
А. Ватаманюк
на 100 %
СОЗДАНИЕ, ОБСЛУЖИВАНИЕ
И АДМИНИСТРИРОВАНИЕ
СЕТЕЙ
Освойте на 100 %:
• основные подходы к проектированию и созданию сетей различных типов
• способы обслуживания сетей
• правила настройки и администрирования сетей
ПИТЕР

Александр Иванович Ватаманюк

Создание, обслуживание и администрирование сетей на 100%

http://litres.ru
А. Ватаманюк. Создание, обслуживание и администрирование сетей на 100%: Питер; Санкт-Петербург; 2010
ISBN 978-5-49807-702-4

Аннотация

Что такое компьютерные сети? Всего-навсего несколько компьютеров и соединяющие их провода? И да, и нет. Причем «нет» прежде всего потому, что устройство и механизм работы каждой сети уникальны и далеко не так просты, как может показаться рядовому пользователю. Данная книга содержит всю необходимую информацию о проектировании и создании сетей различных типов и режимах их работы, а также обо всех тонкостях обслуживания и администрирования сетей. Освойте организацию сетей на 100% с помощью этого максимально подробного и доступного практического руководства.

Содержание

Ватаманюк Александр Иванович Создание, обслуживание и администрирование сетей на 100%

Введение

Компьютер уже давно стал неотъемлемой частью жизни людей. Он помогает решать множество вопросов. Практически в любой отрасли деятельности человека используются компьютеры. Образовательные программы, медицинское обслуживание, промышленные процессы – везде применяются компьютеры. На сегодня компьютеризация достигла такого уровня, что обойтись без них никак нельзя.

Отдельная эра в истории развития компьютеров началась с появлением локальных сетей, которые позволяют объединять компьютеры между собой. Именно локальная сеть подняла функциональность компьютера на невиданную до сих пор высоту. Даже один компьютер способен выполнять огромное количество операций, тем самым позволяя обрабатывать большое количество данных и выдавать требуемый результат. А представьте себе, что можно сделать с помощью тысячи компьютеров, объединенных в одну сеть! Это дает возможности для выполнения таких заданий, на решение которых раньше уходили годы и были задействованы тысячи людей. Даже если не «копать» так глубоко, преимущества использования локальных сетей очевидны: общее использование ресурсов, баз данных, общение, Интернет и многое другое.

Сегодня существует большое количество способов объединения компьютеров в локальную сеть. Разного размера проводные и беспроводные локальные сети сотнями появляются каждый день. При этом если большие корпоративные сети требуют соответствующих знаний и уровня подготовки для их создания, то небольшие офисные и тем более домашние сети могут создавать простые пользователи. Главное при этом – достаточный уровень знаний и желание добиться результата.

Что касается желания, то это зависит только от вас. А вот в первом вопросе вам поможет книга, которую вы держите в руках. В ней собрано все необходимое для того, чтобы изучить принцип функционирования сетей и применить эти знания на практике. Дело остается только за малым: требуется ваше желание.

От издательства

Ваши замечания, предложения, вопросы отправляйте по адресу электронной почты gromakovski@minsk.piter.com (издательство «Питер», компьютерная редакция).

На веб-сайте издательства http://www.piter.com вы найдете подробную информацию о наших книгах.

Часть 1
Теоретические сведения о сетях

○ Основные типы сетей
○ Топология и режимы работы сети
○ Модель ISO/OSI
○ Протоколы передачи данных
○ Среда передачи данных
○ Методы доступа к передающей среде
○ Понятие сетевого стандарта
○ Особенности функционирования беспроводных сетей
○ Стандарты IEEE 802.3
○ Стандарты IEEE802.11
○ Спецификации Bluetooth
○ Спецификации HomePNA
○ Спецификации HomePlug
○ Механизмы и особенности управления сетью
○ Сетевое оборудование

Глава 1
Основные типы сетей

□ Одноранговая сеть
□ Сеть на основе сервера

Появление компьютерных сетей было логичным шагом в истории компьютеризации общества. Благодаря этому шагу компьютеры получили еще большее распространение, а самое главное – практически в каждый дом пришел Интернет, предоставляющий доступ к практически неограниченным источникам информации.

Компьютерные сети прошли долгий этап развития. В результате на сегодня компьютеры можно объединить как в локальном, так и в глобальном масштабе.

Итак, существует два варианта сетей – локальные и глобальные. Принцип объединения в них компьютеров и работы в этих сетях практически идентичен, но масштабы сети накладывают свои ограничения и требования.

Локальная сеть, LAN (Local Area Networks) – сеть, с помощью которой компьютеры объединяются на ограниченной территории. Такой вариант сети встречается в офисах, на предприятиях, в залах ожидания аэропортов, вокзалов, в кафе, ресторанах и т. д. Главное ее предназначение – организация доступа к общим ресурсам внутри сети. При этом локальная сеть часто имеет подключение к Интернету, что делает ее частью глобальной сети.

Глобальная сеть, WAN (Wide Area Networks) – разновидность сети, которая, согласно существующим легендам, образовалась из локальной сети достаточно больших масштабов. В результате появилась Всемирная паутина, она же Интернет.

Наиболее важным понятием, характеризующим сеть, является ее тип. Именно от типа сети зависят ее возможности, безопасность, управляемость и, самое главное, – доступ к важным данным.

Различают два типа сетей – одноранговую и сеть на основе сервера. Сети обеих разновидностей выполняют поставленные перед ними задачи, но делают это по-разному, в чем вы сможете убедиться далее.

Одноранговая сеть

Одноранговая сеть (рис. 1.1) является наиболее простой и дешевой в создании. Тем не менее она способна обеспечить своих пользователей всем необходимым для получения доступа к нужной информации, в том числе и к Интернету.

Главной особенностью такой сети является то, что каждый участник сети – рабочая станция – имеет одинаковые права и выступает в роли администратора своего компьютера. Это означает, что только он может контролировать доступ к своему компьютеру и только он может создавать общие ресурсы и определять правила доступа к ним. С одной стороны, это делает сеть очень простой в создании, но с другой – администрирование такой сети вызывает достаточно много проблем, особенно если количество участников сети превышает 25–30.

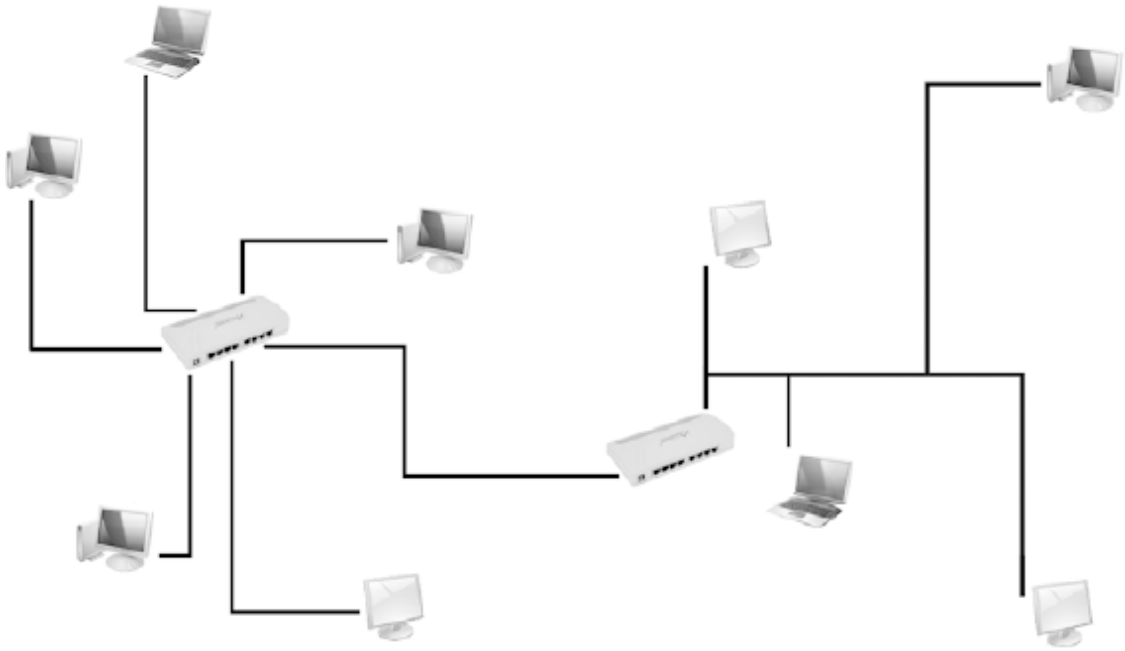

Рис. 1.1. Пример одноранговой сети

Одноранговые сети находят свое применение в небольших офисах, ресторанах и кафе, залах ожидания, то есть в тех местах, которые позволяют поддерживать работу сети с небольшим количеством подключений. Однако, хотя это и противоречит всем принципам, одноранговые сети также используются в так называемых домашних сетях, количество подключений к которым может быть очень большим, например 1000 и более компьютеров. Главное объяснение этому факту – хаотичный способ создания сети, который к тому же, как правило, не требует больших финансовых вложений.

Одноранговая сеть является крайне неуправляемой с точки зрения системного администратора, и чем больше участников сети, тем более этот факт заметен. Например, чтобы ограничить работу пользователя с теми или иными устройствами, потребуется выполнить определенные настройки операционной системы. Сделать это централизованно невозможно, поэтому требуется личное присутствие администратора возле каждого компьютера либо применение программ удаленного управления компьютером. Это же касается обновления антивирусных баз, установки обновлений операционной системы и офисных программ и т. д.

Учитывая изложенные факты, а также практику работы одноранговых сетей, ее использование можно считать оправданным только в случае, если количество узлов сети достаточно мало и все они расположены на небольшой территории, например в пределах одного или нескольких офисов.

Поддержка одноранговых сетей имеется в любой современной операционной системе семейства Microsoft Windows. По этой причине для организации такой сети никакого дополнительного программного обеспечения не требуется.

Внимание

В одноранговой сети доступ к общему ресурсу одновременно могут получить только 10 участников сети. Если для вас важен этот момент, то вам следует установить серверную операционную систему.

В табл. 1.1 приведены основные преимущества и недостатки одноранговой сети, на которые обязательно стоит обратить внимание, прежде чем выбрать тип будущей локальной сети.

Таблица 1.1. Особенности одноранговых сетей

Преимущества сети	Недостатки сети
Простая и дешевая в создании	Отсутствует централизованное хранилище 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 антивирусных баз (и другого программного обеспечения) отвечает пользователь
	Низкий уровень защиты информации

Сеть на основе сервера

Сеть на основе сервера (рис. 1.2), или, как ее еще часто называют, сеть типа «клиент – сервер», – наиболее востребованный тип сети, основными показателями которой являются высокие скорость передачи данных и 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 никакие другие задачи выполнять на нем не следует. Этот сервер называется *контроллер домена*. Он является наиболее важным объектом сети, поскольку от него зависит работоспособность всей сети. Именно поэтому данный сервер обязательно подключают к системе бесперебойного питания. Кроме того, в сети, как правило, присутствует дублирующей сервер, который называется вторичный контроллер домена.

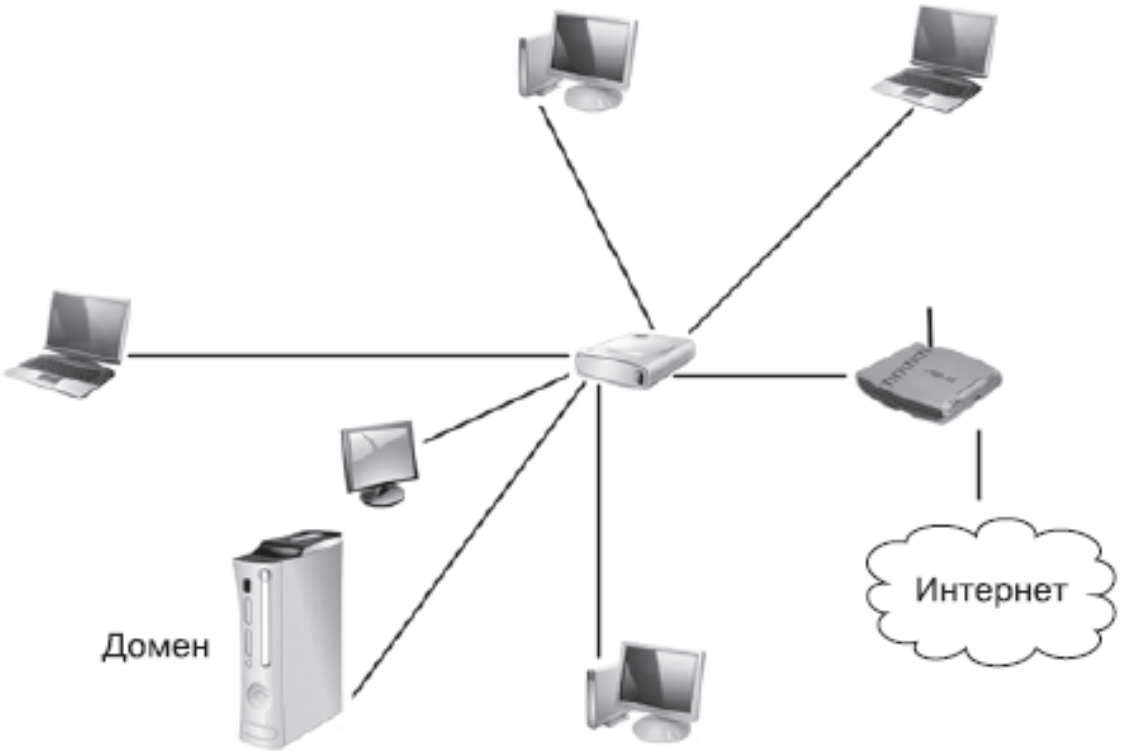

Рис. 1.2. Пример сети с управляющим сервером

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 файловые ресурсы, аудио– и видеофайлы и многое другое. Главное требование к файловому серверу – надежная дисковая подсистема, которая может обеспечивать 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 пользователей в случае непредвиденных сбоев оборудования.

□ **Сервер базы данных.** Серверы подобного типа наиболее востребованы, поскольку позволяют обеспечить доступ к единой базе данных. В качестве таковой могут выступать базы данных бухгалтерского и другого типа учета, юридическо-правовые 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 важным является факт организации архивирования 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 выполнение программ, требующих обмен с базой данных, происходит максимально быстро и эффективно. Кроме того, за счет такой организации повышается безопасность доступа к данным и увеличивается управляемость процессом, поскольку легче контролировать работу одного компьютера, нежели сотни.

□ **Принт-сервер.** Специальный сервер, позволяющий сделать процесс печати более контролируемым и быстрым. Используется в сетях, которым необходим доступ к общему принтеру. Сервер подобного рода обеспечивает управление очередью печати и доступ к принтеру для клиентов любого типа: при проводном или беспроводном соединении, для переносного устройства или мобильного телефона.

□ **Интернет-шлюз.** Данный сервер позволяет предоставить пользователям локальной сети доступ в Интернет, а также организовать доступ к ресурсам по протоколам FTP и HTTP. Поскольку данный сервер является «окном» во внешнюю сеть, к нему предъявляются определенные требования, среди которых основными являются требования к безопасности локальных данных и защита от доступа к ним извне. Именно поэтому на таком сервере устанавливают различные сетевые фильтры и брандмауэры, позволяющие эффективно фильтровать входящий и исходящий трафик, что делает использование Интернета более безопасным.

□ **Почтовый сервер.** Практически каждое серьезное предприятие, применяющее для организации обмена данными сеть на основе сервера, 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. Подобную систему обмена информацией позволяет реализовать почтовый сервер с соответствующим программным обеспечением. На этот сервер дополнительно устанавливаются разнообразные антиспамовые фильтры, позволяющие бороться (насколько это возможно) со все возрастающим объемом рекламных писем, которые и называются *спамом.*

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

С точки зрения системного администратора, сеть на основе сервера хотя и наиболее сложная в создании и обслуживании, но в то же время наиболее управляемая и контролируемая. Благодаря наличию главного компьютера управление учетными записями пользователей происходит очень легко и, самое главное, – эффективно. Благодаря политикам безопасности также упрощается контроль над самими компьютерами, что делает сеть более управляемой, а данные в ней более защищенными.

На сервер устанавливается серверная операционная система, которая, в отличие от обычной операционной системы, обладает некоторыми преимуществами, например поддержкой нескольких процессоров, б**о**льшего объема оперативной памяти, инструментами администрирования сети и т. д. К таким операционным системам относятся Windows Server 2003, Windows Server 2008 и т. д.

В табл. 1.2 показаны основные недостатки и преимущества сетей на основе выделенного сервера.

Таблица 1.2. Особенности сетей на основе выделенного сервера

Преимущества сети	**Недостатки сети**
Высокая скорость и производительность сети	Дорогая в создании и обслуживании
Использование выделенных серверов, что облегчает работу с ресурсами и упрощает контроль за их использованием	Постоянная необходимость в системном администраторе
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	

От выбора типа сети зависит ее будущее: расширяемость, возможность использования того или иного программного обеспечения и оборудования, надежность сети и многое другое. В этом плане сеть на основе сервера является наиболее предпочтительной и выгодной.

Глава 2
Топология и режимы работы сети

□ Топология «шина»
□ Топология «кольцо»
□ Топология «звезда»

При проектировании и создании сети важное значение имеет способ объединения компьютеров и участников сети. От этого зависит скорость передачи данных, надежность сети, степень устойчивости к поломкам, возможности администрирования и многое другое. Поэтому первым и, пожалуй, самым важным правилом, от которого зависят упомянутые показатели, является топология сети.

Таким образом, *топология сети*, или *сетевая топология*, – это описание схемы сети, включающее в себя способ взаимного расположения компьютеров и их объединения. Кроме того, это описание содержит множество правил, связанных с прокладкой кабеля, подключением оборудования, взаимодействием управляющих устройств и т. д.

Различают сетевую топологию четырех видов: физическую, логическую, информационную и топологию управления обменом. Однако чаще всего понятие сетевой топологии ассоциируется именно с расположением компьютеров относительно друг друга, то есть с физической топологией.

Существует достаточно много способов объединения компьютеров, то есть сетевых топологий. К их числу относятся топологии «шина», «звезда», «кольцо», «двойное кольцо», «дерево», «решетка» и др. Наибольшее распространение получили сетевые топологии «шина», «звезда» и «кольцо», поэтому рассмотрим их подробнее.

Топология «шина»

Согласно топологии «шина», или, как ее еще часто называют, «общая шина», или «магистраль», все участники сети подключаются к центральному кабелю (рис. 2.1).

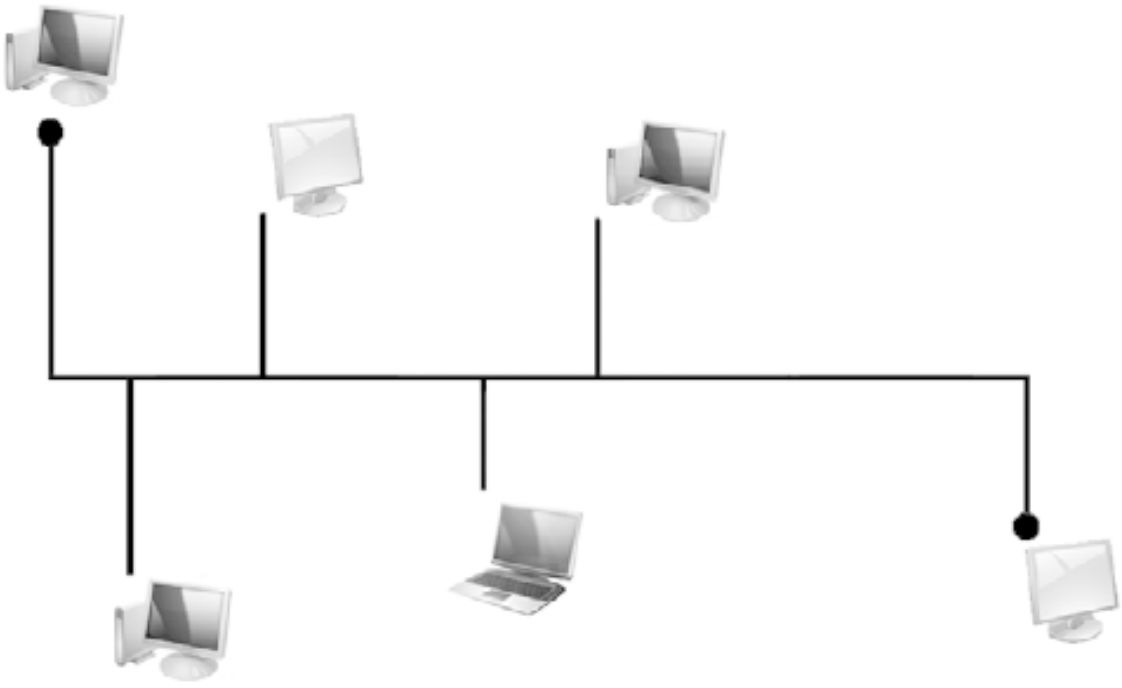

Рис. 2.1. Пример топологии «шина»

Для предотвращения дальнейшего распространения и возможного отражения сигнала на концах кабеля устанавливаются специальные заглушки – терминаторы, один из которых обязательно заземляется.

Данные в такой сети направляются сразу всем компьютерам, поэтому задача каждого компьютера – проверить, кому 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.

Главное преимущество такой сети – простота и дешевизна создания. При ее построении используется минимальное количество кабеля и не требуется никакого управляющего оборудования: в обмене данными участвуют только сетевые адаптеры компьютеров. 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 – сильная зависимость скорости передачи данных от количества подключенных компьютеров: чем больше компьютеров и других устройств, тем ниже скорость передачи данных. Кроме того, обрыв центрального кабеля парализует работу всей сети.

Топология «кольцо»

Согласно топологии «кольцо» все компьютеры сети подключены последовательно и образуют своего рода замкнутую кольцевую систему (рис. 2.2).

Для передачи данных в сети используется маркерная система, то есть данные в конкретный момент может передавать только один компьютер. Причем 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, к маркеру добавляется адрес компьютера, которому эти данные предназначены, и маркерный блок отправляется в сеть по кругу. Таким образом, каждый компьютер, который лежит на пути следования маркерного блока, считывает из него адрес получателя и сравнивает его со своим адресом: если адреса не совпадают, они отправляются далее по кругу. Если адреса совпали, то есть отправитель найден, формируется подтверждающий блок и передается далее по кругу к отправителю. В дальнейшем данные уже передаются по найденному пути до тех пор, пока в этом есть необходимость. Как только передача данных заканчивается, маркер освобождается и идет далее по кругу до первого компьютера, которому необходимо передавать данные.

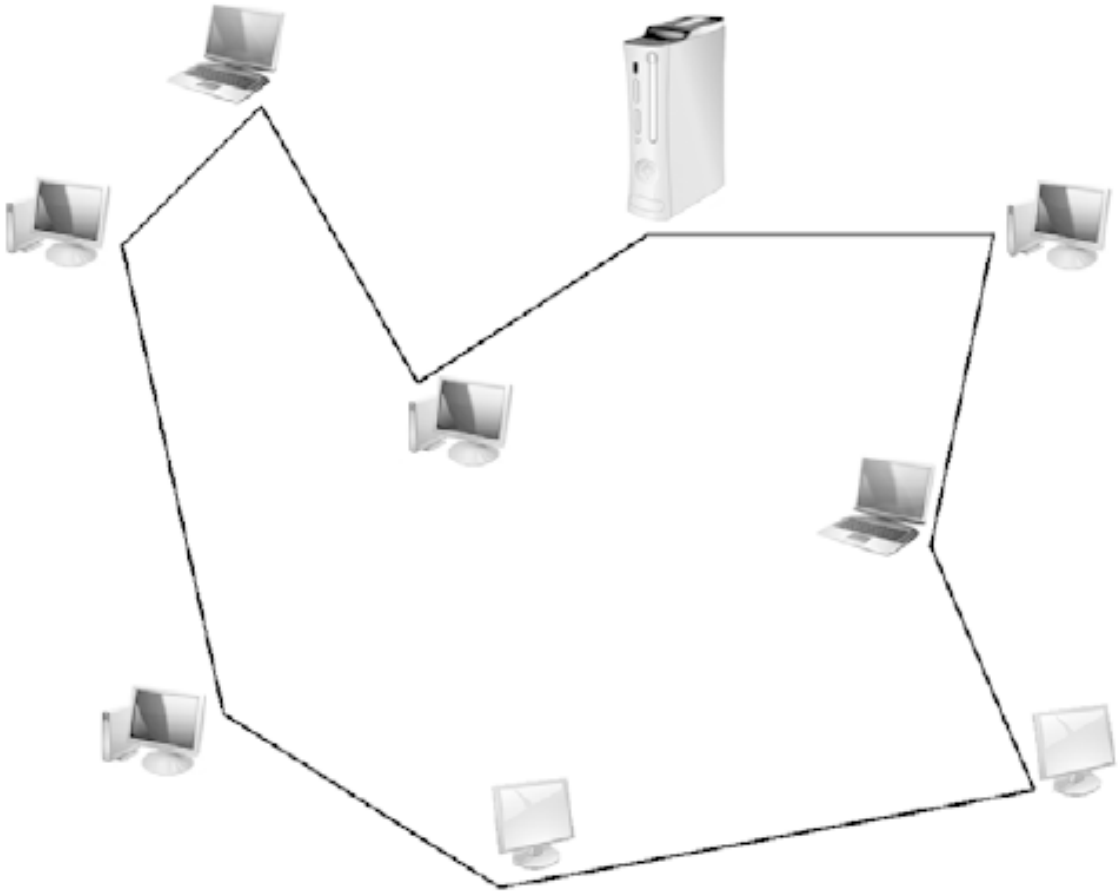

Рис. 2.2. Пример топологии «кольцо»

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

У данного типа сети есть также и недостатки. Так, подключение нового компьютера требует остановки работы всей сети. Аналогичная ситуация происходит, если один из компьютеров выходит из строя: сеть становится неработоспособной. Кроме того, поиск неисправности в такой сети сопряжен со множеством сложностей.

Топология «звезда»

Топология «звезда» на сегодня является наиболее распространенной. Согласно ей каждый компьютер или устройство сети подключается к центральному узлу, образуя подобным образом один сегмент сети (рис. 2.3).

Сегменты сети могут соединяться между собой одним из доступных способов, например посредством центрального либо промежуточного узла, образуя более сложную сеть или входя в состав комбинированной сети.

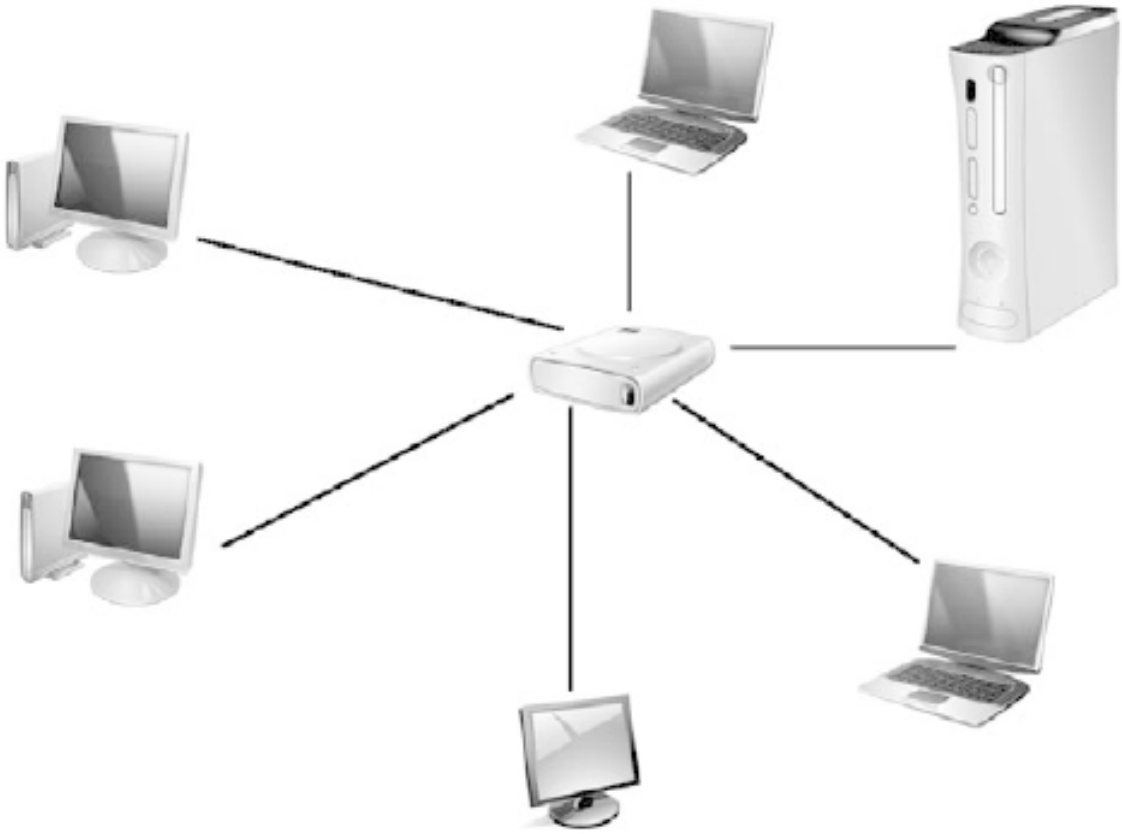

Рис. 2.3. Пример топологии «звезда»

В качестве центрального узла используется любое активное сетевое устройство с достаточным количеством портов. В самом простом случае в роли центрального узла выступает концентратор, который в силу своих ограничений позволяет передавать данные в конкретный момент только одному компьютеру. При этом поступившие на концентратор данные он сразу пересылает всем подключенным к нему устройствам. Если на концентратор в один момент поступают данные от двух разных отправителей, то оба пакета игнорируются.

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

Несмотря на то что «звезда» наиболее дорогостоящая в использовании по сравнению с другими топологиями, благодаря своей надежности и высокой скорости передачи данных она уже практически стала стандартом. Большую роль играет также тот факт, что принятый уже достаточно давно стандарт ATX подразумевает наличие на материнской плате персонального компьютера интегрированного сетевого адаптера, который изначально предназначен для работы с этой топологией.

Глава 3
Модель ISO/OSI

Функционирование сети подчиняется определенным теоретическим правилам. В качестве такой теоретической основы выступает 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 Standards Organization, 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 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 представляет собой среду передачи данных. Если же данные принимаются, то они проходят путь от физического до прикладного уровня (рис. 3.1).

Рис. 3.1. Схематическое отображение модели ISO/OSI

Описанная модель является стандартом для любой среды передачи данных, которых на сегодня используется три: кабель, радиоволны и инфракрасное излучение. Однако, в зависимости от 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, а также обойти вопрос совместимости оборудования, которое используется для этого.

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 существующему каналу связи получателю, а также прием данных от отправителя и их конвертация согласно существующим таблицам кодирования сигналов.

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 позволяет сосредоточиться только на процессе передачи и приема данных.

Канальный уровень

Задача канального уровня (Data Link Layer) – обеспечение гарантированной передачи 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.

Что касается локальных сетей, то за работу канального уровня 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 фреймов и т. д.

Уровень LLC имеет 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 умеет передавать данные либо с помощью датаграмм, либо с использованием процедур с обеспечением качества передачи.

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 (Network Layer) – один из важнейших уровней модели взаимодействия открытых систем. Поскольку для построения сети могут использоваться различные технологии и, а сеть может состоять из нескольких сегментов с абсолютно разными сетевыми топологиями, чтобы «подружить» эти сегменты, требуется соответствующий 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 выполняет 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 определять 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 подготовленный канал связи. При этом отсле-

живается 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 доставки данных и их целостность.

На транспортном уровне предусмотрено пять классов сервиса с различными уровнями надежности. Они различаются скоростью, возможностями восстановления данных и т. д. Например, некоторые классы работают без предварительной установки связи и не гарантируют доставку пакетов в правильной последовательности. В этом случае за выбор маршрута отвечают промежуточные устройства, которые попадают 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, контролирующие данный процесс.

Для управления сеансом применяется маркер, обладатель которого гарантирует себе право на связь. Кроме того, используются служебные сообщения, с помощью которых стороны могут, например, договариваться о способе передаче 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 или нижестоящему уровню. С его помощью обеспечивается совместимость компьютерных систем, использующих разные способы представления данных.

Этот уровень удобен тем, что именно здесь 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 обеспечивает связь пользовательских приложений с сетевыми сервисами и службами на всех уровнях модели ISO/OSI, а также передачу служебной информации, синхронизирует взаимодействие прикладных процессов и т. д.

Глава 4
Протоколы передачи данных

□ Понятие протокола
□ Основные протоколы

Понятие протокола

В предыдущей главе мы познакомились с эталонной моделью, описывающей принцип подготовки, приема и передачи данных через любой имеющийся канал связи. Каждый из ее семи уровней решает поставленную перед ним задачу, выполняя свою функцию в подготовке или обработке данных. Для этого он использует стандартные процедуры межуровневого обмена информацией и протоколы передачи данных. Таким образом, получается, что модель ISO/OSI является теоретической основой функционирования сети, а сетевые протоколы – это то, что превращает теорию в практику.

Протокол передачи данных можно сравнить с набором правил и соглашений, которые описывают способ передачи данных между двумя и более объектами в сети.

Для обслуживания модели взаимодействия открытых систем используется достаточно большое количество сетевых протоколов. Многие из них вполне специфичны и часто выполняют только одно определенное действие, но делают это быстро и, самое главное, правильно. Существую также и более продвинутые и функциональные протоколы, которые могут выполнять определенные действия, захватывая сразу несколько 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 довольно много недостатков В частности, наиболее слабым звеном в модели стал транспортный уровень По этой причине существует достаточно много протоколов, которые выполняют работу сразу нескольких уровней, что идет вразрез с самой моделью 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. Этот факт позволяет создавать любое количество протоколов разного применения, делая их настолько гибкими, как того требует современная ситуация.

В табл. 4.1 приведены названия некоторых популярных протоколов и их положение в модели взаимодействия открытых систем.

Таблица 4.1. 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
Сетевой	IPX, IP, ARP, ICMP, DDP
Транспортный	TCP, UDP, SPX, RTCP, RDP, RUDP
Сеансовый	RPC, SSL, WSP
Уровень представления данных	Telnet, FTP, SMTP, SNMP, TDI, XDR, NCP
Прикладной	HTTP, FTP, DHCP, DNS, POP3, SNMP, LDAP, Gopher

Основные протоколы

Как вы уже могли заметить, количество протоколов, обслуживающих модель взаимодействия открытых систем, достаточно велико. Некоторые из этих протоколов, особенно низкоуровневые, не представляют особого интереса в плане знакомства с их принципом работы. Но принцип работы и возможности других протоколов все же стоит знать, особенно таких, как TCP/IP, UDP, POP3 и др.

Стеки протоколов

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

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

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

Плюсом использования стеков протоколов является то, что протоколы, работающие на нижних уровнях, применяют давно отлаженные и популярные сетевые протоколы, такие как Ethernet, FDDI и т д. Благодаря аппаратной реализации этих протоколов становится возможным 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, и очень часто случается 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, и если при попытке установления связи с адресатом с помощью первого стека произошла ошибка, автоматически происходит переключение на использование протокола из следующего стека. В этом случае важным моментом является очередность привязки, поскольку она однозначно 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 «один к нескольким», так и «несколько к одному», то есть один стек протоколов можно привязать сразу к нескольким адаптерам или несколько стеков к одному адаптеру.

TCP/IP

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

Протокол был создан в 70-х годах прошлого века управлением Министерства обороны США. Именно с его подачи началась разработка протокола, целью которого было соединение любых двух компьютеров, как бы далеко они ни находились. Конечно, они преследовали свою цель – обеспечить постоянную связь с центром управления, даже если все вокруг будет разрушено в результате военных действий. В итоге 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 протокола TCP/IP возросла.

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

TCP (Transmission Control Protocol) – транспортный протокол, предназначенный для управлением передачей данных в сетях, использующих стек протоколов 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 фрагментации пакетов данные, несмотря на качество канала связи, в любом случае доходят до адресата. Кроме того, благодаря наличию IP-протокола становится возможной передача данных между разнородными сегментами сети.

Недостатком TCP/IP-протокола является сложность администрирования сети. Так, для нормального функционирования сети требуется наличие дополнительных серверов, например DNS, DHCP и т. д., поддержание работы которых и занимает большую часть времени системного администратора.

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 до недавнего времени 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 небольшого размера, поэтому в больших сетях его использование малоэффективно: излишнее использование широковещательного вещания на низкоскоростных линиях связи недопустимо.

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 другие, 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.

Чтобы обмен между компьютерами был возможен, каждый из них должен обладать логическим именем.

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 адресатам.

Главные плюсы протокола NetBEUI – скорость работы и очень малые требования к ресурсам. Если требуется организовать быстрый обмен данными в небольшой сети, состоящей из одного сегмента, лучшего протокола для этого не найти. Кроме того, для доставки сообщений установленное соединение не является обязательным требованием: 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 самых высоких 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 был усовершенствован (вышло три его версии), что позволило применять его даже в таких современных операционных системах, как Microsoft Vista и Windows 7. Протокол SMB универсален и может работать в паре практически с любым транспортным протоколом, например TCP/IP и SPX.

HTTP

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

Протокол HTTP (HyperText Transfer Protocol) разрабатывался специально для Интернета: для получения и передачи данных по Интернету. Он работает по технологии «клиент –

сервер», которая подразумевает, что есть клиенты, запрашивающие информацию (например, просмотр содержимого веб-страницы), и серверная часть, которая обрабатывает эти запросы и отсылает ответ.

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 динамичные изображения, возможностей протокола стало не хватать и он постепенно начал изменяться.

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 ухудшает восприятие информации. Кроме того, протокол полностью лишен каких-либо механизмов сохранения состояния, что делает невозможной навигацию по веб-страницам посредством одного лишь HTTP-протокола. По этой причине вместе с HTTP-протоколом используются сторонние протоколы либо пользователю необходимо работать с браузером, обрабатывающим HTTP-запросы.

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 с/на FTP-сервер.

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 – передачи команд. Кроме того, порты могут быть динамическими.

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 позволяет перехватить начальный трафик и определить с его помощью имя пользователя, а также его пароль подключения к FTP-серверу. Чтобы избежать подобной ситуации, 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 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. Авторизации 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 сообщения 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 применяется 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 порта.

IMAP

IMAP (Interactive Mail Access Protocol) – еще один почтовый протокол, созданный на основе протокола POP3. Он был разработан позже протокола POP3. В результате в нем были учтены все недостатки и добавлено большое количество новых востребованных функций.

Наиболее полезными 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. Эти каналы не всегда быстрые и незагруженные, поэтому наличие такой функции существенно облегчает жизнь пользователя. Имеется также возможность передачи сообщений по небольшим частям, что очень полезно, 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 организа-

циях, 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 выполняет эти функции, так как обладает дополнительными возможностями. Кроме того, в отличие от SLIP, PPP может взаимодействовать не только с TCP/IP, но и с IPX/SPX, NetBIOS, DHCP, которые широко используются в локальных сетях.

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

X.25

Протокол X.25, который был создан в 1976 году и усовершенствован в 1984 году, работает на физическом, канальном и сетевом уровнях модели взаимодействия ISO/OSI. Его разработкой занимался консорциум, состоящий из представителей многих телефонных компаний, и создавали его специально для использования на существующих телефонных линиях.

Когда разрабатывался X.25, цифровая телефонная линия была редкостью – использовалась в основном аналоговая. По этой причине в нем присутствует система обнаружения и коррекции ошибок, что существенно повышает надежность связи. В то же время эта система замедляет скорость передачи данных (максимальная – 64 Кбит/с). Однако этот факт не мешает использовать его там, где прежде всего требуется высокая надежность, например в банковской системе.

Frame Relay

Frame Relay – еще один протокол, предназначенный для передачи данных по телефонной линии. Помимо высокой надежности (как у X.25), он обладает дополнительными полезными нововведениями. Поскольку передаваемые данные могут иметь формат видео, аудио или содержать электронную информацию, есть возможность выбирать приоритет передаваемого содержимого.

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

AppleTalk

Протокол 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 протокола 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 маошрутизаторов, 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 5
Среда передачи данных

□ Коаксиальный кабель
□ Кабель «витая пара»
□ Оптоволоконный кабель
□ Телефонная проводка
□ Электропроводка
□ Радиоволны
□ Инфракрасное излучение

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;
□ администрирование сети;
□ возможность модернизации.

Этот список можно продолжать долго, 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. Поскольку скорости тогда были не столь высоки, как сегодня, 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 приемлемой скоростью.

Различаются тонкий и толстый коаксиальный 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 вследствие дальнейшего усовершенствования существующих сетевых стандартов.

Толстый и тонкий кабели внешне различаются толщиной. Однако иногда могут быть и другие различия (рис. 5.1).

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

Рис. 5.1. Разные варианты коаксиального кабеля

Основные различия между этими типами кабелей заключаются в их составе: могут присутствовать дополнительные оплетки, диэлектрики, экраны из фольги и т. д.

Типичное строение самой простой реализации тонкого и толстого коаксиального кабеля показано на рис. 5.2 и 5.3.

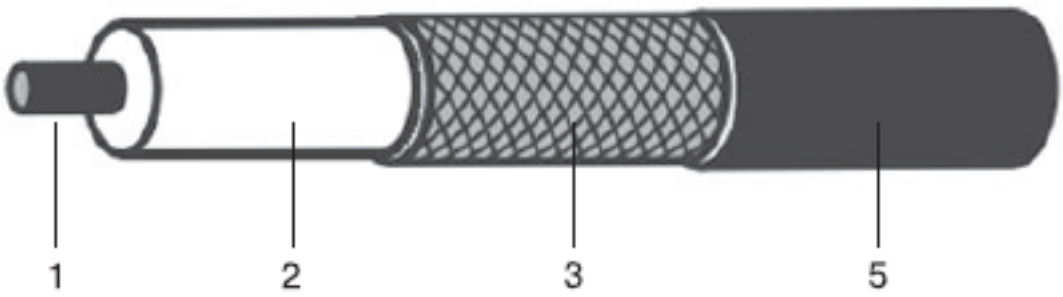

Рис. 5.2. Строение тонкого коаксиального кабеля

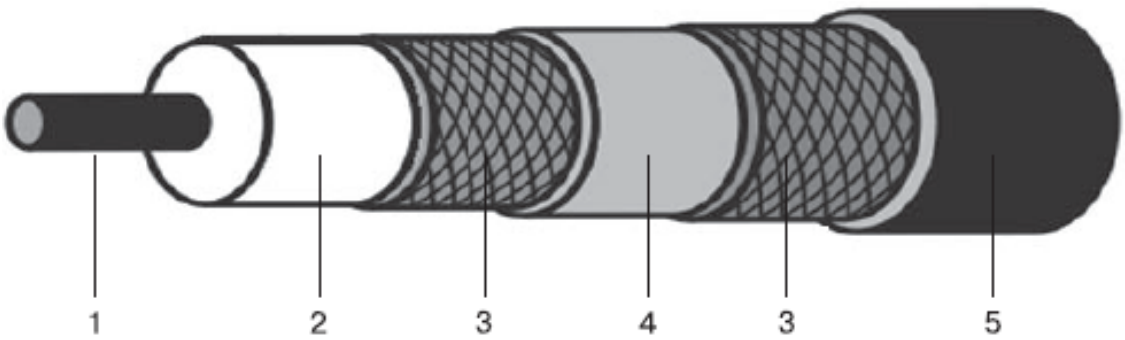

Рис. 5.3. Строение толстого коаксиального кабеля

Рассмотрим элементы коаксиального кабеля, отмеченные на рисунках цифрами.

1. Центральный проводник (Center Conductor). Представляет собой металлический стержень, цельный или состоящий из нескольких проводников. В качестве металла, как пра-

вило, 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, которые используются 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 определенными 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 RG[1]-8, 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. Если требуется увеличить диаметр сети, то используется толстый коаксиальный кабель. Иногда тонкий и толстый кабели применяются одновременно: тонким кабелем соединяют близкорасположенные компьютеры, а толстым – компьютеры на большом удалении или два сегмента сети.

Кабель «витая пара»

На сегодня кабель «витая пара» (Twisted Pair) получил наибольшее распространение. В первую очередь это произошло благодаря его 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 возможностях ее модернизации и скорости передачи данных.

Свое название он получил благодаря особенности внутреннего исполнения. Так, внутри кабеля может находиться от одной до двадцати пяти пар проводников, скрученных между собой и имеющих определенный цвет.

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. 5.4).

[1] RG (от англ. Radio Grade) – волновод.

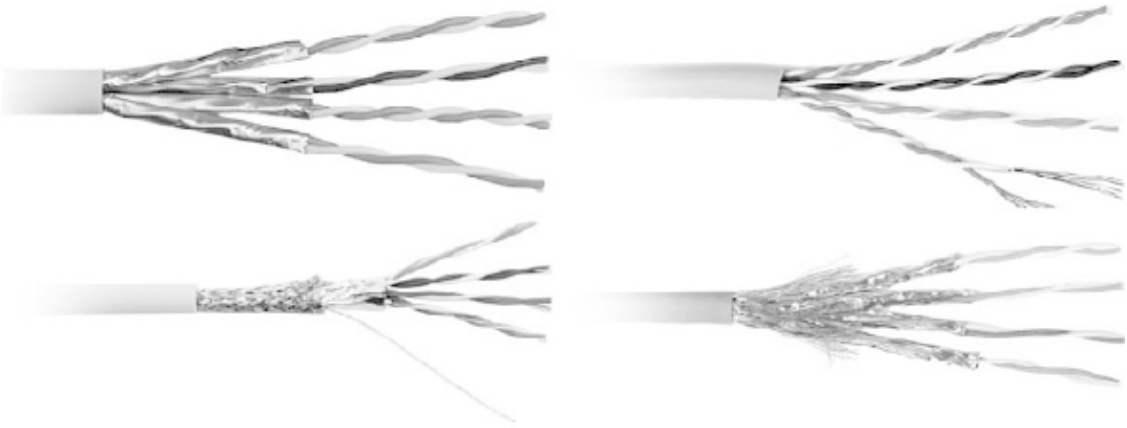

Рис. 5.4. Внешний вид некоторых вариантов кабеля «витая пара»

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, эканированная 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. Так, 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 начиная с шестой категории делает возможной передачу данных на скорости 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, однако при этом скорость передачи данных 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). Именно оптоволоконный кабель благодаря своим характеристикам 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 оптоволокна. Существует два варианты оптоволокна, которые однозначно влияют на характеристики кабеля. Так, различают одномодовое (SM, Single Mode) и многомодовое, или мультимодовое (MM, Multi Mode), волокно.

Упрощенная схема оптоволоконного кабеля показана на рис. 5.5.

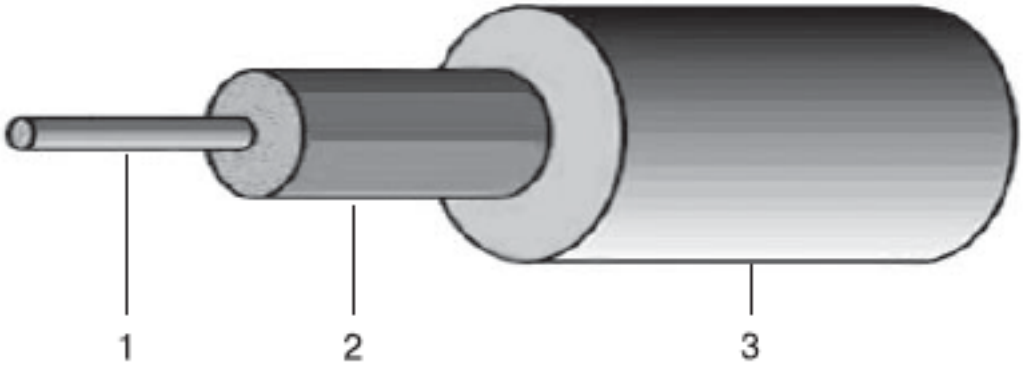

Рис. 5.5. Строение оптоволоконного кабеля

Основная деталь оптоволоконного кабеля – оптоволокно или, как его еще называют, световод (*1*), по которому непосредственно передается световой сигнал. Чтобы сигнал не уходил из световода, вокруг последнего располагается отражающая оболочка (*2*) толщиной 125 мкм. И еще один элемент – оболочка (*3*), которая защищает кабель от внешнего воздействия, 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, большое распространение получили кабели с несколькими световодами, что позволяет значительно увеличить пропускную способность кабеля.

Преимущества и недостатки одномодового и многомодового оптоволокна понять достаточно просто. Так, по световоду передаются световые сигналы с длиной волны в диапазоне 0,85–1,3 мкм. Многомодовое волокно, в зависимости от типа стандарта, 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. 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 существующая практика: скорость передачи сигнала в простейшем одномодовом кабеле может достигать 2,5 Гбит/с при длине сегмента 20 и более километров.

Распространение оптоволоконного кабеля сдерживают несколько факторов, основными из которых является 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, к другому компьютеру или к Интернету. Для этого существует достаточно большое количество соответствующих протоколов и технологий: 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 заведомо существующего канала связи, возможность развертывания сети там, где другой способ связи по разным причинам невозможен.

Существующее подключение к телефонной линии 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 этого 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, как десять лет назад появилась организация HomePlug Powerline Alliance. Ее стараниями на свет появился первый стандарт HomePlug, который 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 реальный выход из ситуации.

Из плюсов использования электрического кабеля в качестве среды передачи данных можно отметить то, что 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 нашу планету!

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 задачей.

Любая технология передачи данных использует определенный диапазон радиочастот, который принят в качестве стандарта. Существуют даже соответствующие 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, а именно – мобильностью клиентов: никакая другая среда передачи данных не может

похвастаться такими возможностями. С другой стороны, беспроводные сети более чувствительны к разного рода препятствиям и помехам распространению сигнала, что часто становится серьезным препятствием в их использовании.

Применение «радиоэфира» достаточно часто практикуется для подключения компьютеров к «домашней» локальной сети. Существуют даже такие «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 именно беспроводные точки доступа, очень чувствительны к грозам и молниям. Очень часто эти явления становятся причиной выхода из строя оборудования, даже несмотря на наличие грозозащиты. Именно поэтому зачастую все же выбирают проводное соединение компьютеров, пусть даже и более дорогое.

Инфракрасное излучение

Использование инфракрасного излучения в качестве среды передачи данных практикуется уже достаточно давно. Эту среду можно сравнить с радиоволнами, 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 расположенных рядом компьютеров или компьютера с периферией.

Глава 6
Методы доступа к передающей среде

□ Ethernet
□ Token Ring

Как вы уже знаете, для передачи данных по сети используется множество протоколов, работающих на разных уровнях модели ISO/OSI. Чтобы они могли сделать свою работу качественно, процесс передачи данных должен пройти гладко и без ошибок.

Поскольку используются разные технологии построения сетей, например различные сетевые топологии, принцип передачи данных между ними неодинаков. Однако это никак не должно волновать отправителя и получателя информации. Чтобы исключить разнообразные коллизии, когда сразу несколько компьютеров пытаются передавать данные, используются специальные протоколы канального уровня, которые организуют доступ к передающей среде, предварительно исследовав ее и захватив нужный ресурс.

Как мы уже говорили выше, за работу канального уровня отвечают два подуровня – LLC и MAC. Первый из них служит для управления логическим каналом, а второй – для управления доступом к общей среде передачи данных. Именно второй уровень, то есть MAC, представляет наибольший интерес, и именно на нем работают некоторые протоколы, которые предоставляют доступ к разделяемой среде, то есть каналу связи. А уже после того как доступ к передающей среде получен, за работу принимается более высокий уровень, то есть LLC, и начинается передача данных.

Наибольшую популярность в локальных сетях получили два метода доступа к разделяемой среде – Ethernet и Token Ring. Первый из них используется в сетях с применением топологий «шина» и «звезда», а второй – в сетях, построенных по топологии «кольцо».

Ethernet

Метод доступа Ethernet – получил свое распространение преимущественно в сетях стандартов IEEE 802.3. Этот метод имеет несколько модификаций, которые называются CSMA, CSMA/CD и CSMA/CA.

CSMA

Метод доступа к передающей среде CSMA (Carrier Sense Multiple Access) является первым из подобных методов. В данный момент используются его более совершенные модификации. Тем не менее подходы, применяемые в нем, используются и в последующих его модификациях.

Принцип работы метода CSMA достаточно простой и базируется на том, что, прежде чем начать передачу данных, в течение конкретного промежутка времени идет прослушивание канала. Если обнаружены шумы (синхронизирующий сигнал определенной частоты), то есть уже ведется передача данных другими объектами, процесс прослушивания повторяется по прошествии некоторого времени. Если никаких шумов не обнаружено, канал считается незанятым, и начинается передача пакетов с данными.

CSMA/CD

Метод доступа к передающей среде CSMA/CD (Carrier Sense Multiple Access with Collision Detection), или метод множественного доступа с контролем несущей частоты и

обнаружения коллизий, является улучшенной модификацией протокола CSMA. Этот метод используется во всех существующих сетях Ethernet, Fast Ethernet и Gigabit Ethernet, работа которых описана спецификацией IEEE 802.3.

При использовании метода CSMA часто происходит так, что, прослушав канал на наличие синхронизирующего сигнала и не обнаружив такового (то есть линия считается «чистой»), передачу данных могут произвести сразу несколько компьютеров, что, естественно, вызовет коллизии, и данные будут потеряны.

Согласно методу CSMA/CD, прослушивание линии происходит постоянно, при этом если передаваемые сигналы и наблюдаемые сигналы не совпадают, значит, кто-то еще делает попытку передачи данных. В этом случае, чтобы избежать коллизий и потери данных, передача данных временно прекращается, и отправитель отправляет в линию специальный сигнал jam (32-битная последовательность), который информирует все остальные компьютеры о том, что уже ведется передача данных и компьютерам запрещено осуществлять аналогичные действия. По истечении случайного промежутка времени происходит повторная попытка передачи данных. С каждой новой попыткой время ожидания увеличивается, но если после 16 последовательных попыток передача данных не будет возобновлена, фиксируется ошибка, говорящая о том, что канал передачи данных недоступен, и сообщение об этом поступает протоколу верхнего уровня.

Благодаря такому подходу передача данных происходит не только быстрее (не нужно повторно передавать весь объем), но и с большей гарантией того, что они будут доставлены, даже несмотря на то, что за качество доставки отвечает уровень LLC.

CSMA/CA

Метод доступа к передающей среде CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), или метод множественного доступа с контролем несущей частоты и избеганием коллизий, также является модификацией протокола CSMA. Данный метод доступа к среде чаще всего используется в беспроводных сетях, работа которых описана спецификацией IEEE 802.11.

В отличие от метода доступа к среде CSMA/CD, в которой jam-сигнал высылается только при обнаружении коллизии, метод CSMA/CA сначала отправляет jam-сигнал, информирующий о том, что станция хочет передавать данные, и только потом передает сигнал. После того как выслан jam-сигнал, станция еще некоторое время ожидает и проверяет канал на наличие аналогичных jam-пакетов. Если таковой обнаружен, то есть кто-то уже ведет вещание, станция ждет случайный промежуток времени, и затем процесс повторяется. Если никаких чужих передач не обнаружено, станция начинает передавать данные до тех пор, пока все они не будут переданы. При таком подходе, даже если будет обнаружен чужой jam-пакет, это приведет не к коллизии при передаче данных, а лишь к коллизии jam-пакетов.

Token Ring

Данный метод доступа к общей передающей среде характерен только для сетей, построенных с применением сетевой топологии «кольцо», представителями которых и являются Token Ring и FDDI.

В данном методе используется понятие маркера (Token) – метки специального типа, которая является одним из типов кадра, применяемых для обмена информацией в сетях подобного рода. При наличии маркера любой компьютер сети может передавать данные столько, сколько это будет необходимо, и при этом ему никто не помешает.

Организация сети по топологии «кольцо» подразумевает, что данные передаются по кругу всем участникам сети. При этом блок данных снабжается адресом отправителя, адресом получателя и маркером. Когда получатель, предварительно сверив адрес из блока данных со своим физическим адресом, понимает, что данный пакет адресован ему, он изменяет блок данных, убрав из него маркер. Этот факт и является свидетельством того, что передача данных уже ведется, и другие участники сети просто передают данные далее. После того как данные попали к отправителю, он начинает передачу данных по сформировавшемуся маршруту и ведет ее до тех пор, пока весь объем данных не будет передан. Затем получатель освобождает маркер, добавив его в последний пакет подтверждения доставки, и после этого любой участник сети может захватить его для своих нужд.

Глава 7
Понятие сетевого стандарта

Функционирование локальной сети обусловлено разнообразными стандартами, в частности моделью взаимодействия открытых систем. Кроме того, на основе модели ISO/OSI создано множество стандартов, которые ориентированы на передачу данных в локальной сети с достаточными по современным меркам скоростью и безопасностью.

На сегодня существует уже 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. Принимая во внимание современные требования и возможности, организации разрабатывают все необходимые правила, использование которых позволяет создать сеть с необходимыми возможностями. 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 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 процессы, которые возникают при передаче разного рода 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 занимается разработкой стандартов 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, большая 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, а в основе сети 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 занято стандартизацией функционирования локальных сетей (WiMAX) с использованием беспроводной связи в широком диапазоне частот (2-66 ГГц).

Глава 8
Особенности функционирования беспроводных сетей

□ Режимы функционирования беспроводных сетей
□ Методы и технологии обработки сигнала
□ Шифрование и аутентификация

Использование радиоволн в качестве среды передачи данных имеет целый ряд особенностей, не позволяющих применять методы и режимы работы, которые с успехом используются в проводных сетях. В связи с этим для существующих сетевых стандартов предусмотрены собственные средства доступа к передающей среде, обработки сигнала, шифрования данных и аутентификации и т. д. Далее рассмотрим особенности использования этих механизмов в беспроводных сетях, основанных на принципах Ethernet.

Режимы функционирования беспроводных сетей

Существует два режима или, как их еще называют, конфигурации работы беспроводного оборудования, которые были описаны 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») – один из режимов работы беспроводной локальной сети, причем самый простой из них. Это выражается в том, что для организации беспроводной сети не нужно никакого дополнительного оборудования, кроме беспроводных адаптеров, установленных на рабочих станциях. При этом каждый беспроводный адаптер сотрудничает сразу со всеми беспроводными адаптерами в сети (рис. 8.1).

Если провести аналогию с проводными сетями, то можно сказать, что данный режим очень похож на топологию «шина», когда данные от одного устройства отправляются сразу всем устройствам и сами устройства 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 настроить идентификатор сети, метод аутентификации и шифрования, ключ сети и т. д.

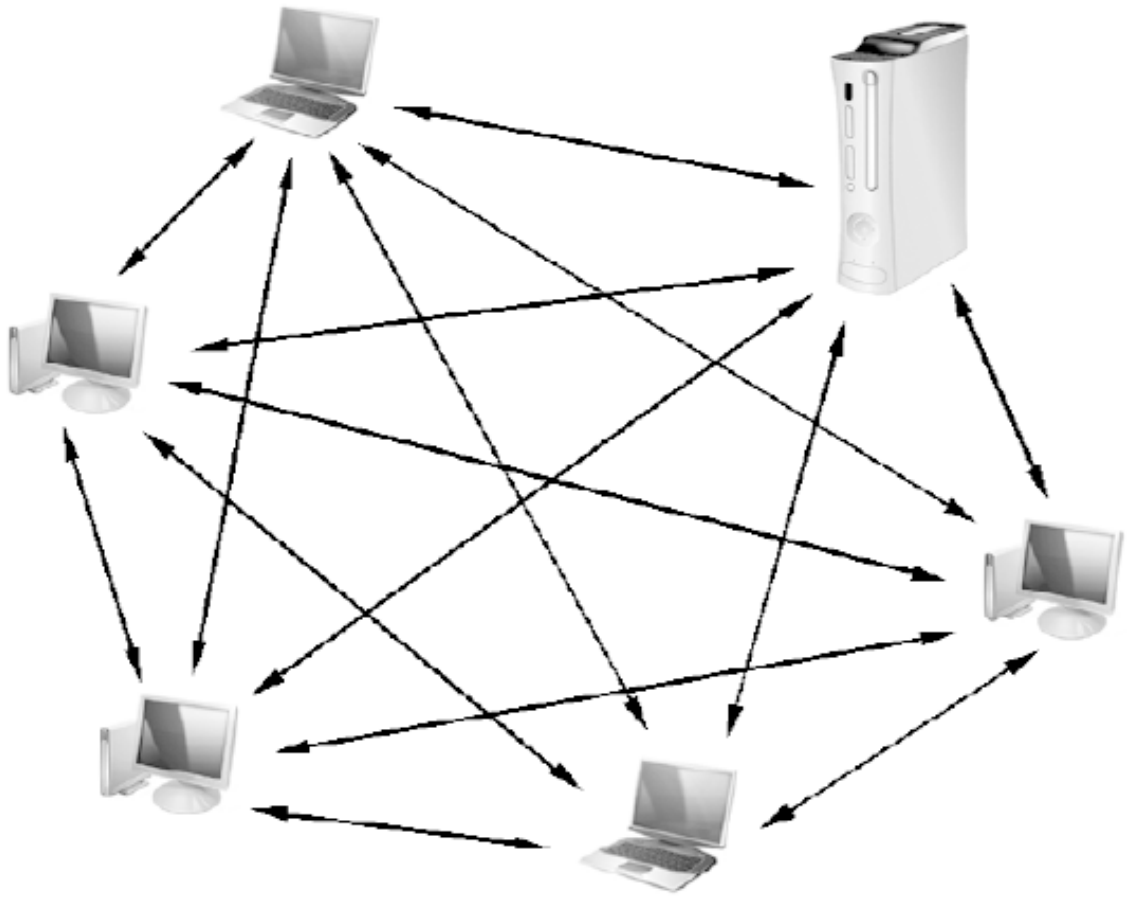

Рис. 8.1. Беспроводная сеть в режиме IBBS

Данный режим конфигурации сетевого оборудования имеет свои плюсы и минусы.

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 и более километров).

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

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 стоит использовать режим BBS.

BBS

Базовый набор служб, или режим инфраструктуры, – еще один режим работы беспроводной сети, который подразумевает использование центрального управляющего узла, называемого точкой доступа (Access Point). Все беспроводные станции подключаются к этой точке доступа (рис. 8.2).

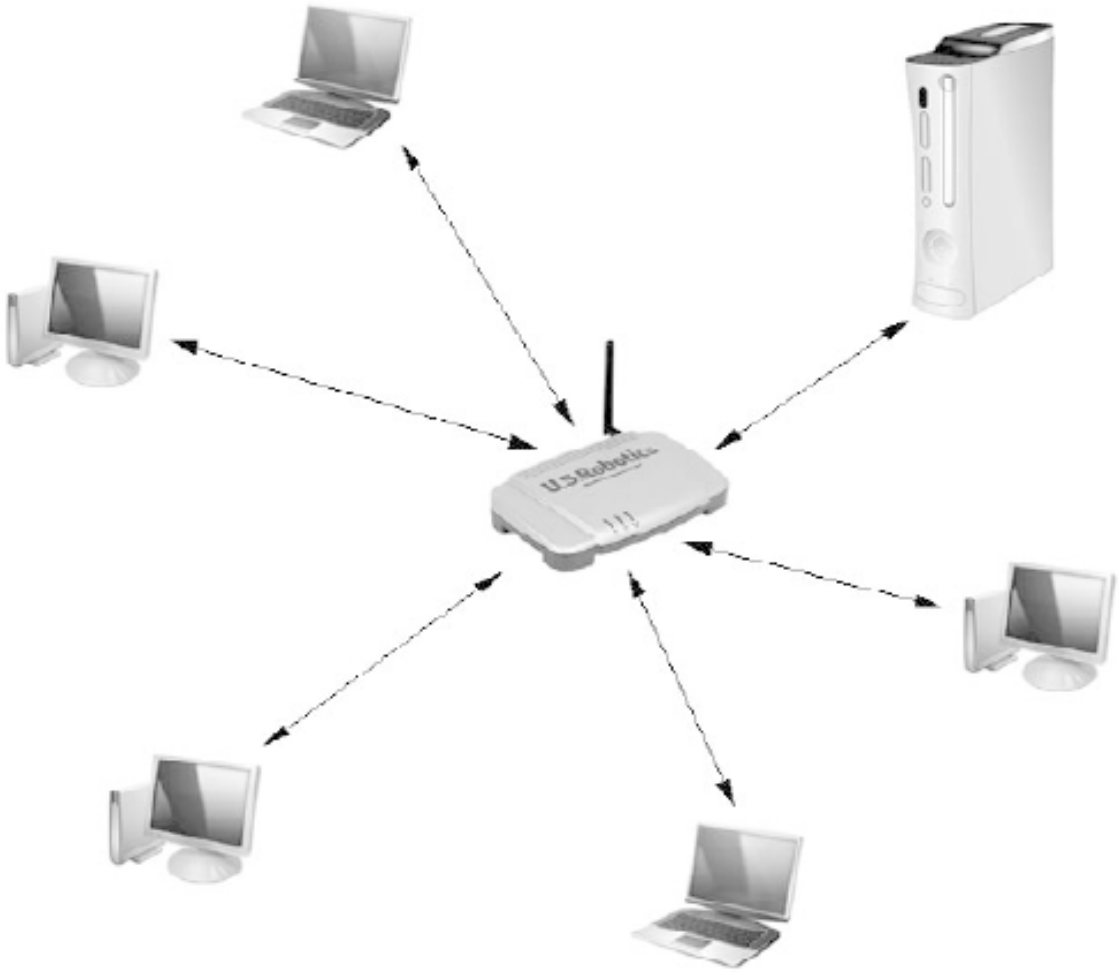

Рис. 8.2. Беспроводная сеть в режиме BBS

При этом вся необходимая для функционирования сети информация находится в точке доступа. Чтобы подключиться к ней, каждый беспроводной адаптер должен быть настроен соответствующим образом: необходимо указать идентификатор сети, выбрать метод шифрования и т. д.

Такой принцип организации работы является очень гибким и эффективным, он позволяет не только легко менять методы шифрования и аутентификации и расширять сеть, но и создавать комбинированные сети с большим количеством сегментов.

Если, опять же, проводить аналогию с проводным вариантом сети, то режим инфраструктуры практически повторяет топологию «звезда». При этом очень многие технические показатели локальной сети зависят от возможностей точки доступа.

Интересным моментом является возможность увеличения радиуса действия сети. Так, наиболее простой вариант сети подразумевает использование одной точки доступа, но их количество может быть и б**о**льшим. В этом случае получается некая модификация конфигурации сети, которая получила название расширенного набора служб (Extended Service Set, ESS) (рис. 8.3).

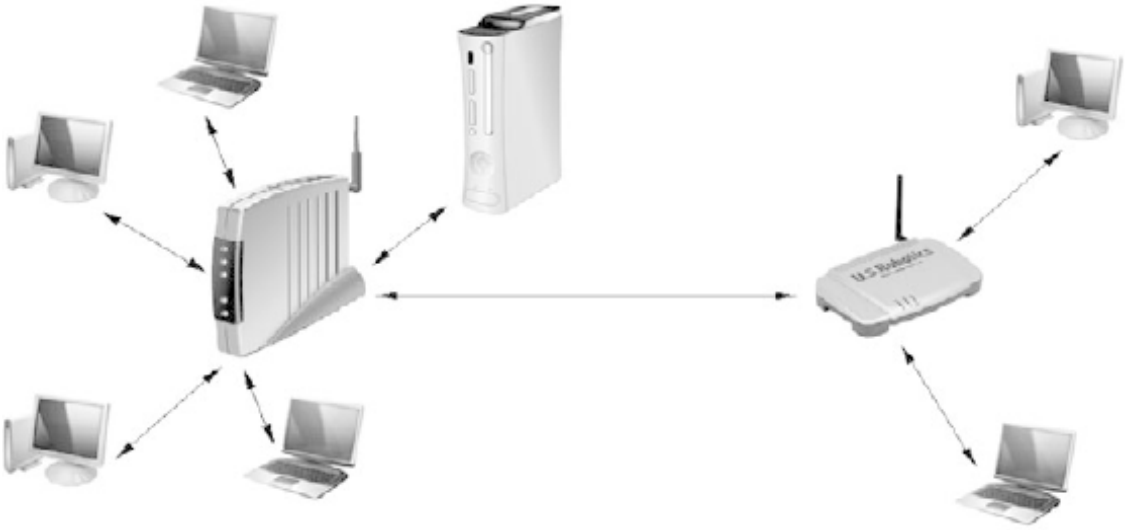

Рис. 8.3. Беспроводная сеть в режиме ESS

Если в беспроводной сети используется несколько точек доступа, они все представляют собой одно целое, то есть умеют обмениваться между собой всей необходимой информацией. 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 рабочая станция перемещается.

