко разъема, проследив, чтобы они равномерно распределились по всей его ширине (рис. 14.7).

7. Проталкивая проводники вглубь коннектора, обратите внимание, чтобы они не поменяли свое расположение относительно друг друга.

8. Вставив проводники до упора, еще раз убедитесь в правильности их расположения согласно выбранному стандарту.

9. Вставьте коннектор в соответствующее гнездо обжимного инструмента и сильно сожмите ручки инструмента (рис. 14.8).

10. Задвиньте на обжатый коннектор защитный колпачок (рис. 14.9).

Аналогичным образом проведите обжим второго конца кабеля.

Глава 15
Тестирование и диагностика сети

Процесс монтажа кабельной системы локальной сети не может гарантировать 100 %-ную работоспособность всех сегментов сети. Связано это с использованием достаточно большого количества механических операций, автоматизировать которые невозможно по ряду причин. Именно поэтому монтаж локальной сети всегда сопровождается постоянным тестированием готовых сегментов. Кроме того, в случае создания большой локальной сети, когда монтаж полностью завершен, проводится полная проверка работоспособности сети с подготовкой соответствующей технической документации.

Подобная процедура – стандартный подход в случае, когда проектированием и монтажом локальной сети, или, как ее называют в этом случае, СКС (структурированная кабельная система), занимается фирма-подрядчик. Поскольку она получает за это деньги, соответственно, она должна предоставить качественный продукт.

По понятным причинам создание подобной документации не производится, когда речь идет о небольшой локальной сети офисного или домашнего применения, тем более что в этом случае тестирование работоспособности сети происходит с использованием простейших методов.

Как бы там ни было, существуют определенные методы проверки работоспособности сети, которые позволяют устранить возникшую неисправность как на этапе монтажа

локальной сети, так и после его завершения.

Использование тестеров

Наиболее объективным и эффективным способом тестирования всех особенностей локальной сети является использование разного рода тестеров. Они позволяют максимально автоматизировать и упростить процесс тестирования, поэтому при монтаже больших сетей их использование обязательно.

Существуют разные варианты тестеров, отличающиеся методами тестирования, количеством разнообразных тестов, а также способом выдачи результатов. От этих функций напрямую зависит и стоимость такого оборудования. На рынке присутствует достаточно много тестирующего оборудования от разных производителей, стоимость которого колеблется в широком диапазоне: от $50 до $20 000. По понятным причинам использовать дорогостоящее оборудование может себе позволить лишь серьезная фирма, предоставляющая профессиональные услуги по монтажу СКС. На практике при тестировании большей части создаваемых локальных сетей с 30–50 компьютерами применяются простейшие тестеры, которые позволяют только проверять состояние кабельного сегмента, чего в 90 % случаев вполне достаточно.

Различают два основных вида тестеров: для тестирования физических линий и сетевые анализаторы.

Тестеры для тестирования физических линий получили наибольшее распространение благодаря своей цене. Такой тестер способен определять неисправность кабельного сегмента на физическом уровне, вплоть до определения места обрыва проводников. Кроме того, он может, например, протестировать волновое сопротивление линии или измерить скорость передачи данных, что позволяет определить используемый сетевой стандарт или соответствие определенному стандарту. Покупку такого тестера может позволить себе даже небольшая фирма, которая хочет иметь возможность быстро определять и устранять неисправность в процессе эксплуатации локальной сети.

Сетевые анализаторы – дорогостоящее оборудование, приобретение которого могут себе позволить только сетевые интеграторы. С помощью такого сетевого анализатора можно не только исследовать характеристики кабельной структуры, но и получить полную информацию о процессе, происходящем при прохождении сигнала от любого узла к любому узлу, с определением проблемных сегментов и узких мест. Кроме того, можно даже прогнозировать состояние сети в ближайшем будущем и пути решения или предотвращения будущих проблем.

Внешний вид тестера, позволяющего оценить физическую целостность кабельного сегмента любой длины, показан на рис. 15.1.

Хороший тестер позволяет оценить максимальное количество параметров кабеля, для чего в комплекте с тестером часто идут разного рода переходники и вспомогательные инструменты. Например, используя соответствующие переходники, можно производить тестирование как коаксиальных сегментов, так и сегментов кабеля «витая пара». Что касается оптоволоконных линий, то оборудование для их тестирования имеет более сложную конструкцию и часто ориентировано только на тестирование оптоволокна.

Тестирование кабельного сегмента происходит разными способами, которые зависят от наличия доступа к кабелю. Один из способов заключается в следующем: конец обжатого кабеля подключается к разъему на тестере, а на второй конец устанавливается специальная заглушка. В результате тестер может проверить сопротивление каждого проводника, а также соответствие их подключения одному из стандартов. Использование данных о сопротивлении проводников позволяет определить технические характеристики кабеля, а также выяснить расстояние до точки обрыва.

Использование программного способа

Когда возможности приобретения тестера нет, что часто происходит при монтаже офисной или домашней» сети целостность и качество кабельного сегмента можно проверить и программным путем, используя, например, системную утилиту ping.

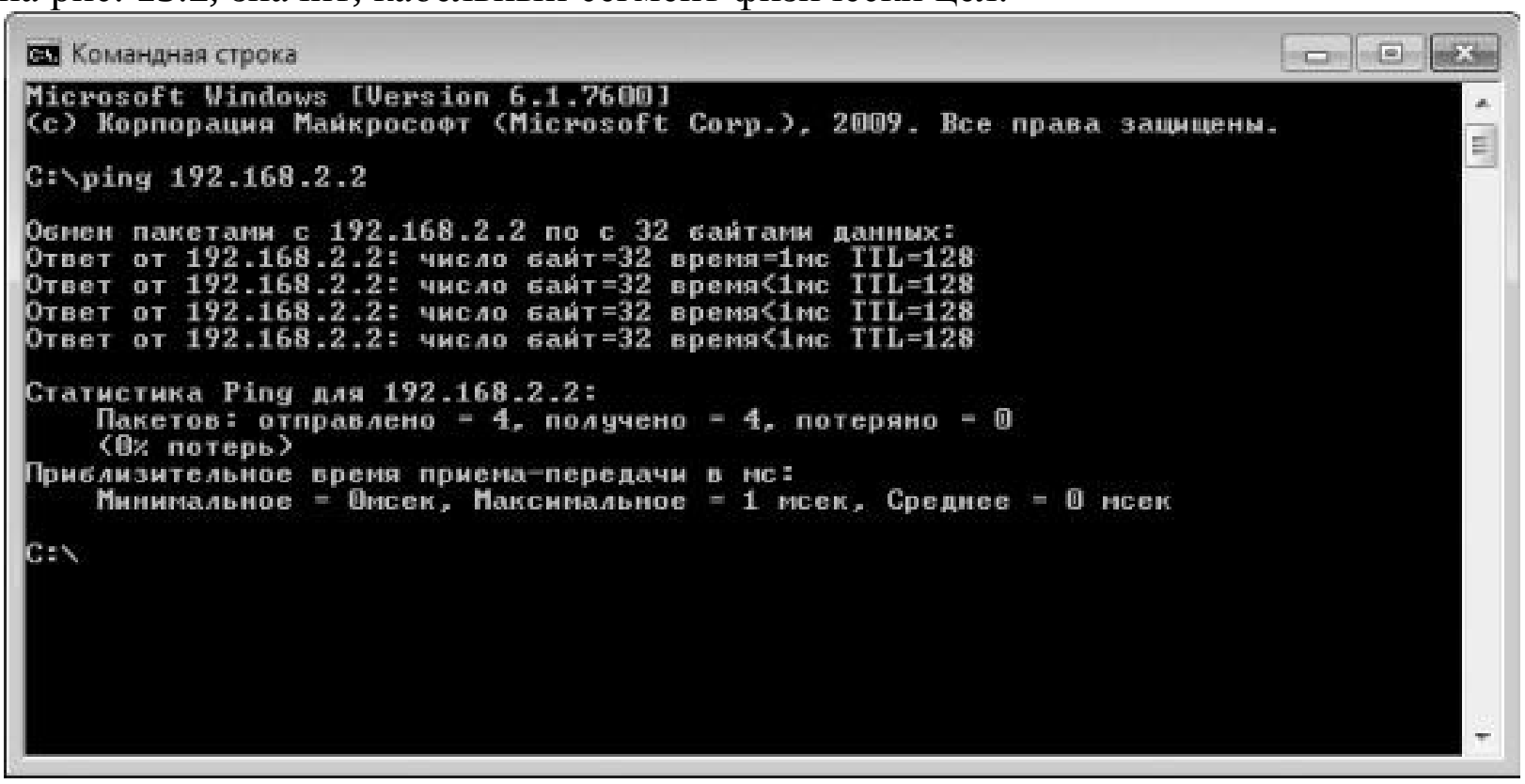
Принцип работы этого метода крайне прост и сводится к тому, чтобы попытаться передать через кабель любые данные с одного компьютера на другой, используя этот кабель.

Например, чтобы проверить сегмент коаксиального кабеля, необходимо соединить им два компьютера и установить на них терминаторы. Далее нужно настроить IP-адресацию каждого компьютера, присвоив одному, например, IP-адрес 192.168.2.1, а второму – 192.168.2.2 с маской подсети 255.255.255.0. Затем на компьютере с адресом 192.168.2.1 следует запустить утилиту Командная строка (Пуск ► Стандартные ► Командная

строка), в которой ввести такую команду:

ping 192.168.2.2

Если в результате выполнения этой команды последует ответ, похожий на показанный на рис. 15.2, значит, кабельный сегмент физически цел.



Если же в результате выполнения команды на экране появится надпись Превышен интервал ожидания для запроса, это будет свидетельствовать о том, что кабель имеет обрыв или коннекторы обжаты неправильно.

Подобным образом можно производить тестирование любого кабеля, в том числе и кабеля «витая пара». В случае с кабелем «витая пара» подобного рода подключение возможно только для варианта кроссовер (подключение типа «компьютер – компьютер»). Если же необходимо протестировать работоспособность кабеля типа патч-корд, им нужно подключить компьютер к центральному узлу, например коммутатору, а в паре с ним использовать заведомо рабочий кабель, которым к центральному узлу подключить второй компьютер.

Глава 16
Соединение двух компьютеров

В последнее время очень часто становится необходимым соединить два компьютера в сеть. Достаточно часто в домашнем хозяйстве имеется уже два компьютера: один используется для работы, а второй – для обеспечения досуга. Или, например, для работы применяются оба компьютера, только один из них стационарный, а второй – ноутбук или

нетбук, который часто путешествует вместе с вами. В любом случае появляется вполне оправданное желание соединить их, чтобы обмениваться данными или использовать принтер, подключенный к одному из компьютеров.

Похожая ситуация может возникнуть в малых офисах, где работает несколько человек, но рабочих мест только два, и их нужно объединить в производственных целях, например для работы с единой базой данных. Кроме того, существует еще Интернет и очень большое желание им пользоваться…

В данной главе мы рассмотрим некоторые варианты соединения компьютеров. Каждый из них имеет свои преимущества и недостатки. Конечно, разные способы соединения двух компьютеров дают различную максимальную скорость обмена данными между ними. Но определить оптимальный вариант по показателям «цена – качество – скорость» должен сам пользователь, ведь это зависит от его реальных потребностей, а также от возможного наличия аппаратных средств (сетевых адаптеров, кабеля и т. п.).

Соединение через Bluetooth

На сегодня поддержка технологии Bluetooth есть практически в любом устройстве, начиная с мобильных телефонов и компьютеров и заканчивая бытовыми приборами. Этот факт является очень привлекательным, а иногда он становится решающим аргументом, когда нужно быстро соединить два устройства.

Недостаток Bluetooth – малый радиус действия, а также невысокая (до 24 Мбит/с) скорость передачи данных, которая к тому же зависит от расстояния между компьютерами.

Тем не менее, когда нет особых требований к скорости передачи данных, а в наличии имеются два Bluetooth-адаптера, можно воспользоваться этим способом связи.

Для соединения персональных компьютеров требуется наличие двух Bluetooth-адаптеров. Если вы еще только собираетесь приобрести такой адаптер, выбирать необходимо модель класса A, поскольку именно этот класс устройств позволяет осуществлять обмен данными на расстоянии до 100 м.

Как правило, Bluetooth-адаптеры предлагаются только в USB-исполнении (рис. 16.1), то есть для их подключения требуется свободный USB-порт. Для ноутбуков также предлагается вариант с подключением к PCMCIA-слоту.

Несомненным плюсом использования технологии Bluetooth является то, что ее можно применять также и для обмена данными с мобильным телефоном или любым портативным устройством, например наладонником. Таким образом, при выборе Bluetooth-адаптера вы убиваете двух зайцев: получаете достаточно быструю сеть и возможность обмена с любыми портативными устройствами, «понимающими» Bluetooth.

Соединение с помощью коаксиального кабеля

Для соединения двух компьютеров можно применять те же средства, что и для соединения большого их количества. В частности, для этой цели отлично подойдет коаксиальный кабель.

Вам потребуются две сетевые карты, которые имеют разъем для подключения BNC-коннектора, два Т-коннектора и два терминатора, один из которых необходимо заземлить.

При использовании коаксиального кабеля можно достичь скорости передачи данных 10 Мбит/с, причем в этом случае практическая скорость (которая обычно меньше теоретической в 1,5–2 раза) вплотную приближается к теоретической. Этой скорости вполне хватит для обмена большими объемами информации.

Соединение с помощью кабеля «витая пара»

Этим способом можно соединить любое количество компьютеров. В случае соединения двух точек (а также двух концентраторов, двух коммутаторов и т. д.) используют специальный кабель кроссовер-корд, обжим коннекторов в котором отличается от стандартного патч-корда (табл. 16.1).

Таблица 16.1.Схема обжима коннекторов кроссовер-корда

Номер контакта	Первый коннектор	Второй коннектор
1	Бело-зеленый	Бело-оранжевый
2	Зеленый	Оранжевый
3	Бело-оранжевый	Бело-зеленый
4	Синий	Бело-коричневый
5	Бело-синий	Коричневый
6	Оранжевый	Зеленый
7	Бело-коричневый	Синий
8	Коричневый	Бело-синий

Данный способ соединения двух компьютеров наиболее практичен: поскольку необходимый сетевой контроллер уже интегрирован в материнскую плату, подключение сводится только к подготовке кабеля нужной длины. Кроме того, если на материнских платах окажется сетевой контроллер стандарта 1000Base-T и для соединения будет применяться кабель 6-й или 7-й категории, то вы получите в свое распоряжение скорость передачи данных, близкую к теоретической, то есть 1000 Мбит/с, что, согласитесь, с головой хватит для любых нужд.

Соединение через USB-порт

Все современные персональные компьютеры имеют как минимум два USB-порта, которые можно использовать для подключения USB-устройств, расширяющих функциональность компьютера. Примером такой функциональности является возможность соединения двух компьютеров через специальный USB-кабель.

Скорость работы USB-порта, особенно последних стандартов, очень высокая, что позволяет получить отличный результат при соединении двух компьютеров.

При этом теоретически можно достичь скорости 480 Мбит/с. С другой стороны, создание подобного соединения потребует поиска соответствующего кабеля.

К сожалению, соединить компьютеры обычным USB-кабелем нельзя: это может привести к выходу из строя материнской платы. Поэтому для создания сети из двух компьютеров используют специальный USB-кабель (рис. 16.2), главной особенностью которого является наличие специального модуля. Этот модуль и отвечает за необходимое согласование сигналов и напряжений.

Длина такого кабеля обычно составляет 3–3,5 м, хотя может быть и больше.

У данного способа имеется один недостаток, который сдерживает его распространение: длина USB-кабеля не должна превышать 10 м. Мало того, чем короче он будет, тем выше будет скорость передачи данных, а это означает, что данный способ подходит только для случаев, когда компьютеры, которые необходимо соединить, находятся достаточно близко друг к другу.

Соединение через FireWire-порт

Использование FireWire-порта для связи двух расположенных рядом компьютеров – еще один вид соединения, обладающий высокой скоростью передачи данных, которая теоретически может достигать 400 Мбит/с.

Многие современные модели материнских плат персональных компьютеров, а также многие модели ноутбуков и нетбуков имеют в своем составе FireWire-контроллер, поэтому вполне реально воспользоваться данным способом, чтобы организовать обмен данными. Однако, как и в случае с использованием USB-соединения, главная сложность – малая длина кабеля. Кроме того, этот кабель достаточно дорогой, и чем больше его длина, тем он дороже.

Внешний вид кабеля зависит от того, какого типа порты FireWire используются для соединения компьютеров (четырех– или шестиконтактные), а также от качества кабеля, основной характеристикой которого является наличие экранирующей оплетки (рис. 16.3).

Соединение с помощью беспроводных адаптеров

Любой беспроводной сетевой стандарт обеспечивает возможность работы беспроводной сети, не требуя при этом наличия точки доступа, стоимость которой достаточно существенна. Поэтому если у вас есть два беспроводных адаптера, то соединение двух компьютеров не займет много времени. При этом вы получите достаточно высокую скорость соединения и, самое главное, мобильность. А учитывая тот факт, что в домашних условиях все чаще используется сочетание «компьютер + ноутбук» или даже «ноутбук + ноутбук», использование подобного способа соединения компьютеров очень заманчиво.

Чтобы достичь максимальной эффективности работы подобного соединения,

рекомендуется использовать оборудование одного стандарта и, желательно, одного производителя. В этом случае вы получите максимально возможную скорость передачи данных, а также сможете воспользоваться некоторыми фирменными технологиями от производителя оборудования. Все, что вам остается сделать, – настроить оба адаптера на использование одного идентификатора сети и выбрать один из способов аутентификации и шифрования данных.

Часть 3
Беспроводная сеть

Глава 17
Беспроводные стандарты

Разработкой правил функционирования локальных сетей с беспроводной средой передачи данных WLAN (Working Group for Wireless Local Area Networks, рабочая группа по беспроводным локальным сетям), использующих частоты 2,4 и 5 ГГц, занимается подкомитет 802.11. В его состав входит более 100 компаний, которые непосредственно связаны с производством сетевого оборудования, программного обеспечения для беспроводных локальных сетей и т. п.

Особенности некоторых беспроводных стандартов будут рассмотрены ниже.

IEEE 802.11

Стандарт IEEE 802.11, разработка которого началась сразу после образования комитета 802.11 (а это произошло в 1990 году), является первым беспроводным стандартом, который использовался для создания локальной беспроводной сети.

Перед комитетом ставилась задача разработать стандарт, который позволил бы добиться устойчивой работы беспроводной сети. При этом необходимо было достичь стандартной скорости передачи данных 1 Мбит/с и опциональной скорости передачи данных 2 Мбит/с. Результат был получен, но на это ушло целых 7 лет работы.

Стандарт IEEE 802.11 описывает функционирование беспроводной сети в диапазоне частот 2400–2483,5 МГц, а также в инфракрасном диапазоне частот. При этом для обработки сигналов используются методы, имеющие разный принцип работы, что делает их несовместимыми между собой.

Рассматриваемый стандарт предполагает выполнение следующих положений:

- в локальной сети используется оборудование, работающее в диапазоне радиочастот 2400–2483,5 МГц;
- радиус сети не превышает 300 м;
- стандартная скорость передачи данных – 1 Мбит/с, опциональная – 2 Мбит/с.

При использовании стандарта IEEE 802.11 теоретический радиус сети, как уже было отмечено, составляет 300 м. На практике же он редко превышает 50-100 м, что обусловлено особенностями распространения сигнала в присутствии разного рода препятствий. Этого радиуса вполне достаточно для организации работы локальной сети в небольшом офисе. Однако скорость передачи данных даже для 1997 года, когда появился этот стандарт, оказалась слишком низкой. Проводные варианты сети уже в то время

предлагали скорость на порядок выше. Данный факт и стоимость оборудования и стали причиной того, что этот стандарт не нашел широкого применения.

IEEE 802.11b

Со стандарта IEEE 802.11b началось широкое распространение беспроводных сетей. Именно этот стандарт обусловил появление понятия Wi-Fi (Wireless Fidelity, беспроводная точность).

Проанализировав все ошибки и недостатки стандарта IEEE 802.11, а также приняв во внимание новые требования, комитет в 1999 году разработал стандарт IEEE 802.11b (еще одно название – IEEE 802.11 high rate), который долгое время был очень популярным. Появилось большое количество оборудования этого стандарта, а также в ноутбуки и другие переносные устройства стали встраивать адаптеры стандарта IEEE 802.11b. Беспроводные локальные сети данного стандарта даже сейчас часто встречаются.

Стандарт предусматривает следующие правила и соглашения:

- для работы в локальной сети используется оборудование, которое функционирует в диапазоне радиочастот 2400–2483,5 МГц;
- радиус сети не превышает 300 м;
- стандартная скорость передачи данных – 1 и 5,5 Мбит/с, опциональная – 2 и 11 Мбит/с;
- в качестве протокола безопасности используется протокол WEP.

Чтобы добиться скорости передачи данных 11 Мбит/с, используется метод DSSS, применяющий 5 перекрывающихся поддиапазонов, а также новая система шифрования.

Из плюсов IEEE 802.11b можно отметить то, что оборудование этого стандарта имеет наибольшую чувствительность и помехоустойчивость. Как результат – качество связи гораздо выше, чем при использовании оборудования с более современными стандартами. Кроме того, некоторые производители предлагают оборудование, которое может работать на скорости 22 Мбит/с (IEEE 802.11b+) при условии применения оборудования от одного производителя.

Недостатком стандарта является то, что скорость передачи данных может падать до 1 Мбит/с, что зависит от количества преград между передатчиком и приемником сигнала. Кроме того, оборудование стандарта IEEE 802.11b использует WEP-шифрование, безопасность работы которого очень низкая. При использовании соответствующих программ получить ключ к беспроводной сети с таким шифрованием можно достаточно быстро.

IEEE 802.11a

Конечно, было бы логично, если бы стандарт IEEE 802.11a появился раньше, чем IEEE 802.11b. Но несмотря на то, что работа над этими стандартами велась параллельно, стандарт IEEE 802.11a был принят позднее, в 2001 году.

При разработке данного стандарта комитет пошел несколько другим путем, решив использовать в качестве диапазона частот сразу три полосы: 5,15-5,25 МГц, 5,25-5,35 МГц и 5,725-5,825 МГц. Это позволяет добиться бóльшей пропускной способности, а также использовать менее «зашумленный» диапазон частот. При этом применяются новые методы обработки сигнала и усовершенствованные алгоритмы шифрования.

Стандарт предусматривает следующие положения:

- для работы в локальной сети используется оборудование, которое функционирует в диапазоне радиочастот 5,15-5,25 МГц, 5,25-5,35 МГц и 5,725-5,825 МГц;
- радиус сети не превышает 100 м;
- стандартная скорость передачи данных – 1, 6, 12 и 24 Мбит/с, опциональная – 2, 9, 18,

36, 48 и 54 Мбит/с.

Главным достоинством этого стандарта является высокая скорость передачи данных, однако это практически единственный его плюс. Минусов гораздо больше, основными из которых являются следующие:

▪ малый радиус сети, который резко уменьшается при наличии даже незначительных препятствий сигналу;

▪ несовместимость IEEE 802.11a с существующими стандартами (кроме 802.11n), что делает использование сетевого адаптера невозможным, если применяется точка доступа с другим стандартом;

▪ большое потребление энергии, делающее его неудобным для использования на переносных компьютерах;

▪ практически во всех странах требуется наличие специального разрешения или даже лицензии на использование оборудования для работы в указанных диапазонах частот.

Эти недостатки привели к тому, что стандарт IEEE 802.11a не стал таким популярным, как ожидалось, даже несмотря на высокую скорость передачи данных.

IEEE 802.11g

В начале 2000-х годов многие ожидали появления стандарта IEEE 802.11g, поскольку наиболее распространенный на то время стандарт IEEE 802.11b уже перестал удовлетворять требованиям скорости и безопасности. И это сдерживало распространение беспроводных сетей.

Оборудование стандарта IEEE 802.11g, как это обычно бывает, появилось на рынке гораздо раньше, чем был принят сам стандарт (он был принят в 2003 году). И надо сказать, что ожидание полностью оправдалось: новый стандарт получился очень функциональным, а главное, имел новый уровень безопасности. Кроме того, совместимость IEEE 802.11g со стандартом IEEE 802.11b позволила использовать оборудование стандарта IEEE 802.11b в сетях IEEE 802.11g.

Основные правила и соглашения, описанные в стандарте IEEE 802.11g:

▪ для работы в локальной сети используется оборудование, которое функционирует в диапазоне частот 2400–2483,5 МГц;

▪ радиус сети не превышает 300 м;

▪ стандартная скорость передачи данных – 1, 5,5, 11, 24, 33 и 48 Мбит/с, опциональная – 2, 9, 12, 18, 36 и 54 Мбит/с;

▪ в качестве протоколов безопасности и аутентификации используются WPA, WPA2, AES, TKIP и др.;

▪ максимальное количество подключений – 2048.

Поддержка этого удачного стандарта сразу же была реализована в ноутбуках и переносных устройствах, что также увеличило его популярность. Кроме того, как и в случае со стандартом IEEE 802.11b, некоторые производители, например D-Link, выпустили на рынок устройства, способные работать на скорости 108 (IEEE 802.11g+) и даже 125 Мбит/с, что сделало данный стандарт еще более привлекательным.

IEEE 802.11n

Появление стандарта IEEE 802.11g на некоторое время решило все актуальные задачи. Однако потребности в скорости передачи данных росли с каждым днем, а проводные

варианты сетей уже предлагали 100 и даже 1000 Мбит/с. Это привело к тому, что распространение беспроводных сетей опять замедлилось и они стали актуальны лишь для небольших сетей домашнего применения и малых офисов.

Однако процесс разработки новых стандартов не стоял на месте. Правда, практически все усилия комитета были направлены на решение вопросов безопасности, совместимости, маршрутизации и т. д. Велась также разработка нового стандарта, но его принятие постоянно откладывалось в силу разных причин, в результате чего более пяти лет никаких сдвигов на беспроводном фронте не наблюдалось.

Тем не менее еще в 2006 году на рынке стали появляться несертифицированные устройства еще не принятого стандарта IEEE 802.11n. Такое положение вещей сохранялось достаточно долгое время, пока в 2009 году наконец-то не был принят стандарт IEEE 802.11n, который начал новую эру в развитии беспроводных сетей.

Использование оборудования данного стандарта позволяет достигать достаточно значительных скоростей передачи данных, вплоть до 300 Мбит/с. Такая скорость передачи данных стала возможной благодаря более оптимальному использованию полос радиочастот, а также применению качественно новых аналоговых чипов обработки сигналов с раздельным приемным и передающим трактами. Так, в отличие от стандарта IEEE 802.11g, новый стандарт использует деление доступного частотного диапазона на полосы шириной 40 МГц с параллельной передачей данных сразу по нескольким полосам.

Стандарт IEEE 802.11n предусматривает следующие правила.

▪ Беспроводное оборудование работает с частотами 2,4 и 5 ГГц (2400–2483,5 МГц; 5,15-5,25 ГГц, 5,25-5,35 ГГц и 5,725-5,825 ГГц). Выбор диапазона зависит от режима работы, который в свою очередь зависит от стандартов оборудования, работающего в локальной сети. Например, если в сети используется оборудование разных стандартов, то будет выбран режим совместимости с наиболее старым стандартом и скорость передачи данных при этом будет соответствующая. Если же применяется только оборудование стандарта IEEE 802.11n, то будет выбран режим с максимальной скоростью передачи данных.

▪ Радиус сети не превышает 450 м.

▪ Скорость передачи данных зависит от режима использования оборудования и составляет от 54 Мбит/с (в режиме совместимости со стандартами IEEE 802.11a, IEEE 802.11b и IEEE 802.11g) до 300 Мбит/с (при использовании устройств стандарта IEEE 802.11n).

На сегодня стандарт IEEE 802.11n является наиболее перспективным, тем более что стоимость оборудования этого стандарта вполне доступна. Кроме того, по некоторым данным, ждать появления нового стандарта, обещающего увеличенную вдвое скорость передачи данных, придется ни много ни мало – до 2016 года.

Глава 18
Технология Bluetooth

Слово Bluetooth слышал, наверное, каждый (возможно, даже не понимая, что это такое). Более того: пользователи мобильных телефонов или переносных устройств знают, что с помощью Bluetooth можно передавать и получать данные. Однако почти никто не задумывается о том, что с помощью технологии Bluetooth можно строить беспроводные локальные сети, пусть и с небольшим количеством подключенных устройств.

ПРИМЕЧАНИЕ

В настоящий момент разрабатывается технология, позволяющая посредством Bluetooth объединять устройства любого типа, чтобы можно было быстро получать или передавать

нужные данные.

История появления названия Bluetooth достаточно интересна. В начале прошлого тысячелетия в Дании правил король Гаральд Блютус (Harald Bluetooth), который прославился тем, что разными законными и не очень путями, в том числе и военным, объединил многие разрозненные земли Дании и Норвегии. Видимо, создатели технологии Bluetooth также замахнулись на то, чтобы разработать стандарт, с помощью которого можно было бы объединить компьютерную и телекоммуникационную индустрии. Нужно сказать, они в этом преуспели.

Работа над спецификацией Bluetooth («синий зуб») как средства связи в персональных беспроводных сетях WPAN (Wireless Personal Area Network, персональная беспроводная сеть) началась еще в середине 90-х годов прошлого века. Изначально разработкой Bluetooth занималась только одна компании – Ericsson Mobile Communication. Создавалась эта технология для нужд компании, но в итоге своими возможностями заинтересовала многих.

В конце 90-х годов прошлого века была сформирована рабочая группа Bluetooth SIG (Bluetooth Special Interest Group), под эгидой которой для совместных разработок объединились крупнейшие производители телекоммуникационной и компьютерной техники, такие как Ericsson, IBM, Intel, Toshiba и Nokia. Когда и другие компании сообразили, что за технологией Bluetooth стоит большое будущее, ряды SIG пополнили более тысячи новых членов. Конечно, бóльшая часть из них лишь хотели получить свой кусок «пирога славы», но тем не менее столь грандиозный консорциум сделал свое дело.

Чтобы иметь возможность пользоваться Bluetooth, необходимо иметь Bluetooth-адаптер. Для персональных компьютеров он чаще всего выполнен в виде USB-адаптера, подключаемого к свободному USB-порту. Портативные или переносные устройства, такие как ноутбук, нетбук, наладонники и т. д., часто оборудованы интегрированными контроллерами Bluetooth.

Существует три класса контроллеров Bluetooth, которые отличаются мощностью передатчика и, соответственно, радиусом действия.

- Class 1. Мощность передатчика 100 мВт (20 дБм), радиус действия 100 м.
- Class 2. Мощность передатчика 2,5 мВт (4 дБм), радиус действия 10 м.
- Class 3. Мощность передатчика 1 мВт (0 дБм), радиус действия 1 м.

Чаще всего встречаются устройства первого и второго классов, которые позволяют обмениваться данными на максимальном расстоянии.

Технология Bluetooth использует так называемый ISM-диапазон частот (Industry, Science and Medicine, промышленность, наука и медицина) 2,4–2,4835 ГГц, предназначенный для промышленного, медицинского и научного оборудования. Однако поскольку данный диапазон не является жестко регламентируемым, в нем работают тысячи разнообразнейших устройств, включая и оборудование беспроводных сетей.

При обработке сигнала используется метод, позволяющий разбить весь диапазон частот на полосы шириной в 1 МГц. При этом несущая частота изменяется 1600 раз в секунду, а схема переключения частот согласовывается между отправителем и получателем на этапе установки связи. Это позволяет не только достичь достаточного уровня безопасности при передаче данных, но и уменьшить помехи от работающих «чужих» устройств.

За все время работы группы Bluetooth SIG было разработано шесть спецификаций Bluetooth, которые по договоренности с IEEE в 2002 году стали частью стандартов IEEE 802.15.

Bluetooth 1.0, 1.0A, 1.0B

Стандарт Bluetooth 1.0 (IEEE 802.15.1) появился в 1998 году (последняя версия – 1.0B – была принята в 1999 году). В данной ситуации справедлива пословица «первый блин – комом». Данный стандарт явно поспешили выпустить в свет только затем, чтобы привлечь внимание общественности к разработке вообще.

Спецификация версии 1.0B предусматривает обмен данными между устройствами с заранее известными физическими адресами (уникальными идентификаторами устройств). Это является одним из недостатков, поскольку невозможен анонимный обмен данными. Однако это не так критично, как проблема совместимости устройств от разных производителей. Именно она обусловила провал Bluetooth 1.0. Главной причиной этого стали недоработки и несоблюдение производителями соглашений спецификации.

Однако в любом случае цель была достигнута – обмен данными между совместимыми устройствами был обеспечен. При этом теоретическая скорость передачи данных составляла 732,2 Кбит/с на расстоянии до 100 м.

Bluetooth 1.1

Через два с половиной года, в 2002 году, произошло «второе пришествие» Bluetooth в виде спецификации 1.1 (IEEE 802.15.1-2002). Она стала более успешной, поскольку были исправлены многочисленные ошибки и решена проблема несовместимости устройств.

Самым значительным нововведением стала поддержка работы по незашифрованным каналам и возможность выбора наиболее подходящего канала для передачи данных благодаря поддержке индикации уровня мощности сигнала RSSI (Radio Signal Strength Indicator).

Bluetooth 1.2

Спецификация Bluetooth 1.2, появившаяся в 2003 году, является дальнейшим развитием технологии Bluetooth, и нужно сказать, что она стала настолько удачным решением, что во многие переносные и портативные устройства начали встраивать контроллер Bluetooth 1.2. Его до сих пор можно встретить в устройствах, приобретенных несколько лет назад.

Главными особенностями новой версии Bluetooth стали:

- ускоренный поиск устройств и ускоренное подключение к ним;
- внедрение поддержки технологии eSCO (Extended Synchronous Connections, расширенное синхронное соединение), улучшающей качество связи со звукопередающей и воспроизводящей гарнитурой;
- внедрение технологии адаптивного изменения канала AFH (Adaptive Frequency Hopping, скачкообразная адаптация частоты), позволяющей выбирать канал связи исходя из количества препятствий сигналу;
- обратная совместимость с устройствами предыдущих версий;
- увеличенная скорость передачи данных;
- поддержка до 8 устройств.

Bluetooth 2.0

Начиная с версии 2.0, которая появилась в 2004 году, технология Bluetooth стала совершенствоваться как в плане возможностей, так и в плане скоростных характеристик.

Основными нововведениями этой спецификации Bluetooth стали:

- технология EDR [4 - По этой причине часто встречается название Bluetooth 2.0+EDR] (Enhanced Data Rate, увеличенная пропускная способность), позволившая значительно

увеличить скорость передачи данных;
▪ скорость передачи данных до 3 Мбит/с;
▪ обратная совместимость со старыми версиями Bluetooth;
▪ механизм параллельной работы устройств;
▪ сервис качества QpS (Quality of Service), контролирующий качество связи и устраняющий эффект торможения при параллельной работе устройств;
▪ поддержка до 256 устройств;
▪ уменьшенное энергопотребление.

Как видите, версия 2.0 действительно значительно отличалась от предыдущих. Именно с ее появлением распространение Bluetooth приобрело массовый характер: как в мобильных устройствах, так и в компьютерной технике.

Bluetooth 2.1

В 2007 году в свет вышла новая доработанная версия – Bluetooth 2.1, основными нововведениями в которой стали:
▪ улучшенная система безопасности, исключающая возможность перехвата данных;
▪ технология уменьшения энергопотребления Sniff Subrating, позволяющая снизить потребление энергии в 3-10 раз по сравнению со старыми версиями Bluetooth;
▪ новая система обмена ключа шифрования, позволяющая производить обмен ключами без разрыва соединения.

Как и в версии 2.0, в Bluetooth 2.1 имеется поддержка технологии EDR, в связи с чем повсеместно используется название Bluetooth 2.1+EDR.

Bluetooth 3.0

Спецификация Bluetooth 3.0, или Bluetooth High Speed, принятая в 2009 году, на сегодняшний день является наиболее привлекательной для обмена данными между устройствами.

Новая версия Bluetooth имеет следующие нововведения:
▪ скорость передачи данных до 24 Мбит/с;
▪ уменьшенное энергопотребление;
▪ применение профилей;
▪ поддержка работы одновременно с 7 устройствами, при этом 255 устройств могут находиться в режиме ожидания;
▪ технология EPC (Enhanced Power Control, улучшенное управление питанием), позволяющая уменьшить количество обрывов при перемещении Bluetooth-устройств даже при кратковременном пропадании сигнала.

Bluetooth-адаптеры нового стандарта уже вполне могут составить конкуренцию сетям Wi-Fi, тем более что стоимость самих устройств очень низка. Данный стандарт просто незаменим для быстрого соединения двух компьютеров и передачи данных.

Глава 19
Особенности функционирования беспроводных сетей

Использование радиоволн в качестве среды передачи данных имеет целый ряд особенностей, не позволяющих применять те методы и режимы работы, которые с

успехом используются в проводных сетях. Поэтому существующими беспроводными стандартами предусмотрено использование собственных методов обработки сигнала, шифрования данных и аутентификации и т. д.

Режимы функционирования

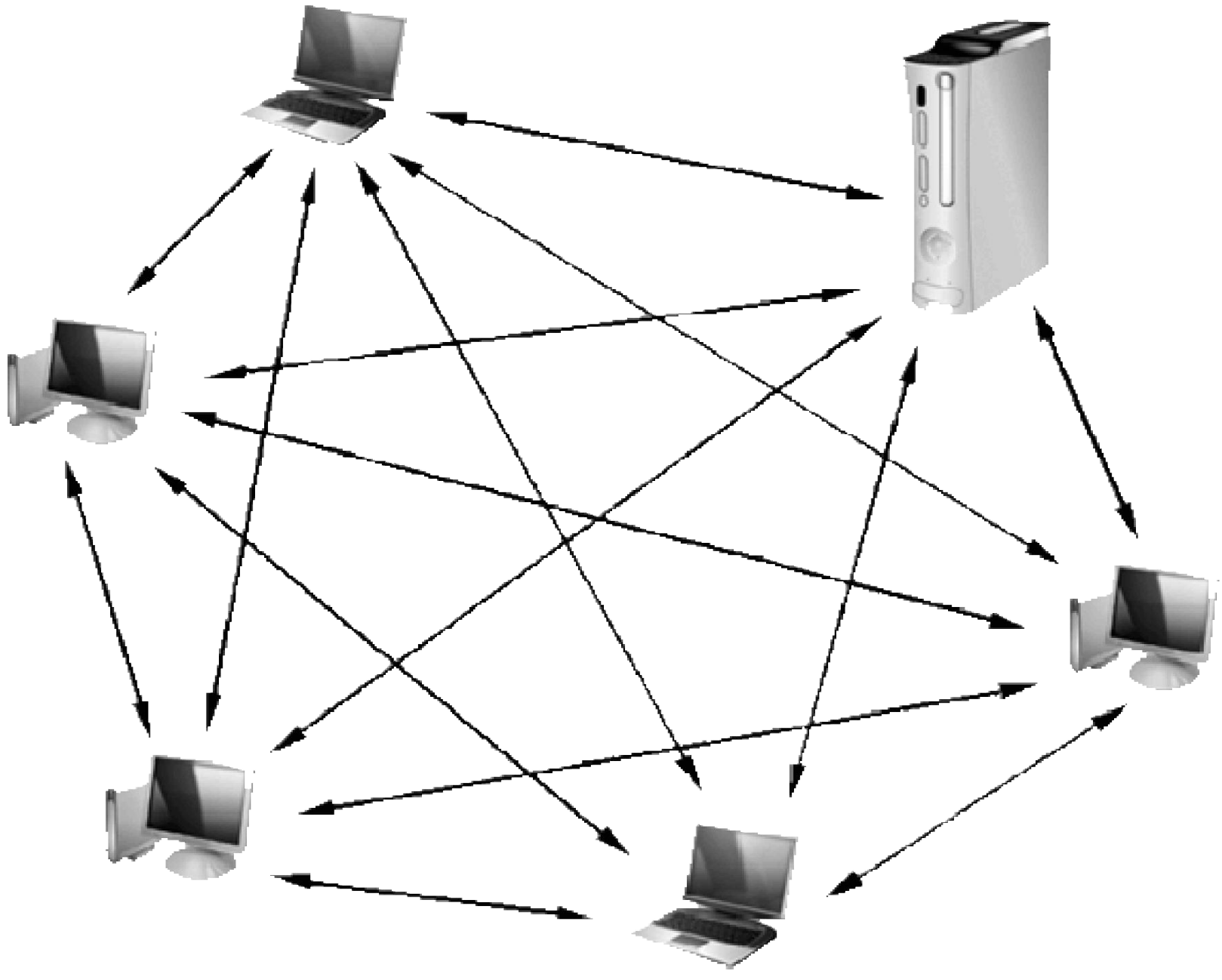
Существует два режима, или, как их еще называют, конфигурации, работы беспроводного оборудования, которые были описаны самым первым беспроводным стандартом IEEE 802.11:

- IBBS (Independent Basic Service Set), независимый базовый набор служб;
- BBS (Basic Service Set), базовый набор служб.

Выбор режима определяет принцип функционирования сети, используемое для этого оборудование, характеристики сети, сложность администрирования и многое другое.

IBBS

Независимый базовый набор служб (его называют также ad-hoc, режим независимой конфигурации, «точка – точка») – самый простой режим работы беспроводной сети. Для передачи и приема данных достаточно лишь беспроводных адаптеров, установленных на компьютерах (или других устройствах). При этом каждый беспроводной адаптер обменивается данными сразу со всеми беспроводными адаптерами сети (рис. 19.1).



Если провести аналогию с проводными сетями, то данный режим очень похож на топологию «шина», когда данные от одного устройства отправляются сразу всем устройствам, а сами устройства уже определяют, кому эти данные адресованы.

Хотя при этом не используется отдельно стоящее центральное управляющее устройство, тем не менее, чтобы объединить все рабочие станции в локальную сеть, один из беспроводных адаптеров нужно настроить в качестве «ведущего»: необходимо выбрать идентификатор сети, метод аутентификации и шифрования, ключ сети, номер канала и т. п.

Данный режим конфигурации сетевого оборудования имеет свои плюсы и минусы.