Возможности точки доступа на этом не заканчиваются. Так, точка доступа может использоваться не только для обслуживания беспроводных устройств: зачастую точка доступа представляет собой коммутатор стандарта 100Base-TX или ему подобного, что позволяет соединять беспроводной и проводной сегменты сети в одно целое с возможностью маршрутизации пакетов между сегментами. Такая организация сети встречается на практике очень часто.

Методы и технологии обработки сигнала

Вне зависимости от того, какую среду передачи данных использует в своей работе локальная сеть, существует целый набор технологий и методов обработки сигнала, которые применяются совместно с протоколами передачи данных, чтобы передаваемые данные не просто достигли адресата, но дошли быстро, без ошибок и желательно без необходимости их повторной передачи.

Беспроводная среда, которая всегда была непредсказуемой из-за влияния различных факторов, имеет по сравнению с проводным способом организации сети другой способ обработки сигнала. Так, для уверенной и качественной передачи и обработки данных при различной скорости их пересылки приходится использовать сложные методы и технологии кодирования данных, придающие им большую устойчивость к помехам и, как следствие, уменьшающие скорость их передачи. К тому же, учитывая постоянные физические помехи и наличие большого количества бытовых устройств, создающих радиопомехи, требуется применение целого ряда методов управления модуляцией сигнала и эффективного выбора каналов частот для его передачи.

Далее мы рассмотрим некоторые основные методы, с помощью которых данные превращаются в радиосигнал, передаются адресату и подвергаются обратному декодированию в формат, понятный компьютеру.

DSSS

DSSS (Direct Sequence Spread Spectrum, расширение спектра методом прямой последовательности) – один из основных методов модуляции сигнала, используемый в беспроводных локальных сетях. Данный метод применяется для преобразования исходного сигнала и передачи его одновременно по нескольким каналам связи определенной ширины.

Принцип его работы достаточно простой и выглядит следующим образом. Диапазон частот, выделенный для беспроводной сети (2400–2483,5 МГц), разбивается на 11 каналов шириной 22 МГц. Далее с помощью метода последовательностей Баркера каждый бит данных превращается в 11 бит, в результате чего получается 11-кратная избыточность. После этого данные передаются параллельно сразу по всем 11 каналам. Такой подход позволяет гарантированно передать и принять весь объем данных даже при слабом уровне сигнала и высоком уровне шумов в каналах. Это не только позволяет экономить энергию, используемую для передачи данных, но и не мешает работе соседних узкополосных устройств, поскольку широкополосная передача данных небольшой мощности воспринимается как обычный шум.

FHSS

FHSS (Frequency Hopping Spread Spectrum, псевдослучайное изменение рабочей частоты) – еще один метод обработки сигнала с целью расширения его спектра, используемый в беспроводных локальных сетях.

Метод FHSS также разбивает диапазон частот 2400–2483,5 МГц на полосы, но, в отличие от DSSS, эти каналы имеют ширину 1 МГц и их количество составляет 79. На этом их сходство заканчивается, и дальнейшие принципы работы коренным образом отличаются друг от друга.

Согласно методу FHSS данные передаются только по одному каналу, но сам канал с частотой не более 20 мс изменяется псевдослучайным образом. Причем схема изменения канала определяется и согласовывается между передатчиком и приемником заранее, на этапе соединения. Подобный подход позволяет значительно уменьшить вероятность того, что передаче данных что-то может помешать. Даже если в один из моментов передачи данных какое-то другое беспроводное оборудование займет нужный канал, сигнал об этом поступит отправителю, и необходимый фрагмент данных будет отправлен повторно.

По сравнению с DSSS метод FHSS является более помехозащищенным. Причиной является ширина канала, который используется для передачи данных. Так, возможность возникновения помехи для передачи, которая ведется с помощью 79 каналов шириной в 1 МГц, гораздо ниже, чем вероятность появления помехи для передачи, которая использует канал шириной в 22 МГц. Даже если рассмотреть вариант узкополосных помех, то случайное изменение несущей частоты, то есть смена каналов, делает такое влияние некритичным и приводит лишь к незначительному падению скорости передачи данных за счет отсылки дополнительных частей данных.

По этой причине на практике системы FHSS оказываются более устойчивыми к широкополосным помехам и могут продолжать работать (хотя и с пониженной пропускной способностью) в условиях, когда системы DSSS уже не способны нормально воспринимать полезный сигнал.

OFDM

OFDM (Orthogonal Frequency Division Multiplexing, ортогональное частотное мультиплексирование) – один из методов цифровой модуляции сигнала, позволяющих увеличить скорость передачи данных за счет разумного использования каналов связи и метода передачи данных. Главной причиной появления и применения этого метода обработки сигнала является поиск способов борьбы с широкополосными помехами – основной причиной плохой связи в условиях большого количества крупногабаритных препятствий в виде многоэтажных жилых домов и других зданий.

Принцип работы данного метода основан на разбиении потока данных с помощью инверсного дискретного преобразования Фурье на более мелкие составляющие, которые передаются параллельно, каждый на своей частоте. Это позволяет не только добиться высокой скорости передачи данных, но и свести к минимуму разного рода помехи, особенно в виде отображенного сигнала (сигнал, отбиваемый от препятствий, которые стоят на пути его прямого следования). За счет частично перекрывающихся каналов передаваемый код получается избыточным, что может использоваться для восстановления утерянных частей.

Данные, поступившие получателю, происходят процедуру восстановления целостности, для чего, опять же, используется быстрое дискретное преобразование Фурье, только на этот раз прямое.

PBCC

PBCC (Packet Binary Convolutional Coding, двоичное пакетное сверточное кодирование) – один из методов кодирования данных, позволяющий увеличить скорость передачи данных за счет сжатия кода.

Принцип работы метода сверточного кодирования заключается в следующем. При прохождении так называемого сверточного кодера последовательность входящих бит изменяется: каждому биту данных ставится в соответствие дополнительный бит или биты информации. За счет этого получается нужная избыточность кода, которая делает данные более устойчивыми к помехам и позволяет расшифровать их, даже если часть сообщения будет утеряна.

Что касается избыточности кода, то этот параметр регулируется в зависимости от потребностей. Так, если каждому биту информации соответствует два бита, то скорость сверточного кодирования составляет 1/2, если каждым двум битам соответствует 3 бита, то скорость кодирования составляет 2/3 и т. д.

Сверточный кодер использует определенную систему запоминающих ячеек, которые хранят состояние предыдущего сигнала. Например, если применить систему из шести запоминающих ячеек, то в результате можно получить данные о шести предыдущих состояниях. Этот факт и позволяет восстанавливать данные, даже если большая часть из них будет повреждена или утеряна.

После того как на выходе получается избыточный код, он подвергается фазовой модуляции с помощью одного из методов, например BPSK (двоичная модуляция), QPSK (квадратичная модуляция), 8-PSK (восьмипозиционная фазовая модуляция) и т. д.

При попадании сигнала в приемник данные проходят обратный процесс преобразования, для чего, как правило, используется декодер Витерби.

CCK

CCK (Complementary Code Keying, кодирование с использованием комплементарных кодов) – одна из технологий, при использовании которой данные проходят этап кодирования с целью получения избыточности кода и применения этой избыточности для восстановления (если появится такая необходимость).

Технология CCK достаточно сложна с математической точки зрения, но общий принцип ее работы сводится к следующему: каждый бит передаваемых данных кодируется с помощью восьмибитовой последовательности (слова), что приводит к добавлению дополнительных бит информации.

Эта технология применяется в паре с одним из методов модуляции сигнала, который занимается непосредственно передачей данных.

Для декодирования данных со стороны приемника используется та же схема кодирования, которая применялась для кодирования информации.

CCK-OFDM

CCK-OFDM – гибридная технология кодирования, представляющая собой симбиоз технологии CCK и метода модуляции сигнала OFDM. Такой подход позволяет увеличить скорость передачи данных за счет того, что заголовок кадра, то есть служебная часть данных, кодируется с помощью технологии CCK, а сами данные передаются с использованием кодирования ODFM.

MIMO

MIMO (Multiple Input, Multiple Output, множественный прием/передача) – технология, с помощью которой прием и передача данных ведется с помощью раздельных антенн, количество которых может быть любым.

Причиной появления данной технологии стала необходимость увеличения радиуса сети и скорости передачи данных. Конечно, повышения дальности и качества связи можно достичь и за счет использования более мощных передатчиков и антенн с увеличенным коэффициентов усиления. Однако существующие стандарты строго ограничивают мощность передатчика, особенно для систем офисного или домашнего применения, поэтому такой подход не является эффективным.

Как уже было сказано, для приема и передачи данных используются разные антенны, при этом существуют алгоритмы и методы обработки сигнала, позволяющие свести к минимуму взаимные наводки в передающем и приемном тракте устройства.

Повышение скорости передачи данных стало возможным также за счет увеличения ширины канала со стандартных 22 до 40 МГц и применения более совершенных методов кодирования.

Шифрование и аутентификация

Безопасность работы в локальной сети, а тем более безопасность ваших личных данных всегда была и будет тем вопросом, которому уделяется 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 навряд ли понравится, если содержимое вашей личной переписки узнает кто-то другой 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 ничего нельзя сделать.

Как и в реальной жизни, 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 особенностей среды передачи данных.

В данном разделе книги рассмотрим методы безопасности, которые используются в беспроводных локальных сетях. Почему именно беспроводных? Все очень просто: если в проводных сетях подключение к сети можно проконтролировать, то использование радиоэфира проконтролировать физически невозможно: злоумышленник может сидеть рядом за стенкой или через дорогу в автомобиле и, держа в руках ноутбук или любое другое достаточно «умное» устройство с беспроводным оборудованием, 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 сегодняшний день при работе беспроводного оборудования используются такие алгоритмы безопасности и аутентификации, как WPA, WPA2, AES, TKIP, RADIUS и др.

WEP

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

Разработка данного алгоритма началась в средине 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[2], в связи с чем различают две версии алгоритма – WEP-40 и WEP-104 соответственно.

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 аутентификации. Так, по проишествии совсем небольшого времени после появления WEP был найден достаточно простой способ взлома этого алгоритма: достаточно иметь любой беспроводный адаптер и соответствующую программу, умеющую перехватывать и анализировать пакеты сети; десять минут работы приложения – и вы получаете нужный вам ключ подключения к локальной сети. А вскоре были найдены еще как минимум два способа взлома сети. Они анализируют вектор инициализации или внедряют

[2] На самом деле используются ключи длиной 64 и 128 бит, но 24 бита применяются в качестве вектора инициализации, содержащего данные для расшифровки сообщения.

ARP-запросы[3], которые спокойно пропускаются точкой доступа, и получают нужную для взлома информацию.

Пытаясь хоть как-то спасти положение 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 аналогичного назначения.

В данном случае речь не идет об аутентификации в серьезном смысле этого понятия. Любой беспроводный клиент может подключиться к другому беспроводному клиенту или точке доступа. При этом беспроводный клиент отправляет запрос на подключение, содержащий данные об идентификаторе устройства. Если никаких исключений или других правил подключения, например таблиц MAC-адресов, на точке доступа не настроено, беспроводный клиент получает разрешение на подключение и сразу может начать работу в локальной сети. Если же по какой-либо причине беспроводный клиент «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 подключения к беспроводной локальной сети прописывается как в точке доступа, так и в беспроводном адаптере каждого беспроводного клиента, который подключается к сети. Не зная данный ключ, произвести подключение к беспроводной сети не получится, поэтому администратор сети сам выбирает, кому сообщать этот ключ.

Процесс аутентификации с общим ключом состоит из трех этапов.

1. Беспроводный 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», беспроводный 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 результаты 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 возникший в середине 2003 года.

---

[3] Речь идет о протоколе сетевого уровня ARP (Address Resolution Protocol), который лишен какой-либо защиты от взлома. Отсылаемые и получаемые пакеты не контролируются на целостность и достоверность. Протокол предусматривает получение случайных незатребованных ответов, используя которые злоумышленник и может получить доступ к необходимой информации.

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 большого количества создателей беспроводных сетей. Это также 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 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 находятся такие, как MD5, TLS, TTLS, PEAP, SIM, AKA, LEAP, FAST и др.

В процессе аутентификации используется 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 надежнее защитить данные от их возможного перехвата. MIC работает как на отправителе, так и на получателе, что позволяет максимально защитить передаваемые данные. Работает система очень просто: каждый пакет данных снабжается восьмибитовым 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 WPA, уже зафиксированы способы обхода 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 дальнейшей модификацией алгоритма WPA. Появление этого алгоритма связано с возникновением в 2004 году нового стандарта безопасности IEEE 802.11i. Все сертифицированные устройства, начиная с 2006 года выпуска, 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 используется 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, что приводит к увеличению трафика в сети и как следствие – к уменьшению полезной скорости передачи данных. Однако такой подход вполне оправдан: на сегодняшний день не известны способы взлома этого алгоритма, что вселяет надежду и гарантирует дальнейшее распространение беспроводных локальных сетей.

Глава 9
Стандарты IEEE 802.3

Разработкой стандартов и правил функционирования локальных сетей стандарта Ethernet с физической средой передачи данных в виде коаксиального, оптоволоконного кабеля и кабеля «витая пара» занимается комитет 802.3. За время своего существования на свет появилось достаточно много стандартов. Наиболее известными среди них являются стандарты 10Base-5, 10Base-2, 10Base-T, 100Base-TX, 1000Base-X. Особенности некоторых из них мы рассмотрим в данной главе.

10Base-5, 10Base-2

Данные стандарты описывают принцип функционирования сети с применением сетевой топологии «шина» и коаксиального кабеля в качестве среды передачи данных. До их возникновения существовали и другие стандарты, однако именно с появлением стандарта 10Base-5 локальные сети стали набирать популярность.

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

Стандарт 10Base-5 предусматривает определенные правила подключения к локальной сети и ее функционирования. Наиболее важными среди них 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, с помощью которых устраняется 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 не должна превышать 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 не должно быть меньше 2,5 м;

□ длина кабеля от трансивера до сетевой карты станции не должна превышать 50 м.

При соблюдении всех этих правил 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 использовал коаксиальный кабель, но его тонкий вариант. Соответственно, он получил название *тонкий Ethernet.* Так как в качестве среды передачи данных использовался тонкий коаксиальный кабель, создание сети стало более легким, поскольку толщина кабеля позволяла выбрать оптимальный маршрут его прокладки. Кроме того, при этом для подключения компьютера перестали требоваться трансивер и репитер. Однако все эти преимущества привели к тому, что максимальная длина сегмента уменьшилась более чем в два раза и составила около 200 м.

Изменения также коснулись и других требований:

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

□ в сети может присутствовать максимум 5 сегментов, при этом общая протяженность центральной магистрали составляет 925 м;

□ минимальное расстояние между точками подключения – 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 достаточно сложно определить участок обрыва, 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, больш**а**я протяженность сегмента является безусловным плюсом, поскольку это позволяет соединить между собой удаленные точки.

Тем не менее стандарты 10Base-5 и 10Base-2 не имеют перспектив, поскольку скорость передачи данных 10 Мбит/с на сегодня слишком мала для обеспечения потребностей сети. Особенно с учетом того, что скорость делится между всеми участниками сети, и чем больше будет их количество, тем меньше будет полезная скорость передачи данных.

10Base-T

Топология «шина» была первой из использовавшихся в локальных сетях топологий. Она применялась достаточно долго, почти целое десятилетие. Однако наступил момент, когда эта сетевая топология (по крайней мере с использованием коаксиального кабеля) перестала удовлетворять требованиям скорости передачи данных, и особенно – надежности сети. Уменьшение скорости передачи данных при значительном увеличении количества рабочих станций 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 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 и стало важнейшим этапом в распространении локальных сетей.

Использование топологии «звезда» сделало локальные сети более гибкими и 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. При этом одна пара проводников применяется для передачи данных, а вторая – для их приема;

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

□ для увеличения диаметра 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 данного стандарта позволяет достичь скорости передачи данных 10 Мбит/с. Главной особенностью локальных сетей с применением топологии «звезда» является то, что скорость передачи данных не зависит от количества подключенных участников.

При этом сеть стала еще более гибкой, поскольку ее максимальный радиус можно легко увеличить, используя, например, толстый коаксиальный кабель. Это позволяет создавать разные удаленные сегменты сети 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 также подразумевает использование сетевой топологии «звезда». Однако он имеет одно очень 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 агрессивной физической среды.

Стандарт 10Base-F подразумевает выполнение следующих условий:

□ для передачи данных используется оптоволоконный кабель с различным сечением световода, то есть 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 доступны благодаря принципу передачи сигнала и малому уровню его затухания в оптическом волокне. Это свойство часто используют для того, чтобы увеличить максимальный радиус 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, так и в дуплексном режимах. При этом дуплексный режим обеспечивает максимально возможную для стандарта скорость передачи данных в 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, при этом максимальный радиус сети 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.

Немало влияние на широкое распространение 100Base-TX произвела стандартизация материнских плат (ATX), которая сделала наличие сетевого адаптера на материнской плате обязательным.

100Base-T4

Этот стандарт относится к серии 100-мегабитных. Он также подразумевает использование топологии «звезда» и кабеля витая пара (UTP). Однако, в отличие от 100BaseTX, данный стандарт позволяет в качестве среды передачи данных использовать кабель ниже пятой категорий. Данный факт является наибольшим плюсом этого стандарта. Так, пользователи локальной сети стандарта 10Base-T, которая подразумевает применение кабеля «витая пара» третьей категории, могут перейти на сеть со скоростью передачи данных 100 Мбит/с, просто заменив используемое оборудование на поддерживающее стандарт 100Base-T4, а также изменив обжим кабеля.

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

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

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

□ для увеличения диаметра сети может использоваться не более 2 репитеров, при этом максимальный радиус сети составляет 205 м;

□ максимальное 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 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 используется в сетях с топологией «звезда», при этом в качестве среды передачи данных применяется 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 в кабеле и мощностью используемых передатчиков, что позволило 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 качестве 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 снизилась достаточно серьезно, использование многомодового кабеля не имеет особого смысла.

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

Появление стандартов, поддерживающих скорость передачи данных не менее 1 Гбит, было лишь делом времени. Случилось это в 1998 году, когда комитет принял стандарт 1000Base-X, объединивший в себе сразу 4 гигабитных стандарта: 1000Base-LX, 1000Base-CX, 1000Base-LH и 1000Base-LX.

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 м (1000Base-SX, многомодовый кабель) до 10 000 м (1000Base-LH, одномодовый кабель).

1000BaseT

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 1000BaseT приходит на смену интегрированному на материнской плате сетевому контроллеру стандарта 100Base-TX.

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 выполнение следующих условий:

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

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

□ для увеличения диаметра сети может использоваться не более 2 репитеров, при этом максимальный радиус сети 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.

Достаточно переход со стандарта 100Base-TX на 1000Base-T требует только замены оборудования, поскольку очень часто при построении сети используется кабель категории 5.

Глава 10
Стандарты IEEE802.11

□ IEEE 802.11

Разработкой правил функционирования локальных сетей стандарта Ethernet 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 из беспроводных стандартов будут рассмотрены ниже.

IEEE802.11

Стандарт IEEE 802.11, разработка которого была начата сразу после образования комитета 802.11, что произошло в 1990 году, является первым беспроводным стандартом, который можно было использовать для создания локальной 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 DSSS и FHSS, имеющие разный принцип работы, что делает их несовместимыми между собой.

Рассматриваемый стандарт предусматривает выполнение следующих положений:

□ для работы в локальной сети используется оборудование, которое работает в диапазоне радиочастот 2400-2483,5 МГц;

□ радиус сети не превышает 300 м;

□ стандартная скорость передачи данных – 1 Мбит/с, опциональная – 2 Мбит/с;

□ используется метод прямой последовательности DSSS с технологией модуляции сигнала PSK или метод частотных скачков FHSS с технологией модуляции FSK.

При использовании стандарта IEEE 802.11 теоретический радиус сети составляет 300 м. На практике же он редко превышает 50-100 м, что обусловлено наличием большого количества препятствий для распространения сигнала. 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. И это при том, что проводные варианты сети 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 802.1 1b началось широкое распространение беспроводных сетей. Именно этот стандарт стал причиной появления 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, в ноутбуки и другие переносные устройства также стали встраивать поддержку стандарта IEEE 802.11b. Беспроводные локальные сети данного стандарта даже сейчас встречаются часто.

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;

□ для работы с сигналом применяется метод прямой последовательности DSSS с восьмиразрядными последовательностями Уолша и CCK;

□ в качестве протокола безопасности используется протокол WEP;

□ для доступа к передающей среде применяется метод CSMA/CA.

Чтобы добиться скорости передачи данных 11 Мбит/с, используется метод DSSS, применяющий 5 перекрывающихся поддиапазонов. Для шифрования данных применяется последовательность дополнительных комплементарных кодов. Это позволяет добиться большей устойчивости кода за счет его избыточности.

Из плюсов IEEE 802.11b можно отметить то, что оборудование этого стандарта имеет наибольшую чувствительность. По этой причине качество связи с применением такого оборудования гораздо выше, чем при использовании оборудования с более новыми стандартами. Кроме того, некоторые производители предлагают оборудование, которое может работать на скорости 22 Мбит/с (IEEE 802.1 1b+) при условии применения оборудования от одного производителя.

Минусом стандарта является то, что скорость передачи данных может падать вплоть до самой низкой, что зависит от количества преград между передатчиком и приемником сигнала. Кроме того, оборудование стандарта IEEE 802.11b использует WEP-шифрование, безопасность которого очень низкая. При использовании соответствующих программ получить ключ 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 другим путем, решив использовать в качестве диапазона частот сразу три полосы: 5,15-5,25 МГц, 5,25-5,35 МГц, 5,725-5,825 МГц. Это позволяет добиться б**о**льшей пропускной способности, а также использовать более свободный диапазон частот. При этом применяются новые методы обработки сигнала, а также новые, более усовершенствованные алгоритмы шифрования.

Стандарт предусматривает следующие правила и соглашения:

□ 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;

□ применяется метод ортогонального частотного мультиплексирования OFDM.

Главным достоинством этого стандарта является высокая скорость передачи данных, однако это практически единственный его плюс. Минусов гораздо больше, и основные из них следующие:

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

□ несовместимость IEEE 802.1 1a с существующими стандартами (кроме 802.1 1n), что делает использование сетевого адаптера невозможным, если применяется точка доступа с другим стандартом;

□ практически во всех странах требуется наличие соответствующего разрешения и даже лицензии на использование оборудования для работы с указанными диапазонами частот.

Эти недостатки привели к тому, что стандарт IEEE 802.11a не получил того распространения, которое ожидалось, даже несмотря на высокую скорость передачи данных.

IEEE 802.11g

В начале 2000 года многие ожидали появления стандарта IEEE 802.11g, поскольку наиболее распространенный на то время стандарт IEEE 802.11b уже не удовлетворял своими возможностями как в плане скорости, так и в плане 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, 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;

□ для работы с сигналом применяется усовершенствованный метод прямой последовательности CCK-DSSS и метод двоичного пакетного сверточного кодирования PBCC;

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

□ для доступа к передающей среде применяется метод CSMA/CA;

□ максимальное количество подключений – 2048.

Поддержка этого удачного стандарта сразу же была реализована в ноутбуках и переносных устройствах, что также повысило его популярность. Кроме того, как и в случае со стандартом IEEE 802.1 1b, некоторые производители, например D-Link, выпустили на рынок устройства, способные работать на скорости 108 (IEEE 802.1 1g+) и даже 125 Мбит/с, что сделало данный стандарт еще более привлекательным.

IEEE 802.11n

Принятие стандарта IEEE 802.11g на некоторое время решило стоящие задачи. Однако потребности в скорости передачи данных увеличивались с каждым днем, а проводные варианты сетей уже предлагали скорости 100 и даже 1000 Мбит/с. Это привело к тому, что рас-

пространение беспроводных сетей опять затормозилось, и они стали актуальны лишь для 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 длилось почти год, и в 2009 году наконец-то был принят стандарт IEEE 802.11n, который начал новую эру в развитии беспроводных сетей.

Использование оборудования данного стандарта позволяет достигать значительных скоростей передачи данных, вплоть до 300 Мбит/с (по некоторым данным – до 600 Мбит/с). Такая скорость передачи данных стала возможной благодаря более оптимальному использованию полос радиочастот, а также применению более качественных 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 в диапазонах частот 2,4 и 5 ГГц, выбор которых происходит в зависимости от режима работы. Он зависит от стандартов оборудования, которое работает в локальной сети. Например, если в сети используется оборудование разных стандартов, то будет выбран режим совместимости с предыдущими стандартами, и скорость передачи данных при этом будет гораздо ниже стандартной. 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);

□ для обработки сигнала применяется усовершенствованный метод ортогонального частотного мультиплексирования OFDM и технология многоканальных антенных систем MIMO.

На сегодняшний день 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, который позволит вдвое увеличить пропускную способность сети, придется ни много ни мало – до 2016 года.

Глава 11
Спецификации Bluetooth

Слово Bluetooth слышал, наверное, каждый (возможно, даже не понимая, что это такое). Мало того: каждый пользователь мобильного телефона и любого переносного устройства знает, что с помощью Bluetooth он может передавать и получать данные. Однако почти никто не задумывается о том, что с помощью технологии Bluetooth можно даже строить беспроводные локальные сети, пусть и с небольшим количеством подключенных устройств. В настоящий момент разрабатывается технология, позволяющая посредством Bluetooth объединять устройства любого типа с целью быстро получить или передать нужные данные.

История появления названия Bluetooth достаточно интересна. В начале нашего 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, в этом они 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 средине 90-х годов прошлого века. Изначально разработкой Bluetooth занималась только одна компания, а именно Ericsson Mobile Communication. Создавалась эта технология для нужд компании, но в итоге своими возможностями заинтересовала многих.

Таким образом, 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 кроется большое будущее, ряды SIG пополнились более чем 1000 новых членов. Конечно, большая часть из них лишь хотели получить свой «кусок пирога» от славы, но, тем не менее, столь грандиозный консорциум сделал свое дело.

Чтобы иметь возможность пользоваться Bluetooth, необходимо иметь адаптер Bluetooth. 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, расстоянием действия.

- **Class 1.** Мощность передатчика 100 мВт (20 дБм), расстояние действия 100 м.
- **Class 2.** Мощность передатчика 2,5 мВт (4 дБм), расстояние действия 10 м.
- **Class 3.** Мощность передатчика 1 мВт (0 дБм), расстояние 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 этом диапазоне частот работают тысячи разнообразнейших устройств, включая оборудование беспроводных сетей.

Как и в беспроводных локальных сетях, технология Bluetooth для обработки сигнала использует метод скачкообразного изменения рабочей частоты FHSS и схему модуляции сиг-

нала GFSK (Gaussian Frequency Shift Keying, кодирование Гаусса со сдвигом частоты). При этом доступный диапазон частот разбивается на полосы шириной в 1 МГц, а смена несущей частоты, то есть полосы частот, происходит 1600 раз в секунду. О схеме переключения частот отправитель и получатель договариваются на этапе установки связи, поэтому вероятность того, что передаче данных помешают другие рядом работающие устройства, достаточно низкая.

За все время работы группы Bluetooth SIG было разработано шесть стандартов 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, физические адреса (идентификаторы устройств) которых заранее известны. Это является одним из недостатков, поскольку невозможен анонимный обмен данными. Однако это не так критично, как проблемы с совместимостью устройств. Именно они обусловили провал Bluetooth 1.0. Главной причиной этого стали недоработки и несоблюдения производителями соглашений спецификации. Это привело к тому, что широкополосные и узкополосные варианты устройств оказались полностью несовместимы между собой.

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 с расстоянием действия 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). Данная спецификация стала более успешной, поскольку было решено множество проблем, связанных с ошибками и несовместимостью 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, она стала настолько удачным решением, что во многие переносные и портативные устройства начали встраивать контроллер Bluetooth 1.2. Их 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 по ходу сигнала;

□ обратная совместимость с устройствами предыдущих версий;

□ увеличенная реальная 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 версии Bluetooth стали:

□ технология EDR (Enhanced Data Rate, увеличенная пропускная способность), позволившая значительно увеличить скорость передачи данных. По этой причине данную версию Bluetooth часто называют Bluetooth 2.0+EDR;

□ скорость передачи данных до 3 Мбит/с;

□ обратная совместимость со старыми версиями Bluetooth;

□ поддержка механизма Multi-Cast, позволяющего отправлять данные сразу нескольким устройствам;

□ сервис качества QoS (Quality of Service), контролирующий качество связи и устраняющий эффект торможения при работе с несколькими устройствами;

□ распределенный контроль доступа к передающей среде, позволяющий поддерживать работу с 256 устройствами;

□ уменьшенное энергопотребление.

Как видите, в версии 2.0 действительно произошли значительные изменения. В результате 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:

□ технология NFC (Near Field Communication), делающая соединение более безопасным и исключающим возможность перехвата данных третьими лицами;

□ технология уменьшения энергопотребления Sniff Subrating, благодаря которой энергопотребление снизилось в 3-10 раз по сравнению со старыми версиями Bluetooth;

□ обновление ключа шифрования 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 перспективной в плане использования для организации обмена данными между устройствами.

Новая версия Bluetooth имеет следующие нововведения:

□ скорость передачи данных до 24 Мбит/с;

□ уменьшенное энергопотребление;

□ использование альтернативных протоколов IEEE 802.11;

□ 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.

Устройства 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 12
Спецификации HomePNA

В последнее время наблюдается бурное развитие локальных сетей: компьютеры все чаще объединяются в единую структуру для получения доступа к общим ресурсам, периферии и Интернету.

Появлению локальных сетей способствует доступность их создания. Существует достаточно много способов это сделать, даже не прибегая к услугам специалистов. Кроме чисто сетевых способов, которые используются уже достаточно продолжительное время, существуют и некоторые, можно сказать, экзотические методы создания сети. Один из них – применение стандарта HomePNA.

История появления стандарта HomePNA достаточно проста. Мысль использовать существующую инфраструктуру, точнее – телефонную проводку, для создания дешевого способа передачи нужных данных возникала уже давно. Не хватало только знаний и возможностей, чтобы это сделать. Кроме того, пугала неоднородность и неопределенность структуры подобного функционирования, ведь характеристики телефонной проводки могут изменяться, при этом ее топология становится все более запутанной. В таких условиях возможность создания сколь-нибудь подходящего способа для передачи данных была очень сомнительной. Тем не менее рано или поздно такой способ должен был быть найден, что 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). Заданием 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 телекоммуникации ITU (International Telecommunication Union) – известная в телекоммуникационных кругах организация.

Стоит отметить, что HomePNA изначально была ориентирована на обслуживание небольшого количества подключений, что явно отслеживается в некоторых ее характеристиках. Именно этот факт и определил возможные сферы ее использования – домашние сети, небольшие офисы, рестораны и кафе и т. п.

Технология HomePNA получила достаточно широкое распространение, особенно в «домашних» сетях. Так, она часто используется 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. Плюсом этого способа подключения является то, что подобным образом к одному Ethernet-кабелю можно подключить все компьютеры, находящиеся в квартире.

Рассмотрим некоторые спецификации HomePNA.

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 метода доступа к передающей среде CSMA/CD. Часто можно встретить мнение, что на самом деле это не что иное, как Ethernet, но по телефонной линии.

Спецификацией HomePNA определяются следующие правила функционирования локальной сети:

□ используется топология «звезда», подразумевающая применение коммутатора;

□ в качестве среды передачи данных используется обычная телефонная проводка с двумя проводниками;

□ для доступа к передающей среде применяется метод множественного доступа с контролем несущей и обнаружения коллизий CSMA/CD;

□ 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.;

□ применяется кодировка одиночного битового импульса PMM (Pulse Position Modulation), позволяющая подстраиваться под условия среды;

□ максимальная скорость передачи данных составляет 1 Мбит/с, при этом каждый узел получает скорость в полном объеме;

□ возможна работа 25 подключений;

□ максимальный диаметр сети – 150 м (на практике можно достичь более 300 м, что зависит от качества кабеля).

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

Однако спецификация HomePNA не нашла столь широкого распространения. Причина кроется в необходимости использования коммутатора для соединения компьютеров в сеть. Применение коммутатора делает сеть более дорогой и сложной, поскольку требуется определить место, где может быть расположен этот коммутатор (место схождения всех кабелей), а также произвести разводку портов.

HomePNA2.0

Можно смело утверждать, что восприятие HomePNA как альтернативы построения небольших локальных сетей началось именно с появления 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 также использовать кабель «витая пара» 5 категории, радиопроводку и любой кабель, даже не с медными проводниками;

□ используется технология кодирования QAM (Quadrature Amplitude Modulation, квадратурная амплитудная модуляция), позволяющая добиться увеличения длины сегментов сети;

□ применяется сервис качества QoS (Quality of Service);

□ максимальная скорость передачи данных составляет 10 Мбит/с, при этом скорость передачи данных меняется в зависимости от расстояния и качества используемого носителя и делится между всеми участниками сети;

□ поддерживается работа 32 подключений;

□ максимальный диаметр сети – 350 м (на практике можно достичь более 1000 м, что зависит от типа кабеля и применяемой аппаратуры);

□ для передачи данных используется диапазон частот 4-21 МГц.

Как показала практика, данный стандарт получился очень гибким и функциональным. Особого внимания заслуживает диаметр сети, который, по мнению некоторых, иногда превышает 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 стала составлять 128 Мбит/с. Это 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.

Главные особенности спецификации HomePNA 3.0 следующие:

□ в качестве среды передачи данных используется телефонная проводка или коаксиальный кабель;

□ максимальная скорость передачи данных составляет 128 Мбит/с;

□ максимальный диаметр сети – 350 м;

□ поддерживается работа 32 устройств;

□ применяется технология кодирования QAM (Quadrature Amplitude Modulation);

□ используется сервис качества QoS (Quality of Service);

□ для передачи данных используется диапазон частот 4-36 МГц.

HomePNA 3.1

На сегодня 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.

Основные показатели спецификации 3.0 следующие:

□ 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;

□ максимальный диаметр сети составляет 350 м при использовании телефонной проводки и 600 м – коаксиального кабеля;

□ поддерживается работа 64 устройств;

□ используется технология кодирования QAM (Quadrature Amplitude Modulation);

□ применяется сервис качества QoS (Quality of Service);

□ для передачи данных используется диапазон частот 4-65 МГц;

□ имеется автоматическая адаптация скорости и схемы применения частотных каналов в зависимости от зашумленности канала;

□ существует обратная совместимость с оборудованием предыдущих спецификаций;

□ стоимость оборудования невысока.

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

Глава 13
Спецификации HomePlug

В предыдущей главе мы рассмотрели один из экзотических способов объединения компьютеров в локальную сеть с применением в качестве среды передачи данных телефонной проводки. Казалось бы, какой помощник из телефонной проводки, если даже телефон иногда отказывается на ней работать. Оказывается, все не так плохо, а при определенных условиях – очень даже хорошо!

В этой главе книги мы опишем еще один вариант технологии создания локальной сети с применением способа, который по экзотичности даже превосходит предыдущий. Речь идет 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 налицо – существует большое количество локальных сетей разного размера, которые работают именно по электрической проводке.

Не секрет, что кабель, по которому передается электричество, проложен практически везде, где находится человек. Ведь другого способа быстро передать электричество от источника к месту обитания человека или просто нужному месту просто не существует. 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 давно. Ведь если бы это стало возможным, создание сети свелось бы к простому подключению «вилки к розетке».

В марте 2000 году 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 метод модуляции сигнала OFDM (Orthogonal Frequency-division Multiplexing), технологии кодирования DBPSK (Differential Binary Phase Shift Keying) или DQPSK (Differential Quadrature Phase Shift Keying), а также шифрование данных алгоритмом DES (Data Encryption Standard). При этом для передачи данных используется 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 понятны: 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 фазе. К ним также относится недостаток топологии «шина» – скорость делится между всеми устройствами сети.

HomePlug 1.0

Первая «электрическая» спецификация стандарта HomePlug была разработана и принята уже после года работы 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;

□ максимальный диаметр сети составляет 100 м (на практике расстояние может составлять более 1000 м, но с более низкой скоростью передачи данных);

□ допускается применение репитеров, что позволяет увеличить расстояния передачи данных до 10 000 м;

□ используются адаптивные механизмы изменения частоты или отключения определенных каналов при обнаружении сильных помех;

□ применяется сервис качества QoS (Quality of Service) с четырьмя уровнями качества доставки;

□ для шифрования данных используется метод DES с 56-битным ключом шифрования.

Как видите, технические характеристики спецификации HomePlug 1.0 достаточно привлекательны, особенно если учесть, что для подключения сети достаточно приобрести PowerLine-адаптер, вставить его в розетку и подключить кабелем к Ethernet-адаптеру стандарта 100Base-TX или ему подобного.

По прошествии небольшого промежутка времени 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 «билетом в жизнь» для HomePlug как стандарта для локальных сетей.

HomePlug AV

Принятие в 2005 году спецификации HomePlug AV[4] стало знаменательным событием, поскольку позволило использовать этот стандарт для работы с большими потоками информации, например с видеопотоком в HD-качестве (HDTV). Если проанализировать данную спецификацию детально, то можно заметить, что при ее разработке были пересмотрены многие подходы, 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;

□ используется метод доступа к передающей среде CSMA/CA;

□ применяется сервис качества QoS (Quality of Service);

□ для шифрования данных используется технология AES со 128-битным ключом шифрования.

Возможности спецификации HomePlug позволяют создать сеть в небольшом офисе или дома. Скорости такой сети с запасом хватит для выполнения любых поставленных задач,

[4] Аббревиатура AV указывает на то, что спецификация ориентирована на работу с аудио-, видеосодержимым в реальном времени.

вплоть до изначального предназначения спецификации – передачи аудио– и видеосодержимого высокого разрешения.

Глава 14
Механизмы и особенности управления сетью

- □ Операционная система
- □ IP-адресация
- □ Рабочая группа
- □ Доменная структура
- □ DNS
- □ DHCP
- □ Active Directory
- □ SSID

Локальная сеть (и проводная, и беспроводная) – сложная структура, к которой относятся многие понятия: топология, среда передачи данных, протоколы передачи данных, оборудование и многое другое. Только организация работы всех этих составных частей позволяется добиться того, для чего, собственно, сеть и предназначена, – передачи данных.

Кроме большого объема работы, который скрыт от пользователя и часто выполняется без его участия на аппаратном уровне, существует и такая часть работы, в которой требуется его вмешательство. Сюда входит настройка операционной системы для работы в сетевом окружении, настройка адресации, выбор варианта подключения к сети, поддержка работы большого количества системных механизмов, делающих возможным использование сетевых сервисов, и многое другое. В данной главе рассмотрим тот необходимый минимум, без которого подключиться к сети и работать в ней, а уже тем более администрировать ее 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 многое другое.

На сегодня существует достаточно много операционных систем, предназначенных для разных целей. Некоторые из них созданы для определенных производственных нужд, другие больше ориентированы на решение локальных задач, но подобные системы нас не интересуют. Главный интерес 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 имеют существенные различия. Так, можно выделить *серверные* и *клиентские* операционные системы.

Серверные операционные системы ориентированы на то, что их роль в локальной сети будет ведущей, в связи с чем они содержат множество системных механизмов, которые позволяют производить администрирование локальных сетей. 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. Если рассматривать продукцию компании Microsoft, то примерами таких операционных систем выступают Windows 2000 Server, Windows Server 2003, Windows Server 2008.

Клиентские операционные системы отличаются от серверных тем, что они 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 ведущими компьютерами (серверами) с серверной операционной системой. Клиентская операционная система обладает всеми необходимыми механизмами – протоколами, службами и сервисами, которые необходимы для того, чтобы подключиться к локальной сети и получить от нее необходимый уровень обслуживания. Если рассматривать продукты компании Microsoft, то 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. Протокол TCP/IP является универсальным. Он может использоваться практически в любой ситуации, касающейся передачи данных. Так, он является единственным протоколом, который применяется в Интернете. Что касается локальных сетей, то и в них он показал себя с наилучшей стороны. Конечно, для работы локальной сети могут использоваться любые протоколы передачи данных, но если речь идет о Windows-сетях, то без TCP/IP не обойтись.

На сегодня существует две версии протокола TCP/IP: четвертая и шестая, TCP/IPv4 и TCP/IPv6 соответственно. Различие между этими протоколами заключается в разном принципе адресации и, соответственно, в функциональности.

Шестая версия протокола появилась, когда стало понятно, что 32 бит явно недостаточно для того, чтобы обеспечить адресами все устройства, которые в этом нуждаются, и было решено перейти на 128-битную адресацию. Однако внедрение TCP/IPv6 заняло больше времени, чем предполагалось, поэтому сегодня пока используется старая версия протокола, то есть TCP/IPv4. Именно ее мы и будем рассматривать далее.

В основе работы протокола 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, определить, к какой сети и подсети он относится, и сделать на основании этого необходимые выводы.

Таким образом, под адресацию отводится диапазон адресов 0.0.0.0–255.255.255.255. Если подсчитать, то получается примерно 4 млрд адресов (2554) – не так много, как кажется. Кроме того, не все адреса из этого диапазона адресов доступны для использования. Существуют адреса и даже 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 в использование. Различают три основных класса сети, которые однозначно идентифицируются первым числом в группе чисел IP-адреса, то есть первым байтом адреса. В табл. 14.1 показано, как распределяются адреса в зависимости от класса сети.

Таблица 14.1. 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 количества 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, большая часть контроля была возложена на основных 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 локальных сетей различных типов, как больших, так и малых.

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 означает следующее: 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, наша локальная сеть принадлежит 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. В случае с одной сетью это не приведет к каким-либо негативным результатам, 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 для адресации узлов использует несколько другой, более рациональный способ выдачи адресов, который позволяет применять ровно столько адресов, сколько нужно 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: если рассматривать двоичное представление маски, то на месте адреса узла всегда стоят нули, на месте номера сети – единицы. Пример работы маски подсети приведен в табл. 14.2.

Таблица 14.2. Пример классового и бесклассового способа адресации

Параметр	Значение
IP-адрес:	
в десятичном представлении	129.64.134.5
в двоичном представлении	10000001.01000000.10000110. 00000101
Маска подсети:	
в десятичном представлении	255.255.128.0
в двоичном представлении	11111111.11111111.10000000. 00000000
Номер подсети:	
при классовой адресации	129.64.0.0
при бесклассовой адресации	129.64.128.0
Номер узла:	
при классовой адресации	0.0.134.5
при бесклассовой адресации	0.0.6.5

Как видите, бесклассовый способ адресации 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 становиться понятно, что использование большого количества сегментов очень быстро уменьшает количество адресов для нумерации компьютеров, поэтом злоупотреблять этим не стоит.

На практике почти все локальные сети небольшого размера используют маску подсети 255.255.255.0, что позволяет использовать для адресации узлов адреса из диапазона 192.168.1.1–192.168.1.254.

Рабочая группа

Основное предназначение локальной сети – использование общих ресурсов разного типа: файлов, принтеров и сканеров, хранилищ данных, Интернета и т. д. При этом основная задача – дать пользователю ровно столько, сколько ему нужно, и только то, что он может иметь. 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 компьютеров «чужой» рабочей группы. Однако в этом случае уровень доверия к компьютерам будет совсем другим, чем к компьютерам из одной рабочей группы.

Использование рабочей группы имеет преимущества, однозначно влияющие на ее выбор:

□ не нужно тратиться на покупку дополнительного оборудования;

□ нет необходимости в дополнительном программном обеспечении;

□ в большинстве случаев не требуется наличие системного администратора, следящего за порядком в локальной сети.

Кроме всего прочего, каждый конкретный пользователь является «сам себе администратором», 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 решаете, когда, как и сколько вы хотите находиться в той или иной рабочей группе.

Рабочие группы чаще всего используются в локальных сетях небольших офисов и в «домашних» локальних сетях. Основная причина этого – экономия денежных средств, которая заставляет отказаться от управляющих компьютеров. Однако рабочая группа более чем из 24 компьютеров – это парадокс.

Если же речь идет о локальной сети достаточно большой организации, то в этом случае гораздо разумнее будет использовать другой механизм – доменную структуру.

Доменная структура

Доменную структуру сети можно назвать цивилизованным способом организации работы локальной сети, к которому должен стремиться каждый администратор, создающий локальные сети.

Данный способ подразумевает наличие в локальной сети специализированного, выделенного компьютера – сервера, который занимается исключительно обслуживанием работы сети. В идеальном случае количество управляющих серверов не меньше двух, что позволяет обеспечить функционирование сети в случае выхода из строя основного сервера.

Управляющий сервер называется *контроллером домена.* Его единственная задача – управление сетью. Часто встречается ситуация, когда контроллер домена решает дополнительные задач, например выступает в качестве файлового сервера. Подобное положение вещей является крайне нежелательным, поскольку не только усложняет обслуживание сервера, но и делает сеть более подверженной риску выхода сервера из строя.

Под нужды будущего контроллера домена выделяется мощный компьютер, обладающий производительной дисковой подсистемой, мощным процессором и большим объемом оперативной памяти. На него устанавливается серверная операционная система, специально предназначенная для таких случаев.

Как уже упоминалось ранее, серверная операционная система содержит в себе целый ряд инструментов, с помощью которых осуществляется администрирование локальной сети. К ним относятся Active Directory, DNS– и DHCP-сервер, хранилище сертификатов и т. д.

Использование доменной структуры имеет ряд преимуществ, среди которых:

□ контролируемое подключение к локальной сети путем использования учетной записи пользователя;

□ полный контроль над участниками сети;

□ мощная система управления правами доступа;

□ контролируемая организация доступа к общим ресурсам;

□ система архивирования;

□ настраиваемые политики работы в локальной сети;

□ автоматическая установка необходимых пакетов обновления системы и программных продуктов;

□ корпоративная антивирусная защита локальной сети.

Поскольку контроллер домена является центральным компонентом локальной сети, от которого зависит работа всей локальной сети, обеспечение его работоспособности – важнейшая задача системного администратора. Именно он должен позаботиться о том, что бы настроить резервный сервер, который сможет выполнять все функции контроллера домена в случае, если с ним что-то произойдет. При наличии резервного компьютера он получает название вторичного контроллера домена, а основной сервер – первичного контроллера домена или основного контроллера домена.

DNS

Поскольку локальная сеть является частным случаем глобальной сети, то она должна придерживаться такого же принципа организации доступа к данным, как это происходит в глобальных сетях. Если отступить от этих принципов, то может возникнуть ситуация, когда функционирование сети будет 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.

Выше мы упомянули про Интернет. Стоит объяснить, почему это так важно для локальной сети. Вспомните, каким образом вы просматриваете веб-ресурсы? Правильно, для этого вы используется URL – строку с адресом веб-ресурса, например www.google.ru или www.yandex.ru. Но какое отношение имеет эта строка к принятой системе IP-адресации? На самом деле для доступа к указанным сайтам мы должны были бы использовать адреса 74.125.87.99 и 87.250.251.11 соответственно. Согласитесь, не очень удобно запоминать цифры вместо понятного и простого адреса.

Вот мы и подошли к объяснению нужного нам понятия. 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. Для обеспечения ее актуальности применяется система, позволяющая синхронизировать данные на DNS-серверах Интернета.

DNS-сервер, кроме транслирования IP-адресов для Интернета, выполняет аналогичную работу и для локальной сети, поскольку в локальной сети также могут существовать веб-ресурсы локального использования или, например, применяться почтовый сервер.

Как уже упоминалось выше, для обеспечения актуальности базы данных DNS существует достаточно разветвленная сеть DNS-серверов, которые постоянно взаимодействуют между собой, придерживаясь при этом определенной иерархии.

Принцип данной иерархии заключается в следующем. Предположим, пользователь локальной сети 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 соответствующего 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 по прошествии сравнительно небольшого интервала времени о регистрации ресурса узнают все DNS-серверы, и он становится доступным для просмотра браузером или другой программой.

DNS-сервер, как правило, настраивается как дополнительный сервис на контроллере домена и его дублирующих системах. Это позволяет быстро получать нужную информацию, даже если первичный контроллер домена выйдет из строя.

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

Исходя из стратегии TCP/IP-подхода, 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 применение TCP/IP-протокола является обязательным, а значит, обязательной является и IP-адресация.

Представьте себе локальную сеть, состоящую из сотни компьютеров, десятка сетевых принтеров и десятка управляемых коммутаторов и маршрутизаторов – типичный пример локальной сети уровня достаточно большой организации, расположившейся на 2–3 этажах высотного здания. Вы являетесь системным администратором локальной сети доменной структуры, управляемой операционной системой Windows Server 2008, которая только что была создана и требует проведения необходимой настройки, чтобы можно было начать работу.

Вам в одиночку за два часа необходимо выполнить достаточно большой объем работы. Проведя предварительные расчеты, вы понимаете, что за эти два часа вам нужно осуществить IP-адресацию доброй полторы сотни оборудования разного характера. Но, к счастью, существует такой механизм, как DHCP-сервер, который вы не забыли настроить на контроллере домена, поэтому вам остается всего ничего – пройтись по двум десяткам устройств и настроить только нужные IP-адреса.

Прежде чем описать принцип работы DHCP-сервера, стоит немного рассказать о принципе раздачи IP-адресов. Представьте себе участника локальной сети, только на этот раз не системного администратора, а обычного пользователя, который ничего не знает о принципах функционирования сети. У него есть только одно требование – он должен войти в сеть и начать работу со своими офисными документами. Разве ему интересно будет знать, какой у него IP-адрес и нужен ли он ему вообще?

При этом в локальной сети применяется контроллер домена, есть файловый сервер, интернет-шлюз, сервер «1С:Предприятие» и другие важные компьютеры, доступ к которым должен быть постоянным, независимо от того, где они находятся сегодня или будут находиться завтра.

В итоге получаем два списка оборудования разной важности. Логично предположить, что в первую очередь необходимо настроить IP-адреса важного оборудования, а уж потом при необходимости можно приступить к настройке всего остального оборудования.

Наверное, вы уже поняли, о чем идет речь. Дело в том, что существуют узлы, которым IP-адрес нужен или положен по «долгу службы», а также узлы, которым он безразличен, но все же нужен, чтобы не отступать от правил.

Теперь можно вернуться к принципу работы DHCP-сервера.

DHCP-сервер позволяет осуществлять *статическую* и *динамическую* IP-адресацию. Таким образом, если продолжать тему нашего рассказа, важное оборудование должно получить статические IP-адреса, а все остальные могут довольствоваться динамическими IP-адресами. Благодаря такому подходу наш администратор отлично уложится в выделенные ему два часа – ему нужно будет только правильно настроить DHCP-сервер.

Использование динамических адресов оправдано в любом случае, поскольку позволяет значительно ускорить процесс подключения существующих или новых рабочих мест в сети: достаточно подключить сетевой кабель и настроить компьютер на работу в составе домена.

Active Directory

Если разговор заходит о механизме Active Directory, это означает, что речь идет о локальной сети с доменной структурой, поскольку без Active Directory в данном случае просто не обойтись.

Active Directory является основным инструментом администрирования всего, что связано с работой локальной сети: учетных записей пользователей и компьютеров, работы сетевых принтеров, прав доступа к общим ресурсам, политики безопасности и многого другого.

Active Directory состоит из нескольких отдельных механизмов. Каждый из них отвечает за настройку определенных объектов, которые можно разделить по функциональности и назначению. Данный механизм присутствует в любой серверной операционной системе, которая устанавливается на управляющий сервер. Кроме того, именно с помощью одного из механизмов Active Directory происходит настройка ролей сервера, в частности создание контроллера домена, установка DNS-и DHCP-серверов и т. д.

Когда контроллер домена создан, Active Directory является наиболее используемым инструментом, поскольку без его участия невозможно создание и управление учетными записями пользователей, добавление их в группы, настройка профилей пользователей и т. п.

SSID

Понятие SSID тесно связано с функционированием беспроводных локальных сетей. К проводным сетям оно отношения не имеет.

SSID (Service Set Identifier, идентификатор беспроводной сети) – это не что иное, как имя сети, которое идентифицирует беспроводную сеть и позволяет выделить ее из других сетей, которые могут работать по соседству. Идентификатор сети представляет собой любой набор латинских букв, знаков и цифр длиной не более 32 бита, например **my_name_is_earl**.

Данная последовательность символов играет важную роль. Ее должен знать каждый, кто хочет подключиться к беспроводной сети. Конечно, знание только одного SSID не является достаточным для подключения, однако он необходим для настройки беспроводного оборудования. Например, обычно 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, его знание необходимо.

Глава 15
Сетевое оборудование

□ Активное оборудование
□ Пассивное оборудование

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

□ топология сети;
□ тип среды передачи данных;
□ 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. Его задача – обработать получившие данные согласно требованиям физического уровня модели ISO.

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 преобразует поступившие от компьютера данные в электрический сигнал и отправляет его каналу, используемому для передачи данных. В режиме получения данных он выполняет противоположное действие: преобразует электрические сигналы в данные и передает их протоколам верхнего уровня.

Главное различие сетевых адаптеров, не учитывая конструктивные особенности, – 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 исполнения 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 и 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 минула эта участь и сетевые адаптеры. Мало того, часто USB-порт становится

единственным способом подключения дополнительных устройств. Часто для подключения адаптера используется удлинительный USB-шнур. Кроме варианта с USB-подключением, нередко встречаются адаптеры, которые с помощью удлинительного шнура подключаются к FireWire-порту на материнской плате или дополнительном FireWire-контроллере.

□ **Интегрированный адаптер.** Данный вариант сетевого адаптера получил, пожалуй, наибольшее распространение. Причиной тому стал ATX-стандарт материнских плат, который предусматривает использование интегрированных решений. Однако этот стандарт подразумевает присутствие только сетевого адаптера стандарта 100Base-TX или ему подобного. Правда, иногда встречаются материнские платы, которые содержат интегрированный беспроводный контроллер стандарта IEEE 802.11b или IEEE 802.11g.

Как уже было упомянуто выше, внешний вид адаптера, а именно присутствие того или иного вида порта, зависит от 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. 15.1.

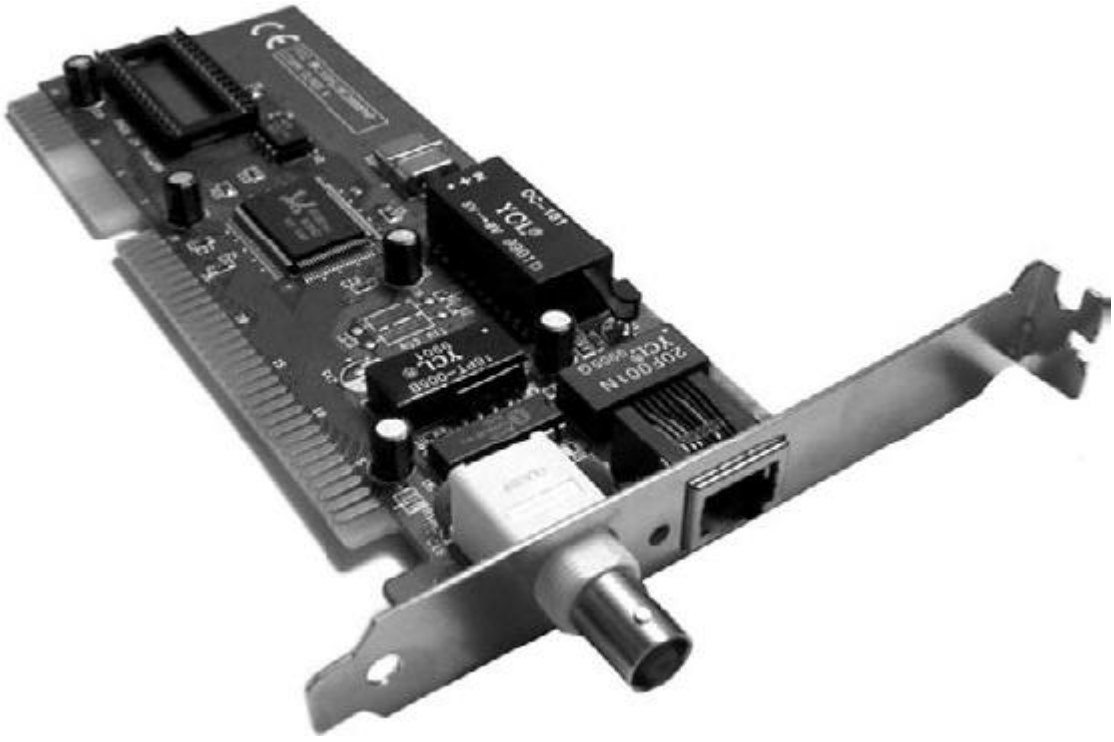

Рис. 15.1. Сетевой адаптер для коаксиальных стандартов

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. 15.2, а в USB-варианте – на рис. 15.3.

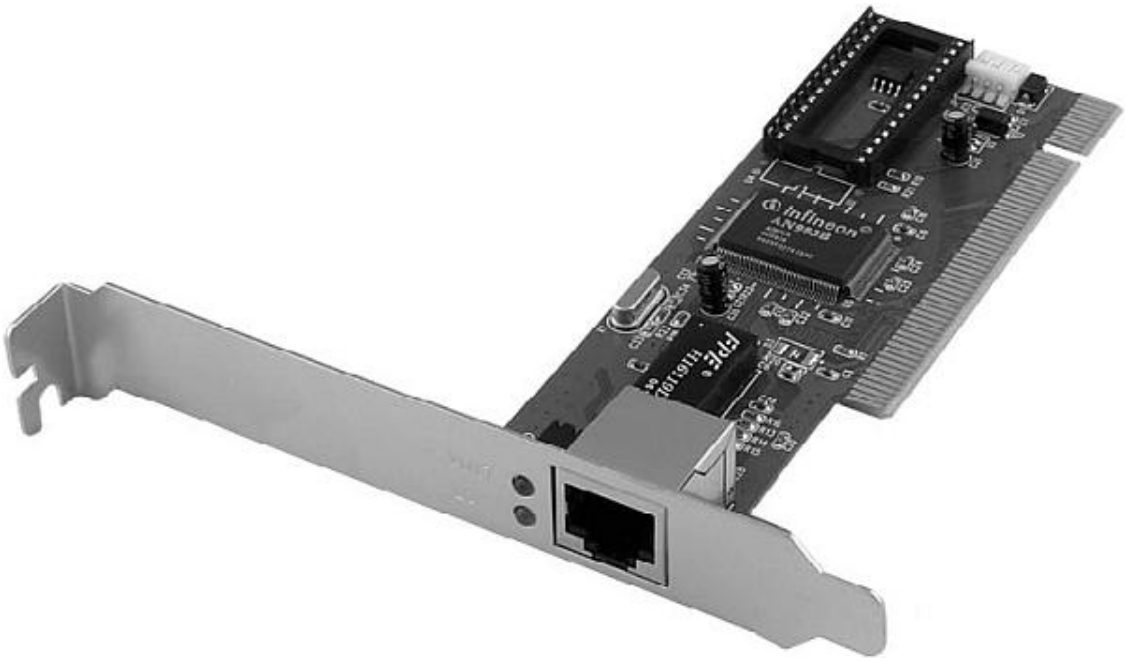

Рис. 15.2. Сетевой адаптер в виде платы расширения для кабеля «витая пара»

Рис. 15.3. Сетевой адаптер стандарта 100Base-TX в USB-исполнении

Несколько иначе выглядят сетевые адаптеры, предназначенные для работы со стандартами HomePNA (рис. 15.4) и HomePlug (рис. 15.5).

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

Рис. 154. Сетевой адаптер стандарта HomePNA

Рис. 15.5. Сетевой адаптер стандарта HomePlug

Особняком стоят адаптеры, предназначенные для установки в переносные компьютеры. Как правило, адаптеры подобного рода изначально снабжаются максимальным количеством устройств всевозможных видов связи. Однако если среди них отсутствует сетевой адаптер нужного типа, всегда можно воспользоваться PCMCIA-разъемом (рис. 15.6), который предназначен именно для таких случаев.

Рис. 15.6. Сетевой адаптер для установки в PCMCIA-порт

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, – наличие 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. 15.7).

Рис. 15.7. Сетевой беспроводной адаптер с одной приемопередающей антенной

Что касается беспроводных адаптеров стандарта IEEE 802.11n, то особенности его использования подразумевают наличие двух, иногда трех антенн (рис. 15.8).

Рис. 15.8. Сетевой беспроводной адаптер с несколькими антеннами

Большая часть беспроводных адаптеров позволяет использовать антенны с разным уровнем усиления, поэтому стандартные антенны, идущие в комплекте с сетевым адаптером, можно заменять антеннами с большим 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 протяженности 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. Его непосредственным заданием является распространение поступившего по одному из портов сигнала на все остальные порты. При этом для него абсолютно неважно, какого типа данные передаются и кому: в любом случае данные транслируются сразу на все порты, что увеличи-

вает трафик в сети, уменьшая тем самым полезную скорость. В связи с этим использование концентратора как центрального устройства оправдано лишь в небольших сетях. В сетях с количеством подключений более 12–14 желательно использовать более интеллектуальное устройство, например коммутатор.

Концентратор представляет собой устройство, содержащее определенное парное количество портов, как правило, не более 24 (рис. 15.9).

Рис. 15.9. Внешний вид концентратора

При этом, как правило, на передней панели коммутатора находятся светодиоды, отображающие активность портов.

Чаще всего встречаются концентраторы, предназначенные для использования с кабелем «витая пара», то есть содержащие порты RJ-45. Однако бывают также концентраторы, которые в дополнение к портам RJ-45 имеют один порт с BNC-коннектором. Это 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, который 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.

Мост является более интеллектуальным устройством, чем коммутатор. 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. 15.10). В последнее время мост как отдельное оборудование используется достаточно редко, поскольку практически любой коммутатор может выполнять аналогичные функции.

Рис. 15.10. Сетевой мост

Коммутатор

Коммутатор (свитч) – основное устройство активного типа, применяемое в качестве центрального узла для подключения компьютеров в сетях, основанных на топологии «звезда». Его ближайшим по функциональности, но не по «интеллекту» устройством является концентратор, который еще не так давно в силу своей меньшей стоимости получил более широкое распространение.

Большей, чем у концентратора, функциональности коммутатор обязан протоколам, работающим на канальном уровне. Это позволяет избежать лишнего трафика, когда необходимо передать данные от отправителя конкретному компьютеру, не затрагивая при этом остальные компьютеры. За счет этого достигается высокая скорость передачи данных.

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-адрес каждого компьютера, подключенного к его портам, 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 (как правило, не более 48) портов RJ-45 (рис. 15.11).

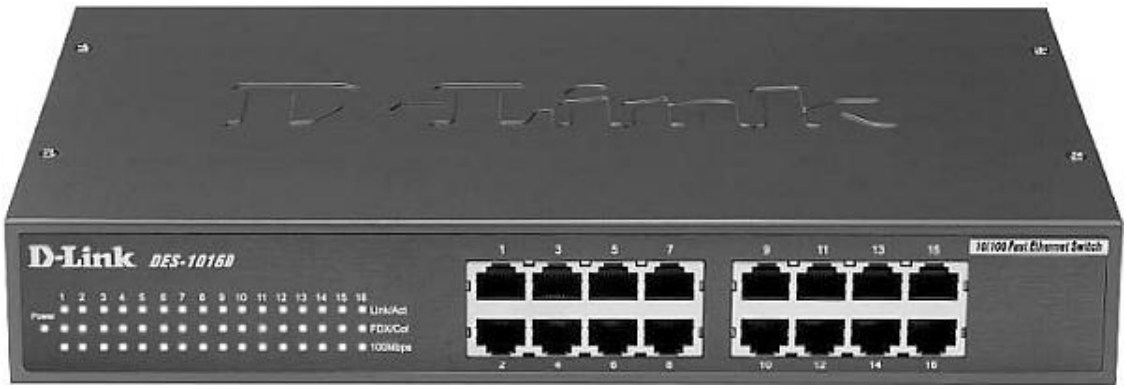

Рис. 15.11. Внешний вид коммутатора

Как и в случае с концентраторами, часто встречаются стоечные коммутаторы, предназначенные для установки в монтажный шкаф. При этом стоечные коммутаторы обычно

можно соединять. Для этого используется либо отдельный RJ-45 порт на задней панели, либо один из свободных портов на передней панели.

Еще одним плюсом коммутаторов является возможность управления. Так, 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 коммутатор снабжается статическим IP-адресом, который при необходимости всегда можно изменить.

Маршрутизатор

Маршрутизатор (роутер) – еще один представитель активного оборудования, который играет роль центрального узла в случае использования топологии «звезда» или комбинированной топологии. По свои возможностям он является наиболее «интеллектуальным» и может делать все, что выполняют концентратор, мост и коммутатор вместе взятые. А кроме того, 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 тем более 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, которой 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.

Поскольку маршрутизатор является очень ценным устройством для локальной сети, он обычно позволяет управлять собой, для чего может использоваться либо веб-интерфейс с доступом по определенному IP-адресу, либо один из управляемых портов.

Внешний вид маршрутизатора мало чем отличается от коммутатора и концентратора, поэтому многие часто путают их (рис. 15.12).

Рис. 15.12. Внешний вид маршрутизатора

Как правило, маршрутизатор содержит от 16 до 64 портов и обязательно поддерживает возможность установки в стойку монтажного шкафа. Маршрутизатор с 8 портами встречается достаточно редко, и причиной является высокая цена маршрутизатора вообще. Поэтому когда речь идет о приобретении маршрутизатора, то многие предпочитают приобретать устройство с 16 и более портами – так сказать, про запас.

Точка доступа

Точка доступа (Access Point) – представитель активного типа устройств, необходимых для объединения компьютеров в беспроводную сеть. Его 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 поддержка работы DNS– и DHCP-серверов, что позволяет строить 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 аутентификации пользователей.

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 оборудуется как минимум одним портом RJ-45, посредством которого она подключается к сетевому адаптеру компьютера. Далее, применяя веб-интерфейс или программное обеспечение, идущее в комплекте с точкой доступа, пользователь имеет возможность настраивать необходимые параметры работы точки доступа.

Внешний вид точки доступа зависит от некоторых факторов.

□ Наличие дополнительных портов RJ-45. Достаточно часто точка доступа является тем средство, которое позволяет объединить в одну сеть как беспроводных, так и проводных клиентов. В связи с этим для подключения последних используют порты RJ-45 стандарта

100Base-TX или подобного. Количество этих портов может быть разным, но обычно их не более четырех.

□ Количество и мощность антенн. Различные сетевые стандарты подразумевают использование разного количества антенн, поэтому на точке доступа их будет столько, сколько это предусмотрено стандартом (рис. 15.13).

Однако часто встречаются точки доступа, которые содержат дополнительную антенну, что позволяет сделать покрытие сети более широким и увеличить уровень сигнала. Кроме того, некоторые точки доступа позволяют подключать внешнюю антенну, для чего оборудуются соответствующим гнездом либо делают стандартную антенну съемной, и на ее место можно вкрутить антенну с большим коэффициентом усиления.

□ Средства индикации. На передней панели точки доступа всегда присутствует определенное количество светодиодов, которые сигнализируют о переходе точки доступа в тот или иной режим, а также отображают активность дополнительных портов. Количество средств индикации напрямую зависит как от функциональных возможностей точки доступа, так и от количества дополнительных портов на задней панели.

□ Тип 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 различаются вид и материал корпуса. Могут быть и другие отличия, например в наличии портов и креплений для громо– и грозозащиты, портов для подключения внешней антенны, питания и т. п.

Рис. 15.13. Внешний вид точки доступа

Модем

Модем – активное оборудование, предназначенное для соединения двух удаленных точек, например компьютеров или сегментов сети. 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 (цифро-аналоговые 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 аналогово-цифрового модема (рис. 15.14) обмен информацией происходит по обычной телефонной линии в диапазоне частот 300–3400 Гц.

Рис. 15.14. Внешний аналогово-цифровой модем

Преобразование аналогового сигнала осуществляется достаточно просто: с определенной частотой измеряются его характеристики и записываются в цифровой форме по определенному алгоритму. В обратной последовательности идет преобразование цифровой информации.

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 случае с персональным компьютером это слот PCI или PCI Express, в случае с переносными устройствами – слот PCMCIA.

В зависимости от типа модема и среды передачи данных различается скорость их передачи. Скорость обычного цифрово-аналогового модема, работающего с телефонной аналоговой линией, равна 33,6–56 Кбит/с. Кроме того, широкое распространение получили ADSL-модемы (рис. 15.15), которые используются для организации скоростного подключения к Интернету.

Рис. 15.15. Внешний ADSL-модем

Скорость передачи данных у таких модемов обычно находится в пределах 1–8 Мбит/с, но теоретически возможна скорость выше 20 Мбит/с.

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

Антенна

В беспроводной сети антенна имеет большое значение, особенно если к ней подключено активное сетевое оборудование, например точка доступа, концентратор, маршрутизатор и т. д. Хорошая антенна позволяет сети работать с максимальной отдачей, достигая при этом своих теоретических пределов дальности сигнала и скорости передачи данных.

Антенны бывают всенаправленные (рис. 15.16) и узконаправленные (рис. 15.17), а также различаются вариантом их использования: внутри здания или на открытом воздухе.

Рис. 15.16. Всенаправленная антенна

Кроме того, основным показателем возможностей антенны является ее коэффициент усиления сигнала. Например, узконаправленная антенна позволяет достичь большего радиуса сети, что используют, когда необходимо соединить два удаленных сегмента беспроводной сети. Всенаправленная антенна распространяет сигнал вокруг себя, что дает возможность другим устройством, установленным рядом, взаимодействовать друг с другом. Однако, учитывая особенности распространения сигнала, ожидать от такого способа особых результатов не приходится. Использование антенны с б**о**льшим коэффициентом усиления позволяет увеличить радиус сети и, соответственно, уровня сигнала, особенно на дальних точках подключения.

Рис. 15.17. Узконаправленная антенна

Пассивное оборудование

Оборудование, которое также присутствует при передаче данных, но принимает в этом лишь пассивное участие, называется *пассивным*. Сюда относятся монтажные шкафы, распределительные панели, сетевые розетки, кабель, коннекторы и т. д. К этой группе можно также отнести 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 большую 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 также устанавливать серверы стоечного типа, блоки бесперебойного питания, KVM-переключатели (для вывода изображения с серверов на один монитор) и т. д.

Существуют разные варианты монтажных шкафов, различающиеся в основном только двумя показателями – типом исполнения (напольный, 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 исполнение подбираются исходя из количества компьютеров в сети и количества оборудования, которое планирует установить в шкаф. Если в сети подключено 30–40 компьютеров, то вполне достаточным будет использование подвесного варианта шкафа (рис. 15.18).

Рис. 15.18. Монтажный шкаф подвесного исполнения

Если же в сети насчитывается большее количество компьютеров или решено использовать серверы стоечного типа, то стоит остановить свой выбор на напольном варианте исполнения с размерами, которые не только позволят поместить все необходимое оборудование,

но и дадут возможность установить его в серверной или другой комнате, обеспечив к нему свободный доступ (рис. 15.19).

Чтобы дать доступ к оборудованию и кабельной системе, монтажный шкаф оборудуется как минимум одной дверкой из стекла. Это вполне оправданное решение, поскольку позволяет визуально контролировать оборудование, 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 определенного размера, что зависит от размеров самого монтажного шкафа.

Рис. 15.19. Монтажный шкаф настенного исполнения

Основное предназначение кросс-панели – обеспечение удобного способа монтажа кабеля в контактных площадках разъемов с последующим соединением этих разъемов с портами на активном сетевом оборудовании установленном в монтажном шкафу.

Внешний вид кросс-панели зависит от количества и типа портов, которые располагаются на ее передней панели, а также 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 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. 15.20).

Для облегчения монтажа кабеля и создания необходимой проектной документации каждый порт на кросс-панели пронумерован. Кроме того, рядом с портом обычно находится специальный участок, на котором маркером можно сделать любую нужную короткую запись.

Рис. 15.20. Кросс-панель

На задней панели кросс-панели находится система разводки портов, то есть непосредственно контактные площадки портов, которые используются для зажима в них проводников кабеля или монтажа оптоволоконных жил. Каждый порт снабжается фиксирующим устройством или скобами, позволяющими закрепить кабель, который идет к конкретному порту. Присутствует также общая система фиксирования, позволяющая зафиксировать 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. Существует несколько типов кабелей, основными из которых являются «витая пара», коаксиальный и оптоволоконный.

Есть разные категории кабеля, каждая из которых имеет свои характеристики и особенности использования. Основными отличительными параметрами являются:

- □ диаметр проводников;
- □ диаметр проводника с изоляцией;
- □ количество проводников (пар);
- □ 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. 5.

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. 15.21).

Рис. 15.21. Патч-корд

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 соединения активного оборудования между собой.

Коннекторы

Когда речь идет о кабеле, используемом для создания проводных вариантов сети, то без коннекторов он не представляет никакой ценности. Именно коннекторы завершают его целостность и позволяют использовать его по назначению – для передачи данных между отправителем и получателем. С помощью коннекторов кабель подключается к нужным разъемам на оборудовании, как активном, так и пассивном.

Тип коннектора описывают существующие 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 на основе коаксиального кабеля. Существует несколько коннекторов BNC-типа, которые различаются свои назначением.

□ BNC-коннектор. Применяется для обжима концов коаксиального кабеля (рис. 15.22).

Рис. 15.22. BNC-коннектор

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. 15.23) похож на обычный BNC-коннектор, но имеет отводы для врезки в центральную магистраль.

Рис. 15.23. Т-коннектор

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

□ I-коннектор. Этот тип коннектора (рис. 15.24), который часто называют барел-коннектором, используется в качестве соединителя сегментов кабеля без применения активного оборудования.

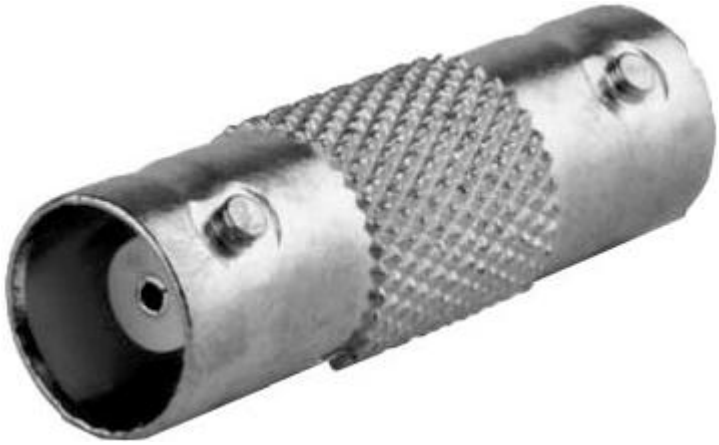

Рис. 15.24. I-коннектор

Соединение сегментов кабеля бывает необходимо, когда появляется разрыв центральной магистрали либо ее отростка или в случае, когда необходимо удлинить кабель.

□ Терминатор (рис. 15.25) представляет собой своего рода заглушку, которая необходима для того, чтобы препятствовать появлению отбитого сигнала.

Рис. 15.25. Терминатор

Такой коннектор устанавливается на обоих концах магистрали, при этом один из теминаторов 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 двух– или четырехжильного телефонного кабеля. Однако, в отличие от него, он шире и содержит в два раза 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. 15.26.

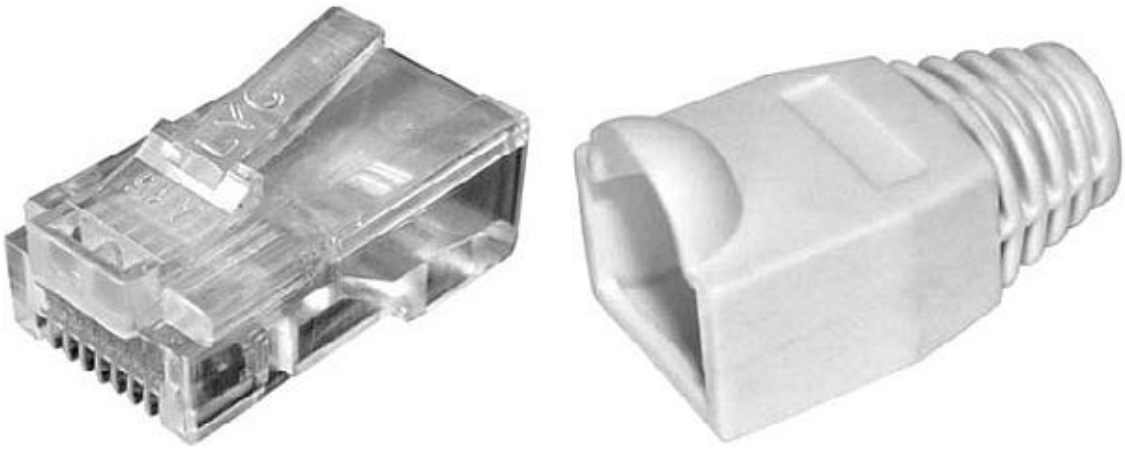

Рис. 15.26. Коннектор RJ-45

Особенностью коннектора является его ограниченный срок службы, что связано с особенностями конструкции и материалом, из которого сделан коннектор. Для фиксации коннектора в разъеме используется пластиковый фиксатор, при поломке которого фиксация коннектора в разъеме становится невозможной. Как правило, стандартным сроком службы этого фиксатора является 2000 подключений.

В паре с коннектором RJ-45, как правило, идет специальный защитный колпачок из мягкого материала, например обрезиненного пластика, который надевается на коннектор и часть кабеля, скрывая и защищая тем самым наиболее уязвимое место – место обжима. Однако его использование не является обязательным, поэтому очень часто, особенно в небольших локальных сетях офисного или домашнего масштаба, в целях экономии денежных средств он не применяется.

Розетка RJ-45

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

Розетки применяются при необходимости. Их выбор критичен только для локальных сетей с большим количеством компьютеров и других устройств. Подобные сети, как правило, обслуживают большие организации, которые могут себе позволить сделать все по правилам, одним из которых является использование сетевых розеток. Применение сетевых розеток делает кабельную систему более устойчивой к разному роду неприятностям в виде обрывов кабеля, пропадания контактов в соединениях и т. д. Что касается небольших офисных сетей или «домашней» сети, чаще всего использование розеток игнорируется. В этом случае компьютеры или другие устройства подключаются напрямую к портам коммутатора.

Внешний вид сетевой розетки зависит от следующих факторов:

□ категории 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 может применять систему крепления проводников с помощью шурупов, в то время как розетка высокой категории использует для этого монтажную контактную площадку;

□ типа розетки и способа ее крепления. Встречаются розетки с внутренним и внешним способами монтажа. Внутренний способ монтажа подразумевает монтаж розетки в монтажной коробке, для которой в стене делается соответствующее отверстие. Внешний вариант монтажа позволяет крепить розетку прямо на стену с помощью шурупов, встраивать ее в сетевой короб или просто приклеивать ее к гладкой поверхности с помощью двухстороннего скотча;

□ наличия дополнительных портов. Часто на розетке присутствуют дополнительные разъемы, например дополнительные RJ-45 или RJ-11, что повышает ее универсальность, позволяя использовать одну конструкцию для обслуживания нескольких устройств.

Внешний вид розетки, предназначенной для крепления на стене, показан на рис. 15.27.

Рис. 15.27. Розетка RJ-45

Инструменты для работы с кабелем

Без соответствующих инструментов произвести качественный обжим коннектора на кабеле или зажим проводников кабеля в контактной площадке очень сложно. Это означает, что качество такой работы будет достаточно низким, что может стать причиной неработоспособности всей сети[5] или отдельного ее сегмента.

Для обжима коннекторов на коаксиальном кабеле и кабеле «витая пара» используются разные инструменты.

Как правило, для работы с коаксиальным кабелем и BNC-коннектором применяется специальный инструмент, включающий в себя резак грубой обрезки и обжимной механизм (рис. 15.28).

Он позволяет ровно обрезать кабель и подготовить его к более ювелирной обрезке и подготовке к обжиму, для чего используется совсем другой инструмент (рис. 15.29).

[5] 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 производится подключение к коммутатору отдельного сегмента сети, неработоспособным будет только этот сегмент.

Рис. 15.28. Инструмент для обжима BNC-коннектора на коаксиальном кабеле

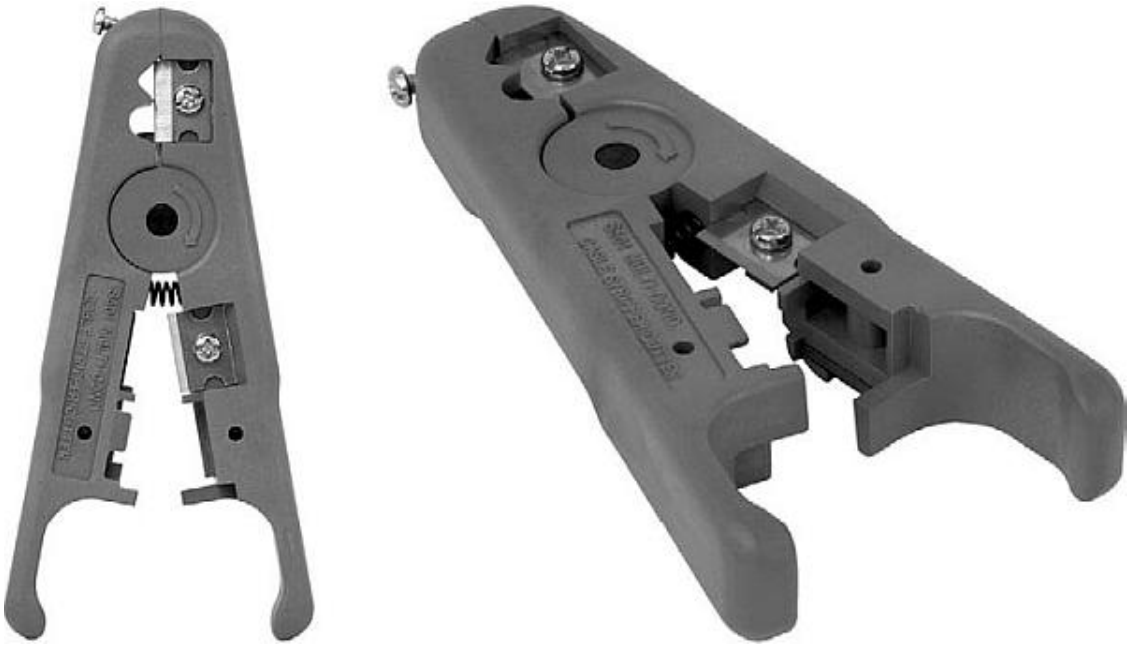

Рис. 15.29. Инструмент для обрезки коаксиального кабеля

С его помощью 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 находится специальный механизм регулировки, отдельно для изоляции и диэлектрика.

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

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

Внешний вид инструмента зависит от его функциональности. Так, некоторые инструменты позволяют также производить обжим коннекторов RJ-11, что делает необходимым наличие соответствующего отверстия на инструменте (рис. 15.30).

Рис. 15.30. Инструмент для обжима кабеля «витая пара»

При монтаже сетевых розеток или зажима проводников на кросс-панели используется специальный нож-вставка (рис. 15.31).

Рис. 15.31. Инструмент для зажима проводников в контактной площадке

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

Часть 2
Проектирование и создание сети

- Выбор и проектирование сети
- Монтаж сети с использованием коаксиального кабеля
- Монтаж сети с использованием кабеля «витая пара»
- Создание беспроводной сети
- Соединение двух компьютеров
- Тестирование и диагностика сети

Глава 16
Выбор и проектирование сети

□ Определение потребностей
□ Выбор сетевого стандарта
□ Проектирование сети

Процесс выбора и проектирования сети – наиболее важный этап в создании локальной сети. От этого выбора зависят все технические возможности будущей сети в дальнейшем, наиболее критичными из которых являются:

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

К выбору сети и особенно к ее проектированию необходимо отнестись очень тщательно. Торопиться не стоит: неудачный выбор не всегда возможно исправить простым путем…

Выбор и проектирование сети в различных случаях происходит по-разному. Так, 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 с гарантированным результатом. Что касается создания локальной сети в пределах небольшой организации, офиса или дома, то вопросом выбора и проектирования сети занимается один-два человека. В случае с офисом или организацией этим, как правило, занимается штатный программист или системный администратор, а в домашних условиях, естественно, сам хозяин или его друзья. Соответственно, денежные затраты на выбор и проектирование сети зависят от задействованных для этого процесса сил.

В любом случае выбор и проектирование локальной сети 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 в выполнении тех или иных задач определяет нужную скорость обмена информации и потребность в соответствующем оборудовании, а значит, и выбор сетевого стандарта.

3. Выбирается оптимальный сетевой стандарт, который будет использован при проектировании и создании сети. Главный показатель выбора сетевого стандарта – скорость передачи данных и ее распределение между участниками, а также возможность расширяемости сети.

4. Создается проект будущей сети и определяется количество и тип оборудования. Чем точнее будет составлен проект, тем точнее можно будет подсчитать количество необходимого оборудования. На данном этапе особое внимание необходимо обратить на пассивное

оборудование, поскольку именно оно влияет на качество, скорость и полноту выполнения работ.

В принципе, ничего сложного в этих заданиях нет, поэтому не стоит отклоняться от этого порядка действий. В противном случае можно попасть в непредвиденную ситуацию, выход из которой будет связан с лишними денежными тратами и нервами. По этой причине далее мы рассмотрим все этапы подробнее.

Определение потребностей

Итак, первый шаг – определение и анализ потребностей всех будущих участников локальной сети.

Сначала необходимо подсчитать количество компьютеров и других устройств, таких как сетевой принтер, которые будут подключены к будущей локальной сети. Это несложно сделать, главное – ничего не упустить. Кроме того, желательно узнать конфигурацию компьютера пользователя – будущего участника сети, а также наличие и тип в нем сетевых адаптеров. Это позволит подсчитать количество сетевых адаптеров нужного типа, когда будет выбран сетевой стандарт будущей сети.

После того как будет подсчитано количество сетевых устройств, необходимо пообщаться с каждым участником будущей сети и с максимальной детальностью узнать, чем конкретно он занимается на компьютере и с какими документами или базами данных работает или хотел бы работать, если появится локальная сеть. Если сеть планируется делать в офисе, кроме потребностей пользователей, обязательно необходимо учесть и требования руководства.

Затем стоит проявить немного фантазии и представить себе, какое еще оборудование и программное обеспечение может понадобиться для обслуживания сети. Например, если вы создаете не «домашнюю» сеть, то желательно обдумать следующие моменты:

□ если будет локальная сеть, значит, почти однозначно потребуется организовывать общий доступ в Интернет;

□ в ведении бухгалтерского учета рано или поздно будет участвовать насколько человек, значит, потребуется общая база данных и программа, которая ею управляет;

□ если фирма будет расширяться, значит, в ней скоро появится юрист, а ему понадобится постоянно обновляемая база юридических данных;

□ возможно сети больше подойдет доменная структура;

□ как нужно будет организовать централизованный источник хранения данных и систему архивирования данных;

□ какой корпоративный антивирусный пакет с автоматическим обновлением баз вирусных сигнатур установить.

Ответы на эти вопросы необходимо зафиксировать в блокноте, и после этого можно приступить к анализу собранной информации.

Ваша задача – более-менее точно подсчитать плановое количество возможных подключений с учетом расширения или добавления разного рода серверов и другого оборудования.

Далее, принимая во внимание полученное количество подключений, нужно приблизительно представить себе трафик, который будет создаваться в сети при использовании имеющегося и предполагаемого в будущем программного обеспечения. Чтобы получить хотя бы приблизительную цифру, можно использовать следующий способ: определите максимальный размер реально документа, с которым работает пользователь, и умножьте его на количество пользователей.

Предположим, максимальный размер документа составляет 300 Кбайт, а в сети планируется работа 30 пользователей. В результате умножения получаем: 30 **x** 300 = = 9000 Кбайт, то есть примерно 9 Мбайт, или 72 Мбит.

Если предположить, что все пользователи одновременно захотят получить доступ к своим документам, то этим действием они создадут трафик 72 Мбит/с. Конечно, подсчет очень приблизительный, сюда еще не включен трафик баз данных, Интернета, пакетов обновления системы, антивирусной проверки клиентов и т. д. Тем не менее на эту цифру вполне можно ориентироваться. Таким образом, можно сделать вывод: чтобы пользователи сети не испытывали неудобств от «соседства» друг с другом, а также могли работать с необходимым набором программного обеспечения, скорость сети должна быть не менее 72 Мбит/с.

Таким образом, если учитывать возможность расширяемости сети, то при выборе сетевого стандарта следует принимать во внимание, что скорость сети должна быть не меньше 72 Мбит/с, а лучше – 100 Мбит/с.

Выбор сетевого стандарта

После тщательного анализа потребностей пользователей следует выбрать сетевой стандарт будущей локальной сети. Если же не производить анализ потребностей, то можно ошибочно остановиться на выборе такого стандарта, который в результате не сможет обеспечить нормальную скорость функционирования сети. И если данный факт обнаружится уже после создания сети, то сделать что-то при используемом типе оборудования может оказаться невозможным.

Имея в руках два основных параметра, полученных в результате предварительного анализа, а именно количество будущих подключений и приблизительный трафик данных, можно приступить к выбору будущего сетевого стандарта.

Итак, в нашем распоряжении есть такие варианты сети, как беспроводная и проводная, а также «реальные» технологии сети – Ethernet, HomePNA, HomePlug.

Как вы уже знаете, каждая из этих технологий сети содержит множество стандартов и спецификаций, которые имеют свои особенности. В табл. 16.1 приведены основные показатели этих стандартов.

Таблица 16.1. Сравнение основных сетевых стандартов

Сетевой стандарт	Среда передачи данных	Скорость передачи данных, Мбит/с	Максимальное количество подключений	Максимальная дальность связи, м
802.11	Радиоволны	2	128	300
802.11a	Радиоволны	54	2048	100
802.11b	Радиоволны	11	2048	300
802.11g	Радиоволны	54	2048	300
802.11n	Радиоволны	300	2048	450
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
Bluetooth 3.0	Радиоволны	24	8	100
HomePNA 3.1	Телефонная проводка, коаксиальный кабель	320	64	600
HomePlug AV	Электропроводка	200	64	300

Как видите, сетевые стандарты даже у разных по принципу работы сетей имеют достаточно неплохие технические показатели. Конечно, часть стандартов, предлагающих низкую скорость передачи данных и малое количество поддерживаемых узлов, смело можно откинуть, поскольку современные требования просто лишают их будущего. Среди них:

□ коаксиальные стандарты 10Base-5, 10Base-2 и 10Base-T;

□ стандарты со скоростью передачи данных ниже 54 Мбит/с: 10Base-T, 10Base-F, IEEE 802.11, IEEE 802.11b, Bluetooth 3.0.

Далее на выбор стандарта однозначно влияет месторасположение локальной сети. Так, для достаточно большой офисной сети качество работы является более критичным, нежели качество работы домашней сети. И это вполне объяснимо: от работоспособности сети и выполнения поставленных задач в полном объеме зависит зарплата работников офиса и развитие самого офиса. Именно поэтому офису нужно локальная сеть, скорость передачи в которой является стабильной и в максимально большой мере независимой от каких-либо факторов. Если принять во внимание подобные суждение, можно дополнительно откинуть в сторону наиболее медленный беспроводный стандарт, а также экзотические стандарты, которые предполагают деление общей скорости между всеми участниками сети, что при большом их количестве приводит к значительному снижению скорости.

С помощью таких простых и логичных рассуждений мы легко можем распределить оставшиеся сетевые стандарты согласно разным случаям и вариантам использования локальной сети (табл. 16.2).

Таблица 16.2. Варианты использования сетевых стандартов в локальных сетях

Вариант локальной сети	Сетевой стандарт
Офисная сеть, в составе которой до 5 компьютеров, 1 сервер базы данных, 1 сетевой принтер	802.11g, 802.11n, 100Base-TX, HomePNA 3.1, HomePlug AV
Офисная сеть, в составе которой 5–10 компьютеров, 1 сервер базы данных, 1 файловый сервер, 1 сетевой принтер	802.11g, 802.11n, 100Base-TX, HomePNA 3.1, HomePlug AV
Офисная сеть, в составе которой 10–20 компьютеров, 1 управляющий сервер, 1 файловый сервер, 2 сервера баз данных, 2 сетевых принтера	100Base-TX, 1000Base-T
Корпоративная сеть, в составе которой 30–50 компьютеров, 2 управляющих сервера, 1 файловый сервер, интернет-шлюз, почтовый сервер, 2 сервера баз данных, 5 сетевых принтеров, ADSL-модем	100Base-TX, 1000Base-T
Корпоративная сеть в двух удаленных зданиях, в составе которой 50–150 компьютеров, 2 управляющих сервера, 1 файловый сервер, 1 терминальный сервер, интернет-шлюз, почтовый сервер, 3 сервера баз данных, 10 сетевых принтеров, ADSL-модем	100Base-TX, 100Base-FX, 1000Base-T
Корпоративная сеть, в составе которой более 200 компьютеров	100Base-FX, 1000Base-T
Два компьютера на незначительном удалении друг от друга, в пределах прямой видимости	802.11g, 802.11n, 100Base-TX, HomePNA 3.1, HomePlug AV, Bluetooth 3.0, другие способы соединения
Сеть в квартире или 1–2-этажном доме из 2–3 компьютеров	802.11g, 802.11n, 100Base-TX, HomePNA 3.1, HomePlug AV
«Домашняя» сеть, любое количество компьютеров	Любое сочетание стандартов

Стоит сказать, что наиболее прогнозируемой и предпочтительной для офиса является сеть с использованием одного из проводных стандартов, в качестве которого чаще всего выступает 100Base-TX, а иногда и 1000Base-T. Если же требуется максимальная мобильность, лучше остановиться на беспроводном стандарте IEEE 802.11n. При небольшом количестве компьютеров также очень неплохой альтернативой другим вариантам сети является сеть с использованием стандарта HomePlug AV.

Проектирование сети

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

Проект локальной сети представляет собой чертеж на листе бумаги, который отображает реальное расположение узлов пассивного оборудования сети относительно имеющегося плана помещения (комнаты), в котором будет создаваться сеть. При этом чем точнее будет чертеж, тем правильнее можно будет рассчитать необходимое количество расходных материалов.

Проект сети очень сильно зависит от того, какая среда передачи данных будет использоваться – проводная или беспроводная, а также от того, где сеть будет располагаться и для чего будет использоваться. Так, если планируется создание сети в квартире или небольшой сети в офисе, то в проекте вообще нет смысла. Если же речь идет о сети с количеством компьютеров более десяти, то проект крайне необходим.

Проектирование беспроводной сети

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 клиентских компьютеров.

При серьезном подходе для этого используется специальное оборудование, которое позволяет определить траекторию и радиус распространения сигнала 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 сигналом.

Однако поскольку беспроводная сеть часто представляет собой небольшую офисную или домашнюю сеть в пределах одного-двух помещений, использование данного метода поиска оптимального местоположения точки доступа неоправданно и не имеет особого смысла.

Итак, главная задача – определить оптимальное расположение точки доступа. Это можно сделать с помощью ноутбука или другого переносного устройства, оборудованного беспроводным адаптером, следующим образом.

1. Установите ноутбук в место, где размещается наиболее удаленный компьютер.
2. Включите точку доступа и расположите 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 доступа.
6. Если после прохождения всех мест расположения компьютеров в некоторых из них все же нет сигнала достаточного уровня либо связь постоянно обрывается, 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. Если в процессе поиска оптимального размещения точки доступа некоторые компьютеры были исключены из списка, необходимо задействовать еще одну точку доступа, установив ее в центре пересечения исключенных устройств и первой точки доступа. После этого, используя приведенный алгоритм, нужно найти оптимальное расположение дополнительной точки доступа.

Проектирование проводной сети

В отличие от беспроводной сети, проводная Ethernet-сеть требует более серьезной подготовки перед созданием. Причиной всему является используемая среда передачи данных, в роли которой выступают кабели разных типов.

Проект для проводной среды создается не столько для указания мест размещения компьютеров и другого активного оборудования, сколько для обозначения места и вариантов размещения пассивного оборудования – кабеля, сетевых розеток, монтажного шкафа и т. п. Именно от этого зависит правильность подсчета количества кабеля, розеток, коробов и других расходных материалов, необходимых для прокладывания локальной сети. Активное

оборудование, конечно, также играет значимую роль, и места его будущего расположения тоже важны.

Наиболее важным моментом при проектировании локальной сети является информация о ее топология. Именно от нее зависит количество и способ прокладки кабеля, а соответственно – расположение сетевых устройств. Так, использование топологии «шина» предполагает один способ прокладки и отвода кабеля от центральной магистрали, а топологии «звезда» – совсем другой. Первый проект получается гораздо проще второго, но зато сеть, построенная с применением топологии «звезда», гораздо гибче и функциональнее сети, выполненной по топологии «шина».

В качестве примера рассмотрим 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 впоследствии подключается к сети с другой топологией.

Использование коаксиального кабеля в качестве среды передачи данных делает проектирование сети достаточно простым. Подобного рода сеть подразумевает применение одной центральной магистрали, от которой в сторону компьютеров или других устройств делается отвод. По этой причине главный вопрос, который необходимо решить, – где можно проложить центральный кабель, чтобы это оказалось оптимальным для подключения компьютеров.

В связи с этим существует два подхода прокладывания центрального канала:

□ использовать для подключения компьютеров небольшой длины отводы, 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 является местом подключения отвода к точке. Плюсом такого подхода является возможность достижения теоретического показателя максимальной длины сегмента. Минусом – сам отвод. Создание отводов кабеля предусмотрено только в стандарте с использованием толстого коаксиального кабеля и трансиверов, который на сегодняшний день уже не применяется. При использовании же тонкого коаксиального кабеля создание отводов не приветствуется, но на практике все же иногда применяют отводы длиной 1-2 метра. Даже если отвод получается слишком длинным, всегда можно сделать небольшую петлю, удлинив кабель с помощью I-коннекторов.

Второй вариант прокладывания центрального канала хотя и позволяет осуществлять подключения по правилам, однако подвержен большему риску обрыва центральной магистрали. Это достаточно часто происходит, когда производят перестановку компьютера, не отключив предварительно кабель.

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

Еще одним важным вопросом, который нужно решить, является расположение центральной магистрали. В идеале кабель должен размещаться так, чтобы исключить возможность повреждения или обрыва, электромагнитных наводок, тепло-и гидровлияния и т. п., то есть необходимо обеспечить максимально комфортные условия. Конечно, идеальных условий, особенно учитывая особенности построении помещения и присутствия в нем проводки других кабелей, достичь тяжело. Тем не менее можно найти место, которое удовлетворяет этим условия в максимальной мере.

Как показала практика, одним из оптимальных мест проведения кабеля, в том числе и коаксиального, является район плинтуса или место на небольшом удаления от него над ним. Можно выделить следующие положительные стороны такого размещения:

□ как правило, отсутствует проводка других кабелей, за исключением перпендикулярного канала в направлении снизу или сверху к имеющимся 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 перегородками, в перегородках либо проделываются новые сквозные отверстия, либо используются существующие. Места таких отверстий выбираются исходя из особенностей проводки кабеля или оптимального пути его расположения. Поэтому прежде всего необходимо исследовать расположение компьютеров в комнате и возможность их перестановки. Исходя из этого и выбирается место для межкомнатных отверстий, например параллельно дальней или ближней от входа стене в районе плинтуса.

При проектировании локальной сети необходимо заранее предусмотреть возможность ее расширения, то есть подключения новых рабочих мест. Особенно это критично для сетей на основе коаксиального кабеля, поскольку каждое новое механическое соединение уменьшает надежность сети. В связи с этим также существует два подхода:

□ при прокладке кабеля заранее предусматриваются запасные рабочие места, для чего делаются врезания Т-коннекторов либо выполняются небольшие петли, длины которых будет достаточно для удобного расположения и подключения компьютера. Плюсом этого способа является возможность заранее рассчитать длину центральной магистрали. Минусом – скопление большого количества петель, которые не закреплены и могут вызывать электромагнитные наводки;

□ запасные точки подключения не создаются заранее, а выполняются только тогда, когда действительно необходимо произвести подключение нового рабочего места. В этом случае центральная магистраль с помощью врезки I-коннекторов удлиняется нужной длиной кабеля. Преимущества такого подхода очевидны.

После учета всех нюансов можно переходить непосредственно к составлению проекта на бумажном носителе. Будет очень неплохо, если вы сможете получить реальный проект помещения и, убрав лишние обозначения и пометки, используете его для нанесения своего рисунка.

Если такой возможности нет, можно создать упрощенный вариант проекта помещений, предварительно узнав размеры ключевых объектов, размещение проемов, дверей и окон и их размеры. После этого можно приступать к выполнению изображения.

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 завершение указываются условные обозначения компьютеров с пометками об их важности, а также их нумерация. Она пригодится, когда необходимо будет произвести IP-адресацию или наименование компьютеров.

В принципе, на этом создание проекта завершено. Остается только подсчитать и зафиксировать количество составляющих: сетевых адаптеров, кабеля, коннекторов, коробов и т. д. Именно на этом этапе и важна точность создания рисунка: чем точнее он будет сделан, тем ближе к реальности окажутся расчеты, а значит, и денежные траты. В конце расчетов желательно составить список из необходимого оборудования и расходных материалов и еще раз его проанализировать, чтобы исключить недоразумения, которые могут возникнуть после

создания локальной сети. Например, список необходимого оборудования и расходных материалов для проектирования сети из 30 компьютеров может выглядеть так, как показано в табл. 16.3.

Таблица 16.3. Список оборудования и расходных материалов для сети из 30 компьютеров

Наименование	Единица измерения	Количество
Сетевой адаптер	шт.	30
Кабель	м	150
Терминатор	шт.	2
BNC-коннектор	шт.	58
Т-коннектор	шт.	30
Скобы	шт.	300

Кабель «витая пара». Использование в качестве среды передачи данных кабеля «витая пара» получило наибольшее распространение среди создателей сетей. Есть простое и логичное объяснение этого факта: современные стандарты, подразумевающие применение кабеля «витая пара», позволяют получить локальную сеть с техническими характеристиками, которые полностью удовлетворяют современным потребностям. Кроме того, такая сеть является наиболее приспособленной к расширению без ущерба для скорости передачи данных и остальной функциональности.

Существуют определенные особенности проектирования локальных сетей с применением кабеля «витая пара». Главной причиной этого является использование топологии «звезда», которая подразумевает подключение каждого участника сети с помощью отдельного кабеля и применение как минимум одного управляющего устройства, к которому все эти кабели будут подключаться. Все эти особенности необходимо заранее предусмотреть в процессе проектирования сети.

Первое, с чего необходимо начать проектирование сети, – это определение месторасположения центрального управляющего пункта, будь то монтажный шкаф или отдельный центральный узел. При выделении под центральный пункт отдельной комнаты, которую называют серверной, проектирование сети нужно начинать именно с этой комнаты.

Для небольшого офиса использование монтажного шкафа является неоправданным, поскольку его стоимость может быть равной стоимость монтажа всей сети. В этом случае центральное устройство можно расположить в любом скрытом от глаз месте, к которому будет иметься постоянный доступ. Выбор такого места не является принципиальным, поскольку благодаря максимальной длине сегмента (примерно 200 м) в пределах небольшого помещения можно подключить все рабочие места без особых проблем. В этом случае также не имеет особого смысла использование сетевых розеток: рабочие места подключаются напрямую к центральному узлу. Способ прокладки кабеля в этом случае также некритичен, но если хочется, чтобы прокладка сети вписалась в существующий интерьер помещения, лучше все-таки использовать коробы для скрытия кабеля, тем более что в них можно скрыть и дополнительные кабели.

Если речь идет о достаточно большой сети в пределах нескольких помещений или даже этажей здания, то стоит задуматься об использовании монтажного шкафа, (возможно, даже о его напольном варианте), а также сетевых розеток. Как уже было сказано, начинать проектирование нужно с места расположения монтажного шкафа, но в этом случае необходимо предусмотреть варианты объединения сегментов разных этажей.

Наиболее распространенный вариант – делать межэтажное отверстие в районе расположения монтажного шкафа или использовать для этого существующие межэтажные каналы, которые, как правило, расположены в одном из концов общего для всех комнат коридора. Что касается прокладки кабеля, необходимо учесть что, на определенных участках локальной сети собирается достаточно большое количество сегментов кабелей. Если все эти кабели прокладывать внутри комнат, для этого потребуется использование коробов внушительных объемов, что не добавит красоты интерьеру комнаты. По этой причине чаще всего практикуют следующий способ: центральная магистраль, которая содержит большое количество проходящих мимо сегментов кабелей, прокладывается вне комнат, в общем коридоре, вдоль следования комнат, а в комнату заходит только нужное для подключения имеющихся компьютеров количества кабелей. Входящие кабели также прячутся в короба, но размер этих коробов значительно меньше, и они достаточно просто вписываются в дизайн комнат.

Плюсом данного подхода является то, что ничего не мешает креплению центрального короба. Крепление же меньших по размеру коробов, которые проходят по каждой из комнат, зависит только от размещения коробов в комнате и также не вызывает никаких сложностей.

Особое внимание необходимо обратить на расширяемость сети, то есть возможность подключения дополнительных рабочих мест. Если для небольших офисных сетей этот вопрос не вызывает никакой сложности, то в больших сетях это может стать проблемой. Чтобы избежать использования дополнительного активного оборудования, «раскиданного» в разных местах локальной сети, подключение новых рабочих мест необходимо предусмотреть еще до прокладывания кабеля, что позволяет разместить кабель в тех же коробах. Конечно, предусмотреть, насколько нужно будет расширить сеть через несколько лет, очень тяжело, но можно хотя бы приблизительно определить данный показатель. Для этого достаточно визуально прикинуть, сколько еще компьютеров можно поставить в каждую комнату. Исходя из этих данных и нужно установить дополнительные сетевые розетки с подключением к центральному узлу.

Когда предварительные расчеты будут завершены, следует приступить к нанесению проекта на бумагу. Сначала необходимо нарисовать схему помещений со всеми важными размерами и объектами. После этого указать размещение монтажного узла, нанести кабельную систему с подробным отображением отводов к каждому рабочему месту и указать размещение сетевых розеток с их нумерацией. Завершающий шаг – нанесение условного обозначения рабочих мест и другого оборудования с указанием его важности.

В результате созданный проект должен максимально отображать реальную картину будущей сети. Не бойтесь вносить изменения и оптимизировать проект, путем изменения трасс прохождения сегментов, не трогая при этом расположения рабочих мест. Однако будьте внимательны и не допускайте случаев, когда длина отдельных сегментов превышает максимально допустимую длину, то есть 185 м.

После того как проект сети будет завершен, обязательно составьте список необходимого оборудования и особенно расходных материалов, поскольку именно последние сильно влияют на итоговую стоимость сети. После составления списка распечатайте его и в спокойной обстановке тщательно проанализируйте, чтобы сделать подсчеты более точными.

Пример списка оборудования и расходных материалов для сети с 50 компьютерами, расположенными на 2 этажах, может выглядеть так, как показано в табл. 16.4.

Таблица 16.4. Список оборудования и расходных материалов для сети из 50 компьютеров

Наименование	Единица измерения	Количество
Сетевой адаптер рабочего места	шт.	45
Сетевой адаптер (контроллер домена)	шт.	1
Сетевой адаптер (файловый сервер)	шт.	1
Сетевой адаптер (интернет-шлюз)	шт.	1
Сетевой адаптер (сервер базы данных)	шт.	2
Монтажный шкаф для размещения активного оборудования	шт.	1
Кросс-панель, 32 порта	шт.	2
Коммутатор 100Base-TX, 24 порта	шт.	2
Маршрутизатор 100Base- TX, 16 портов	шт.	1
ADSL-модем для подключения к Интернету	шт.	1
Коннектор RJ-45 с защитными колпачками	шт.	50
Патч-корд для соединения рабочих мест с сетевыми розетками	шт.	50
Кросс-корд для соединения портов кросс-панели и активного оборудования, а также соединения активного оборудования между собой	шт.	53
Сетевые розетки	шт.	50

Кроме того, в данный список еще необходимо включить инструмент для обработки кабеля, короба разного сечения, переходники между коробами, заглушки, монтажные стяжки и т. д.

Глава 17
Монтаж сети с использованием коаксиального кабеля

□ Правила прокладки кабеля
□ Крепление коробов
□ Подготовка кабеля
□ Монтаж разъемов BNC
□ Подключение коннекторов
□ Фиксация коробов

Как вы уже знаете, сеть можно создавать, используя разные варианта кабеля, а также радиоволны. Сеть, построенная с применением сетевых стандартов, в качестве среды передачи у которых используется коаксиальный кабель, является одним из самых первых и простых вариантов сети. Для ее создания используется специальный сетевой коаксиальный кабель, имеющий волновое сопротивление 50 Ом. Кабель может быть различного диаметра, что, в свою очередь, определяется выбранным сетевым стандартом.

При построении сети на основе коаксиального кабеля применяется топология «шина». Это означает, что все компьютеры подключаются к общей магистрали, отводы от которой создаются с помощью специального устройства – Т-коннектора.

Если проводить аналогию с сетью, в основе которой лежит кабель «витая пара», то Т-коннектор играет ту же роль, что и сетевая розетка. И к первому, и ко второму 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 на основе коаксиального кабеля с каждым годом встречается все реже. Происходит это из-за того, что пропускная способность такой сети составляет всего 10 Мбит/с (на практике этот показатель зависит от количества подключенных рабочих мест) и поднять ее производительность невозможно. Однако если вы хотите создать сеть, затратив минимум усилий и финансов, и не предъявляете высоких требований к ее производительности, то сеть на основе коаксиального кабеля подойдет как нельзя лучше.

Правила прокладки кабеля

Использование коаксиального кабеля для монтажа сети имеет достаточно много особенной, что обусловлено спецификацией сетевого стандарта. Например, чтобы подключить рабочее место к коаксиальному кабелю, центральную магистраль необходимо разделить на две части и установить специальный отвод, к которому и происходит подключение компьютера. Наличие подобных отводов уменьшает надежность кабеля, и чем больше будет таких отводов, тем ниже будет физическая устойчивость к обрыву. Данный факт, а также множество других моментов требуют использования 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. По понятным причинам наиболее критичными участками являются места соединения кабеля с коннекторами.

> **Внимание**
>
> Нарушение целостности контактов или обрыв кабеля приводит к нестабильной работе сети или ее полному выходу из строя Обнаружение проблемного места в этом случае может вылиться в достаточно серьезную проблему

Помните о необходимости обеспечения целостности, когда вам придется прокладывать кабель между двумя домами или на открытом пространстве. В таком случае в качестве основы используйте толстую стальную проволоку. После того как проволока натянута и закреплена между стенами домов или другими объектами, с помощью стальных или жестяных хомутиков можно закрепить на ней коаксиальный кабель. Это простое приспособление обеспечит кабельной системе хорошую защиту от обрыва, который может произойти, например, при сильном ветре.

3. Избегайте создания лишних петель кабеля. Каждая лишняя петля кабеля не только уменьшает длину сегмента, но и создает электрические наводки, особенно если лишний кабель хаотично организован или сложен петлями. Если избавиться от петли путем натяжения центрального кабеля нет возможности, 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 BMC-коннекторов используйте I-коннектор.

В результате вы не только уберете лишнюю петлю кабеля, но и при необходимости сможете 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 как следствие – изгиба кабеля. По этой причине, 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 кабеля не должен быть меньше 5 см.

Несоблюдение этого простого правила часто приводит к тому, что кабель получает разного рода повреждения на участке изгиба, что делает его дальнейшее использование невозможным.

5. Избегайте прокладки кабеля возле проводов электропитания и электрощитов. Электрическая проводка является мощнейшим источником 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 протяженный участок электропроводки, то лучше обойти его, проложив кабель ниже или выше этого

участка. Этим вы, конечно, увеличите общую протяженность 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. По этой причине 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, в определенных условиях (постоянная влажность земли, ее минеральный и химический состав и т. д.) она может увеличиться многократно.

Аналогичным образом негативно влияет внешняя окружающая среда 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, например специальные пластиковые коробы или трубы.

Крепление коробов

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

Что касается внутреннего объема коробов, то его выбор зависит от того, собираетесь ли вы применять короб для скрытия дополнительных кабелей, например телефонного, телевизионного, кабеля сигнализирующих устройств и т. д. Даже если количество таких кабелей на разных участках локальной сети различается, не стоит особенно переживать по данному поводу: существуют переходники разного размера, позволяющие соединять различие коробы.

Крепление короба зависит от его размера и того, куда он буде крепиться. Как правило, для крепления коробов используются шурупы определенного размера (подбираются согласно размеру короба). Если внутренний размер короба минимален и он должен крепиться к гладкой стене, не покрытой составом на основе песка, часто используется двухсторонний скотч. Если же структура покрытия стены другая, без шурупов не обойтись.

Крепление короба шурупами наиболее предпочтительно, поскольку обеспечивает более плотный контакт со стеной. Это, в свою очередь, делает возможным открытие уже закрытых коробов с целью проводки дополнительных видов 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 степень крепления.

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

Стандартная длина короба обычно не превышает 4 м, что связано со сложностью его транспортировки. По этой причине, когда вам потребуется длина короба более 4 м, придется компоновать ее из нескольких частей. Этого не стоит бояться, поскольку места соединения коробов скрываются с помощью внешней части короба, которая подбирается таким образом,

чтобы соединять два соседних короба. Тем самым обеспечивается визуальная целостность сегмента сети.

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, который используется для построения сети на основе коаксиального кабеля, применяется тонкий коаксиальный кабель. Однако это совсем не означает, что вы не можете использовать толстый коаксиальный кабель. На практике обычно для соединения двух отдаленных сегментов сети часто применяется именно толстый коаксиальный кабель, поскольку он позволяет добиться максимальной длины сегмента.

После этого можно приступать к работе. Вспомним принцип построения сети на основе коаксиального кабеля.

□ Центральная магистраль кабеля с обоих концов требует использования специальных коннекторов – терминаторов, которые используются для гашения сигнала, чтобы избежать появления эффекта отбитого сигнала. При этом обязательным условием является заземление одного из терминаторов.

□ 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 разрезается и обжимается BNC-коннекторами. Эти коннекторы используются для подключения Т-коннектора, тем самым обеспечивая целостность центрального кабеля и давая 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 было упомянуто 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 предпочтительнее, поэтому рассмотрим его более детально.

Основная ваша задача – подготовка отрезков кабеля необходимой длины и обжим 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.

Отмерив отрезок кабеля от этого компьютера до соседнего компьютера с учетом всех особенностей пути или ориентируясь на закрепленный заранее короб, обрежьте его. Для этого воспользуйтесь обрезным инструментом (рис. 17.1) или обычными ножницами.

Рис. 17.1. Обрезка кабеля с помощью инструмента

Далее необходимо обжать кабель, тем самым закончив создание кабеля для подключения одного рабочего места.

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, как это было описано выше.

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. Основное преимущество обжимных коннекторов – обеспечение надежного контакта и легкость обжима. Недостаток – одноразовость: в случае обрыва провода требуется новый коннектор, поскольку применение старого коннектора невозможно в силу полученных при обжиме деформаций. 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 его осуществления 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 требуется паяльник и припой. Недостатком является сложность, требующая опыта проведения паяльных работ. Нарушение контакта в случае плохой пропайки контактов приводит к постоянным сбоям сети и к трудностям локализации места пропадания контакта.

Как уже было упомянуто, на сегодняшний день можно найти только первый вариант коннекторов, то есть обжимной коннектор. Его мы и будем рассматривать в дальнейшем.

Принцип алгоритма обжима 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 оголении центрального проводника и экранирующей оплетки.

Обрезать кабель старайтесь аккуратно, чтобы обрез получился ровным – это избавит вас от повторного обрезания кабеля и, как следствие, уменьшения 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, освобождая 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. 17.2).

Рис. 17.2. Пример правильно обрезанного кабеля

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 нажать обжимную трубку – основной компонент коннектора, который и позволяет обжать его, то есть надежно зафиксировать на кабеле.

Далее приступаем 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. Смысл этого действия заключается в том, чтобы добиться оптимальной длины выступа сердечника из коннектора. Если сердечник будет выступать недостаточно, качество контакта с Т-терминатором 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, его необходимо будет укоротить, воспользовавшись для этого резаком или ножницами. Если же сердечник выступает недостаточно, необходимо 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 устано-

вить кабель с сердечником. Убедившись в том, что центральный проводник вставлен в сердечник до упора, произведите обжим (рис. 17.3).

Рис. 17.3. Обжим сердечника коннектора

Для этого сожмите ручки инструмента до появления щелчка. Это 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 в том, 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 момент, который обязательно нужно проконтролировать. На качество обжима коннектора сильно влияет толщина используемого кабеля. По этой причине если кабель слишком тонкий, то, чтобы получить более качественный обжим, может потребоваться задвинуть выступающую часть коннектора под внешнюю изоляцию. Определить, требуется ли такое действие, достаточно просто: установите обжимную трубку на ее «законное» место и проконтролируйте, насколько легко это происходит. Если это происходит очень легко, то есть кабель слишком тонкий, значит, необходимо провести 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 в соответствующий вырез коннектор и сильным сжатием произведите обжим (рис. 17.4).

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

Описанным образом необходимо произвести обжим второго конца кабеля, чтобы завершить подготовку сегмента.

Подключение коннекторов

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

Рис. 17.4. Обжим коннектора

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

На готовый отрезок кабеля необходимо установить Т-коннектор, с помощью которого в дальнейшем 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 исключает неправильное его подключение, поэтому сделать это очень просто.

В дальнейшем, 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 необходимо с самой дальней точки.

Конец кабеля, равный примерно 50 см, необходимо оставить торчать из крайней точки кабеля, чтобы в дальнейшем можно было его использовать 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 концы кабеля, если это было предусмотрено объемом 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 мере по сравнению с остальными участками сети.

Глава 18
Монтаж сети с использованием кабеля «витая пара»

□ Ограничение длины сегмента
□ Правила прокладки кабеля
□ Прокладка и монтаж коробов
□ Прокладка кабеля
□ Монтаж сетевых розеток
□ Монтаж кросс-панели
□ Обжим кабеля

Сеть, построенная с применением кабеля «витая пара», – самый распространенный тип, используемый как для малых, так и для больших локальных сетей. Особенно популярен он для организации сети в домашних условиях, поскольку наличие интегрированных сетевых адаптеров подходящего стандарта 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 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.

Прежде чем приступить к созданию сети, нужно подготовиться к этому. Теоретические сведения явно не будут лишними, скорее, их незнание может повлиять на работоспособность будущей сети.

Ограничение длины сегмента

Прежде всего вспомним об основных ограничениях сети, построенной с применением кабеля «витая пара»:

□ длина сегмента не должна превышать 100 м;
□ количество компьютеров, подключаемых к сети, должно быть не больше 1024;
□ количество повторителей в сети – не более 3.

Почему длина сегмента должна быть не более 100 м? Все очень просто. Возьмем для примера сеть, состоящую из двух компьютеров и одного репитера.

Предположим, что сформированный особым образом электрический сигнал должен пройти от одного компьютера к другому. Основными факторами, которые влияют на скорость доставки сигнала от отправителя к адресату, являются следующие.

□ Сетевая карта отправителя. Формируется пакет данных, снабженный необходимой служебной информацией. После этого сигнал передается по кабелю, сопротивление которого идеально соотносится с сопротивлением выхода на сетевой карте. В обоих случаях оно составляет 50 Ом. Таким образом, первая задержка осуществляется сетевой картой и составляет 0,25 мкс – время, необходимое для формирования сигнала.

□ Сигнал передается по кабелю, проходя расстояние от сетевой карты отправителя до первого репитера (концентратора, коммутатора или подобного устройства). Учитывая то, что задержка, вызываемая сопротивлением кабеля, составляет 0,55 мкс[6], получаем вторую задержку.

[6] Данный показатель определяет задержку в передаче сигнала на расстояние, равное 100 м.

□ Сигнал проходит через репитер. Репитер обладает некоторыми функциями, одна из которых служит для обновления сигнала, то есть сигнал формируется заново. В самом простом случае он отправляется на все остальные порты репитера, кроме порта, с которого был получен. Таким образом, в зависимости от типа репитера[7] получаем третью задержку – от 0,35 до 0,7 мкс (в зависимости от класса репитера и скорости репитера).

Данная последовательность описывает только половину пути, которую проходит сигнал от сетевой карты отправителя. Другая половина пути тратится на доставку сигнала через остальную часть кабеля и сетевую карту получателя (адресата).

Согласно требованиям, предъявляемым к скорости передачи данных, общая задержка, например, для сети со скоростью 100 Мбит/с должна быть не более 5,12 мкс. Таким образом, получаем следующую формулу:

2 х первая задержка + 2 х вторая задержка + 2 х *X* х третья задержка < 5,12 мкс.

Чтобы узнать, какое количество репитеров можно использовать в сети, вводится неизвестное *X*. Если количество репитеров больше положенного, то сигнал будет недостаточно сильным, что приведет к появлению коллизий.

При создании сети применяется одна из двух топологических моделей.

Суть первой модели заключается в том, что при расчете задержек сигнала, которые возникают при его прохождении через сетевые карты, кабель и концентраторы, предполагается, что эта задержка является максимально возможной.

Вторая модель подразумевает вычисление реальной задержки. Это позволяет добиться максимальной длины сегмента. Подсчитать правильные задержки, не имея специального оборудования, достаточно сложно, поэтому вторая модель используется реже.

В случае применения первой модели допускается два варианта:

□ используется только один репитер (длина каждого сегмента не должна превышать 100 м);

□ применяются два репитера (длина каждого сегмента не должна превышать 100 м; репитеры соединяются отрезком кабеля длиной до 5 м).

Правила прокладки кабеля

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

1. Правильно выберите место прокладки кабеля. Старайтесь исключить ситуацию, когда на кабель можно случайно наступить. Кабель при этом может деформироваться или оборваться, что приведет к выходу из строя целого сегмента сети. На кабель также нельзя ставить тяжелые предметы.

2. Исключите натяжение кабеля. Излишнее натяжение кабеля может привести к его обрыву 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 хомуты, которыми будет удерживаться кабель.

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

[7] Различают репитеры двух классов. Репитеры второго класса формируют и передают сигнал примерно в 1,5–2 раза быстрее, чем аналогичные репитеры первого класса.

4. 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» не должен быть менее 4–5 см.

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

6. Не прокладывайте кабель возле отопительных элементов. Батарея центрального отопления, а также другие теплогенерирующие приборы отрицательно влияют на кабель. Излишний нагрев может вызвать изменения в сопротивлении кабеля, из-за чего также могут возникнуть коллизии. Если возможности обойти препятствие не существует или 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 обожмите коннекторы. 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 положительным образом повлияет на дизайн помещения.

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

> **Примечание**
>
> Многие пользователи, планирующие возможное появление локальной сети в домашних условиях, прокладывают кабель на этапе ремонта помещений.

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

Как уже упоминалось ранее, создание большой локальной сети принято доверять профессионалам, и это вполне оправданно. Причиной является наличие у подобных организаций не только соответствующего опыта, но, самое главное, соответствующего оборудования, с помощью которого можно обследовать будущую магистраль на наличие разного рода проводки.

В условиях же работы 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 объемом: коробы с большим объемом применяются при монтаже ближе к центральному управляющему узлу, коробы с меньшим объемом – в непосредственной близости от компьютеров. При этом чем дальше вы будете отходить от центрального узла, тем меньше по размеру будут оказываться коробы, что вполне объясняется особенностями топологии «звезда».

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

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

Вследствие ограниченной длины короба нужная длина достигается путем использования необходимого количества отрезков короба. В местах изгибов крепление коробов необходимо производить более тщательно и аккуратно, применяя для этого увеличенное количество мест крепления.

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

Прокладка кабеля

В отличие от монтажа сети с использованием коаксиального кабеля, когда кабели 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 создают межкомнатные переходы и отверстия, сквозь которые бывает тяжело провести нужное количество кабелей. По этой причине очень часто протягиваются все сегменты кабеля сразу, что, конечно, имеет недостаток – большой расход кабеля.

Когда же дело касается небольших офисных или домашних сетей, когда стоимость их создания достаточно жестко лимитируется, 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, что его нужно протянуть от центрального узла до конечного с учетом всех особенностей пути или расположения коробов. При этом обязательным условием является обеспечение определенного запаса кабеля, который потом можно легко устранить в районе центрального узла. Запас кабеля пригодится для монтажа сетевых розеток либо для процесса обжима коннекторов.

При прокладке кабеля, чтобы не перепутать сегменты местами, желательно использовать систему обозначений. Для этого к обеим 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, прикрепив его с помощью скотча.

Монтаж сетевых розеток

Как уже упоминалось ранее, использование сетевых розеток практикуется в том случае, когда планируется создание 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 часто отказываются.

Согласно существующим требованиям сетевые розетки поддерживают разный уровень безопасности работы, а соответственно, различаются конструкцией и сложностью.

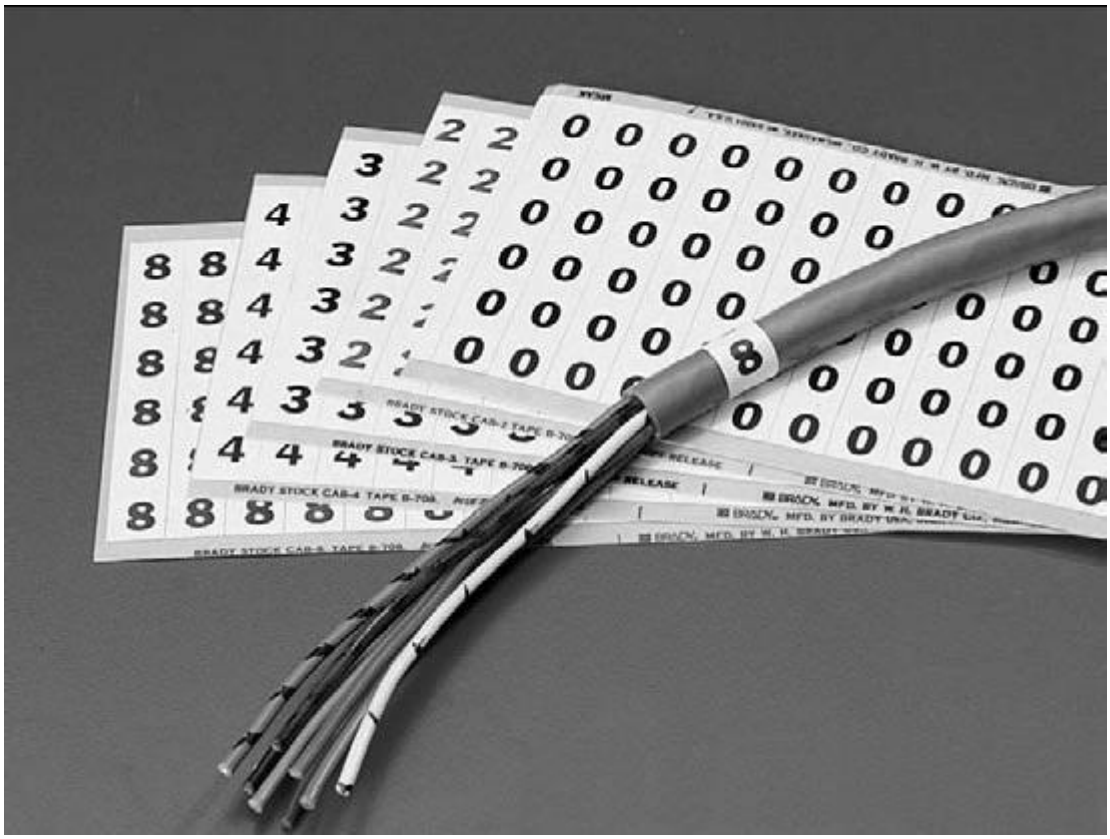

Рис. 18.1. Использование маркировки кабеля

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 подразумевает крепление на стене с помощью шурупа или клейкого двухстороннего скотча. Подобного рода розетка состоит из трех частей: основы, крышки и платы с контактной группой (рис. 18.2).

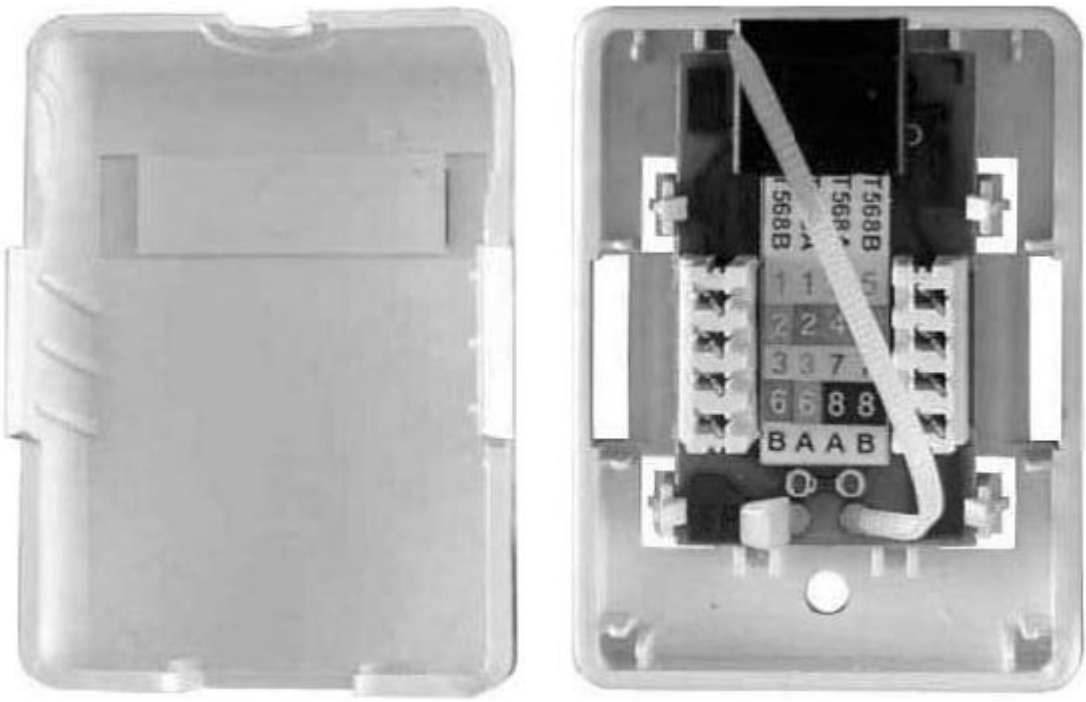

Рис. 18.2. Составные части сетевой розетки

При работе с такой розеткой, как правило, необходимо придерживаться следующей последовательности действий.

1. Разобрать розетку на составные части, чтобы получить 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 метод.
5. Закрыть розетку крышкой.

Как правило, розетка использует систему замков, поэтому, чтобы ее разобрать, инструменты не нужны: просто определите места расположения 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 наносится 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 этого 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. 18.3).

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

Для фиксации кабеля в розетке могут применяться разные методы, одним из которых является использование монтажной стяжки. Затянув как можно сильнее стяжку, обрежьте лишний конец стяжки, закройте розетку крышкой и переходите далее.

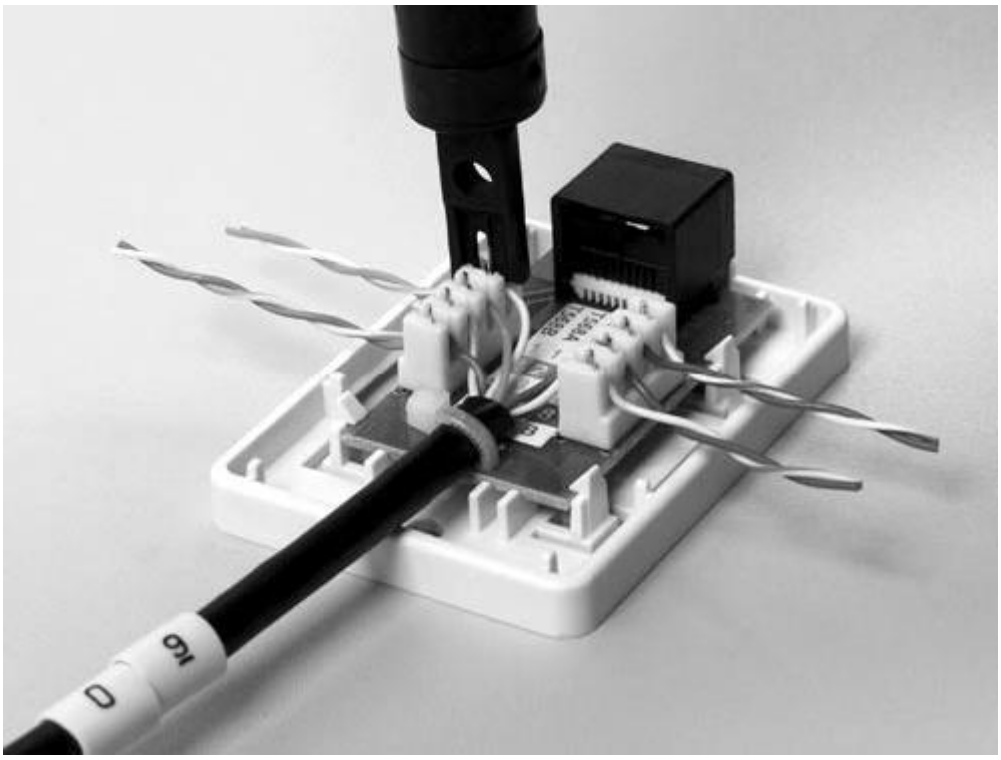

Рис. 18.3. Фиксация проводников в контактной площадке

Монтаж кросс-панели

Кросс-панель, как и сетевая розетка, представляет собой лишь удобное средство подключения кабеля независимо от того, зачем этот кабель используется. В случае с кросс-панелью 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. Внешний вид контактной площадки и принцип работы с ней 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 повторяет процесс 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 с использованием кабеля «витая пара», так и единственным. Так, если локальная сеть создается с минимумом затрат, обжим отрезков кабеля нужной длины – одна операция, которую требуется выполнить для создания сети. Если же речь идет о создании достаточно большой локальной сети, то в первую оче-

редь 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 небольших офисных сетей или сети в домашних условиях. Большого размера сеть подразумевает использование готовых патч-кордов и кросс-кордов. Тем не менее, знание принципа обжима и приобретение такого опыта является необходимым, поскольку рано или поздно приходится создавать дополнительные кабели для подключения оборудования. По этой причине рассмотрим данный процесс более детально на примере создания патч-корда.