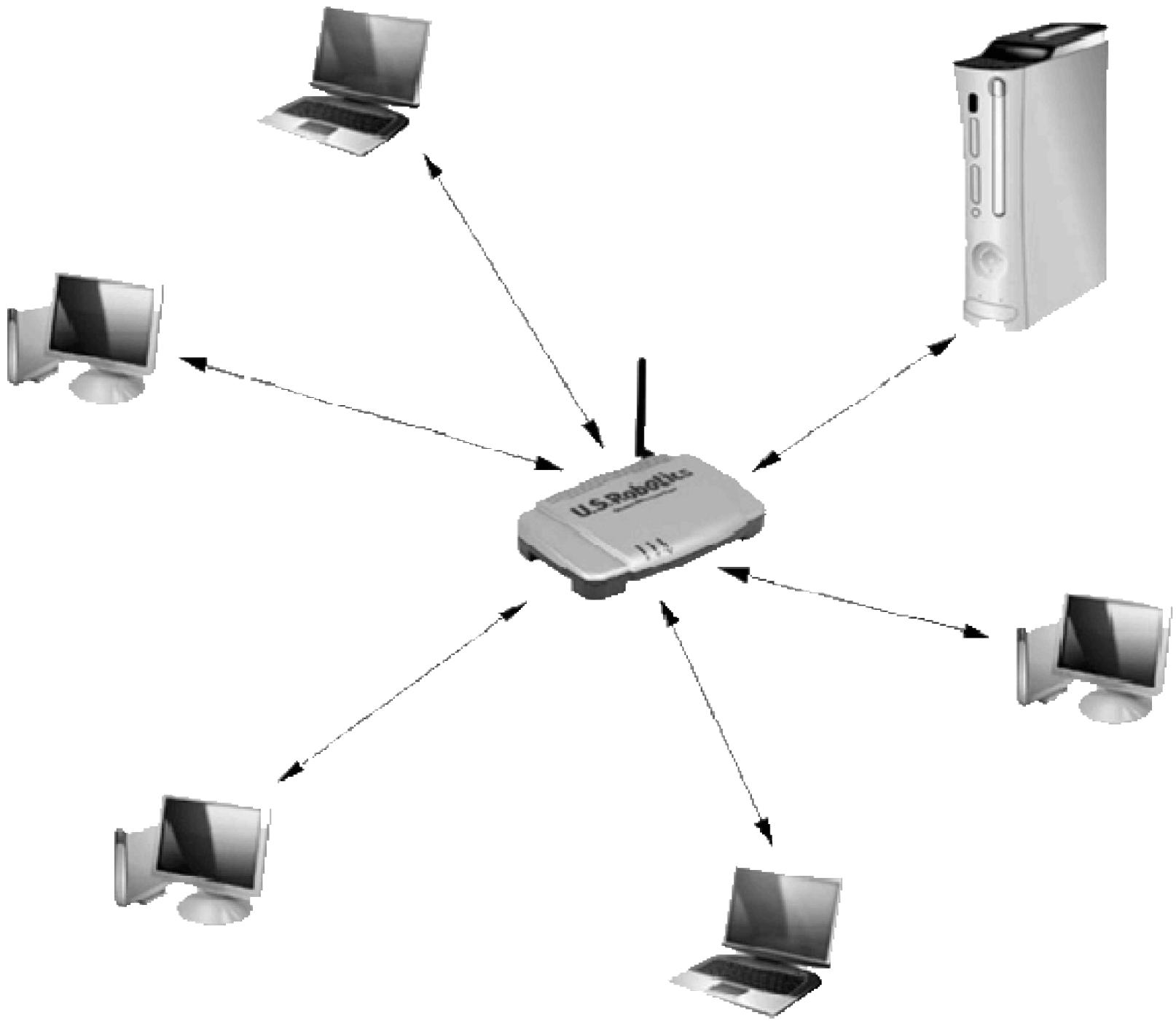
Главные минусы – низкая скорость передачи данных (не более 11 Мбит/с), которая к тому же делится между всеми участниками локальной сети, и малый радиус сети.

Из плюсов можно отметить быстрое развертывание сети в любых условиях, поддержку до 256 подключений, возможность соединения двух рабочих станций на значительном удалении друг от друга (10 километров и более).

Данная конфигурация сети идеально подходит, когда нужно быстро соединить между собой два компьютера, чтобы передать между ними небольшой объем данных. Если же требуется выполнение более серьезных задач, то данный режим неэффективен.

BBS

Базовый набор служб, или режим инфраструктуры, подразумевает использование центрального управляющего узла, называемого точкой доступа (Access Point). При этом все беспроводные адаптеры обмениваются между собой информацией, используя для этого данную точку доступа (рис. 19.2).

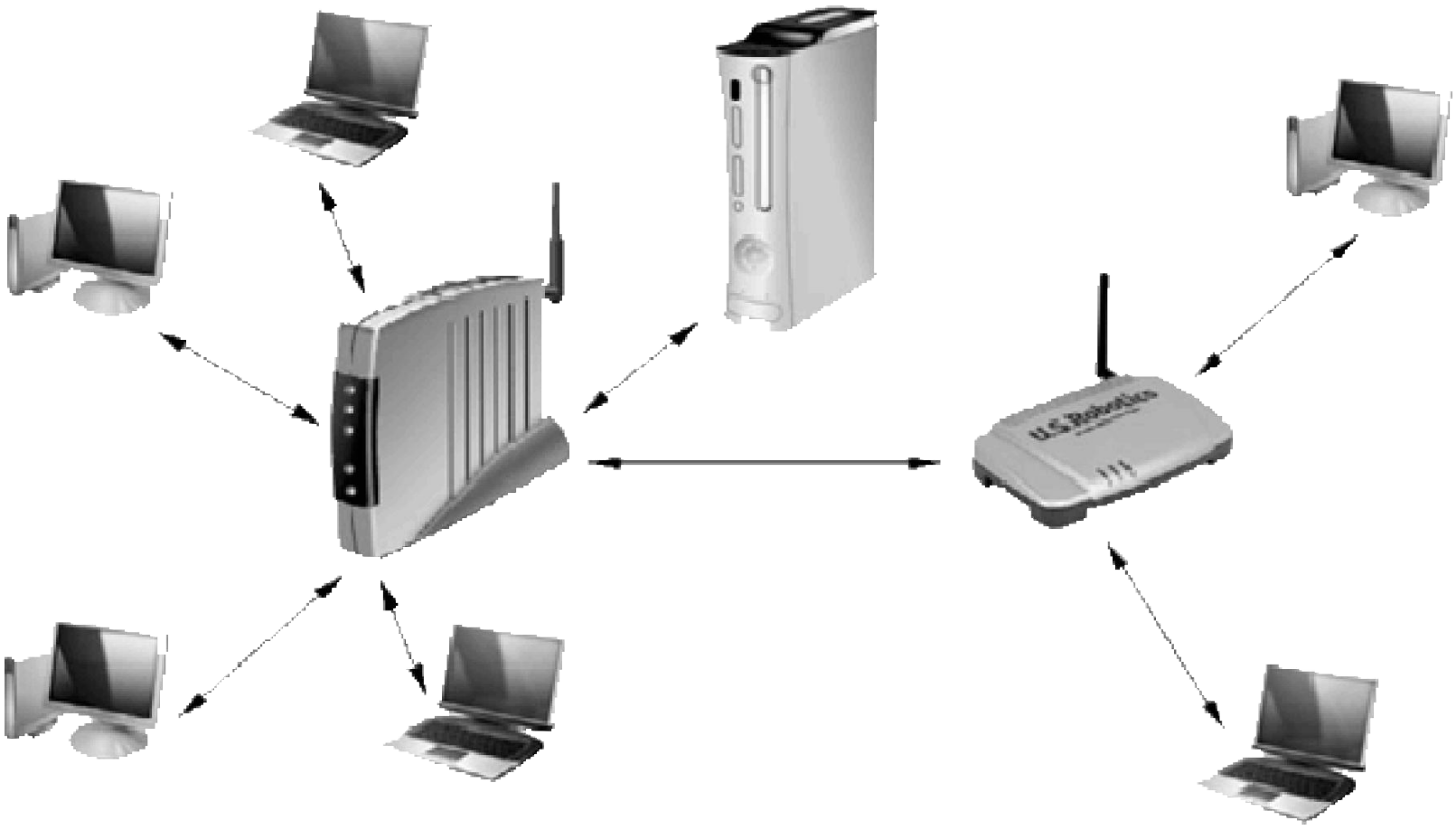


Вся необходимая для функционирования сети информация находится в точке доступа (идентификатор сети, метод шифрования и т. д.). Чтобы подключиться к ней, беспроводной адаптер должен иметь полностью аналогичные настройки.

Такой принцип организации работы является очень гибким и эффективным. Он позволяет быстро и легко менять методы шифрования и аутентификации, подключать дополнительные компьютеры и устройства, «чужеродные» сегменты сети и т. д.

Если снова провести аналогию с проводным вариантом сети, то режим инфраструктуры практически повторяет топологию «звезда». При этом технические показатели локальной сети зависят от возможностей точки доступа.

Отдельного внимания заслуживает возможность увеличения радиуса действия сети. Так, наиболее простой вариант сети подразумевает использование одной точки доступа, но их количество может быть и бóльшим. В этом случае получается некая модификация конфигурации сети, которая получила название расширенного набора служб (Extended Service Set, ESS) (рис. 19.3).



Если в беспроводной сети используется несколько точек доступа, они обмениваются между собой всей необходимой информацией, включая служебные данные. Кроме того, беспроводные адаптеры сами могут выбирать, к какой точке доступа им подключаться. Это позволяет получить более устойчивую связь или переключаться с одной точки доступа на другую, если беспроводной клиент перемещается.

Возможности точки доступа на этом не заканчиваются. Так, точка доступа может использоваться не только для обслуживания беспроводных устройств: зачастую она имеет один и несколько разъемов стандарта 100Base-TX или ему подобного, что позволяет соединять беспроводной и проводной сегменты сети в одно целое с возможностью маршрутизации пакетов между ними. Такой способ организации сети встречается на практике очень часто.

Методы обеспечения безопасности

Безопасности работы в локальной сети, а тем более безопасности ваших личных данных всегда необходимо уделять повышенное внимание. Даже несмотря на то, что разные данные представляют различную ценность, они в любом случае должны быть защищены от кражи и использования без вашего ведома. Согласитесь, вам вряд ли понравится, если содержимое вашей личной переписки узнает кто-то посторонний или результатами ваших продолжительных исследований воспользуется ваш конкурент. А еще меньше вам понравится, если в один прекрасный день вы обнаружите, что ваш банковский счет «внезапно» и без вашего ведома опустел и с этим уже ничего нельзя сделать.

Конечно, компьютерные сети имеют достаточно много механизмов, которые делают

работу пользователей более безопасной. Многие даже не подозревают об их существовании, но тем не менее они есть. Методы безопасности (шифрование и кодирование данных, аутентификация пользователей и устройств, ограничение прав на использование ресурсов и т. д.) разработаны с учетом требований и ограничений среды передачи данных.

В данном разделе мы рассмотрим основные нюансы методов безопасности, использующихся в беспроводных локальных сетях. Почему именно беспроводных? Все очень просто: если в проводных сетях подключение к сети можно проконтролировать, то отследить использование радиоэфира физически невозможно: злоумышленник может сидеть рядом за стенкой или через дорогу в автомобиле и, держа в руках ноутбук с беспроводным адаптером, перехватывать данные, транслируемые в сети. А обладая соответствующим программным обеспечением, расшифровать можно любую информацию. Именно поэтому так много внимания уделяется разработке и улучшению методов обеспечения безопасности в беспроводных сетях.

Разработка сетевых методов безопасности всегда ведется параллельно с созданием сетевых стандартов: занимаются этим все те же подкомитеты группы IEEE 802.

За все время существования локальных сетей было разработано, стандартизировано и внедрено в жизнь множество алгоритмов безопасности, которые с каждым разом становились все совершенней. На сегодня при работе беспроводного оборудования используются такие алгоритмы безопасности и аутентификации, как WPA, WPA2, AES, TKIP, RADIUS и др.

WEP

WEP (Wired Equivalent Privacy, беспроводной вариант защиты) – один из первых алгоритмов безопасности, обеспечивающий защиту данных, которые передаются по беспроводной локальной сети.

Разработка данного алгоритма началась в середине 90-х годов прошлого века. В его основу был положен популярный потоковый шифр RC4, который применяется в разных системах защиты информации, например в протоколах передачи данных SSL и TLS или для шифрования данных в операционной системе.

Шифр RC4 предусматривает возможность использования ключа переменной длины, вплоть до 256 байт, но WEP использует только два типа ключей – длиной 40 или 104 бита [5 - На самом деле используются ключи длиной 64 и 128 бит, но 24 бита применяются в качестве вектора инициализации, содержащего данные для расшифровки сообщения.], в связи с чем различают две версии алгоритма – WEP-40 и WEP-104.

Алгоритм WEP позволяет использовать всего два сервиса аутентификации: открытую систему и распределенный ключ. Как показала практика, как первый, так и второй варианты создают лишь видимость защиты. Так, по происшествии совсем небольшого времени после появления WEP был найден достаточно простой способ взлома этого алгоритма, для чего достаточно иметь беспроводной адаптер и соответствующую программу, умеющую перехватывать и анализировать пакеты сети: десять минут работы приложения – и вы получаете ключ подключения к точке доступа. А вскоре были найдены еще как минимум два способа взлома сети, позволяющие получить информацию, необходимую для подключения к точке доступа и ресурсам сети.

Пытаясь хоть как-то спасти репутацию беспроводных сетей, разработчики алгоритма WEP предложили его модификации – WEP2, WEP Plus и Dynamic WEP, – но существенных изменений это не принесло.

Открытая система

Аутентификация с помощью открытой системы, или аутентификация с открытым ключом, – наиболее простая среди существующих систем такого назначения.

В данном случае речь не идет об аутентификации в серьезном смысле этого понятия. Любой беспроводной клиент (компьютер) может подключиться к другому беспроводному клиенту или точке доступа. При этом компьютер отправляет запрос на подключение, содержащий данные об идентификаторе беспроводного адаптера. Если никаких исключений или других правил подключения, например таблиц MAC-адресов, на точке доступа не настроено, компьютер получает разрешение на подключение и сразу может начать работу в локальной сети. Если же по какой-либо причине беспроводной адаптер компьютера «не понравился» объекту, к которому он подключается, запрос на подключение отклоняется.

Распределенный ключ

Аутентификация на основе распределенного ключа, или аутентификация с общим ключом, представляет собой более защищенный вариант аутентификации. Смысл данного способа аутентификации заключается в том, что ключ соединения с беспроводной локальной сетью прописывается как в точке доступа, так и в беспроводном адаптере каждого клиента, который подключается к сети. Не зная данного ключа, не получится подключиться к беспроводной сети, поэтому администратор сети сам выбирает, кому сообщать этот ключ.

Процесс аутентификации с общим ключом состоит из трех этапов.

1. Беспроводной клиент посылает запрос на аутентификацию, указывая свой идентификатор и имеющийся у него ключ.

2. Точка доступа не сравнивает переданный клиентом ключ с ключом, указанным в настройках точки доступа, а отсылает в ответ так называемый «фрейм вызова» – случайный текст в открытом незашифрованном виде.

3. Получив «фрейм вызова», беспроводной клиент шифрует его, используя для этого имеющийся ключ, и отсылает результат обратно. При получении результата точка доступа выполняет противоположные действия, то есть декодирует полученный от клиента результат с помощью имеющегося у нее ключа. Если тексты совпадают, значит, клиент имеет право доступа. В противном случае запрос авторизации отклоняется.

WPA

WPA (Wi-Fi Protected Access, защищенный доступ к беспроводной сети) – один из алгоритмов шифрования и аутентификации, являющийся «наследником» WEP и появившийся в середине 2003 года.

Алгоритм WEP, служивший для защиты беспроводной сети, оказался слишком слабым для выполнения поставленной перед ним задачи. По этой причине появление его усовершенствованной версии – алгоритма WPA – вызвало целую бурю положительных эмоций у множества пользователей беспроводных сетей. Это, естественно, положительно повлияло на дальнейшее распространение беспроводных сетей.

WPA использует более стойкий алгоритм шифрования AES (Advanced Encryption Standard) и новые совершенные механизмы аутентификации. Компания Wi-Fi Alliance, которая является создателем WPA, дала данному алгоритму такую характеристику в виде формулы:

WPA = 802.1X + EAP + TKIP + MIC.

Это означает, что WPA работает вместе с сетевым стандартом IEEE 802.1X и алгоритмами AEP, TKIP и MIC.

AEP (Extensible Authentication Protocol) – расширяемый протокол аутентификации, который представляет собой набор из большого количества (порядка 40) методов аутентификации. Среди этих методов есть такие, как MD5, TLS, TTLS, PEAP, SIM, АКА, LEAP, FAST и др.

При этом используется специальный сервер аутентификации. Наиболее предпочтительным вариантом является применение RADIUS-сервера, содержащего данные о пользователях, которые имеют сертификаты, то есть сведения о тех пользователях, доступ которым к сервисам точки доступа разрешен. Если же возможности использования RADIUS-сервера нет, например в домашних условиях или в небольшом офисе, то часто применяют метод WPA-PSK (Pre-Shared Key), основанный не на системе сертификатов, а на парольном доступе по предварительно оговоренному общему ключу.

TKIP (Temporal Key Integrity Protocol) – механизм динамической генерации ключей шифрования, который позволяет сделать процесс обмена информацией более безопасным и исключает возможность перехвата данных. Данная система дает возможность снабдить временным ключом не только каждого беспроводного клиента, но и каждый пакет данных, который передается по сети. TKIP оперирует 128-битовыми ключами, которые генерируются и рассылаются автоматически.

После успешной аутентификации TKIP, используя алгоритмы 802.1X, генерирует базовый ключ для начала сеанса связи и отправляет этот ключ точке доступа и клиенту, а также настраивает систему генерирования динамических ключей и управления ими. Каждый новый динамический ключ не только отсылается клиенту и точке доступа, но и участвует в шифровании данных, поэтому подобрать его за короткое время невозможно (существует более 500 млрд вариантов).

MIC (Message Integrity Check) – система проверки целостности пакетов, позволяющая еще лучше защитить данные от их перехвата. MIC работает как на отправителе, так и на получателе, что позволяет максимально защитить передаваемые данные. Работает система очень просто: каждый пакет данных снабжается 8-битовым кодом целостности, который шифруется на этапе шифрования данных. При получении пакета с данными код целостности расшифровывается и заново вычисляется. Если результат сравнения положительный, пакет считается верным, если нет – ложным и отбрасывается. Кроме того, параллельно с этим ведется нумерация новых кадров, что также позволяет блокировать подмененные пакеты с данными.

Даже несмотря на все меры безопасности, принимаемые для защиты беспроводной сети с помощью протокола WPA, уже зафиксированы способы обхода системы защиты и получения доступа к данным. Наиболее «эффективный» из них позволяет сделать это менее чем за одну минуту, что сводит на нет все усилия по защите данных.

WPA2

Алгоритм WPA2 является модификацией WPA. Появление этого алгоритма связано с возникновением в 2004 году нового стандарта безопасности IEEE 802.11i.

ПРИМЕЧАНИЕ

Всесертифицированныеустройства, выпущенные с 2006 года, обязательно должны поддерживать этот алгоритм.

WPA2 – наиболее защищенный алгоритм шифрования данных, что делает его просто незаменимым для организации работы беспроводной локальной сети.

Как и WPA, WPA2 использует шифрование с помощью алгоритма AES со 128-битным

ключом. Изменения коснулись только «напарника» AES – механизма управления ключами TKIP. Ему на смену пришел метод CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, протокол шифрования с кодом аутентификации сообщения с режимом сцепления блоков и счетчика).

Метод CCMP использует более сложную систему управления ключами и создания контрольных сумм блоков, за счет чего каждый пакет данных увеличивается в длине на 16 байт, уменьшая полезную скорость передачи данных. Однако такой подход вполне оправдан: на сегодняшний день неизвестны способы взлома этого алгоритма, что вселяет надежду и гарантирует дальнейшее распространение беспроводных локальных сетей.

Глава 20
Законность работы беспроводной сети

Нельзя оставить без внимания еще один важный вопрос использования беспроводных сетей. Дело в том, что применение радиоволн в качестве среды передачи данных практикуется уже очень давно и повсеместно. Радиоволны используются не только в бытовых целях, например для обслуживания радиотелефонов или мобильной связи. Они применяются и для организации работы государственных органов: милиции, медицинских организаций и т. п. И если ваша или другая беспроводная сеть станет причиной сбоев важного оборудования, это может привести к непоправимым последствиям.

Учитывая этот факт, практически в каждой стране были созданы государственные организации, которые контролируют использование радиочастот. Они регистрируют появившиеся беспроводные сети и решают вопросы о разрешении или запрете работы новых беспроводных сетей. К сожалению, единых правил использования радиочастот не существует, поэтому в полной мере познакомить вас с особенностями этого вопроса невозможно. В связи с этим можно только посоветовать: перед тем как создать беспроводную сеть, ознакомьтесь с документами, которые освещают данный процесс.

В Российской Федерации контроль за использованием радиочастот возложен на Государственную комиссию по радиочастотам (ГКРЧ).

С недавних пор начало действовать положение, которое вносит некоторые поправки в существующий закон об использовании радиочастот, значительно упрощающие процесс регистрации беспроводных сетей, а в некоторых случаях даже позволяющие использовать беспроводные сети без разрешения ГКРЧ.

Таким образом, если вы собираетесь организовать работу беспроводной сети и хотите быть уверены, что никакие разрешения вам для этого не нужны, убедитесь в том, что выполняются следующие правила:

- беспроводная сеть находится внутри здания, закрытого складского помещения или производственной территории;
- используется оборудование, работающее в диапазоне частот 2400–2483,5 МГц;
- применяется оборудование, имеющее соответствующий сертификат для использования на территории России;
- используемые точки доступа имеют мощность излучения, не превышающую 100 мВт;
- используются только стандартные (идущие в комплекте) антенны без возможности подключения другой антенны либо присоединяется антенна, рекомендованная производителем оборудования.

Существуют и некоторые другие правила, но они имеют второстепенное значение. Если хотя бы один из пунктов правил не выполняется, требуется обязательная регистрация беспроводной сети в ГКРЧ и получение разрешения на использование диапазона радиочастот в указанном районе.

Обратите также внимание на то, что даже если вы создали беспроводную сеть с соблюдением всех перечисленных правил, но используете ее для оказания каких-либо платных услуг, вам не только придется пройти регистрацию и получить разрешение, но и дополнительно понадобится соответствующая лицензия на работу беспроводной сети.

Получить более детальную информацию по данному вопросу можно на веб-сайте Министерства связи и массовых коммуникаций Российской Федерации по адресу http://www.minsvyaz.ru, а также на специализированных форумах в Интернете.

Глава 21
Создаем сеть Wi-Fi

Организация беспроводной сети, в отличие от любого проводного варианта, требует от ее создателя минимум усилий, поскольку нет необходимости осуществлять монтаж кабельной системы. Единственное, с чем приходится столкнуться, – это выбор оптимального места расположения точки доступа. Его нужно выбирать с таким расчетом, чтобы уровень сигнала был достаточным для его приема всеми беспроводными адаптерами, установленными в компьютеры, стационарные или портативные.

Проектирование сети

Проектирование беспроводной сети, как и проектирование проводной сети, требует учитывать многие факторы, влияющие как на стоимость сети, так и на ее функциональность. Однако если проводная сеть полностью зависит от среды передачи данных и требует планирования будущего маршрута кабельных магистралей, то беспроводная сеть лишена этого недостатка. Тем не менее при проектировании беспроводной сети следует учитывать:

- потребность в скорости передачи данных;
- количество подключаемых компьютеров;
- необходимый уровень безопасность работы;
- возможность подключения дополнительных компьютеров и других устройств;
- возможность подключения сегментов с другой топологией и способом передачи данных, например проводных сегментов стандарта 100Base-TX.

Процесс проектирования беспроводной сети в основном аналогичен процессу проектирования проводной сети, поэтому повторяться не будем. Однако стоит понимать, что беспроводная передача данных, особенно на высокой скорости, требует основательного планирования, поскольку препятствие любого размера уменьшает не только скорость передачи данных, но и уровень сигнала, что в свою очередь приводит к резкому уменьшению радиуса сети.

На практике скорость передачи данных с использованием любого беспроводного сетевого стандарта значительно ниже теоретических показателей, поэтому в большинстве случаев беспроводные сети используют на ограниченных территориях, например в небольших офисах. Однако преимущество беспроводного вида связи в том, что беспроводную сеть можно организовать там, где использование любого типа кабеля нежелательно: в кафе, аэропортах, музеях и других общественных местах.

Выбор сетевого стандарта

Как вы знаете, за все время развития локальных компьютерных сетей было разработано достаточно много технологий беспроводной передачи данных. В частности, существует достаточно много спецификаций и стандартов, описывающих функционирование беспроводных сетей Wi-Fi.

В табл. 21.1 представлены основные технические показатели некоторых беспроводных стандартов, оборудование которых можно использовать для создания сети. (Напомним, что каждый из этих стандартов в качестве среды передачи данных использует радиоволны.)

Таблица 21.1.Сравнение основных сетевых стандартов

Сетевой стандарт	Скорость передачи данных, Мбит/с	Максимальное количество подключений	Максимальный радиус сети, м
802.11	2	128	300
802.11a	54	2048	100
802.11b	11	2048	300
802.11g	54	2048	300
802.11n	300	2048	450
Bluetooth 3.0	24	8	100

Понятно, что наиболее привлекательными являются стандарты с высокой скоростью передачи данных. Кроме того, оборудование с поддержкой современных стандартов вытесняет старое оборудование, поэтому вопроса выбора стандарта как такового не существует.

Что касается технологии Bluetooth, то на практике она применяется только в случае, когда необходимо быстро соединить 2–3 компьютера, а для соединения большего количества она уже малопригодна. Единственное, что оправдывает ее применение, – возможность обмена данными с мобильными устройствами, например коммуникаторами или наладонниками.

Таким образом, если речь идет о создании небольшой беспроводной сети, например в пределах нескольких комнат в офисе, обычно используют оборудование стандартов IEEE 802.11g или IEEE 802.11n. Как правило, используется оборудование обоих этих стандартов, поскольку адаптеры стандарта IEEE 802.11n в переносных компьютерах пока применяется редко. Тем не менее использование стандарта IEEE 802.11n считается идеальным вариантом, так как позволяет добиться максимально возможной скорости передачи данных на достаточно большом расстоянии.

Размещение точки доступа

Как уже говорилось, когда речь идет о такой среде передачи данных, как радиоволны, проектирование сети сводится в основном к определению наиболее оптимального размещения точки или точек доступа относительно используемых компьютеров.

При серьезном подходе для этого применяется специальное оборудование, позволяющее определить зоны покрытия сигналом точки доступа в зависимости от наличия преград и разного рода помех. В результате можно составить схему распространения волн и, анализируя ее, определить либо более оптимальное местоположение точки доступа, либо место (места) установки дополнительной точки доступа для увеличения зоны покрытия. Однако из-за того, что беспроводные сети проводятся в основном в небольших офисах или домашних условиях, таким методом поиска оптимального местоположения точки доступа не пользуются.

Итак, главная задача – определить оптимальное расположение точки доступа. Самый простой способ сделать это – использовать беспроводной адаптер ноутбука или другого переносного устройства следующим образом.

1. Установите ноутбук в место, где размещается наиболее удаленный компьютер.
2. Включите точку доступа и установите ее в предполагаемом центре пересечения всех компьютеров.
3. Проверьте на ноутбуке уровень сигнала от точки доступа.
4. Если сигнал есть, перенесите ноутбук к следующей отдаленной точке и снова проверьте уровень сигнала.
5. Если уровень сигнала слишком низкий и постоянно пропадает, передвиньте точку доступа в вертикальной или горизонтальной плоскости на расстояние не более 1 м в сторону ноутбука и снова проверьте уровень сигнала.
6. Если после прохождения всех мест расположения компьютеров в некоторых из них все же нет сигнала достаточного уровня либо связь постоянно обрывается, то необходимо исключить самый удаленный компьютер из списка, установить точку доступа в новом центре пересечения и повторить процесс проверки уровня сигнала сначала.

В результате этих простых действий вы сможете расположить точку доступа в том месте, откуда ее сигнал будет доступен всем участникам сети. При этом если в процессе поиска оптимального размещения точки доступа некоторые компьютеры были исключены из списка, необходимо задействовать дополнительную точку доступа, установив ее в центре пересечения исключенных устройств и первой точки доступа.

После этого, используя приведенный алгоритм, найти оптимальное расположение дополнительной точки доступа.

Организация работы беспроводной сети

Если ориентироваться на проект сети, то вам останется только установить точку доступа на место, признанное в процессе проектирования наиболее оптимальным, и заняться проверкой этого предположения на практике.

Сделать это достаточно просто – включите несколько противоположных по размещению компьютеров и попробуйте настроить связь с точкой доступа. Если это удалось с первого раза – можете себя поздравить: проектирование беспроводной сети прошло успешно. Если же со связью наблюдаются перебои, необходимо поступить так, как это было указано ранее: переставить точку доступа ближе к рабочим местам и установить дополнительную точку доступа, которая бы своим сигналом покрыла остальные компьютеры.

Если связь будет неустойчивой даже после установки дополнительной точки доступа, можно применить еще один способ: связать точки доступа с помощью кабеля «витая пара». Это позволит установить их там, где будет обеспечен максимальный радиус покрытия, и в то же время обеспечит максимальную скорость передачи данных между точками доступа.

Если вы действительно хотите добиться максимальной скорости работы беспроводной сети, придерживайтесь следующих рекомендаций.

- Уровень сигнала, а значит и скорость работы, зависит от расстояния, на котором находятся компьютеры от точки доступа. Поэтому повысить скорость передачи данных возможно только при уменьшении этого расстояния.
- Чем меньше препятствий, тем сильнее сигнал. Старайтесь располагать компьютеры в зоне прямой видимости точки доступа.
- Не используйте оборудование разных стандартов. Оборудование одного стандарта позволяет достичь максимально возможной для него скорости работы.
- Применение оборудования от разных производителей также нежелательно.

Оборудование от одного производителя позволяет использовать фирменные аппаратные разработки, например увеличенную скорость передачи данных.

▪ Установка нескольких точек доступа снижает общую скорость передачи данных, особенно между наиболее удаленными сегментами. По этой причине либо используйте более мощную точку доступа, либо применяйте кабель «витая пара» для соединения точек доступа.

Часть 4
Работа в составе локальной сети

Глава 22
Основные механизмы сети

Локальная сеть – и проводная, и беспроводная – это сложная структура, в основе которой лежат многие понятия: топология, среда передачи данных, протоколы передачи данных, оборудование и многое другое. С ними мы уже познакомились в предыдущих главах книги. Правильная организация работы всех этих составных частей позволяет добиться того, для чего, собственно, сеть и предназначена, – быстрой и надежной передачи данных.

Кроме большого объема работы, который скрыт от пользователя и часто выполняется без его участия на аппаратном уровне, есть и такие процессы, которые требуют его вмешательства. Сюда относятся настройка операционной системы для работы в сетевом окружении, настройка IP-адресации, выбор варианта подключения к сети и многое другое. В данной главе будут рассмотрены основные понятия, без понимания которых подключиться к сети и работать в ней невозможно.

Операционная система

Операционная система – интерфейс между пользователем и аппаратной частью компьютера. От ее возможностей зависит все: качество работы с программами, получение доступа к тем или иным возможностям локальной сети и Интернету, безопасность работы с внешними и локальными источниками данных и др.

На сегодня существует достаточно много операционных систем. Некоторые из них созданы для определенных производственных нужд, другие больше ориентированы на решение локальных задач, но подобные системы нас не интересуют. Главный интерес для нас представляют только те операционные системы, которые являются универсальными, то есть рассчитаны не только на локальную работу, но и на работу в сетевом окружении с реальными сетевыми задачами.

Практически все современные операционные системы подходят для работы в локальных сетях, но функциональные возможности операционных систем в этом плане существенно различаются. Принято выделять серверные и клиентские операционные системы.

Серверные операционные системы используются на серверах, установленных в локальной сети, поэтому они включают в себя множество системных механизмов, облегчающих работу администратора. С помощью этих механизмов осуществляется управление учетными записями пользователей и устройств сети, настраиваются уровни,

полномочия и права доступа к сетевым ресурсам и сервисам, обеспечивается сохранность важных данных и т. д. Среди продукции компании Microsoft примерами таких операционных систем выступают Windows 2000 Server, Windows Server 2003, Windows Server 2008.

Клиентские операционные системы, в отличие от серверных, лишены административной части управления работой локальной сети, да им это и не нужно. Такие системы не играют особой роли в жизни локальной сети и являются ведомыми, то есть управляются серверами. Клиентская операционная система содержит все необходимое – протоколы, службы и сервисы, – что требуется для подключений компьютера к локальной сети и получения от нее необходимого уровня обслуживания. Из продуктов компании Microsoft к таким операционным системам можно отнести Windows 98/XP/Vista и самую новую систему – Windows 7.

IP-адресация

IP-адресация – самый важный момент в организации работы любого типа сети, как глобальной, так и локальной. Каждое подключаемое к сети устройство должно обладать каким-то уникальным идентификатором, который позволит однозначно определить данное устройство. В качестве такого идентификатора выступает IP-адрес, за правильную работу которого отвечает протокол TCP/IP.

Протокол TCP/IP является универсальным. На сегодняшний день это единственный протокол, который применяется как в Интернете, так и в локальных сетях. Конечно, для работы локальной сети могут использоваться и другие протоколы передачи данных, но если речь идет о Windows-сетях, то без TCP/IP не обойтись.

В настоящее время существует две версии протокола TCP/IP: четвертая (TCP/IPv4) и шестая (TCP/IPv6). Эти протоколы различаются между собой разными принципами адресации и, соответственно, функциональностью.

Шестая версия протокола появилась, когда стало понятно, что 32 бита (именно такой длины IP-адрес) явно недостаточно для того, чтобы обеспечить адресами все нуждающиеся в этом устройства. В связи с этим было решено перейти на 128-битную адресацию. Однако TCP/IPv6 по ряду причин пока не смог стать единым стандартом, поэтому сегодня по-прежнему популярен протокол TCP/IPv4, который мы и будем рассматривать далее.

В основе работы TCP/IPv4 лежит принцип использования уникального идентификатора устройства, в качестве которого применяется IP-адрес – 32-битный набор из четырех десятичных цифр, разделенных точкой, например 192.168.1.2. Почему именно в таком виде? Каждая группа имеет свое предназначение и определение. При этом все вместе они позволяют идентифицировать данный узел и определить, к какой сети и подсети он относится.

Под адресацию отводится диапазон адресов 0.0.0.0-255.255.255.255 [6 - Примерно 4 млрд адресов (2554).]. Однако не все адреса из этого диапазона доступны для использования. Существуют адреса и даже целые диапазоны адресов специального применения, которые либо зарезервированы, либо имеют конкретное назначение. К таким, например, относятся адреса 0.0.0.0 (адрес узла владельца передаваемого пакета данных), 127.0.0.1 («закольцованный» адрес, позволяющий производить локальную отладку процессов), 255.255.255.255 (для широковещательной передачи данных) и др.

Ключевым понятием в IP-адресации является класс сети, который влияет на сам принцип адресации и выдачи адресов. Существуют три основных класса сети, которые различаются первым числом в группе чисел IP-адреса, то есть первым байтом адреса. В табл. 22.1 показано, как распределяются адреса в зависимости от класса сети.

Таблица 22.1.Принцип адресации в сетях различных классов

Класс сети	Диапазон, первый байт	Максимальное количество адресов в классе	Пример адреса
A	1–126	16 777 214	101.2.14.192
B	128–191	65 534	150.2.2.1
C	192–223	254	192.168.2.1

Класс сети определяет ее значимость в общей структуре, а также способ определения адреса подсети, адреса узла и количество компьютеров, которое она может обслуживать.

Изначально протокол TCP/IP предназначался для нужд Интернета, но в силу своей универсальности стал применяться и в локальных сетях. В связи с этим был разработан механизм раздачи адресов, главным действующим лицом в котором стала организация InterNIC (Internet's Network Information Center). Со временем, когда контроль над выдачей IP-адресов слишком усложнился, бóльшая часть контроля была возложена на основных интернет-провайдеров – владельцев IP-адресов сети класса A.

С процессом IP-адресации тесно связаны понятия классовой и бесклассовой адресации.

Классовая адресация основана на принципе определения класса сети с помощью метода, приведенного выше. Но практика показала, что данный способ адресации слишком неэффективный и приводит к быстрому истощению запасов свободных IP-адресов. Причиной тому стало очень быстрое появление больших и малых локальных сетей различных типов.

Для примера рассмотрим адреса, приведенные в таблице.

▪ 101.2.14.192. Данный адрес означает следующее: узел принадлежит сети класса A, адрес подсети – 101, адрес узла – 0.2.14.192, под адресацию отводится 3 байта, максимальное количество узлов – 16 777 214.

▪ 150.2.2.1. Данный адрес можно расшифровать так: узел принадлежит сети класса B, адрес подсети – 150.2, адрес узла – 0.0.2.1, под адресацию отводится 2 байта, максимальное количество узлов – 65 534.

▪ 192.168.2.1. Данный адрес означает следующее: узел принадлежит сети класса C, адрес подсети – 192.168.2, адрес узла – 0.0.0.1, под адресацию отводится 1 байт, максимальное количество узлов – 254.

Предположим, мы имеем дело с малой сетью, в состав которой входит 20 компьютеров. Следуя принципу классовой адресации, нашу локальную сеть следует отнести к классу C. Это означает, что ей необходимо выделить 254 IP-адреса, из которых реально задействованы будут только 20 IP-адресов, а 234 адреса останутся незадействованными. На одну такую сеть еще можно было бы закрыть глаза, но если взять тысячу подобных сетей, то в воздухе «зависнет» почти 23,5 тысячи адресов. Подобное расточительство недопустимо, поэтому решено было использовать другой способ адресации.

Бесклассовая адресация узлов использует более рациональный принцип, который позволяет выделять ровно столько адресов, сколько требуется для нужд сети.

Суть данного способа адресации состоит в следующем. Параллельно с 32-битным IP-адресом используется 32-битная маска подсети, которая также состоит из четырех чисел, разделенных точкой, но на этом сходство с IP-адресом заканчивается.

Применение маски базируется на следующем правиле: в двоичном представлении маски на месте адреса узла всегда стоят нули, а на месте номера сети – единицы. Пример работы

маски подсети приведен в табл. 22.2.

Таблица 22.2.Пример классового и бесклассового способа адресации

Параметр	**Значение**
IP-адрес: в десятичном представлении в двоичном представлении	 129.64.134.5 **10000001.01000000.10000110.00000101**
Параметр	**Значение**
Маска подсети: в десятичном представлении в двоичном представлении	 255.255.128.0 **11111111.11111111.10000000.00000000**
Номер подсети: при классовой адресации при бесклассовой адресации	 129.64.0.0 129.64.128.0
Номер узла: при классовой адресации при бесклассовой адресации	 0.0.134.5 0.0.6.5

Как видите, бесклассовый способ позволяет производить адресацию более гибко, а главное – гораздо экономнее. Главное средство управления адресацией в этом случае – маска подсети. Именно с помощью маски подсети вы можете разбивать локальную сеть на сегменты, используя при этом единственный IP-адрес, который вам выделен. Как это сделать и сколько компьютеров такая сеть сможет обслуживать? Это очень просто выяснить, используя правило маски: единицы стоят там, где указан номер подсети, то есть в нашем случае – сегмента.

На практике это выглядит следующим образом.

Предположим, имеется IP-адрес 129.64.134.5 и локальная сеть из 3 сегментов.

Согласно правилу маски для нумерации сегментов нам придется использовать 2 бита из восьми доступных (00 – первый сегмент, 01 – второй сегмент, 10 – третий сегмент, 11 – не используется). Это означает, что маска подсети будет иметь вид 11111111.11111111.11111111.11000000, а в десятичном представлении – 255.255.255.192.

Теперь несложно подсчитать, что 6 бит, которые остались для нумерации компьютеров сети, составят 64 IP-адреса (2 в степени 6), из которых два адреса окажутся недоступны для использования в силу правил резервирования. Таким образом получается, что в сети с четырьмя сегментами смогут работать только 62 устройства.

Если следовать данной логике, то становится понятно, что использование большого количества сегментов очень быстро уменьшает количество адресов для нумерации компьютеров, поэтому злоупотреблять этим не стоит.

На практике почти все локальные сети небольшого размера используют маску подсети 255.255.255.0, что позволяет применять для адресации узлов диапазон 192.168.1.1-192.168.1.254.

Рабочая группа

Основное предназначение локальной сети – использование общих ресурсов разного типа: файлов, принтеров, сканеров, хранилищ данных, Интернета и т. д. При этом основная задача – дать пользователю ровно столько, сколько ему нужно, и только то, что он может использовать. В противном случае можно получить хаотичную структуру, в которой каждый делает все, что ему захочется. Чтобы такого не произошло, существуют

определенные механизмы, контролирующие предоставляемый доступ. Одним из таких механизмов является рабочая группа.

Рабочая группа — это сообщество компьютеров и других устройств, у которого имеются свои правила использования ресурсов. Они основаны на правах доступа, которые определяют сами обладатели ресурсов. Компьютеры, входящие в состав рабочей группы, получают определенное положение. Оно выражается в уровне доверия, которое предоставляется этим компьютерам.

Количество рабочих групп зависит только от потребностей сети и пользователей, которые ее формируют. Компьютеры соседствующих рабочих групп могут получать доступ к ресурсам «чужой» рабочей группы. Однако в этом случае уровень доверия к компьютерам будет совсем другим, нежели к компьютерам из одной рабочей группы.

Создание рабочей группы дает некоторые преимущества:

- не нужно тратиться на покупку дополнительного оборудования;
- нет необходимости в дополнительном программном обеспечении;
- в большинстве случаев не требуется системный администратор, который следил бы за порядком в локальной сети.

Кроме всего прочего, каждый конкретный пользователь здесь «сам себе администратор», и только он решает, предоставлять общий доступ к своим ресурсам или нет.

Естественно, у использования рабочих групп есть и недостатки:

- практически полностью отсутствует административный контроль;
- при большом количестве компьютеров усложняется обслуживание сети;
- тяжело следить за работоспособностью клиентских компьютеров;
- отсутствуют механизмы централизованного архивирования важных данных.

Поддержка рабочих групп имеется во всех клиентских операционных системах, поэтому вы сами можете решить, когда, как долго и на каких условиях вы хотите находиться в той или иной рабочей группе.