Для обжима кабеля «витая пара» используются коннекторы RJ-45, что регламентировано существующими сетевыми стандартами, при которых этот кабель используется в качестве среды передачи данных. Нумерация контактов в коннекторе производится так, как показано на рис. 18.4

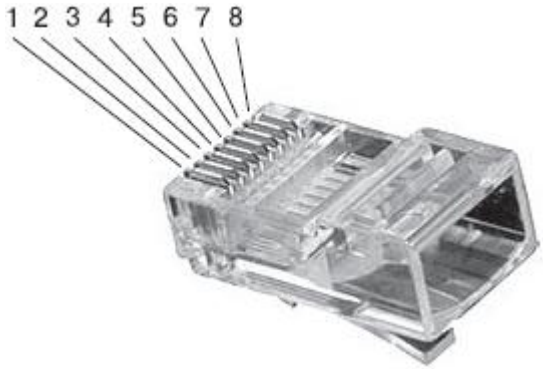

Рис. 18.4. Нумерация контактов в коннекторе RJ-45

Существуют определенные правила, которых необходимо придерживаться при обжиме кабеля. Независимо от используемого стандарта следует соблюдать особый принцип подключения проводников, причем, как уже было сказано, данный принцип надо соблюдать на всех этапах проведения работ.

На практике используются две схемы обжима или зажима проводников (табл. 18.1).

Принципиального различия между этими схемами нет, поэтому можно выбрать и придерживать той, которая вам больше нравится.

Таблица 18.1. 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

При обжиме кабеля можно придерживаться следующего алгоритма действий.

1. Наденьте на конец кабеля изоляционный колпачок, развернув его таким образом, чтобы широкий конец колпачка смотрел в сторону обрабатываемого конца кабеля (рис. 18.5).

Рис. 18.5. Надетый колпачок

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 обжимным инструментом 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. 18.6, и расположите проводники согласно одному из стандартов, например T568A.

Рис. 18.6. Выравниваем и обрезаем проводники

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. Медленным движением руки вставьте концы проводников в окошко разъема, проследив, чтобы они равномерно распределились по всей его ширине (рис. 18.7).

Рис. 18.7. Вставляем проводники в коннектор

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. 18.8).

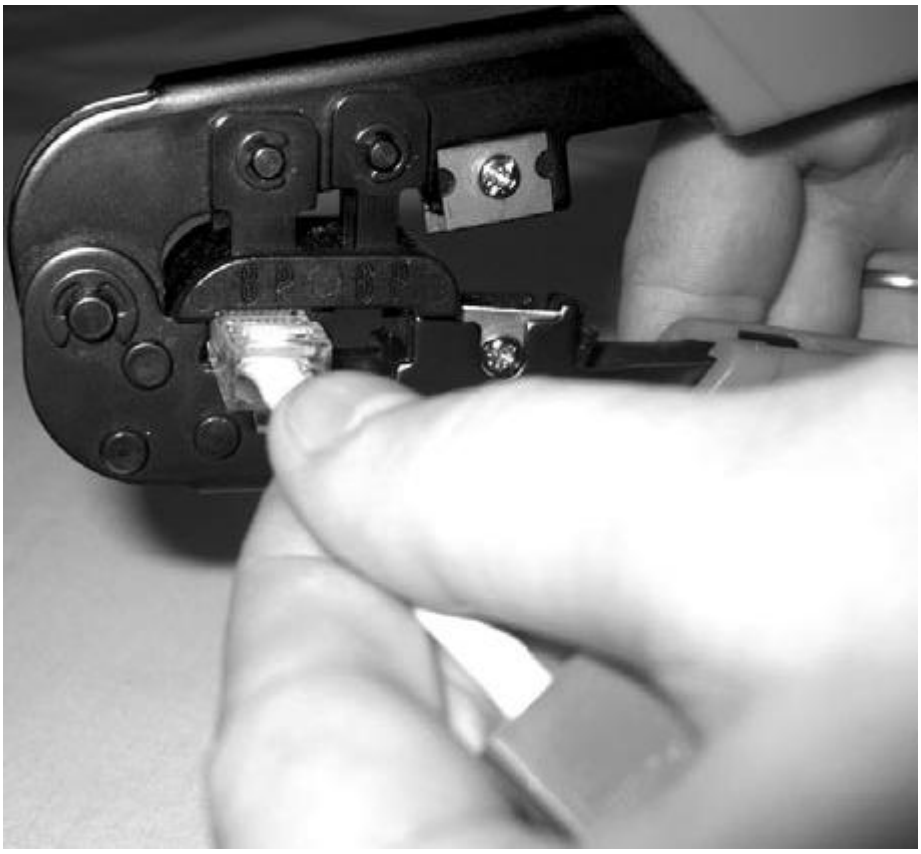

Рис. 18.8. Обжимаем коннектор с помощью инструмента

10. Задвиньте на обжатый коннектор защитный колпачок (рис. 18.9).

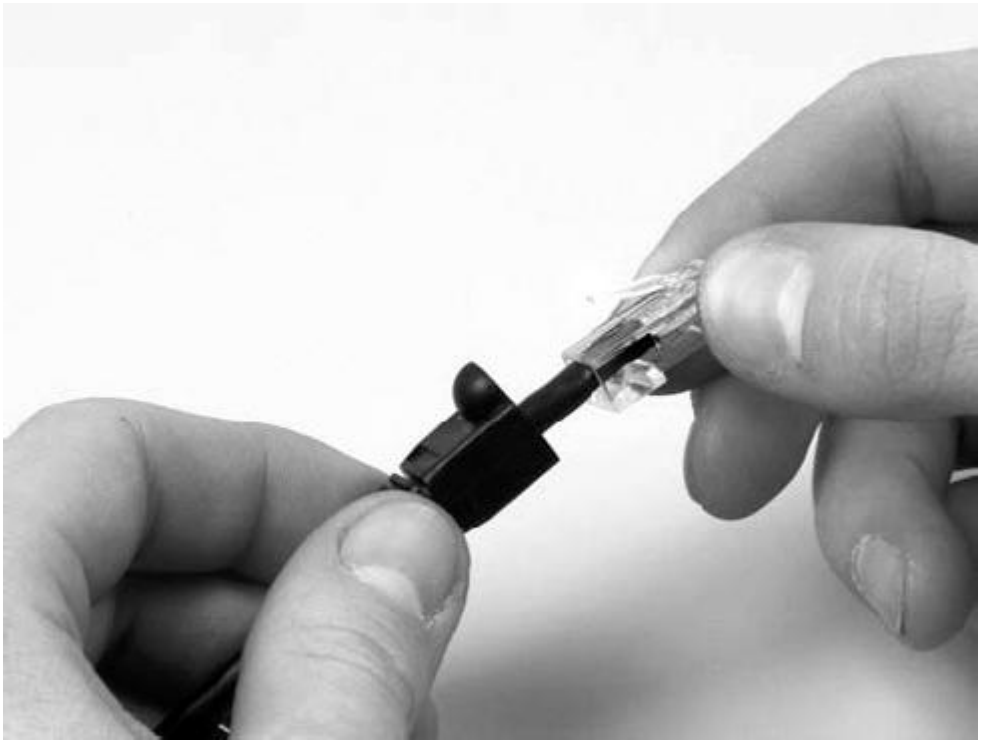

Рис. 18.9. Надеваем колпачок

Аналогичным образом проведите обжим второго конца кабеля.

Глава 19
Создание беспроводной сети

□ Организация работы беспроводной сети
□ Вопросы законности использования беспроводной сети

Организация беспроводной сети, в отличие от любого варианта проводной сети, требует от ее создателя минимума усилий, поскольку среда передачи данных уже готова и не требует монтажа. Единственное, с чем приходится столкнуться, – выбор месторасположения точки доступа. Его нужно производить с таким расчетом, чтобы уровень сигнала был достаточным для приема всеми беспроводными рабочими местами.

Организация работы беспроводной сети

Если ориентироваться на созданный при подготовке проект сети, то вам остается только установить точку доступа на то место, которое в процессе проектирования признано 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 своим сигналом покрыла бы 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.

При создании беспроводной сети, если вы действительно хотите добиться максимальной скорости работы, необходимо придерживаться следующих рекомендаций.

□ Уровень сигнала, а значит, и скорость работы зависит от расстояния, на котором находятся рабочие места от точки доступа. По этой причине максимальная скорость передачи возможна при как можно более близком контакте точки доступа с компьютером.

□ Чем меньше препятствий, тем сильнее сигнал. Располагайте компьютеры в зоне прямой видимости точки доступа.

□ Не используйте оборудование разных стандартов. Оборудование одного стандарта позволяет достичь теоретически максимально возможной для него скорости работы.

□ Применение оборудования от разных производителей также нежелательно. Оборудование от одного производителя дает возможность использовать фирменные аппаратные разработки, например увеличенную скорость передачи данных.

□ Применение 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 для соединения точек доступа.

Вопросы законности использования беспроводной сети

Существует еще один важный вопрос относительно использования беспроводных сетей, который никак нельзя оставить без внимания. Связан он со средой передачи данных. Дело в том, что применение радиоволн в качестве среды передачи данных практикуется уже очень давно. Радиоволны используются не только в бытовых целях, например для обслужи-

вания радиотелефонов или мобильной связи. Они применяются и для организации работы государственных органов различного назначения: милиции, медицинских организаций и т. п. И если ваша или другая беспроводная сеть станет причиной сбоев важного оборудования, это может привести к непоправимым последствиям.

По причине важности этого вопроса практически в каждой стране были созданы государственные организации, которые контролируют использование радиочастот. Они регистрируют используемые беспроводные сети и решают вопросы о разрешении или запрете применения новых беспроводных сетей. К сожалению, единых правил использования радиочастот не существует, поэтому, перед тем как решить создавать беспроводную сеть, стоит ознакомиться с документами, которые регламентируют данный процесс.

Что касается Российской Федерации, то 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 использование беспроводных сетей без разрешения ГКРЧ.

Таким образом, если вы собираетесь организовать работу беспроводной сети и хотите, чтобы это произошло быстро и без каких-либо осложнений, просто 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;

□ оборудование имеет соответствующий сертификат для использования на территории России;

□ мощность излучения точкой доступа не превышает 100 мВт;

□ используются только стандартные (встроенные) 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 также 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 соответствующие форумах в Интернете.

Глава 20
Соединение двух компьютеров

□ Соединение через Bluetooth
□ Соединение с помощью коаксиального кабеля
□ Соединение с помощью кабеля «витая пара»
□ Соединение через USB-порт
□ Соединение через FireWire-порт
□ Соединение с помощью беспроводных адаптеров

Ситуация, когда необходимо соединить два компьютера в сеть, происходит очень часто, особенно в последнее время. Достаточно часто дома одна семья уже имеет два компьютера: один используется для работы, а второй – для обеспечения досуга. Или, например, для работы применяется два компьютера, только один из них стационарный, а второй – ноутбук или нетбук, который часто путешествует вместе с вами, обеспечивая вам мобильность. В любом случае появляется вполне оправданное желание соединить их, чтобы обмениваться данными или использовать принтер, подключенный к одному из компьютеров.

Такая же ситуация может возникнуть в малых офисах, где работает несколько человек, но в наличии имеется только два компьютеризированных рабочих места, которые 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 существующие варианты соединения компьютеров. Каждый из них имеет свои преимущества и недостатки. Так, разные способы соединения двух компьютеров определяют максимальную скорость обмена между ними. По этой причине вопрос определения оптимального по показателям варианта цена/качество/скорость ложится на самого пользователя и зависит от реальных потребностей.

Соединение через Bluetooth

На сегодня поддержка технологии Bluetooth есть практически в любом устройстве, начиная с бытовых приборов и заканчивая мобильными телефонами и компьютерами. Именно этот факт и является привлекательным и решающим, когда нужно быстро соединить два устройства посредством Bluetooth.

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 требуется приобретение такого адаптера, 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. 20.1), то есть для их подключения требуется свободный USB-порт. Для ноутбуков также предлагается вариант с подключением к PCMCIA-слоту.

Рис. 20.1. Bluetooth-адаптер для подключения к USB-порту

Другим 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, вы тем самым «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 количества компьютеров. В частности, для этой цели отлично подойдет коаксиальный кабель.

В таком случае 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 при соединении только двух компьютеров практическая скорость (которая обычно меньше теоретической в 1,5–2 раза) вплотную приближается к теоретической. Конечно, ее показатель зависит от длины кабеля. Тем не менее этой скорости вполне хватит для обмена информацией любого объема.

Соединение с помощью кабеля «витая пара»

Этим способом можно соединить любое количество компьютеров. В случае соединения двух машин (а также двух концентраторов, двух коммутаторов и т. д.) используют специальный кабель кроссовер-корд, обжим коннекторов в котором отличается от стандартного патч-корда (табл. 20.1).

Таблица 20.1. 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, учитывая наличие интегрированного в материнскую плату Ethernet-контроллера, подключение сводится к созданию кабеля. Кроме того, если на материнских платах окажется сетевой контроллер стандарта 1000Base-T и для создания кабеля будет применяться кабель 6 или 7 категории, вы получите в свое распоряжение скорость передачи данных, близкую к теоретической, то есть 1000 Мбит/с, чего, 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, позволяющих расширить функциональность компьютера. По этой причине в появлении средств соединения двух компьютеров через специальный USB-кабель нет ничего удивительного.

Скорость работы USB-порта, особенно стандарта 2.0, очень высокая, что позволяет организовать соединение двух компьютеров и получить приличный результат. При этом теоретически можно достичь скорости 480 Мбит/с. С другой стороны, создание подобного соединения потребует поиска соответствующего кабеля.

Для USB-соединения двух компьютеров используют специальный кабель (рис. 20.2), главной деталью которого является специальный модуль, отвечающий за соответствующие преобразования сигнала.

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

У данного способа имеется один недостаток, что 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 от друга.

Рис. 20.2. USB-кабель для соединения двух компьютеров

Соединение через FireWire-порт

Использование FireWire-порта для соединения двух рядом расположенных компьютеров – еще один вид соединения, обладающий высокой теоретической скоростью передачи данных, которая 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 можно воспользоваться данный способом, чтобы создать подобное соединение. Однако, как и в случае 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, основным показателем которого является наличие экранирующей оплетки (рис. 20.3).

Соединение с помощью беспроводных адаптеров

Существующие беспроводные сетевые стандарты предусматривают режим работы беспроводной сети, не требующий наличия точки доступа, стоимость которой довольно существенна. По этой причине если у вас есть два беспроводных адаптера, то соединение двух компьютеров не займет много времени. При этом вы получаете 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 компьютера очень заманчиво.

Рис. 20.3. FireWire-кабель с шестиконтактными разъемами

Как уже было упомянуто ранее (смотрите главу о создании беспроводной сети), чтобы достичь максимальной эффективности работы подобного соединения, рекомендуется использовать оборудование одного стандарта и желательно одного производителя. В этом случае вы сможете получить максимальную скорость передачи данных, а также воспользоваться некоторыми фирменными технологиями от производителя оборудования. Все, что вам остается сделать, – настроить оба адаптера на использование одного идентификатора сети и выбрать один из современных способов аутентификации и шифрования данных.

Глава 21
Тестирование и диагностика сети

□ Использование тестеров
□ Использование программного способа

Процесс монтажа кабельной системы локальной сети с учетом разного рода особенностей изначально 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 процессом тестирования. Когда же монтаж локальной сети полностью завершен, осуществляется 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.

В случае же, когда происходит монтаж небольшой сети, за ее создание, как правило, отвечает человек из штата организации – владельца локальной сети. По понятным причинам требовать от данного человека технической документации или других спецификаций не приходится, так как тестирование работоспособности сети происходит с использованием максимально упрощенных методов.

В любом случае 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 простым способом тестирования всех особенностей локальной сети является использование разного рода тестеров. Они позволяют максимально автоматизировать и упростить процесс тестирования, поэтому, если есть такая возможность, желательно применять именно этот способ.

Существуют разные варианты тестеров, отличающихся методами тестирования, количеством разнообразных тестов, а также способом выдачи результатов. От этих функций напрямую зависит стоимость тестирующего оборудования. На рынке существует 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 соответ-

ствие определенному стандарту. Покупку такого тестера может позволить себе даже небольшая фирма, что даст 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. 21.1.

Рис. 21.1. Кабельные тестеры с набором переходников

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 подключению одному из стандартов. Использование данных о сопротивлении 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.

Например, чтобы проверить сегмент коаксиального пути, 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 командную строку, в которой ввести следующую команду:

ping 192.168.2.2

Если в результате выполнения этой команды последует ответ, похожий на показанный на рис. 21.2, значит, кабельный сегмент физически цел (рис. 21.2).

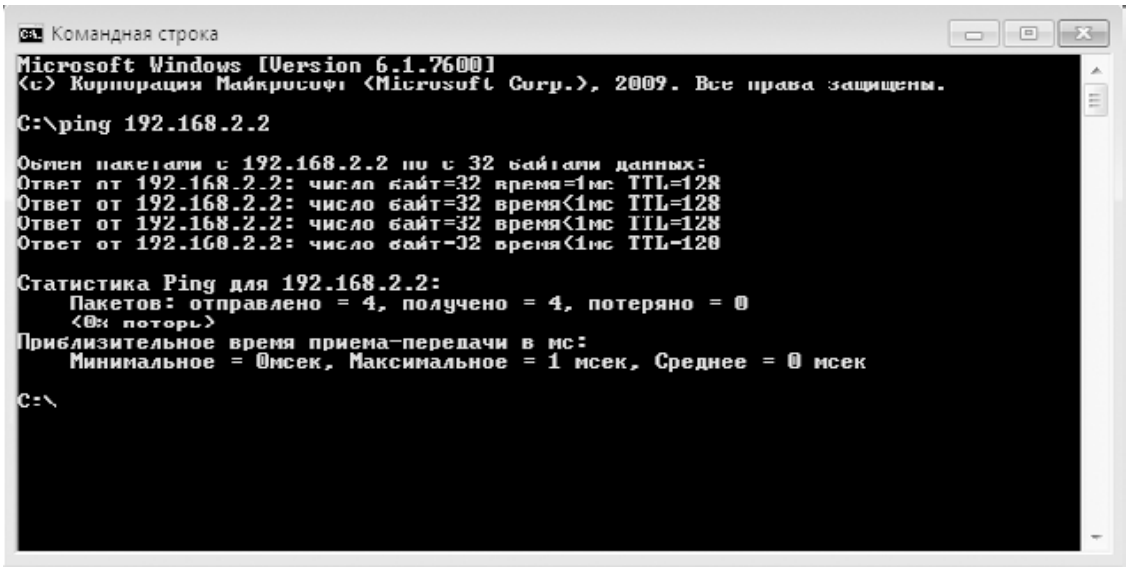

Рис. 21.2. Успешное выполнение команды **ping**

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. Если же необходимо протестировать работоспособность кабеля типа патч-корд, его необходимо подключать к центральному узлу, например коммутатору, а в паре с ним использовать заведомо рабочий кабель, который подключен ко второму компьютеру.

Часть 3
Администрирование сети

○ Выбор способа функционирования сети
○ Выбор управляющего сервера
○ Установка контроллера домена и DNS-сервера
○ Добавление роли DHCP-сервера
○ Настройка DHCP-сервера
○ Использование Active Directory – пользователи и компьютеры
○ Подключение и настройка клиента Windows XP
○ Подключение и настройка клиента Windows Vista
○ Подключение и настройка клиента Windows 7

Глава 22
Выбор способа функционирования сети

□ Рабочая группа
□ Домашняя группа
□ Домен

Главная задача локальной сети – обеспечение потребностей ее участников в определенном сервисе. Это может быть общий доступ к файловым ресурсам и периферии, работа с базами данных, работа в Интернете и т. д. Каким образом пользователь получит нужную информацию, его абсолютно не интересует, как и не интересует способ подключения к сети. Но если процесс получения информации или доступа к определенному сервису, а также остальные действия пользователей должны быть контролируемыми, то это однозначно влияет на выбор способа функционирования сети и как следствие – метода управления ею.

Способ функционирования сети, как правило, определяется еще до ее монтажа и даже проектирования. Количество будущих пользователей примерно известно еще до проектирования сети, а именно этот параметр и является решающим при выборе способа функционирования сети. Мало того, именно это и позволяет спрогнозировать стоимость сети с учетом необходимого оборудования, такого как серверы.

На сегодняшний день, когда дело касается локальной сети, используются следующие способы ее функционирования.

□ **Работа в составе рабочей группы или групп.** Самый простой способ организации работы в сети, подразумевающий использование статичной IP-адресации или динамичной IP-адресации, организованной на аппаратном уровне, например в маршрутизаторе или управляемом коммутаторе. Никакого централизованного управления в этом случае не производится по причине отсутствия соответствующих механизмов.

□ **Работа в составе домашней группы.** Поддержка домашних групп появилась в операционной системе Windows 7. Она является неким подобием рабочих групп и ориентирована на работу небольших сетей, предположительно – сети в домашних условиях.

□ **Работа в составе домена.** Стандартный принцип функционирования сети, который используется, когда необходимо иметь полный контроль над происходящими в сети процессами.

Стоит заметить, что способ функционирования так называемых «домашних» сетей не является результатом логического выбора. Это вполне объясняется сам*о*й хаотичностью «домашней» сети, а именно – использованием наиболее оптимального по показателю скорость/цена подхода подключения компьютеров. В связи с этим практически всегда применяется работа в составе рабочих групп.

Рабочая группа

Как уже было упомянуто ранее, использование рабочих групп является наиболее простым и дешевым способом функционирования локальной сети.

Поддержка работы с рабочими группами имеется во всех операционных системах, даже в самых старых версиях, например Microsoft Windows 95.

Рабочая группа как концепция исторически стала первой в организации работы локальной сети. Простота организации и отсутствие необходимости приобретения дополнительного управляющего сервера с лицензионным программным обеспечением сделали ее распространение повсеместным.

Использование рабочей группы является идеальным решением для сетей, содержащих не более 25-30 компьютеров. Контролировать большее количество компьютеров становится слишком сложно, особенно если они расположены в нескольких помещениях, удаленных друг от друга. Кроме того, сам подход исключает необходимость присутствия человека, который выполнял бы административное управление сетью. Функции контроля возложены на пользователей каждого конкретного компьютера.

Однако, как показала практика, пользователь компьютера не только не готов к выполнению таких обязанностей, а часто и сам является причиной сбойной работы компьютера или выхода его из строя. По этой причине системный администратор, контролирующий сеть на основе рабочих групп, не просто желателен, а крайне необходим.

Как уже было сказано, преимуществом использования рабочих групп является только возможность экономии средств, недостатков же намного больше. Основными из них являются:

сложность контроля общего состояния сети;

отсутствие механизмов централизованного управления пользователями;

необходимость осуществления любых типов обновления программных продуктов отдельно на каждом компьютере;

отсутствие гарантированного доступа к ресурсам;

отсутствие централизованного хранилища данных;

отсутствие системы управления правами доступа к ресурсам.

Таким образом, удел рабочих групп – небольшие офисные или «домашние» сети. Если сеть состоит из большого количества компьютеров, единственный правильный выход – организация доменной структуры и работа компьютеров в составе домена.

Домашняя группа

Домашняя группа – нововведение, появившееся в операционной системе Windows 7. Это означает, что использовать домашние сети могут только компьютеры с установленной операционной системой Windows 7, причем с версией не ниже Home Basic.

Домашняя группа представляет собой некое подобие рабочей группы, но с возможностью организации контролируемого доступа к сервисам группы. Для подключения к домашней сети вам потребуется не только желание это сделать, но и разрешение того, кто организовал домашнюю группу. Только после получения соответствующего пароля и настройки работы операционной системы вы сможете пользоваться ресурсами компьютеров, входящих в состав группы.

Количество домашних групп не ограничено, но одновременно можно быть в составе только одной из них, что вполне логично.

Возможность доступа к ресурсам своего компьютера определяет каждый пользователь, входящий в состав домашней сети. При этом права доступа можно настраивать как для всех участников группы одновременно, так и для каждого участника отдельно, если существует определенный сертификат доверия к пользователю.

Домен

Домен как способ функционирования сети является наиболее сложным, но в то же время наиболее контролируемым. Данный способ отлично работает как в локальных, так и в глобальных сетях.

Использование доменной структуры характерно для локальных сетей с большим количеством подключений либо для сетей, у которых контроль над работой рабочих мест (то есть пользователей) стоит превыше всего.

Преимущества работы в составе домена:

максимальный контроль над пользователями и компьютерами локальной сети;

централизованное обновление программного обеспечения;

централизованная система архивирования важной информации;

бесперебойный доступ к документам, хранимым на сервере;

возможность удаленной настройки рабочих мест;

мощные средства управления доступом к ресурсам;

возможность применения групповых политик безопасности;

контроль над сетевыми подключениями;

наличие системного администратора, отвечающего за работоспособность локальной сети и рабочих мест.

Список далеко не полный, но даже имеющихся пунктов вполне достаточно, чтобы сделать правильные выводы.

Однако за все «удобства» приходится платить, причем немало. Взять хотя бы управляющий компьютер. Чтобы выполнять возложенные на него функции контроллера домена, требуется достаточно серьезная вычислительная мощь и объемная дисковая подсистема. Кроме того, для обеспечения бесперебойной работы сети требуется дополнительный сервер – вторичный контроллер домена, который сможет взять на себя управление сетью, если произойдет непредвиденный сбой или выход из строя первичного контроллера домена. Опять же, организация системы архивирования данных, поддержка работы дополнительных серверов… Все это требует серьезных финансовых вливаний и соответствующего уровня обслуживания сети. Именно поэтому использование доменной структуры практикуется только в том случае, если идет речь о большой сети, то есть организация может себе позволить себе все это оплатить.

Глава 23
Выбор управляющего сервера

□ Операционная система Windows Server 2008 R2
□ Конфигурация сервера
□ Роли сервера

Когда принимается решение использовать в качестве способа функционирования локальной сети доменную структуру, возникает целый ряд вопросов, к решению которых необходимо отнестись с максимальным вниманием. Этого требует сама сложность работы такой системы, а также достаточно серьезные денежные траты, которые необходимо будет произвести, чтобы организовать работу локальной сети.

Работа доменной структуры сети подразумевает использование управляющего компьютера с соответствующей серверной операционной системой, установленной на нем. Это требует не только правильного подбора конфигурации сервера и выбора операционной системы, но и определения его дополнительной функциональности.

Операционная система Windows Server 2008 R2

Как известно, функциональность любого компьютера определяется возможностями операционной системы, которая на нем установлена. Любая операционная система умеет использовать ресурсы компьютера, но не любая операционная система может направить их в необходимое русло, попутно контролируя работу еще нескольких десятков подчиненных операционных систем. Именно поэтому существуют клиентские и серверные операционные системы, об особенностях которых уже не раз упоминалось в книге.

Выбор серверной операционной системы представляет собой осознанное решение, однозначно определяющее будущее и возможности локальной сети, управление которой она будет производить.

Существует достаточно много серверных операционных систем, которые уже успели себе зарекомендовать в работе. Почему же именно Windows Server 2008 R2 стала центром нашего внимания? Все очень просто. Эта операционная система является «венцом» возможностей всех существующих операционных систем семейства Microsoft и предоставляет самые современные методы управления работой локальной сети любого масштаба.

Вот только некоторые особенности операционной системы Windows Server 2008 R2, которые могут стать причиной ее использования:

□ полностью 64-разрядная операционная система (32-разрядных вариантов не существует) с полноценной поддержкой работы 32-разрядных приложений. При этом поддерживается параллельная работа до 256 процессоров, а также присутствует более эффективная система управления оперативной памятью;

□ технология виртуализации Hyper-V, позволяющая полноценно работать с виртуальными машинами, используя под их нужды до 64 процессоров. С помощью данной технологии на одном сервере можно организовать работу сразу нескольких виртуальных серверов, обеспечивая при этом очень быструю миграцию данных с одного сервера на другой;

□ расширение командной строки PowerShell, позволяющее выполнять сценарии (так называемые командлеты), что дает возможность автоматизировать некоторые моменты, касающиеся администрирования сети;

□ новый метод удаленного доступа к ресурсам DirectAccess, который дает возможность даже на загруженных каналах связи получить полноценный доступ к управлению своими документами, а также к любым данным;

□ новая технология Core Parking, позволяющая свести потребление электроэнергии многоядерными процессорами к минимуму путем отслеживания реальной потребности в производительности и отключения простаивающих ядер либо мгновенного их активирования при необходимости;

□ новая система кэширования данных Branch Cache, дающая возможность эффективно управлять трафиком между удаленными точками и центральным сервером;

□ интеграция максимально большого количества сервисов в одной операционной системе, что позволяет отказаться от использования дополнительных серверов разного назначения;

□ новая версия популярного сервера управления веб-приложениями IIS 7.5, основанная на самой современной версии технологии ASP.NET;

□ новые возможности Active Directory: а именно Active Directory Recycle Bin – корзина, позволяющая удалять и восстанавливать объекты Active Directory, подключение к несуществующему домену, новый центр администрирования учетных записей и многое другое;

□ тесная интеграция с системами Windows 7.

Это только часть возможностей, которые предоставляет операционная система Windows Server 2008 R2 системному администратору. Но главное ее преимущество заключается в том, что, в отличие от предыдущих операционных систем, Windows Server 2008 R2 позволяет сделать то, что достигается путем использования нескольких серверов разного назначения, которые используются для администрирования сети и выполнения заданий, требующих участия системного администратора каждый день.

Конфигурация сервера

Сервер, используемый для управления основными процессами, которые происходят в локальной сети, требует достаточно большой мощности. Чем больше серверных ролей приходится выполнять управляющему серверу, тем большую нагрузку он испытывает. По этой причине не стоит удивляться тому, что требования к производительности сервера значительно отличаются от требований, которые предъявляются к обычному рабочему месту.

Выбор конфигурации сервера может осуществляться как на этапе проектирования сети, что позволяет с большей точностью определить стоимость создания сети, так и после того, как монтаж сети завершен и решается вопрос о выборе способа ее функционирования. Если выбор сделан в сторону использования доменной структуры, то этап выбора конфигурации сервера будет обязательным, и покупка сервера – необходимость.

При выборе конфигурации управляющего сервера следует учитывать следующие особенности его использования:

□ бесперебойная работа;

□ обеспечение аутентификации сетевых пользователей;

□ хранение всех данные об учетных записях пользователей и компьютеров;

□ возможность использования для выполнения дополнительных ролей, например DNS– и DHCP-серверов;

□ возможность применения для обслуживания веб-приложений;

□ возможность использования дополнительного программного обеспечения, например корпоративной антивирусной системы;

□ возможность подключения системы архивирования данных, например стримера;

□ синхронизация времени на всех компьютерах сети.

Кроме того, важным вопросом является выбор варианта исполнения сервера: отдельная установка или установка в стойку.

Отдельная установка подразумевает применение отдельно стоящего сервера, что со временем приводит к тому, что серверная комната оказывает загруженной серверами разного назначения. Чтобы поддерживать порядок, приходится использовать импровизированные мебельные стойки, которые позволяют устанавливать серверы в два-три яруса.

Очень часто (особенно это касается больших сетей) в серверной присутствуют специальные серверные стойки, которые используются для установки серверов стоечного типа разного назначения. При этом, как правило, для управления серверами применяется одна клавиатура с монитором и система KVN-переключателей, которая позволяет переключать системы ввода и системы отображения на нужный сервер. Это достаточно удобно, поскольку передние панели серверов находятся всегда перед глазами, что позволяет осуществлять визуальный контроль их работоспособности, а сами стойки имеют при этом вполне приемлемые габариты.

Даже не смотря на то что стоечный сервер занимает меньше места, он имеет существенный недостаток по сравнению с отдельно стоящим сервером – как правило, используется только один блок питания. В отдельно стоящем сервере практически всегда установлено два блока питания, один из которых является резервным, позволяя поддерживать работоспособность сервера, даже если основной блок питания выйдет из строя.

Что касается управляющего сервера, то существует достаточно много стандартных конфигураций, отличающихся мощностью процессора, объемом оперативной памяти, объемом и типом дисковой подсистемы и другими характеристиками.

Одна из типовых конфигураций стоечного сервера, который можно использовать для управления локальной сетью из 80–120 компьютеров, приведена в табл. 23.1.

Таблица 23.1. Конфигурация управляющего сервера стоечного типа

Комплектующие	Расшифровка
Набор микросхем	Intel 5100
Процессоры	1 или 2 Intel Xeon 5xxx (до 8 ядер)
Скорость системной шины	1333 МГц
Максимальный объем оперативной памяти	24 Гбайт двухканальной DDRII-667 ECC
Слоты расширения	1xPCI-E 16x, 1xPCI-E 8x
Встроенные контроллеры	2 порта LSI SAS 1064
Оптические накопители	DVD/CD-RW
Опциональные контроллеры	Контроллеры SAS RAID с поддержкой BBU, адаптеры FibreChannel, 10G Ethernet и InfiniBand HCA
Максимальное количество дисков	2xSAS 3.5" или 4xSATA/SSD 2.5" с возможностью горячей замены
Емкость дисковой подсистемы	До 900 Гбайт SAS/ 3 Тбайт SATA
Сетевые интерфейсы	2x Intel Gigabit Ethernet
Видеоконтроллер	ASPEED AST2000, 8 Мбайт
Интерфейсы	Задняя панель: VGA, RS232, 3xRJ-45, 2xUSB, 2xPS2; передняя панель: 2xUSB
Управление системой	IPMI 2.0, KVM over IP, Virtual Media, Ethernet
Поддерживаемые ОС	SuSE Linux Enterprise Server 10; Novell Open Enterprise Server; Семейство Microsoft Windows Server 2008; Red Hat Enterprise Linux 5.0; Sun Solaris 10
Размеры (Д × Ш × В), мм	1U, 510 × 430 × 44 мм (глубина стойки не менее 800 мм)
Блок питания	400 Вт

Размеры отдельно стоящего сервера позволяют получить б**о**льшую, по сравнению с аналогичным стоечным сервером мощность и функциональность благодаря возможности установки большего количество габаритных комплектующих. Одна из аналогичных типовых конфигураций отдельно стоящего сервера приведена в табл. 23.2.

Таблица 23.2. Конфигурация управляющего сервера отдельно стоящего типа

Комплектующие	Расшифровка
Набор микросхем	Intel 5100
Процессоры	1 или 2 Intel Xeon 5xxx (до 8 ядер)
Скорость системной шины	1333 МГц
Максимальный объем оперативной памяти	24 Гбайт двухканальной DDRII-667 ECC
Слоты расширения	1xPCI-E 16x, 1xPCI-E 8x, 2xPCI 32/33
Встроенные контроллеры	8 портов SAS LSI 1068
Оптические накопители	DVD-RW
Опциональные контроллеры	Контроллеры SAS/SATA с поддержкой BBU, адаптеры FibreChannel и InfiniBand HCA
Максимальное количество дисков	4 стандартно и до 8 SAS/SATA с возможностью горячей замены
Емкость дисковой подсистемы	До 12 Тбайт SATA или 3,6 Тбайт SAS
Сетевые интерфейсы	2xIntel Gigabit Ethernet, IOAT
Видеоконтроллер	ASPEED AST2000, 8 Мбайт
Интерфейсы	Задняя панель: VGA, RS232, 3xRJ-45, 2xUSB, 2xPS2; передняя панель: 2xUSB
Управление системой	IPMI 2.0, KVM over IP, Virtual Media, Ethernet
Поддерживаемые ОС	SuSE Linux Enterprise Server 10; Novell Open Enterprise Server; Семейство Microsoft Windows Server 2008; Red Hat Enterprise Linux 5.0; Sun Solaris 10
Размеры (Д × Ш × В), мм	5U, 620 × 430 × 220
Блок питания	2x550 Вт

Роли сервера

Процесс установки серверной операционной системы на компьютер не зависит от того, для чего она будет использоваться после установки. Например, серверную систему можно установить и на обычный компьютер, который не подразумевает никакого активного участия в сетевой «жизни».

Только после того как операционная система уже установлена, происходит назначение ей определенных ролей, выбор которых зависит от того, для чего планируется использовать данный сервер. Многое обуславливает также его мощность. Чем сервер мощнее, тем больше ролей можно ему назначить.

Любая операционная система дает возможность назначать серверу достаточно много разнообразных ролей, которые позволят расширить возможности административного управления локальной сетью. Операционная система Windows Server 2008 R2 позволяет назначать серверу следующие роли.

□ **DHCP-сервер.** Механизм, с помощью которого настраивается система динамической IP-адресации, а также правила выдачи IP-адресов согласно существующим спискам или диапазонам.

□ **DNS-сервер.** С помощью этого механизма обеспечивается разрешение DNS-имен при работе с TCP/IP-сетями.

□ **Hyper-V.** Роль, позволяющая использовать мощность процессора для организации работы с виртуальными машинами, что дает возможность, например, устанавливать на сервер несколько операционных систем.

□ **Веб-сервер (IIS).** Система развертывания веб-приложений и обеспечения доступа к ним с применением существующих механизмов.

□ **Доменные службы Active Directory (AD DS).** Один из важнейших системных механизмов, позволяющий создавать и хранить данные об учетных записях сетевых пользователей, обеспечивая им доступ к ресурсам сети на основе определяемых прав.

□ **Сервер приложений.** Обеспечивает развертывание и управление любым типом бизнес-приложений, в частности основывающихся на архитектуре «клиент – сервер».

□ **Службы Active Directory облегченного доступа к каталогам (AD LDS).** Хранилище данных приложений, использующих службу каталогов и не зависящих от развернутой службы Active Directory.

□ **Службы UDDI.** Механизм, предназначенный для работы с интрасетями, основная задача которого – обнаружение, описание и интеграция сведений об используемых локальных веб-сервисах и веб-службах.

□ **Службы печати.** Система контроля и управления сетевой печатью, которая используется для централизованного контроля над процессом печати с участием сетевых принтеров и серверов печати.

□ **Службы политики сети и доступа.** Один из механизмов сохранения работоспособности и безопасности работы сети путем предоставления сведений о групповых политиках сети, маршрутизации и удаленном доступе и другой важной информации.

□ **Службы развертывания Windows.** Применяются для быстрого развертывания и установки операционных систем Windows в удаленном режиме. При этом можно использовать сценарии автоматической установки, что очень эффективно при работе компьютеров с одинаковой аппаратной конфигурацией.

□ **Службы сертификации Active Directory (AD CS).** Мощный механизм управления процессом сертификации приложений, позволяющий сделать их использование более безопасным и доверенным.

□ **Службы терминалов.** Очень полезная и часто используемая роль, позволяющая пользователям сети получать доступ к удаленному Рабочему столу для использования ресурсов и вычислительной мощности сервера при работе с общими приложениями.

□ **Службы управления правами Active Directory (AD RMS).** Система управления лицензиями, которая позволяет защитить данные от несанкционированного доступа: прошел авторизацию – получил доступ к защищенным данным.

□ **Службы федерации Active Directory (AD FS).** Система единого способа входа в сеть, позволяющая проверять подлинность пользователя в течение всего времени длительности сеанса связи с использованием разных программных средств.

□ **Файловые службы.** Система хранения и доступа к общим файловым ресурсам, которая дает возможность производить репликацию (синхронизацию содержимого разных копий) и поиск файлов, управлять общими папками и т. д.

□ **Факс-сервер.** Механизм, позволяющий организовать прием и отправку факсимильных сообщений, а также управлять сетевым факсимильным устройством. При этом обеспечивается система архивирования факсимильных сообщений, ведение журнала использования факса, система маршрутизации входящих сообщений и т. д.

Глава 24
Установка контроллера домена и DNS-сервера

Практически любая большая локальная сеть, если не брать во внимание «домашние» сети, не может нормально функционировать и предоставлять необходимый уровень безопасности без использования доменной структуры. Никакой другой способ работы сети не может обеспечить нормального уровня контроля пользователей и всего, что происходит в сети. По этой причине установка контроллера домена – просто необходимая мера обеспечения работоспособности локальной сети.

Далее мы рассмотрим пример установки контроллера домена на основе операционной системы Windows Server 2008 R2 Enterprise, которая на сегодняшний день предоставляет максимум возможностей при максимальном уровне безопасности.

Как уже упоминалось ранее, сразу после установки операционная система ждет от вас указания того, чем она будет заниматься, то есть назначения роли. Об этом постоянно напоминает окно, появляющееся при запуске операционной системы (рис. 24.1).

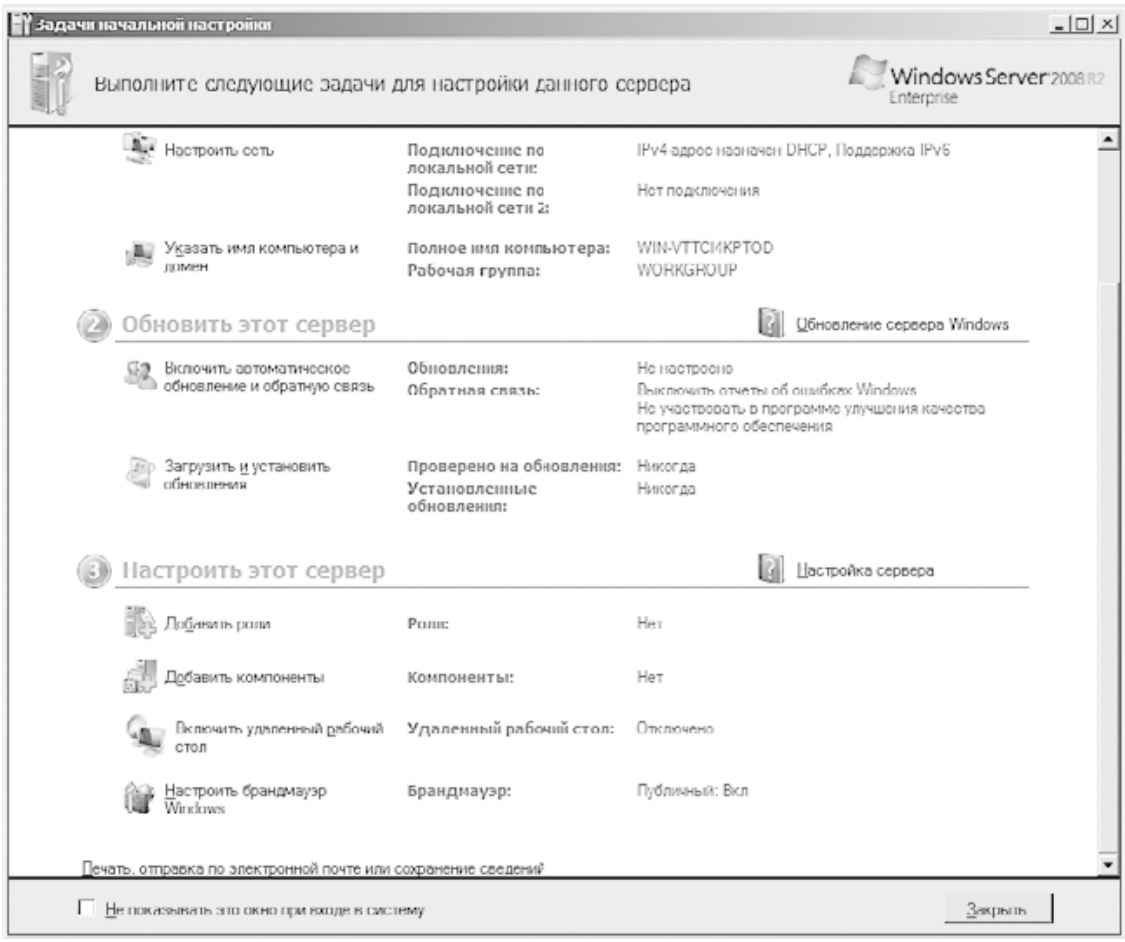

Рис. 24.1. Задачи начальной настройки сервера

В этом окне можно отслеживать критичные для работы сервера параметры. В частности, из нашего примера видно, что существующие сетевые подключения используют динамическую IP-адресацию, что станет причиной появления соответствующей ошибки в процессе установки контроллера домена, в чем вы убедитесь далее.

Итак, приступим к установке контроллера домена и DNS-сервера. Кстати, у вас может возникнуть вопрос, почему установка DNS-сервера происходит именно на этом этапе. В

принципе, DNS-сервер можно поставить и отдельно. Операционная система просто реагирует на то, что контроллера домена нет, а значит, нет и DNS-сервера, поэтому и предлагает его установить. Это вполне логичное предложение, поэтому не стоит от него отказываться.

Чтобы начать процесс установки, пройдите по ссылке Добавить роли, которая находится в нижней части окна, показанного на рис. 24.1. Это приведет к открытию мастера добавления ролей, который будет помогать вам добавить роли (рис. 24.2).

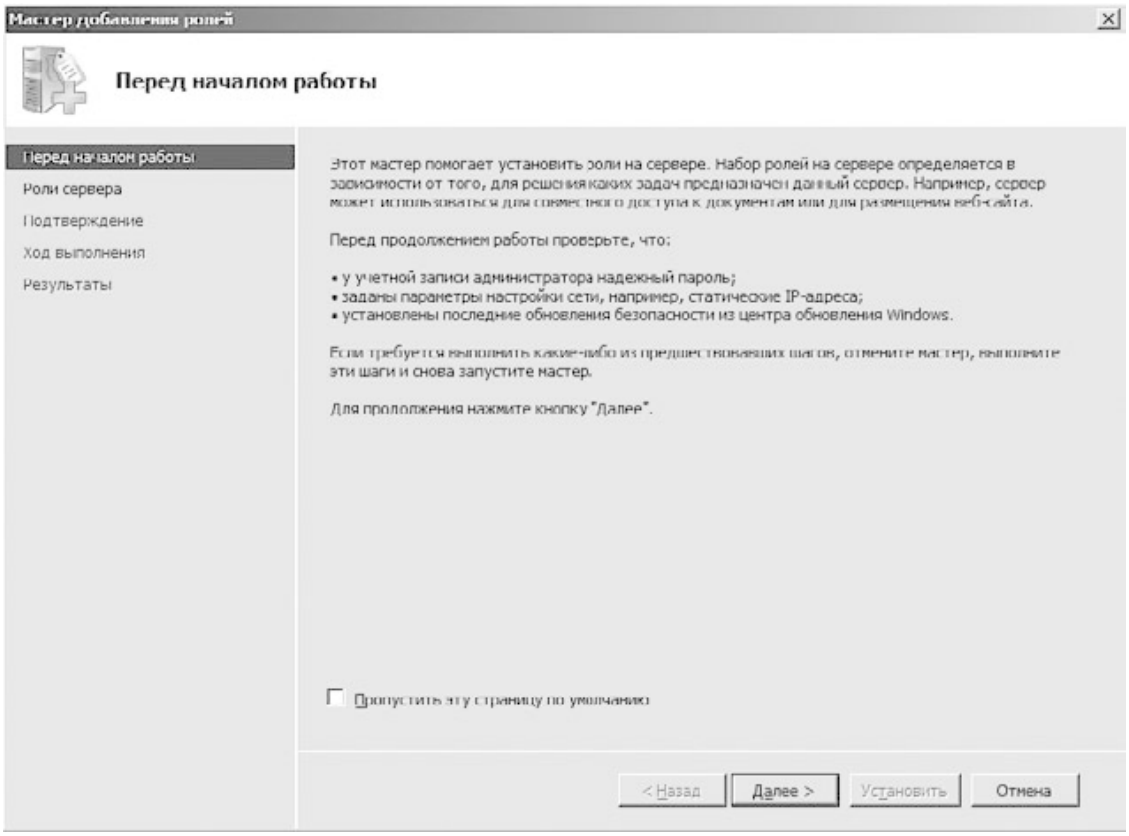

Рис. 24.2. Начальное окно мастера добавления ролей

Мастер начинает работу с информации о том, что перед заданием любой роли желательно выполнить определенные приготовления, например установить обновления системы или убедиться, что администратор использует надежный пароль. В принципе, эти сведения носят лишь рекомендационный характер, поэтому особого внимания на них обращать не стоит.

В следующем окне вы увидите список ролей, которые можно настроить на данном сервере (рис. 24.3).

Краткое описание ролей и их возможностей мы уже рассматривали ранее при описании выбора серверной операционной системы и управляющего сервера (см. гл. 23).

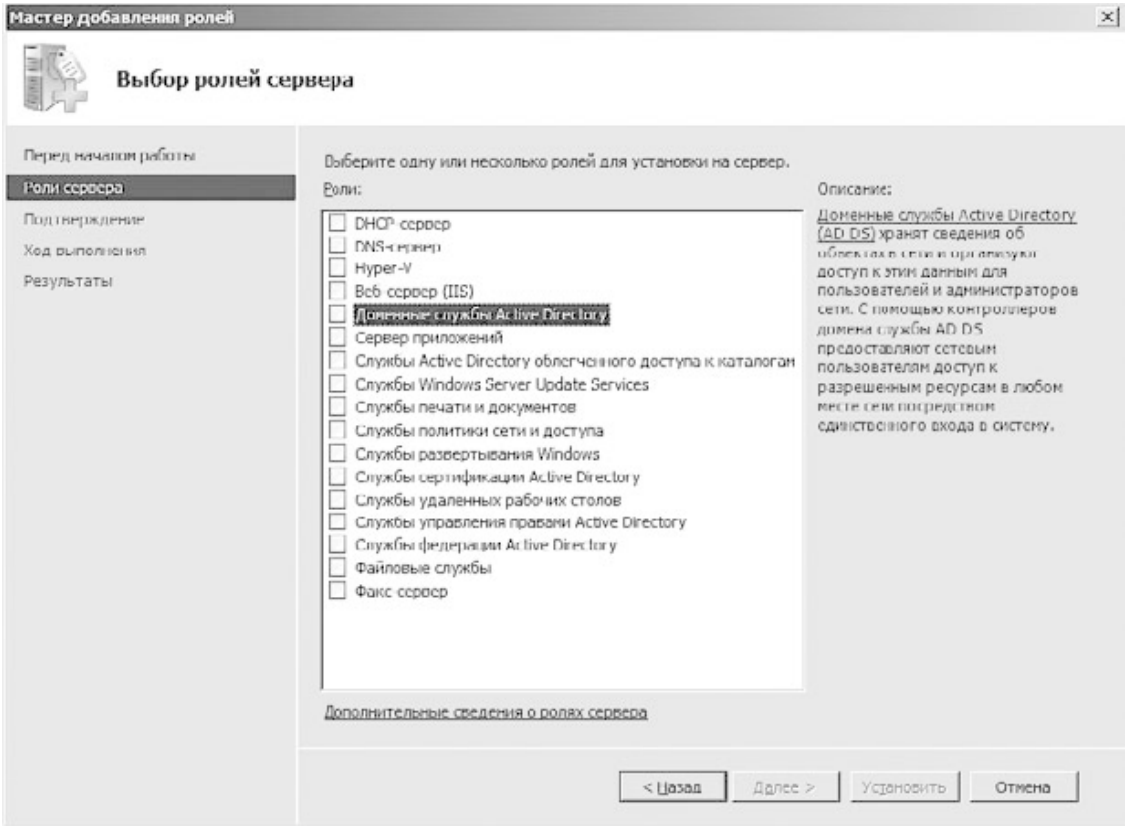

Рис. 24.3. Список доступных ролей сервера

Как вы уже заметили, такой роли, как «Контроллер домена», в списке не существует, и это легко объяснить: чтобы задать такую роль, требуется установить некоторые составляющие части этого сложного механизма, в частности роль **Доменные службы Active Directory**. По этой причине и начнем с установки данной роли.

При попытке установить флажок возле этой роли появится окно (рис. 24.4).

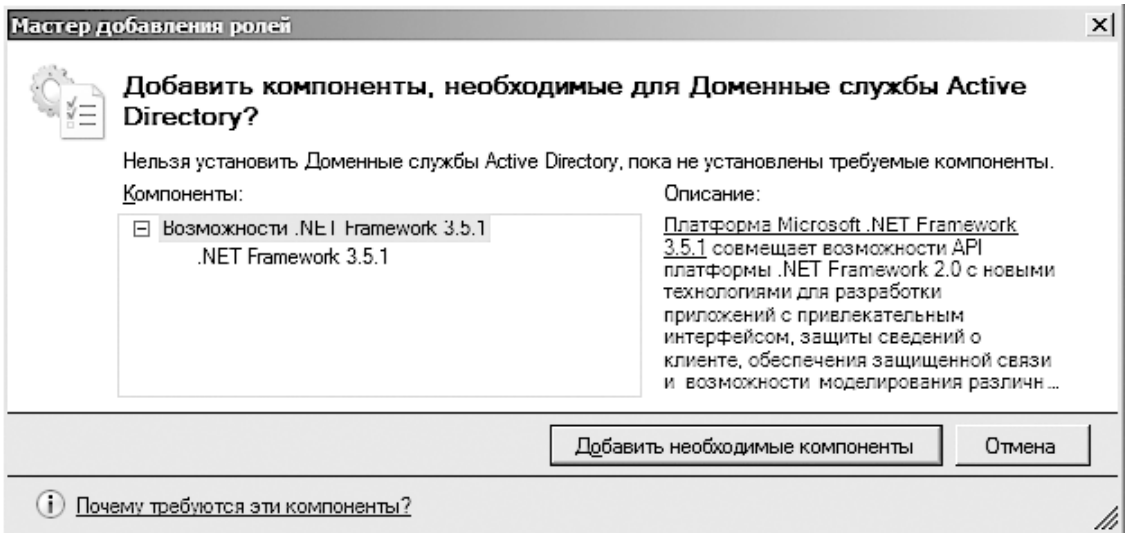

Рис. 24.4. Предупреждение о необходимости установки дополнительных компонентов

Этим окном мастер предупреждает вас о том, что установка выбранной роли невозможна без установки дополнительных компонент в виде .NET Framework 3.5.

Смысл появления этого сообщения не совсем понятен, поскольку мы в любом случае настроены установить нужную роль, а значит, и все компоненты, которые для этого нужны. Хотя, возможно, мастер тем самым просто предупреждает вас, что если вы решите в какой-

то момент удалить .NET Framework 3.5, то это приведет к сбою сервера. Чтобы не прерывать процесс установки роли, выбираем однозначный ответ – **Добавить необходимые компоненты**.

Мастер отобразит следующее окно (рис. 24.5), где находится короткая информация о роли, которую мы собираемся установить.

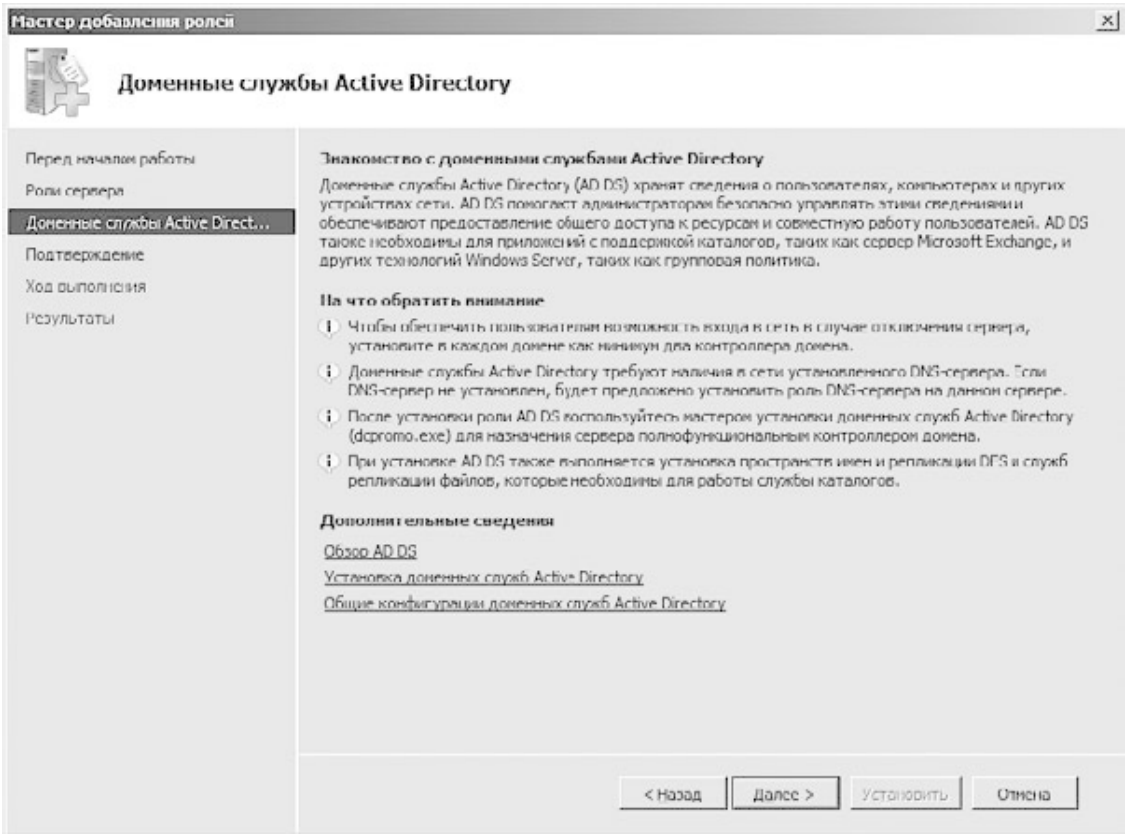

Рис. 24.5. Информация об устанавливаемой роли сервера

Это позволит вам убедиться в том, что устанавливаемая роль – действительно то, что нам нужно. Если это не так, вы всегда можете вернуть к списку выбора ролей, используя для этого кнопку **Назад**. Подтвердив свой выбор нажатием кнопки **Далее**, продолжаем процесс установки роли.

Следующее окно – последний шаг подготовки к установке роли **Доменные службы Active Directory** (рис. 24.6).

Поскольку никаких критичных настроек или действий в процессе выбора параметров установки роли мы не производили, то особо раздумывать над тем, правильно мы это сделали или нет, не имеет смысла. По этой причине просто подтверждаем готовность к установке нажатием кнопки **Установить**.

После этого операционная система приступит к установке нужных для функционирования выбранной роли компонентов, отображая процесс установки с помощью индикатора в нижней части окна. Установка не занимает много времени, и достаточно скоро вы увидите окно, отображающее результат установки роли (рис. 24.8).

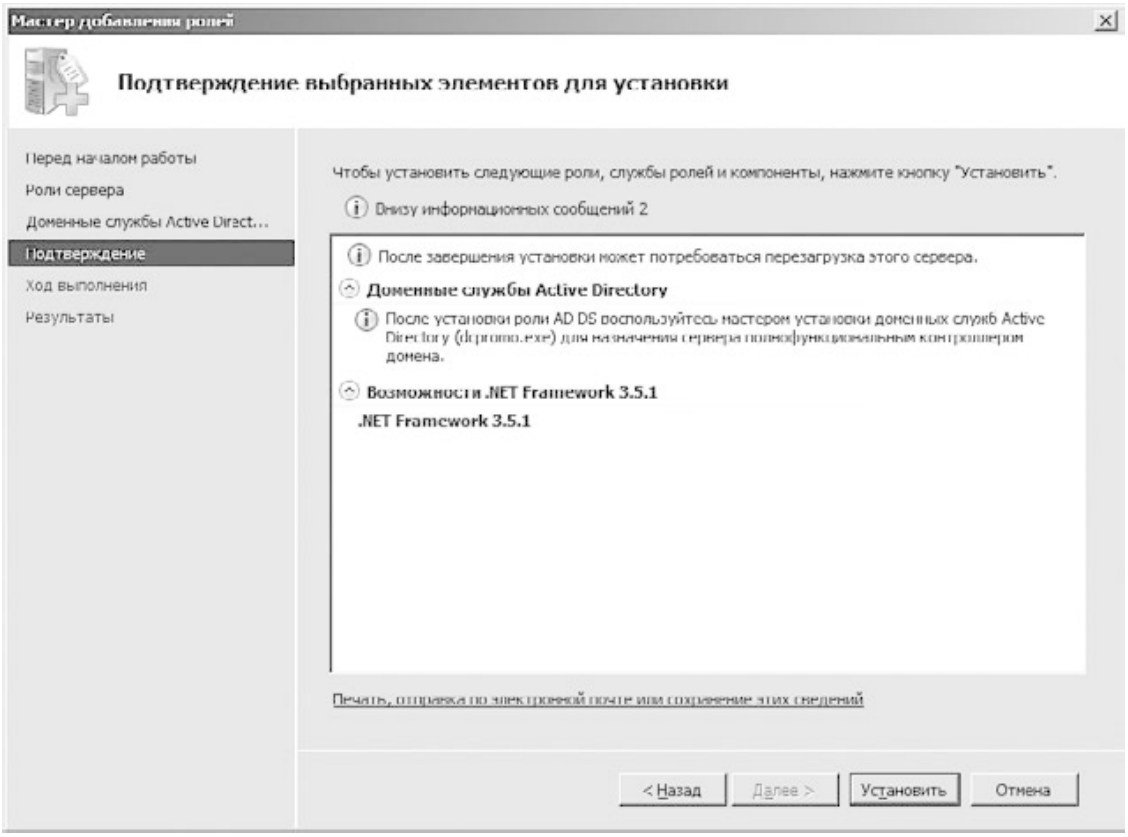

Рис. 24.6. Все готово для установки выбранной роли

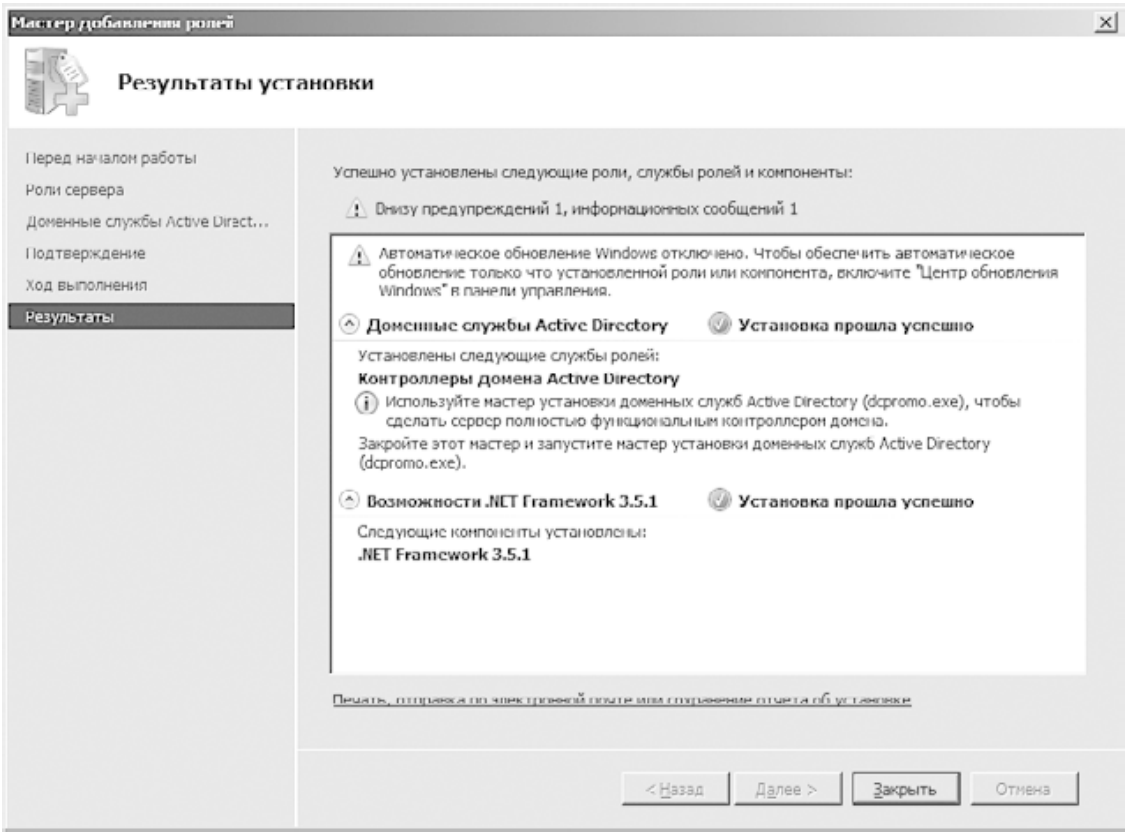

Рис. 24.7. Успешная установка выбранной роли

Здесь же будут показаны основные замечания, возникшие в процессе установки компонентов, а также очень важная информация, используя которую вы сможете продолжить

установку контроллера домена. Так, чтобы добавить роль контроллера домена, после закрытия окна необходимо будет запустить системный механизм **dcpromo**, который продолжит выполнение установки.

Таким образом, после нажатия кнопки **Закрыть** откройте меню Пуск, наберите в строке поиска слово **dcpromo** и нажмите **Enter**.

После этого появится окно **Мастер установки доменных служб Active Directory** (рис. 24.8).

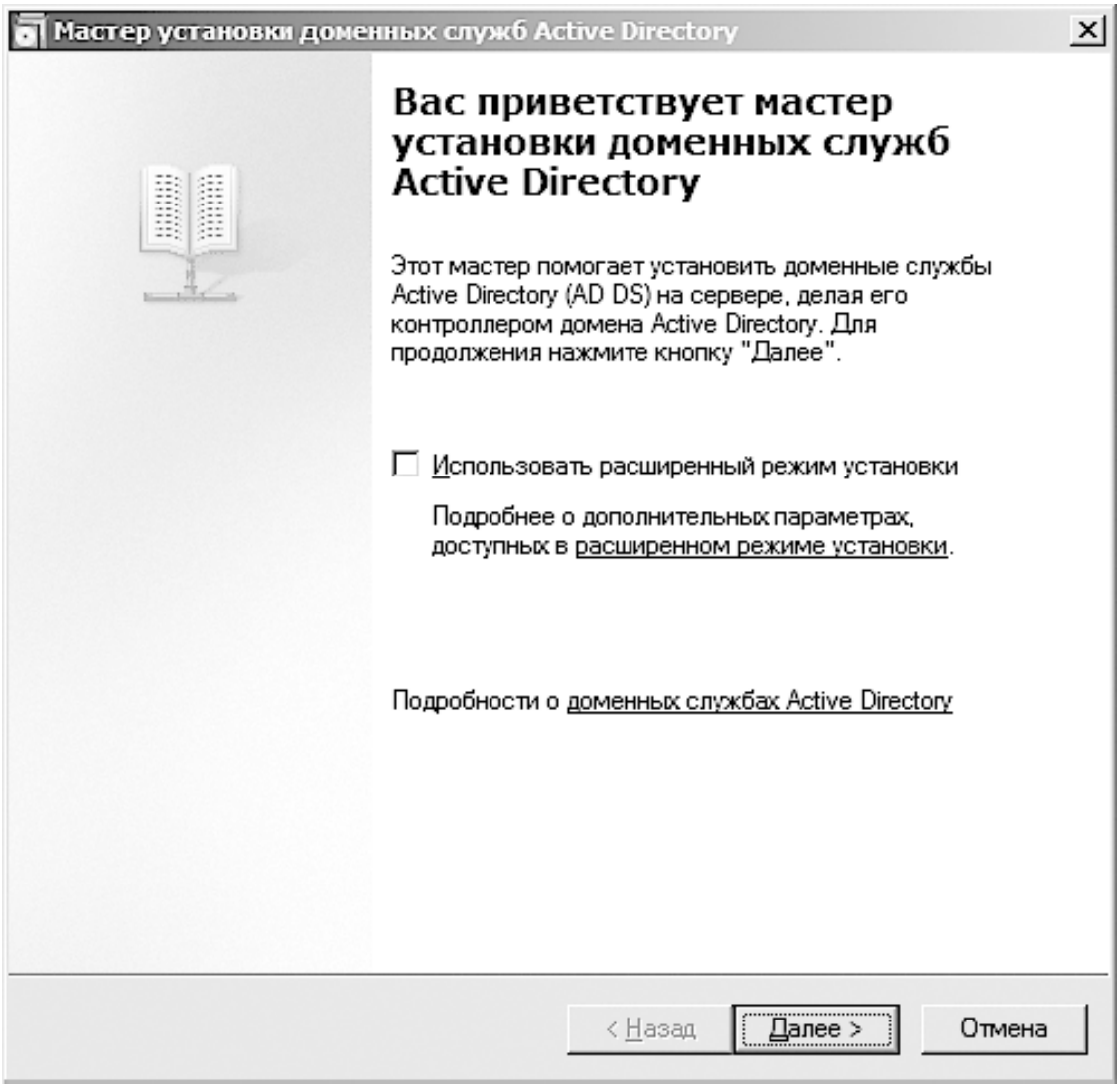

Рис. 24.8. Мастер установки доменных служб Active Directory

Судя по тому, что написано в этом окне, мы на правильном пути, поэтому смело продолжаем процесс установки.