Рабочие группы чаще всего используются в локальных сетях небольших офисов и в домашних локальных сетях. Основная причина этого – экономия денежных средств, которая заставляет отказаться от управляющих компьютеров. Однако рабочая группа более чем из 24 компьютеров – это уже парадокс.

Если же речь идет о локальной сети достаточно большой организации, то в этом случае гораздо разумнее будет использовать другой механизм – доменную структуру.

Домашняя группа

Понятие «домашняя группа» появилось с выходом Windows 7 и означает не что иное, как небольшую рабочую группу в домашних или офисных условиях, но с новыми возможностями.

Основными преимуществами домашней группы перед рабочей являются легкость и быстрота создания, а также контроль над подключением участников. Количество домашних групп в сети ничем не ограничено. При этом вы можете создать свою собственную группу или выбрать, в какой из групп вы хотите работать. Смена одной группы на другую происходит быстро и не требует перезагрузки компьютера.

Членство в группе может получить только тот компьютер и его пользователь, который одобрен владельцем группы. При этом пользователь получает пароль, используя который он может присоединиться к домашней группе. Это исключает самовольное подключение и использование ресурсов группы. Система доступа к группе по паролю работает достаточно эффективно, при этом если создатель группы решит изменить пароль, то ему не обязательно сообщать об этом остальным участникам группы: пароль изменится автоматически на каждом из подключенных компьютеров.

ПРИМЕЧАНИЕ

Одним из плюсов домашней группы является то, что подключиться к ней может даже компьютер, входящий в состав доменной структуры.

Количество общих ресурсов в домашней группе ограничивается лишь потребностями ее участников, при этом каждый сам решает, какие ресурсы будут доступны и кому из участников.

Количество участников домашней группы ничем не ограничивается, однако наиболее часто ее применяют при соединении нескольких компьютеров, о чем может свидетельствовать слово «домашняя».

К сожалению, воспользоваться преимуществами домашней группы могут только пользователи с операционной системой Windows 7 любой версии, кроме Starter и Home Basic.

Доменная структура

Доменная структура – наиболее сложная по организации структура из всех, которые позволяют объединять компьютеры в сеть. Однако несмотря на сложность доменная структура позволяет наиболее полно раскрыть возможности локальной сети по контролю доступа к информации.

Данный способ работы сети подразумевает наличие в ней специализированного, выделенного компьютера – сервера, который называется контроллером домена, главная задача которого – управление сетью. Иногда на контроллер домена возлагаются и дополнительные функции, например файлового сервера. Однако такой подход чреват определенными проблемами, которые могут вывести сервер из строя.

В качестве контроллера домена обычно используется мощный компьютер, на который устанавливается серверная операционная система.

Использование доменной структуры имеет ряд преимуществ, среди которых:

- контроль за подключением к локальной сети при помощи учетной записи пользователя;
- полный контроль над участниками сети;
- мощная система управления правами доступа;
- система архивирования;
- автоматическая установка необходимых пакетов обновления системы и программных продуктов;
- корпоративная антивирусная защита локальной сети.

Контроллер домена – самая уязвимая точка, от работоспособности которой зависит состояние всей локальной сети. Поэтому в локальной сети всегда устанавливается дублирующий сервер, который носит название вторичного контроллера домена и готов приступить к работе в любой момент.

DNS

Поскольку локальная сеть является частным случаем глобальной сети, то она должна придерживаться такого же принципа организации доступа к данным, как и в глобальных сетях. Если отступить от этих принципов, то функционирование сети может стать невозможным или ограниченным. В частности, если в будущем планируется подключение локальной сети к Интернету, то вам просто не обойтись без определенных механизмов, к которым, в частности, относится DNS.

DNS (Domain Name System, система доменных имен) – специальная общая для всех база данных, которая используется для установления соответствия между IP-адресом и последовательностью латинских букв и символов.

На практике это выглядит следующим образом. Каждый раз, когда вы в браузере набираете адрес www.google.ru, система преобразует эту строку в ее числовое представление, а именно, в IP-адрес 74.125.87.99, и именно этот адрес (как уникальный идентификатор) используется для поиска соответствующего компьютера, на котором находится ресурс www.googLe.ru. Как результат – вам не приходится запоминать какие-то числа, а нужно лишь запомнить связный набор букв.

Кроме транслирования IP-адресов для Интернета DNS-сервер выполняет аналогичную работу и для локальной сети, поскольку в ней также могут существовать веб-ресурсы локального использования или, например, почтовый сервер.

Чтобы база данных DNS оставалась актуальной, в Интернете существует достаточно разветвленная сеть DNS-серверов, которые постоянно обмениваются между собой информацией, придерживаясь принципа старшинства.

Данный принцип работает очень просто. Предположим, пользователь набрал в адресной строке браузера адрес веб-узла и запустил поиск. Браузер, как того требуют правила, имеет в локальной сети DNS-сервер, чтобы по указанной адресной строке получить IP-адрес данного ресурса, присоединиться к нему и получить необходимые данные. Если локальный DNS-сервер в своей базе данных не находит нужное соответствие либо DNS-сервер просто отсутствует в локальной сети, производится поиск DNS-сервера в сети, которой принадлежит данная локальная сеть. Если он обнаружен, то выполняется поиск соответствия в его базе. Если нужное соответствие опять не найдено либо не найден сам DNS-сервер, процедура повторяется, только запрос уже идет в сеть уровнем выше и т. д. В итоге либо искомое соответствие будет найдено, либо будет получен негативный результат, свидетельствующий о том, что адрес введен неверно или данного веб-ресурса не существует.

При регистрации нового веб-ресурса информация об этом сначала поступает в DNS-серверы верхнего уровня, а затем постепенно передается на нижние уровни. В результате через сравнительно небольшой промежуток времени о регистрации ресурса узнают все DNS-серверы и он становится доступным для просмотра браузерами или другими программами.

DNS-сервер применяется только в случае, если используется доменная структура сети. Если доступ к сети организован на уровне рабочих групп или без них, вся необходимая для работы информация приходит с DNS-сервера родительской сети.

DHCP

Согласно существующим правилам (не забывайте об уникальности идентификатора устройства) IP-адрес должен быть у каждого компьютера или устройства, которое подключено к локальной сети. Исключения могут быть сделаны только в случаях, когда для организации работы локальной сети используются другие протоколы передачи данных, например протоколы от Novell NetWare. Если же рассматривать Windows-сети, то обязательным является применение TCP/IP-протокола, а значит, и IP-адресации.

Если говорить просто о сложном, то DHCP-сервер используется для статической и динамической IP-адресации устройств локальной сети.

Наиболее просто объяснить его работу можно следующим образом. В сети существует как важное оборудование (серверы, маршрутизаторы, сетевые принтеры), доступ к которому должен быть постоянным, так и оборудование, от которого работоспособность сети не зависит, например компьютер пользователя. Важное оборудование всегда должно быть доступно по постоянному, то есть статическому идентификатору, а «обычному»

оборудованию достаточно будет получить динамический идентификатор. Таким образом, если вернуться от простого к сложному, из доступного диапазона IP-адресов важное оборудование всегда получает статичные IP-адреса, а все остальное оборудование – динамичные IP-адреса.

Active Directory

Active Directory – наиболее сложный объект, используемый в сетях под управлением сервера. Active Directory является основным инструментом администратора, с помощью которого он управляет всем, что связано с работой локальной сети: учетными записями пользователей и компьютеров, работой сетевых принтеров, правами доступа к общим ресурсам, политиками безопасности и т. д.

SSID

SSID (Service Set Identifier, идентификатор беспроводной сети) – это не что иное, как имя беспроводной сети, которое позволяет выделить ее из других сетей, работающих по соседству. Идентификатор сети представляет собой любой набор латинских букв, знаков и цифр длиной не более 32 бита. Как правило, это слово или словосочетание, которое легко запомнить, например the_best_network, хотя ничто не мешает использовать и что-то бессвязное типа leg_lad00be.

Эта последовательность символов играет важную роль. Ее должен знать каждый, кто хочет подключиться к данной беспроводной сети. Конечно, знать только SSID недостаточно для подключения, однако он необходим для настройки беспроводного оборудования. Например, точка доступа сообщает о своем присутствии именно с помощью идентификатора сети. Но возможен режим работы точки доступа, когда SSID не транслируется в целях безопасности, поэтому, если вы собрались подключаться к беспроводной сети, знать его необходимо.

Глава 23
Настройка сетевого расположения

Работа компьютера в составе локальной сети требует от операционной системы соответствующей адаптации. Причина этого достаточно проста: компьютер попадает в среду, которая может стать причиной его нестабильной работы и значительно повышает шанс стать объектом вирусной или иной атаки.

Кроме того, активируется работа стандартных сетевых механизмов, с помощью которых компьютер может отправлять и получать данные, подключаться к общим ресурсам и использовать их и т. д.

В отличие от более ранних операционных систем, например Microsoft Windows XP, операционная система Windows 7 при работе с сетевым окружением шагнула далеко вперед в плане защиты компьютера. При этом защита операционной системы носит комплексный характер и позволяет настраивать практически любую сетевую возможность, например сетевое обнаружение, доступ к файлам, доступ к принтерам и т. д.

В Windows 7 впервые появилось понятие сетевого размещения. Выбор сетевого размещения влияет на уровень защиты операционной системы от возможного воздействия локальной сети, поэтому если правильно подобрать тип размещения, это позволит получить большую защиту.

К примеру, если компьютер работает в составе домашней группы, то сетевое размещение будет иметь больший уровень доверия, нежели при работе компьютера в общественной локальной сети, например в аэропорту. При этом компьютер будет виден другим пользователям сети, а также сможет сам их видеть. Если же вы подключите компьютер к общественной сети, то останетесь невидимы для окружающих.

В Windows 7 используются следующие варианты сетевого размещения.

▪ Домашняя сеть. Это сетевое размещение подразумевает, что компьютер входит в состав небольшой локальной сети, участники которой вам знакомы, а уровень доверия к ним вполне высокий, что позволяет не беспокоиться о сетевых угрозах. Данный вариант размещения устанавливается автоматически, когда вы впервые подключаетесь к одной из домашних групп.

▪ Сеть предприятия, или Рабочая сеть. Данное сетевое размещение подразумевает, что компьютер входит в состав рабочей сети, размер которой не столь важен, главное – достаточный уровень доверия, что позволяет оценивать сеть как доверенную.

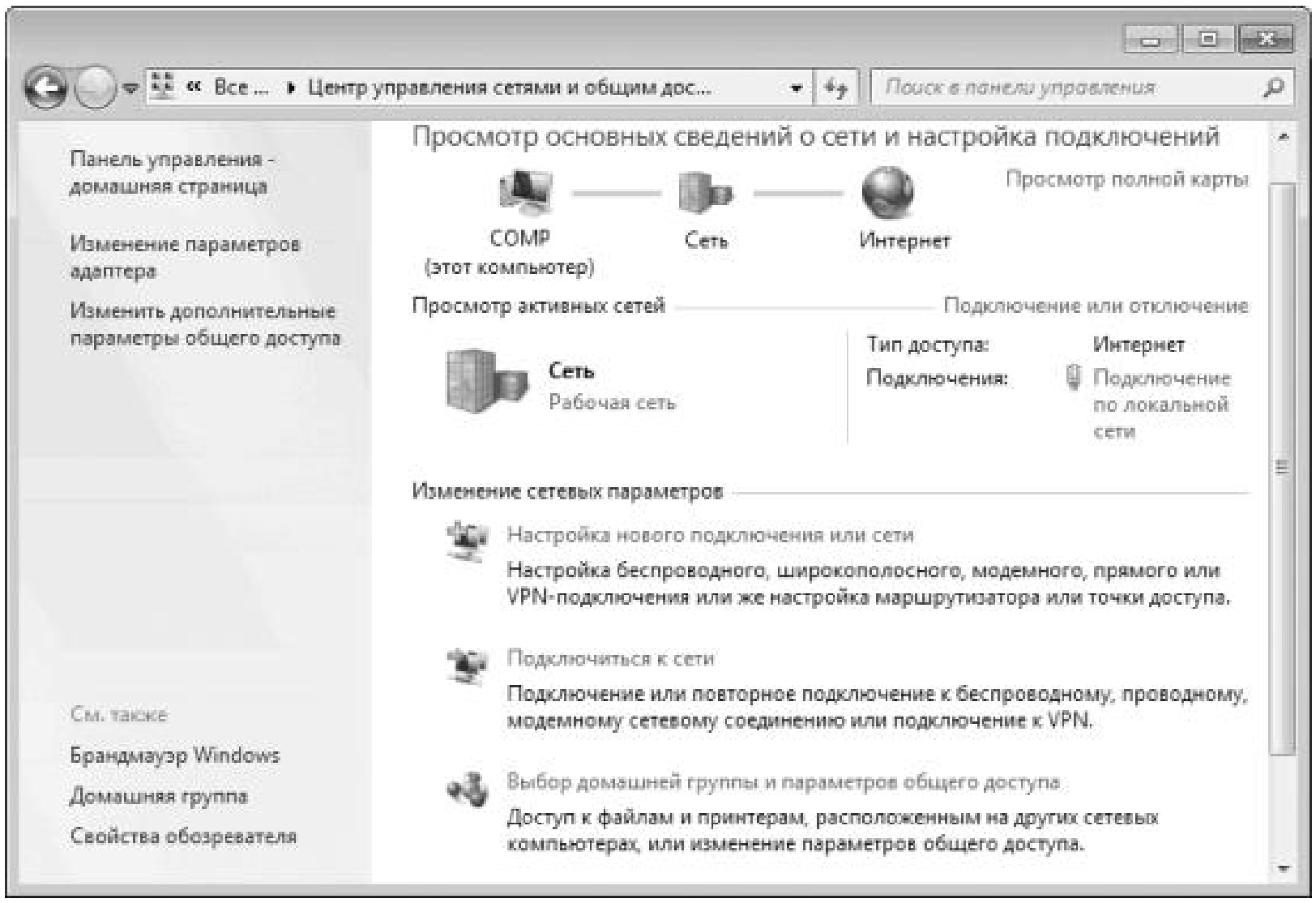
▪ Общественная сеть. Это сетевое размещение подходит для подключения компьютера к случайной или непостоянной сети. Примером такой сети может быть зона Wi-Fi, например в кафе или аэропорту. По понятным причинам данная сеть обладает наименьшей степенью доверия. При ее использовании активируются соответствующие механизмы защиты операционной системы.

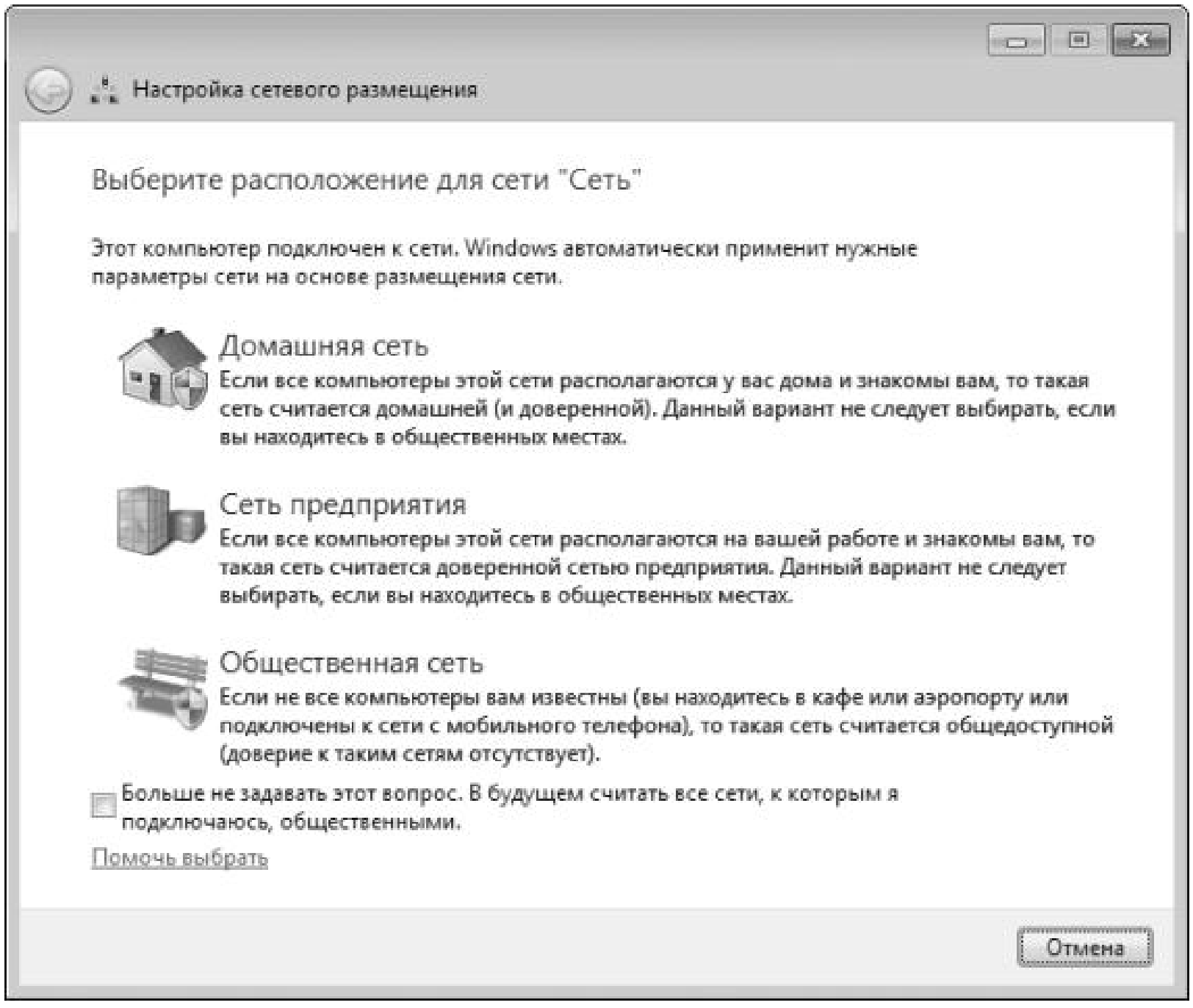
▪ Доменная сеть. Наиболее доверенный тип сетевого размещения, выбор которого в обычном режиме недоступен. Смена на этот тип сетевого размещения происходит автоматически и только в том случае, когда компьютер подключается к домену.

Окно смены сетевого размещения появляется каждый раз, когда компьютер подключается к новой локальной сети, например каждый раз, когда к сетевому адаптеру подключается кабель или беспроводной адаптер подключается к точке доступа. Кроме того, смену сетевого размещения вы можете произвести в любой момент сами, используя для этого системный компонент Центр управления сетями и общим доступом, запустить который можно из Панели управления (рис. 23.1).

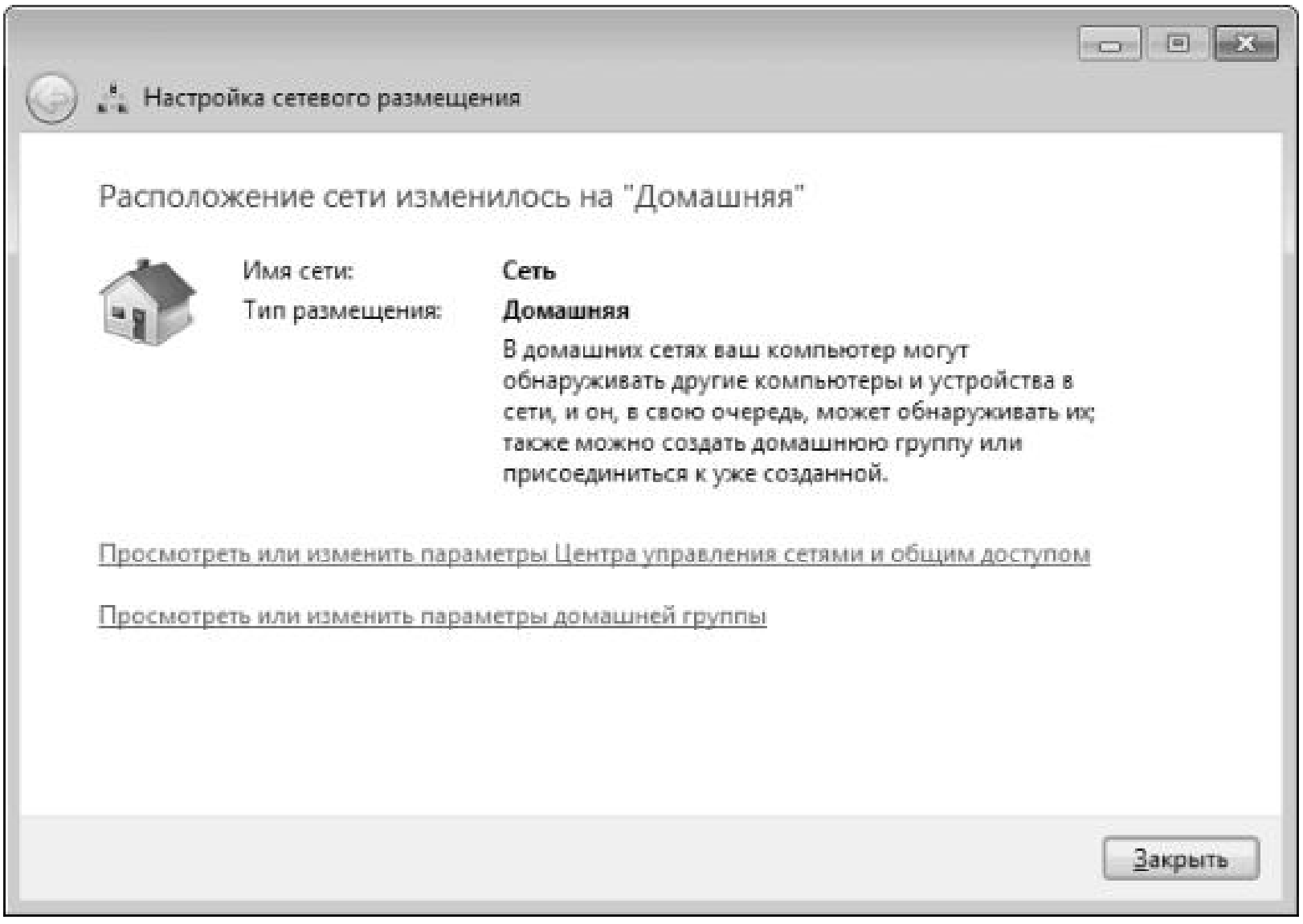
Здесь отображается вся необходимая информация о подключении: тип сетевого размещения, используемое сетевое подключение, наличие доступа к Интернету и т. д.

Чтобы сменить сетевое размещение, щелкните на названии текущего сетевого размещения (в нашем случае это Рабочая сеть). В результате откроется окно со списком сетевых размещений (рис. 23.2).


« Все ... ▸ Центр управления сетями и общим дос...
Поиск в панели управления
Панель управления - домашняя страница
Изменение параметров адаптера
Изменить дополнительные параметры общего доступа
См. также
Брандмауэр Windows
Домашняя группа
Свойства обозревателя
Просмотр основных сведений о сети и настройка подключений
Просмотр полной карты
COMP
(этот компьютер)
Сеть
Интернет
Просмотр активных сетей
Подключение или отключение
Сеть
Рабочая сеть
Тип доступа:
Интернет
Подключения:
Подключение по локальной сети
Изменение сетевых параметров
Настройка нового подключения или сети
Настройка беспроводного, широкополосного, модемного, прямого или VPN-подключения или же настройка маршрутизатора или точки доступа.
Подключиться к сети
Подключение или повторное подключение к беспроводному, проводному, модемному сетевому соединению или подключение к VPN.
Выбор домашней группы и параметров общего доступа
Доступ к файлам и принтерам, расположенным на других сетевых компьютерах, или изменение параметров общего доступа.



Отредактировал и опубликовал на сайте : PRESSI (HERSON)



Далее достаточно просто щелкнуть на нужном размещении. Например, если вы собираетесь подключиться к рабочей или домашней группе, для этого подойдет вариант Домашняя сеть. Если же вы хотите подключиться к домену, выбирать сетевое размещение не стоит, поскольку оно все равно автоматически изменится на другое.

Смена сетевого размещения происходит достаточно быстро и сопровождается появлением соответствующего окна (рис. 23.3).

После этого, если того требуют правила, можно приступать к изменению других параметров, влияющих на работу в локальной сети: принадлежности к сетевой группе, доступа к ресурсам, изменения параметров TCP/IP и т. д.

Глава 24
Работа в составе рабочей группы

Как вы уже знаете, рабочая группа – один из самых простых способов организации работы компьютеров в локальной сети. Простота одновременно является как ее преимуществом, так и недостатком.

Поддержка работы в составе рабочей группы имеется в любой современной операционной системе, в том числе и в Windows 7. Мало того, механизмы работы в составе рабочей группы не изменялись еще со времен операционной системы Windows 95, поэтому говорить о каких-либо особых преимуществах рабочей группы в современных условиях не приходится.

Тем не менее использование рабочих групп достаточно распространено, особенно когда дело касается небольших сетей из 10–15 компьютеров. Кроме того, рабочие группы – излюбленный способ организации работы в домашних сетях.

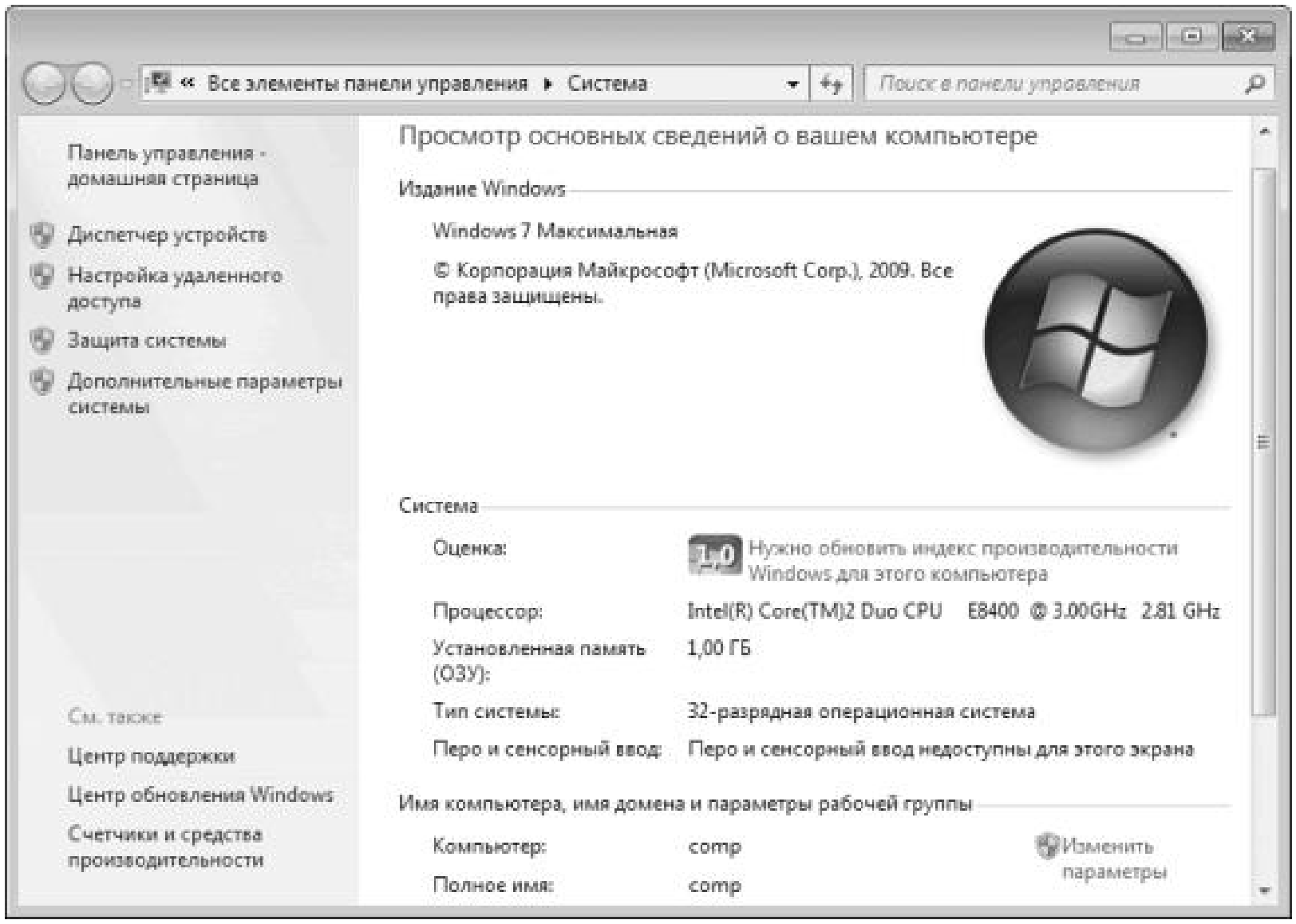
Подключение компьютера к рабочей группе не вызывает никаких сложностей, тем более

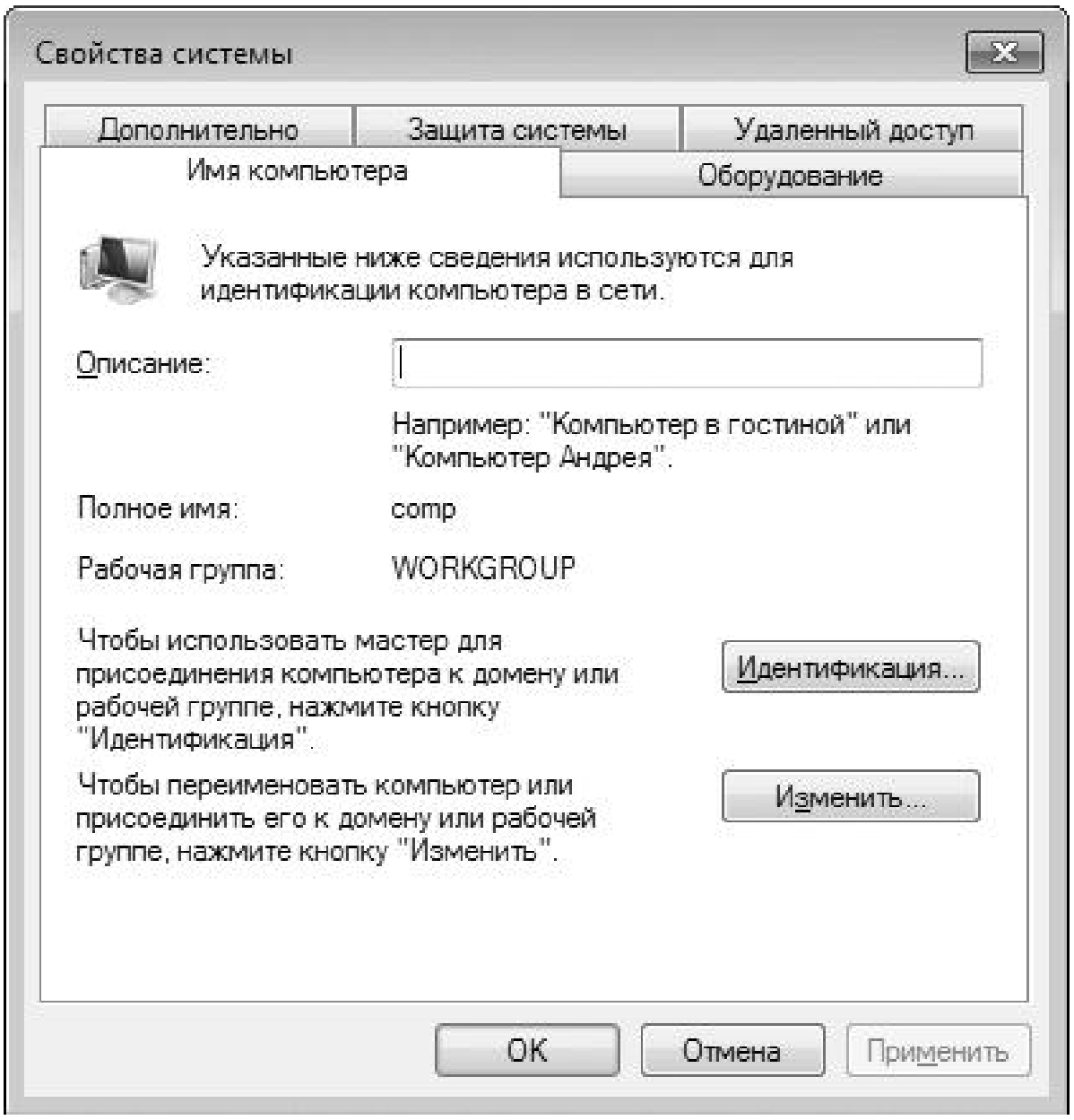
что для этого даже не потребуется пароль или другой способ авторизации. Единственное, что может понадобиться при подключении к рабочей группе (кроме ее названия, конечно), – это конкретный IP-адрес и маска подсети.

Теоретическая часть закончилась, переходим к практическим указаниям.

Для начала необходимо открыть механизм Система, запустить который можно с Панели управления. В результате появится окно, показанное на рис. 24.1.

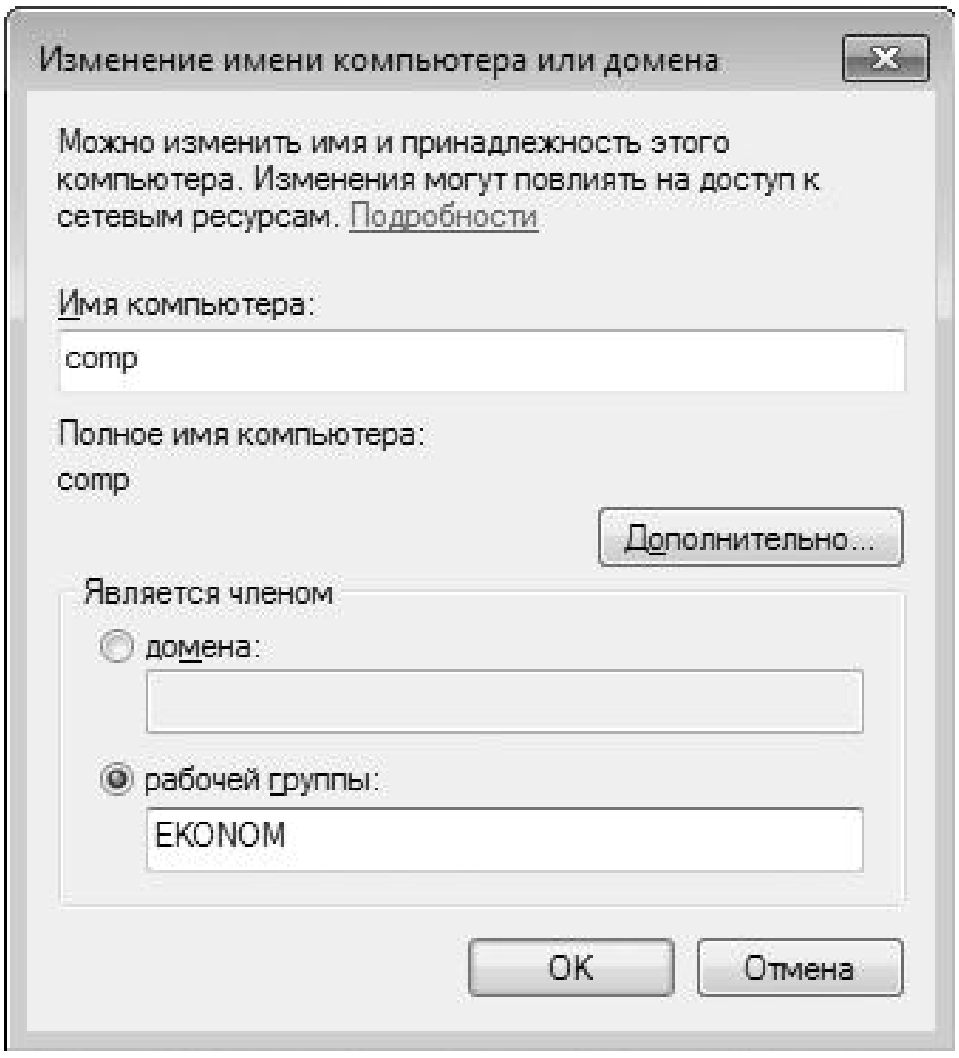
Здесь отображается некоторая информация о компьютере, а также сведения об имени компьютера и его текущей принадлежности к какой-либо сети. Кроме того, здесь находится механизм изменения этого состояния. Чтобы им воспользоваться, перейдите по ссылке Изменить параметры (рис. 24.2).

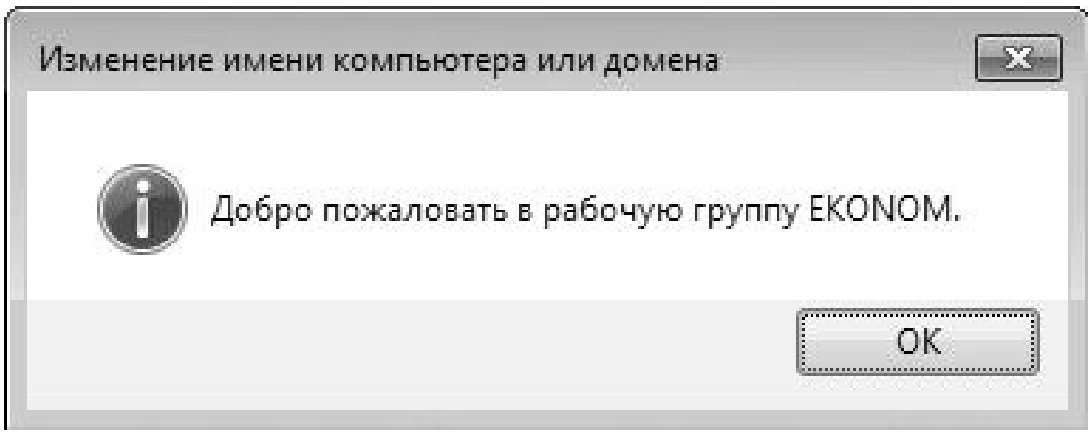




В появившемся окне отображаются описание компьютера, его имя и рабочая группа или домен, к которому он принадлежит. Здесь же присутствуют две кнопки, позволяющие подключить компьютер к рабочей группе или домену.

Для подключения компьютера к рабочей группе щелкните на кнопке Изменить. В результате появится окно, показанное на рис. 24.3.





Чтобы подключить компьютер к нужной рабочей группе, достаточно просто ввести ее название в соответствующее поле и нажать кнопку OK. Как уже говорилось выше, никакой авторизации при этом не требуется, поскольку сам принцип организации рабочей группы подразумевает свободное членство в ней.

Буквально через несколько секунд появится окно с подтверждением того, что компьютер подключен к рабочей группе (рис. 24.4).

Если того требуют правила подключения к рабочей группе, необходимо будет изменить настройки TCP/IP, прописав подходящий IP-адрес и маску подсети. Как это правильно

сделать, рассказано в гл. 27.

Теперь, чтобы начать полноценную работу уже в составе этой рабочей группы, вам остается только перезагрузить компьютер.

Глава 25
Работа в составе домашней группы

Как уже упоминалось, домашняя группа – одно из основных нововведений, которыми может похвастаться Windows 7. Используя домашние группы, вы можете быстро и просто объединить несколько доверенных компьютеров в одну локальную сеть и использовать их ресурсы.

Ниже мы рассмотрим пример создания домашней группы и подключения к уже существующей домашней группе.