В следующем окне вы увидите большой блок информации, предупреждающей о том, что новые возможности Windows Server 2008 R2 могут стать причиной неработоспособности некоторых методов доступа к информации с использованием шифрованного канала. Связано это с тем, что Windows Server 2008 R2 использует более безопасные и стойкие алгоритмы шифрования, реализации которых нет в ранних операционных системах даже серверного типа. Современные потребности часто заставляют отказываться от применения старых версий программного обеспечения, поэтому единственный выход – заранее планировать использование современных версий программного обеспечения.

Следующий шаг – выбор конфигурации развертывания, которая однозначно определяет не только конфигурацию сервера, но и произведенные этим действием изменения в структуре существующей локальной сети (рис. 24.9).

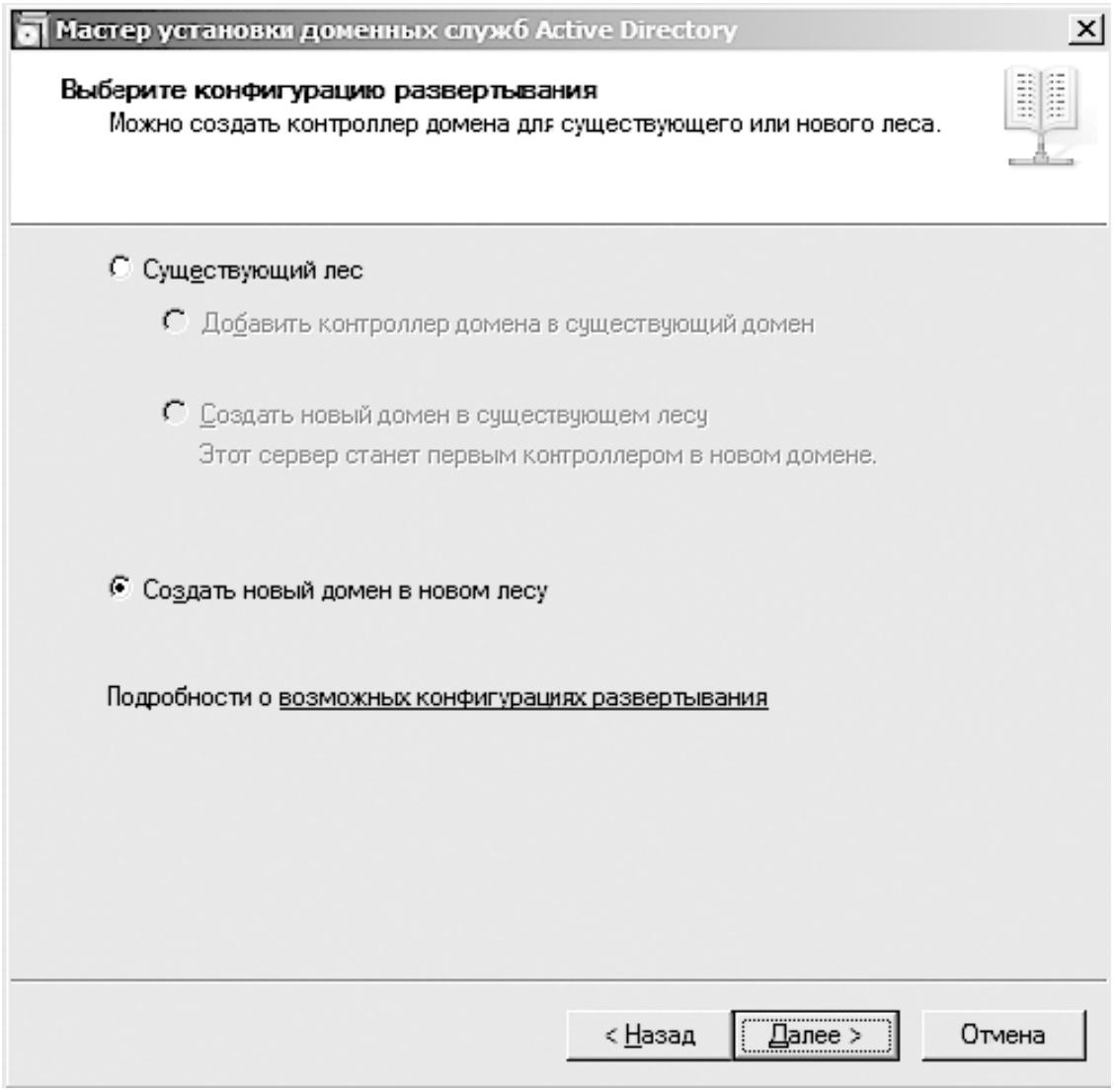

Рис. 24.9. Выбор конфигурации развертывания

Если речь идет о создании контроллера домена в новой локальной сети, в которой не используются управляющие серверы, обязательно необходимо установить переключатель в положение **Создать новый домен в новом лесу**. Если же требуется добавить новый домен в уже существующую доменную структуру, то нужно выбрать положение **Существующий лес** и указать способ добавления домена.

Мы будем рассматривать только первый вариант, то есть создание нового домена и нового леса. Установив переключатель в соответствующее положение, продолжаем процесс установки.

Следующий шаг – ввод имени домена (рис. 24.10).

Существующие стандарты предусматривают использование трехзвенного доменного имени: название домена должно состоять из уникального имени с добавлением имени домена верхнего уровня, то есть указание имени domain, является недопустимым и приводит к появлению соответствующего сообщения. Название должно состоять как минимум из двух слов, разделенных десятичной точкой. В нашем случае в качестве имени применяется выдуманное словосочетание **rene. local**.

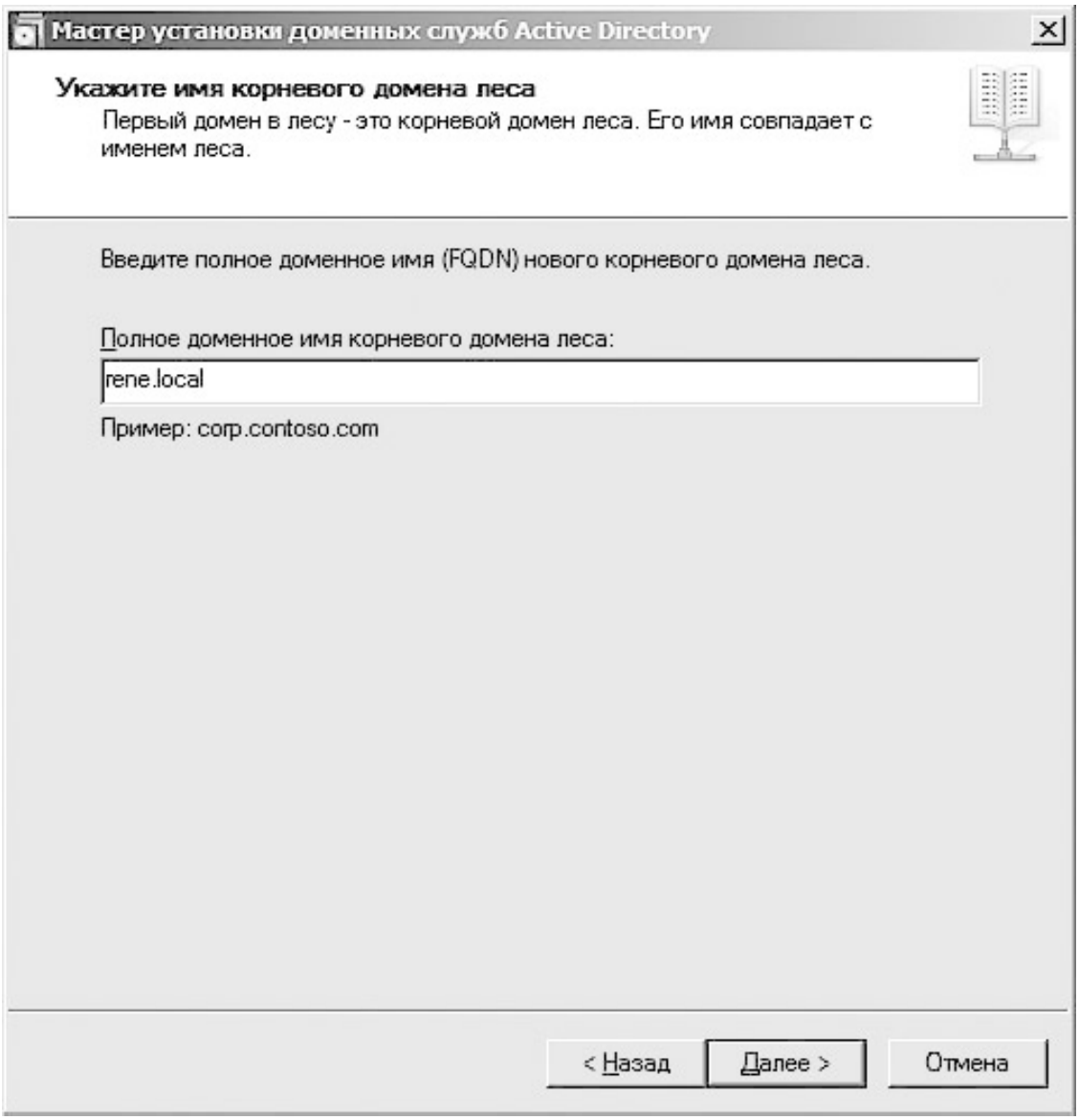

Рис. 24.10. Указание имени домена

После нажатия кнопки Далее мастер проверит уникальность имени леса и имени NetBios-сервера, после чего предложит вам выбрать режим работы леса (рис. 24.11).

Есть четыре режима: **Windows 2000, Windows Server 2003, Windows Server 2008 и Windows Server 2008 R2**. Последний режим позволяет использовать самые новые возможности Active Directory и других механизмов, но тем самым может сделать невозможным работу более старых серверных операционных систем. Применение же первого режима позволит использовать любые серверные операционные системы, но с ограниченными возможностями. Только системный администратор может решить, какой режим работы леса оптимальный в зависимости от того, серверы с какими операционными системами планируется применять в локальной сети.

Для примера мы будем использовать режим **Windows Server 2008 R2**. Выбираем его из списка и продолжаем процесс установки.

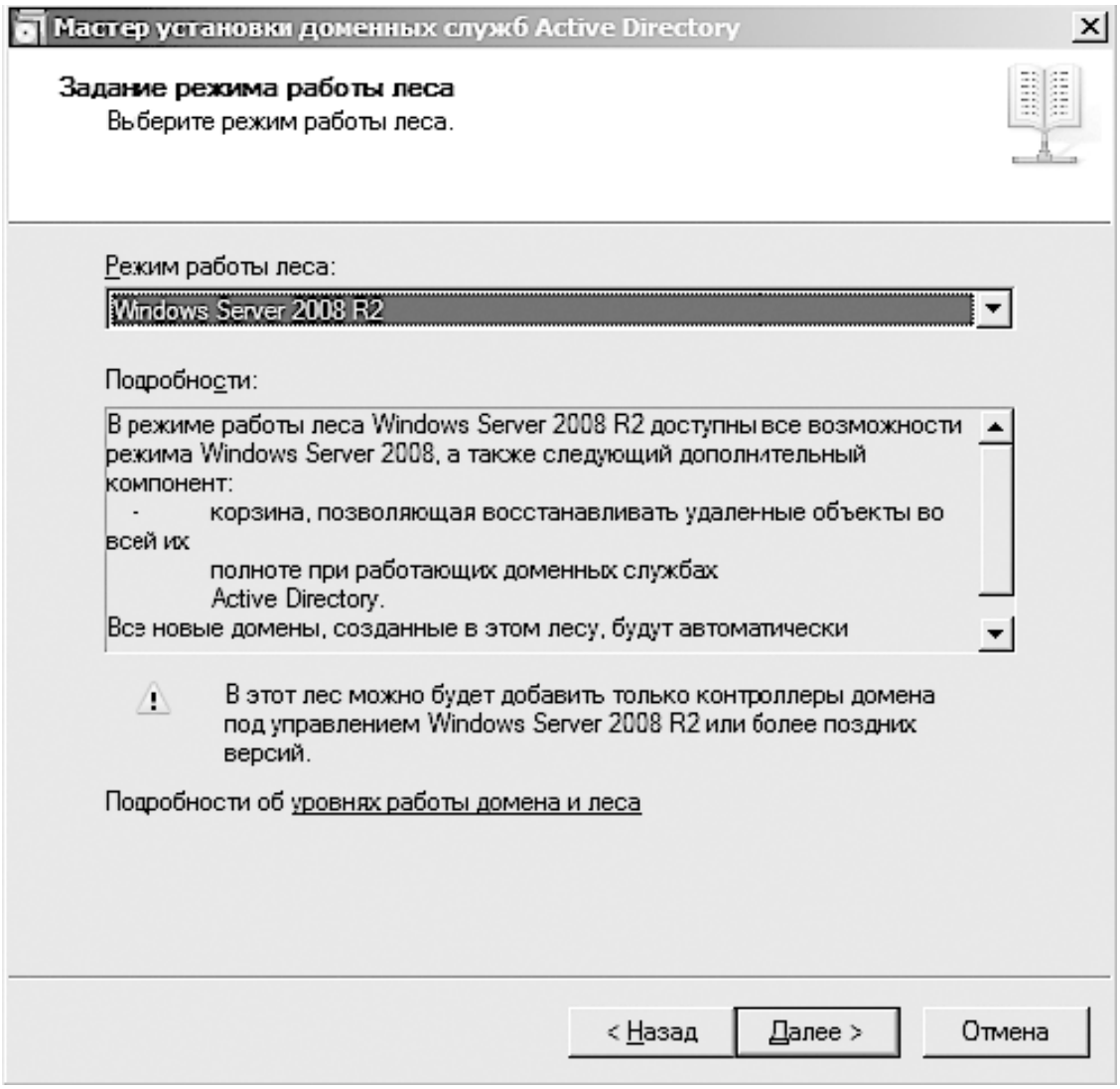

Рис. 24.11. Задание режима работы леса

Прежде чем перейти к следующему этапу, мастер произведет попытку найти в сети функционирующий DNS-сервер. После этого появится окно (рис. 24.12).

Если DNS-сервер обнаружен не будет, в этом окне вам предложат установить данную роль сервера, объясняя значимость этой процедуры. Даже если вы откажетесь от этого шага, вы сможете установить DNS-сервер позже, но если он действительно вам нужен и должен функционировать именно на этом сервере, просто нажмите кнопку Далее для продолжения процесса установки.

Затем наступает интересный момент, о котором было упомянуто в начале процесса установки. Обнаружив, что сетевые адаптеры сервера используют динамические IP-адреса, мастер отобразит соответствующее окно с предупреждением (рис. 24.13).

Сам принцип доменной структуры локальной сети подразумевает применение статического IP-адреса у управляющего сервера, а также у других важных объектов. По этой причине, прежде чем продолжить, необходимо настроить сетевое подключение или подключения на использования статического IP-адреса. Для этого откройте окно свойств сетевого подключения, которое будет использоваться для обслуживания сети, и дважды щелкните на строке **Протокол Интернета версии 4 (TCP/IPv4)**.

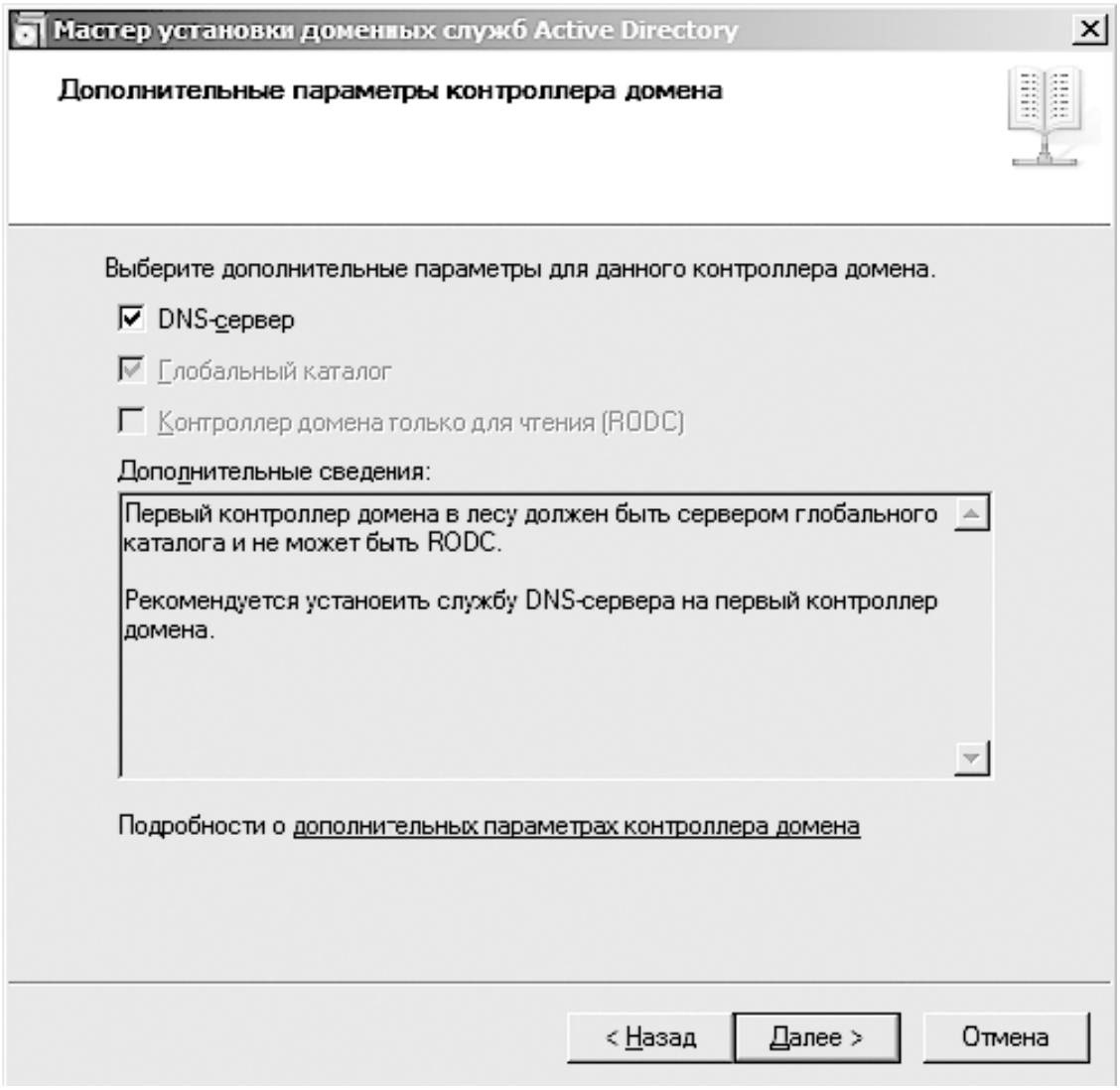

Рис. 24.12. Указание дополнительных параметров

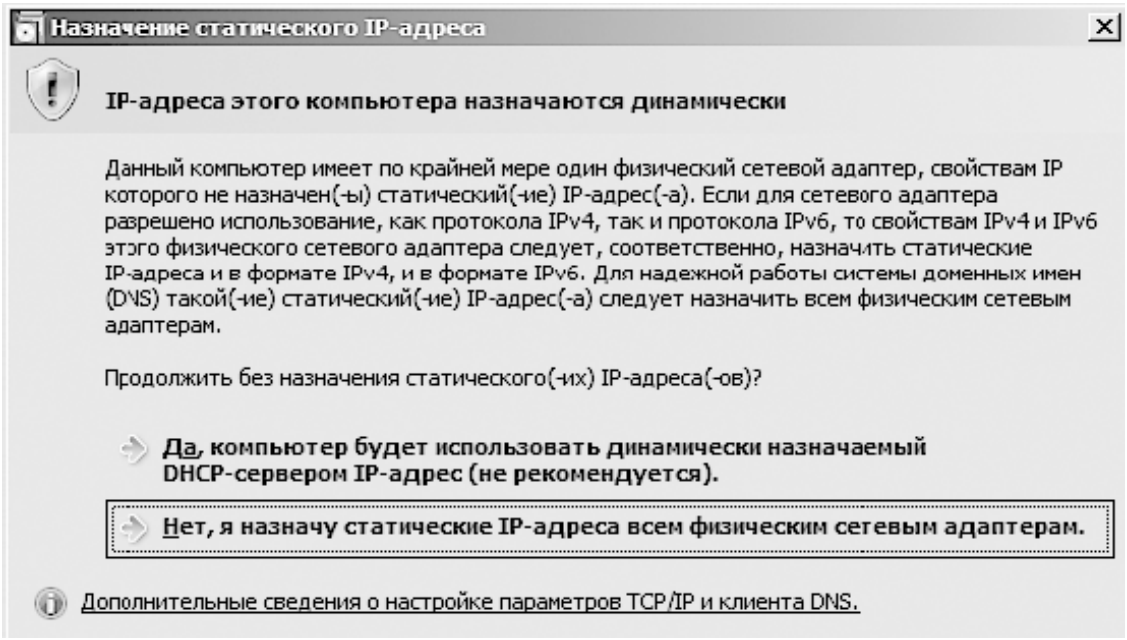

Рис. 24.13. Предупреждение об использовании динамической IP-адресации

В открывшемся окне (рис. 24.14) введите IP-адрес, который вы планируете использовать для контроллера домена. Кроме того, такой же IP-адрес введите в поле **Предпочитаемый DNS-сервер**.

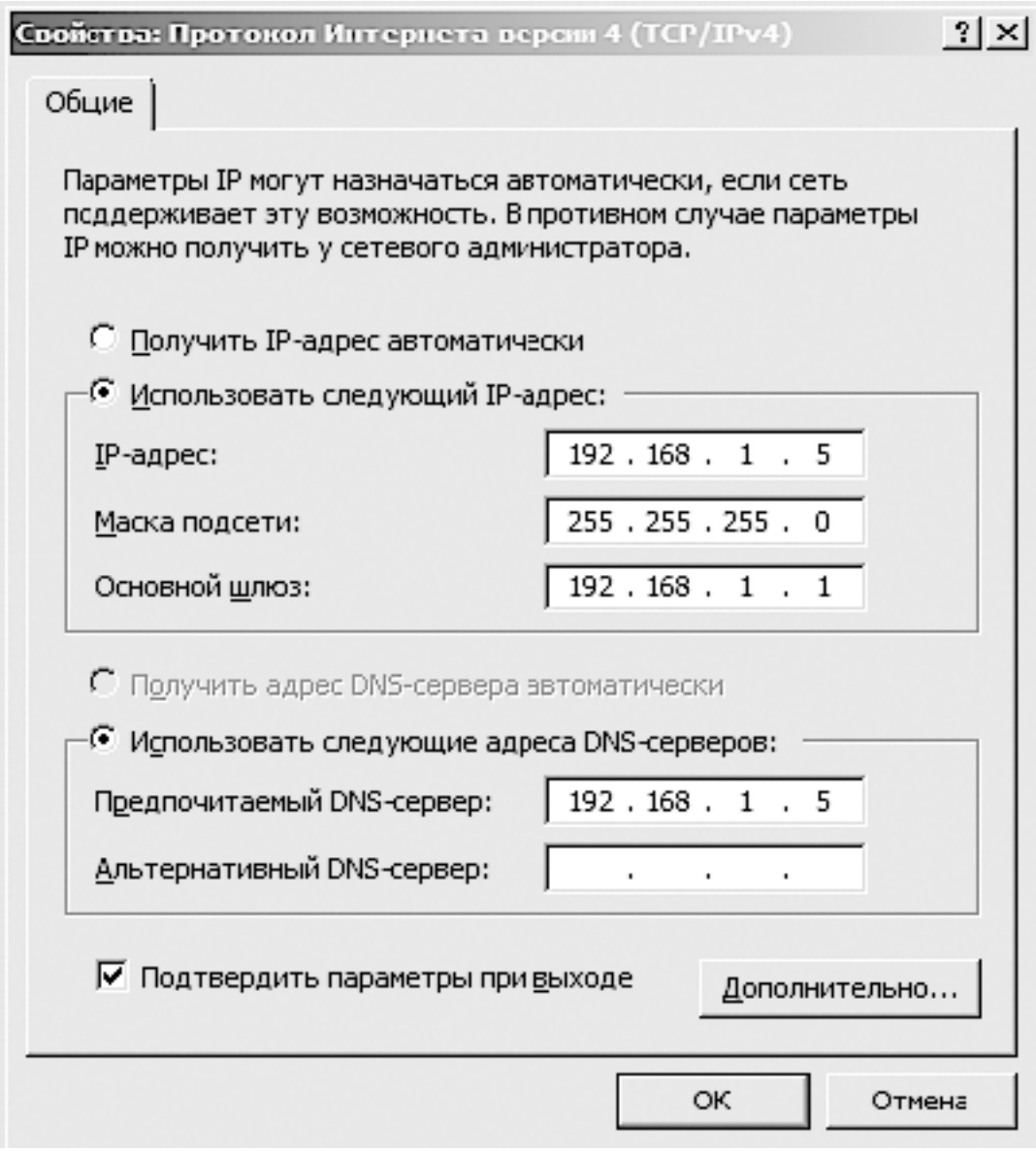

Рис. 24.14. Настройка IP-адреса

Аналогичным образом следует поступить с остальными сетевыми подключениями, которые есть на сервере, либо пока временно отключить их.

После этих действий вернитесь к окну, показанному на рис. 24.13, и нажмите кнопку с названием второго варианта решения. Проанализировав сделанные вами изменения, мастер перейдет к следующему шагу – настройке расположения разного рода баз данных и журналов, которые будут использоваться для хранения служебной информации Active Directory. Пути размещения этих объектов, как правило, оставляют заданными по умолчанию, хотя мастер и советует выбирать для их хранения более надежный источник. Затем потребуется ввести пароль, который будет применяться в случае восстановления службы каталогов.

После ввода всей необходимой информации мастер готов приступить к процессу копирования файлов и внесения необходимых изменений в реестр системы (рис. 24.15).

Прежде чем начать процесс изменения операционной системы, вы еще раз можете проконтролировать параметры, указанные в ходе каждого этапы работы мастера, и при необхо-

димости повторно вернуться к определенному шагу. Если же все параметры заданы верно, нажмите кнопку **Далее**.

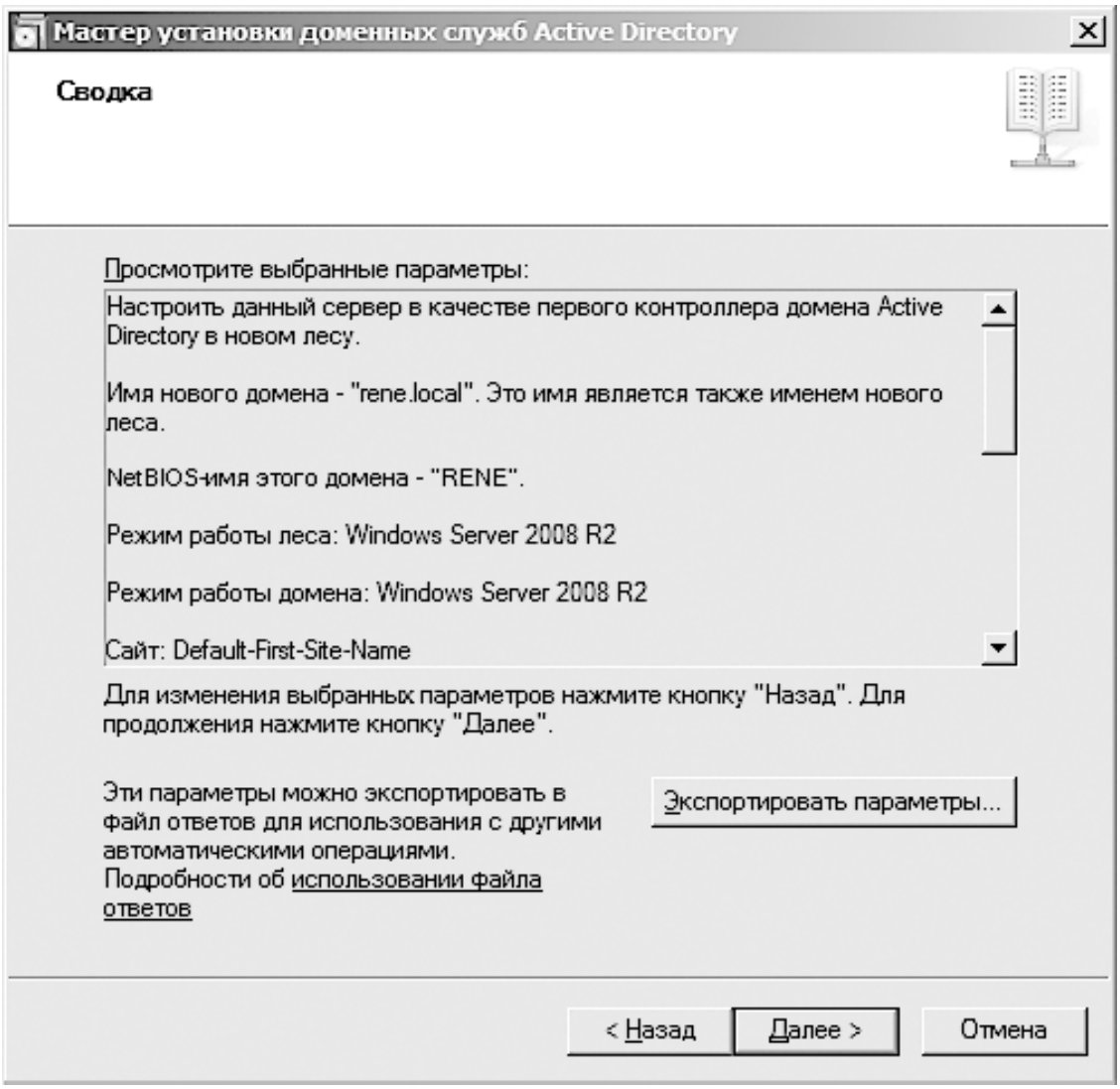

Рис. 24.15. Все готово к началу изменений

После выполнения всех необходимых операций мастер сообщит, что процесс установки доменных служб Active Directory завершен, и предложит перезагрузить компьютер. После перезагрузки компьютера потребуется еще немного времени на настройку и запуск нужных служб, что будет выполнено в автоматическом режиме. Вам остается только дождаться завершения этого процесса.

Глава 25
Добавление роли DHCP-сервера

DHCP-сервер – один из мощнейших и полезнейших инструментов. Без его использования функционирование большой локальной сети сопряжено с определенными трудностями: каждое подключение нового рабочего места требует ручной настройки IP-адреса, маски подсети, IP-адреса DNS-сервера и т. д. Кроме того, доступный диапазон IP-адресов быстро заканчивается, что делает невозможным работу в сети большого количества компьютеров.

Как и роль контроллера домена или DNS-сервера, роль DHCP-сервера легко установить с помощью соответствующего механизма – мастера добавления ролей. Его окно открывается каждый раз, когда происходит загрузка операционной системы. Выбрав в нем пункт **Добавить роли**, вы увидите окно (рис. 25.1).

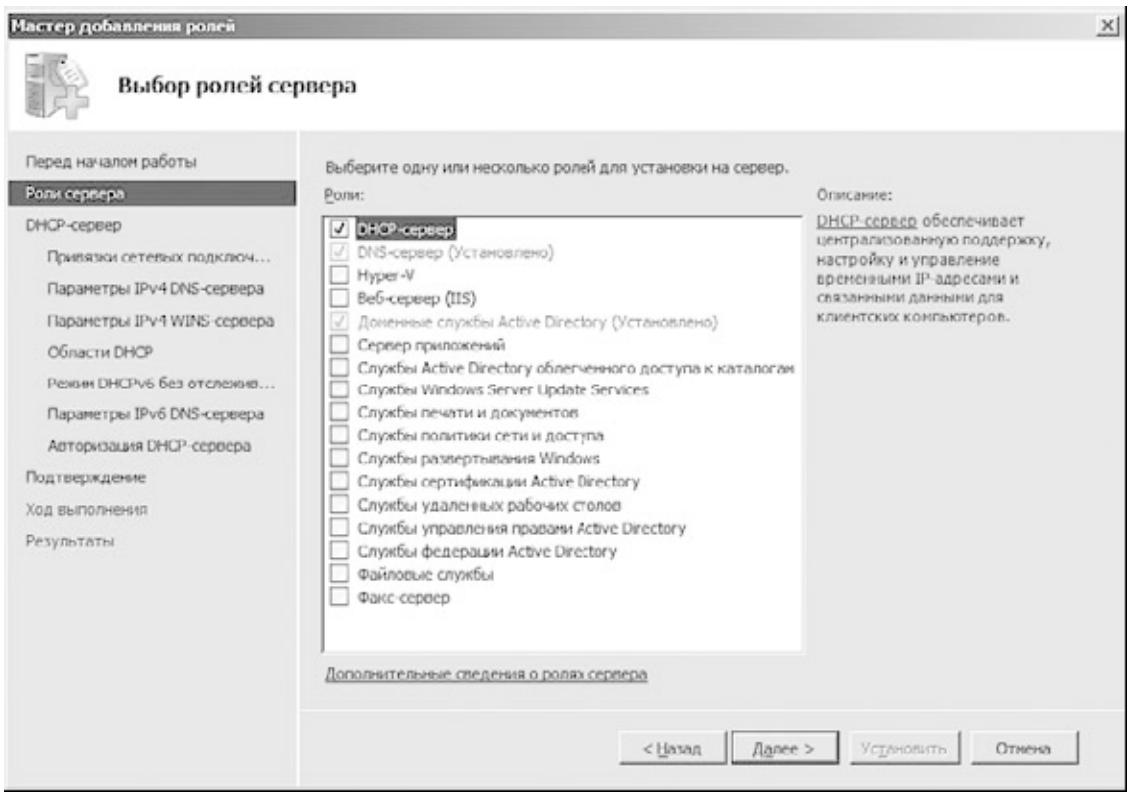

Рис. 25.1. Использование мастера для добавления роли DHCP-сервера

Чтобы начать установку DHCP-сервера, установите флажок **DHCP-сервер** в списке доступных ролей и нажмите кнопку **Далее**.

После ознакомления с описанием того, для чего предназначен DHCP-сервер, можно перейти к настройке параметров установки. Прежде всего вам необходимо будет указать IP-адрес сетевого подключения сервера, которое будет обслуживать запросы к DHCP-серверу (рис. 25.2).

Чтобы помочь вам выбрать, мастер проанализирует существующие сетевые подключения и отобразит их в списке. В нашем случае используется только одно сетевое подключение, поэтому ошибиться с выбором невозможно.

В следующем окне (рис. 25.3) нужно будет указать или подтвердить параметры, которые автоматически рассылают рабочие станции при выделении динамического IP-адреса.

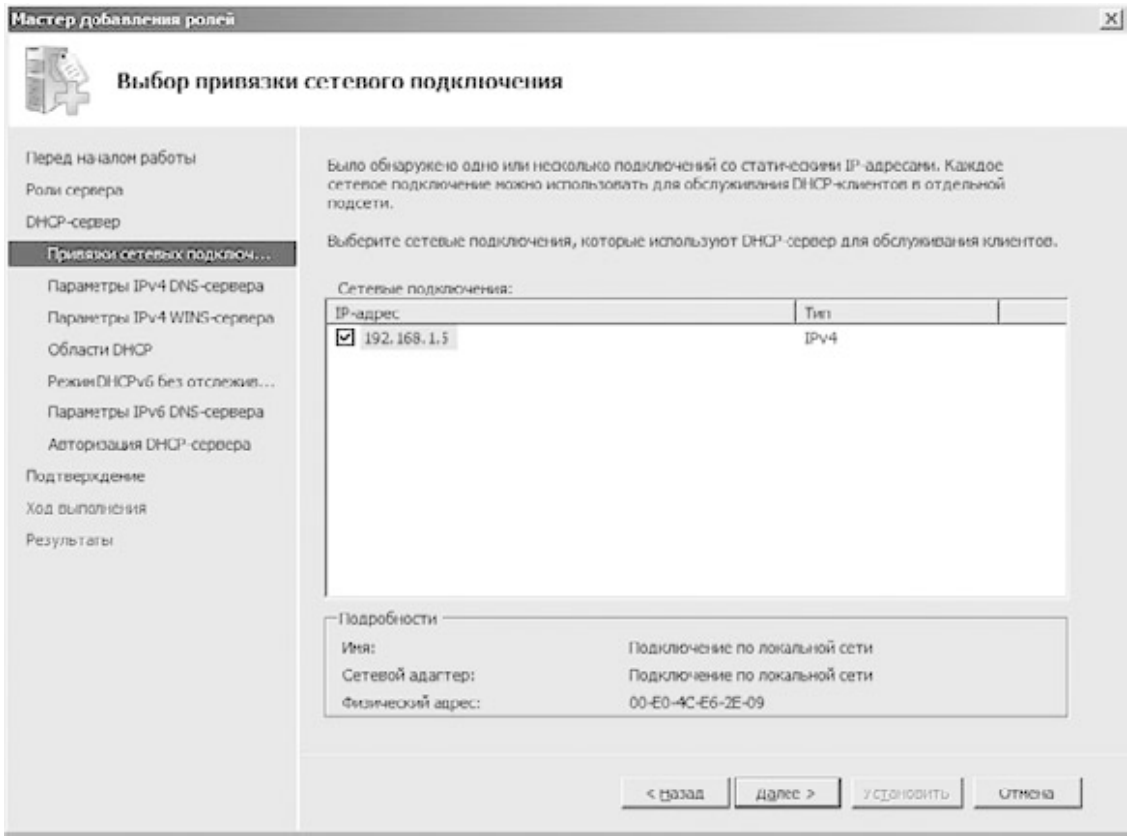

Рис. 25.2. Выбор сетевого интерфейса

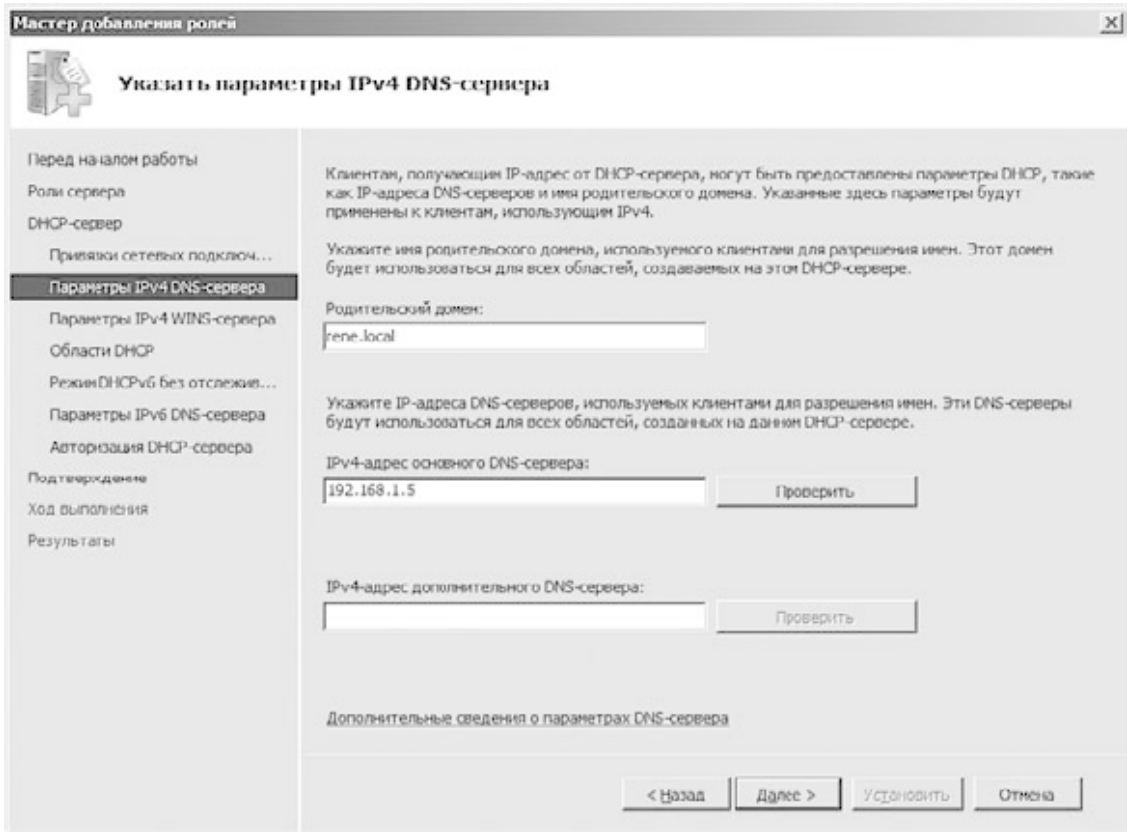

Рис. 253. Параметры DNS-сервера

Как правило, настройки здесь оставляют без изменения, но если в сети существует или планируется альтернативный DNS-сервер, здесь можно указать IP-адрес этого сервера.

Далее необходимо задать параметры WINS-сервера (рис. 25.4).

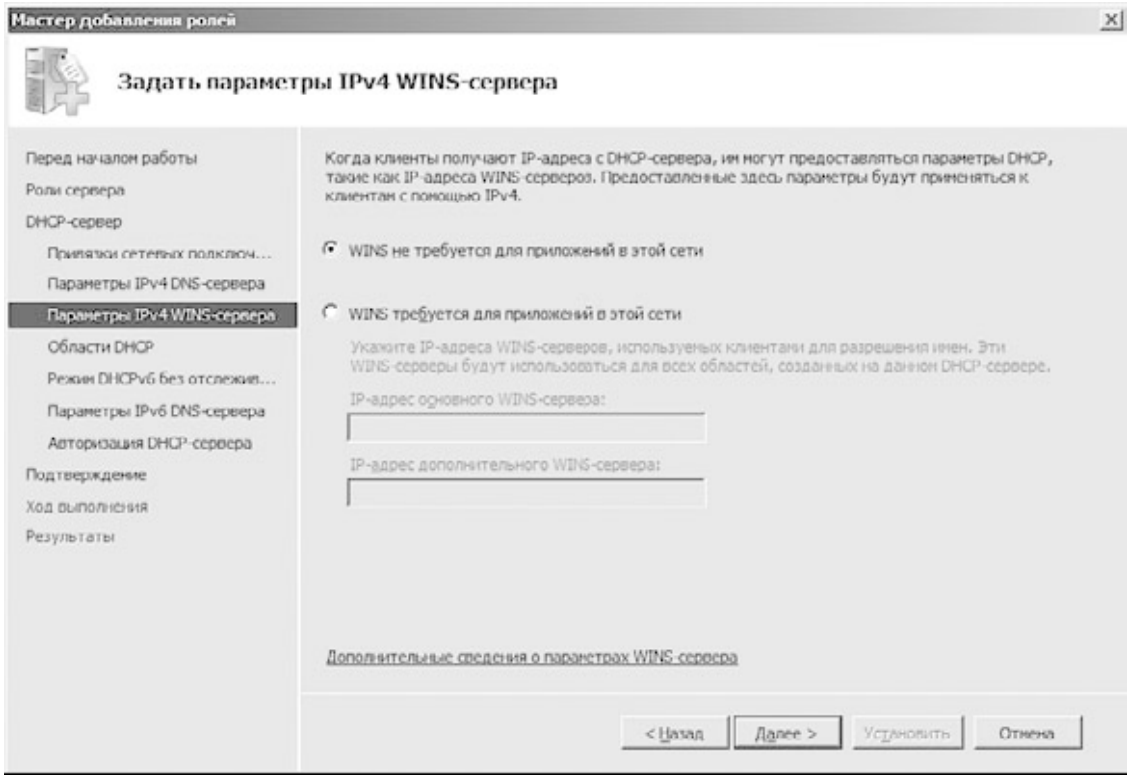

Рис. 25.4. Выбор параметров WINS-сервера

Применение WINS-сервера подразумевает обслуживание рабочих станций, использующих NetBIOS-имена для доступа к ресурсам других компьютеров. Современные операционные системы начиная с Windows 2000 обходятся без применения NetBIOS-имен. Поэтому если в сети не будут использоваться компьютеры с операционной системой ниже Windows 2000 (например, Windows 98), то смысла в применении WINS-сервера нет, тем более что это позволит не загружать работой DHCP-сервер. Установив переключатель в положение **WINS не требуется для приложений в этой сети**, продолжаем процесс установки.

Далее вам будет предложено настроить диапазоны областей IP-адресов, которые будут использоваться для обеспечения как динамической, так и статической IP-адресации. Как правило, этот этап настройки DHCP-сервера выполняется уже средствами самого DHCP-сервера, когда его установка завершена, поэтому сейчас его можно смело пропустить.

Следующий шаг – настройка режима работы DHCP-сервера для случаев, когда требуется обслуживание компьютеров, использующих протокол TCP/IPv6 (рис. 25.5).

Поскольку полноценная поддержка функционирования протокола TCP/IPv6 пока не налажена, нет смысла дополнительно нагружать сервер ненужными обработками, поэтому оставляем значение параметра по умолчанию.

Следующий шаг требует настройки параметров DHCP-сервера, которые будут тсылаться клиентам, использующим динамическую IP-адресацию с примененим протокола TCP/IPv6. Аналогично, оставляем значения параметров без изменения и переходим к последнему шагу – указанию настроек авторизации DHCP-сервера в механизме Active Directory (рис. 25.6).

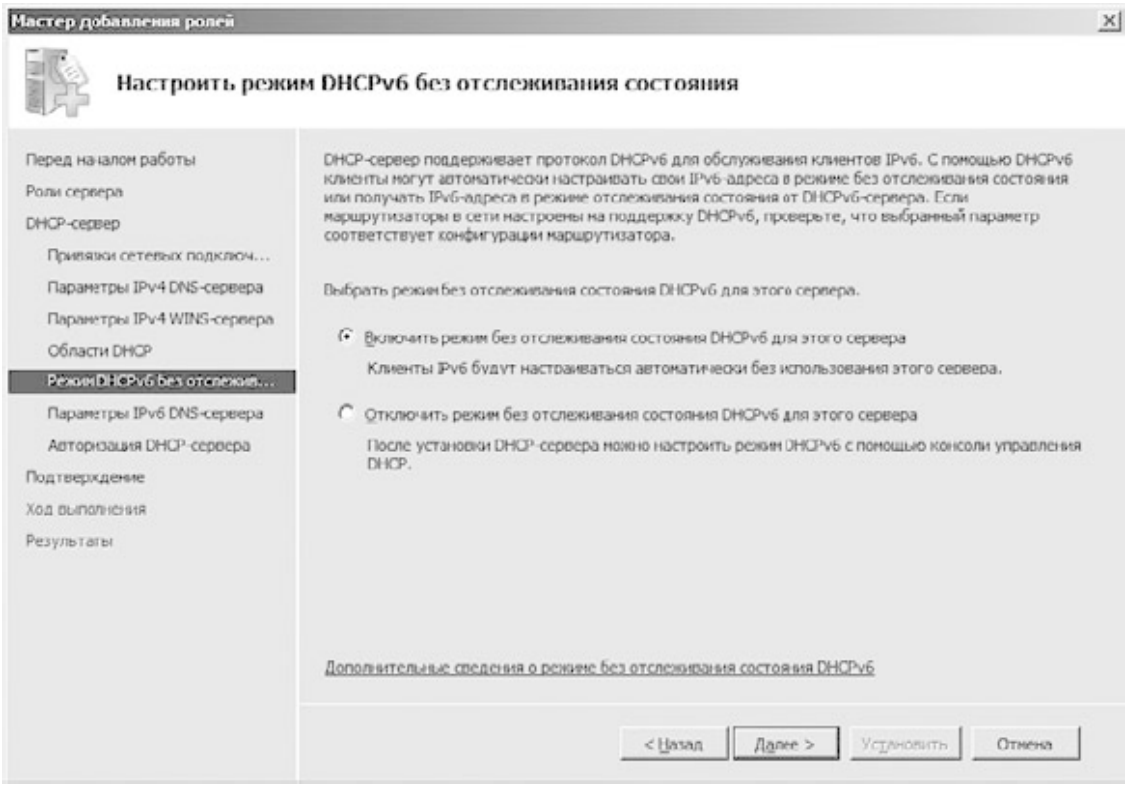

Рис. 25.5. Настройка режима DHCP-сервера для случаев использования TCP/IPv6

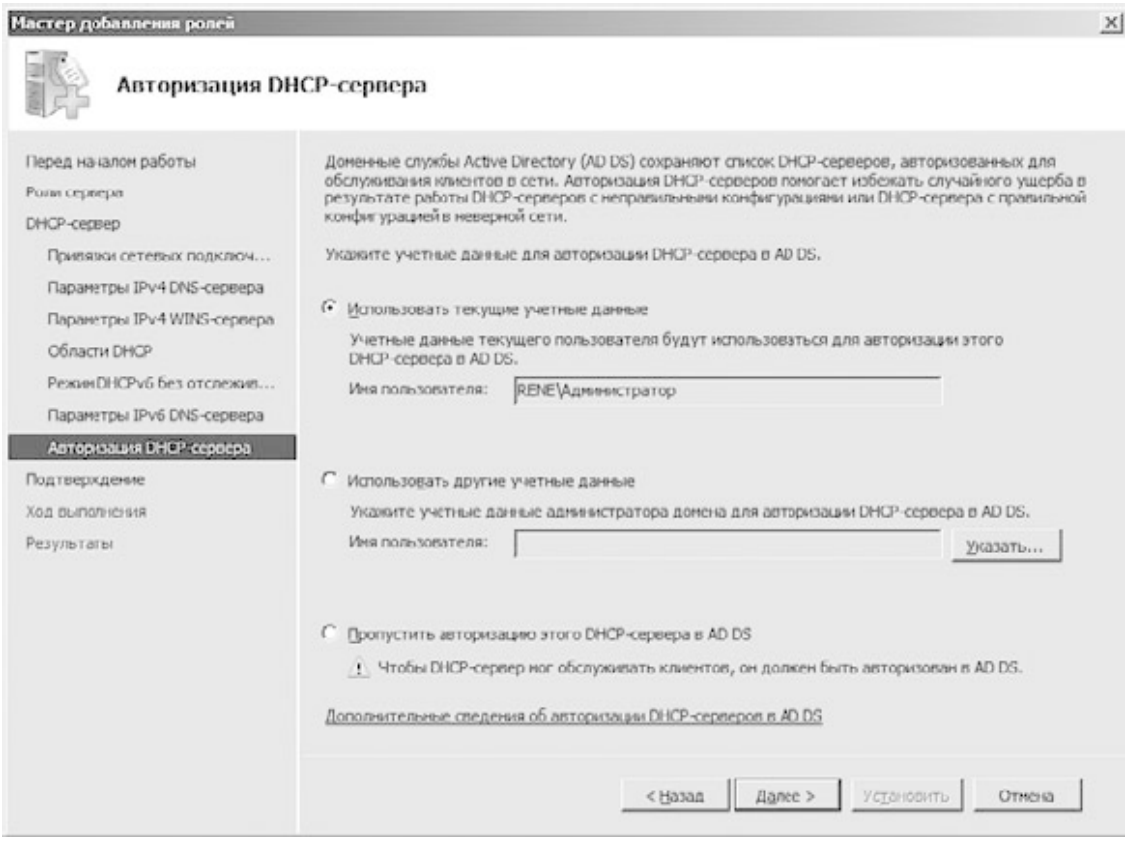

Рис. 25.6. Параметры авторизации DHCP-сервера

Несмотря на то что на выбор предлагаются три варианта авторизации DHCP-сервера в Active Directory, обычно используется автоматическая авторизация с применением существующей учетной записи администратора. Подобный подход вполне оправдан, поскольку

как контроллер домена, так и DHCP-сервер в нашем случае расположены на одном физическом сервере, поэтому разделять этапы авторизации не имеет смысла.

Прежде чем приступить к внесению изменений в работу операционной системы, мастер добавления ролей выдаст окно с информацией, которую вы указывали на всех этапах настройки (рис. 25.7).

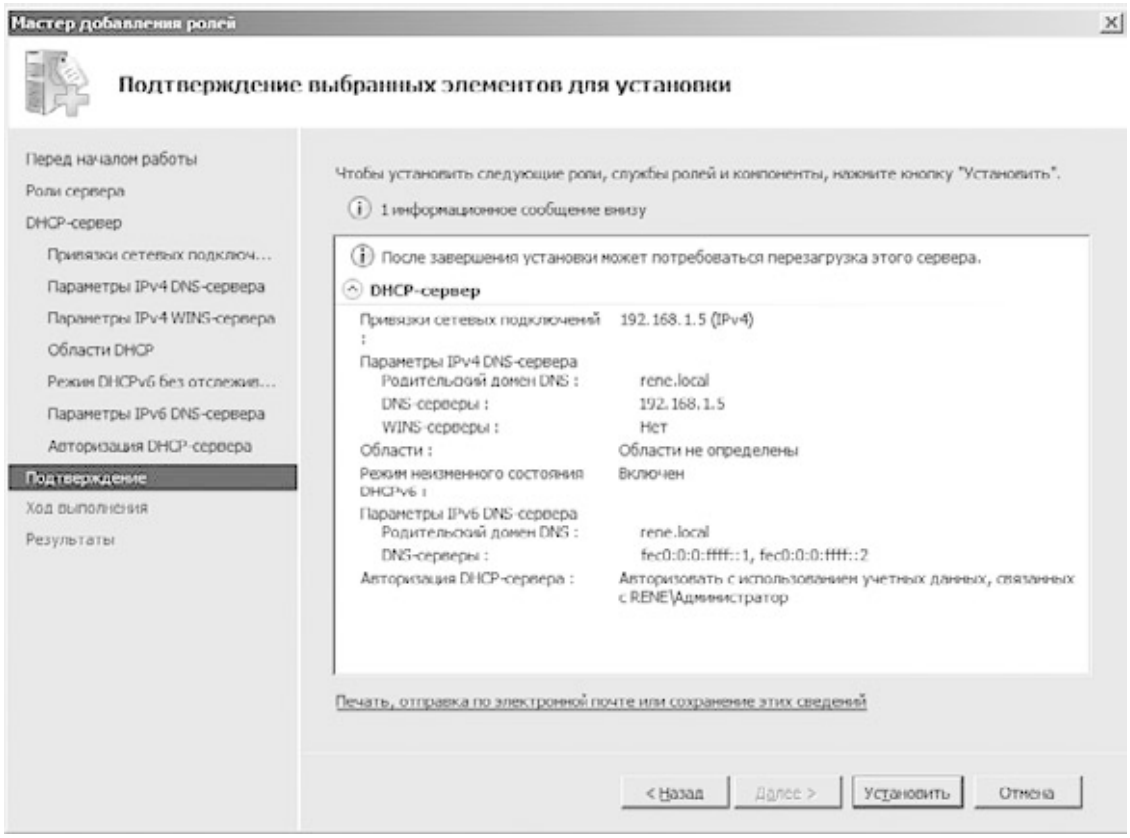

Рис. 25.7. Подтверждение выбранных параметров

Ваша задача – еще раз внимательно проверить все указанные параметры и подтвердить свои намерения нажатием кнопки **Установить**. Если требуется откорректировать некоторые параметры, вы можете вернуться к нужному шагу настройки, используя кнопки навигации.

Изменение параметров работы операционной системы с целью установки роли DHCP-сервера занимает достаточно мало времени, поэтому по истечении буквально нескольких минут вы сможете приступить к настройке всех необходимых параметров функционирования DHCP-сервера.

Глава 26
Настройка DHCP-сервера

В предыдущей главе был подробно описан процесс добавления роли DHCP-сервера на контроллер домена. При этом никакой настройки DHCP-сервера не производилось, а это означает, что, даже установив эту роль, вы не сможете получить от нее пользу, пока не выполните нужную настройку правил IP-адресации.

В этой главе мы рассмотрим задание параметров DHCP-сервера.

Первым делом необходимо запустить программную оболочку, с помощью которой можно настраивать DHCP-сервер. Для этого можно воспользоваться ярлыком **DHCP** из группы **Администрирование**. В результате появится окно, показанное на рис. 26.1.

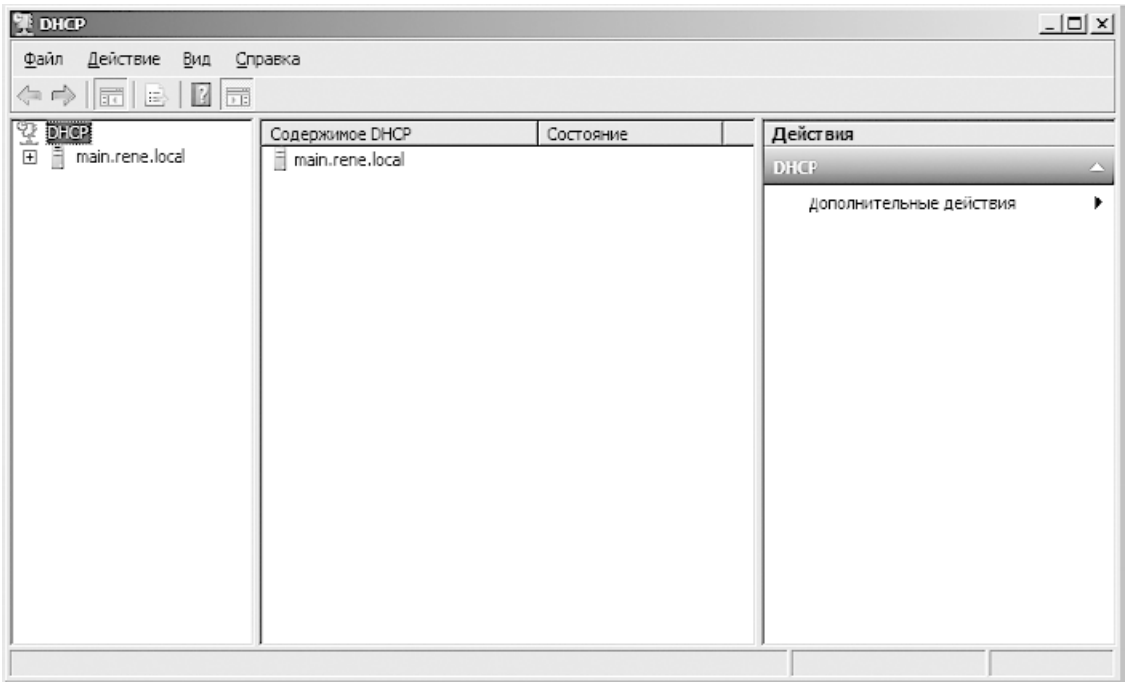

Рис. 26.1. Программа управления DHCP-сервером

Принцип работы DHCP-сервера не изменился со времен появления его реализации в первой серверной операционной системе. Для функционирования системы IP-адресации используется область или диапазон адресов. При этом адреса могут применяться по-разному, поэтому существует изначальное разделение адресов по категориям, в чем вы убедитесь далее.

Начнем работу с того, что создадим область адресов. Поскольку DHCP-сервер может применяться для динамического распределения адресов между клиентами, использующими TCP/IPv4, и клиентами, использующими TCP/IPv6, необходимо изначально делать различие между ними. В связи с этим для разных версий протокола TCP/IP настройка системы адресации происходит отдельно. Поскольку обслуживание клиентов с применением TCP/IPv6 на этапе установки DHCP-сервера решено было не производить, мы настроим сервер только для адресации клиентов, использующих четвертую версию протокола.

Откройте в левой части окна ветку **main.rene.local**. В результате появятся позиции **IPv4** и **IPv6**, отвечающие за настройку IP-адресации клиентов четвертой и шестой версии протокола TCP/IP соответственно (рис. 26.2).

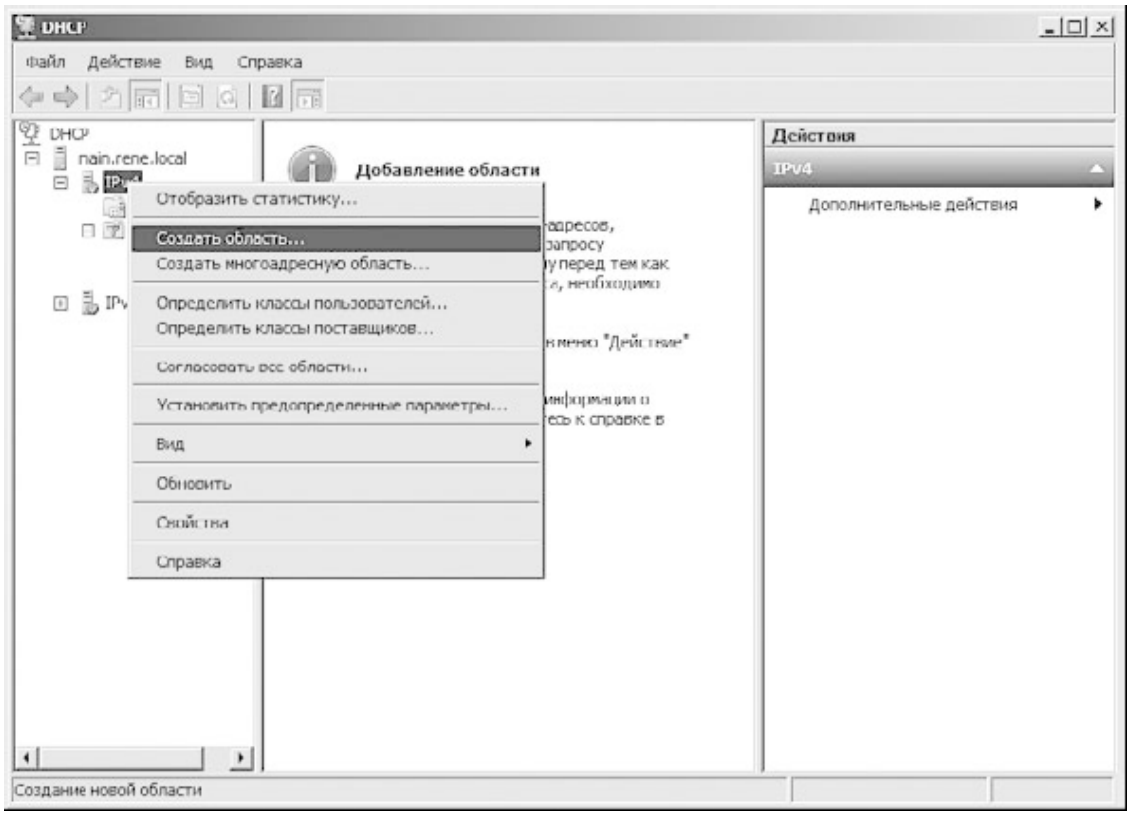

Рис. 26.2. Выбор пункта **Создать область**

Чтобы создать область адресов, щелкните правой кнопкой мыши на строке **IPv4** и в появившемся меню выберите пункт **Создать область**. В результате откроется окно мастера создания области (рис. 26.3).

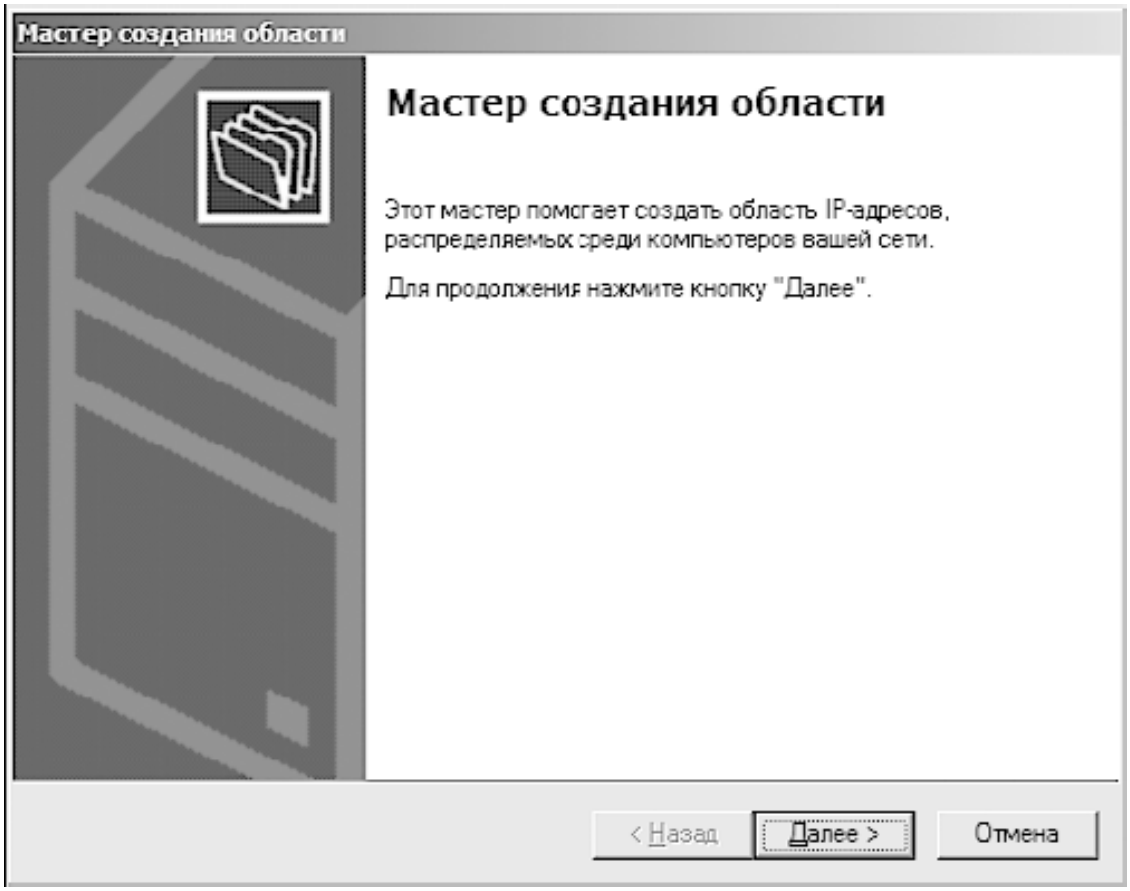

Рис. 26.3. Мастер создания области

В отличие от процесса настройки области адресов более ранних версий DHCP-сервера, новый мастер получился более удобным и функциональным. Нужно сказать, что под понятием «создание области» мастер подразумевает создание нескольких областей разного назначения.

Первое, что необходимо сделать, – указать название области (рис. 26.4).

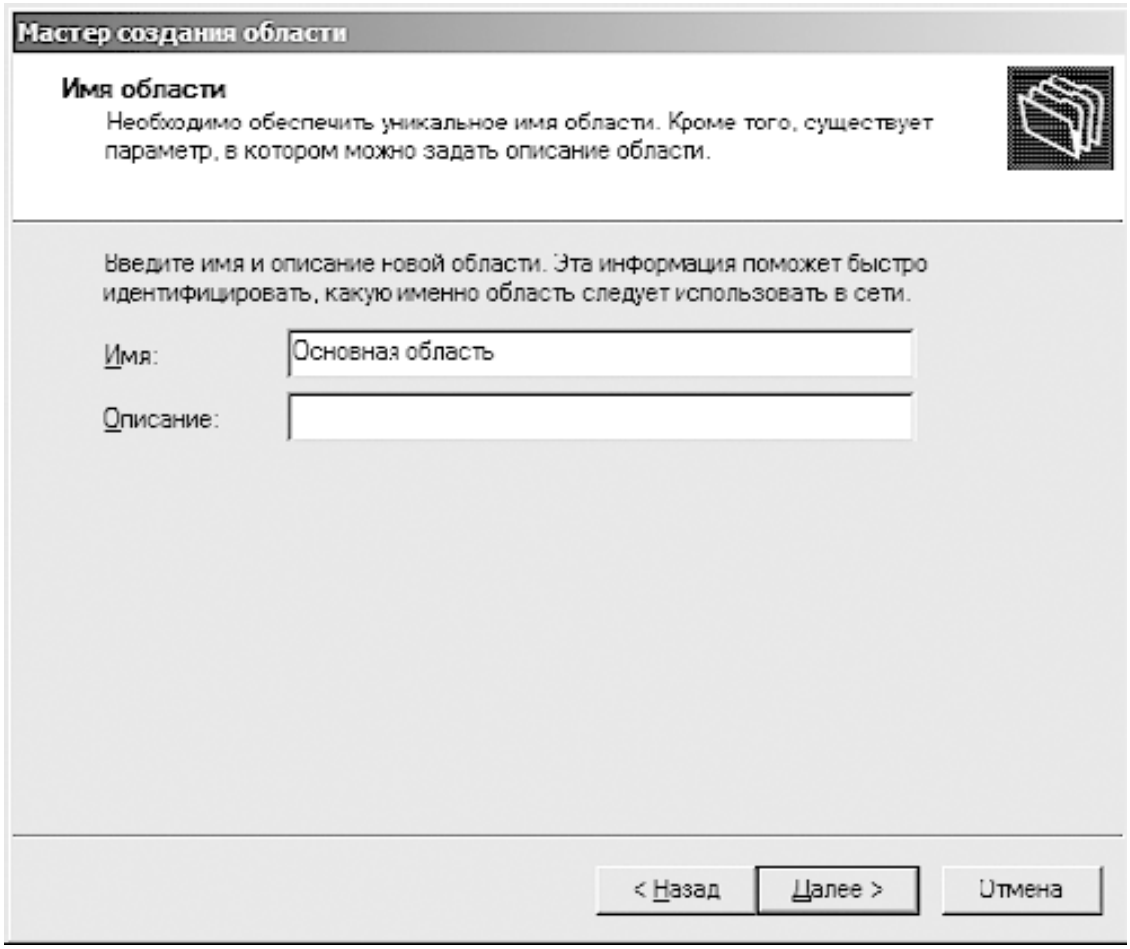

Рис. 26.4. Задание имени области и описания

Название области не играет абсолютно никакой роли, поэтому не стоит уделять этому много внимания. Указав название области и при желании ее короткое описание, нажмите кнопку **Далее**, чтобы продолжить процесс настройки.

В следующем окне нужно указать диапазон адресов, который будет использовать DHCP-сервер (рис. 26.5).

Ввод диапазона подразумевает задание начального и конечного IP-адресов, которые и формируют нужный диапазон. При этом старайтесь указать диапазон больше, нежели реально нужно для обеспечения работоспособности сети. Это позволит составить запас для будущего расширения сети и добавления рабочих мест или устройств любого типа. Маска подсети формируется автоматически, но если вы уверены в своих действиях, можете откорректировать ее.

Следующий важный этап – настройка исключений (рис. 26.6).

В качестве исключений могут быть как отдельные IP-адреса, так и диапазоны адресов, которые будут исключены из общего диапазона адресов и не будут участвовать в процессе IP-адресации, производимой DHCP-сервером. Указав в соответствующих полях адрес или начальный и конечный IP-адреса диапазона, используйте кнопку **Добавить**, чтобы добавить эти данные в список. Количество таких адресов или диапазонов ограничено лишь реальной потребностью, поэтому можете повторить эту операцию столько раз, сколько посчитаете нужным. Если адрес введен неверно, его можно удалить из списка, использовав для этого кнопку **Удалить**.

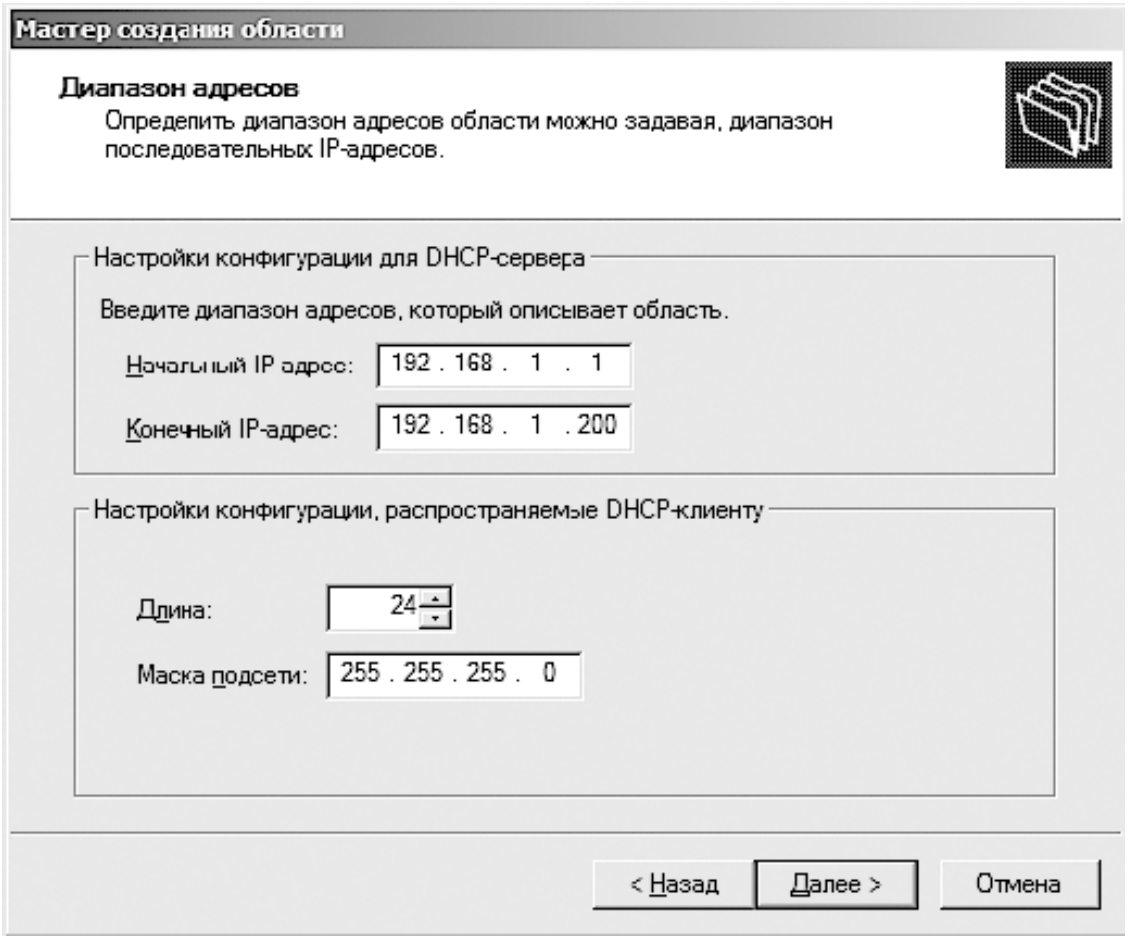

Рис. 26.5. Указание диапазона адресов

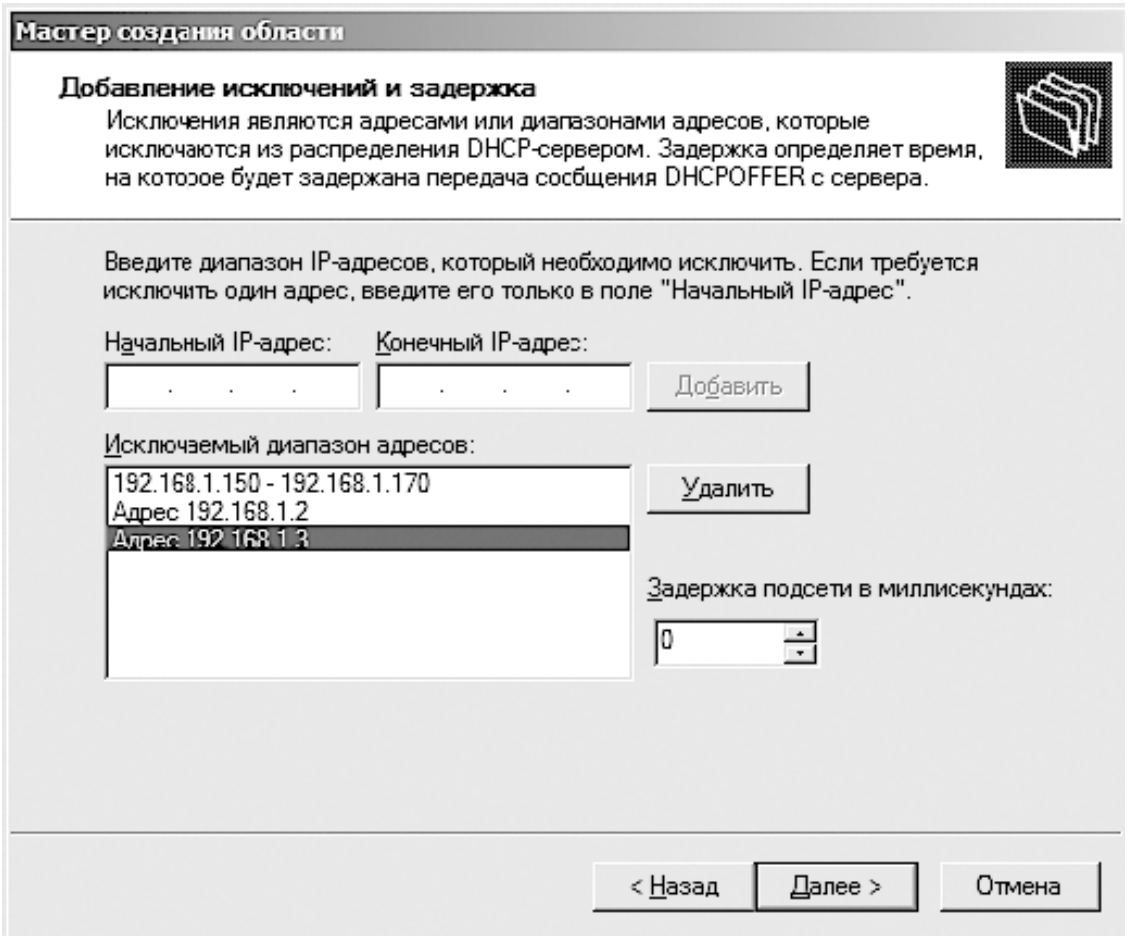

Рис. 26.6. Настройка исключений

Затем следует настроить сроки использования адреса, то есть времени его аренды (рис. 26.7).

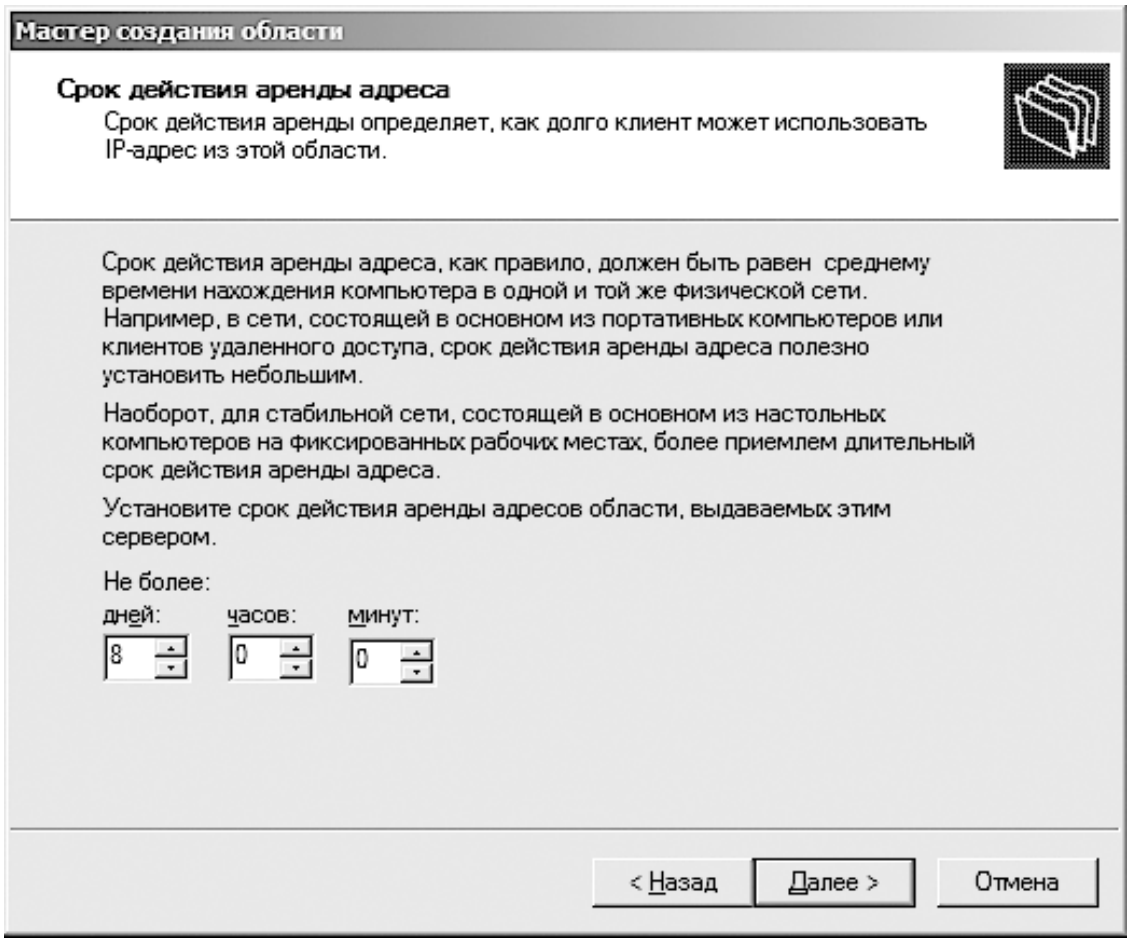

Рис. 26.7. Настройка срока действия аренды адреса

Срок аренды может использоваться в разных целях, например для контроля подключений или элементарной экономии адресов, если количество рабочих мест больше, чем можно использовать для данного типа сети.

По умолчанию предлагается применять восьмидневный срок аренды, но вы можете изменить его на свое усмотрение. Так, если нужно поддерживать работу компьютеров разного типа (например, и персональных, и ноутбуков), можно оставить все как есть. Если же в сети в основном используются ноутбуки, причем в большом количестве, то лучшим решением будет использовать четырех-шеститичасовой период, чтобы вовремя освобождать неиспользуемые адреса.

После нажатия кнопки Далее появится еще одно окно (рис. 26.8), в котором вам предлагается настроить дополнительные параметры DHCP.

Эти параметры клиент получает в случае, если используется динамическое получение IP-адреса. К ним, например, относятся данные о маршрутах, конфигурации WINS-сервера и т. д. Этот этап можно пропустить, поскольку при установке контроллера домена они уже были указаны. Если же их задать сейчас, то старые данные будут заменены указанными в этом окне.

Данный шаг является последним в настройке диапазонов адресов, о чем будет свидетельствовать появление соответствующего окна после нажатия кнопки **Далее**.

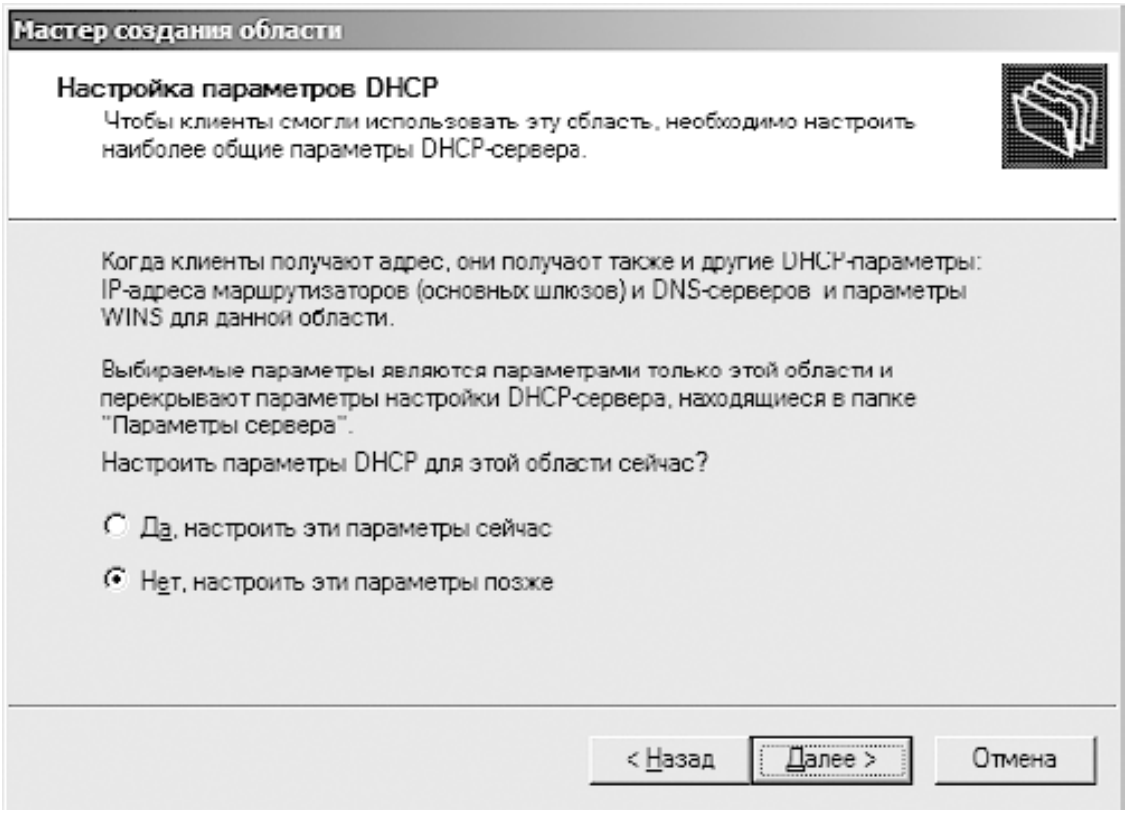

Рис. 26.8. Дополнительные параметры DHCP

Еще одним важным моментом в настройке параметров работы DHCP-сервера является определение зарезервированных адресов. Данный тип адресов используется для указания DHCP-серверу того, что в локальной сети используются важные компьютеры и устройства, которые требуют назначения определенных, то есть статических, IP-адресов. К таким объектам могут относиться файловый сервер, сервер базы данных, основные маршрутизаторы и т. д. При этом, чтобы DHCP-сервер мог их различать, используется уникальный идентификатор устройства – его физический MAC-адрес.

Чтобы начать резервирование адресов, раскройте ветку **IPv4** и дочернюю ветку с названием, составной частью которого является указанное вами в предыдущем шаге название области адресов (рис. 26.9).

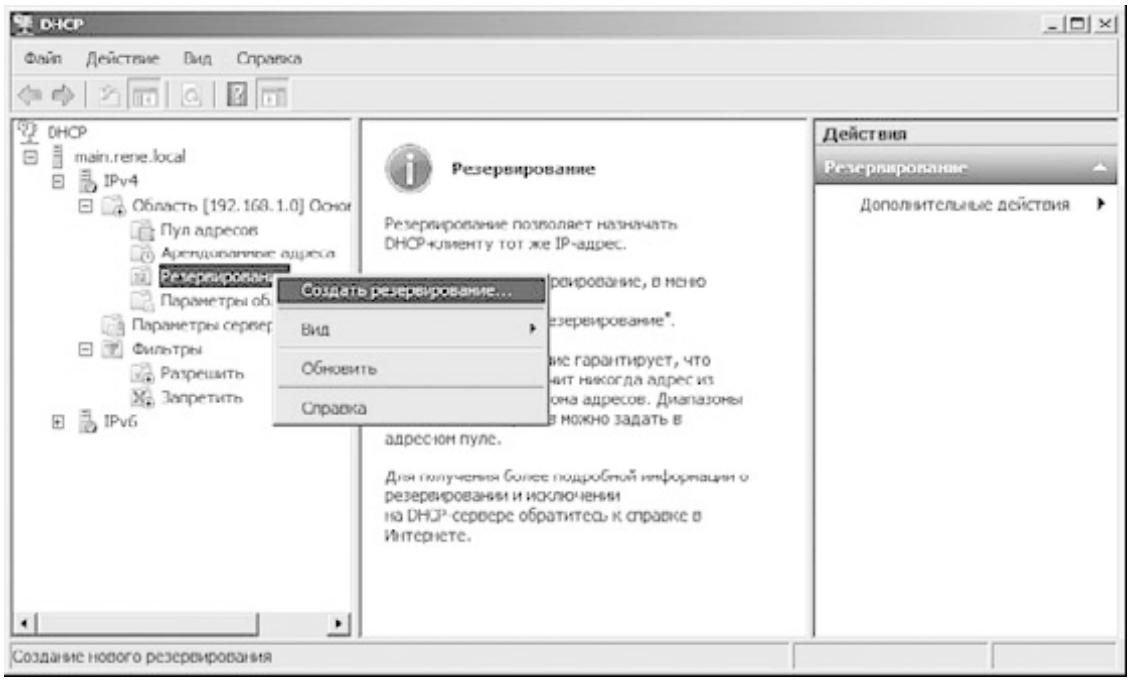

Рис. 26.9. Запуск настройки резервированных адресов

В этой ветке находится строка **Резервирование**. Щелкните на ней правой кнопкой мыши и в появившемся меню выберите пункт **Создать резервирование**. В результате откроется окно создания нового резервирования (рис. 26.10).

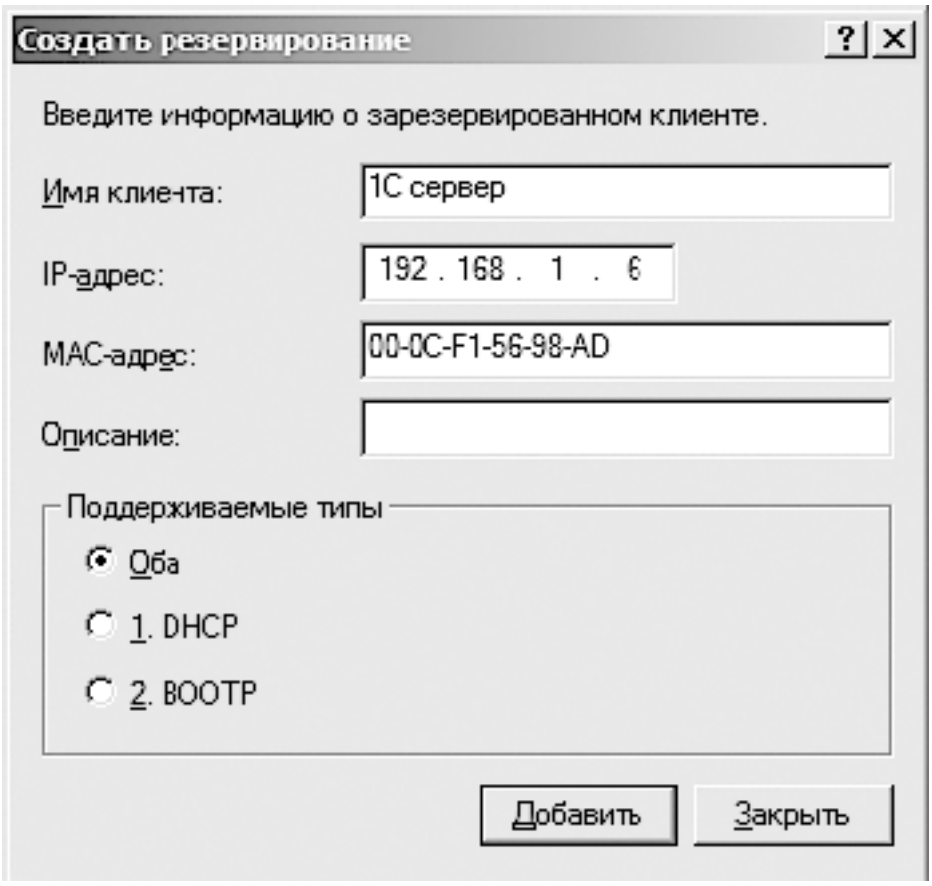

Рис. 26.10. Создание нового резервирования

Вам остается только указать нужные данные: резервируемый IP-адрес, имя клиента и его реальный MAC-адрес. После нажатия кнопки **Добавить** новая запись будет добавлена в область резервирования, а вы сможете продолжать добавление объектов.

На этом процесс настройки DHCP-сервера можно завершить: выполненной настройки вполне достаточно для того, чтобы DHCP-сервер начал выполнять свою работу. В дальнейшем, если возникнет такая необходимость, вы сможете добавлять нужные типы адресов, чтобы поддерживать актуальность данных о важных объектах локальной сети.

Глава 27
Использование Active Directory – пользователи и компьютеры

□ Подразделение
□ Учетная запись пользователя
□ Группа

Active Directory – мощнейший механизм управления локальной сетью. Именно он превращает обычную сеть с использованием рабочих групп в сеть с управляющим сервером, позволяя взять под контроль все происходящие в локальной сети процессы.

Прежде чем сетевые пользователи смогут входить в домен, требуется создать необходимую структуру учетных записей, для чего используется механизм **Active Directory – пользователи и компьютеры**.

Принцип работы с этим механизмом достаточно прост. Главный ключевой объект – объект с названием **Пользователь**, описывающий учетную запись пользователя и способ его входа в локальную сеть. Пользователи могут входить в состав объекта **Группа** или **Подразделение**, что позволяет более гибко управлять учетными записями, применяя групповые политики. Кроме того, существуют объекты, описывающие компьютеры, за которыми работают пользователи, объекты, которые описывают общие ресурсы, и т. д.

Далее рассмотрим все основные операции, которые необходимо выполнить в механизме **Active Directory – пользователи и компьютеры**, чтобы пользователи могли начать работу в составе локальной сети.

Прежде всего необходимо запустить программную оболочку (рис. 27.1), с помощью которой происходит настройка данного механизма. Для этого воспользуйтесь значком **Active Directory – пользователи и компьютеры** в группе **Администрирование**. Внешний вид этой оболочки показан на рис. 27.1

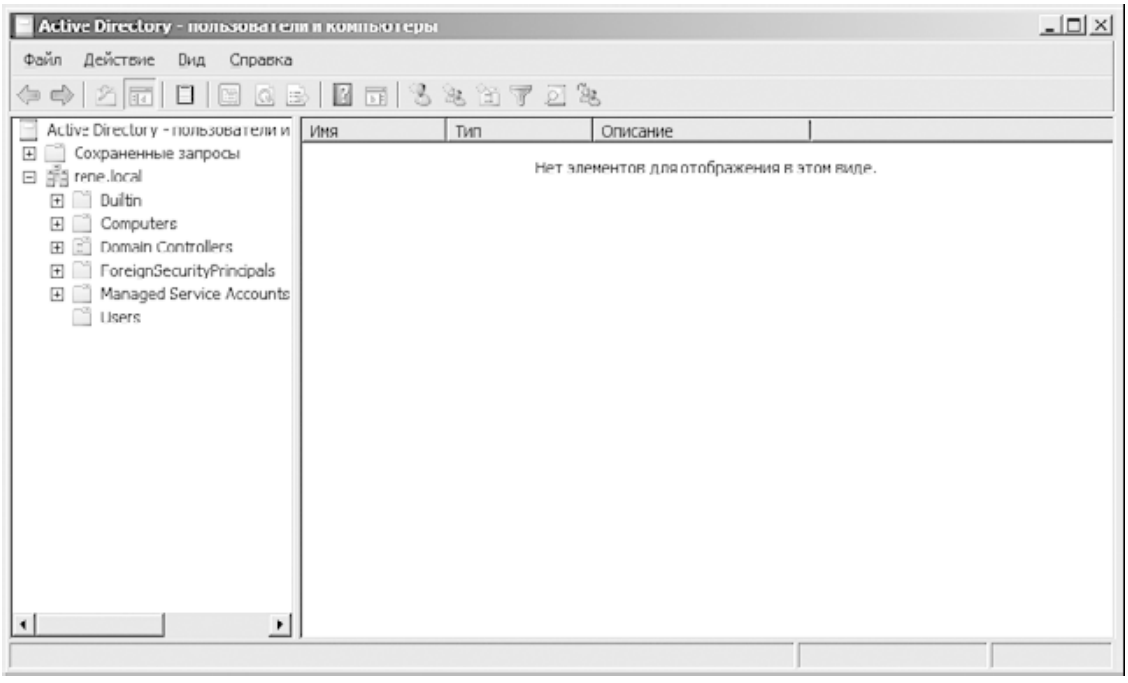

Рис. 27.1. Оболочка для настройки Active Directory – пользователи и компьютеры

В левой части окна отображается древовидная структура с названиями основных объектов, в том числе именем контроллера домена. Если вы раскроете ветку с названием домена (в нашем случае это rene.local), то увидите уже имеющиеся объекты, в частности **Computers, Domain Controllers, Users** и т. п.

При создании всех необходимых объектов мы будем использовать структурированный подход, который в дальнейшем позволит находить в дереве объекты необходимых типов и получать быстрый доступ к ним. В частности, в корневой ветке можно создать объекты **Подразделение**, которые будут представлять собой контейнеры, содержащие все остальные объекты. В качестве названия подразделений можно использовать имена отделов или что-то подобное, позволяющее легко определять содержание контейнера.

Подразделение

Для создания подразделения щелкните правой кнопкой мыши на названии домена и выберите в появившемся меню пункт **Создать ► Подразделение**. В результате откроется окно, показанное на рис. 27.2.

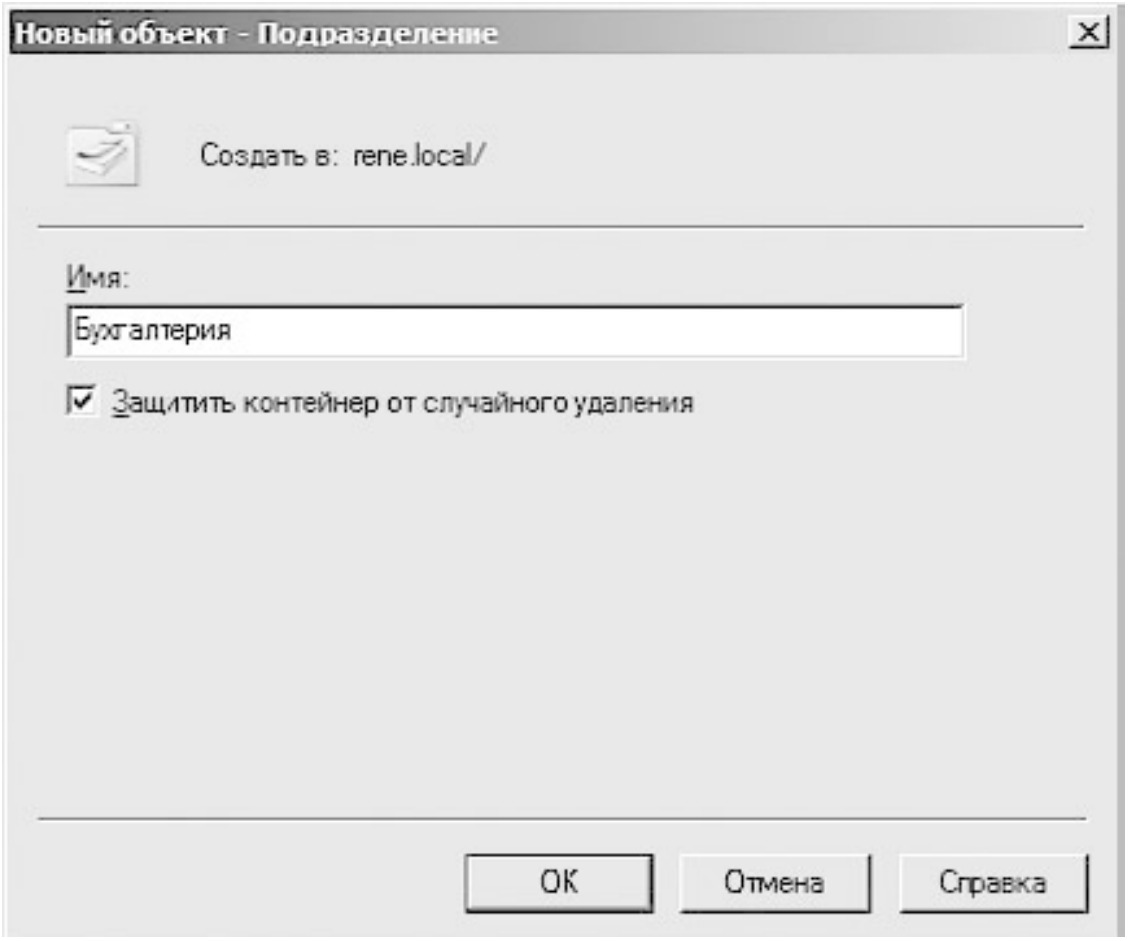

Рис. 27.2. Создаем новое подразделение

В этом окне присутствует всего одно поле, в которое необходимо ввести название подразделения, например **Бухгалтерия**. Здесь же присутствует флажок **Защитить контейнер от случайного удаления**, при установке которого удаление этого объекта будет невозможным без соответствующих полномочий. Это позволяет защитить его от удаления, которое может произойти в результате случайного нажатия клавиши **Delete** или выбора соответствующего действия из контекстного меню.

После нажатия кнопки **ОК** подразделение с именем **Бухгалтерия** будет создано в корневой ветке. После этого все действия, связанные с этим подразделением, необходимо будет выполнять с использование контекстного меню этой строки.

Подобным образом вы можете создать любое количество подразделений, которое требуется для организации структурированной системы управления.

Учетная запись пользователя

С помощью учетной записи пользователя, существующей в контроллере домена, сетевой пользователь может выполнять вход в сеть с применением любого или конкретных компьютеров локальной сети. На этапе авторизации он получает необходимые права доступа к ресурсам локальной сети, что позволяет четко ограничить и контролировать их использование.

Создание учетных записей пользователей мы будем производить с применением объектов типа **Подразделение**, создание которых было описано выше.

Щелкните правой кнопкой мыши на названии нужного подразделения, в нашем случае – на названии отдела. В появившемся меню выберите пункт **Создать ► Пользователь**, как показано на рис. 27.3.

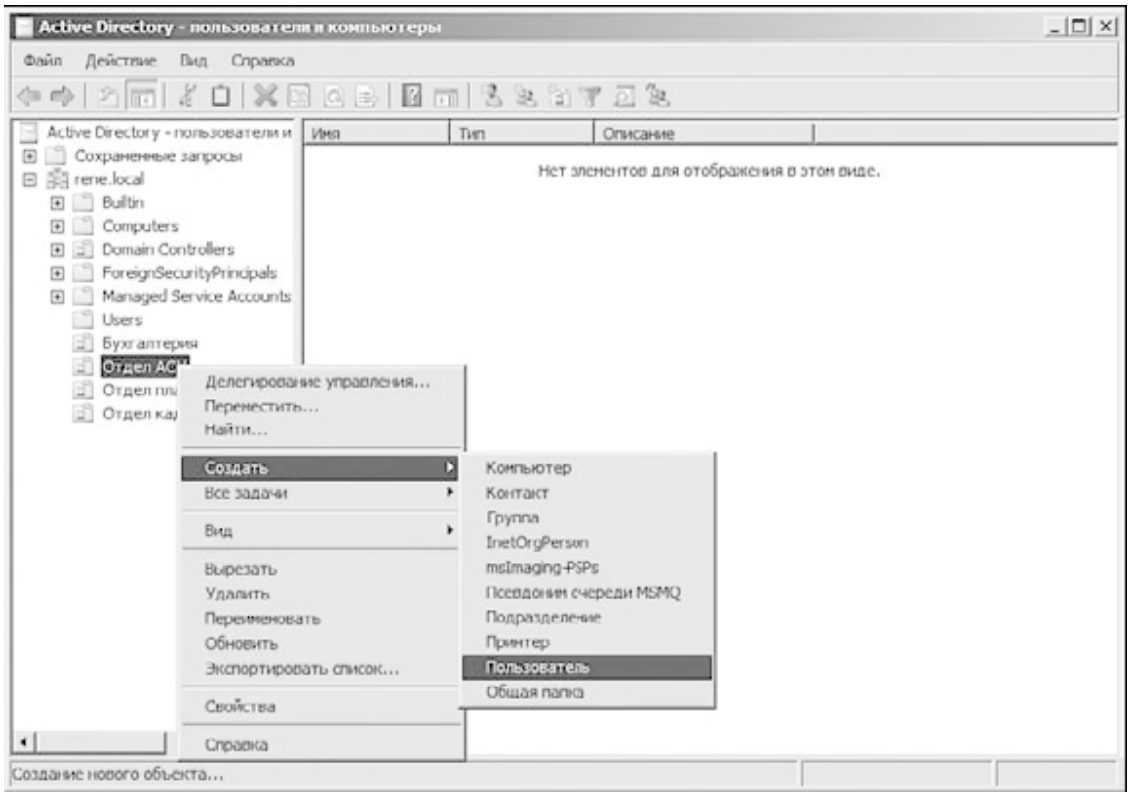

Рис. 27.3. Создание новой учетной записи пользователя

В результате откроется окно (рис. 27.4).

Создание учетной записи пользователя разбито на два этапа. На первом требуется ввести основные данные об учетной записи, такие как имя, фамилия, имя входа и т. д. Состав поля **Полное имя** формируется автоматически путем складывания значений полей **Имя** и **Фамилия**. При этом согласно существующим стандартам на первом месте стоит имя пользователя, что не очень удобно. Если количество пользователей будет довольно большим, быстро найти нужную запись будет достаточно сложно, а сортировка по имени не даст

эффекта. Если же на первое место установить фамилию пользователя, то, используя сортировку в алфавитном порядке, можно будет очень легко отыскать нужную запись.

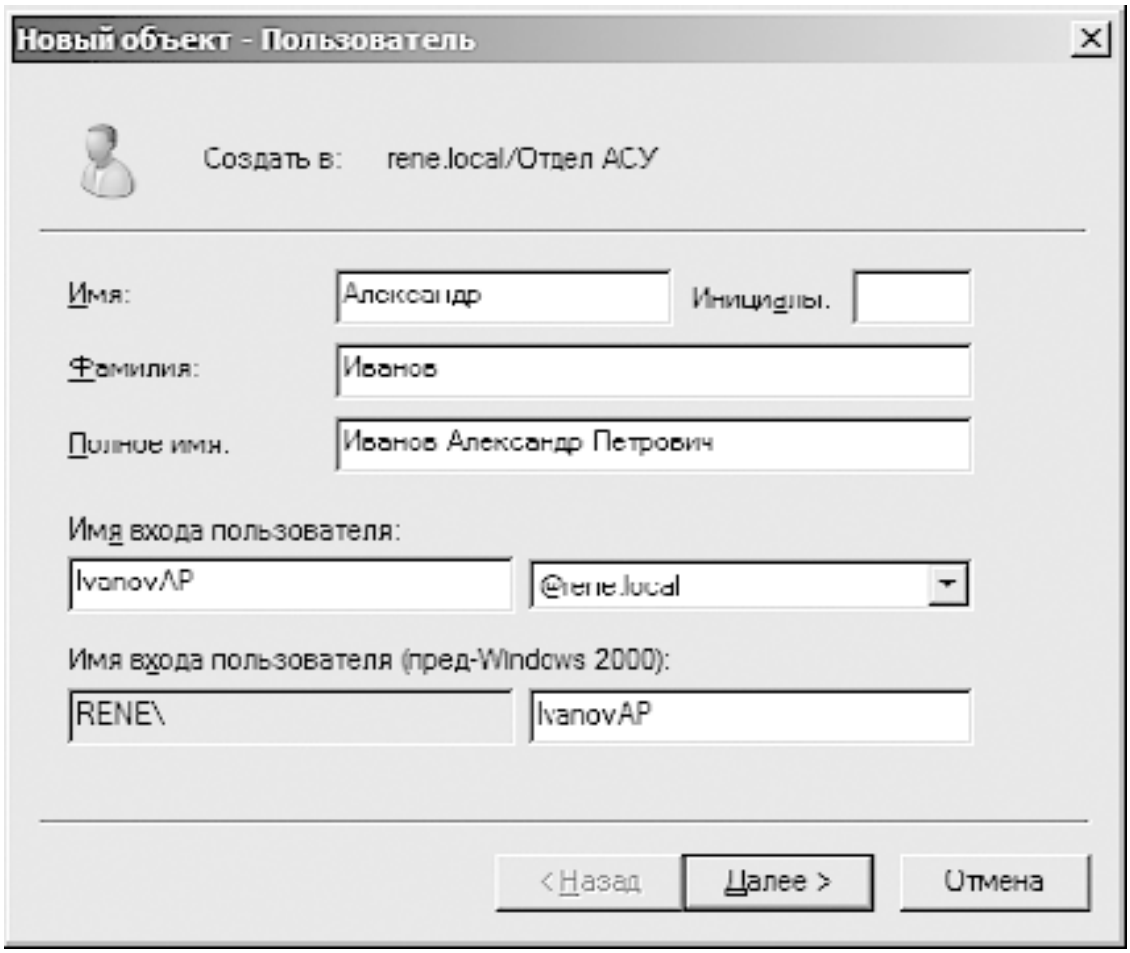

Рис. 27.4. Основные параметры учетной записи пользователя

При вводе имени входа пользователя применяются буквы и символы латинского алфавита. Чтобы облегчить идентификацию пользователя, лучше применять его фамилию и инициалы, написанные латинскими буквами, как это показано на рис. 27.4.

Следующий этап – ввод пароля доступа и задание некоторых дополнительных параметров (рис. 27.5).

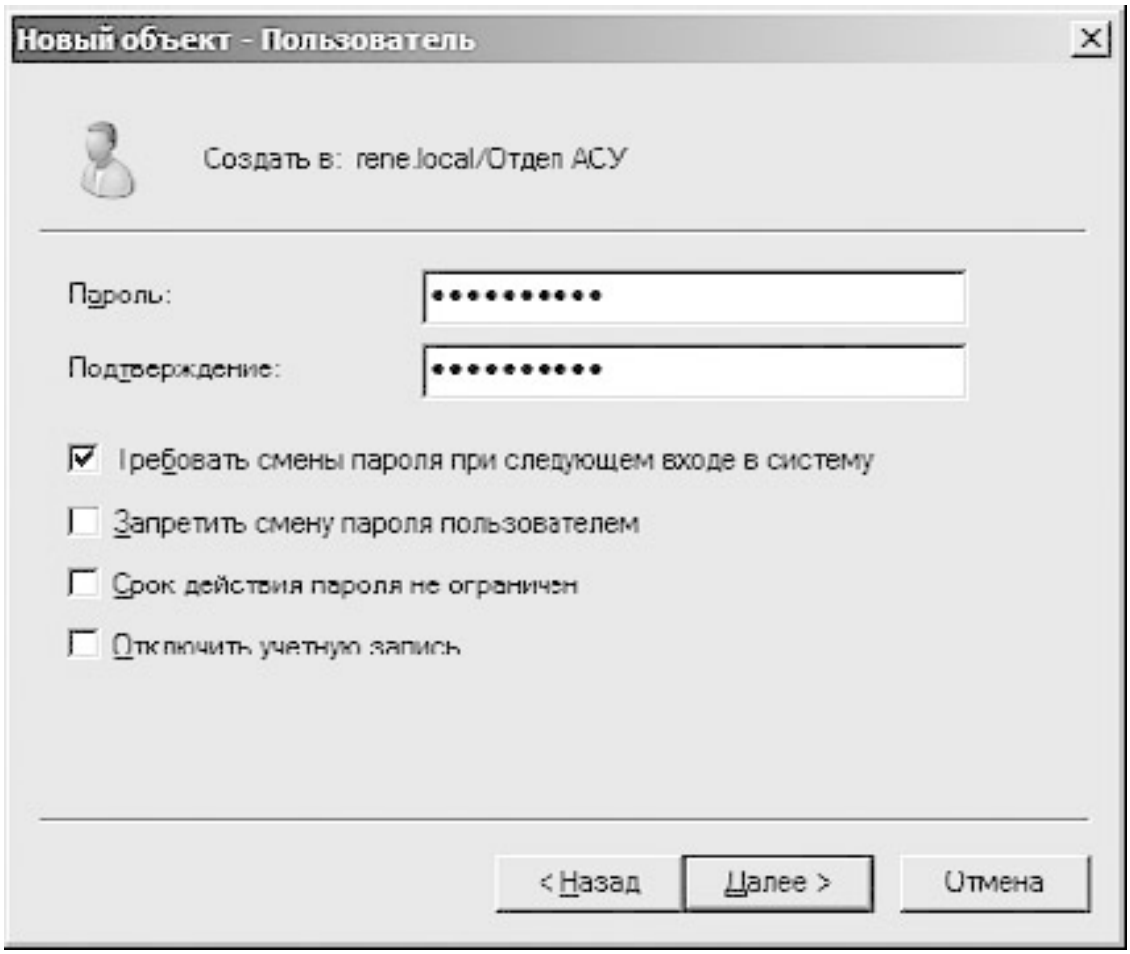

Рис. 27.5. Указание пароля доступа и дополнительных параметров

Ввод пароля происходит согласно существующим правилам безопасности, поэтому указать слишком короткий пароль или пароль, не содержащий определенного набора символов, не получится. Правила ввода пароля можно изменить, но особого смысла в этом нет, поскольку при этом уменьшается уровень безопасности.

На данном этапе также можно задать некоторые дополнительные параметры, влияющие на учетную запись пользователя. Так, достаточно популярным и часто используемым является параметр **Требовать смены пароля при следующем входе в систему**. При установке данного флажка при следующем входе в локальную сеть от пользователя потребуется принудительная смена пароля. Достаточно часто пользователи забывают свои пароли входа. В таких ситуациях подобная возможность просто незаменима.

Кроме того, присутствуют следующие параметры.

□ **Запретить смену пароля пользователем**. Пользователь в любой момент может сменить свой текущий пароль, используя для этого сочетание клавиш **Ctrl+Alt+Delete** и нажатие соответствующей кнопки в появившемся окне. Данный параметр позволяет отключить такую возможность.

□ **Срок действия пароля не ограничен**. Как правило, существующие групповые политики предписывают смену паролей пользователей по истечении определенного периода их использования, например 30 дней. После этого строка пользователь должен изменить пароль, иначе работа в локальной сети будет невозможна. Данный параметр применяется, чтобы отключить необходимость смены пароля.

□ **Отключить учетную запись**. Этот параметр используется, если требуется установить временный или постоянный запрет на применение данной учетной записи.

После задания необходимых настроек и нажатия кнопки **Далее** появится результирующее окно, содержащее информацию об указанных параметрах. Если вы подтверждаете их корректность, нажмите кнопку **Готово**, чтобы создать учетную запись.

Подобным образом создается необходимое количество учетных записей пользователей для каждого подразделения.

После того как учетная запись добавлена, можно выполнить более детальную ее настройку, если дважды щелкнуть на нужной записи либо щелкнуть на ней правой кнопкой мыши и выбрать в появившемся меню пункт **Свойства**. В результате откроется окно (рис. 27.6), содержащее большое количество вкладок с разнообразнейшими параметрами.

Практически все параметры, которые можно настраивать на этих вкладках, имеют чисто описательный характер и никакого влияния ни работу пользователя не оказывают. Однако есть некоторые параметры, с помощью которых можно расширить функциональность учетной записи. Например, чтобы организовать хранение и доступ пользователя к его личным данным на сервере, можно создать домашнюю папку пользователя. Для этого в параметре **Локальный путь** необходимо указать путь к папке на сервере, как это показано на рис. 27.6. При этом размещение папки может быть как локальным, так и сетевым. Чаще всего практикуется сетевой вариант размещения папок, что позволяет разместить их на файловом сервере, на котором настроена система архивирования данных.

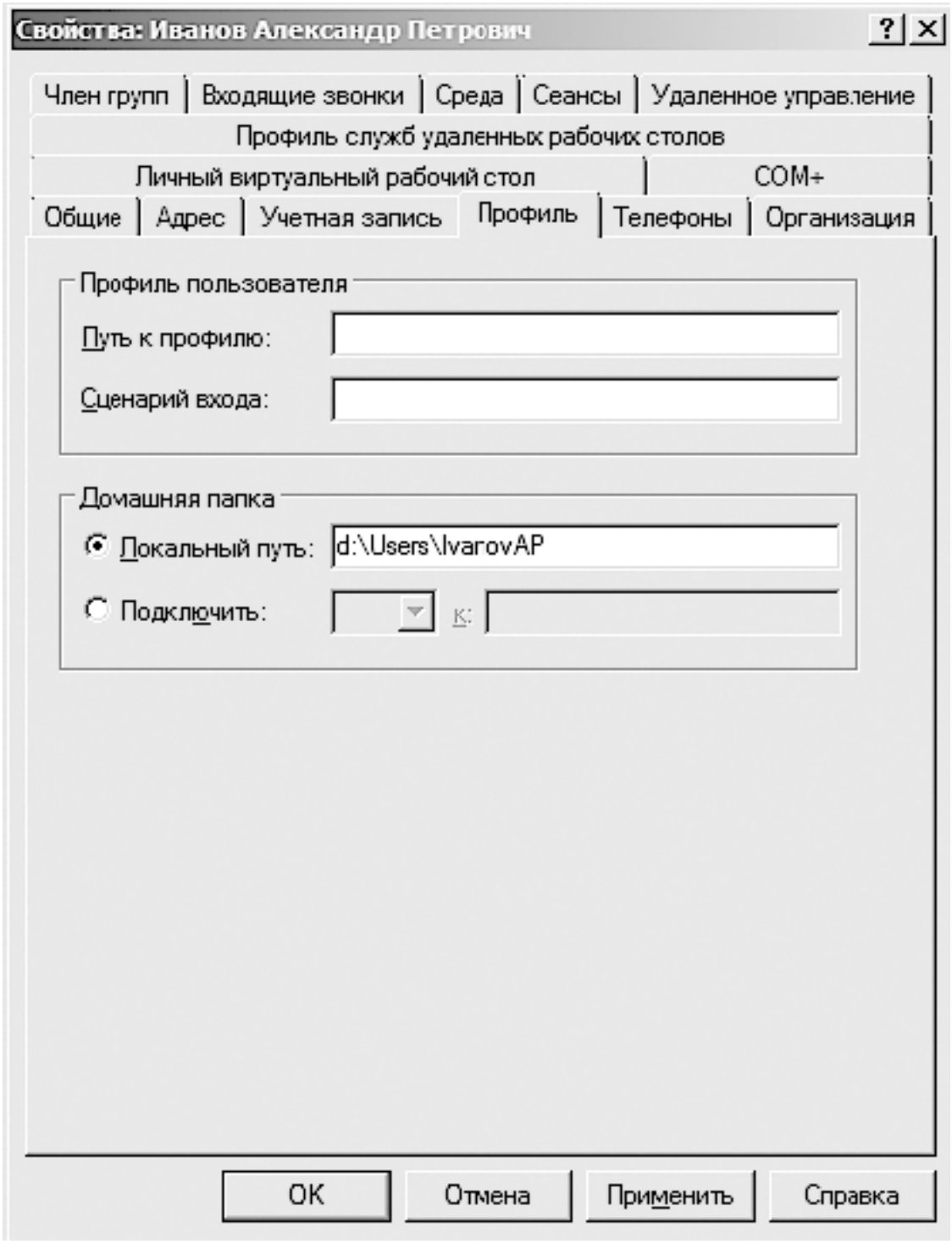

Рис. 27.6. Параметры учетной записи пользователей

Можно изменять и другие важные параметры, например настраивать членство в группах, возможность удаленного доступа, указывать компьютеры, которые могут использоваться для входа, время работы в сети и многое другое.

Группа

Использование групп позволяет получить возможность быстрого назначения прав доступа к ресурсам локальной сети. Особенно это удобно, когда требуется предоставить права доступа многим пользователям или другим группам, что отнимает много времени,

если настраивать доступ для каждого отдельного пользователя. Группы могут располагаться в любой ветке имеющейся структуры, но, как правило, их используют в составе подразделений. Далее рассмотрим именно такой случай.

Предположим, нам нужно создать группу, в состав которой должны входить программисты. Щелкните на подразделении **Программисты** правой кнопкой мыши и в появившемся меню выберите пункт **Создать ► Группу**. В результате откроется окно создания новой группы (рис. 27.7).

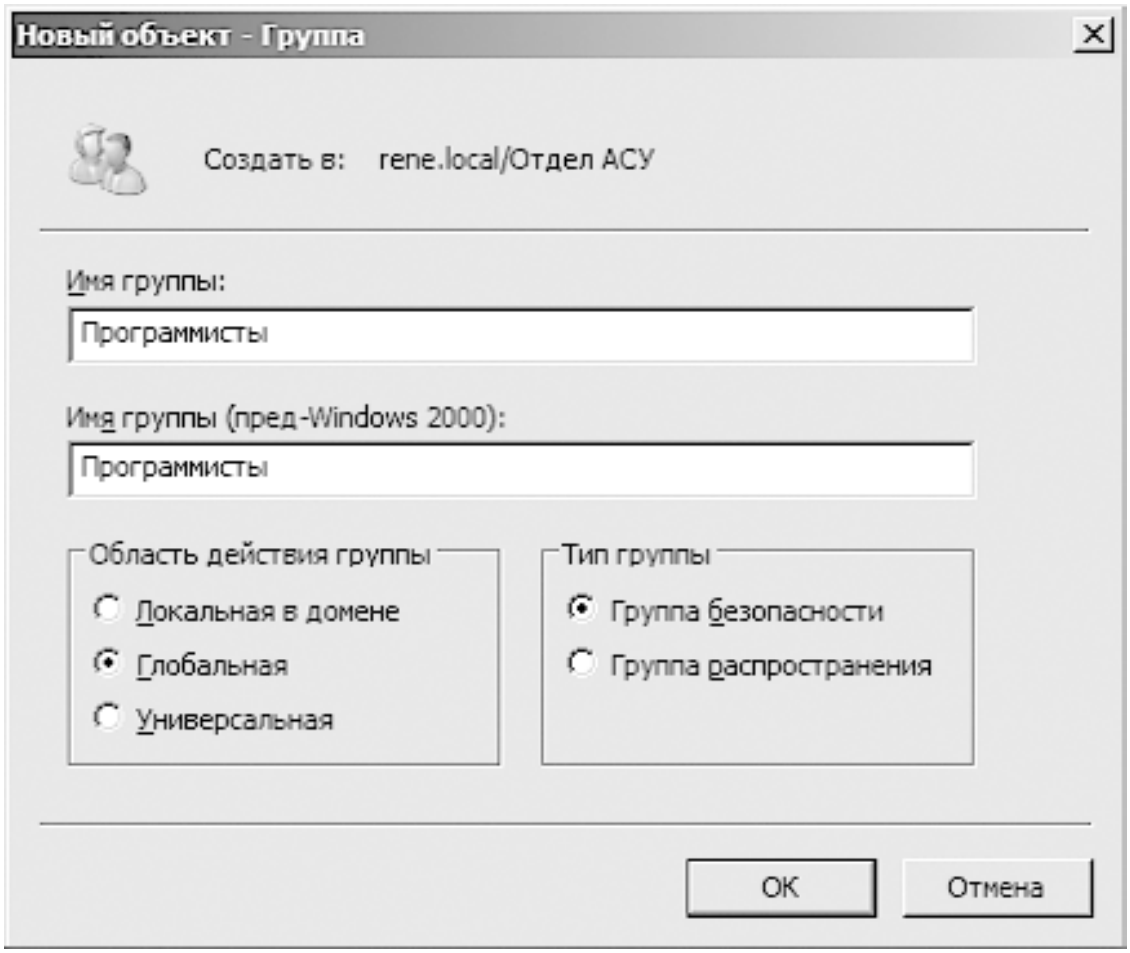

Рис. 27.7. Создание новой группы

В этом окне нужно ввести имя группы и выбрать ее тип и область ее влияния. Тип группы определяет права доступа к определенным действиям.

□ **Группа безопасности.** Пользователи этой группы получают доступ к таким ресурсам, как файлы и принтеры.

□ **Группа распространения.** Пользователи данной группы могут участвовать в различного рода распространении информации.

Область действия группы определяет разные возможности использования учетных записей пользователей. Например, область **Локальная в домене** позволяет использовать учетные записи пользователей только для локальных целей или целей домена. Если же в сети существует несколько доменов, то, чтобы иметь возможность применения пользователей группы в других доменах, она должна быть **Глобальной** или **Универсальной**.

После того как группа создана, можно начать заполнять ее учетными записями пользователей и другими объектами.

Для этого в окне свойств группы перейдите на вкладку **Члены группы** (рис. 27.8) и нажмите кнопку **Добавить**. В результате откроется окно, показанное на рис. 27.9.

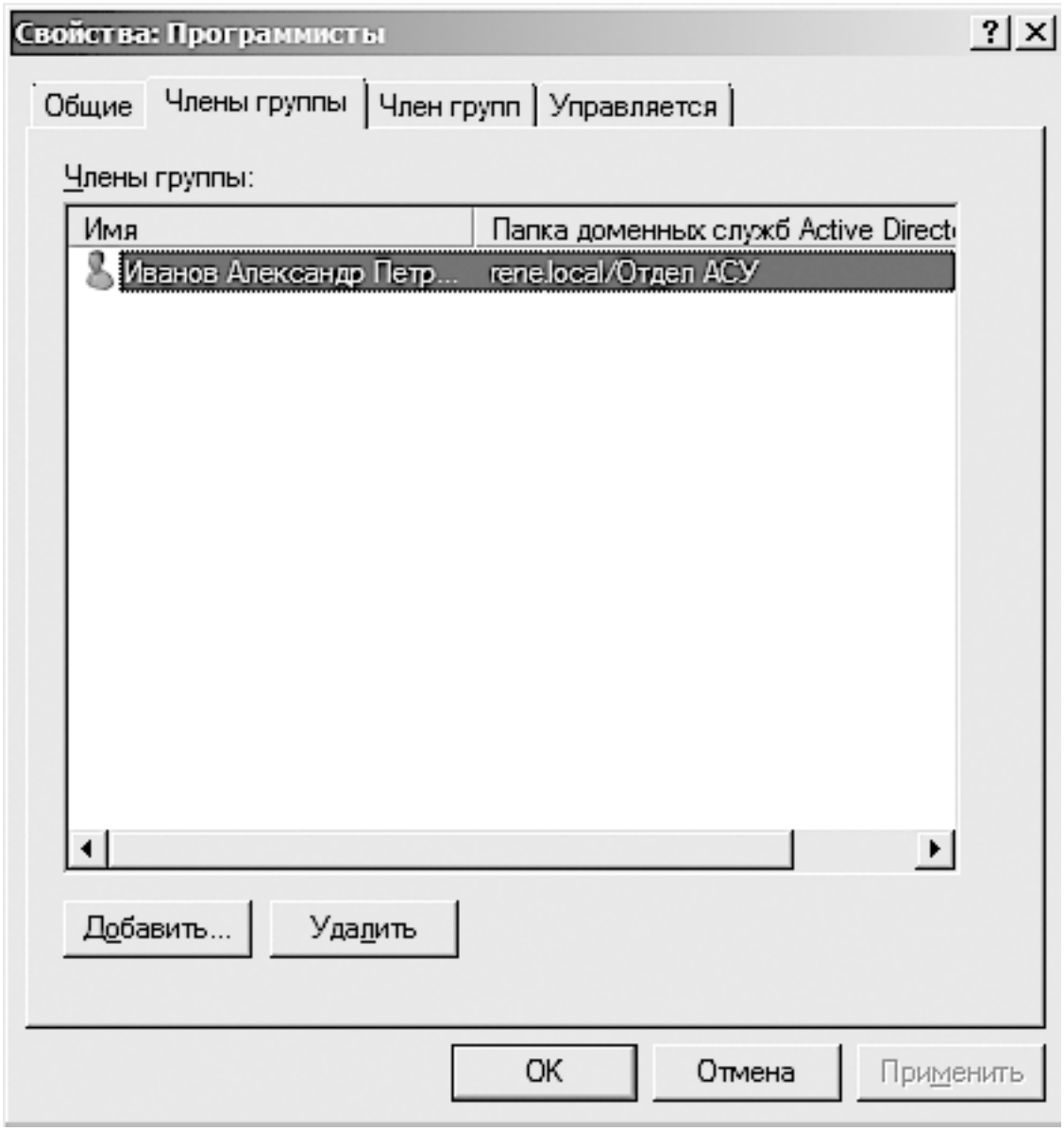

Рис. 27.8. Добавление объектов в группу

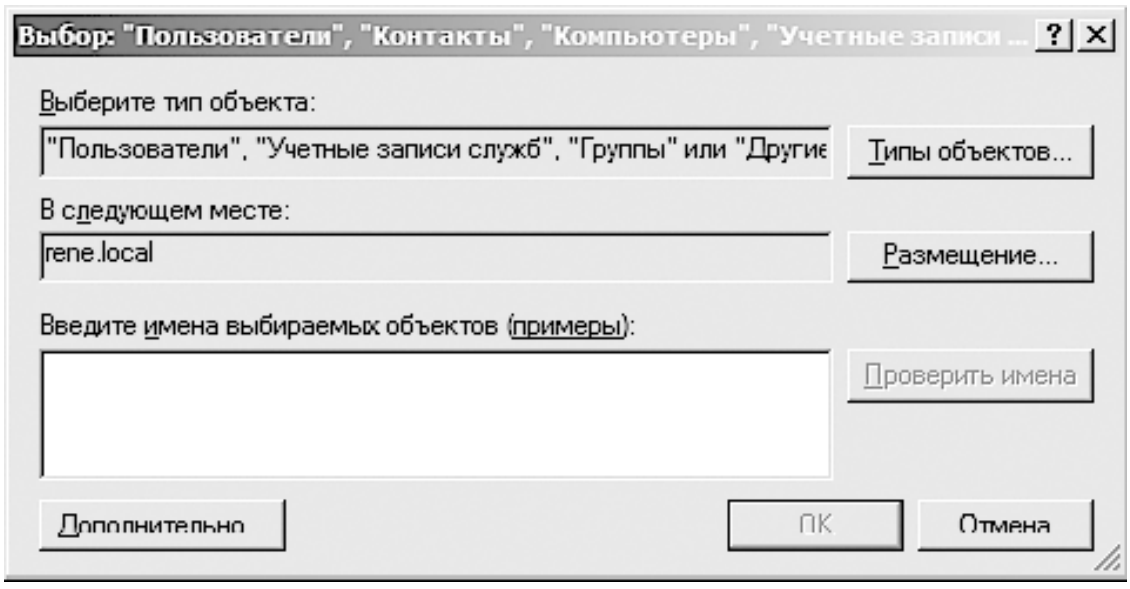

Рис. 27.9. Механизм выбора учетных записей

Выбор учетных нужных объектов происходит в текущем сетевом расположении, в нашем случае – в домене **rene.local**. Учетные записи можно вводить как вручную, набирая их в нижнем поле ввода и разделяя десятичной точкой, так и с использованием автоматизированного механизма выбора, который запускается нажатием кнопки **Дополнительно** (рис. 27.10).

Этот способ ввода более предпочтителен, поскольку позволяет выбрать сразу несколько различных объектов. При этом исключена возможность грамматических ошибок в написании.

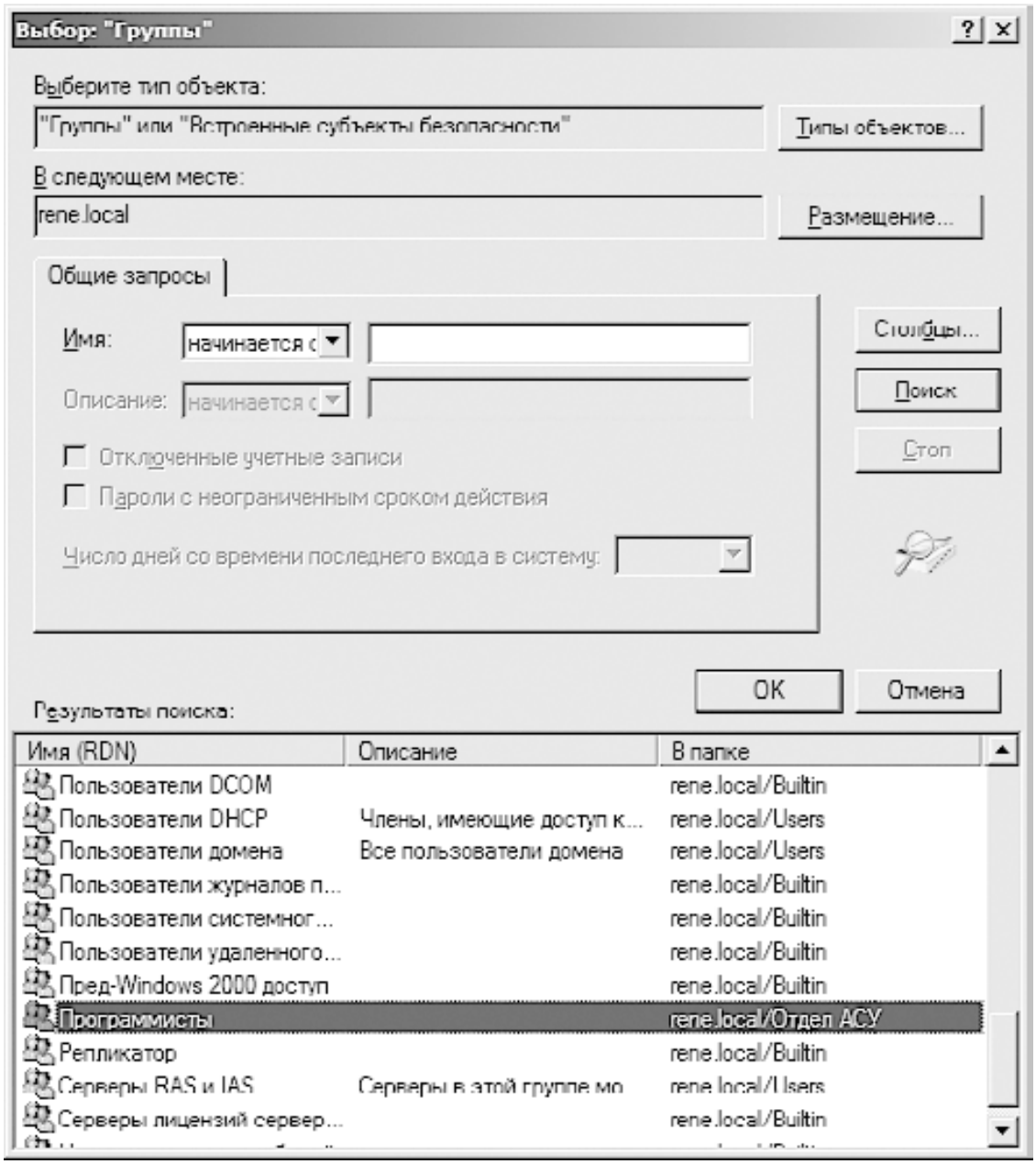

Рис. 27.10. Выбор нужных объектов

После нажатия кнопки **Поиск** в нижней части окна появится список всех зарегистрированных объектов. Возможен как одиночный выбор нужной записи, так и выбор сразу нескольких записей, для чего необходимо удерживать нажатой клавишу **Ctrl**. После нажатия кнопки **OK** все выбранные записи оказываются в предыдущем окне. После нажатия кнопки **OK** они попадают в список членов группы.