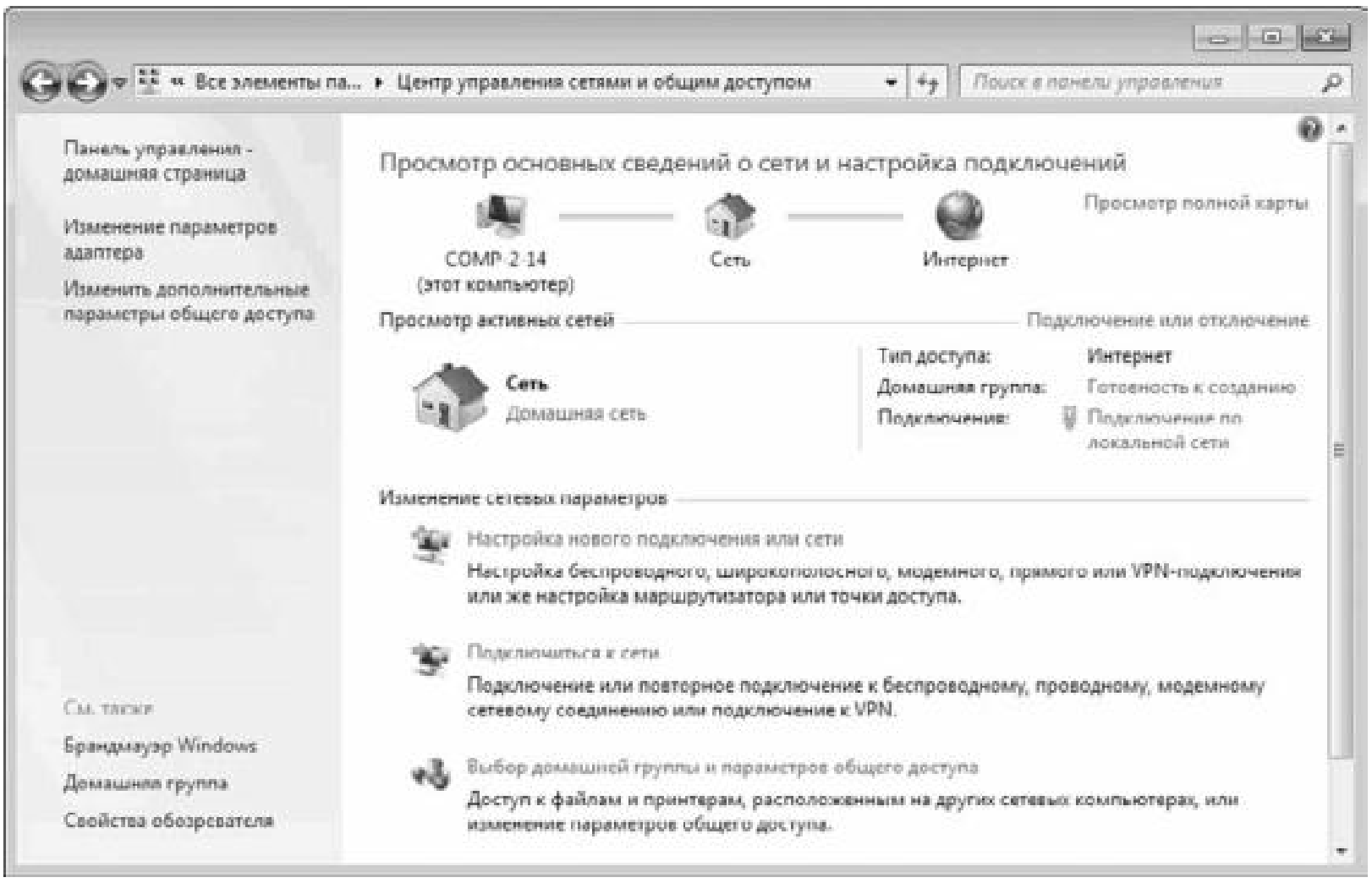
Создание домашней группы

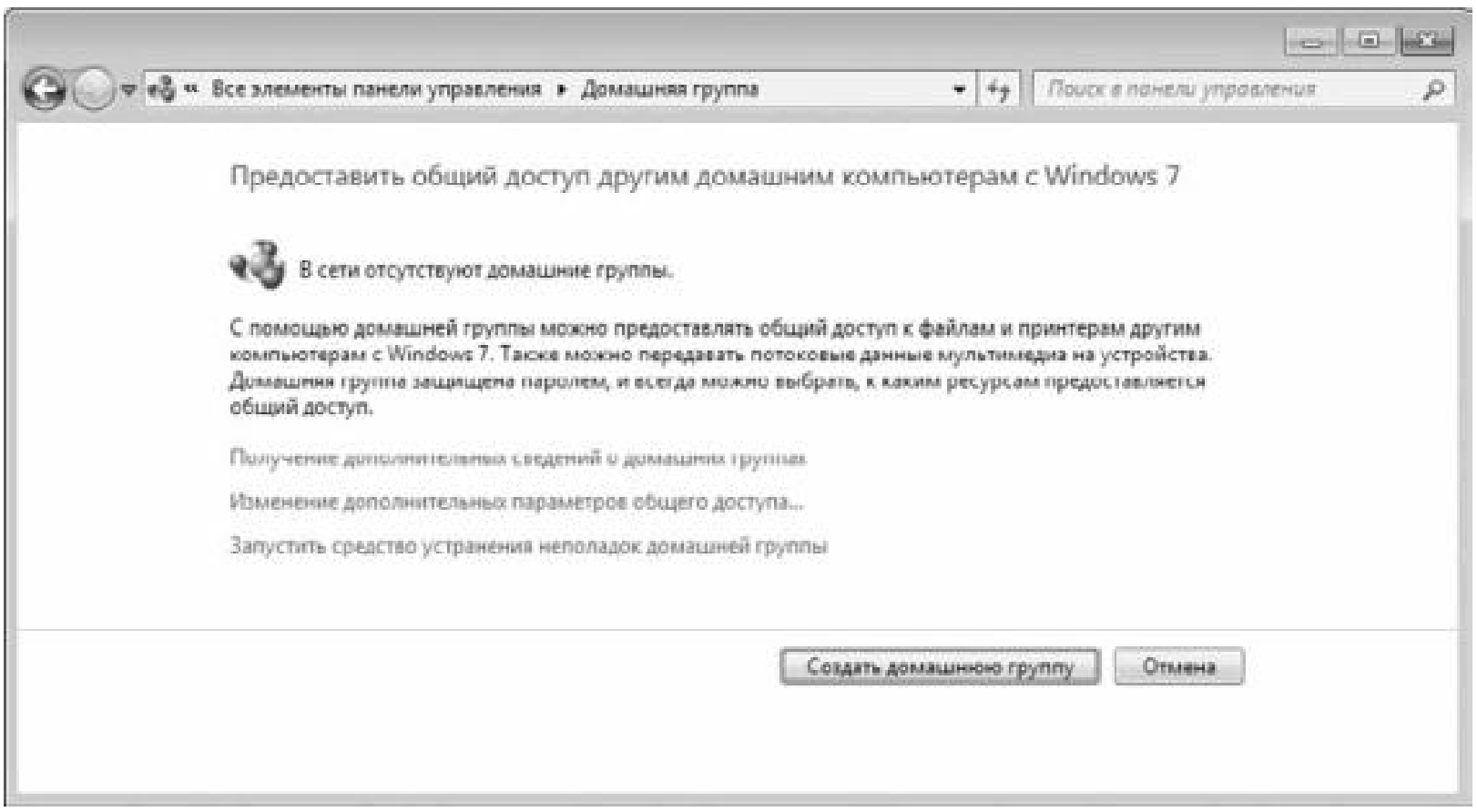
Создание домашней группы происходит очень просто и быстро. Как обычно, когда необходимо настроить сетевое окружение, используем для этого компонент Центр управления сетями и общим доступом, запустить который можно с Панели управления.

Для начала нам потребуется сменить сетевое размещение, установив значение Домашняя сеть, как это показано на рис. 25.1.

Если сетевое размещение другое (обратите внимание на надпись под словом Сеть), щелкните по этому сетевому размещению и в появившемся окне выберите пункт Домашняя сеть (см. рис. 23.2). Смена сетевого размещения происходит достаточно быстро, и уже через несколько секунд вы увидите окно (см. рис. 23.3), сообщающее о выполнении команды.

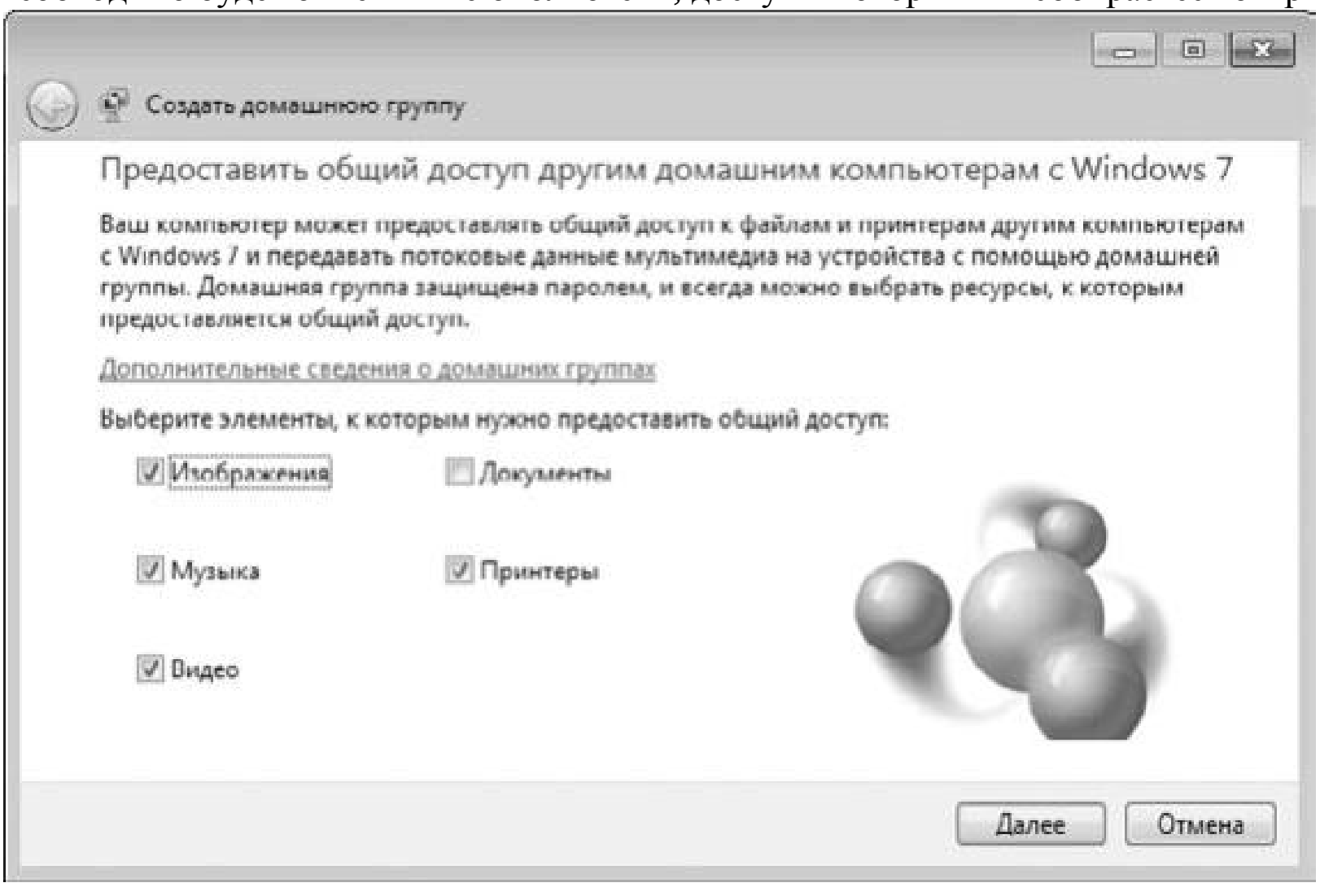
Теперь можно приступить непосредственно к созданию домашней группы. Вообще, любые действия, связанные с домашними группами, осуществляются с помощью системного механизма Домашняя группа, который можно запустить с Панели управления (рис. 25.2).





Сразу после этого мастер управления домашними группами произведет поиск домашних групп в сети. Если таких нет, то в окне появится надпись В сети отсутствуют домашние группы. Если же будет найдена домашняя группа, появится несколько дополнительных позиций, используя которые можно подключиться к группе.

Наша задача – создать свою собственную домашнюю группу. Для этого нажмите кнопку Создать домашнюю группу. В результате появится окно (рис. 25.3), в котором вам необходимо будет отметить те библиотеки, доступ к которым вы собираетесь открыть.



Немного о библиотеках. На самом деле нет ничего общего между папкой и библиотекой, поскольку библиотека – это не что иное, как набор ссылок на разные объекты, которые могут находиться в абсолютно разных папках, на разных дисках и даже сетевых компьютерах. Библиотека является динамичной, то есть вы в любой момент можете добавлять в нее ссылки или удалять их.

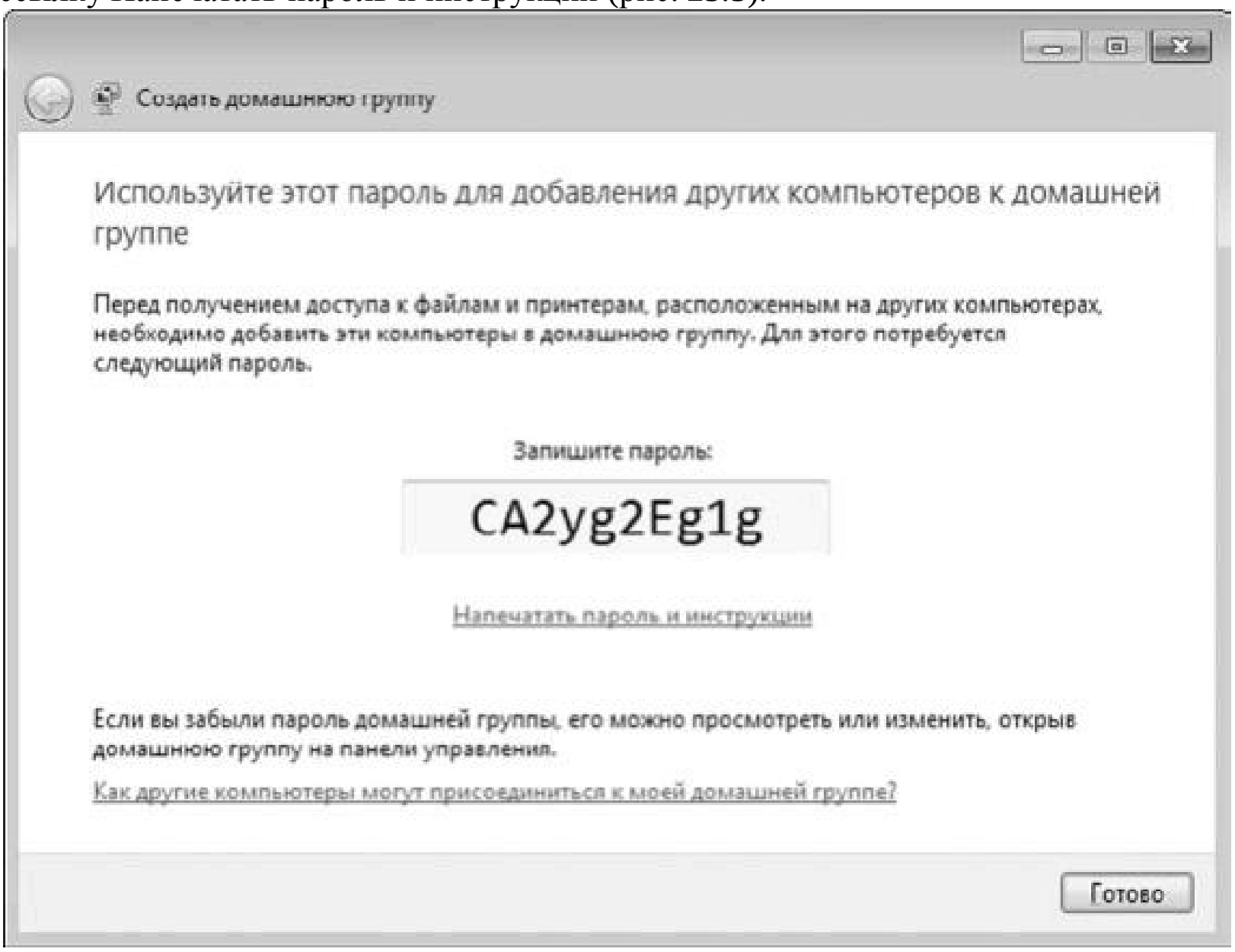
По умолчанию в Windows 7 используется несколько стандартных библиотек, названия которых вы можете увидеть в показанном выше окне. Открывать к ним доступ или нет – решать вам, но знайте, что доступ к той или иной библиотеке можно всегда закрыть, поэтому даже если вы сейчас сделаете что-то не так, в дальнейшем это можно будет исправить. Кроме того, ничто не мешает создать вам свою библиотеку, содержащую ссылки на любые ресурсы.

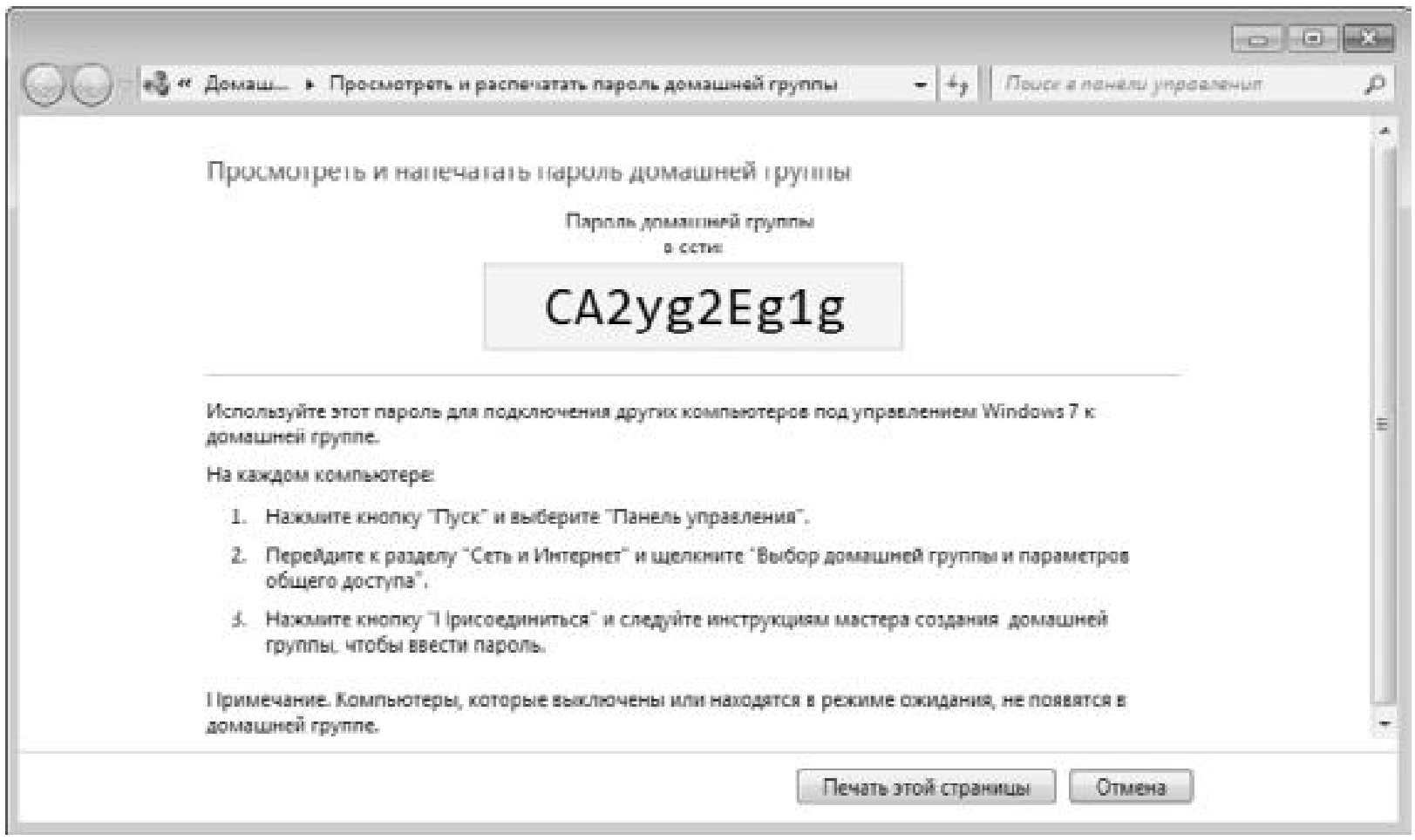
После нажатия кнопки Далее мастер произведет необходимые изменения в параметрах системы, что займет буквально несколько секунд. После этого появится окно, в котором

будет отображен пароль подключения к данной домашней группе (рис. 25.4).

Этот пароль будет необходим в том случае, если вы разрешите подключение к своей домашней группе другим сетевым участникам. Сообщив этот пароль, вы тем самым разрешите им подключиться и использовать ваши ресурсы.

Очень полезной функцией является возможность распечатать данный пароль, который к тому же снабжается короткой инструкцией, как подключиться к домашней группе. Распечатав листок с инструкцией, вы избавите себя от глупых вопросов, которые могут появиться у участников к сети при подключении. Чтобы сделать распечатку, используйте ссылку Напечатать пароль и инструкции (рис. 25.5).



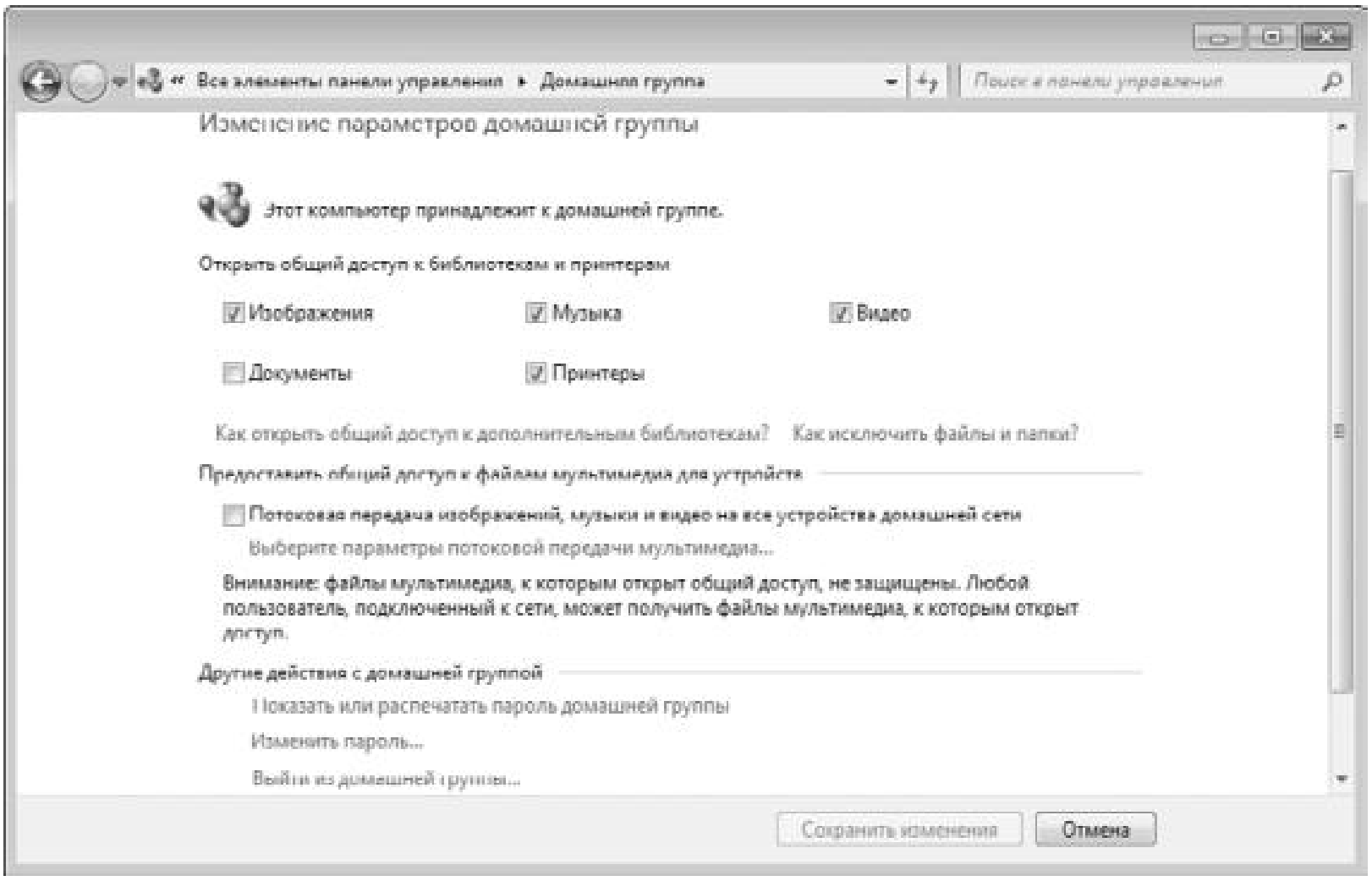


Инструкция откроется в отдельном окне, и чтобы ее распечатать, нажмите кнопку Печать этой страницы.

После нажатия кнопки Готово (см. рис. 25.4) мастер еще раз отобразит окно, в котором вы сможете изменить доступ к ресурсам (рис. 25.6).

Здесь же находится несколько дополнительных параметров, с помощью которых, например, дополнительно можно открыть доступ к потоковой передаче видео, изменить пароль подключения к домашней группе, настроить параметры доступа и др.

После этих действий домашняя группа будет создана, и любой, кто будет иметь пароль, сможет подключиться к ней и использовать ее ресурсы.



Подключение к домашней группе

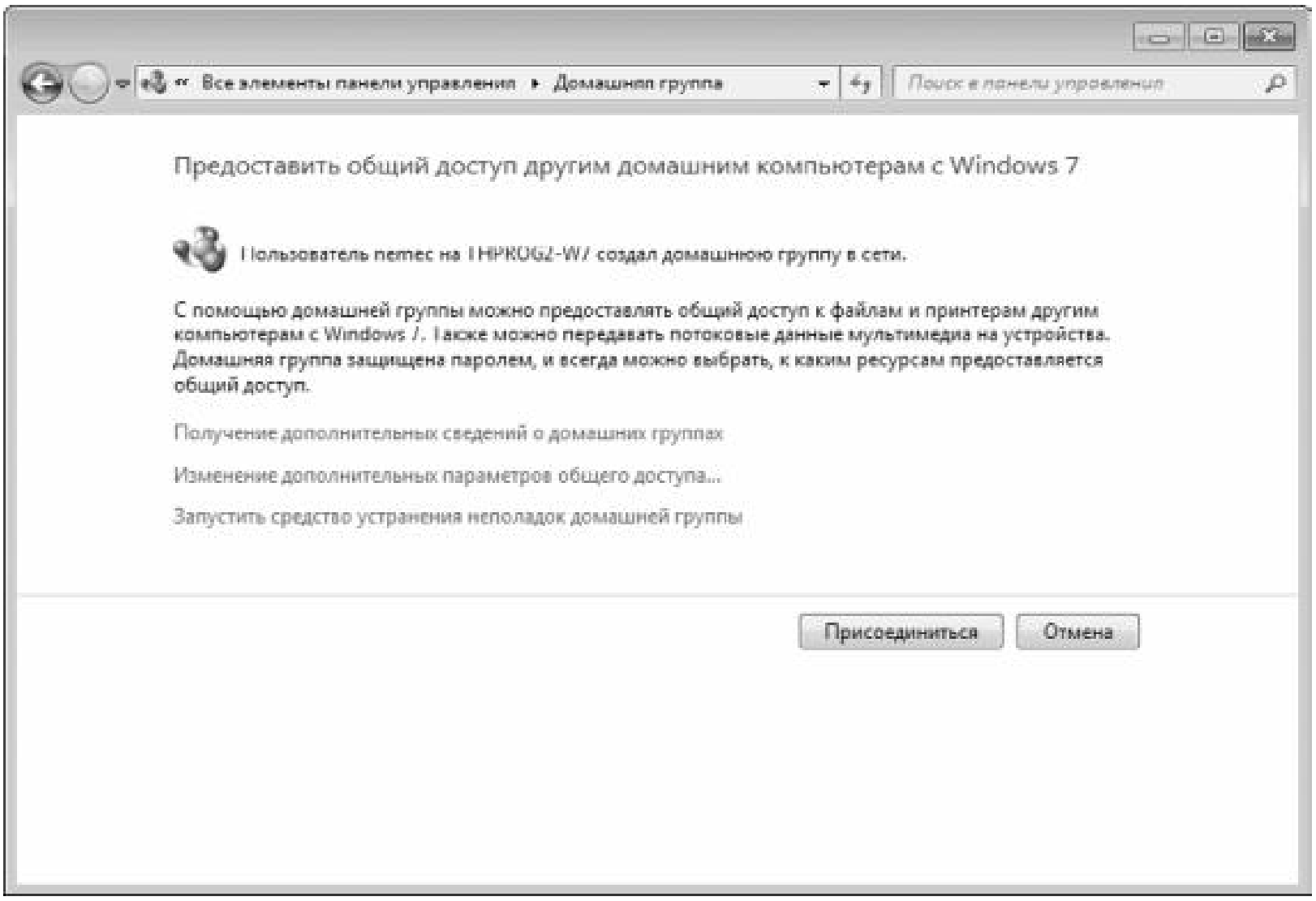
Подключение к домашней группе, как и ее создание, происходит быстро и просто, за что можно поблагодарить разработчиков Windows 7. Все, что вам потребуется, – разрешение на подключение, то есть пароль домашней группы. Однако обо всем по порядку.

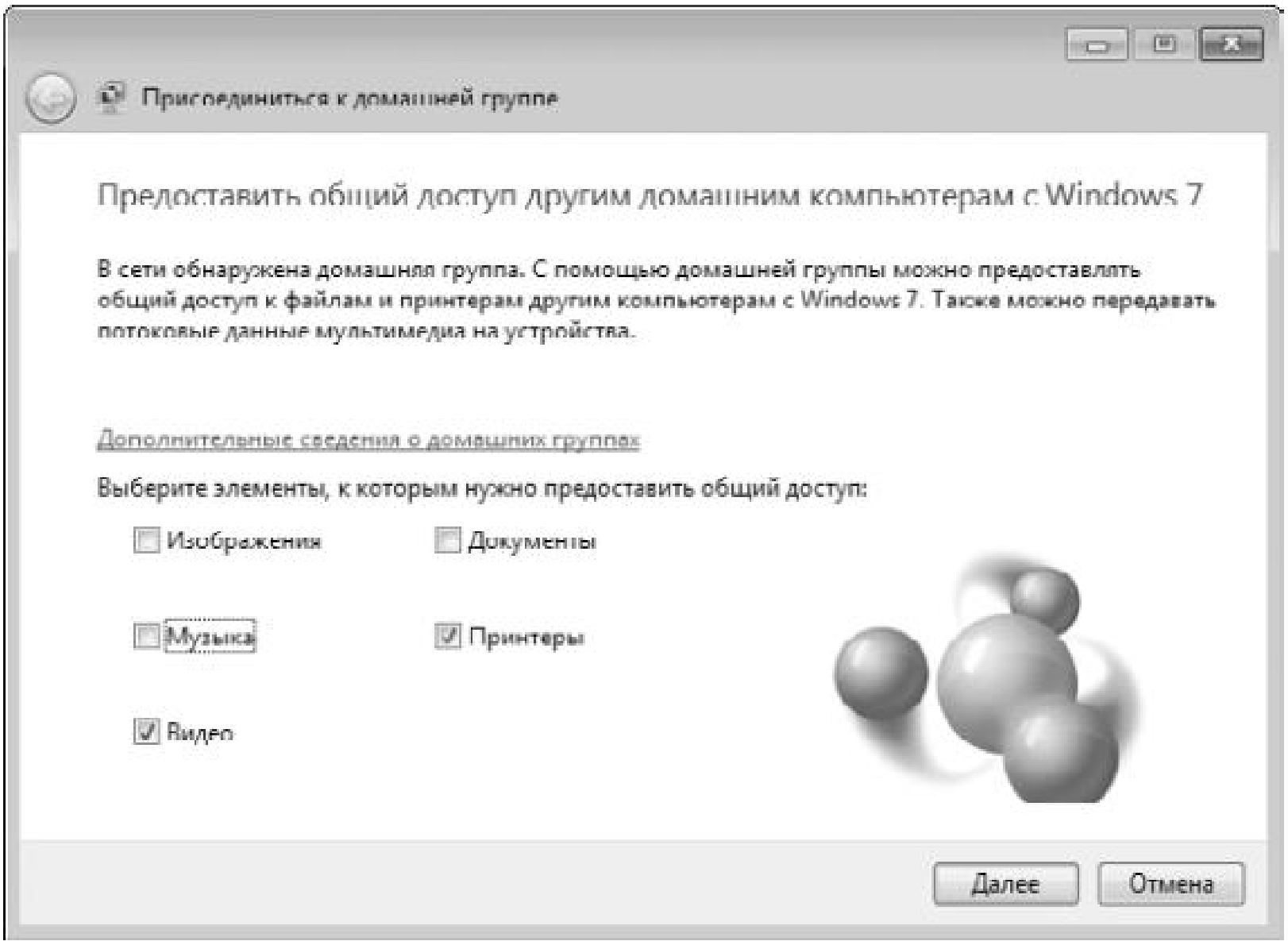
Для подключения к домашней группе будем использовать механизм Домашняя группа, который можно запустить с Панели управления.

После запуска этого механизма мастер подключений произведет поиск домашних групп, и, если таковые существуют, вы узнаете об этом из соответствующего сообщения в окне. В нашем случае мастер обнаружил только одну домашнюю группу, которую создал пользователь nemec на компьютере THPROG2-W7 (рис. 25.7).

Чтобы подключиться к этой группе, нажмите кнопку Присоединиться.

В следующем окне мастер предложит установить флажки рядом с теми из стандартных библиотек, которые вы хотите предоставить в общее использование (рис. 25.8).


Все элементы панели управления ▸ Домашняя группа
Поиск в панели управления
Предоставить общий доступ другим домашним компьютерам с Windows 7
Пользователь nemec на IHPROG2-W7 создал домашнюю группу в сети.
С помощью домашней группы можно предоставлять общий доступ к файлам и принтерам другим компьютерам с Windows 7. Также можно передавать потоковые данные мультимедиа на устройства. Домашняя группа защищена паролем, и всегда можно выбрать, к каким ресурсам предоставляется общий доступ.
Получение дополнительных сведений о домашних группах
Изменение дополнительных параметров общего доступа...
Запустить средство устранения неполадок домашней группы
Присоединиться
Отмена



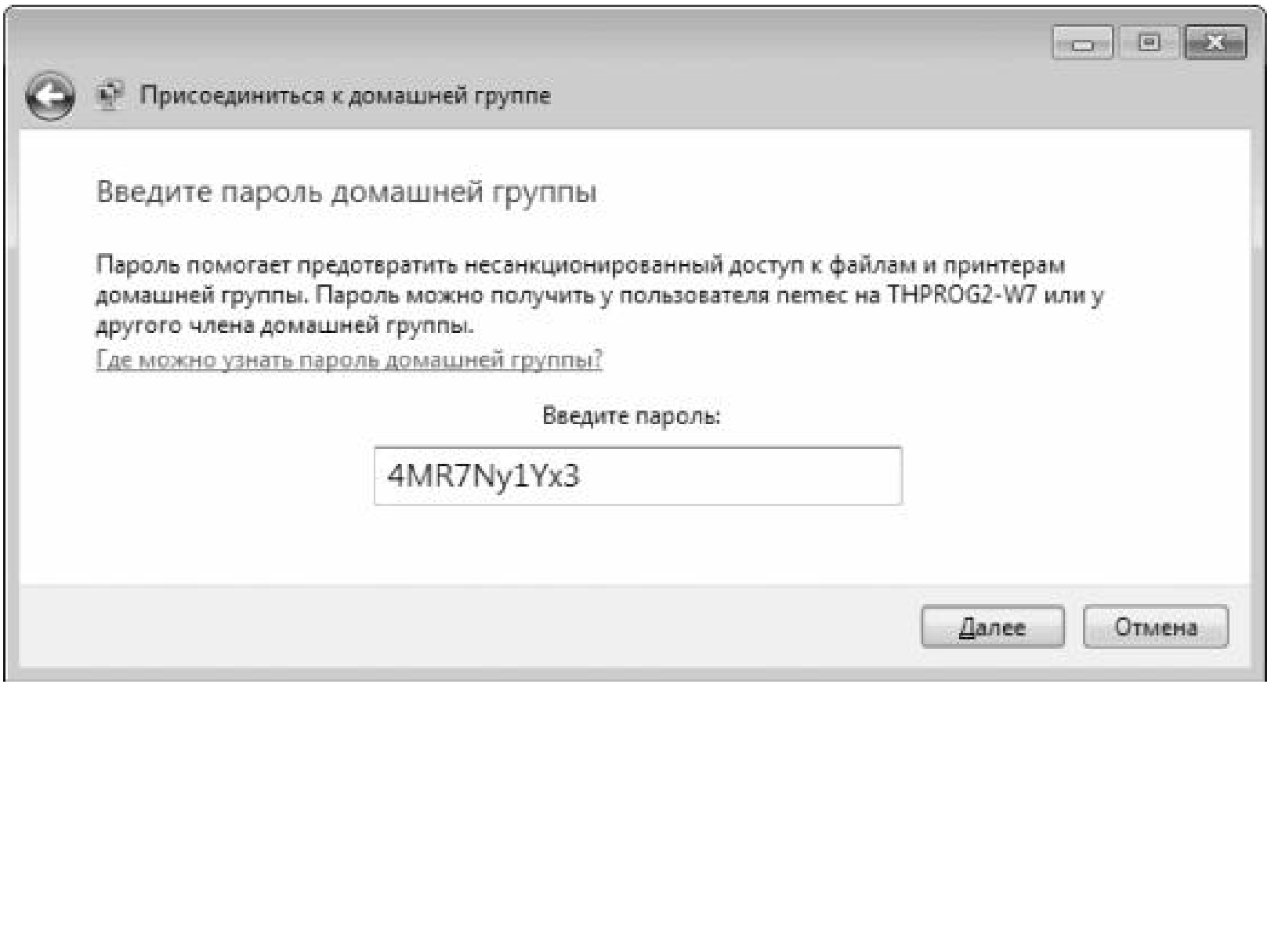
В дальнейшем можно будет создать и другие общие ресурсы, но на данном этапе это сделать невозможно. Отметив нужные библиотеки, нажмите кнопку Далее.

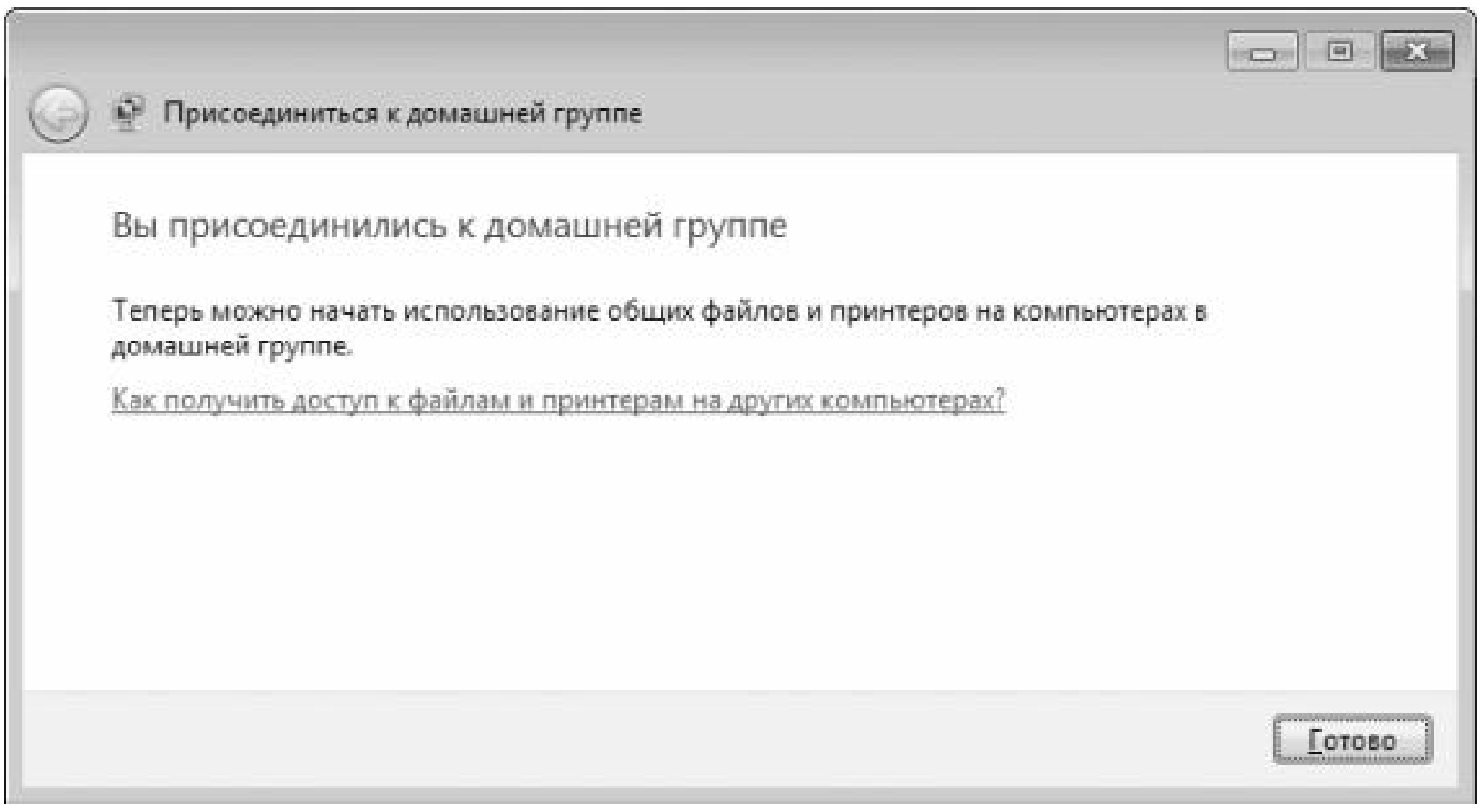
В следующем окне вам необходимо будет указать пароль подключения к домашней группе (рис. 25.9).

При вводе пароля обязательно учитывайте регистр символов! После ввода нажмите кнопку Далее, чтобы мастер мог подключиться к группе.

Если пароль указан верно, вы увидите сообщение о том, что подключение к домашней группе выполнено (рис. 25.10).

После этого вы сможете видеть участников этой домашней группы и общие ресурсы компьютеров в Проводнике в секции Домашняя группа.


Присоединиться к домашней группе
Введите пароль домашней группы
Пароль помогает предотвратить несанкционированный доступ к файлам и принтерам домашней группы. Пароль можно получить у пользователя nemec на THPROG2-W7 или у другого члена домашней группы.
Где можно узнать пароль домашней группы?
Введите пароль:
4MR7Ny1Yx3
Далее
Отмена


Присоединиться к домашней группе
Вы присоединились к домашней группе
Теперь можно начать использование общих файлов и принтеров на компьютерах в домашней группе.
Как получить доступ к файлам и принтерам на других компьютерах?
Готово

Глава 26
Работа в составе домена

Использование домена характерно для достаточно больших локальных сетей, хотя это, конечно, не обязательно. Так, к примеру, если владелец небольшого офиса может позволить себе приобрести сервер и серверную операционную систему, то ничто не мешает создать доменную структуру даже из нескольких компьютеров.

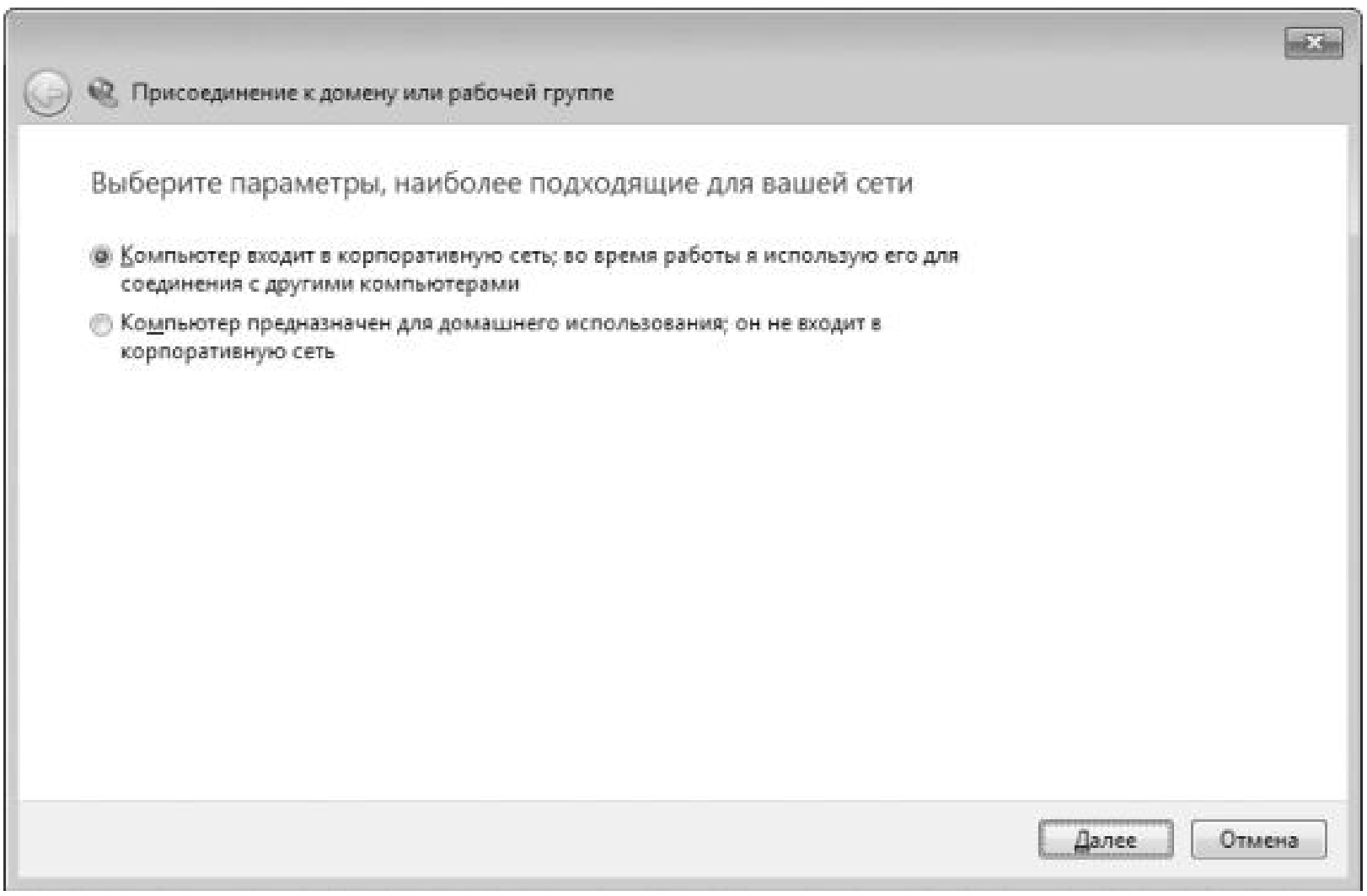
Как вы уже знаете, доменная структура, в отличие от рабочей группы, не только более сложная, но и более контролируемая. Поэтому, когда речь идет о подключении компьютера к домену, нет ничего удивительного в том, что необходимо обладать определенными правами доступа, а точнее, правами на подключение компьютера к домену. Также необходимо заранее побеспокоиться о том, чтобы создать учетную запись сетевого пользователя, который будет работать на этом компьютере.

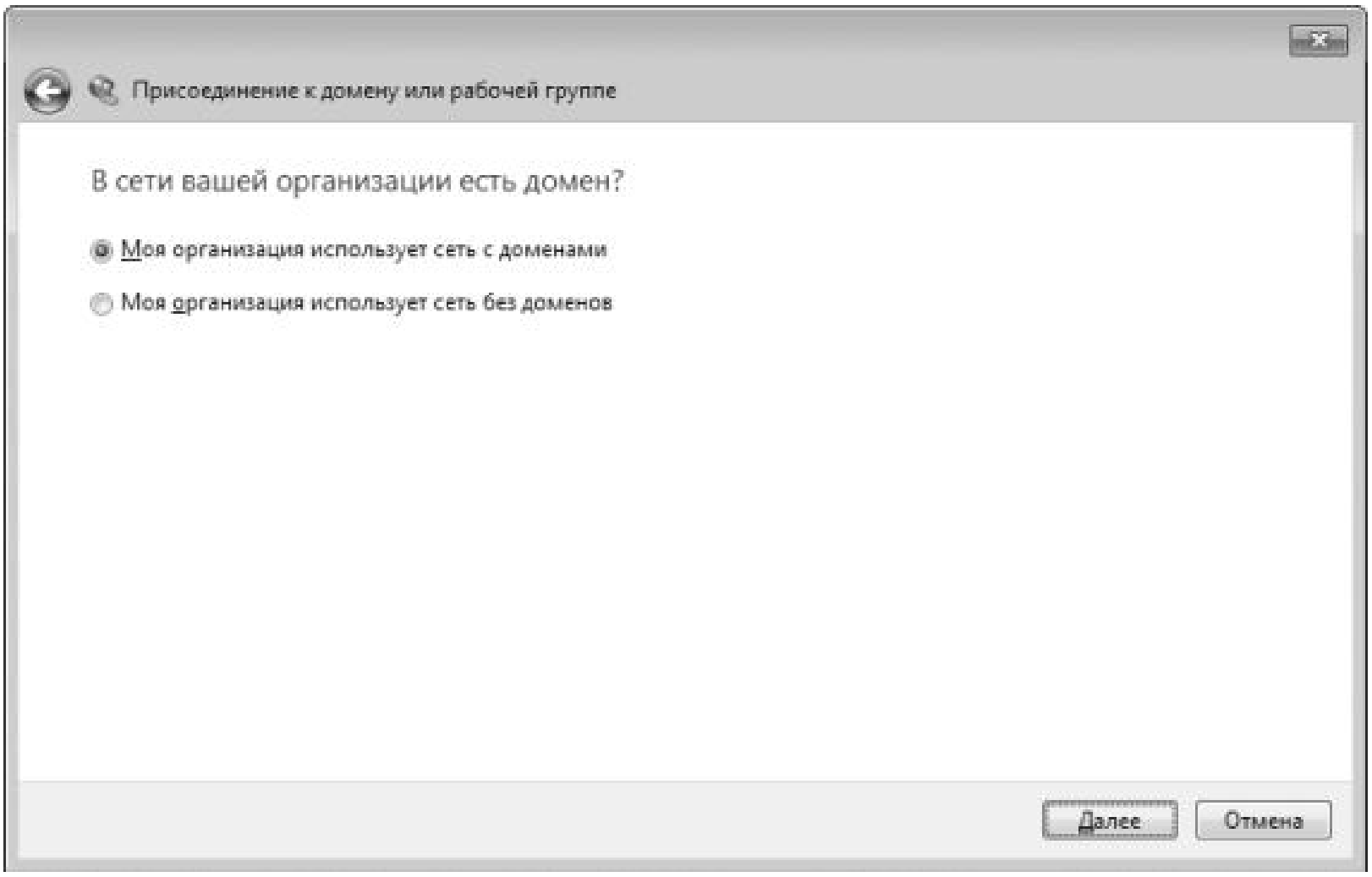
Для подключения к домену используется механизм Система, который можно запустить с Панели управления (см. рис. 24.1). В нем находится ссылка Изменить параметры, переход по которой приведет к открытию окна Свойства системы (см. рис. 24.2).

Процесс подключения к домену, а также добавления сетевого пользователя контролирует мастер подключений, работа которого и начинается после нажатия кнопки Идентификация (рис. 26.1).

Первое, что предстоит сделать, – выбрать направление работы мастера. Мастер универсален: он позволяет подключать компьютер не только к домену, но и к рабочей группе, поэтому чтобы направить его усилия в нужное русло, требуется указать соответствующий вариант. Выбор очевиден, поэтому, установив переключатель в положение с упоминанием корпоративной сети, продолжаем работу мастера.

В следующем окне (рис. 26.2) вам предстоит ответить на вполне очевидный вопрос, от которого зависят дальнейшие действия мастера.

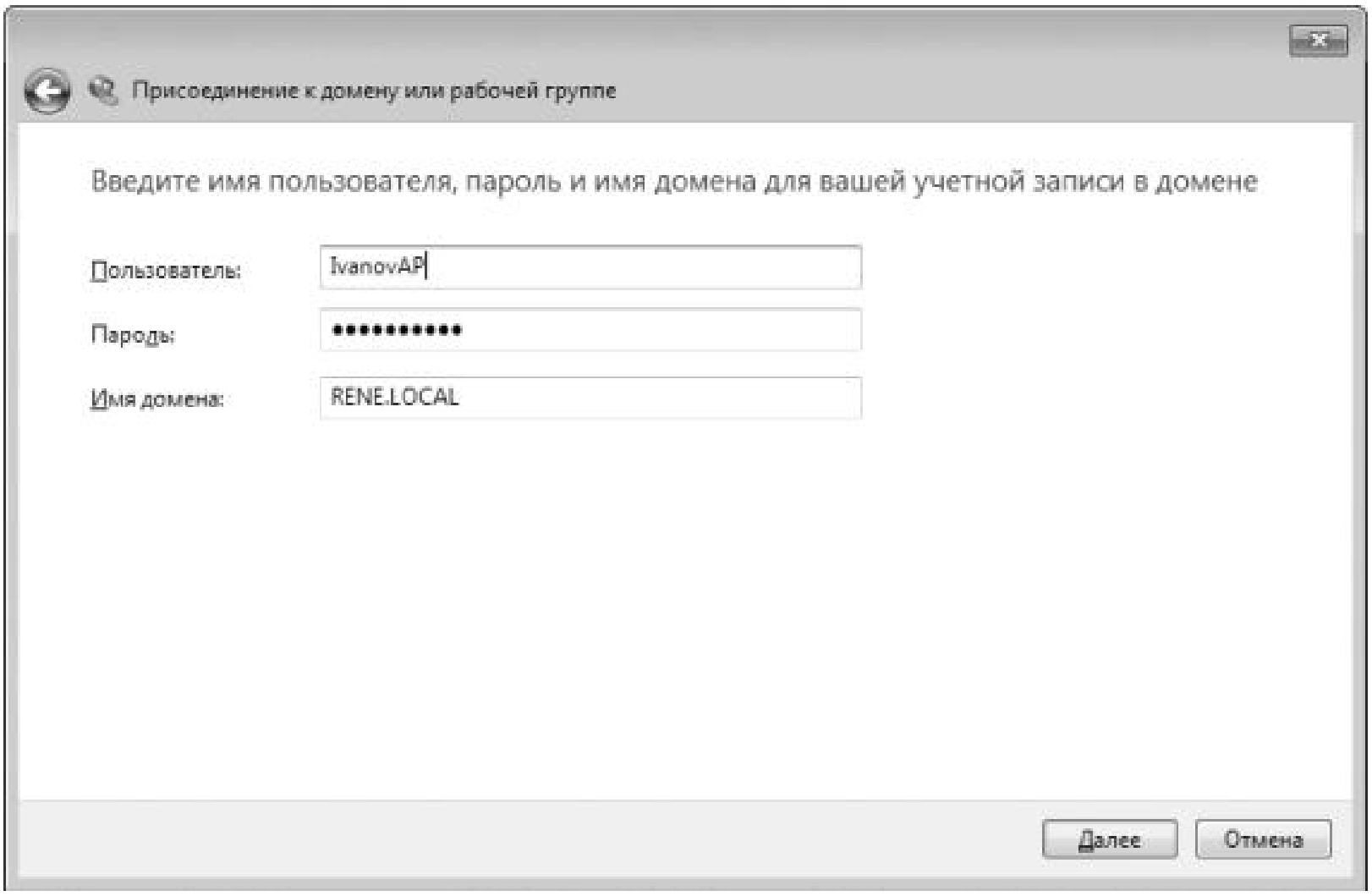




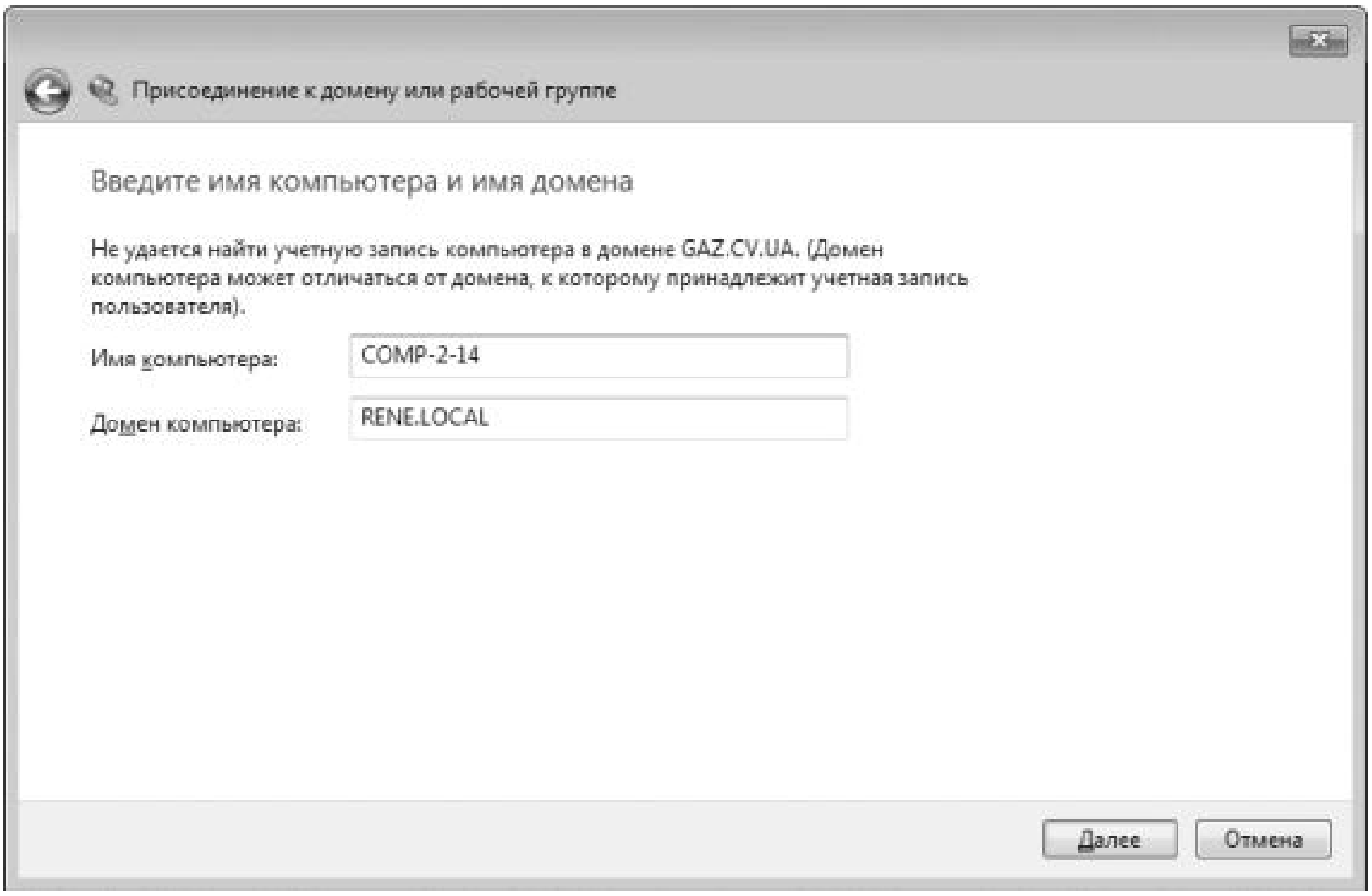
Поскольку наша задача – подключение к домену, выберите соответствующее положение переключателя, в результате чего процесс подключения продолжится.

Далее мастер вас предупредит, что для подключения к домену нужна определенная информация. В частности, сведения об учетных данных сетевого пользователя, который будет работать на данном компьютере, а также имя компьютера, под которым он будет идентифицирован в сети, если данные о нем не будут найдены в Active Directory. Подготовив эту информацию, продолжите процесс.

Когда появится следующее окно (рис. 26.3), вам потребуется ввести запрашиваемые данные, чтобы продолжить работу мастера. При этом помните, что учетная запись пользователя уже должна быть создана, о чем упоминалось выше, иначе подключение будет невозможно.



Если ранее с этого компьютера выполнялось подключение к домену, то информация об этом уже имеется на контроллере домена. Если это так, то в результате появится соответствующее сообщение с предложением использовать существующую учетную запись компьютера для его регистрации в домене. Если же подключение производится впервые, то вы увидите окно, показанное на рис. 26.4.



Здесь нужно указать имя компьютера и имя домена, чтобы можно было зарегистрировать компьютер в домене. После нажатия кнопки Далее потребуется пройти процесс авторизации, указав при этом учетные данные пользователя с правами присоединения к домену.

Если авторизация будет успешной, появится окно, сообщающее о том, что для завершения процесса подключения требуется перезагрузка компьютера. Если же авторизация будет неудачной, то есть имя пользователя и пароль были указаны неверно, потребуется повторно пройти авторизацию, указав правильные данные.

После перезагрузки компьютера вход в операционную систему необходимо будет производить уже с помощью нажатия комбинации клавиш Ctrl+Alt+Del, о чем сообщит соответствующая надпись на экране. Только после ввода данных учетной записи сетевого пользователя вы сможете полноценно войти в систему и использовать сетевые ресурсы.

Глава 27
Настройка TCP/IP-протокола

Настройка TCP/IP-протокола не зависит от того, каким образом компьютер подключен к сети и работает он в составе рабочей группы, домашней группы или домена. Настройка протокола нужна лишь для того, чтобы присвоить ему уникальный идентификатор, если без такового работа компьютера в сети или использование определенного ресурса невозможны.

Один из примеров необходимости такой настройки – организация общего доступа в

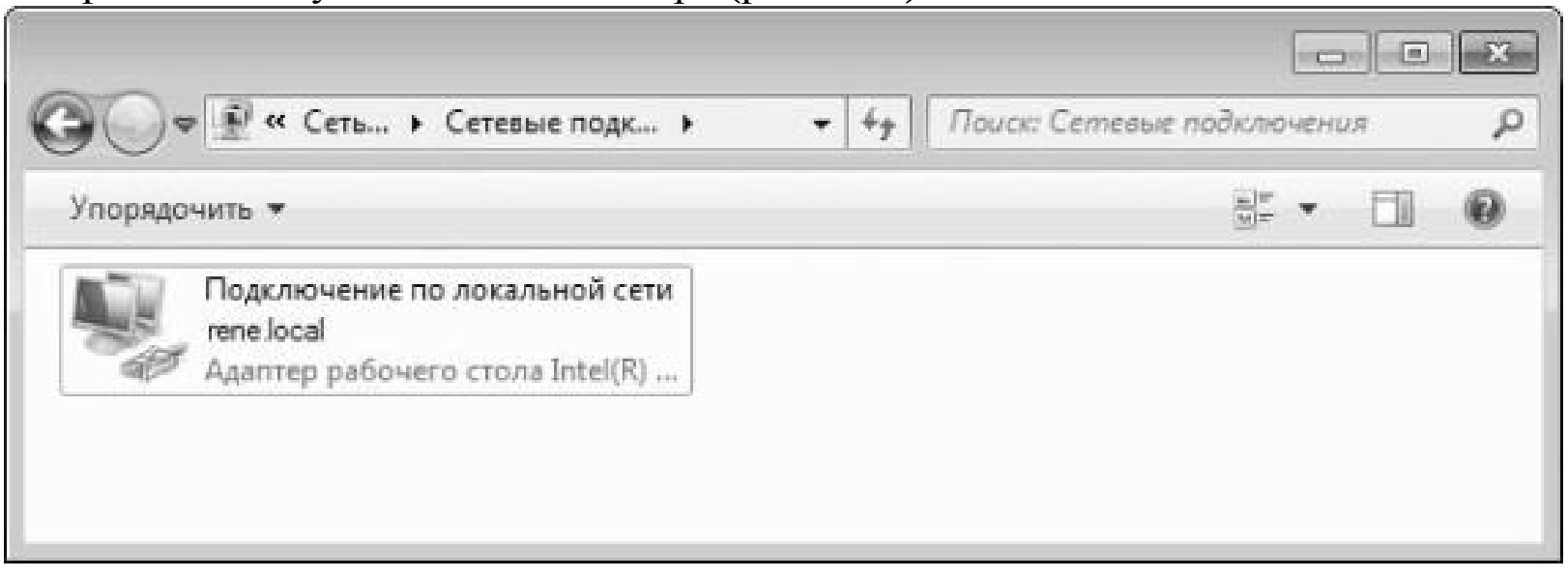
Интернет в одноранговой сети. В этом случае компьютер, не имеющий IP-адреса, не сможет использовать Интернет.

Примером для сети с доменом может быть наличие DNS-сервера или маршрутизатора, обслуживающего сетевой сегмент с другим принципом IP-адресации. В этом случае настройка TCP/IP-протокола требует указания IP-адреса данного маршрутизатора.

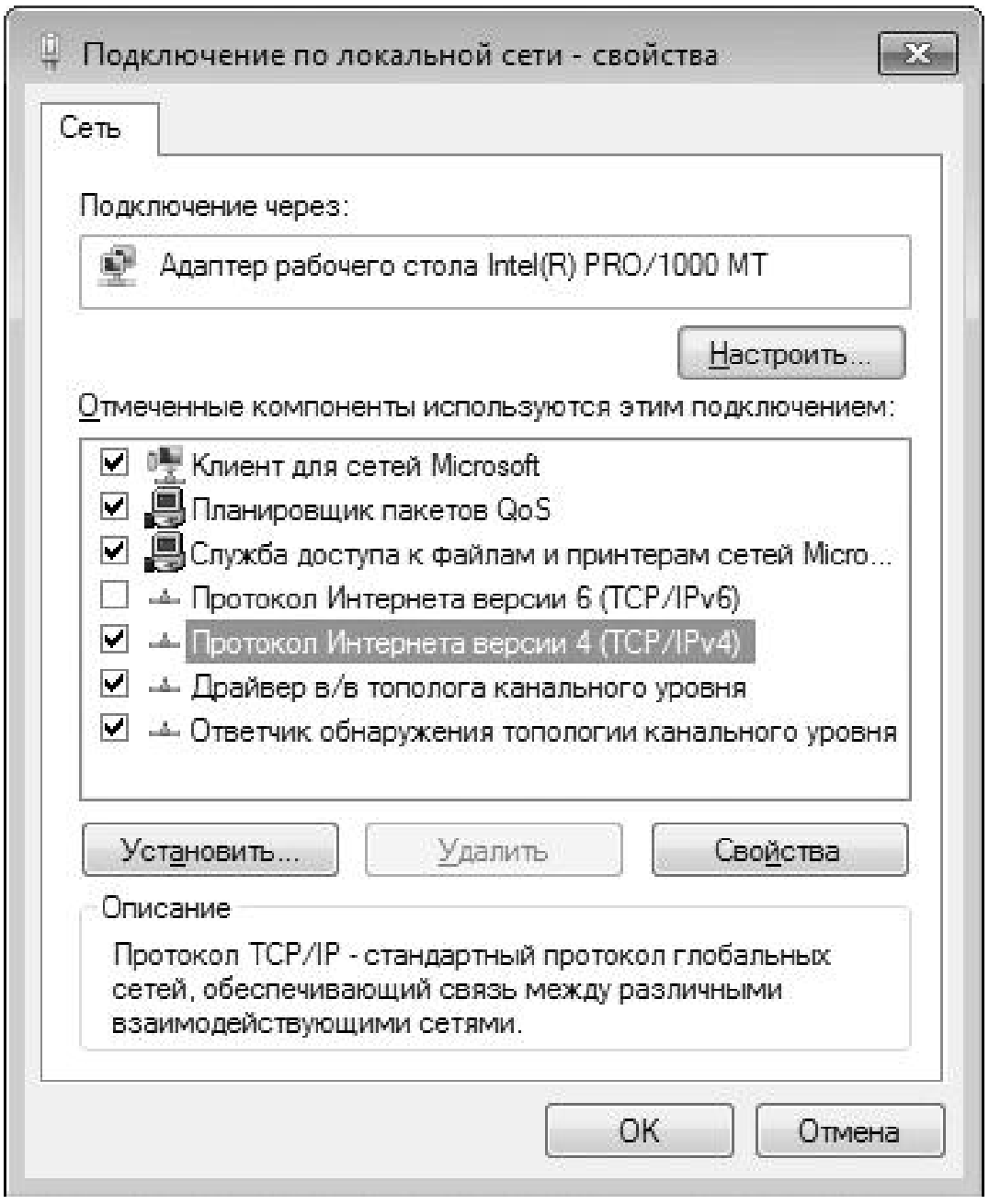
В большинстве случаев настройка TCP/IP-протокола сводится к настройке IP-адреса и маски подсети, что сделать очень просто. Кроме того, настройка протокола не требует перезагрузки компьютера и сразу дает результат, поэтому, даже если вы сделаете что-то неправильно, не стоит особо огорчаться: ситуацию всегда можно исправить.

Для выполнения необходимых изменений будем использовать Центр управления сетями и общим доступом, открыть который можно с Панели управления.

В правой части появившегося окна (см. рис. 24.1) находится несколько ссылок, позволяющих получить доступ к разным функциям. В частности, чтобы изменить настройки сетевого адаптера, необходимо использовать ссылку Изменение параметров адаптера. При ее нажатии откроется окно, содержащее список всех сетевых подключений, которые используются на компьютере (рис. 27.1).

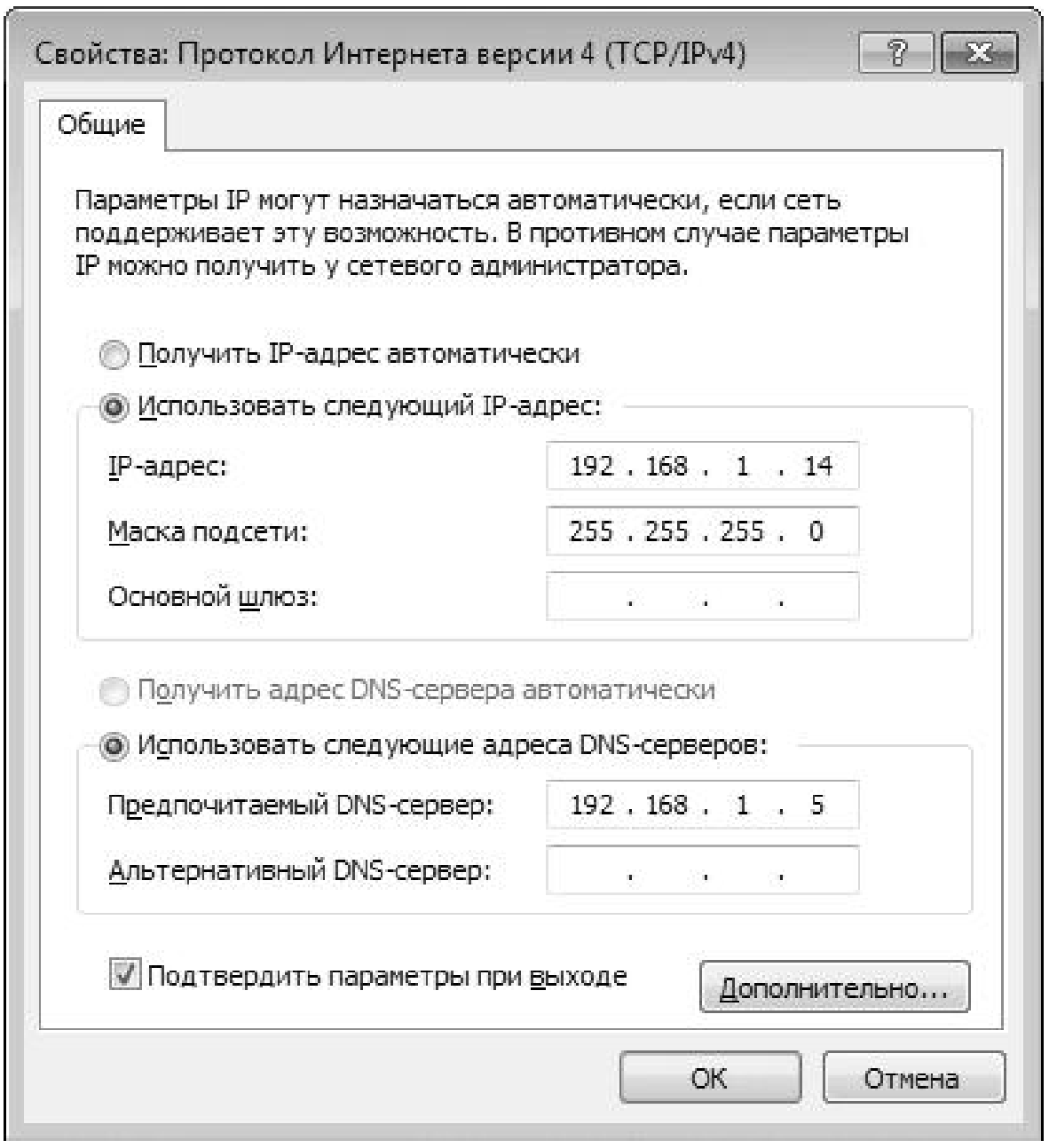


Их количество зависит от количества установленных сетевых адаптеров, а также программно эмулируемых адаптеров [7 - В качестве таковых могут выступать сетевые соединения для обслуживания Bluetooth-устройств, сетевых адаптеров виртуальных машин и т. п.]. Выбрав нужное сетевое подключение из списка, щелкните на нем правой кнопкой мыши и в появившемся контекстном меню выберите строку Свойства. В результате откроется окно свойств данного сетевого подключения (рис. 27.2).



Из всего списка служб и протоколов, которые обслуживают данное сетевое подключение, нас интересует строка Протокол Интернета версии 4 (TCP/IPv4). Дважды щелкните на ней. Появится окно настройки TCP/IP-протокола (рис. 27.3).

В этом окне вы должны будете ввести нужную информацию.



Глава 28
Создание и настройка общих ресурсов

Информация – главное достоинство как локальной, так и глобальной сети. Общая документация, базы данных, системы учета и, в конце концов, Интернет – вот ради чего стоит создавать локальные сети.

Операционная система Windows 7 является наиболее современной, и ее распространение принимает массовый характер. Поэтому очень важно знать, как правильно создать общий ресурс и настроить доступ к нему.

Далее мы приведем примеры создания и настройки общих ресурсов для случаев работы в составе домашней группы, рабочей группы и домена.

Домашняя группа

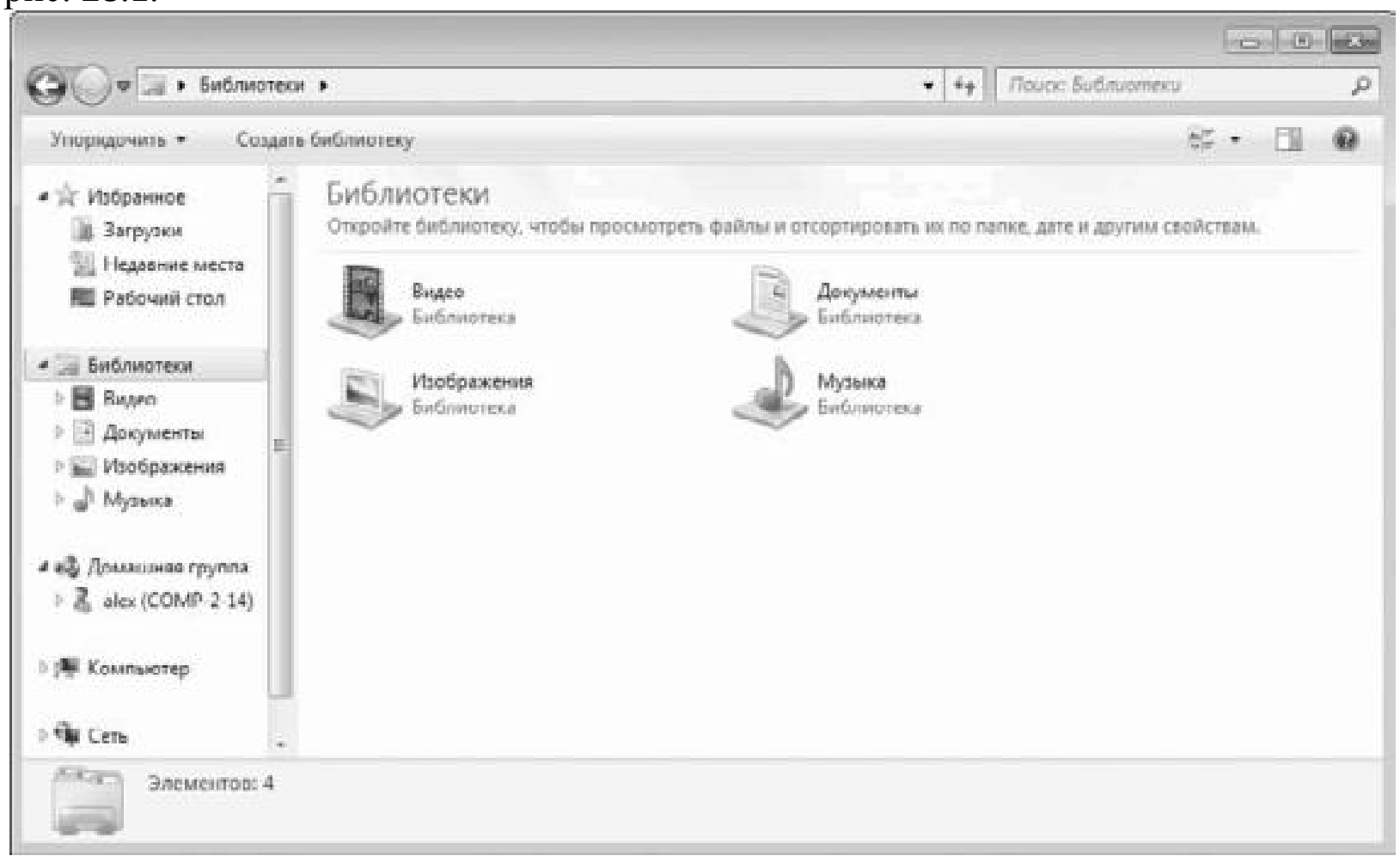
Создание и настройка общих ресурсов в том случае, когда компьютер входит в домашнюю группу, кардинально отличается от аналогичных действий в составе рабочей

группы или домена, поэтому данный вариант мы рассмотрим первым.

Уже упоминалось, что домашняя группа использует в своей работе библиотеки, которые представляют собой ссылки на различные ресурсы. Вы можете использовать стандартные библиотеки или создать дополнительные: они, как правило, больше подходят для организации общих ресурсов. Объяснение этому достаточно простое. Например, если вы хотите показать сетевым участникам свои программы из папки с дистрибутивами, то логичнее будет создать библиотеку с названием, например, Ресурс, нежели добавлять ссылку на них в стандартной библиотеке Видео или Документы.

Создание библиотеки выполняется следующим образом.

Для начала откройте Проводник и выделите позицию Библиотеки, как это показано на рис. 28.1.



Теперь, чтобы создать новую библиотеку, используйте ссылку Создать библиотеку на панели управления окном (рис. 28.2).

После этого укажите название библиотеки, например Ресурс, и нажмите клавишу Enter. Созданная таким образом библиотека пока не представляет никакой ценности, поскольку она не заполнена ссылками на сами ресурсы, поэтому будем исправлять эту ситуацию.

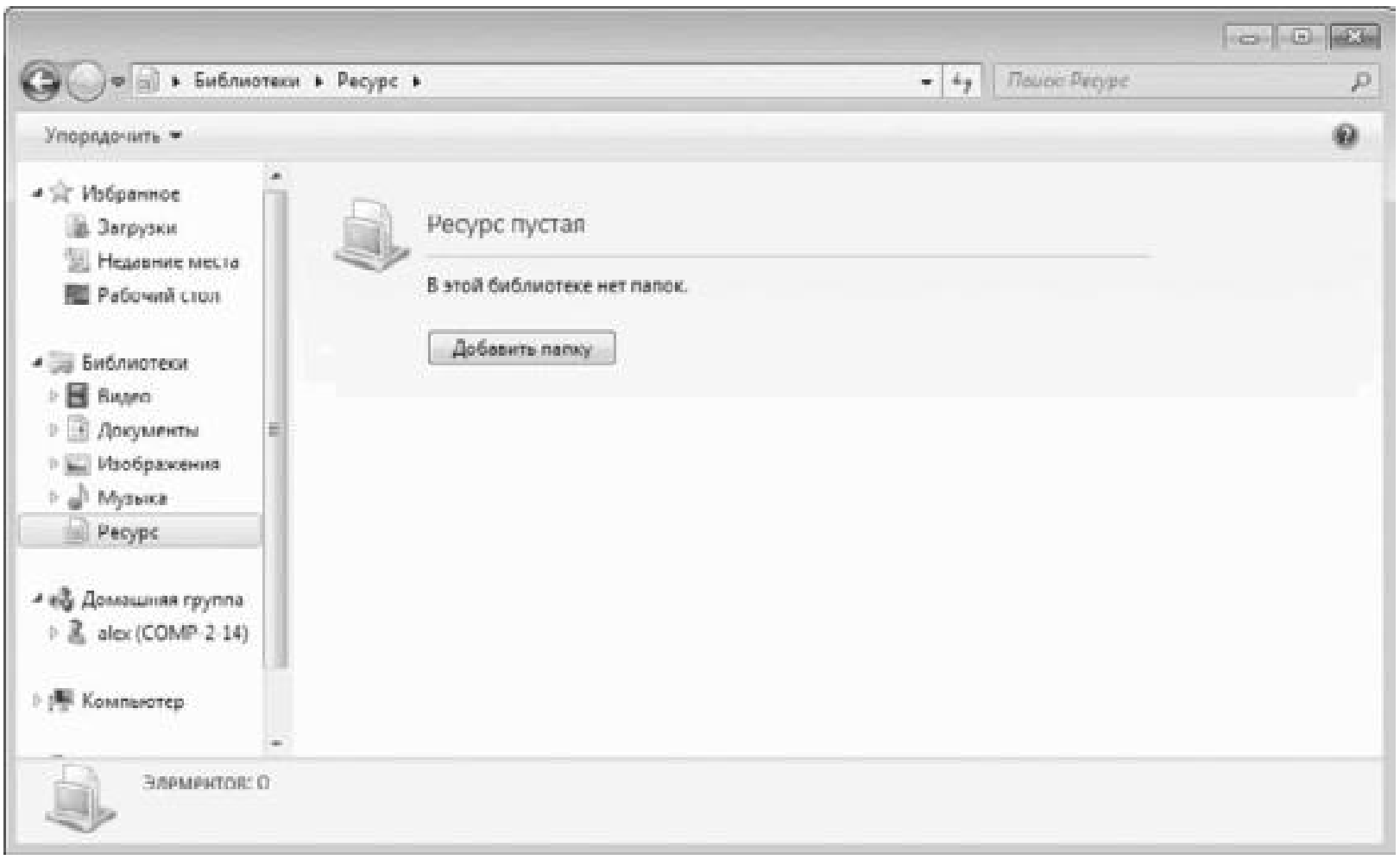
Добавлять ресурсы в библиотеку можно двумя способами. К примеру, можно найти и выделить в Проводнике нужную папку, а затем выбрать на панели управления окном пункт Добавить в библиотеку с последующим выбором названия библиотеки. Либо можно сначала открыть саму библиотеку и уже из нее добавлять нужные папки. В качестве примера рассмотрим второй способ.

Первым делом выделите позицию с названием библиотеки, как это показано на рис. 28.3.

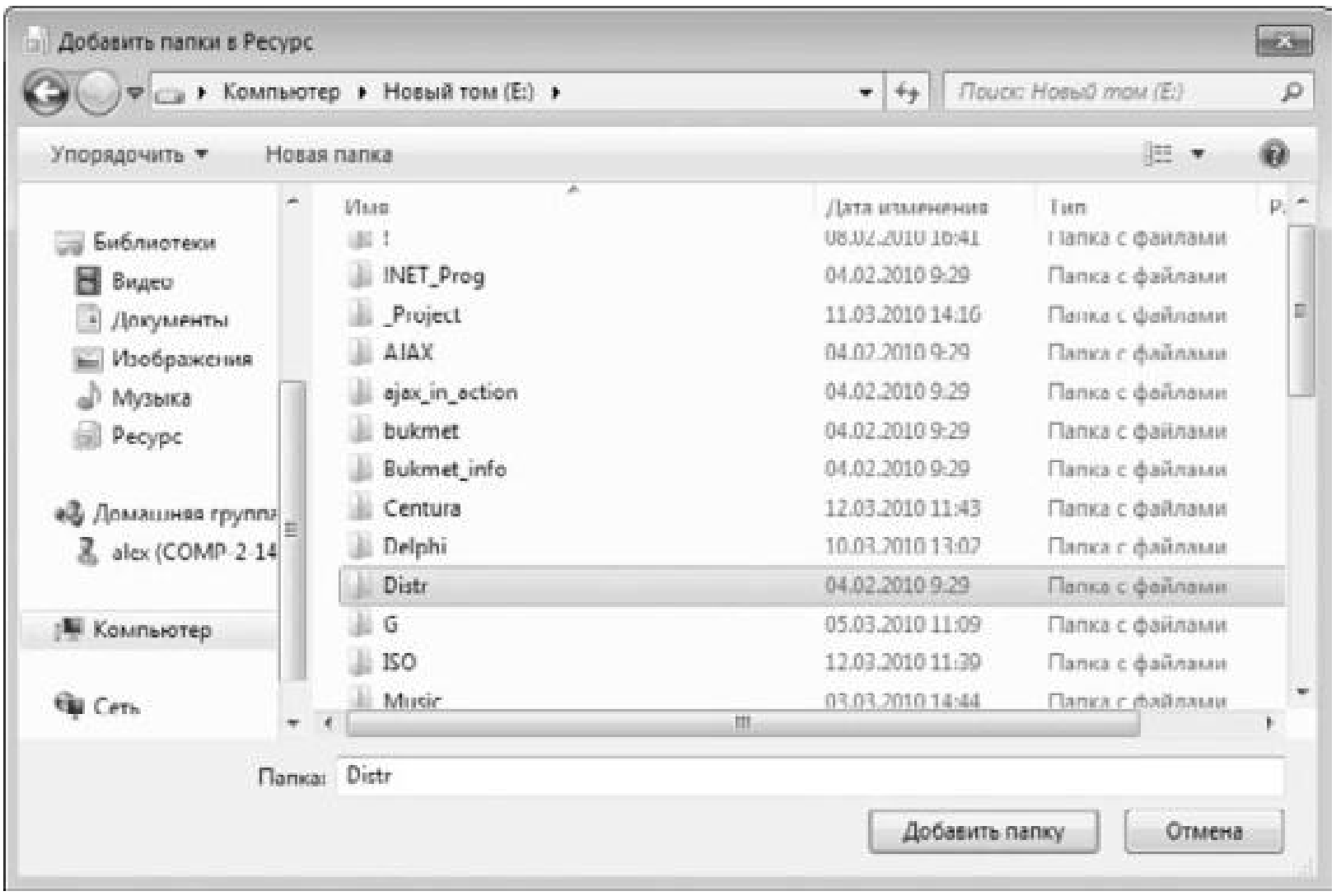
То, что библиотека пустая, лишний раз подтверждает соответствующая надпись в окне.