Глава 28
Подключение и настройка клиента Windows XP

- □ Подключение к рабочей группе
- □ Подключение к домену
- □ Настройка TCP/IP-протокола

Применение операционной системы Microsoft Windows XP все еще достаточно распространено, и этому имеется очень простое объяснения. Если не учитывать элементарную привязанность некоторых пользователей к этой операционной системе, основной причиной работы в ней можно считать недостаточную мощность компьютера, которая не позволяет установить на него более новую операционную систему, например Windows Vista или Windows 7. Кроме того, может играть роль и фактор несовместимости старого оборудования с новой операционной системой. В общем, какими бы причинами ни было вызвано применение Windows XP, если такой пользователь есть в созданной вами локальной сети не удивляйтесь этому факту, а примите его как данность. Однако при этом имейте в виду: поддержка работы компьютера в составе домашней группы в Windows XP отсутствует, поэтому либо применяйте мощные компьютеры с более новой операционной системой, либо используйте другой способ функционирования сети.

Когда речь идет о подключении компьютера к локальной сети, главным вопросом является способ функционирования сети. Если локальная сеть использует рабочие группы, применяется один способ подключения, если используется доменная система – другой, а если решено применят домашние группы – третий. Поскольку Windows XP не поддерживает работу с домашними группами, далее будут рассмотрены только первые два способа.

Подключение компьютера к рабочей группе или домену может стать не единственным требованием, необходимым для удачного присоединения к локальной сети. Кроме всего прочего, дополнительно может потребоваться задать IP-адрес и маску подсети, IP-адрес шлюза, IP-адрес DNS-сервера и т. д. Все это при необходимости можно выполнить в настройках драйвера сетевого адаптера, который используется для подключения к локальной сети.

Подключение к рабочей группе

Сразу после установки операционной системы Windows XP вы уже находитесь в рабочей группе с названием **WORKGROUP**. В этом можно убедиться, открыв окно свойств системы. Это же окно вам нужно будет открыть, если вы решите изменить заданное по умолчанию название рабочей группы на имя реально существующей рабочей группы, к которой вы хотите подключиться (рис. 28.1).

Откройте окно свойств системы и перейдите на вкладку **Имя компьютера**. Здесь отображается текущая принадлежность компьютера к группе или домену, а также его описание. Как видите, имя группы по умолчанию действительно **WORKGROUP**. Как показывает практика, часто в локальной сети действительно присутствует группа с таким именем. Это делается для того, чтобы уменьшить количество манипуляций, необходимых для подключения к рабочей группе. А так все достаточно просто: установил операционную систему – и сразу оказался в нужной группе.

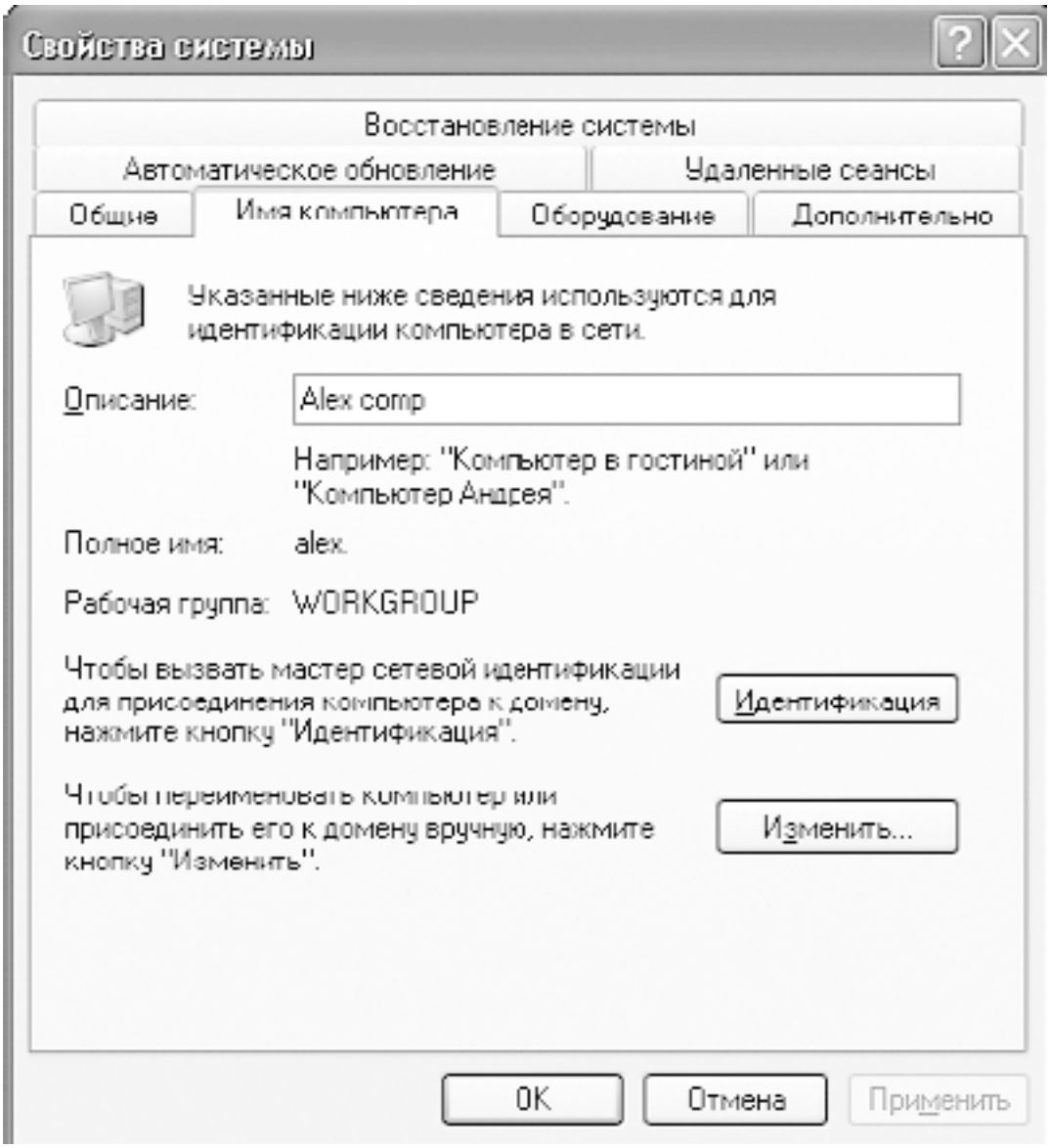

Рис. 28.1. Окно Свойства системы

К сожалению, в большой локальной сети использование единой рабочей группы – редкое явление, поэтому смена группы часто оказывается необходимостью.

Чтобы сменить принадлежность к группе, нужно нажать кнопку **Изменить**. В результате откроется окно (рис. 28.2).

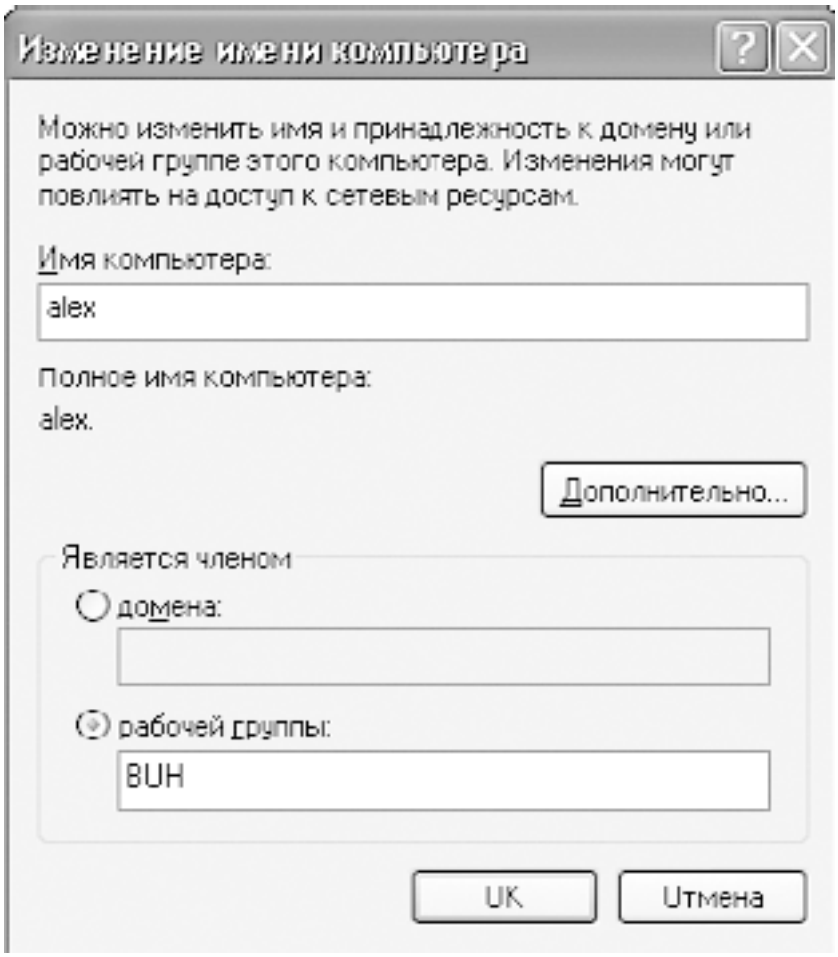

Рис. 28.2. Подключение к рабочей группе

В нижней части окна находится поле. В нем нужно ввести имя группы, к которой вы хотите присоединиться, как это показано на рисунке. После нажатия кнопки **ОК**и недолгого ожидания появится окно (рис. 28.3), приветствующее вас как члена этой группы.

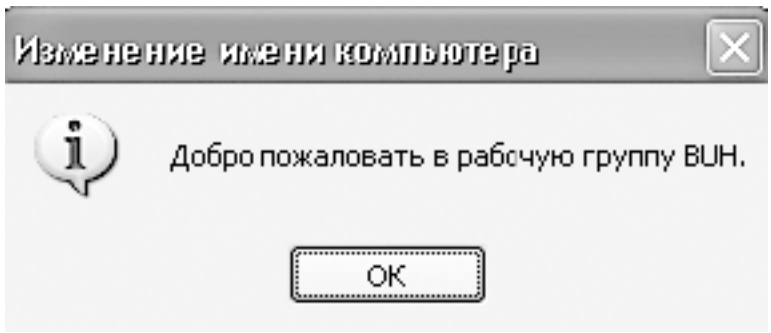

Рис. 28.3. Успешное присоединение к рабочей группе

После перезагрузки компьютера, о необходимости чего оповещает соответствующее сообщение, вы станете полноправным членом указанной группы и сможете пользоваться теми правами, которые определены для участников данной группы.

Подключение к домену

В отличие от рабочей группы, домен является гораздо более важной и сложной структурой. Об этом свидетельствует хотя бы тот факт, что подключение к домену или отключе-

ние от него может произвести либо сам администратор домена, либо пользователь с правами администратора домена.

Для подключения к домену можно применять тот же подход, который используется для подключения к рабочей группе, либо применять более длинный путь, подразумевающий использование мастера подключений. Правда, это выглядит немного странно: зачем использовать мастер подключения к домену администратору домена, если простой пользователь, который мог бы применять этот мастер, не сможет самостоятельно подключиться к домену в силу отсутствия соответствующих прав?

Как бы там ни было, чаще всего применяют именно быстрый способ подключения, который мы и рассмотрим в качестве примера.

Прежде всего необходимо открыть окно свойств системы, перейти на вкладку **Имя компьютера** и нажать кнопку **Изменить**. Далее в открывшемся окне следует указать имя домена, как показано на рис. 28.4.

Имя домена нужно указывать именно так, как оно зарегистрировано, в противном случае его обнаружение будет невозможным.

Примечание

При создании контроллера домена используется трехзвенная структура наименования, включающая в себя не только название домена, но и его принадлежность к доменной зоне, например domen int ru Однако это условие может и не соблюдаться, что делает возможным использование в качестве названия домена одного слова, например domen, как это показано в приведенном здесь примере

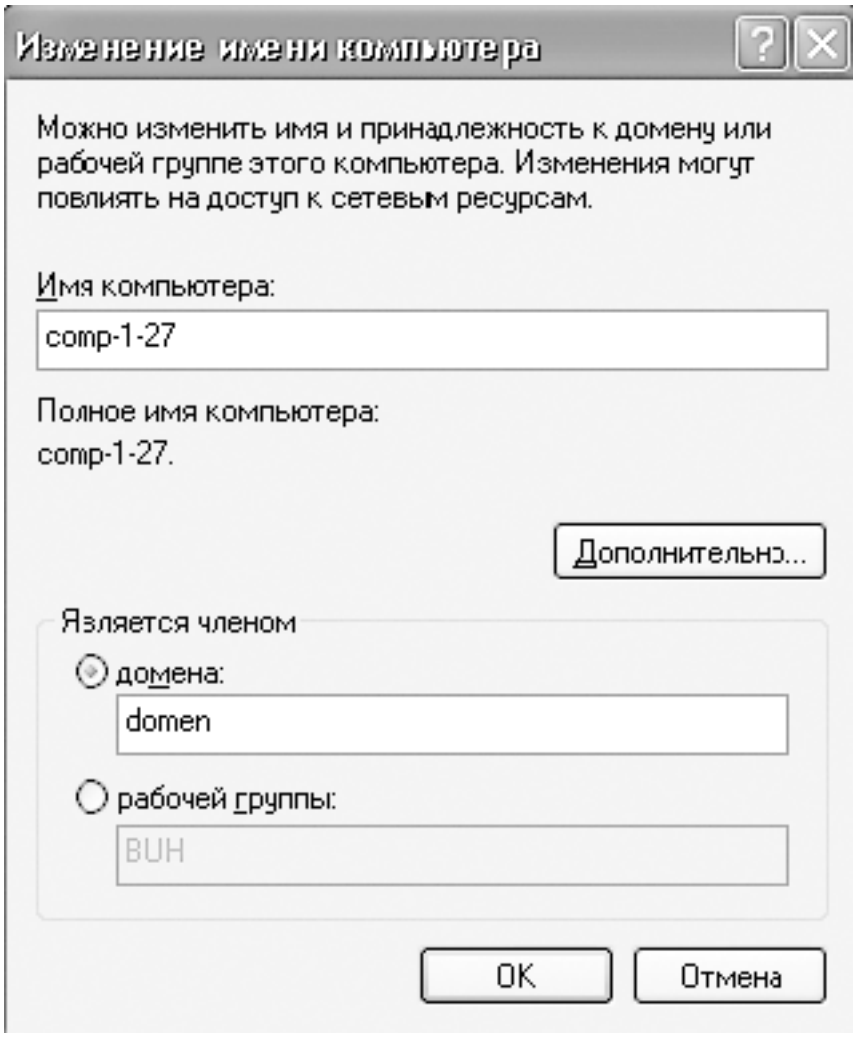

Рис. 28.4. Задание имени домена и имени компьютера

Кроме всего прочего, как правило, при использовании доменной структуры имя компьютера выбирается таким образом, чтобы можно было легко определить место его расположения. В нашем примере применяется имя компьютера **comp-1-27**, которое можно расшифровать как «компьютер на первом этаже в комнате № 27».

После нажатия кнопки **OK** сработает система авторизации подключения к домену, требующая ввода имени и пароля пользователя с правами на подключения к домену (рис. 28.5).

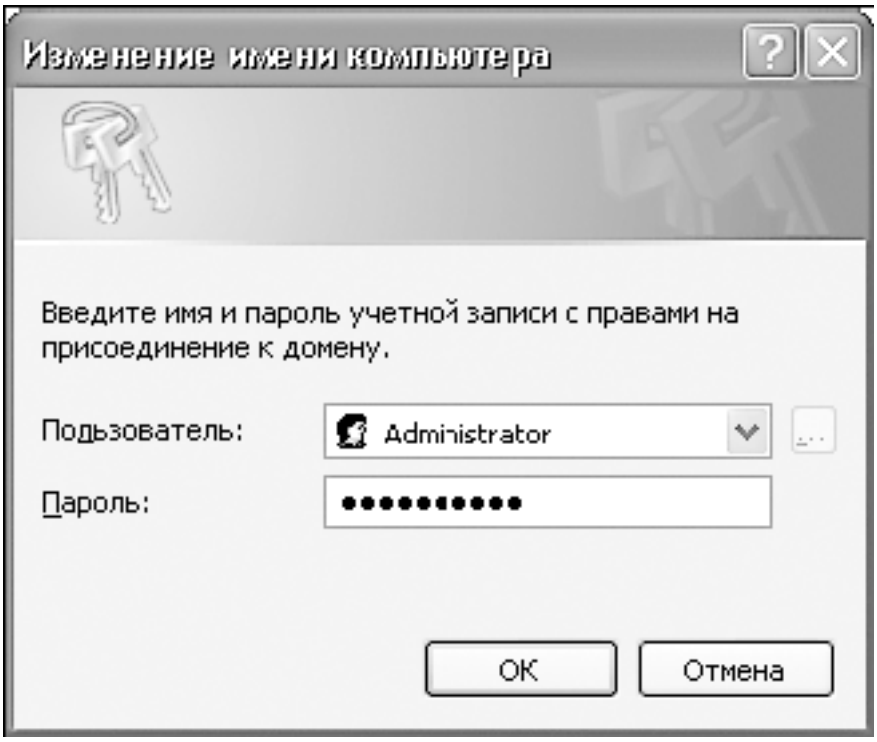

Рис. 28.5. Прохождение авторизации в домене

Если введенные вами данные будут верны, то после нескольких секунд вы окажетесь в домене, о чем будет свидетельствовать появление соответствующего сообщения. Далее, чтобы полноценно начать работу с ресурсами домена, нужно будет перезагрузить компьютер и пройти авторизацию.

Настройка TCP/IP-протокола

Как уже упоминалось ранее, часто присутствие компьютера в рабочей группе или домене требует определенной настройки TCP/IP-протокола, а иногда и IP-адреса DNS-сервера. Это может произойти по нескольким причинам, что в основном связано с важностью компьютера. Примером такой важности может быть установленное на компьютере программное обеспечение, доступ к которому осуществляется с других компьютеров, то есть получается ситуация «клиент – сервер» и компьютер выступает в роли сервера. Ограниченность клиентской части программы может не позволять производить автоматический поиск сервера, поэтому для обеспечения доступа к серверу требуется статический IP-адрес. Могут быть и другие причины использования статичного IP-адреса, но суть не столь важна, главное – уметь его настроить.

Все необходимые настройки TCP/IP-протокола выполняются для соответствующего сетевого подключения, поэтому для начала необходимо открыть свойства этого подключения.

Запустите группу **Сетевые подключения**, воспользовавшись компонентом **Сетевые подключения** на **Панели управления**. В результате должно появиться окно со списком сетевых подключений (рис. 28.6).

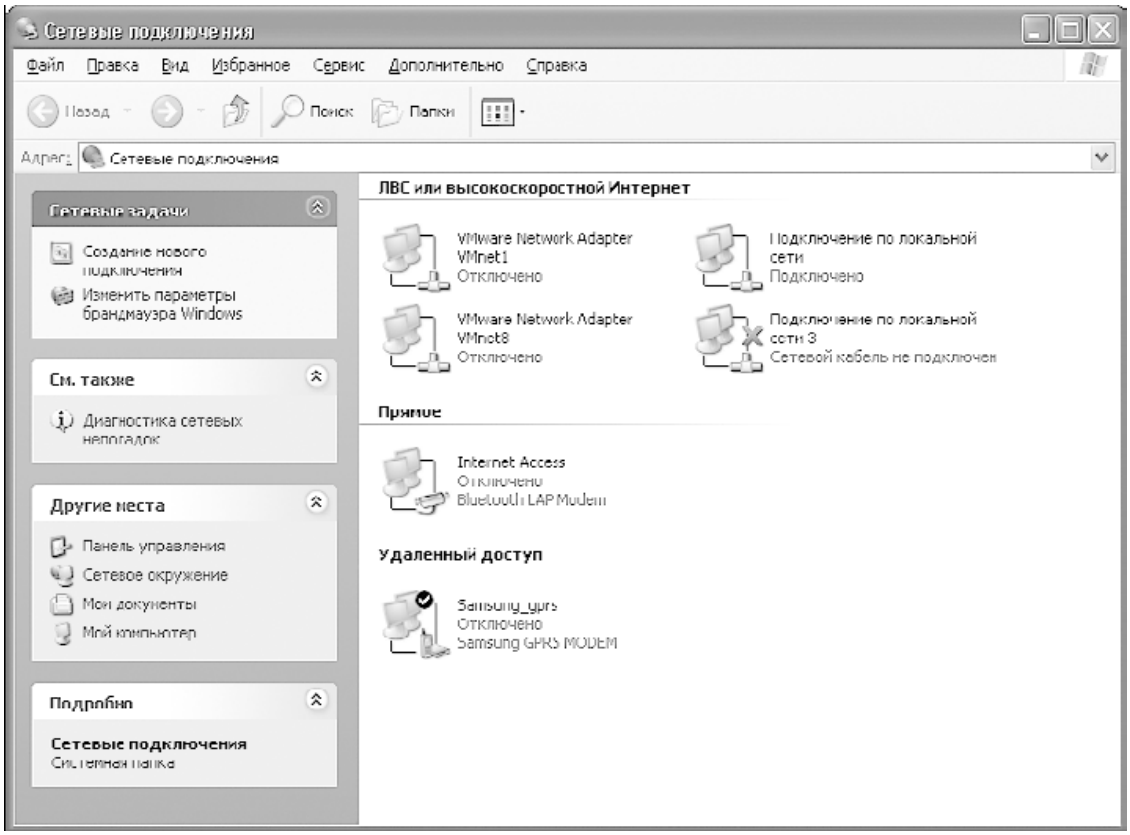

Рис. 28.6. Группа Сетевые подключения

Количество сетевых подключений может быть разным, что зависит от количества установленных сетевых адаптеров и даже установленного программного обеспечения. По этой причине не удивляйтесь, если, открыв сетевые подключения, вы увидите не одно, а несколько сетевых подключений, в том числе и неактивные.

Щелкните правой кнопкой мыши на нужном сетевом подключения и выберите в появившемся меню пункт **Свойства**. Появится окно свойств данного подключения (рис. 28.7).

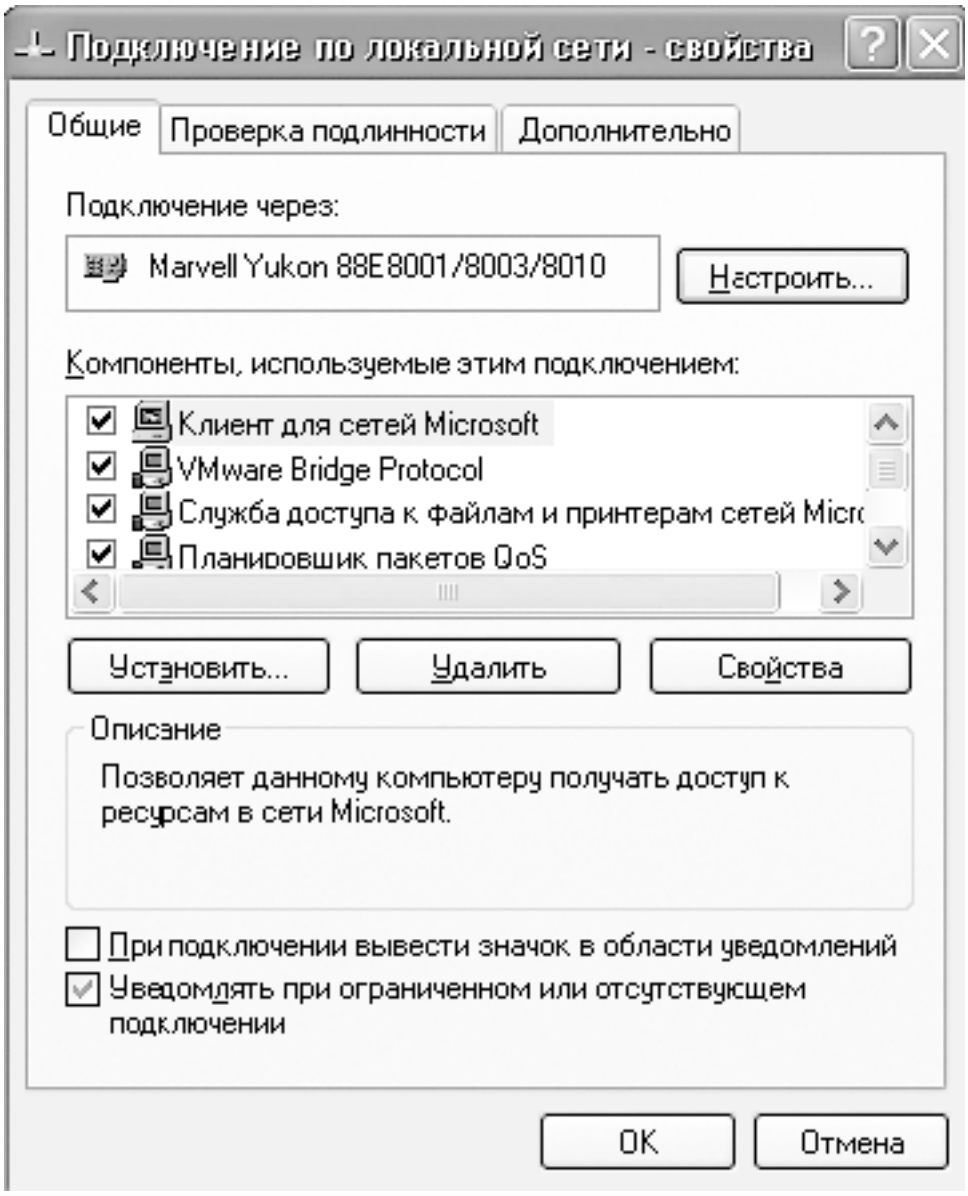

Рис. 28.7. Свойства выбранного сетевого подключения

Чтобы настроить параметры IP-протокола, дважды щелкните на строке **Протокол Интернета (TCP/IP)** или выделите ее и нажмите кнопку **Свойства**. В результате откроется окно свойств протокола, в котором можно будет изменить нужные параметры (рис. 28.8).

Для ввода IP-адреса и маски подсети используются поля **IP-адрес** и **Маска подсети** соответственно. По умолчанию подразумевается автоматическое получение адреса, поэтому чтобы ввести конкретный адрес, сначала установите переключатель в положение **Использовать следующий IP-адрес**.

В этом же окне можно указать и другие важные адреса, если того требуют правила подключения к домену: адрес шлюза и DNS-серверов.

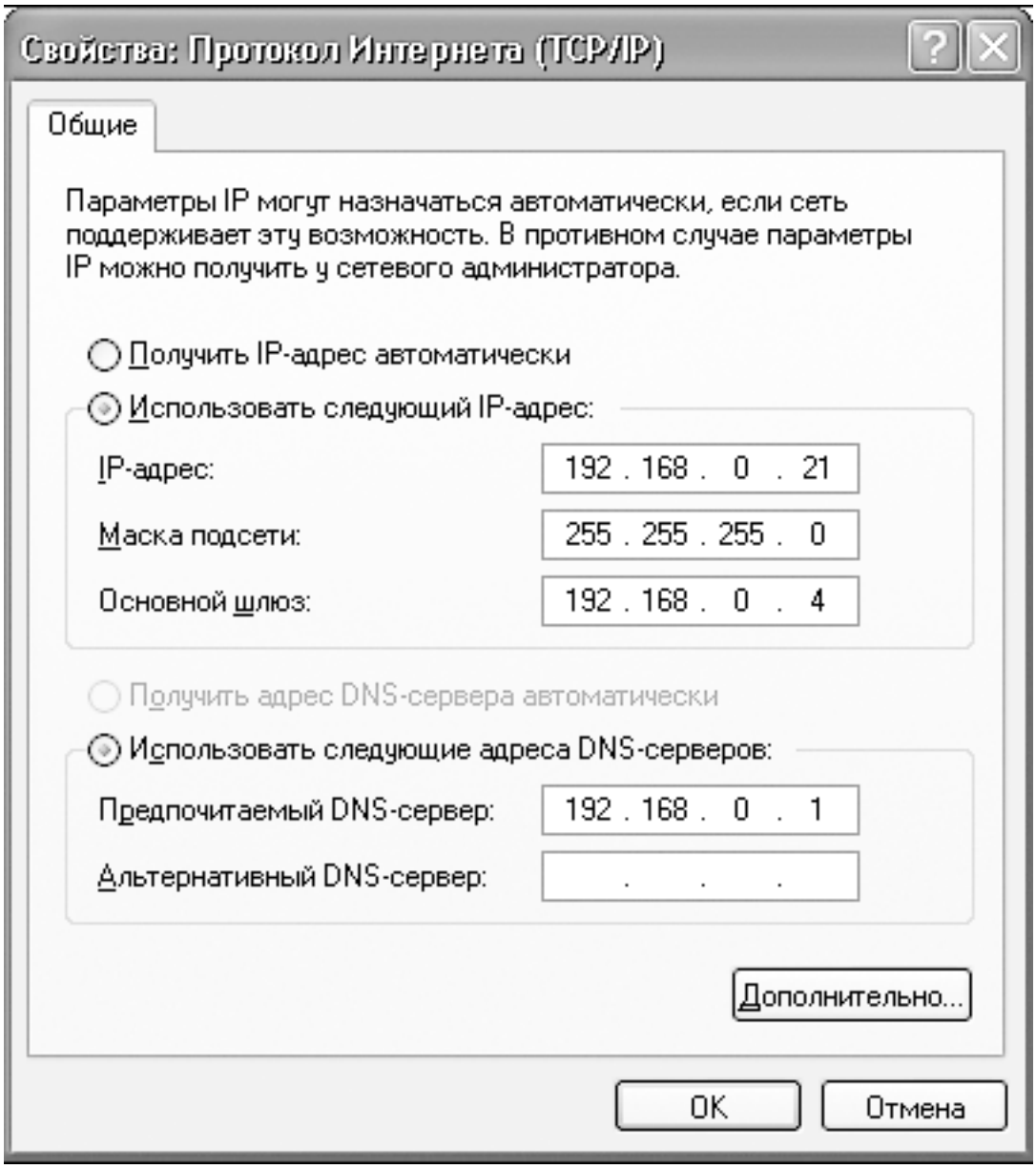

Рис. 28.8. Окно свойства протокола TCP/IP

Применение настроек происходит сразу же, поэтому перезагрузку компьютера производить не нужно.

Глава 29
Подключение и настройка клиента Windows Vista

□ Настройка сетевого обнаружения
□ Подключение к рабочей группе
□ Подключение к домену
□ Настройка общего доступа к файловым ресурсам
□ Настройка общего доступа к принтеру

Операционная система Windows Vista, являющаяся предшественником Windows 7, даже несмотря на большое количество недоработок, помешавших ее широкому распространению, успела стать операционной системой многих компьютеров и ноутбуков. Кроме того, Windows 7 переняла от нее все полезные механизмы работы, в том числе и с локальной сетью.

Механизм работы в составе локальной сети претерпел значительные изменения по сравнению со своим аналогом в операционной системе Windows XP. По этой причине, если потребуется подключить компьютер с Windows Vista к локальной сети, изложенная ниже информация может вам очень пригодиться.

Особенностью Windows Vista является более контролируемый и защищенный процесс работы в локальной сети, позволяющий использовать разные режимы функционирования. Например, подключение к локальной сети можно произвести так, что остальные участники сети даже не узнают об этом, а вы при этом сможете свободно пользоваться всеми ресурсами сети. Для того же, чтобы обнаружить себя в сети или дать возможность другим использовать ваши ресурсы, требуется задействовать определенный механизм. О всех подобных хитростях, а также о том, как подключить компьютер к рабочей группе или домену, рассказано далее.

За работу сетевого окружения отвечает механизм **Центр управления сетями и общим доступом**, который можно запустить с **Панели управления** (рис. 29.1). Откройте ее, найдите раздел **Сеть и Интернет** и пройдите по ссылке **Просмотр состояния сети и задач**.

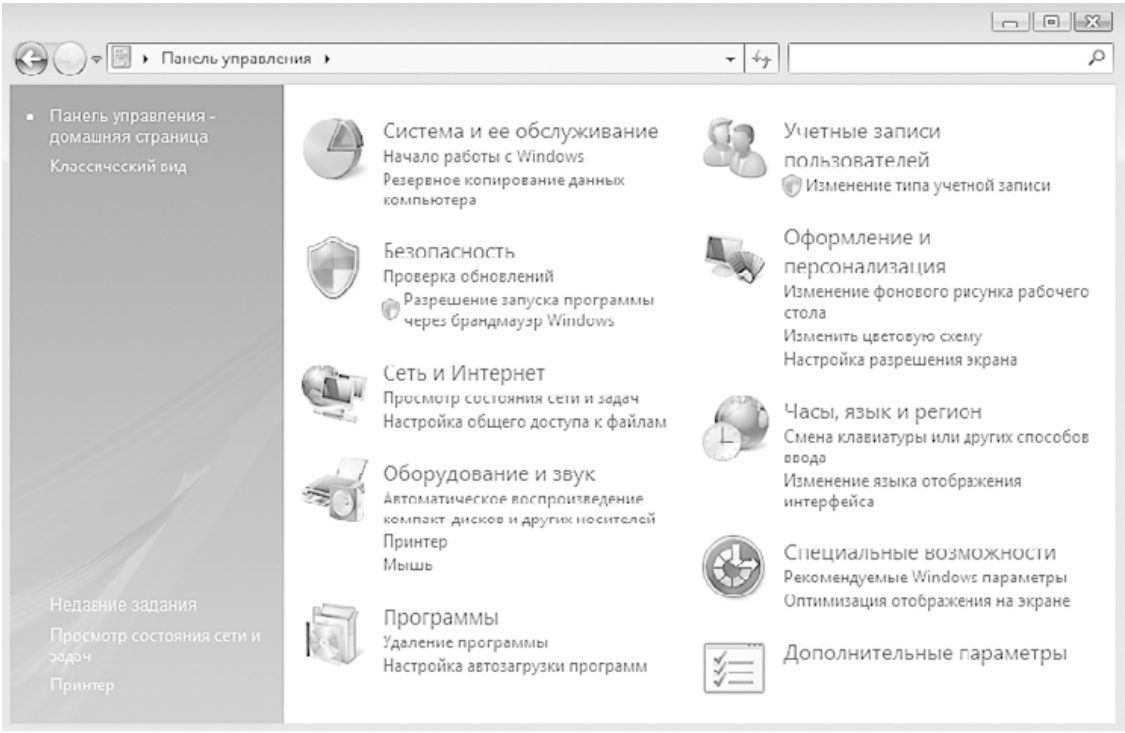

Рис. 29.1. Панель управления

В результате откроется окно (рис. 29.2), в котором находится вся информация, касающаяся текущего состояния сетевого окружения, и механизмы управления этим состоянием.

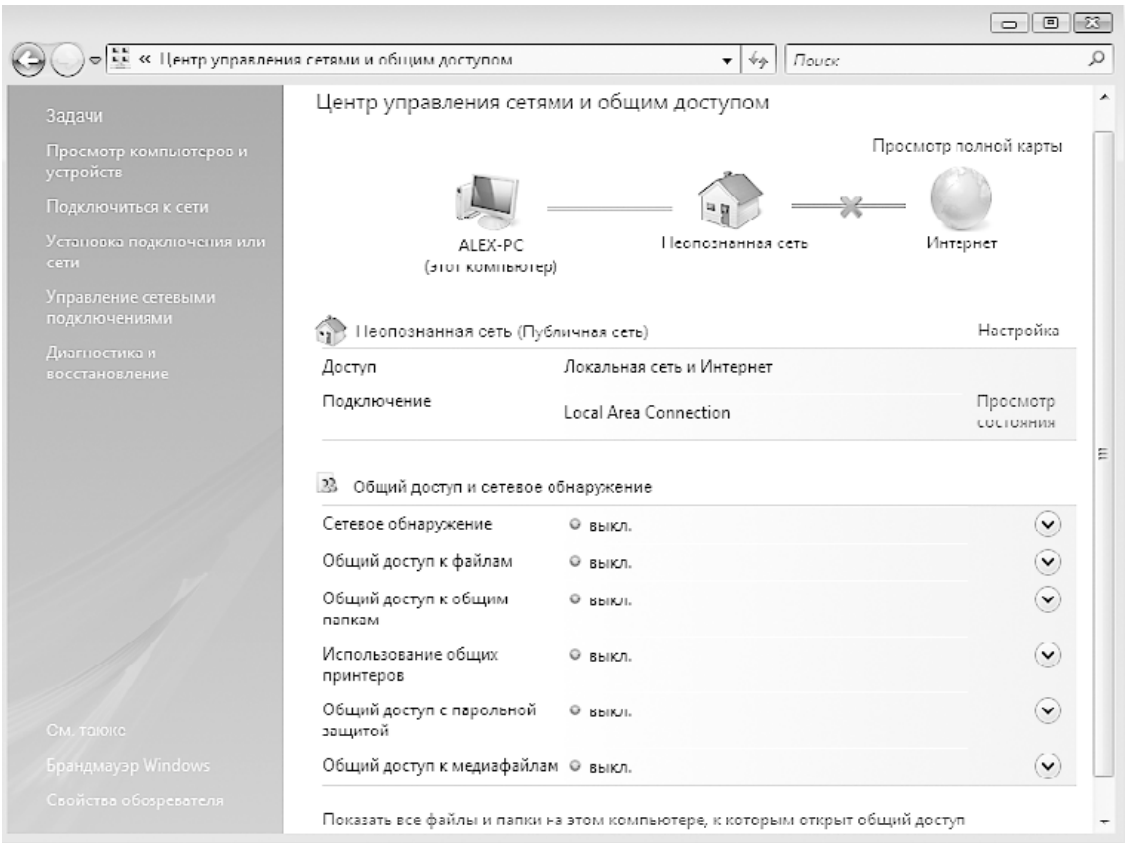

Рис. 29.2. Центр управления сетями и общим доступом

Используя эти механизмы, можно управлять поведением компьютера в сети.

Настройка сетевого обнаружения

Согласно существующим в Windows Vista подходам обеспечения безопасности компьютер при подключении к любому типу сети остается невидимым для всех и сам не видит никого. Поэтому, чтобы можно было начать настройку сетевых параметров системы и увидеть результат, прежде всего необходимо активизировать механизм сетевого обнаружения. Для этого щелкните левой кнопкой мыши на разделе **Сетевое обнаружение**. В результате данный раздел раскроется, отобразив два положения переключателя. Чтобы позволить компьютеру видеть другие компьютеры сети и, в свою очередь, дать возможность видеть себя, установите переключатель в положение **Включить сетевое обнаружение** и нажмите кнопу **Применить** (рис. 29.3).

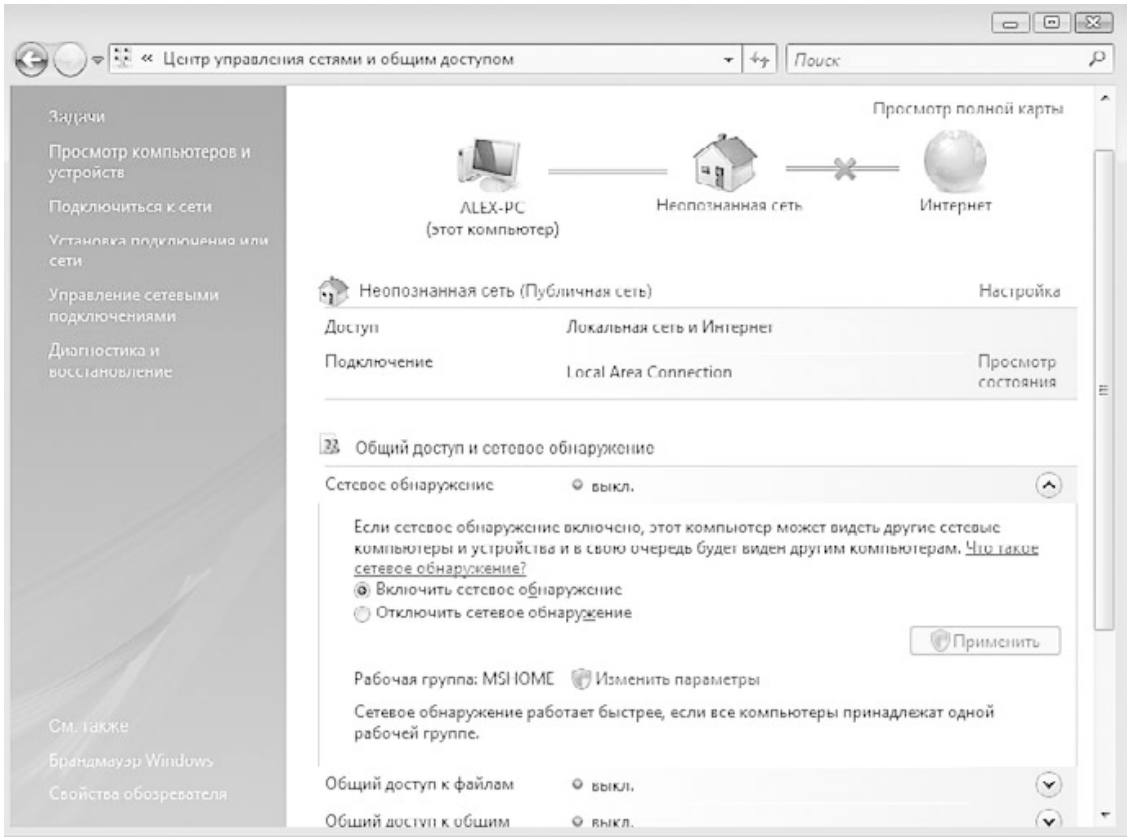

Рис. 29.3. Включение сетевого обнаружения

В результате соответствующий механизм начнет работу, о чем будет свидетельствовать зеленый индикатор с надписью вкл. напротив надписи **Сетевое обнаружение**.

Подключение к рабочей группе

Новый подход в механизмах работы с локальной сетью делает принадлежность компьютера с Windows Vista к определенной рабочей группе неактуальной, но только до тех пор, пока речь идет о компьютерах с такой же или более новой операционной системой, например Windows 7. Если же «соседями» по рабочей группе окажутся компьютеры с более старыми операционными системами и им потребуется доступ к компьютеру с Windows Vista, может возникнуть целый ряд проблем. Чтобы не пришлось решать данные проблемы, лучшим выходом из ситуации будет их не допустить, а именно – присоединиться к рабочей группе.

Чтобы присоединить компьютер к определенной рабочей группе, необходимо выполнить следующие действия. Сначала следует открыть окно свойств системы, что можно сделать, воспользовавшись **Панелью управления** и запустив системный механизм **Системы**. В результате появится окно, показанное на рис. 29.4.

В нижней части окна находится раздел **Имя компьютера, имя домена и параметры рабочей группы**, в котором можно увидеть, к какому из подобных объектов в данный момент подключен компьютер. Здесь же присутствует ссылка **Изменить параметры**, с помощью которой можно изменить это состояние. Если щелкнуть на ней, откроется окно, показанное на рис. 29.5, в котором нужно перейти на вкладку **Имя компьютера**.

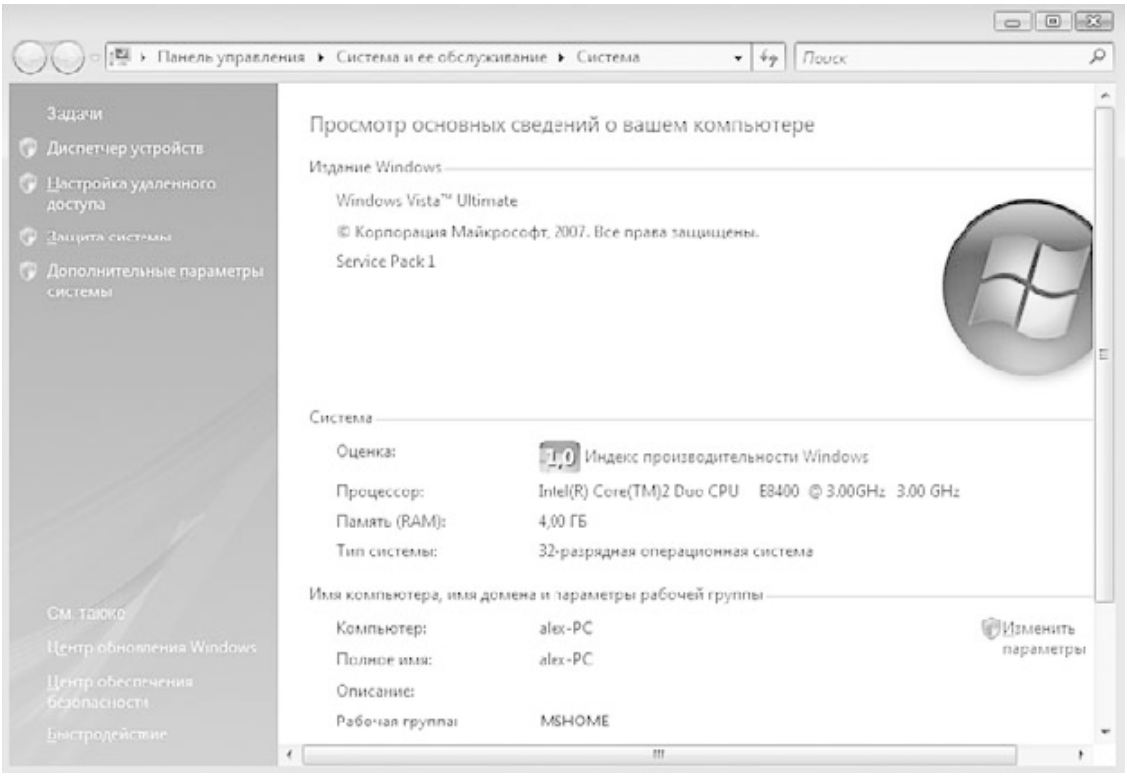

Рис. 29.4. Окно Система

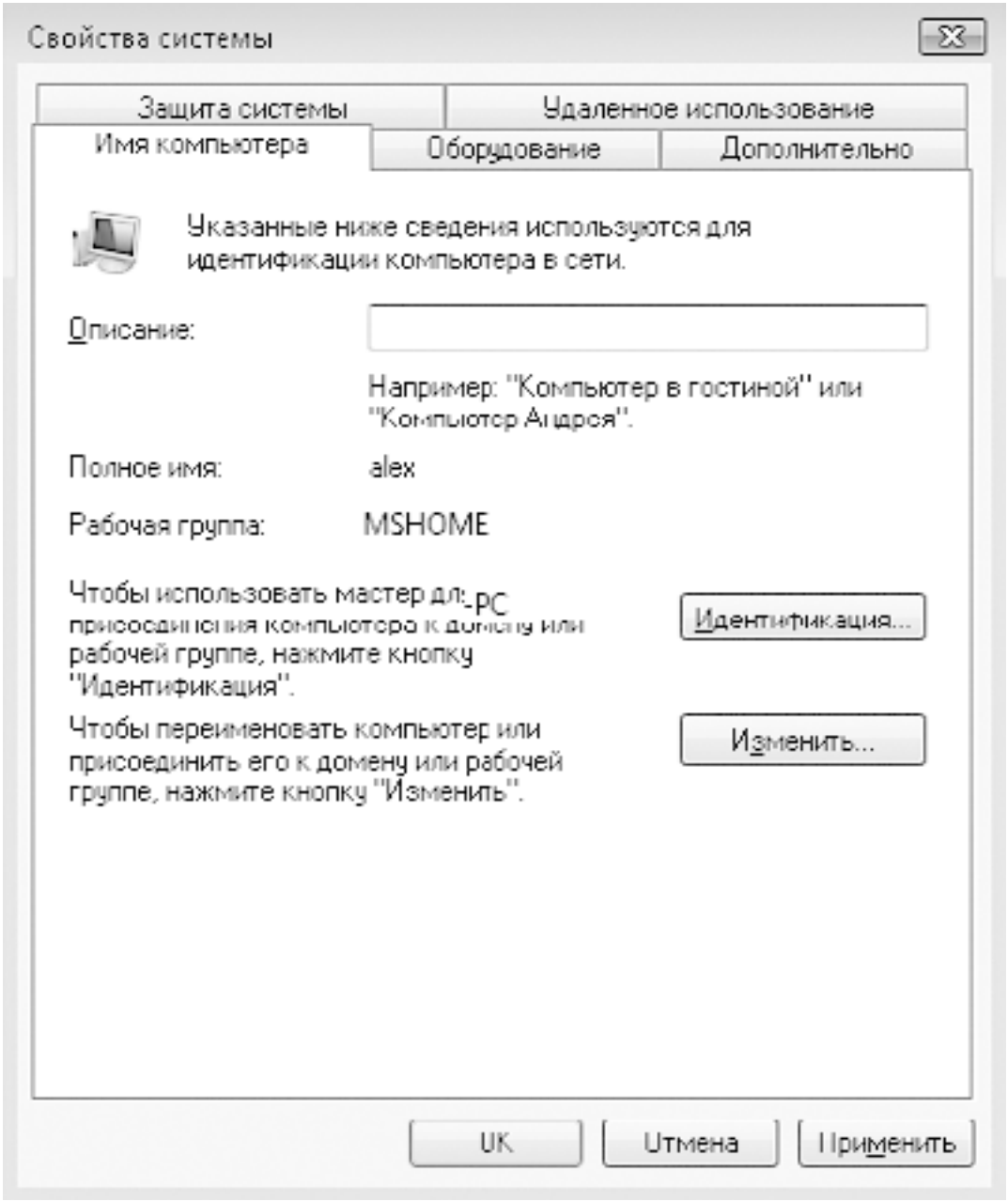

Рис. 29.5. Вкладка Имя компьютера

Для подключения к рабочей группе нажмите кнопку **Изменить**. В результате откроется окно, в котором можно будет указать имя рабочей группы, а также при необходимости изменить имя компьютера (рис. 29.6).

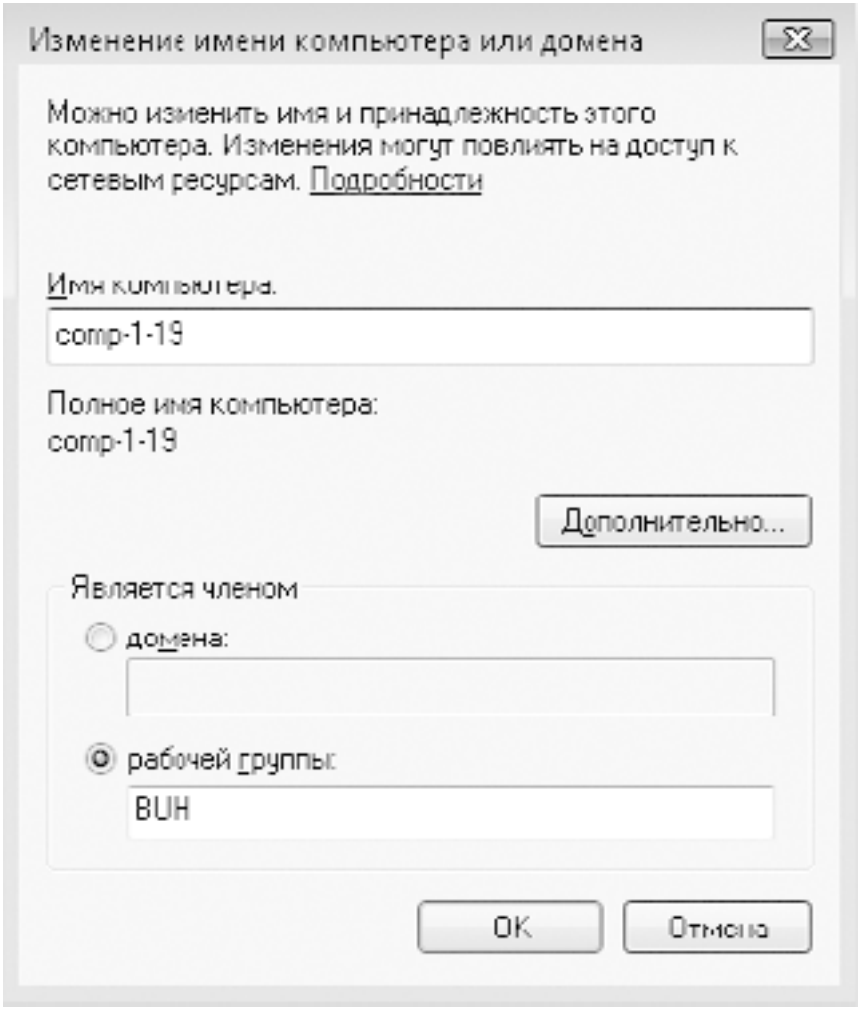

Рис. 29.6. Ввод названия рабочий группы

После нажатия кнопки **OK** появится сообщение, свидетельствующее о том, что вы присоединились к рабочей группе с указанным именем. После этого необходимо перегрузить компьютер, чтобы изменения вступили в силу.

Подключение к домену

Подключение компьютера с установленной операционной системой Windows Vista к домену требует участия администратора домена или пользователя с правами подключения компьютеров к домену.

Происходит процесс подключения достаточно быстро и просто. Если в окне, показанном на рис. 29.5, нажать кнопку **Изменить**, то откроется окно, в котором вы можете выбрать вариант подключения: либо к рабочей группе, либо к домену (рис. 29.7).

После ввода имени домена, как это показано на рисунке, и нажатия кнопки **OK** появится окно, в котором необходимо будет указать имя и пароль пользователя, который имеет право подключать компьютеры к домену (рис. 29.8).

Если данные авторизации указаны правильно, через некоторые время появится сообщение об удачном подключении к домену. В противном случае нужно будет повторить процесс подключения, чтобы ввести правильные регистрационные данные администратора.

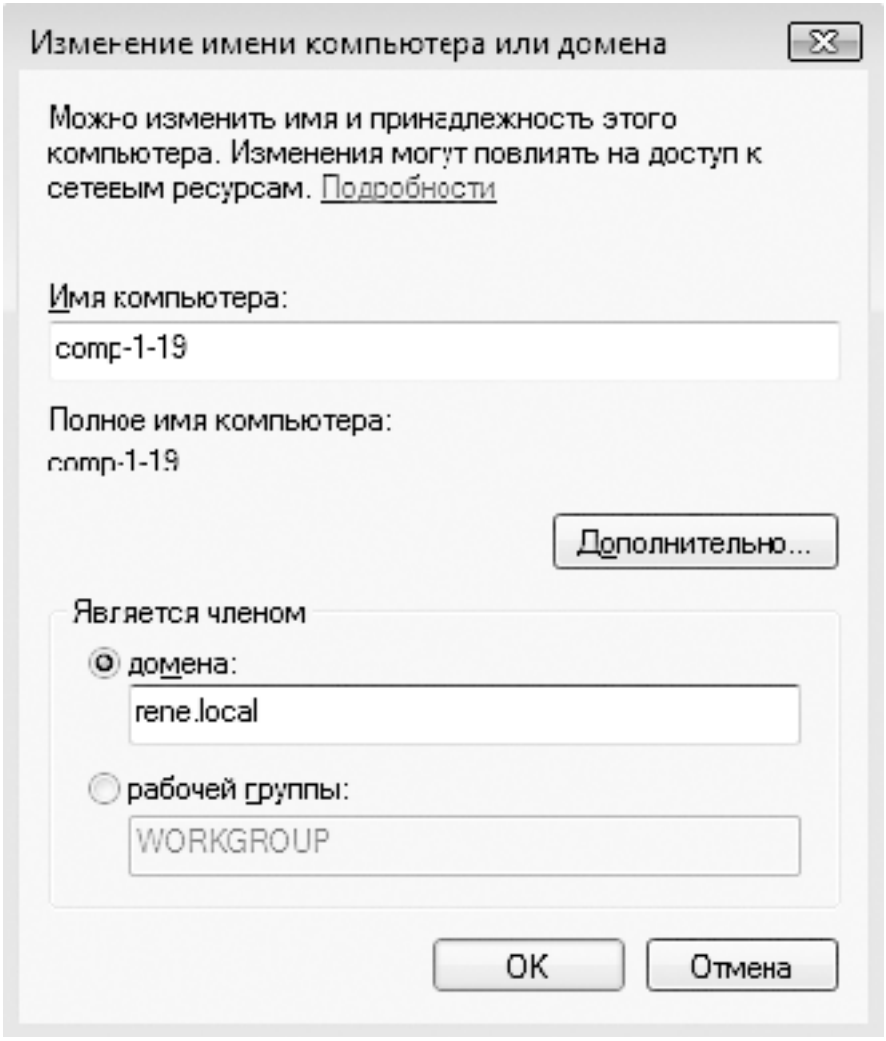

Рис. 29.7. Ввод имени домена

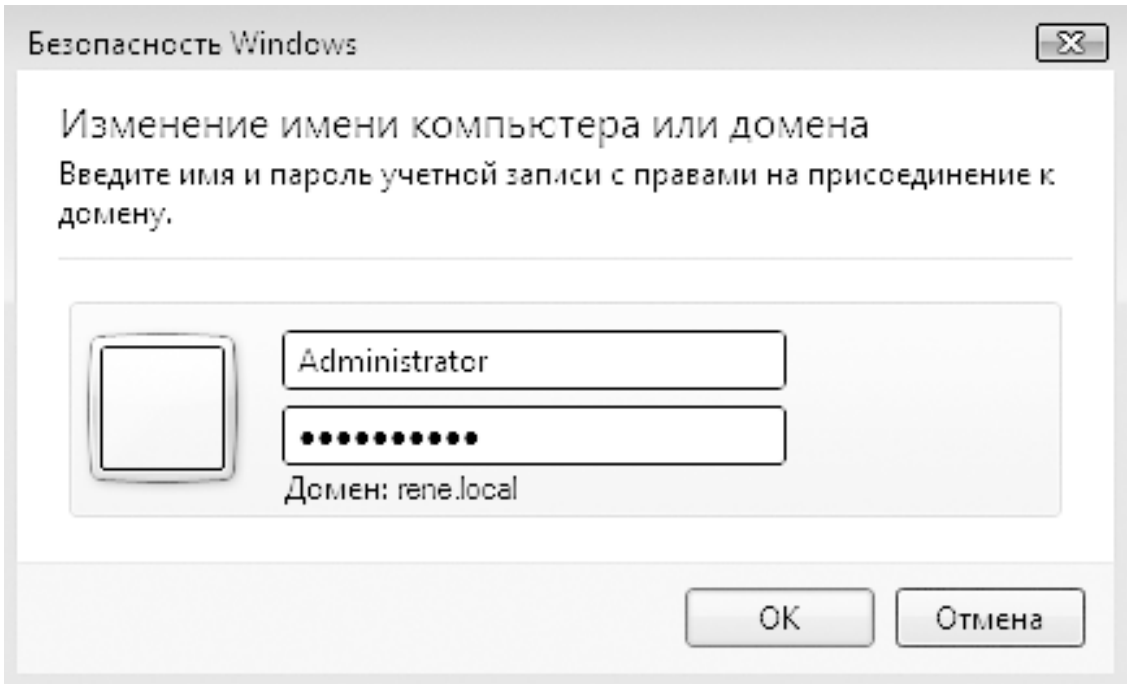

Рис. 29.8. Ввод данных авторизации

Чтобы изменения вступили в силу, требуется перезагрузить компьютер. После перезагрузки компьютера обычный способ входа в систему изменится: теперь для входа в локальную сеть потребуется применение сочетания клавиш **Ctrl+Alt+Delete** с последующим вводом имени пользователя и пароля.

Настройка общего доступа к файловым ресурсам

По умолчанию, даже если вы уже подключены к сети, возможность доступа к ресурсам компьютера будет заблокирована, как это было и в случае с сетевым обнаружением. Поэтому, если стоит вопрос о том, чтобы создать общий ресурс и организовать к нему доступ, нужно будет задействовать соответствующий механизм.

Откройте **Центр управления сетями и общим доступом**, воспользовавшись для этого **Панелью управления**. В появившемся окне щелкните на названии раздела **Общий доступ к файлам**. В результате раздел раскроется и появятся два положения переключателя. Чтобы активизировать возможность доступа к общим файловым ресурсам, необходимо установить переключатель в положение **Включить общий доступ к файлам** (рис. 29.9).

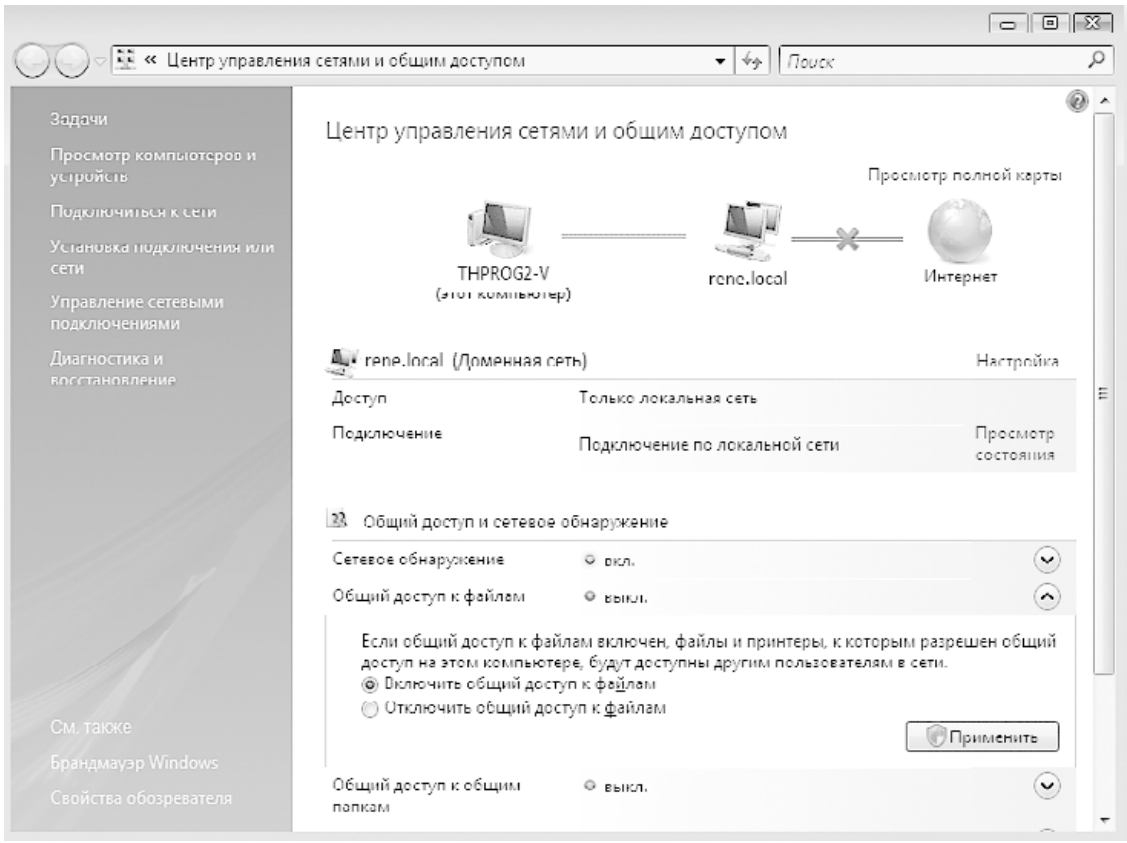

Рис. 29.9. Включение возможности доступа к общим файлам

После нажатия кнопки **Применить** данная функция будет активизирована, о чем будет свидетельствовать зеленый цвет индикатора рядом с надписью **Общий доступ к файлам**.

Теперь рассмотрим, как можно настроить общий доступ к конкретной папке в случае, когда компьютер присоединен к домену.

Используя **Проводник**, найдите папку, которую вы планируете предоставить в общее пользование. Щелкните на ней правой кнопкой мыши и в появившемся меню выберите пункт **Общий доступ** (рис. 29.10).

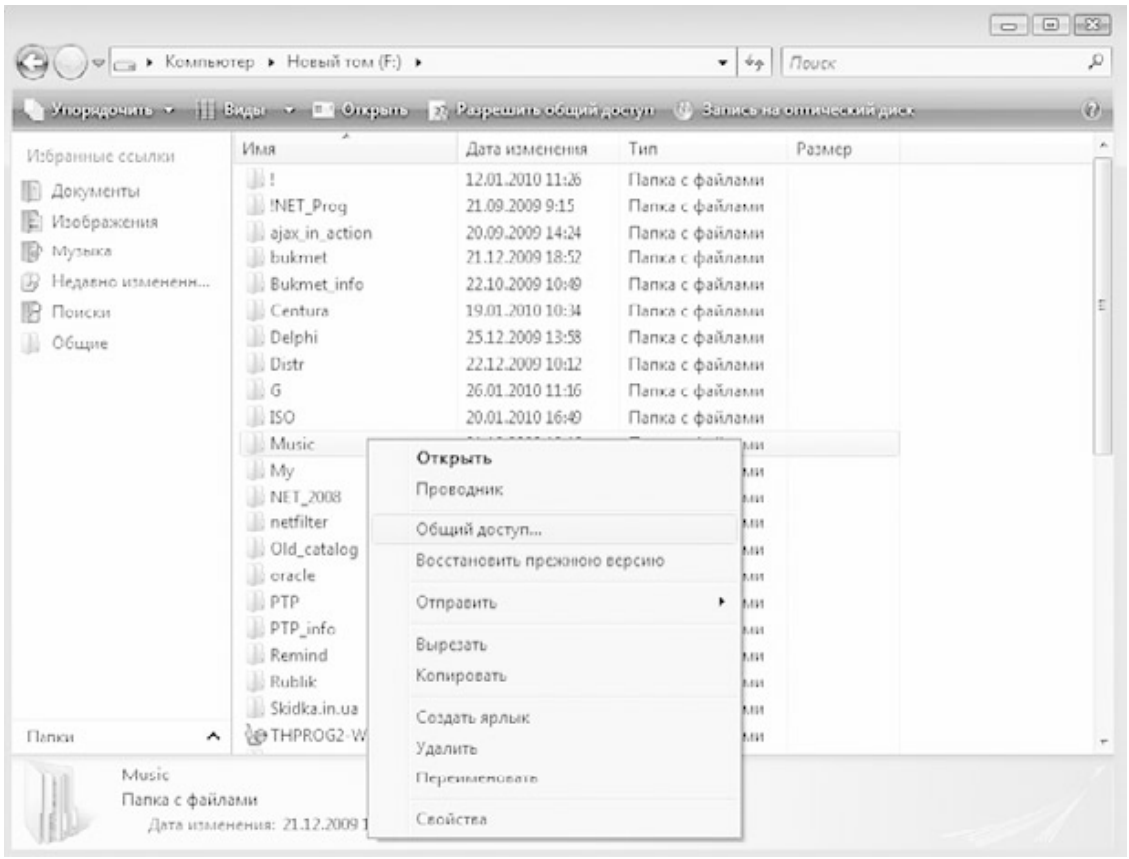

Рис. 29.10. Выбор пункта Общий доступ

В результате откроется окно, где будет отображен список пользователей и групп, которые имеют доступ к вашему ресурсу (рис. 29.11).