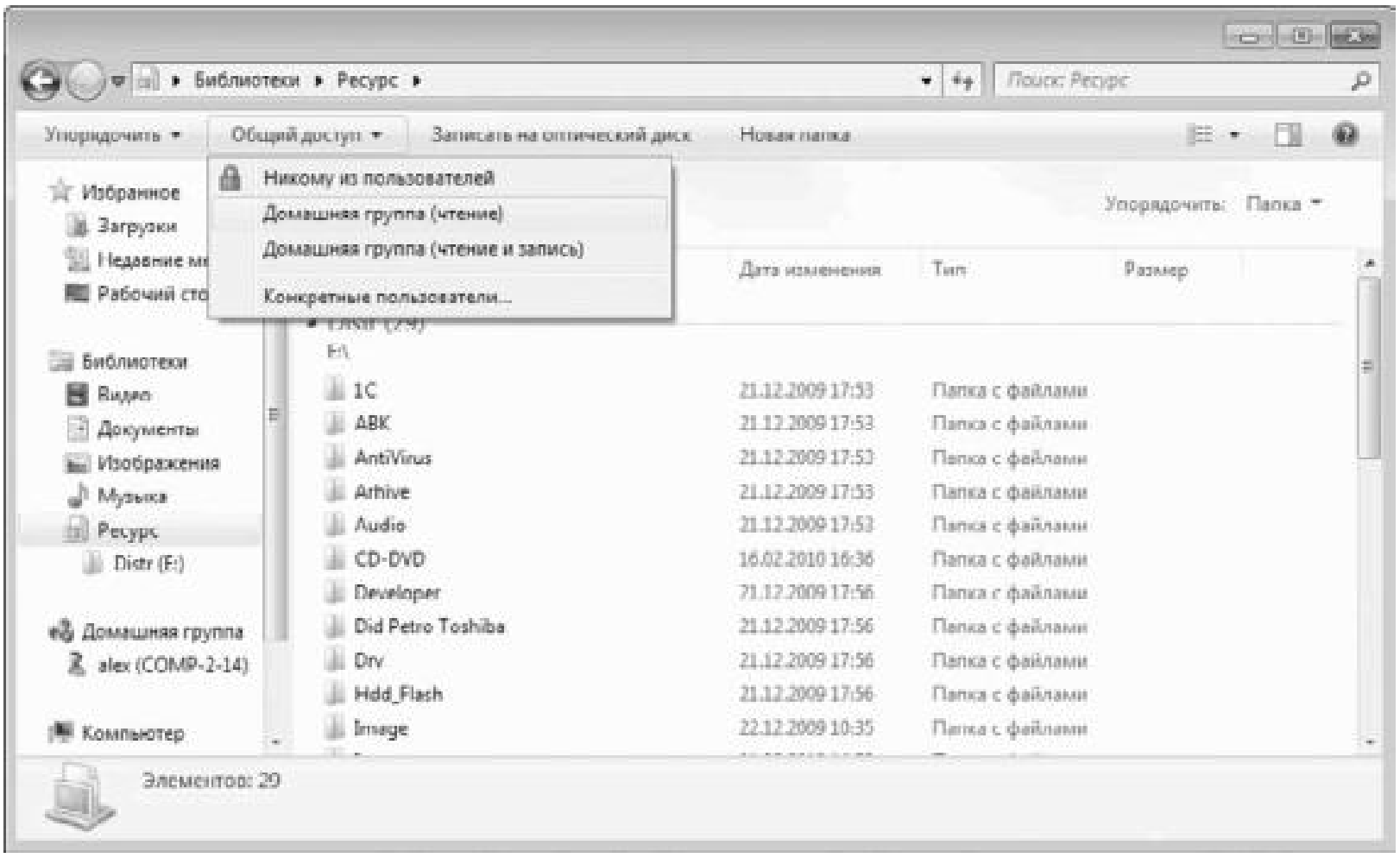
Здесь же присутствует кнопка Добавить папку, которую и необходимо нажать (рис. 28.4).

Это откроет стандартное окно, в котором нужно указать папку и нажать кнопку Добавить папку. После этого выбранная папка будет добавлена в библиотеку.



-

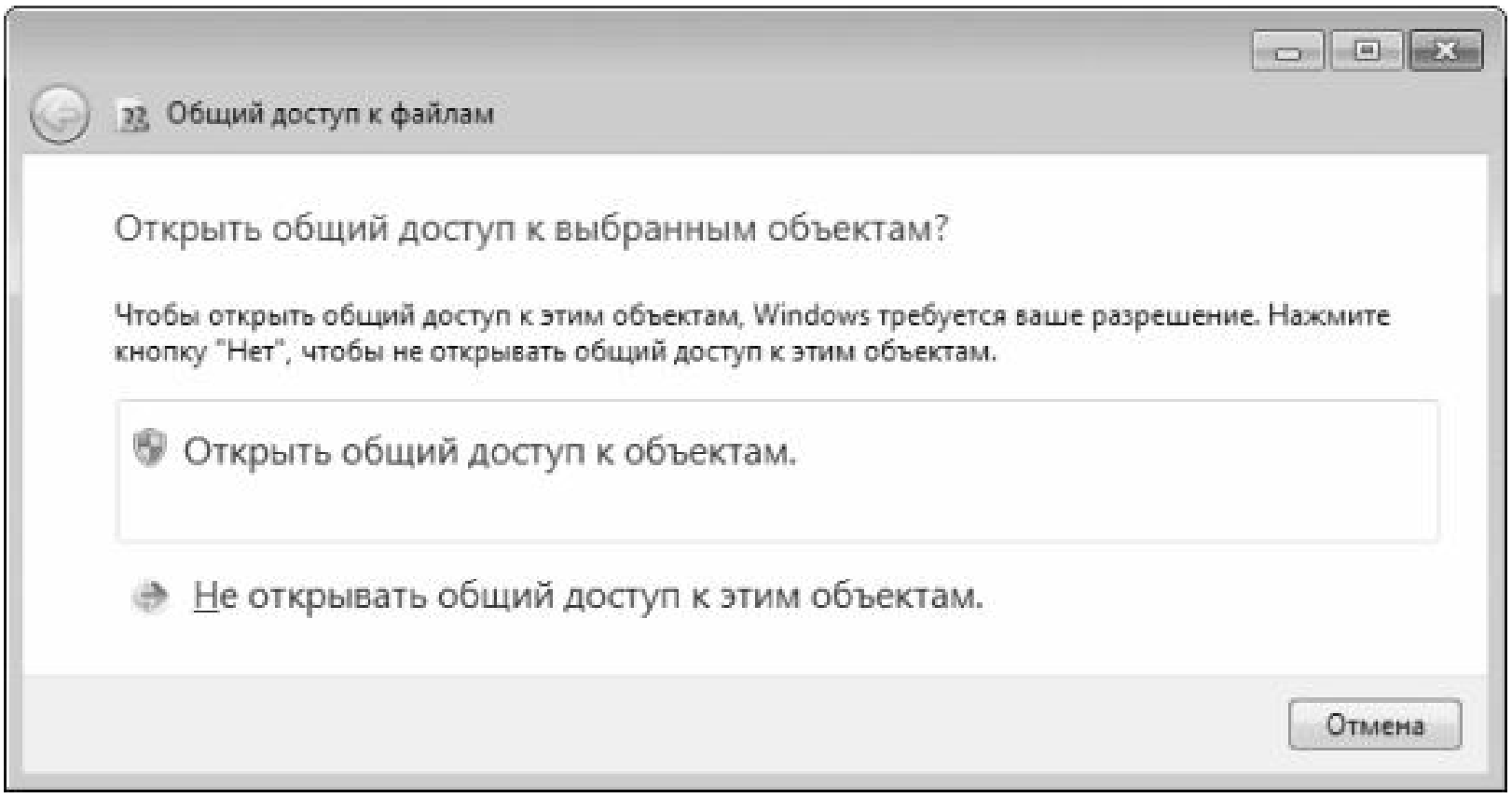

Добавить папки в Ресурс
Компьютер ▸ Новый том (E:) ▸
Поиск: Новый том (E:)
Упорядочить
Новая папка
Библиотеки
Видео
Документы
Изображения
Музыка
Ресурс
Домашняя группа
alex (COMP-2-14
Компьютер
Сеть
Имя
Дата изменения
Тип
!
INET_Prog
_Project
AJAX
ajax_in_action
bukmet
Bukmet_info
Centura
Delphi
Distr
G
ISO
Music
04.02.2010 9:29
Папка с файлами
11.03.2010 14:16
12.03.2010 11:43
10.03.2010 13:07
05.03.2010 11:09
12.03.2010 11:39
03.03.2010 14:44
Папка:
Distr
Добавить папку
Отмена



И наконец, когда в библиотеке уже находятся необходимые ресурсы, следует настроить права доступа к этой библиотеке (рис. 28.5).

Для этого выделите позицию с названием библиотеки и выберите на панели управления окном пункт Общий доступ. Это приведет к открытию небольшого списка, из которого нужно выбрать тип доступа, например Домашняя группа (чтение).

Также в этом списке присутствуют пункты Никому из пользователей (отключает доступ к ресурсу), Домашняя группа (чтение и запись) (разрешает чтение и изменение ресурса) и Конкретные пользователи (позволяет выбирать пользователей, которым будет предоставлен доступ). Тип доступа к ресурсу вы должны определить сами исходя из того, можно этот ресурс изменять или нет. Выберем для примера пункт Домашняя группа (чтение) (рис. 28.6).



В результате появится окно, в котором вам нужно будет либо подтвердить свой выбор и открыть доступ к объектам, либо отказаться от этого действия. Если выбран первый вариант, ваш ресурс автоматически отобразится в домашней группе каждого сетевого участника и будет доступен для просмотра.

Рабочая группа

Для создания общих ресурсов при работе компьютера в составе рабочей группы используются давно отлаженные механизмы, которые были и в более старых операционных системах. Ниже приведен пример создания общего файлового ресурса и создания доступа к общему принтеру.

Создание файлового ресурса

Для создания общего файлового ресурса воспользуйтесь Проводником. Выбрав в нем папку, доступ к которой вы хотите открыть, щелкните на ней правой кнопкой мыши и в появившемся меню выберите Общий доступ ► Конкретные пользователи. Это приведет к открытию окна, показанного на рис. 28.7.

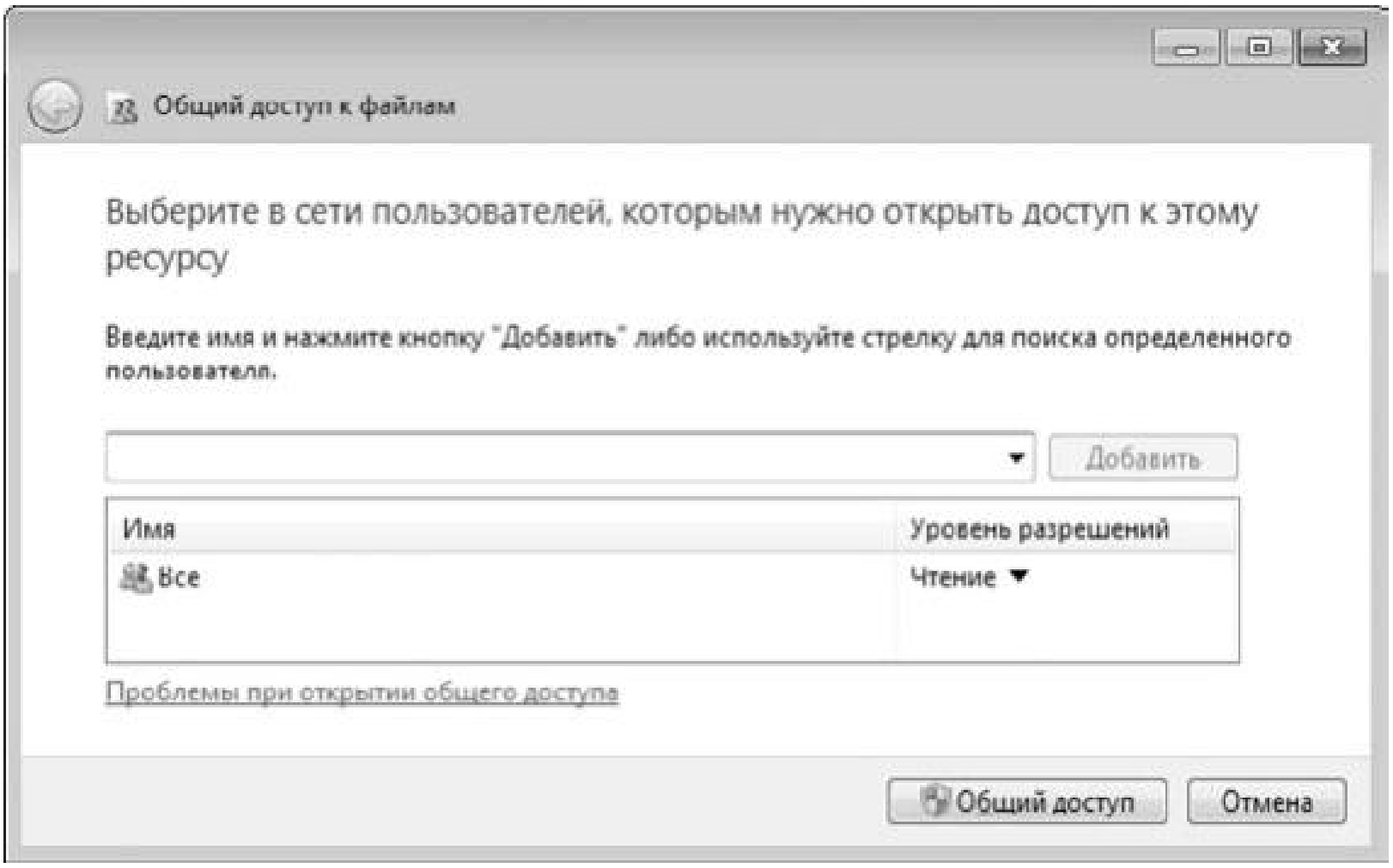
По умолчанию в этом окне присутствует только запись Все. Это означает, что любой пользователь рабочей группы может видеть и использовать ваш ресурс, но только в режиме просмотра. Если вас это устраивает, тогда, чтобы открыть доступ к ресурсу, нажмите кнопку Общий доступ и подтвердите свое решение. Если же вы хотите настроить

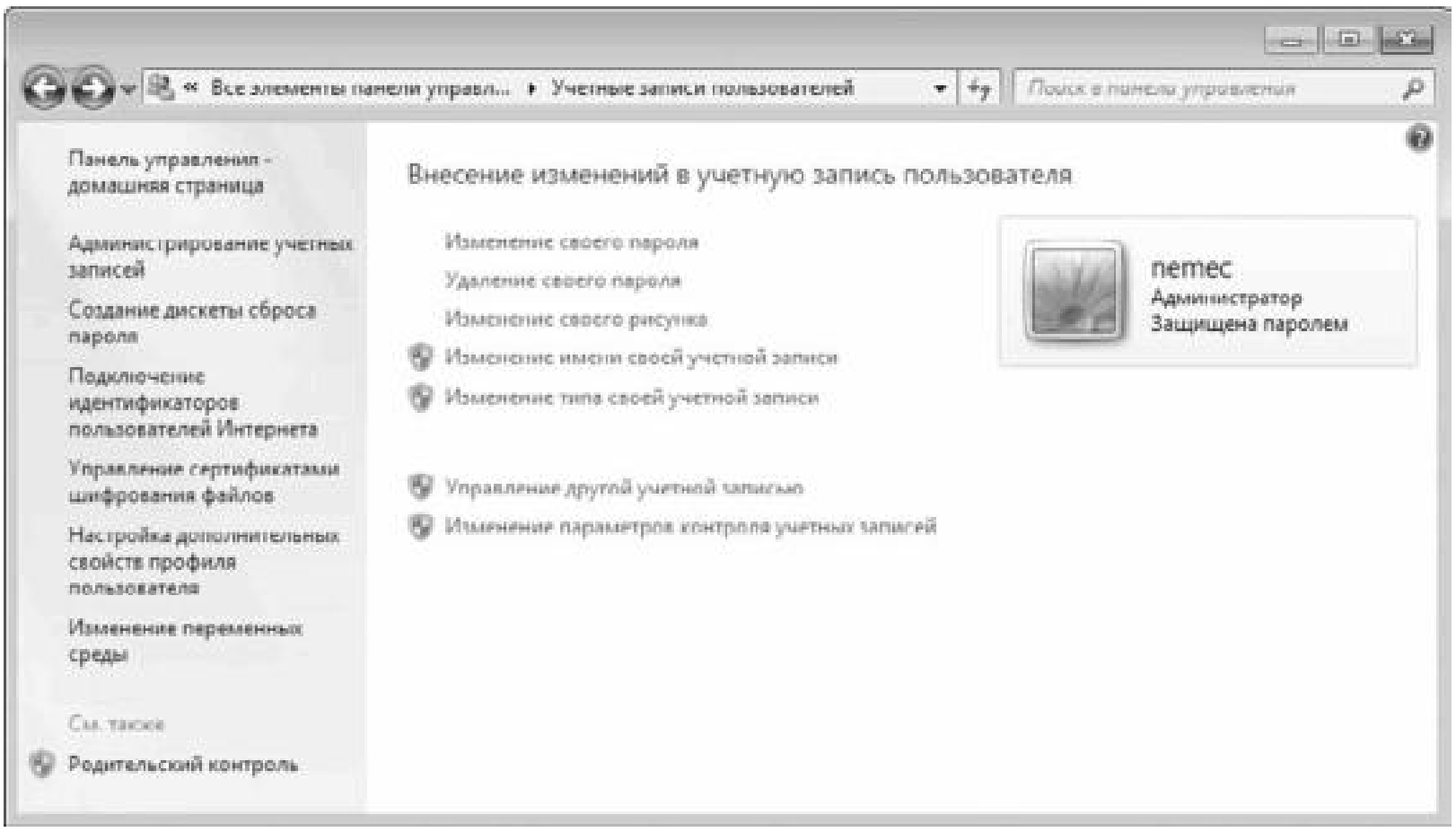
права более детально, придется дополнительно выполнить некоторые действия.

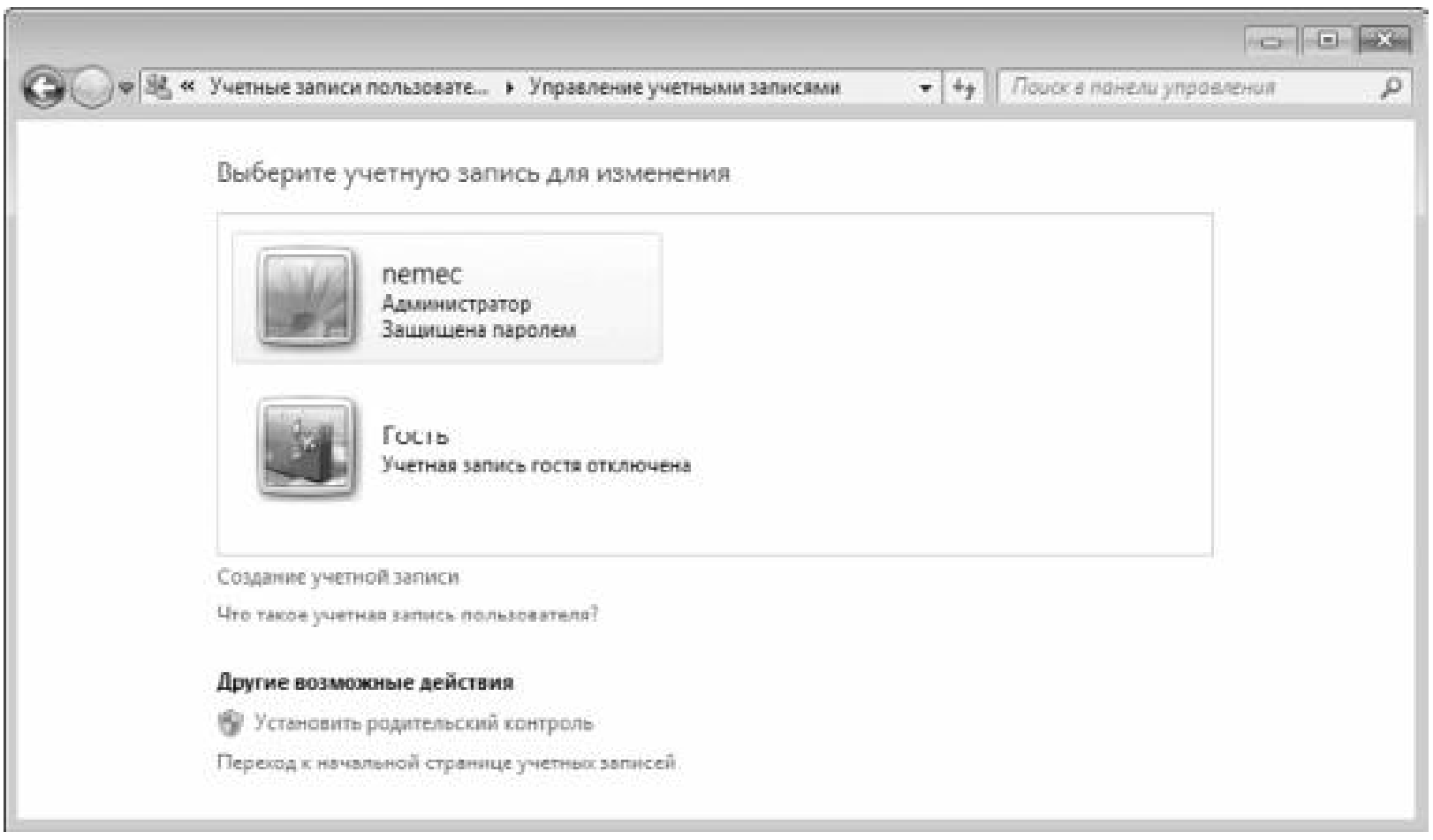
Если вы хотите предоставить доступ к ресурсу конкретным сетевым пользователям рабочей группы, необходимо, чтобы учетные записи этих пользователей были зарегистрированы на вашем компьютере. Кроме того, следует удалить из списка разрешенных учетных записей пункт с именем Все. Тогда при подключении пользователя к ресурсу он будет авторизован с помощью существующей учетной записи. В противном случае при подключении к ресурсу пользователь получит сообщение об ошибке.

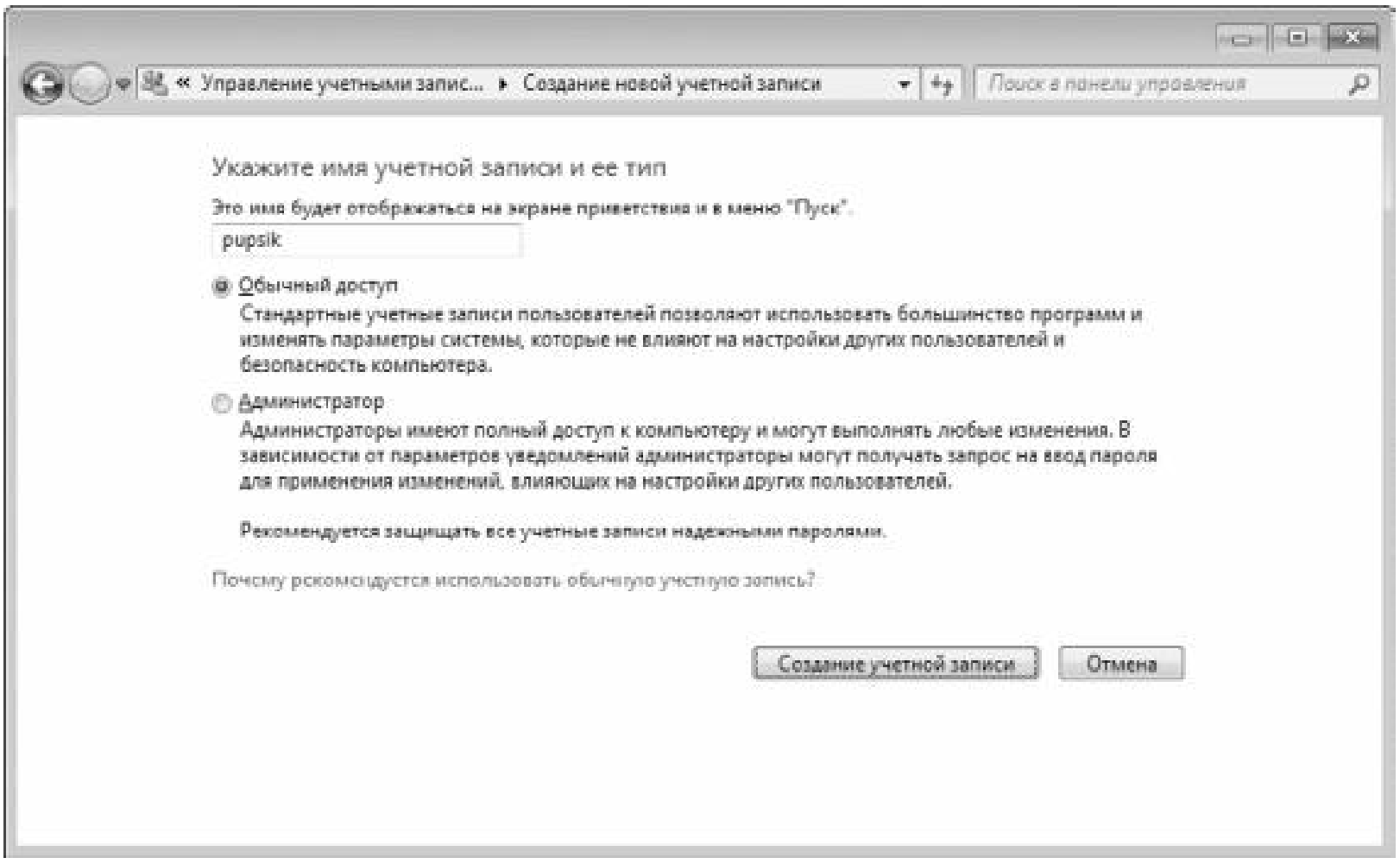
Для добавления новой учетной записи необходимо выполнить следующие действия. Откройте механизм Учетные записи пользователей, который можно запустить с Панели управления (рис. 28.8).

Далее перейдите по ссылке Управление другой учетной записью (рис. 28.9).




« Все элементы панели управл... ▸ Учетные записи пользователей
Поиск в панели управления
Панель управления - домашняя страница
Администрирование учетных записей
Создание дискеты сброса пароля
Подключение идентификаторов пользователей Интернета
Управление сертификатами шифрования файлов
Настройка дополнительных свойств профиля пользователя
Изменение переменных среды
См. также
Родительский контроль
Внесение изменений в учетную запись пользователя
Изменение своего пароля
Удаление своего пароля
Изменение своего рисунка
Изменение имени своей учетной записи
Изменение типа своей учетной записи
Управление другой учетной записью
Изменение параметров контроля учетных записей
nemec
Администратор
Защищена паролем

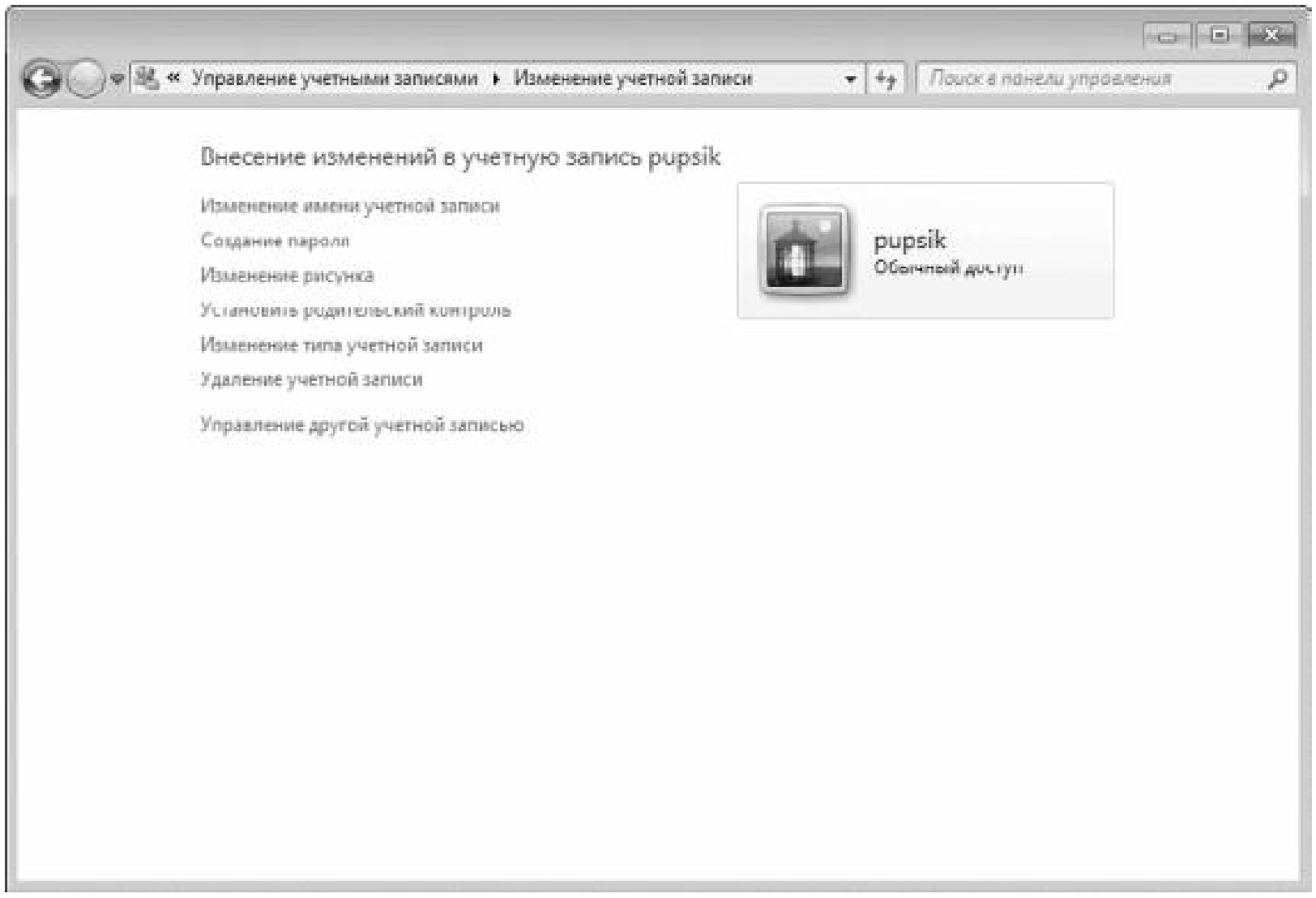

« Учетные записи пользовате... ▸ Управление учетными записями
Поиск в панели управления
Выберите учетную запись для изменения
nemec
Администратор
Защищена паролем
Гость
Учетная запись гостя отключена
Создание учетной записи
Что такое учетная запись пользователя?
Другие возможные действия
Установить родительский контроль
Переход к начальной странице учетных записей



Это приведет к открытию окна со списком зарегистрированных в системе учетных записей. Для создания новой учетной записи воспользуйтесь ссылкой Создание учетной записи (рис. 28.10).

После этого укажите имя учетной записи, тип доступа – Обычный доступ и нажмите кнопку Создание учетной записи. Вскоре вы увидите, что учетная запись с указанным именем появилась в окне, показанном на рис. 28.9.

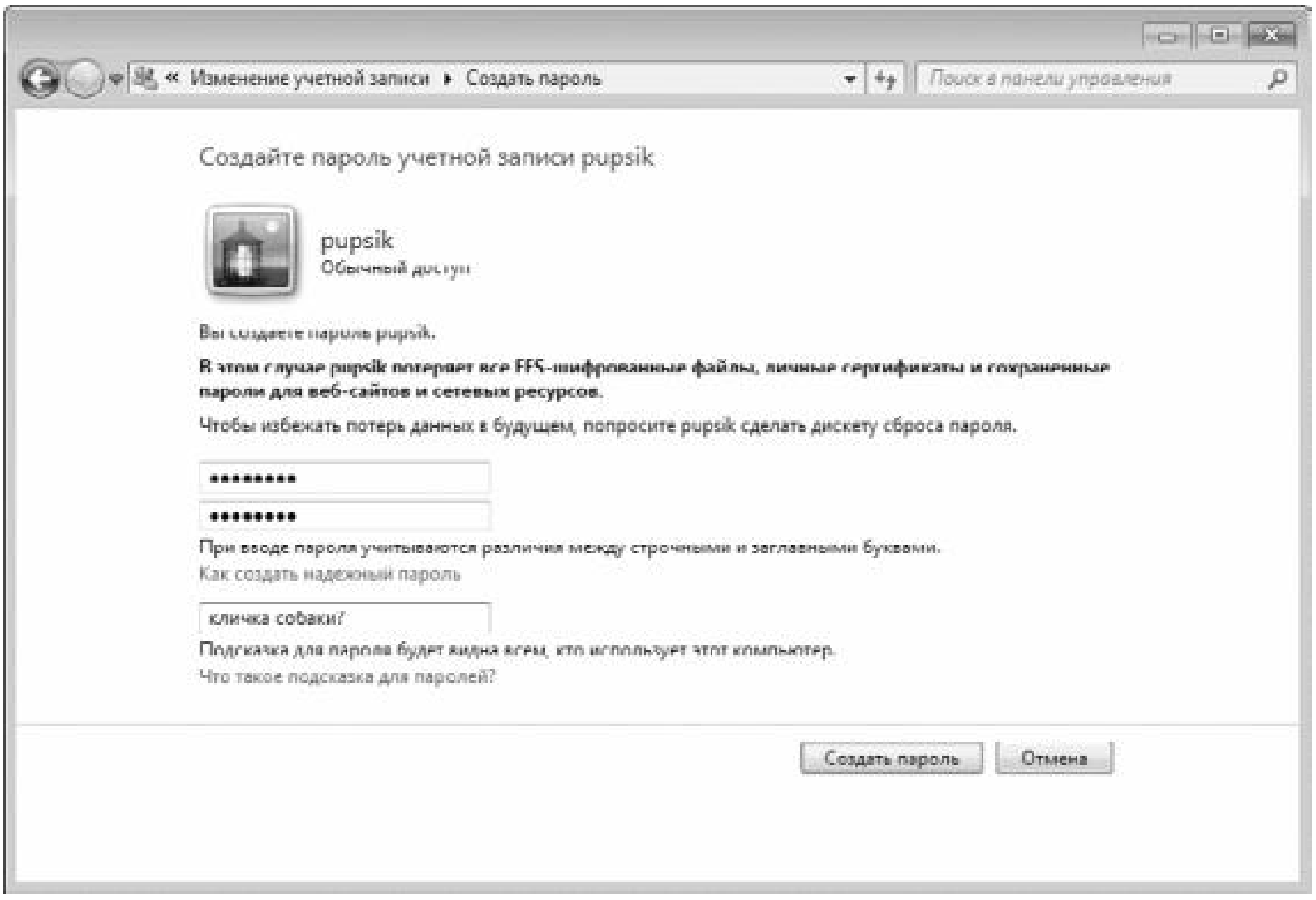
По умолчанию новая учетная запись не содержит пароля входа, и использование ее в таком виде для сетевой авторизации нежелательно. Чтобы установить пароль, щелкните по этой учетной записи (рис. 28.11).



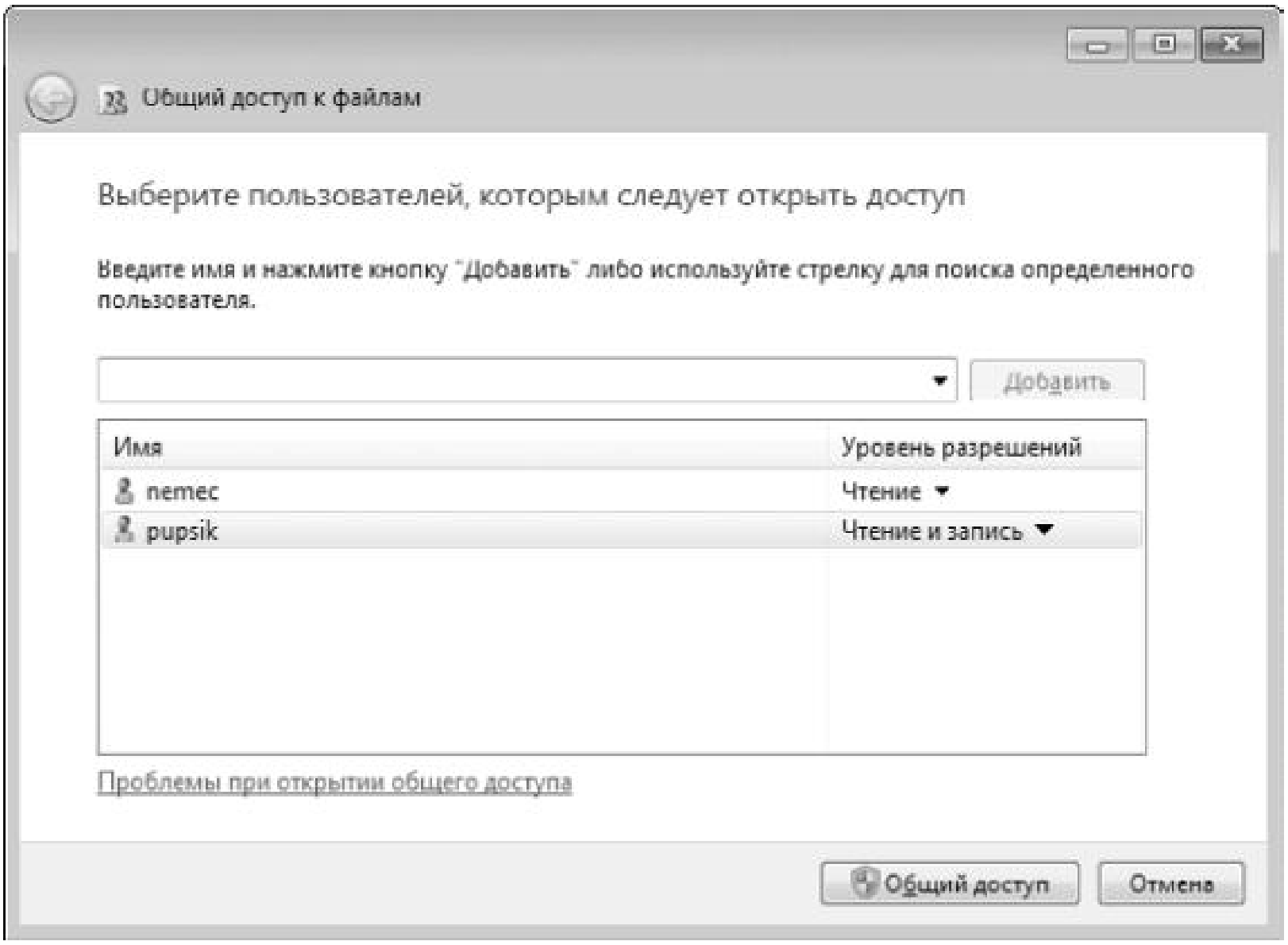
Это откроет окно управления учетной записью, в котором находятся несколько важных ссылок. Для создания пароля воспользуйтесь ссылкой Создание пароля (рис. 28.12).

В открывшемся окне укажите пароль с подтверждением, а также подсказку, которая в случае чего поможет этот пароль вспомнить. После нажатия кнопки Создать пароль мастер создания паролей проверит правильность заполнения данных и, если данные будут введены правильно, создаст пароль.

Теперь, если вы вернетесь к выбору учетных записей, которым необходимо предоставить доступ к ресурсу, то уже обнаружите в списке созданную вами запись (рис. 28.13).



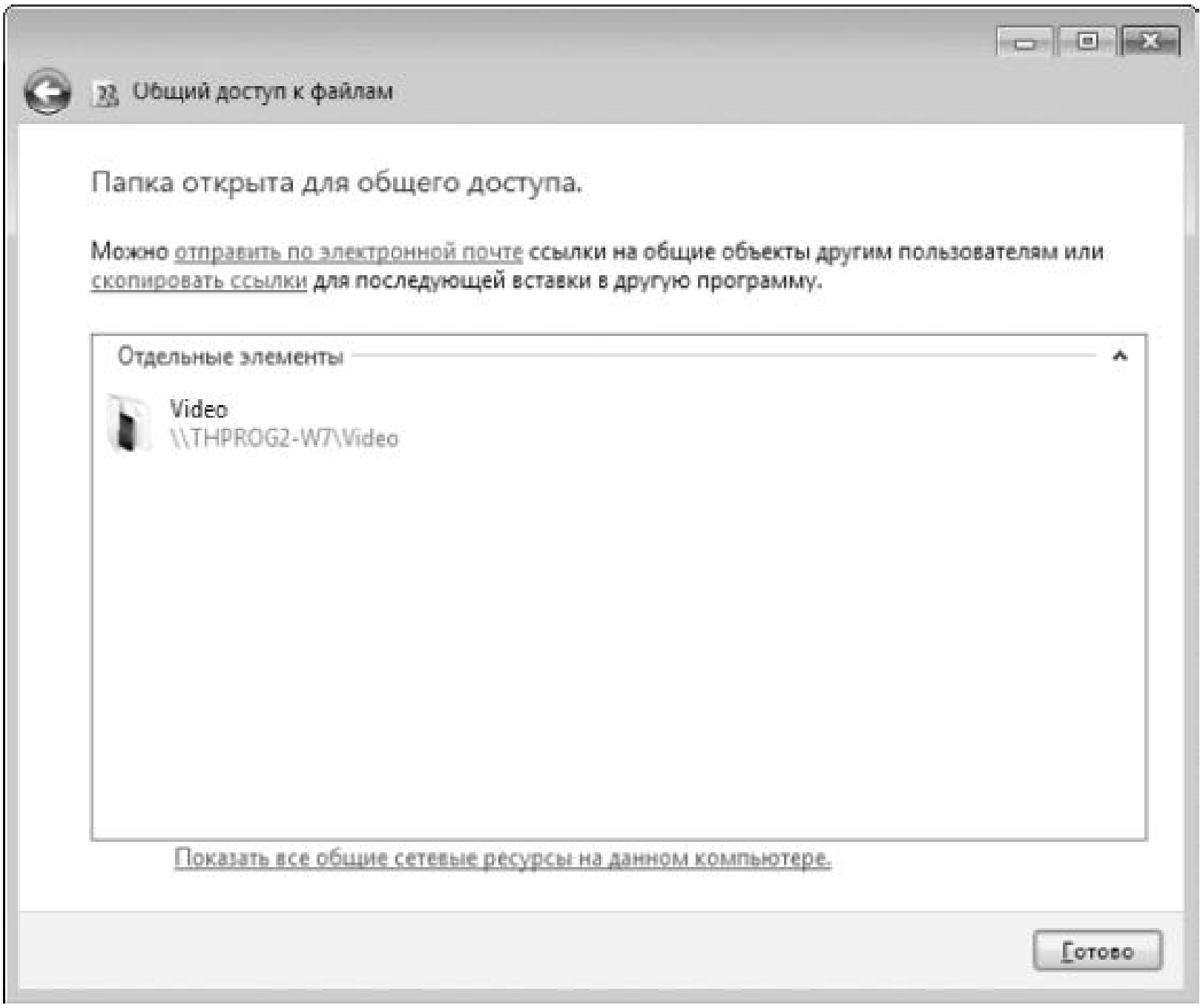
Отредактировал и опубликовал на сайте : PRESSI (HERSON)



Чтобы добавить ее в список доступа, выберите ее и нажмите кнопку Добавить. Теперь осталось только настроить права доступа. Сделать это очень просто: достаточно щелкнуть на учетной записи и в появившемся меню выбрать пункт Чтение или Чтение и Запись.

После того как права доступа отредактированы, нажмите кнопку Общий доступ (рис. 28.14).

Далее операционная система сделает все необходимые изменения, чтобы сетевые пользователи увидели и смогли получить доступ к вашему файловому ресурсу. Вам останется только сообщить нужным пользователям пароль доступа к соответствующим учетным записям.

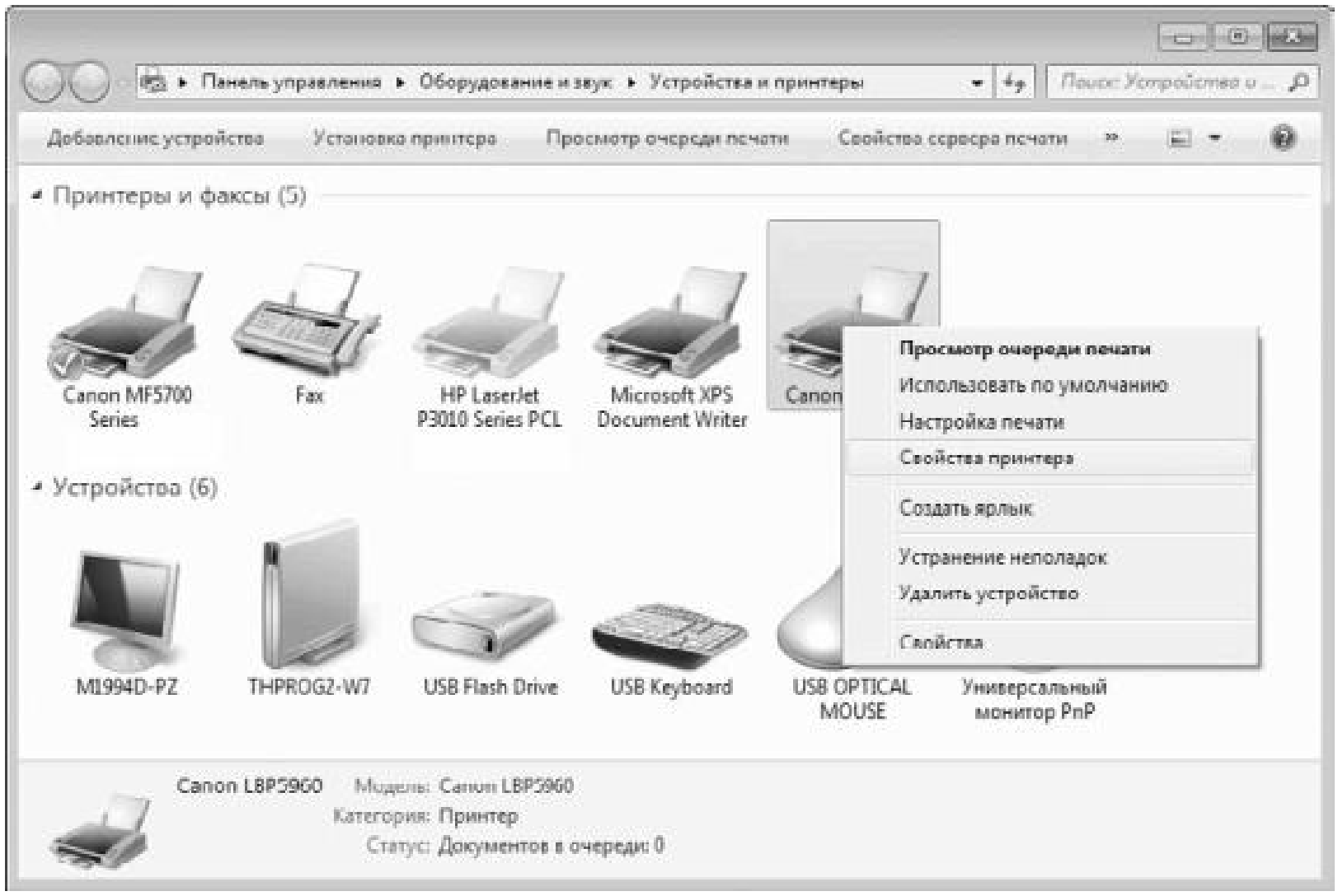


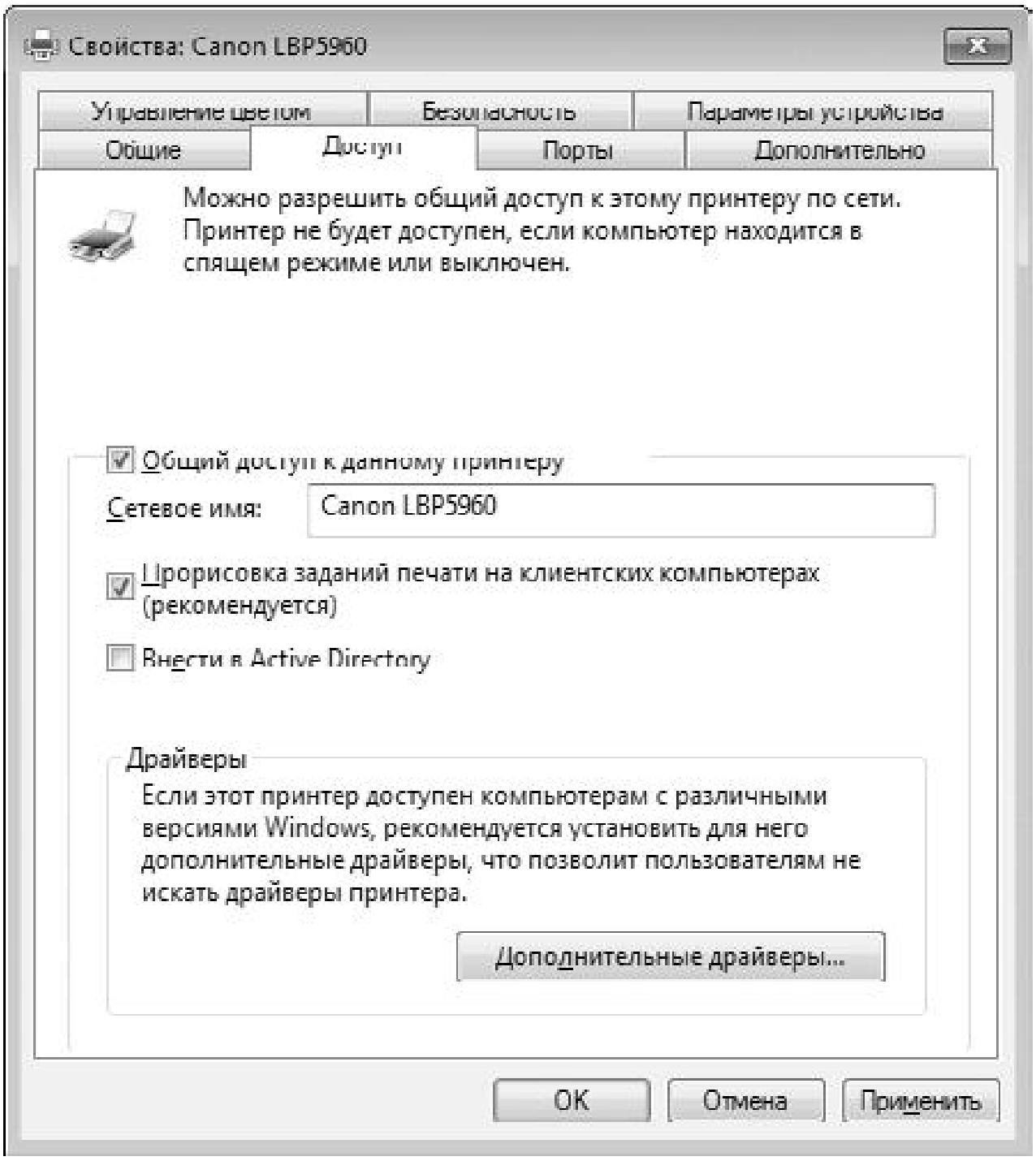
Создание доступа к принтеру

Открыть общий доступ к локальному принтеру не представляет никакой сложности. Прежде всего, откройте окно Устройства и принтеры, доступ к которому можно получить, открыв меню Пуск или Панель управления и выбрав соответствующий значок.

Данная группа содержит список некоторых устройств, которые используются в системе, позволяя получать быстрый доступ к их параметрам. Найдите в списке устройств принтер, доступ к которому вы хотите открыть, щелкните на нем правой кнопкой мыши и в появившемся меню выберите пункт Свойства принтера (рис. 28.15).

В результате откроется окно, содержащее несколько вкладок с параметрами и другой информацией. Нас интересует вкладка Доступ, поэтому переходим на нее (рис. 28.16).

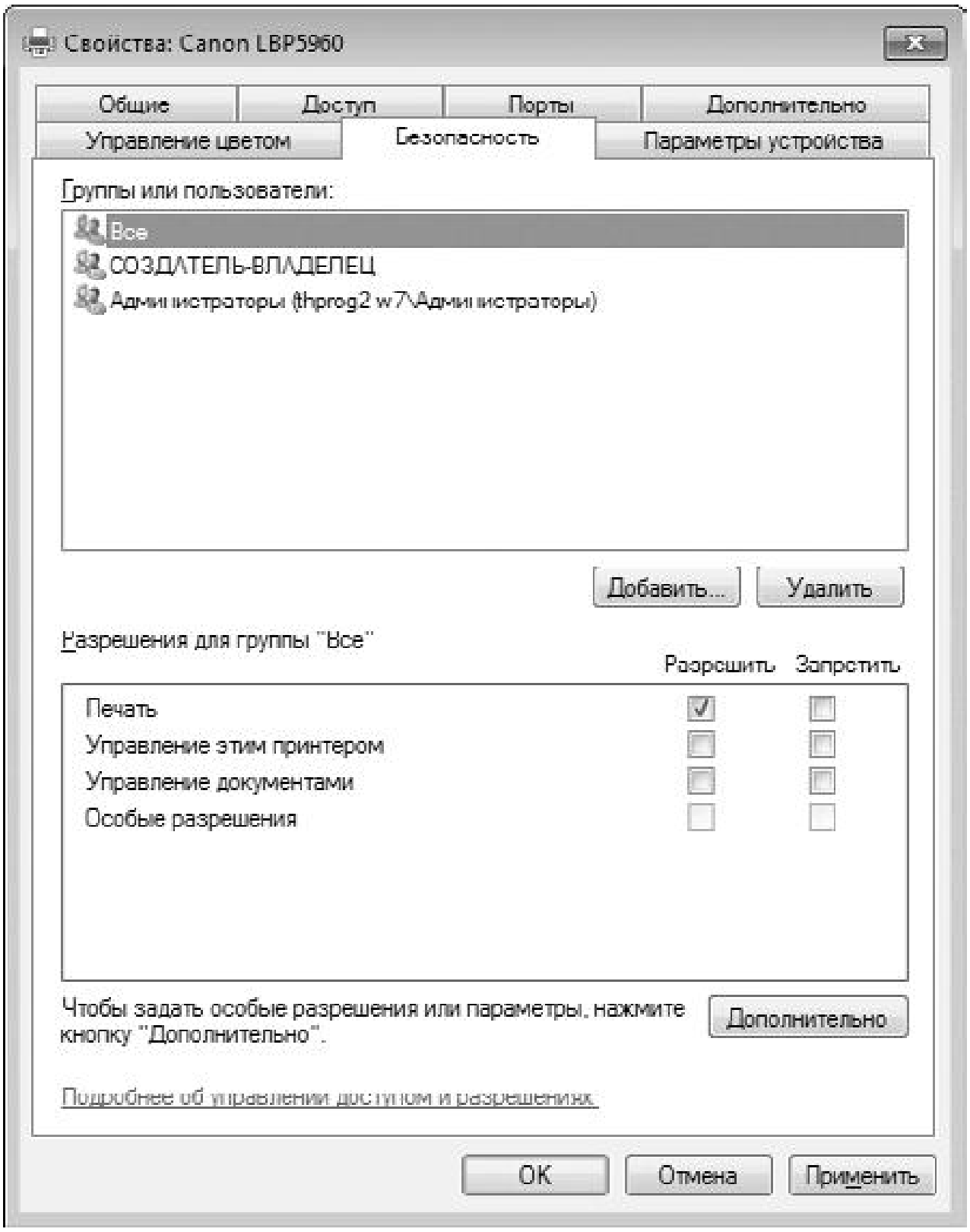

Панель управления ▸ Оборудование и звук ▸ Устройства и принтеры
Поиск: Устройства и ...
Добавление устройства
Установка принтера
Просмотр очереди печати
Свойства сервера печати
Принтеры и факсы (5)
Canon MF5700 Series
Fax
HP LaserJet P3010 Series PCL
Microsoft XPS Document Writer
Canon
Просмотр очереди печати
Использовать по умолчанию
Настройка печати
Свойства принтера
Создать ярлык
Устранение неполадок
Удалить устройство
Свойства
Устройства (6)
M1994D-PZ
THPROG2-W7
USB Flash Drive
USB Keyboard
USB OPTICAL MOUSE
Универсальный монитор PnP
Canon L8P5960
Модель: Canon L8P5960
Категория: Принтер
Статус: Документов в очереди: 0



Чтобы открыть доступ к принтеру, установите флажок Общий доступ к данному принтеру и укажите сетевое имя принтера, под которым его смогут видеть другие пользователи. По умолчанию доступ к принтеру, то есть возможность печати на нем, получат сразу все пользователи локальной сети.

Как и в случае с созданием общего файлового ресурса, если вы хотите, чтобы некоторые пользователи смогли не только печатать на принтере, но и управлять им или управлять очередью печати, нужно будет добавить соответствующие учетные записи, как это было описано выше. Когда они буду созданы, перейдите на вкладку Безопасность (рис. 28.17).

После нажатия кнопки Добавить появится уже знакомое вам окно (см. рис. 28.7), в котором можно будет выбрать учетные записи. После их подтверждения все они появятся в списке на вкладке Безопасность, и, используя флажки в нижней ее части, вы сможете более точно настроить права доступа к принтеру.



Доменная структура

Принцип создания общих ресурсов при работе компьютера в составе доменной структуры практически полностью идентичен случаю использования рабочих групп. Исключение составляет лишь источник, из которого выбираются учетные записи для настройки прав доступа: в случае с рабочей группой использовались локальные учетные записи, а здесь используются учетные записи из домена.

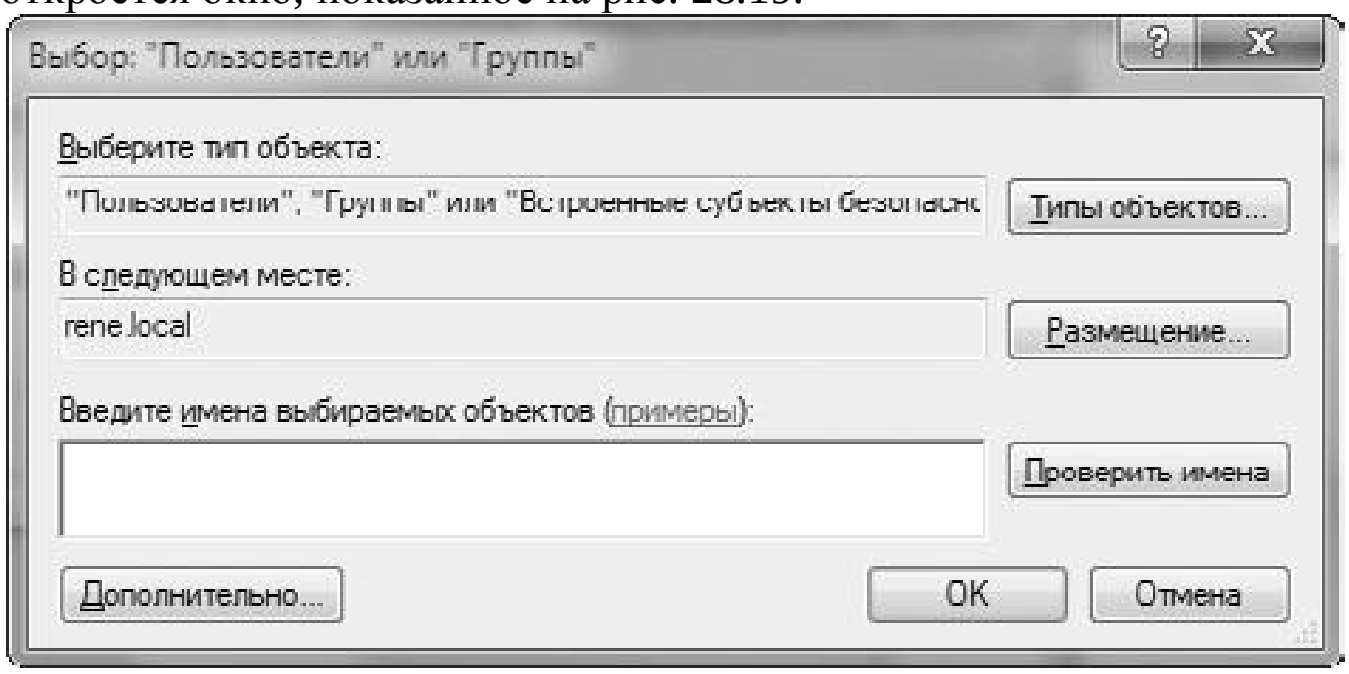
В качестве примера рассмотрим процесс создания общего файлового ресурса с настройкой прав доступа для отдельных пользователей.

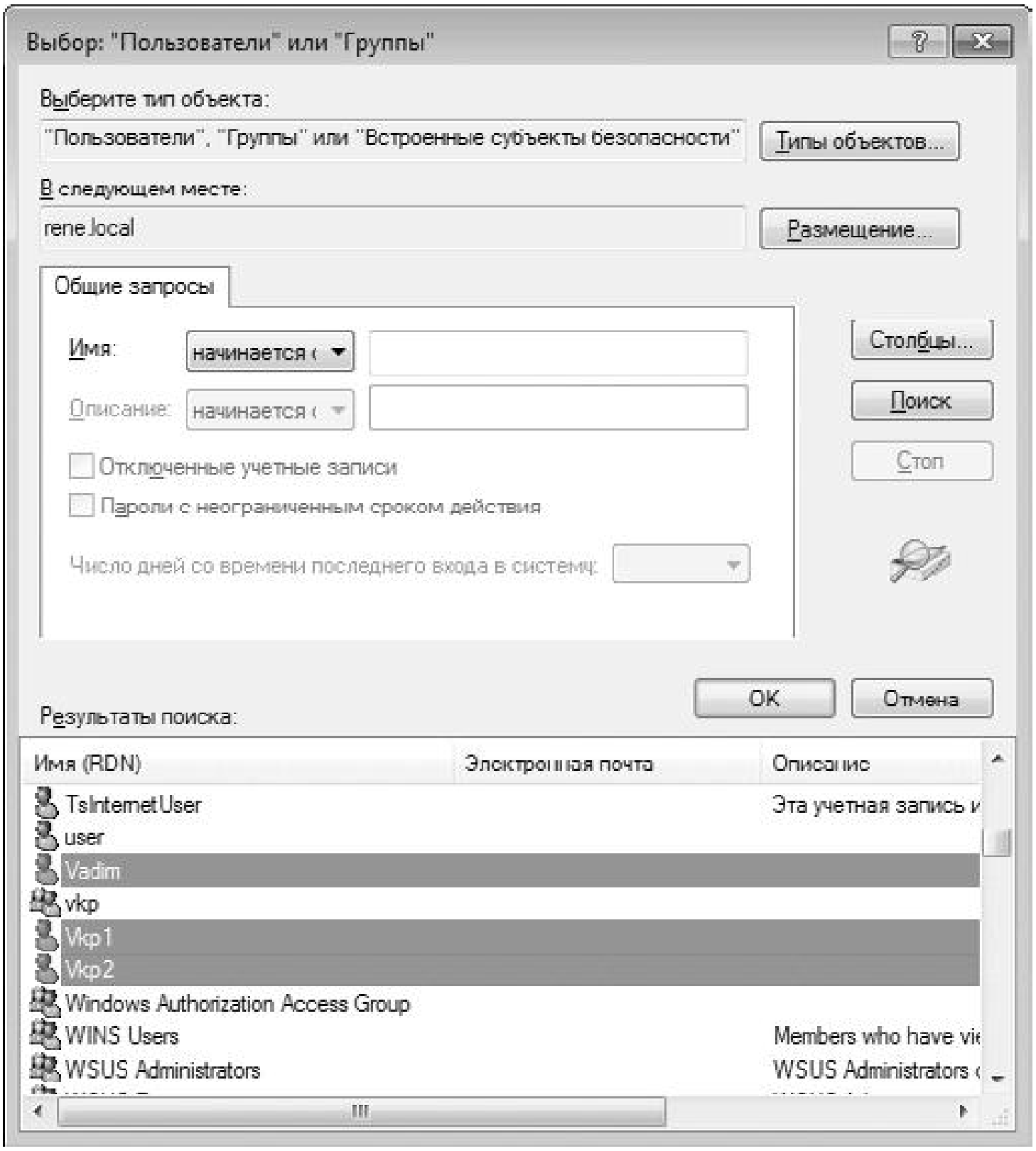
Начнем с того места, когда необходимо создать список объектов (см. рис. 28.7), которым будет предоставлен доступ. Обратите внимание, что в списке выбора пользователей

присутствует позиция Поиск пользователей, которую мы и будем использовать.

После ее выбора откроется окно, показанное на рис. 28.18.

Наиболее простой способ добавления объектов – использовать визуальный список записей. Чтобы им воспользоваться, нажмите кнопку Дополнительно. В результате откроется окно, показанное на рис. 28.19.





Чтобы увидеть список объектов, которые можно выбрать, нажмите кнопку Поиск. Далее в появившемся списке необходимо найти позиции, которые обозначают нужные учетные записи пользователей или групп. Чтобы выбрать сразу несколько групп, при выделении удерживайте нажатой клавишу Ctrl После того как все нужные объекты выбраны, нажмите кнопку ОК.

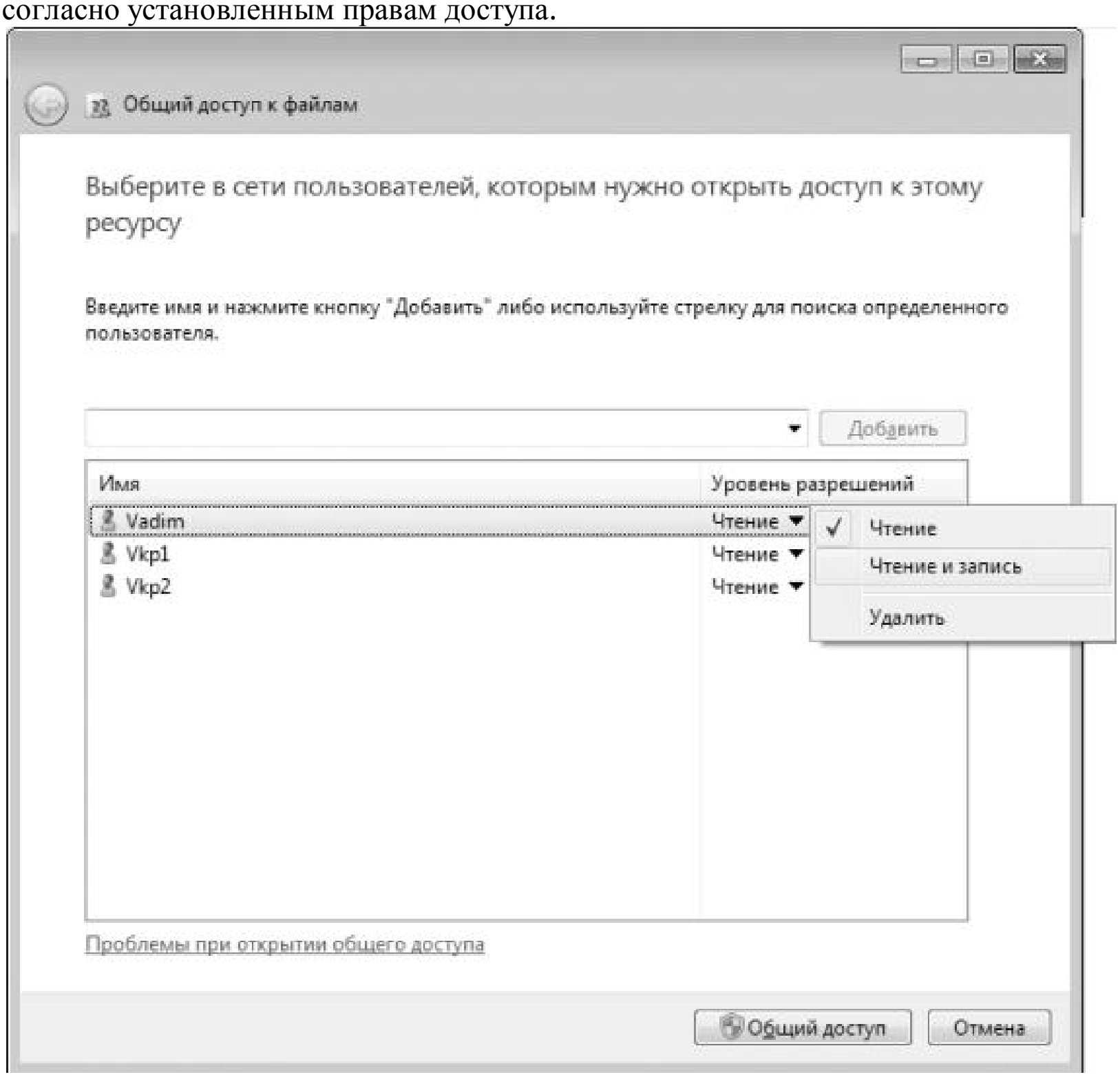
В результате выбранные объекты появятся в окне, показанном на рис. 28.18. Теперь, чтобы продолжить настройку прав доступа, нажмите кнопку ОК.

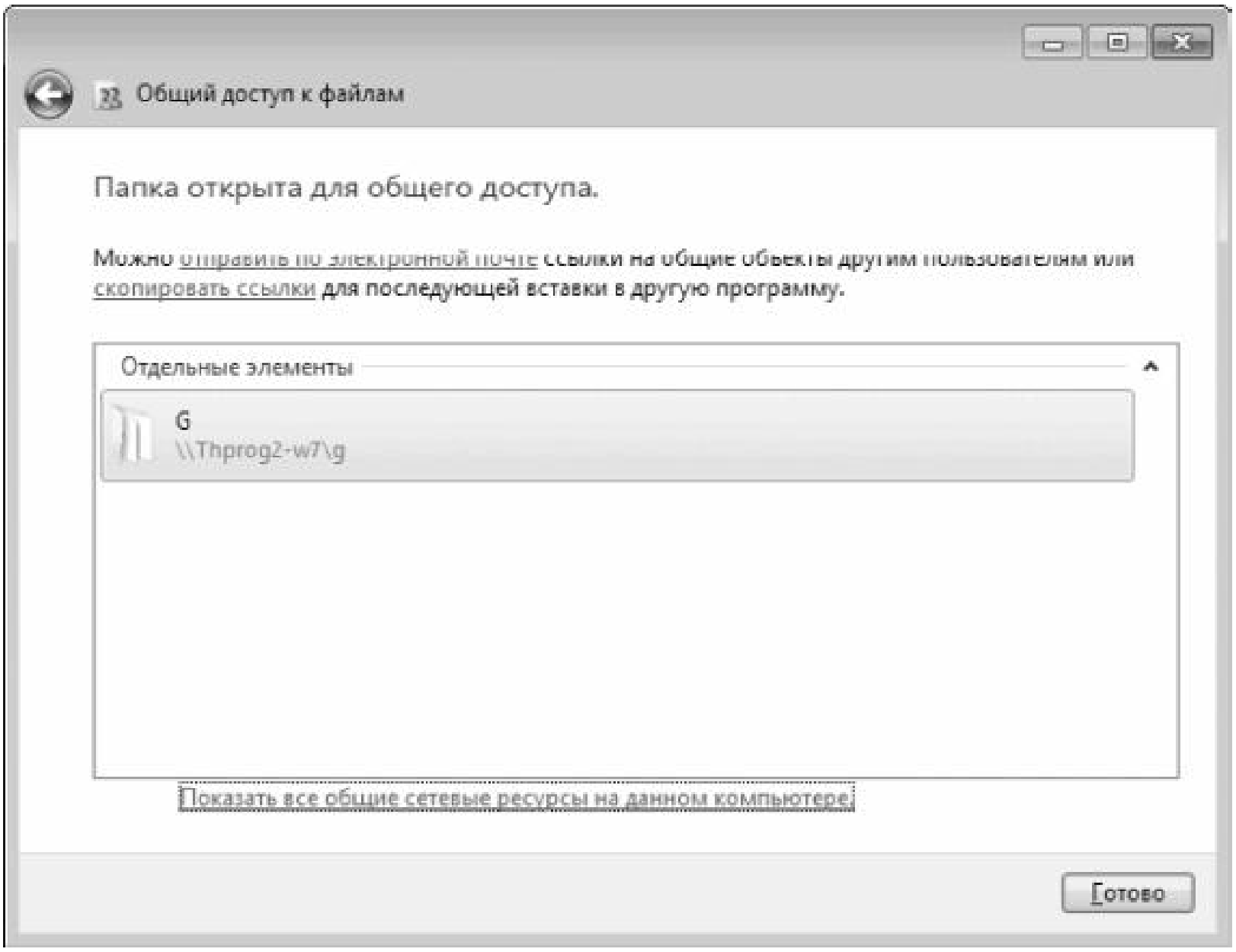
По умолчанию все учетные записи, добавленные в список, смогут использовать ваш ресурс только в режиме чтения, о чем свидетельствует надпись Чтение рядом с каждой учетной записью. Если некоторым учетным записям вы хотите разрешить использовать ресурс с правом изменения, щелкните на строке с именем учетной записи и в появившемся меню выберите пункт Чтение и Запись (рис. 28.20).

На этом настройка прав доступа к будущему общему ресурсу завершена, и, чтобы его

создать, нажмите кнопку Общий доступ. По прошествии небольшого количества времени появится окно, сообщающее, что общий доступ к указанной вами папке открыт (рис. 28.21).

После этого сетевые пользователи смогут увидеть ваш ресурс и использовать его согласно установленным правам доступа.





Глава 29
Антивирусная защита

Компьютер – универсальный помощник, способный решать практически любую поставленную перед ним задачу. Работа с офисными документами, серфинг в Интернете, совместная работа в программах, использование информационных баз данных, обработка аудио– и видеоконтента – это далеко не полный список того, в чем компьютер может проявить себя на все 100 %.

К сожалению, некоторым людям гораздо интересней помешать работе компьютера, нежели помочь ему в этом. Именно они стали причиной появления разного рода вирусов, троянов, шпионских программ и другого вредоносного кода, способного нанести вред операционной системе и компьютеру, украсть важные данные и т. п. Угроза становится еще серьезнее, если компьютер подключается к локальной сети и получает доступ в Интернет.

Чтобы защитить операционную систему и свои личные данные и документы от вирусов, необходимо использовать специальное программное обеспечение. Существует достаточно много разнообразных антивирусных программ, которые позволяют защитить компьютер

от проникновения вирусов и другого вредного кода. После установки такая программа сразу же берет под свой контроль все объекты файловой системы, а также проверяет и при необходимости блокирует все, что проникает в компьютер. При этом используются постоянно обновляемые базы вирусных сигнатур, то есть кусков кода, характеризующих тот или иной вирус. Анализируя любой файл, программа сверяет его код с кодом из данной базы, и, если обнаружено совпадение или подобие кода, файл считается зараженным. Дальнейшая судьба файла зависит от настроек программы: если она умеет, то может попробовать вылечить файл и удалить из него вирусный код. В противном случае файл удаляется или переносится в карантин.

Когда речь идет о корпоративной сети, наилучшим вариантом защиты компьютеров является использование корпоративной версии антивирусной программы. Это позволяет установить серверную часть антивирусной программы на сервер, а на клиентских компьютерах установить, соответственно, ее клиентскую часть. Преимуществом этого подхода является возможность автоматически обновлять базы вирусных сигнатур на сервере, не затрагивая при этом клиентские компьютеры. Кроме того, поскольку сервер всегда включен, вся сеть постоянно находится под защитой.

Если речь идет об одноранговой сети или о сети из небольшого количества компьютеров, то можно использовать антивирусные программы на каждом компьютере, при этом за обновлением базы вирусных сигнатур придется следить каждому пользователю либо системному администратору.

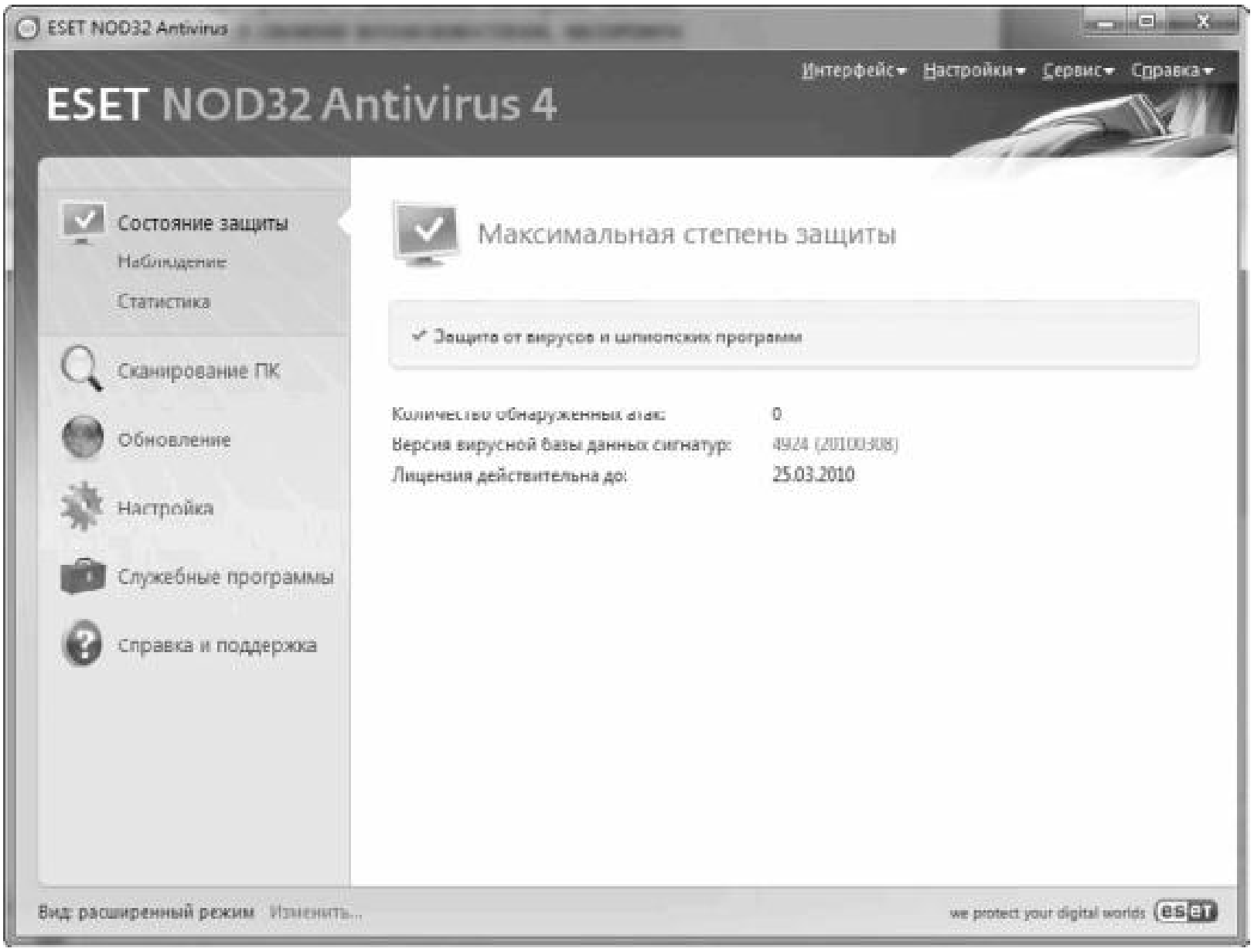
Существует достаточно много антивирусных программ, с помощью которых можно организовать защиту компьютера. Они отличаются своими возможностями, наличием дополнительных систем защиты, например персональным брандмауэром, защитой от спама и т. п. Из наиболее распространенных программ можно отметить Norton Antivirus, ESET, Dr.Web, Антивирус Касперского, Avira и др.

Принцип работы антивирусных программ за исключением некоторых нюансов одинаковый, поэтому не имеет смысла рассматривать каждую из них. Для примера проанализируем возможности программы ESET NOD32 Antivirus.

Нужно сказать, что ESSET выпускает как корпоративные, так и обычные версии антивирусной программы, при этом существует несколько разных модификаций. Из обычных версий наиболее популярными стали ESET Smart Security и ESET NOD32 Antivirus. Smart Security дополнительно имеет в своем составе персональный брандмауэр, что позволяет защитить компьютер как от вирусного кода, так и программ, которые могут отсылать данные, используя для этого незащищенные порты. Однако настройка этой версии программы требует определенных знаний, поэтому ее используют только опытные пользователи. Для «неизбалованных» знаниями пользователей отлично подойдет версия ESET NOD32 Antivirus, которая будет рассмотрена ниже.

Интерфейс программы предельно простой, что делает ее очень удобной в использовании. После установки программы ее значок появляется на Панели задач, и если требуется выполнить какие-либо действия, то открыть главное окно программы можно двойным щелчком на этом значке.

Главное окно программы разбито на две части: в левой части отображается список разделов, выбор одного из которых приводит к смене содержимого правой части окна (рис. 29.1).

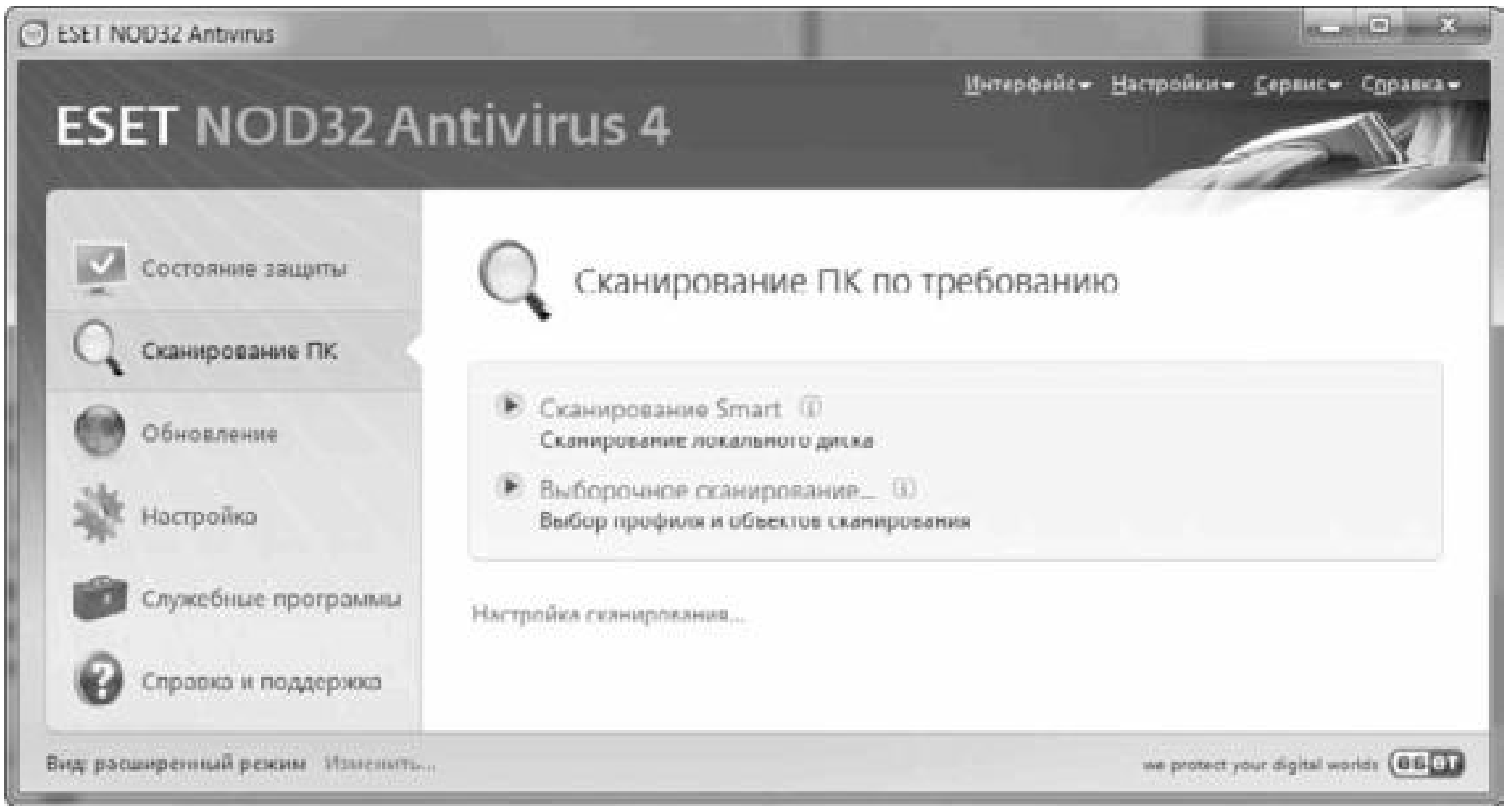


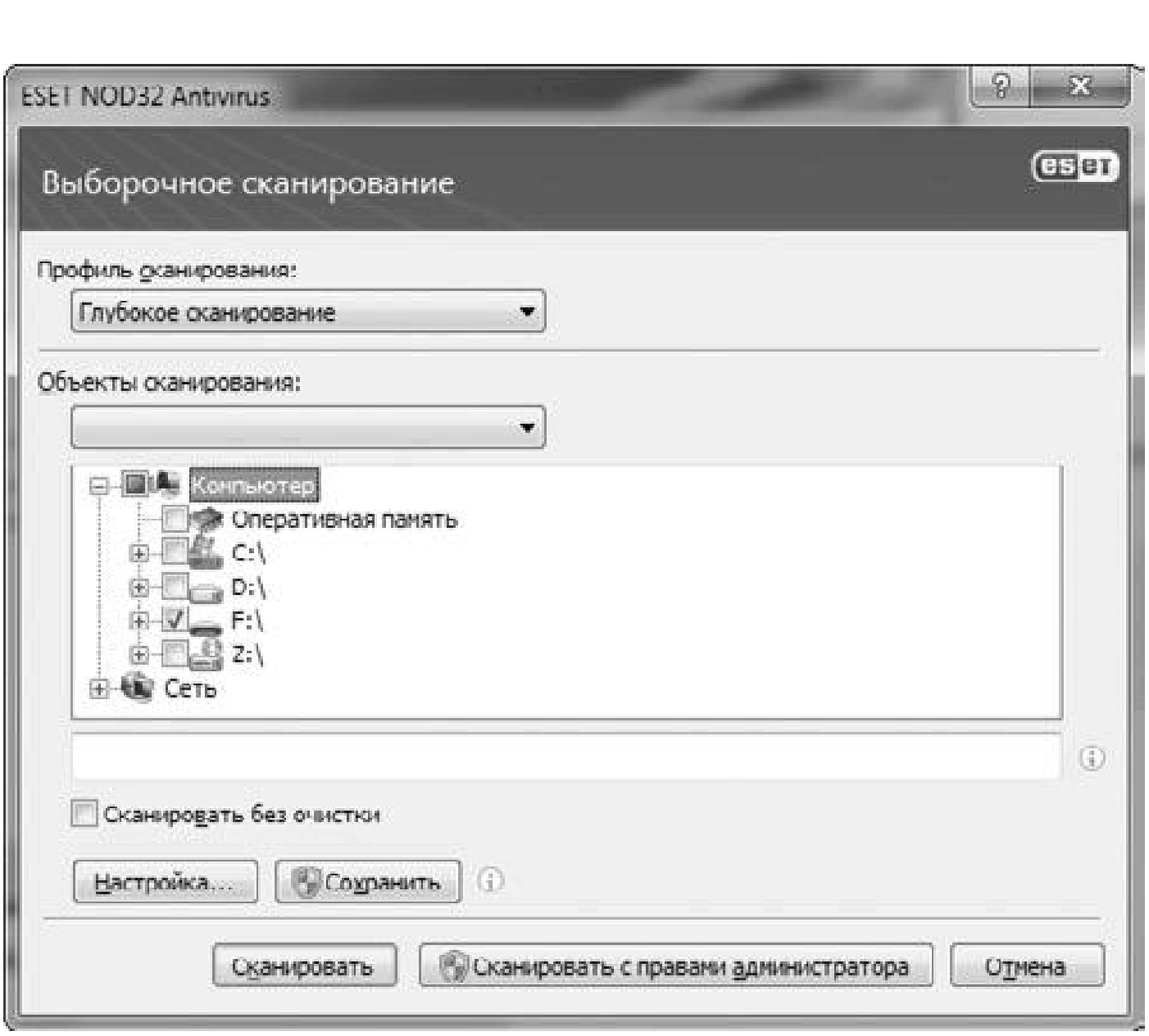
Состояние защиты. Данный раздел включает пункты Наблюдение и Статистика, используя которые вы можете просматривать графики активности файловой системы и статистику по защите от вирусов и шпионских программ в разных режимах работы.

Здесь же можно увидеть текущее состояние работы программы, количество атак, версию базы вирусных сигнатур и, самое главное, состояние лицензии.

Сканирование ПК. Это меню позволяет выбирать режим сканирования компьютеров. Несмотря на то что сканирование и наблюдение за файловой системой происходит постоянно, вы в любой момент можете запустить процесс сканирования. При этом вы можете сделать как полное сканирование системы, включающее сканирование всех доступных дисков, так и выборочное сканирование (рис. 29.2).

К примеру, если требуется проверить DVD или flash-накопитель, вы всегда можете воспользоваться выборочным сканированием, указав при этом параметры сканирования и поведения при обнаружении зараженных или подозрительных объектов. Для этого достаточно выбрать позицию Выборочное сканирование, отметить необходимые объекты, указать параметры сканирования и нажать кнопку Сканировать (рис. 29.3).



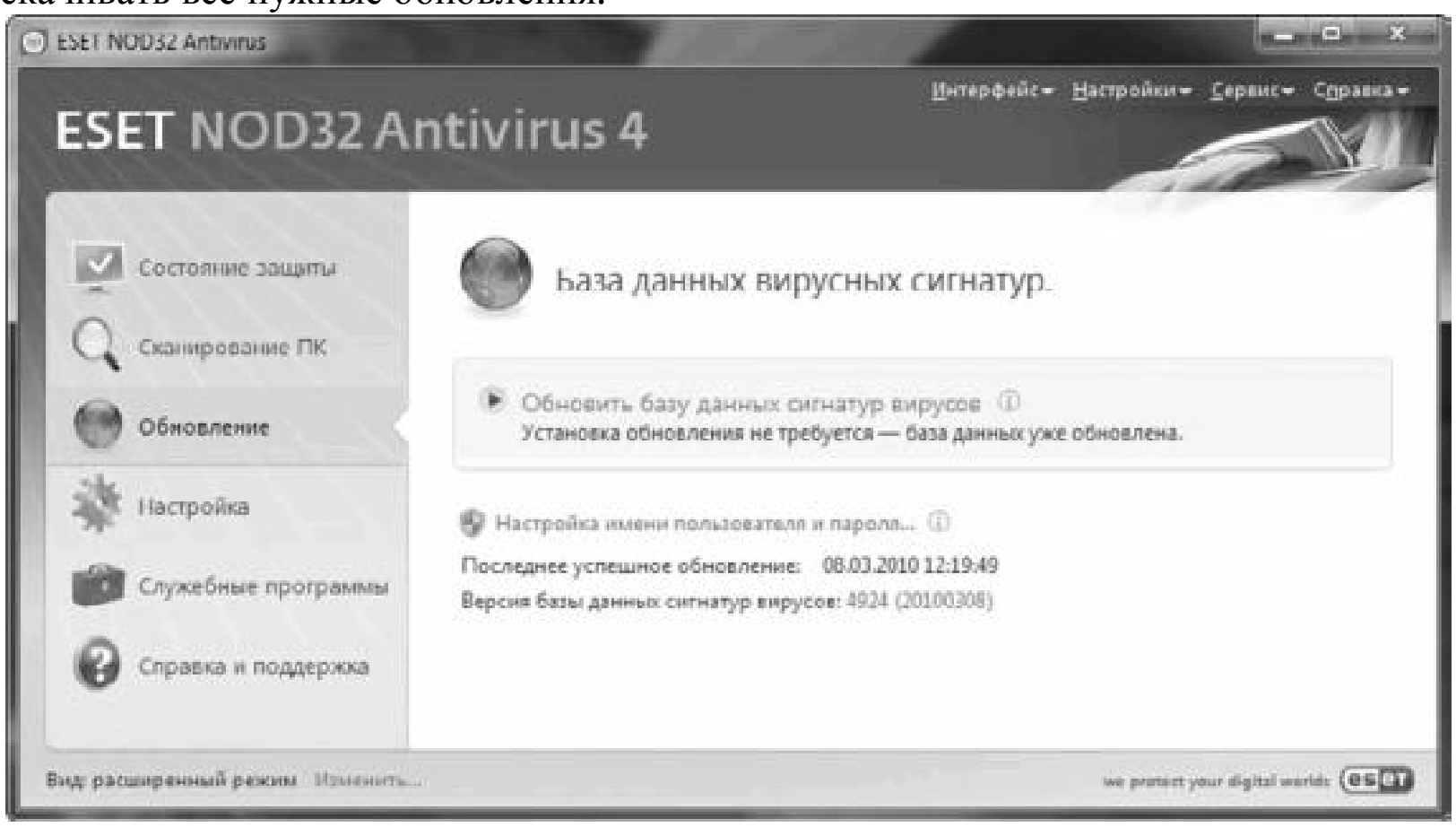


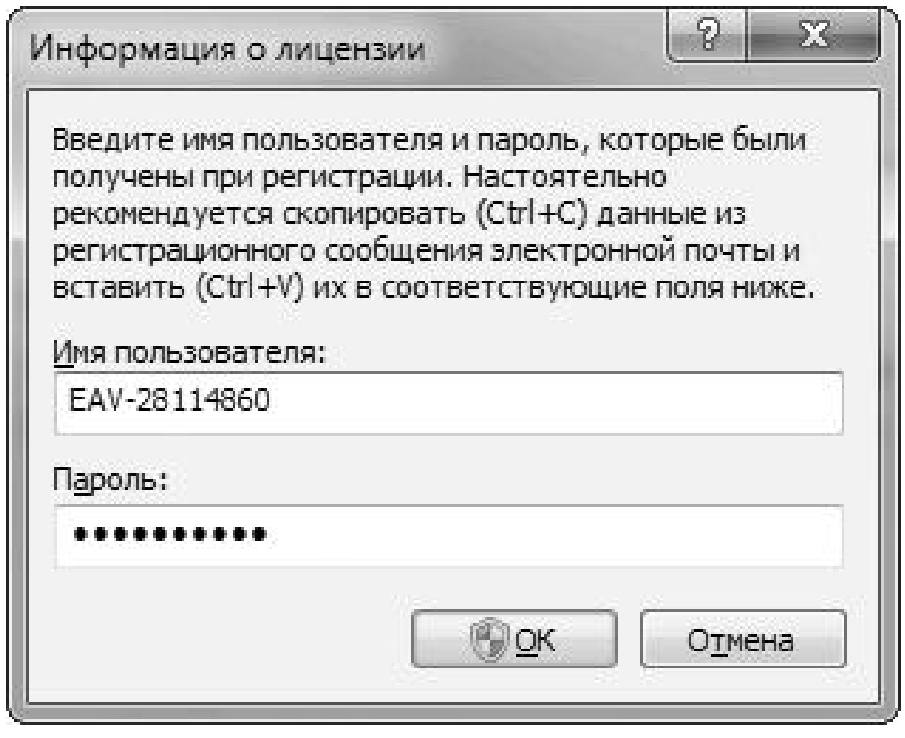
Процесс сканирования может отображаться как в окне, показанном на рис. 29.2, так и в отдельном окне. При этом вы в любой момент можете приостановить сканирование или отменить его. В процессе сканирования выводится информация о сканируемых объектах, поэтому, если будут обнаружены опасные объекты, вы об этом сразу же будете оповещены. Более того, если программа не сможет автоматически определить, что делать с зараженным объектом, появится соответствующее окно, в котором вам необходимо будет выбрать правильный вариант действия.

Обновление. С помощью этого раздела можно обновлять программу и антивирусные базы, а также управлять лицензией, разрешающей использовать программу и скачивать обновления (рис. 29.4).

Лицензия дает право использовать программу на протяжении некоторого времени, например трех месяцев. По истечении этого периода обновление программы и баз вирусных сигнатур будет невозможным, о чем программа будет предупреждать вас каждый раз, когда вы будете пытаться это сделать. В этом случае не остается ничего другого, как купить новую лицензию и добавить данные о ней. Для этого используется ссылка Настройка имени пользователя и пароля.

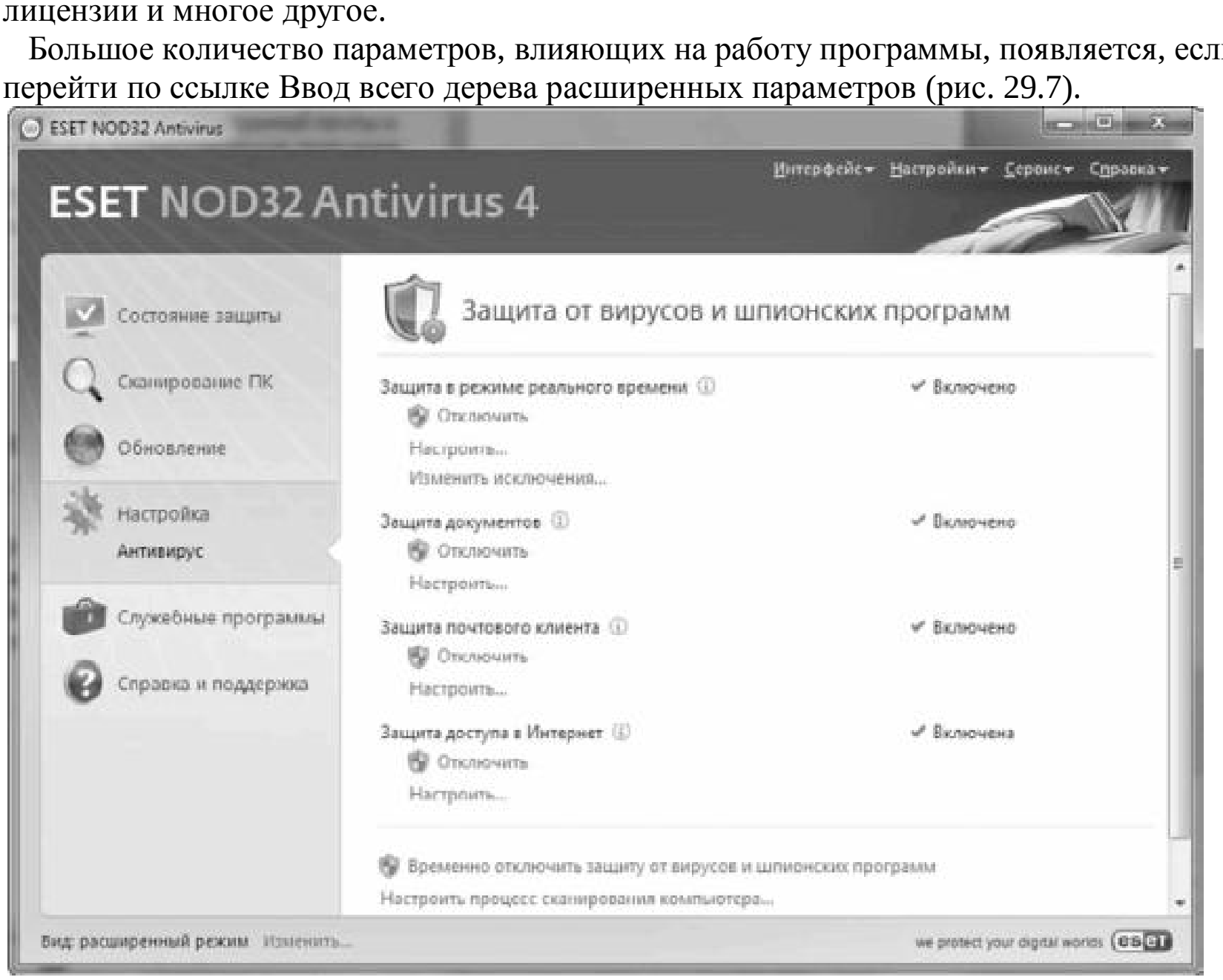
После перехода по этой ссылке появится окно (рис. 29.5), в котором вам необходимо указать новые имя пользователя и пароль, используя которые программа сможет скачивать все нужные обновления.

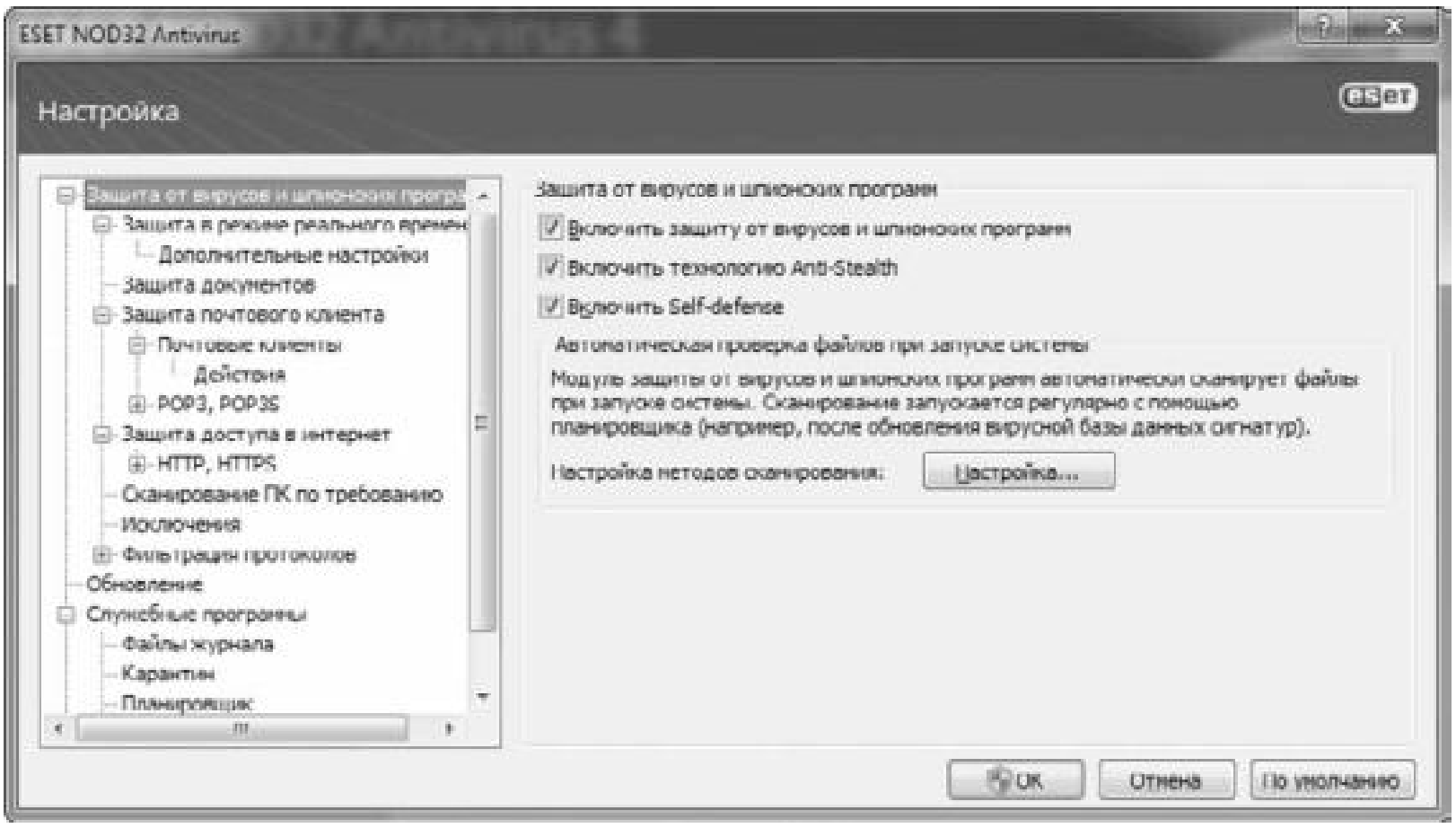




Настройка. Этот раздел программы используется для произведения разного рода настроек. В частности, можно включать и отключать защиту разных областей (рис. 29.6), сохранять или загружать конфигурационный файл программы, настраивать данные лицензии и многое другое.

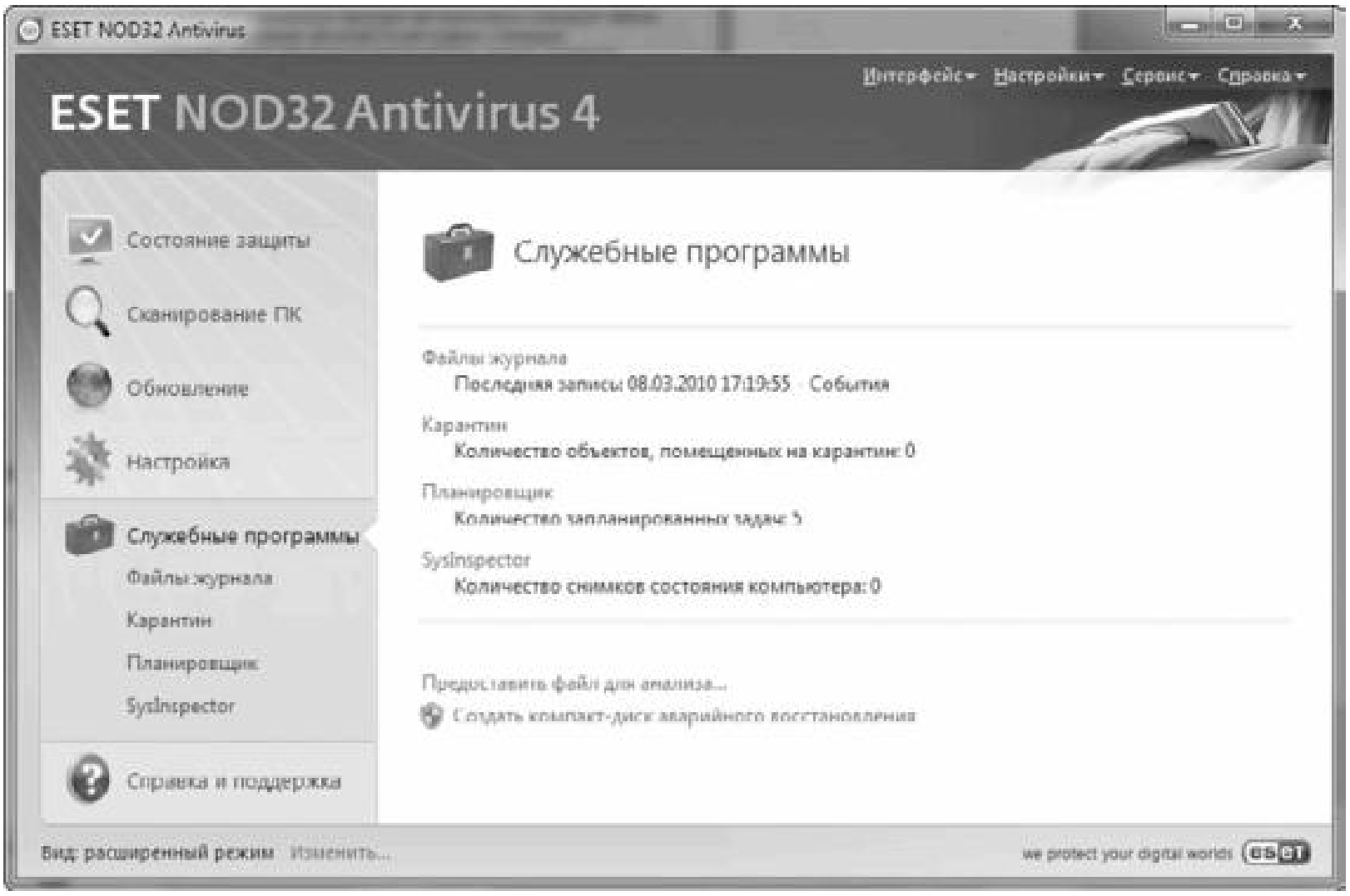
Большое количество параметров, влияющих на работу программы, появляется, если перейти по ссылке Ввод всего дерева расширенных параметров (рис. 29.7).

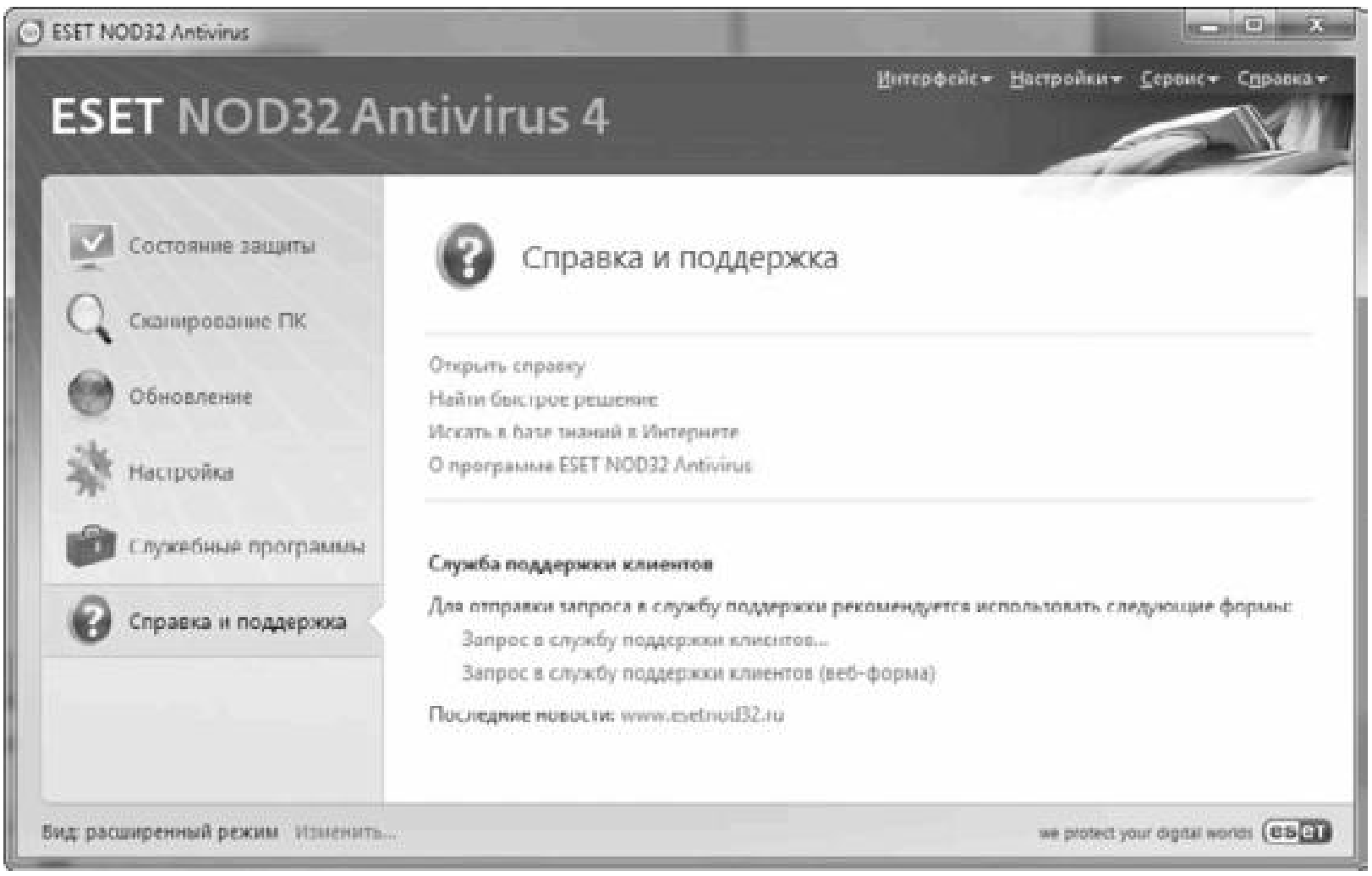




Служебные программы. В этом разделе помещены некоторые дополнительные компоненты программы, позволяющие просматривать служебную информацию, файлы карантина, настраивать автоматическое сканирование компьютера и многое другое (рис. 29.8).

Справка и поддержка. В данном разделе можно познакомиться с некоторой справочной информацией (рис. 29.9), которая может помочь вам разобраться с работой интерфейса программы или, к примеру, найти сведения об интересующем вас вирусе или троянской программе.





Работа программы в большинстве случаев не требует вмешательства пользователя. Для начала ее работы достаточно сразу после установки программы указать данные лицензии и параметры прокси-сервера, если таковой используется. Программа сама знает, что и как делать, автоматически несколько раз в день проверяет обновления программы и баз вирусных сигнатур. Вы будете вспоминать о ней только при виде всплывающих сообщений о том, что программа или антивирусная база обновилась, найден и обезврежен вирусный код или требуется участие пользователя, если случилась непредвиденная ситуация.

Глава 30
Интернет-браузер

Одним из плюсов локальной сети является возможность организации общего доступа в Интернет – к практически безграничному количеству информации разного типа. Документы, графические изображения, музыкальные и видеоколлекции, игры, просмотр фильмов, общение и многое другое – все это будет в вашем распоряжении.

Чтобы просматривать содержимое web– и ftp-ресурсов, используется специальная программа, которая называется интернет-браузером. Существует достаточно много браузеров, например Internet Explorer, Mozilla Firefox, Opera, Google Chrome и др. Однако, несмотря на то что их главная задача – отображать содержимое ресурса, они имеют достаточно серьезные отличия.

Некоторые браузеры могут похвастаться точным отображением содержимого ресурсов по существующим правилам, другие – скоростью загрузки страниц, третьи – удобством интерфейса и т. д. Именно поэтому существует достаточно много браузеров, производители которых постоянно ведут между собой конкурентную борьбу за «обладание» пользователями.

Из наиболее зарекомендовавших себя можно отметить браузеры Mozilla Firefox и Opera. Они могут похвастаться быстрой работой, большим количеством дополнений, расширяющих их возможности, и, самое главное, защищенностью, что делает доступ в Интернет более безопасным.

Ниже мы коротко рассмотрим возможности этих браузеров, в том числе и те, которые делают их столь популярными.

Mozilla Firefox

Браузер Mozilla Firefox получил широкое распространение благодаря своей быстрой и устойчивой работе, но самое главное – он отображает содержимое страниц в полном соответствии со стандартами W3C (World Wide Web Consortium). Этот браузер распространяется свободно и, согласно некоторым независимым исследованиям, является вторым по популярности браузером в мире. Существуют версии браузера, работающие в самых популярных операционных системах, включая Microsoft Windows любой современной версии.

Mozilla Firefox имеет очень простой интерфейс, не перегруженный многочисленными

кнопками (рис. 30.1), поэтому освоить его можно очень быстро и без особых усилий.

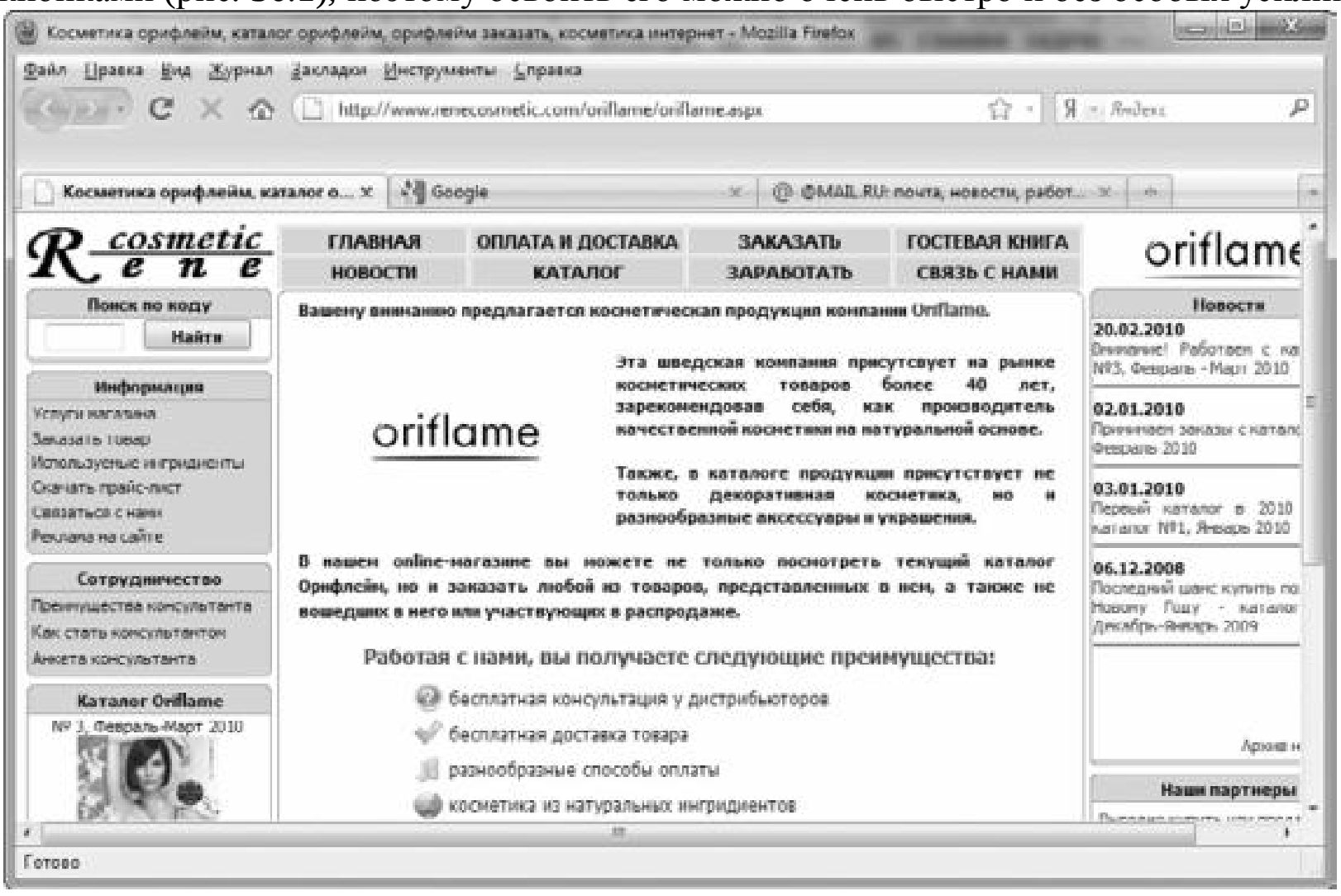


Рис. 30.1. Браузер Mozilla Firefox

Однако, несмотря на внешнюю простоту, его функциональность просто поражает. Вот лишь некоторые из возможностей, которые, собственно, и делают этот браузер очень популярным.

▪ Поддержка работы с вкладками. Вкладки позволяют открывать страницы внутри одного окна, при этом каждая страница располагается на своей вкладке и имеет отдельное от других вкладок управление.

▪ Большое количество дополнений (более 5000). С помощью дополнений можно расширить функциональность браузера, добавив ему много интересных функций, например быстрый запуск страниц, многострочную панель управления, переводчик текста, поддержку блогов и новостей и многое другое.

▪ Консоль ошибок. С помощью консоли ошибок программисты могут отлаживать и тестировать свои проекты веб-ресурсов на предмет совместимости со стандартами W3C.

▪ Быстрое масштабирование страниц. Очень удобный способ рассмотреть слишком мелкий или уменьшить слишком большой текст.

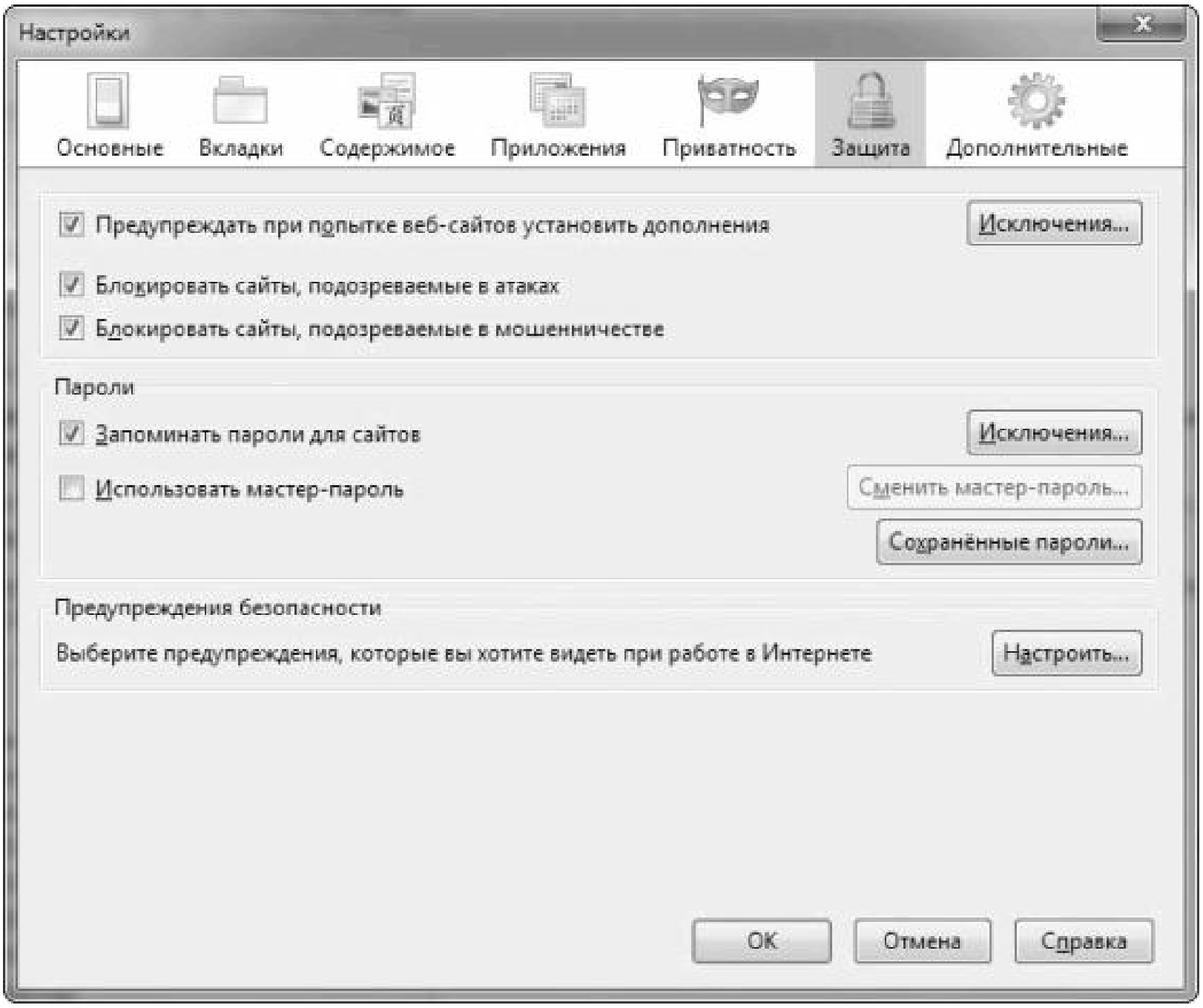
▪ Стили оформления. Если вам надоело стандартное оформление браузера, сменить его не составит особого труда: просто загрузите любой из сотен оригинальных стилей.

▪ Быстрый поиск информации на странице.

▪ Режим приватного просмотра. Используя данный режим, вы сможете просматривать любые интернет-страницы, не оставляя следов своего присутствия.

▪ Автоматическое обновление браузера. Поиск и установка обновлений происходят автоматически, когда вы просматриваете страницы.

Браузер имеет множество параметров, с помощью которых можно влиять на его работу, а также на отображение содержимого веб-страниц. Чтобы их увидеть, необходимо выбрать в верхнем меню пункт Инструменты ► Настройки (рис. 30.2).



Все параметры разбиты по различным вкладкам, переход между которыми осуществляется с помощью верхней панели инструментов. Здесь можно настроить параметры работы с вкладками, параметры выполнения кода на страницах, привязку приложений к разным расширениям файлов, параметры приватности и защиты, параметры прокси-сервера и многое другое.

Пользоваться браузером очень просто и удобно, поэтому многие отдают свое предпочтение именно ему. При этом существуют и полнофункциональные портативные версии, позволяющие использовать браузер без установки, что дает возможность оценить его функциональность на практике, прежде чем окончательно перейти на его использование.

Opera

Браузер Opera уже давно ценится пользователями компьютера за свою скорость работы благодаря продуманному механизму кэширования. Именно этот браузер первым стал поддерживать работу с вкладками и масштабирование содержимого страницы, включая и

графику.

Если браузер Mozilla Firefox получил распространение практически в любой стране мира, Opera в основном распространен в США, Канаде и странах Европы. В результате браузер стал мультиязычным, что очень удобно для пользователей: скачал, выбрал нужный язык и получил желаемое.

Последняя версия браузера может похвастаться не только предельно простым и понятным интерфейсом (рис. 30.3), но и скоростью запуска, не говоря уже о скорости просмотра страниц.

Нужно отметить, что интерфейс Opera продуман и выполнен очень качественно, что и приходится по душе многим пользователям. Все лишние кнопки и панели спрятаны, что позволяет максимально увеличить рабочую область для отображения веб-страниц. Чтобы получить доступ к панелям или другим функциям, достаточно кликнуть по букве О в левом верхнем углу программы.

Браузер имеет достаточно много настроек, которые очень удобно разбиты на редко-и частоиспользуемые, что позволяет получить быстрый доступ к последним, не запуская при этом дополнительных окон.

Браузер очень функционален и правильно отображает страницы любого содержания. Также можно настраивать параметры отображения для любого веб-ресурса: запрещать или разрешать выполнение кода, использование cookies, работу с мультимедийным содержимым и т. д.

Стоит особо отметить режим Opera Turbo, активировав который вы сможете сделать загрузку страниц в некоторых случаях на 80 % быстрее. Очень удобен также механизм Speed Dial, который позволяет настроить доступ к часто посещаемым ресурсам, отображая их миниатюры на стартовой странице браузера, как показано на рис. 30.3.

Заключение

Разнообразие типов и видов локальных сетей может запутать и усложнить выбор подходящего варианта, особенно когда дело касается неискушенного в таких вопросах

пользователя. Но на самом деле ничего сложного в этом нет, и всегда стоит ориентироваться на самый распространенный и доступный тип сети.

Книга, которую вы только что прочитали, не ставила перед собой задачи поразить вас множеством теоретических сведений и практических советов. У нее была более практическая цель – сообщить вам ровно столько, сколько нужно знать о сети, и научить ее создать, пусть даже и в скромных масштабах. И мы уверены, что эта цель достигнута. Успехов вам в создании сетей!