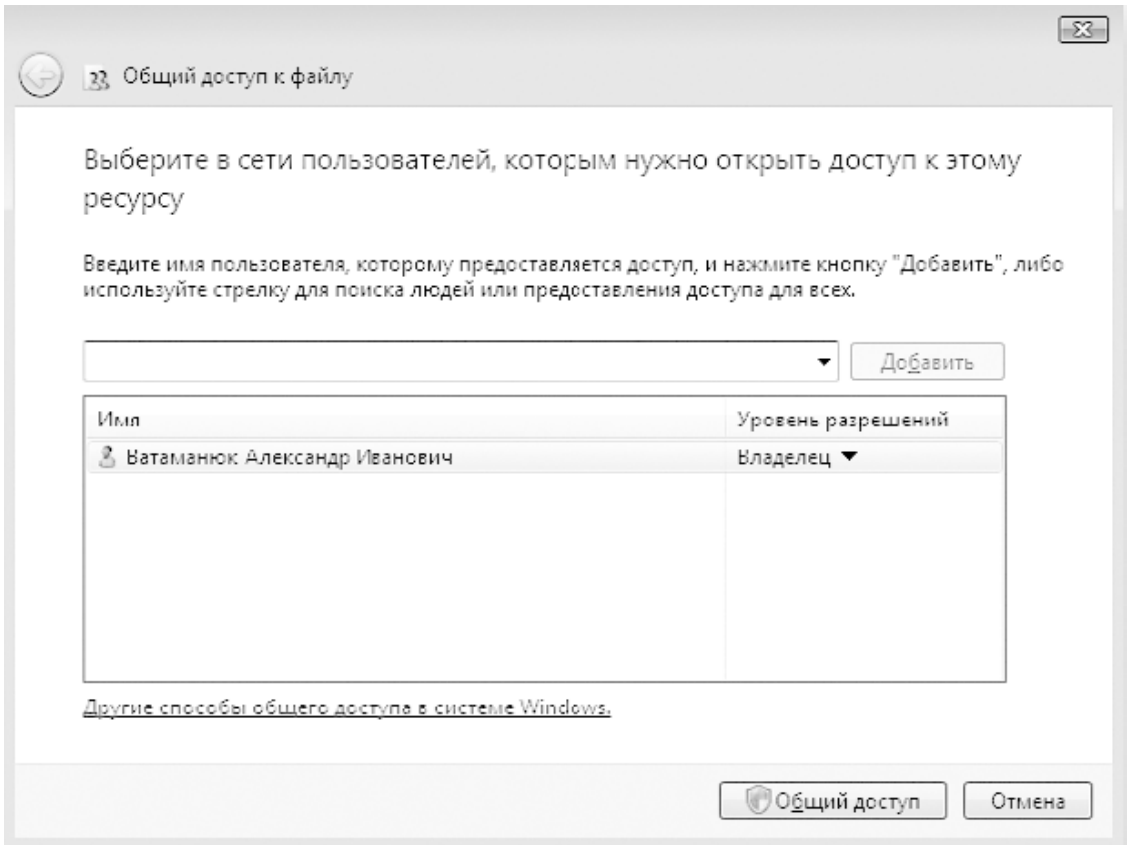

Рис. 29.11. Список пользователей с правом доступа к ресурсу

По умолчанию доступ к ресурсу имеет только владелец компьютера, но это очень легко исправить, используя список в верхней части окна. Для упрощения процесса настройки применяются три варианта доступа: **Читатель, Соавтор** или **Совладелец**. Новая группа или пользователь автоматически добавляется с правами **Читатель**, то есть с правами на чтение ресурса.

Чтобы разрешить доступ к выбранной папке другим пользователям, раскройте список и выберите строку **Найти**. В результате откроется окно, показанное на рис. 29.12.

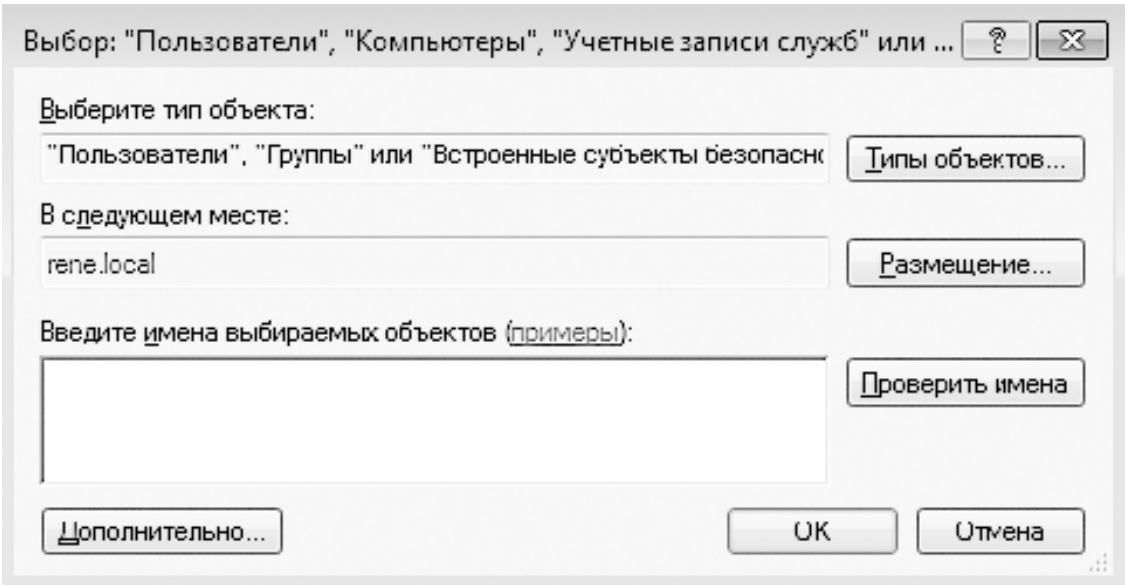

Рис. 29.12. Окно добавления объектов

Существует два варианта добавления объектов, которым необходимо предоставить доступ к ресурсам. Первый из них – ввод вручную с помощью клавиатуры, второй – использование автоматизированного способа добавления.

Первый способ подразумевает ввод имени пользователя, как он указан в домене. Чтобы проконтролировать правильность ввода, используется кнопка **Проверить имена**: если имя пользователя введено правильно, к нему дополнительно прибавится полное имя пользователя, как оно введено в Active Directory. При этом вся запись станет подчеркнутой. Если же имя пользователя указано неверно, ничего не изменится. Если вы в этом случае попытаетесь нажать кнопку **OK**, появится соответствующая ошибка.

Если вы не уверены в написании имени пользователя или требуется добавить сразу несколько пользователей, лучше использовать второй вариант. Для этого нажмите кнопку **Дополнительно**. В результате откроется окно, показанное на рис. 29.13.

Чтобы увидеть список объектов, к которым можно применять какие-либо действия, нажмите кнопку **Поиск**. В результате в нижней части окна появятся такие объекты. Вам следует найти в этом списке строки, которые обозначают нужные вам 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 **OK**.

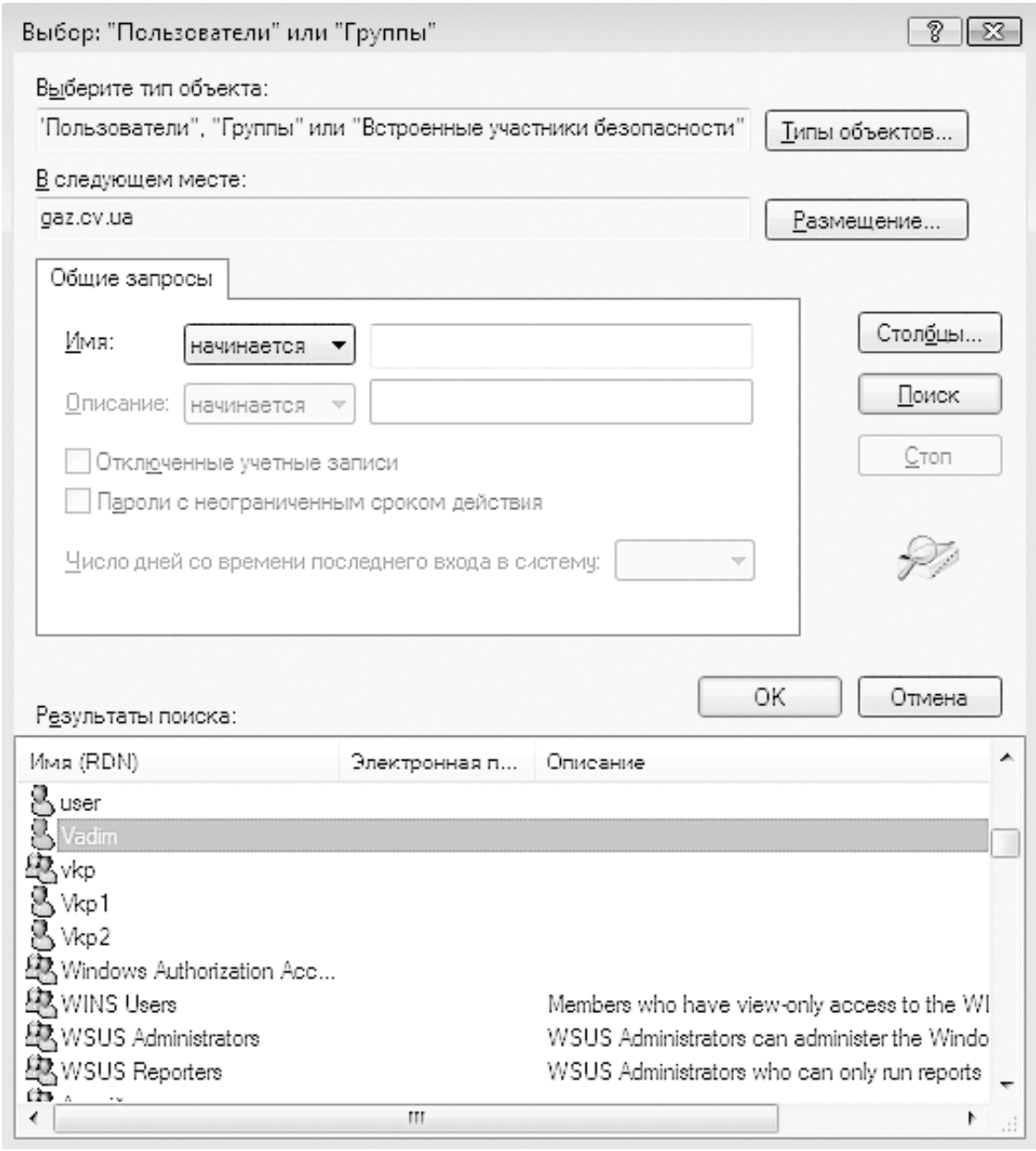

Рис. 29.13. Список объектов

В результате выбранные объекты появятся в окне, показанном на рис. 29.12. Чтобы подтвердить ваше желание продолжить настройку разрешений на доступ к выбранным объектам, нажмите в этом окне кнопку **OK**.

Как уже было упомянуто выше, все новые объекты получают статус **Читатель**.

Если выбранной учетной записи требуется право доступа на чтение и изменение файлов, щелкните на строке с именем учетной записи и в появившемся меню выберите команду **Соавтор** (рис. 29.14).

Теперь, чтобы завершить произведенные действия и открыть общий доступ к выбранному файловому ресурсу, нажмите кнопку **Общий доступ**. По прошествии небольшого количества времени появится окно, в котором сообщается, что общий доступ к указанной вами папке открыт (рис. 29.15).

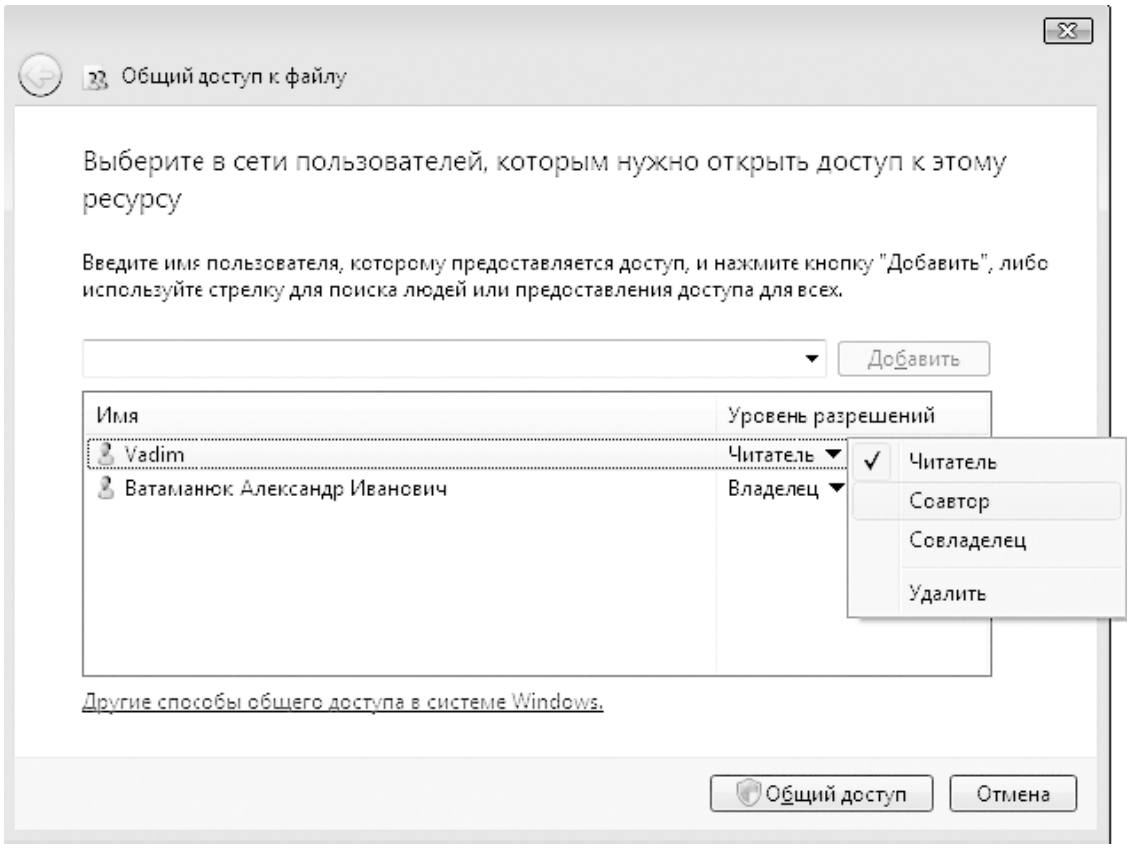

Рис. 29.14. Указание прав доступа

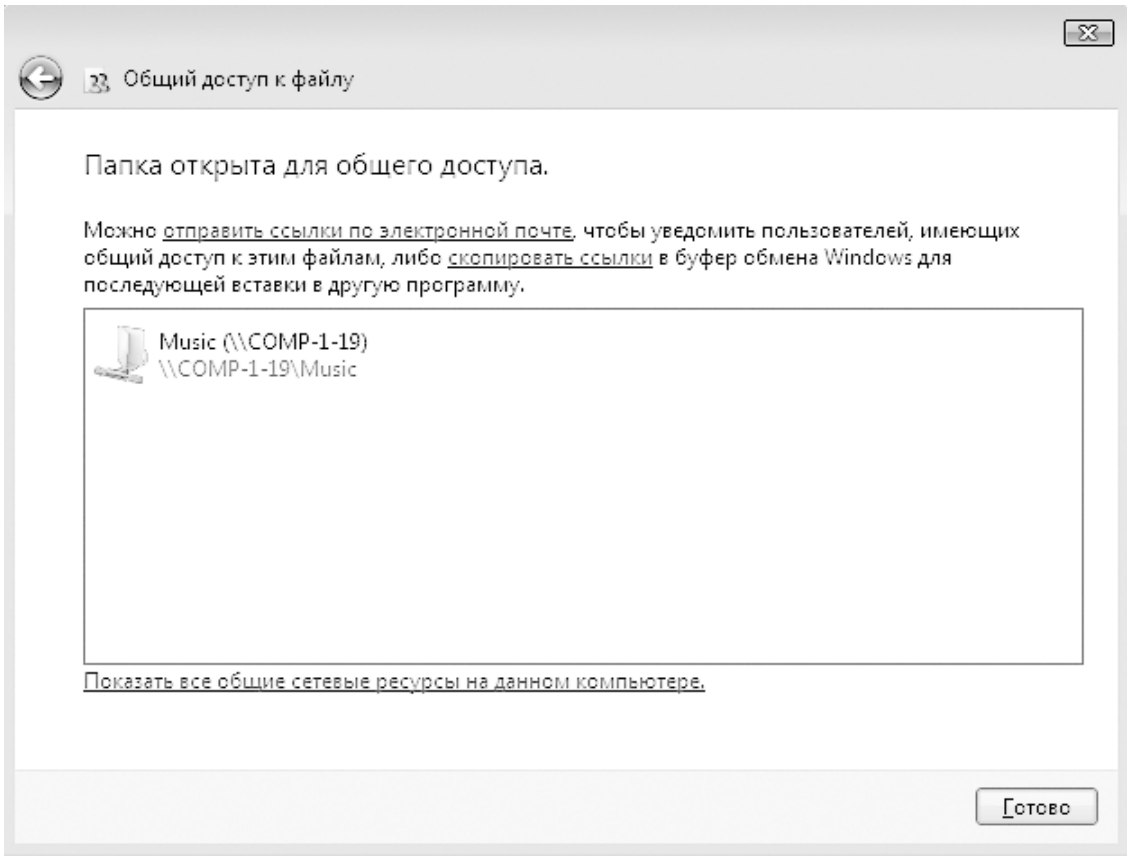

Рис. 29.15. Общий доступ к ресурсу открыт

Если в какой-то момент вы решите прекратить общий доступ к данному файловому ресурсу, то сделать это очень просто. Найдите в **Проводнике** этот ресурс, щелкните правой кнопкой мыши и выберите в меню строку **Общий доступ**. Откроется окно, содержащее два варианта действий (рис. 29.16). Выберите в данном окне команду **Прекратить доступ**.

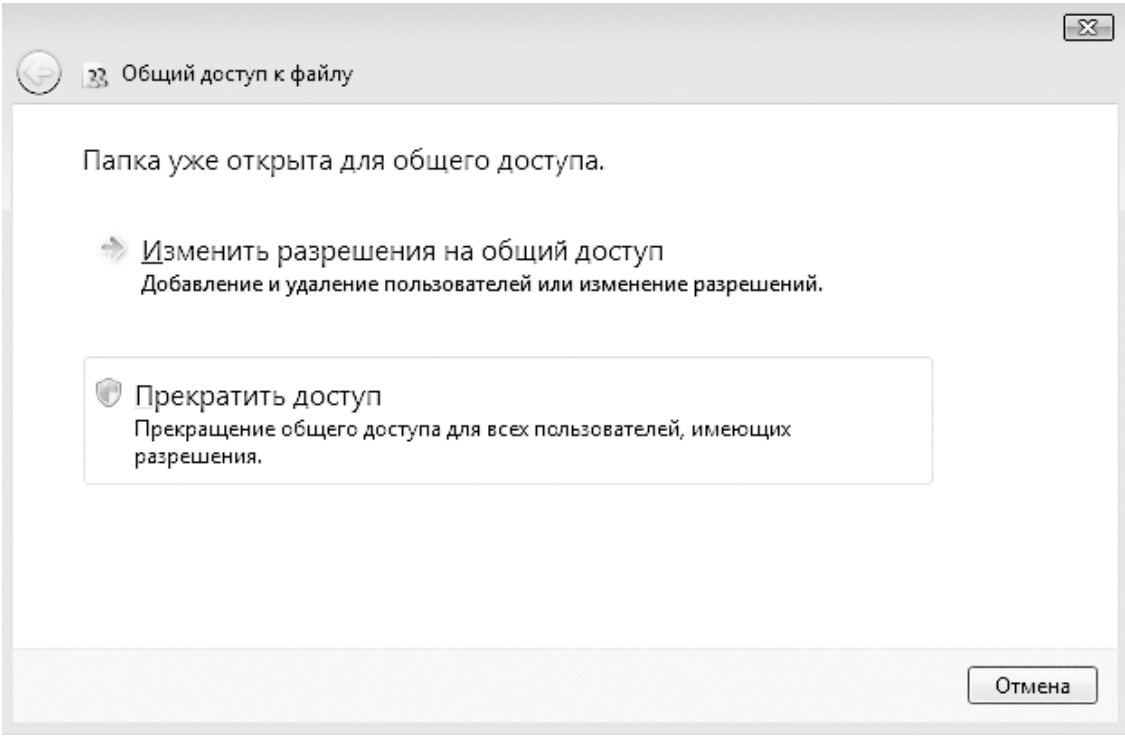

Рис. 29.16. Отменяем общий доступ к ресурсу

Настройка общего доступа к принтеру

Как и в случае с файловыми ресурсами, предоставление общего доступа к принтеру также происходит в два этапа. Прежде всего необходимо активизировать соответствующую возможность, и только потом можно добавлять права на использование принтера.

Откройте **Центр управления сетями и общим доступом**. В появившемся окне нажмите кнопку со стрелкой напротив надписи **Использование общих принтеров**. В результате появятся два положения переключателя (рис. 29.17).

Установите переключатель в положение **Включить общий доступ к принтерам** и нажмите кнопку **Применить**. Система выполнит необходимые настройки и активирует общий доступ к принтерам, о чем сообщит зеленый индикатор рядом с надписью **Использование общих принтеров**.

Следующий шаг – настройка прав доступа. Для этого раскройте группу **Принтеры**, щелкните правой кнопкой мыши на нужном принтере и в появившемся меню выберите пункт **Общий доступ** (рис. 29.18).

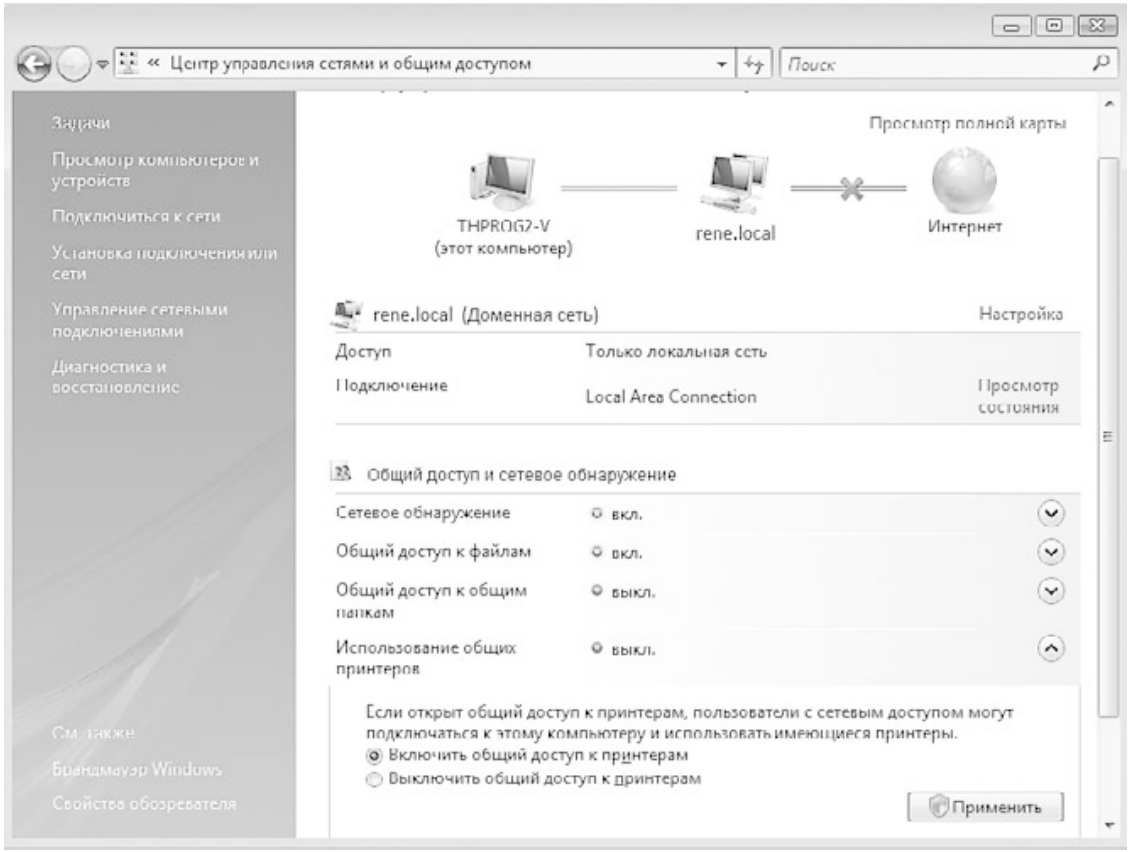

Рис. 29.17. Включение общего доступа к принтеру

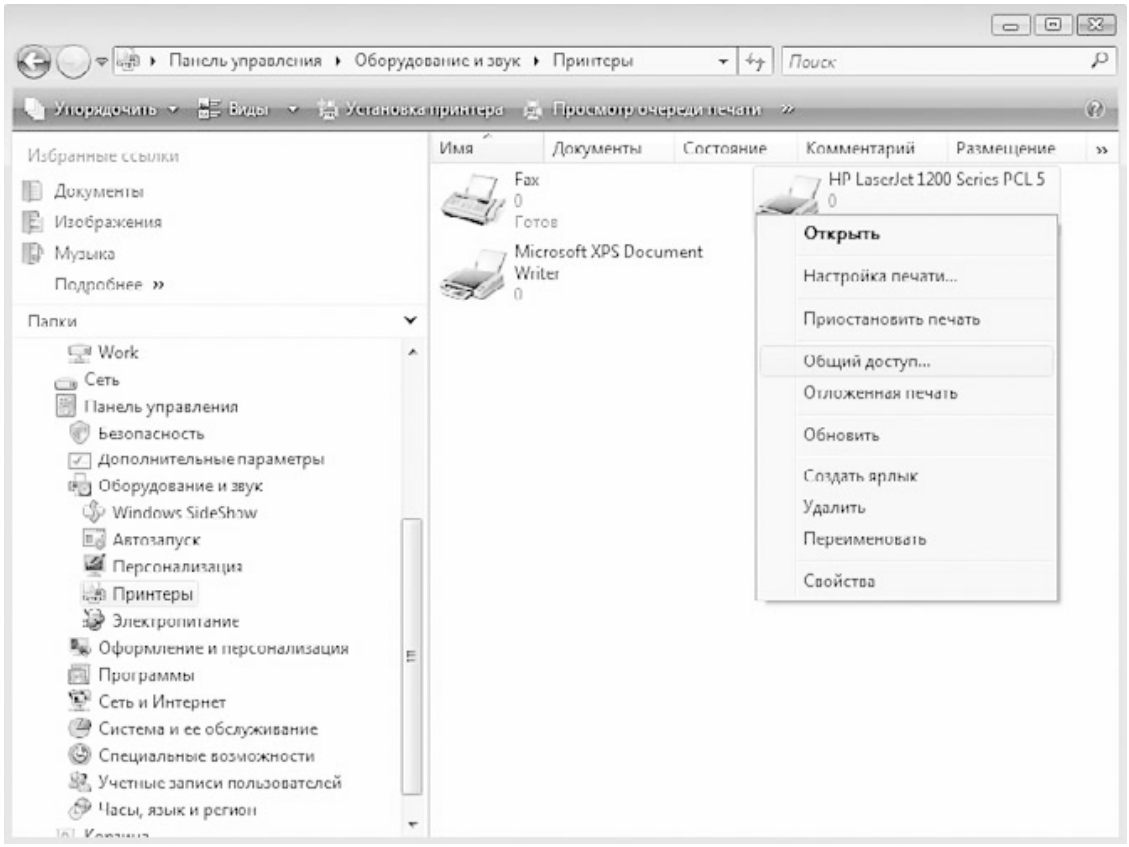

Рис. 29.18. Выбор пункта Общий доступ

Откроется окно настроек принтера с активированной вкладкой **Доступ** (рис. 29.19).

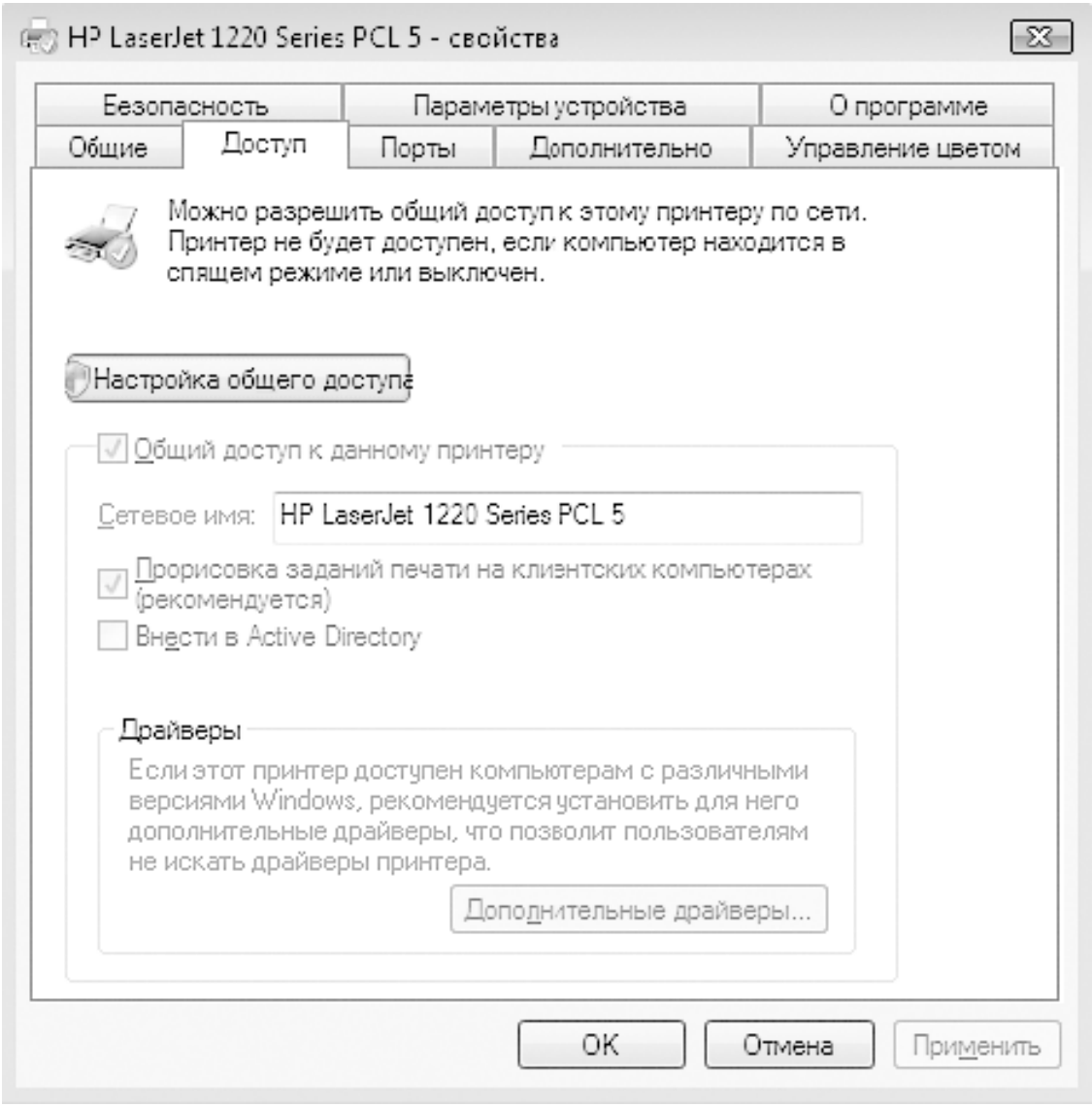

Рис. 29.19. Вкладка Доступ окна настроек принтера

Если служба общего доступа к принтерам уже активирована, то есть действия, описанные выше, уже были выполнены, то доступ к принтеру уже будет открыт. Если по каким-либо причинам флажок **Общий доступ к данному принтеру**, который находится на этой вкладке, не установлен, нажмите кнопку **Настройка общего доступа**.

Это позволит получить доступ к флажку **Общий доступ к данному принтеру**, который необходимо установить. Кроме того, вы сможете изменить имя принтера, под которым он будет виден сетевым пользователям.

Стоит учесть, что по умолчанию доступ к принтеру получают сразу все пользователи. Если такое положение вещей вас не устраивает, перейдите на вкладку **Безопасность** и с помощью кнопки **Добавить** запустите механизм добавления пользователей, работа которого уже была описана выше, когда речь шла о настройке прав доступа к общему файловому ресурсу.

Глава 30
Подключение и настройка клиента Windows 7

□ Выбор сетевого расположения
□ Подключение к рабочей группе
□ Подключение к домену
□ Настройка TCP/IP-протокола

Официальное представление операционной системы Microsoft Windows 7 состоялось не так много времени назад. Однако она успела стать настолько популярной, что складывается впечатление, как будто существует она уже давно. Главной причиной такой популярности стало то, что Windows 7 просто поражает своей скоростью работы. Иногда даже не верится, что она использует в своей основе основные компоненты Windows Vista, насколько она быстрее своей предшественницы.

Когда речь идет о подключении компьютера или ноутбука с Windows 7 к локальной сети, процесс настройки механизмов очень похож на аналогичный процесс в операционной системе Windows Vista. Имеются также и определенные отличия, например в использовании определенного типа сетевого расположения.

Выбор сетевого расположения влияет на защиту операционной системы от возможных воздействий локальной сети, поэтому, если правильно подобрать тип расположения, это позволит получить большую защиту.

Однако данный параметр критичен только в случае, когда компьютер функционирует в составе одноранговой сети и подключен к рабочей или домашней группе. Если же компьютер входит в состав сети, управляемой доменом, весь контроль над защитой компьютера от сетевых атак ложится «на плечи» домена. Поэтому остается только надеяться, что в домене используется соответствующее программное обеспечение, например антивирусная программа.

Выбор сетевого расположения

Как уже было сказано ранее, Windows 7 позволяет использовать разные варианты сетевого размещения компьютера при работе в составе локальной сети. Выбор или смена сетевого размещения влечет за собой изменения в работе соответствующих механизмов операционной системы.

Различают следующие варианты сетевого размещения.

□ **Домашняя сеть.** Это сетевое размещение подразумевает, что компьютер входит в состав небольшой локальной сети, участники которой вам знакомы и уровень доверия к которым вполне высокий, что позволяет не беспокоиться о сетевых угрозах. Данный вариант размещения автоматически устанавливается, когда происходит подключение к одной из домашних сетей, например организованных посредством Windows 7.

□ **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 подразумевает подключение компьютера к случайной или непостоянной сети. Примером такой сети может стать 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 выполняется подключение компьютера к сети с доменом.

Смену сетевого размещения можно производить самостоятельно либо оставить этот выбор на усмотрение операционной системы.

Если требуется изменить сетевое размещение, воспользуйтесь для этого окном **Центр управления сетями и общим доступом**, запустить которое можно из **Панели управления** (рис. 30.1).

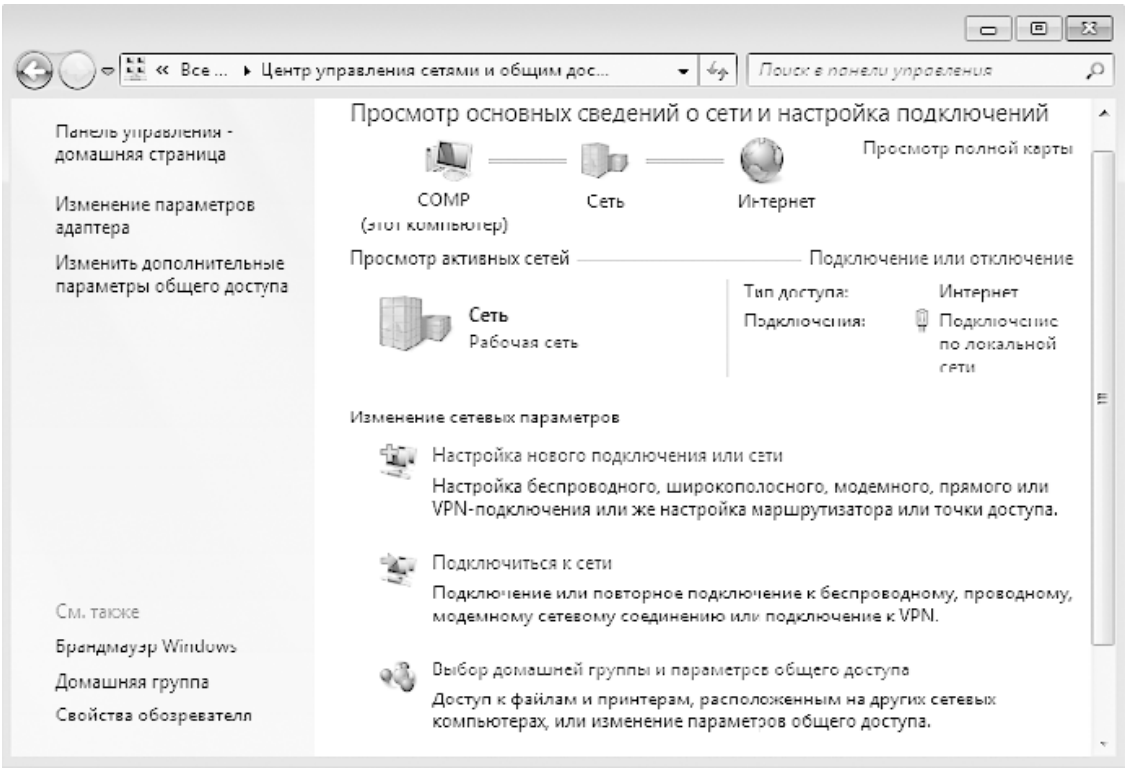

Рис. 30.1. Центр управления сетями и общим доступом в Windows 7

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. 30.2).

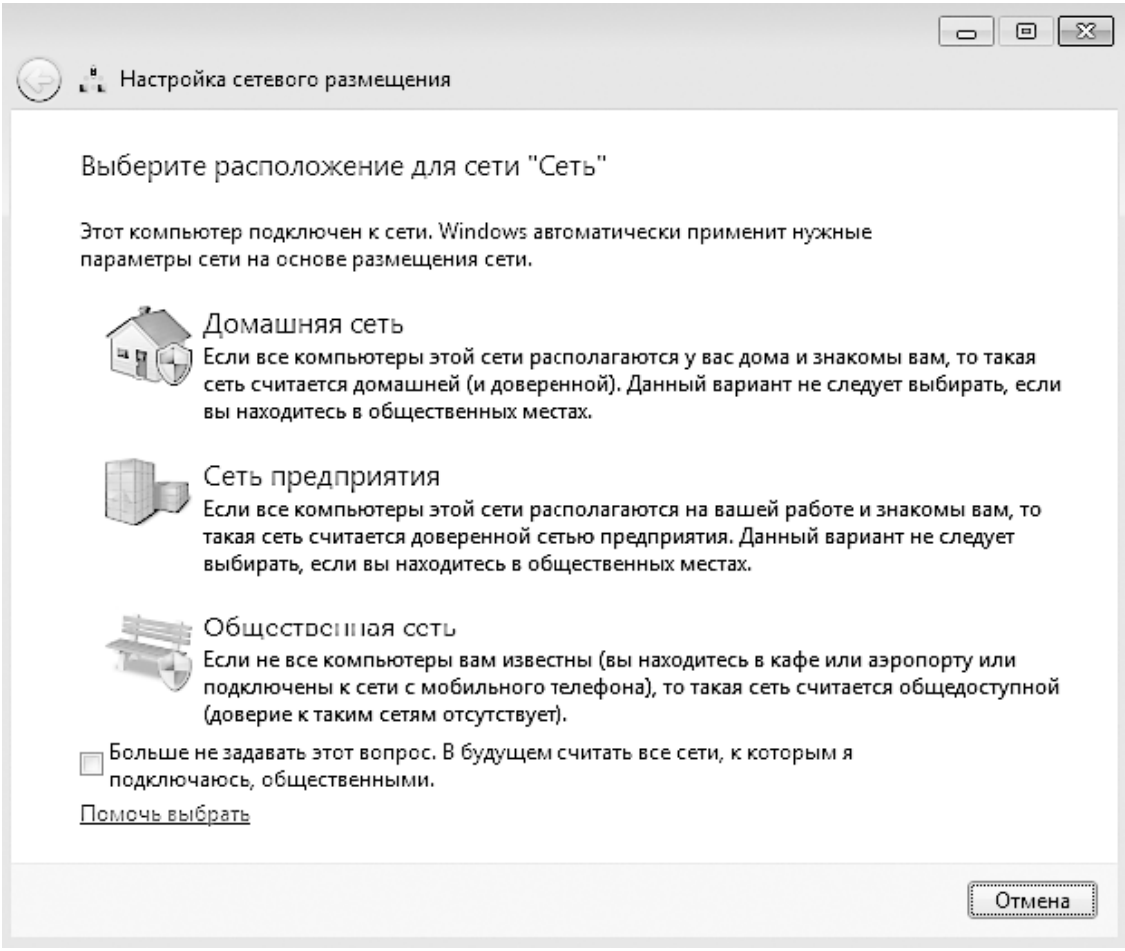

Рис. 30.2. Список доступных сетевых размещений

Чтобы сменить текущее сетевое размещение, достаточно просто щелкнуть на нужном размещении. Например, если вы собираетесь подключиться к рабочей группе 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 будете автоматически изменено на другое.

Смена сетевого размещения происходит достаточно быстро и сопровождается появлением соответствующего окна (рис. 30.3).

После этого 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.

Подключение к рабочей группе

Подключение компьютера с Windows 7 к рабочей группе происходит по тому же алгоритму, что и в Windows Vista, и это неудивительно, поскольку б**о**льшую часть механизмов работы с локальной сетью Windows 7 взяла именно у Windows Vista.

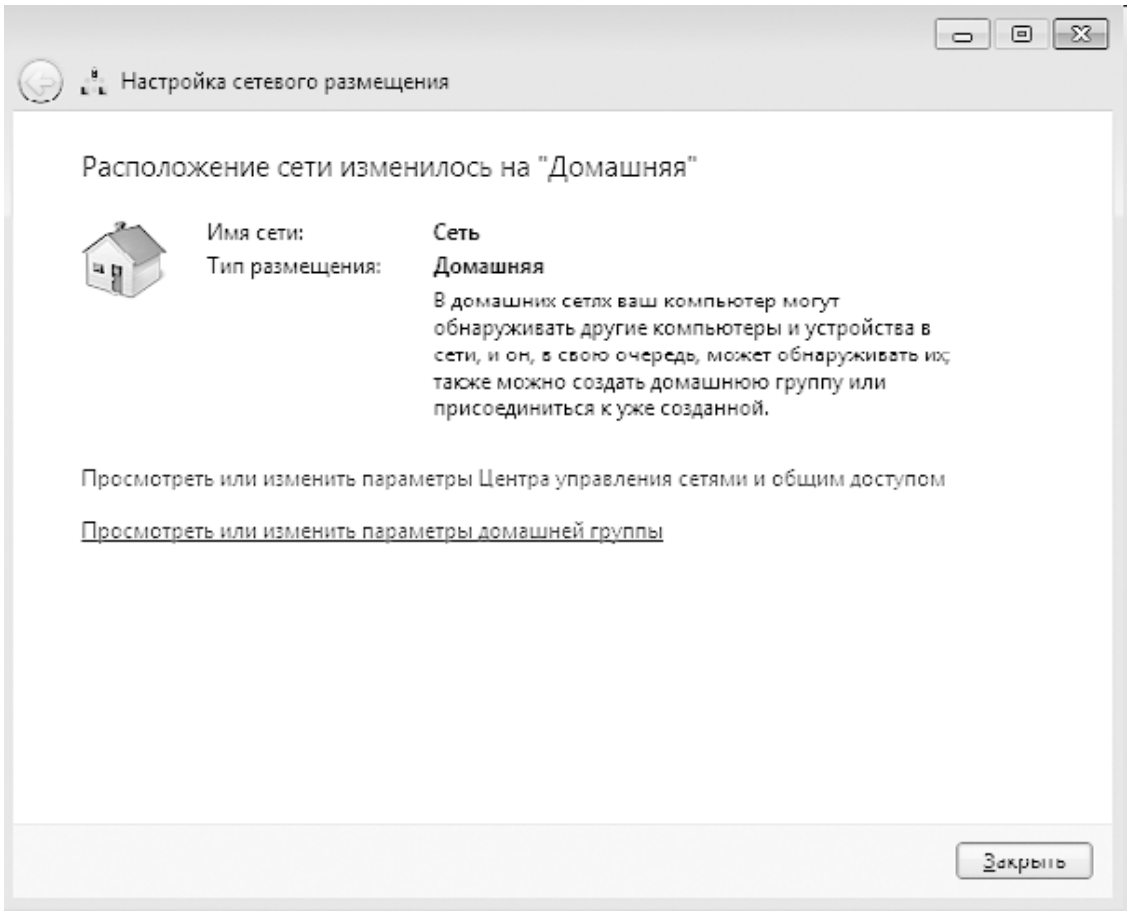

Рис. 30.3. Сетевое размещение изменено

Для начала необходимо открыть механизм **Система**, запустить который можно с **Панели управления**. В результате появится окно, показанное на рис. 30.4.

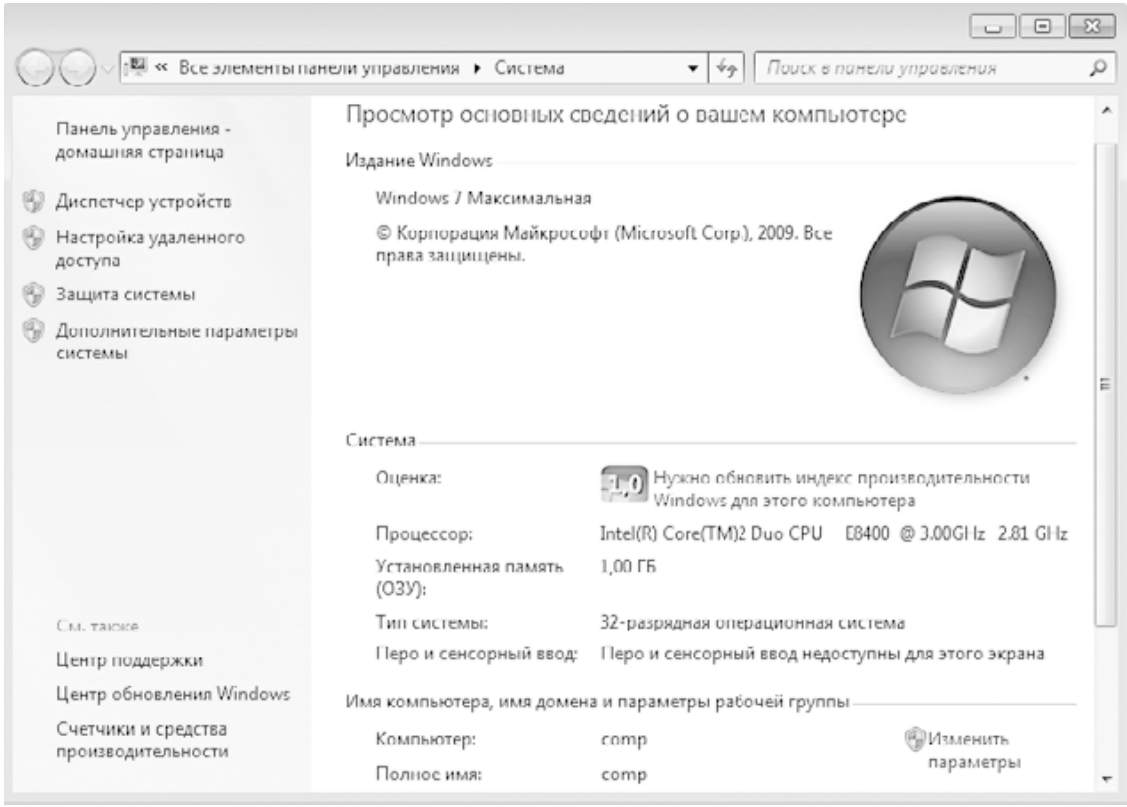

Рис. 30.4. Механизм Система

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. 30.5).

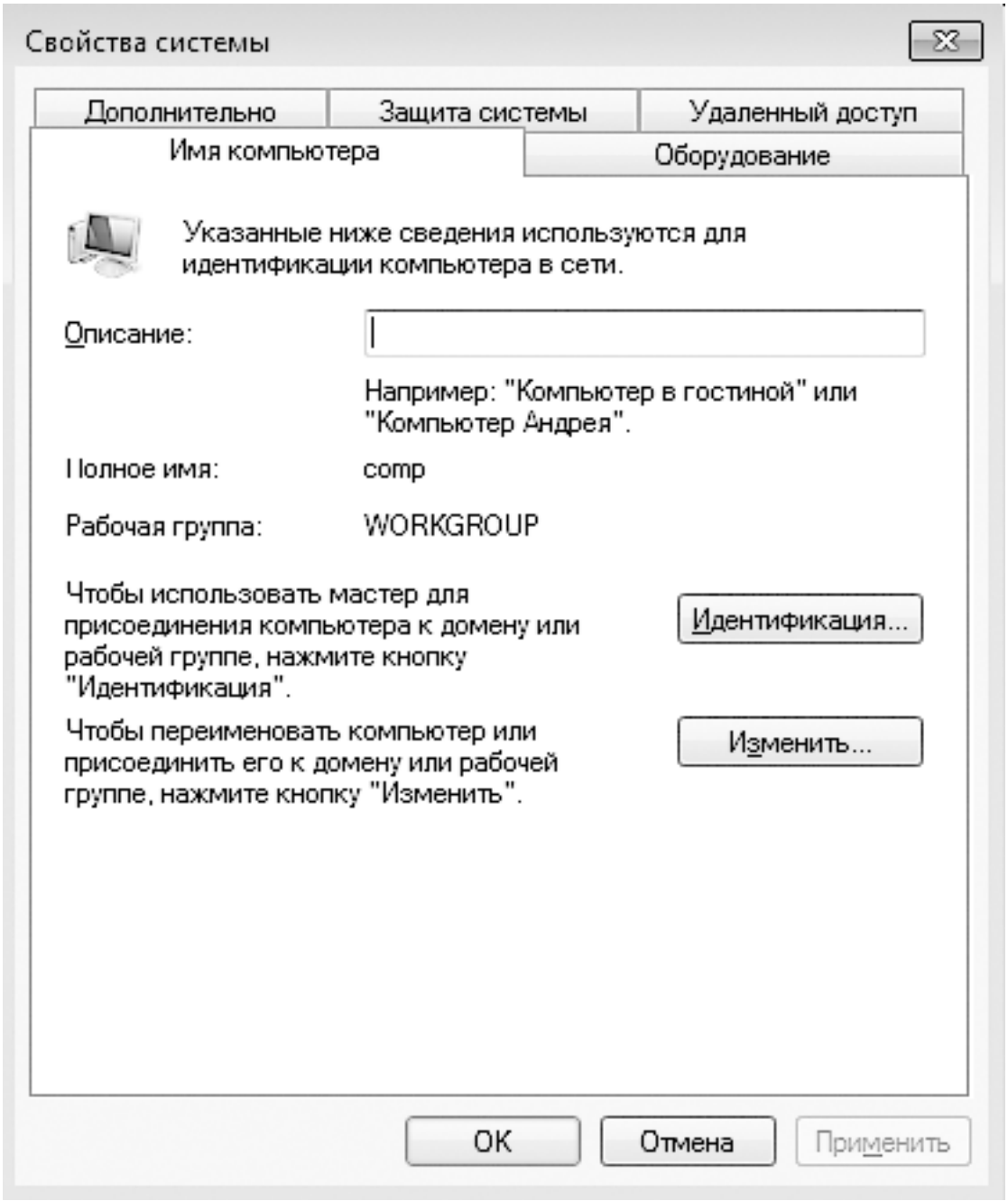

Рис. 30.5. Сведения, идентифицирующие компьютер в сети

В появившемся окне отображается 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. 30.6.

Чтобы подключить компьютер к нужной рабочей группе, достаточно просто ввести ее название в соответствующее поле и нажать кнопку **OK**. Никакой авторизации при этом

не требуется, поскольку сам принцип организации работы рабочей группы подразумевает свободное членство в группе.

Буквально через несколько секунд появится окно с подтверждение того, что компьютер подключен к рабочей группе. Вам остается только перезагрузить компьютер, чтобы начать полноценную работу уже в составе этой рабочей группы.

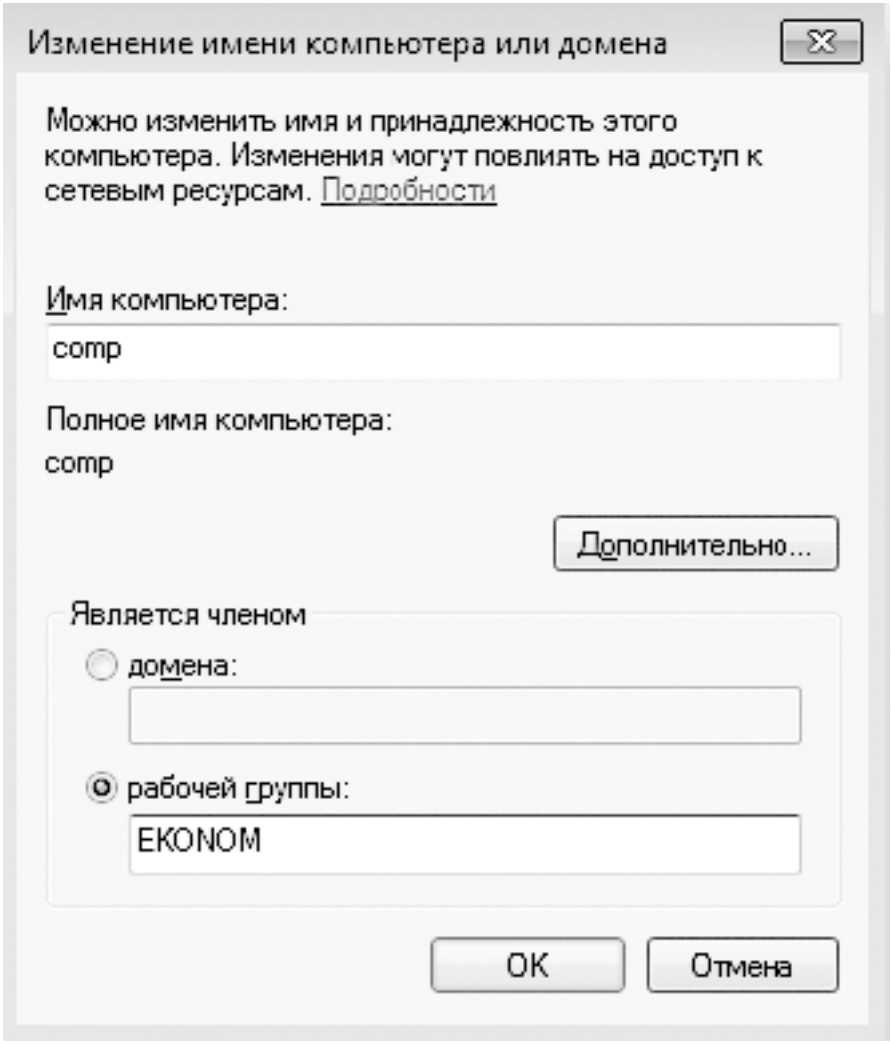

Рис. 30.6. Задание названия рабочей группы

Подключение к домену

Подключение к домену компьютера с операционной системой Windows 7, как и в других операционных системах, требует определенных прав доступа (точнее, прав на подключение компьютера к домену). Кроме того, потребуются данные об учетной записи пользователя, который будет работать на этом компьютере. В этом нет ничего странного, поскольку уровень безопасности в доменной сети подразумевает максимально возможную защиту как вашего компьютера, так и управляющего сервера, который организует работу сети.

Подключение к домену начнем с окна, показанного на рис. 30.5. Нажмите в нем кнопку **Идентификация**. Процесс подключения к домену, а также добавления сетевого пользователя контролирует мастер подключений, работа которого и начинается после нажатия этой кнопки (рис. 30.7).

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 действий. Выбор очевиден, поэтому, установив переключатель в положение с упоминанием корпоративной сети, продолжаем работу мастера.

В следующем окне (рис. 30.8) вам предстоит ответить на вполне очевидный вопрос, от которого зависят дальнейшие действия мастера.

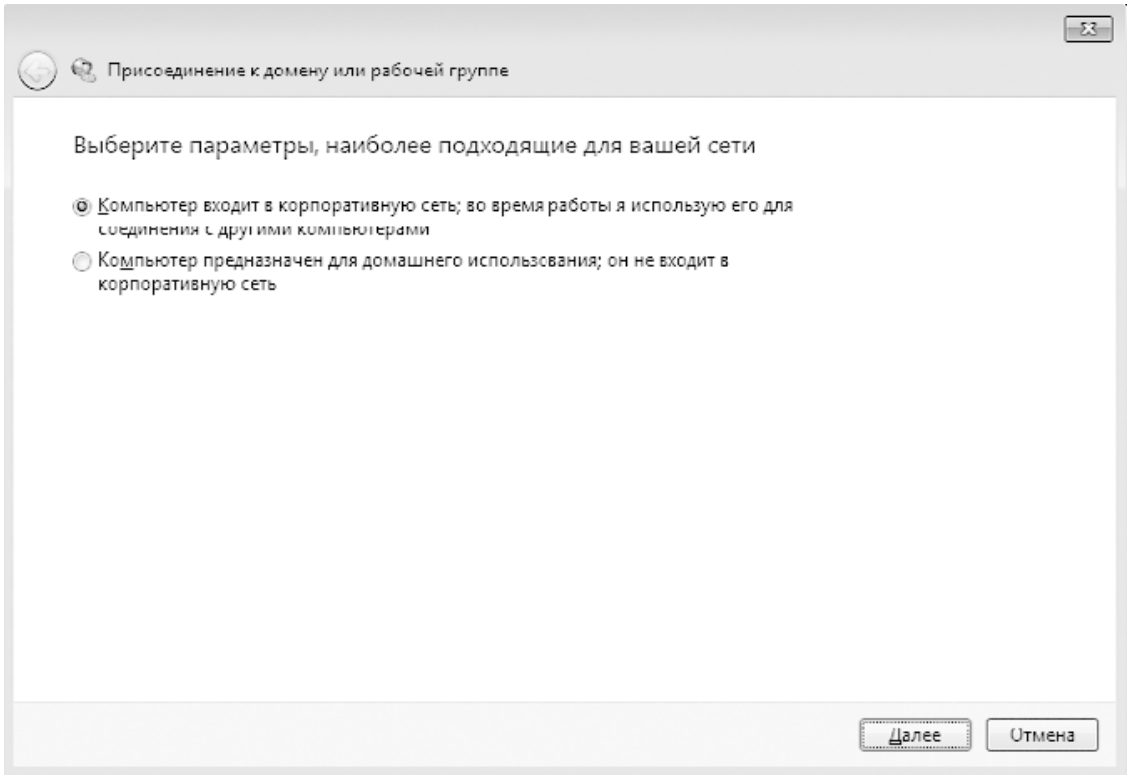

Рис. 30.7. Выбор типа подключения

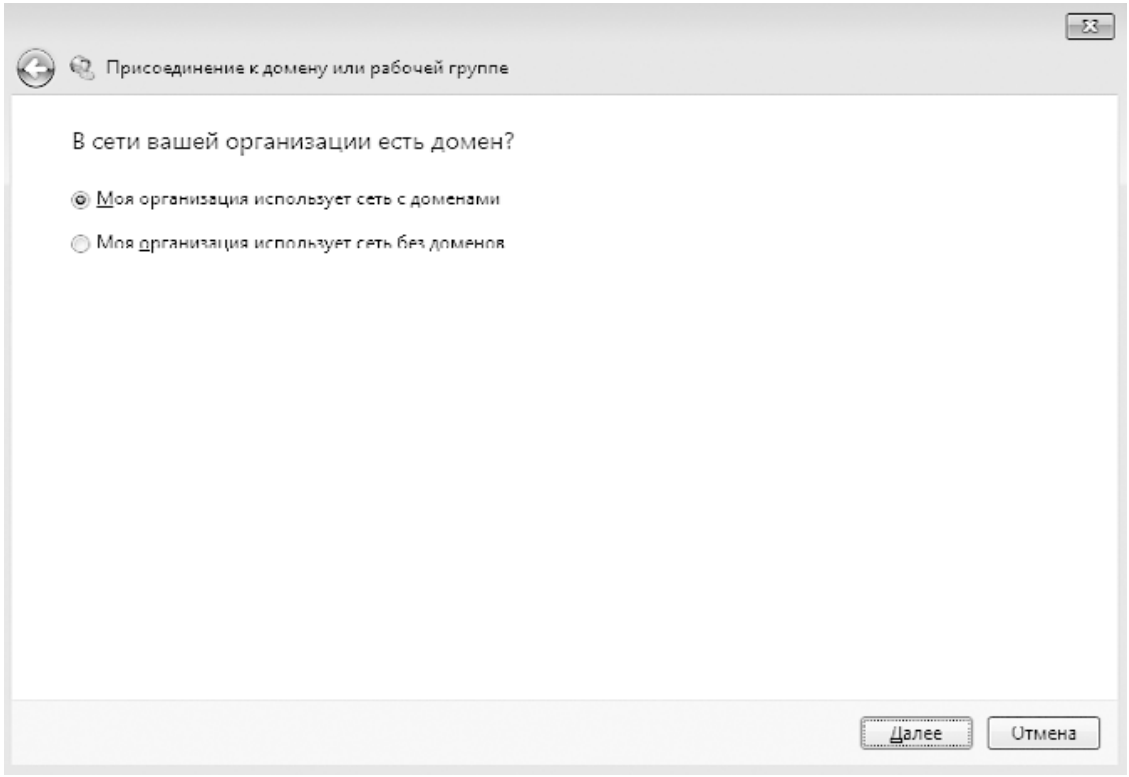

Рис. 30.8. Ответ на следующий вопрос мастера

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. 30.9), вам потребуется ввести запрашиваемые данные, чтобы продолжить работу мастера. При этом следует учитывать, что учетная запись пользователя уже должна быть зарегистрирована в Active Directory, иначе подключение будет невозможно.

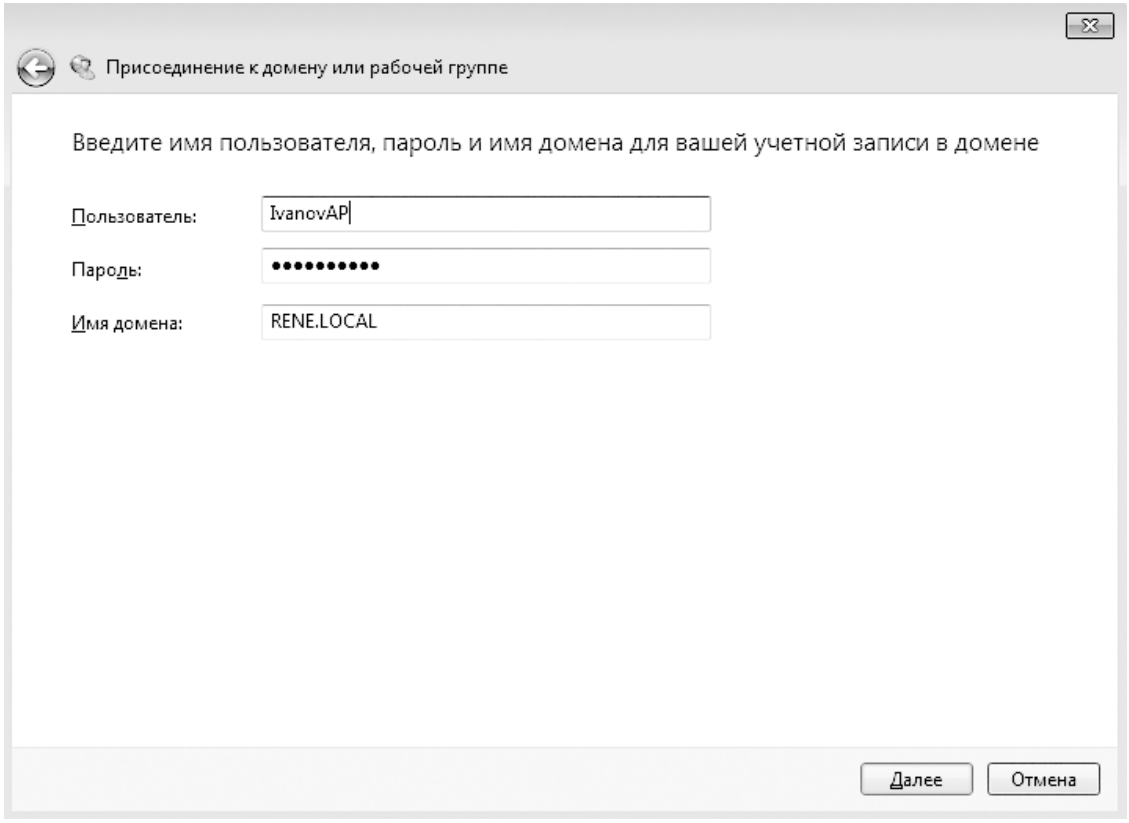

Рис. 30.9. Ввод учетных данных пользователя и имени домена

Если ранее с этого компьютера выполнялось подключение к домену, то информация об этом останется. Это приведет к появлению соответствующего сообщения с предложением использовать ее для регистрации компьютера. Если же подключение производится впервые, то вы увидите окно, показанное на рис. 30.10.

Здесь нужно указать имя компьютера и имя домена, чтобы можно было зарегистрировать компьютер в домене. После нажатия кнопки **Далее** вам необходимо будет пройти авторизацию, указав при этом учетные данные пользователя с правами присоединения к домену.

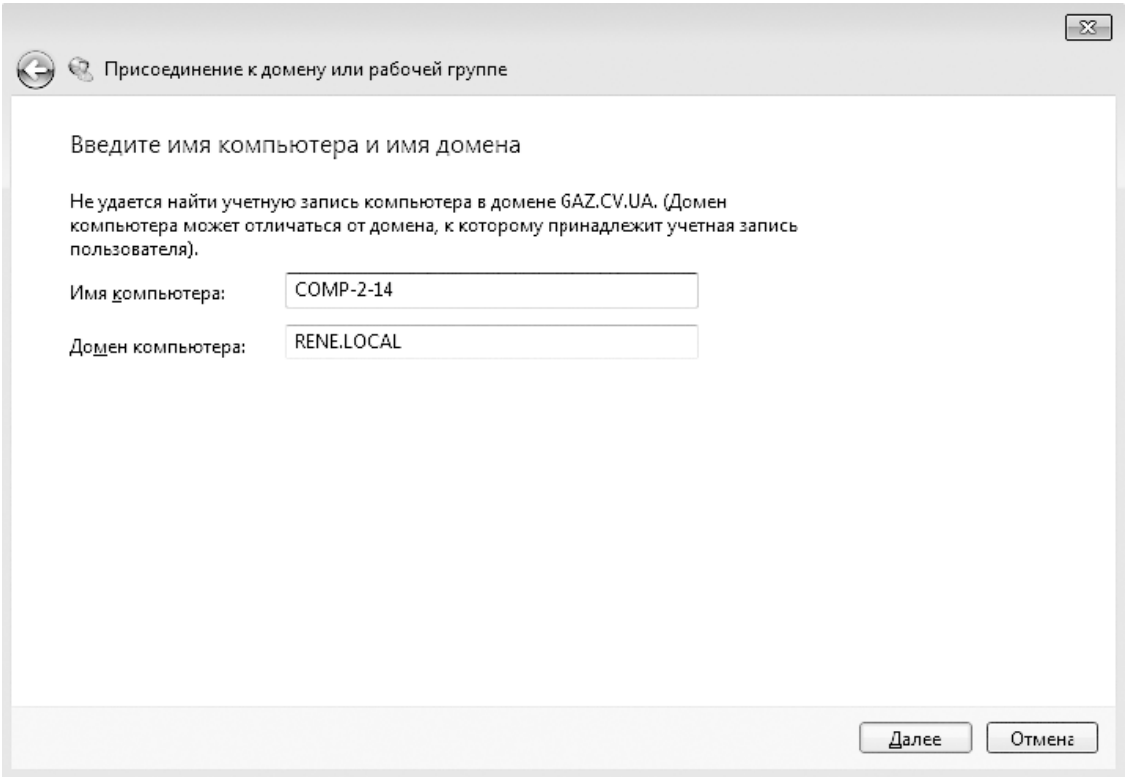

Рис. 30.10. Ввод имени компьютера для регистрации в домене

Если авторизация будет успешной, появится окно, сообщающее, что для завершения процесса подключения требуется перезагрузка компьютера. В противном случае необходимо будет уточнить данные авторизации либо отказаться от подключения к домену.

Настройка TCP/IP-протокола

Настройка параметров TCP/IP-протокола требуется в том случае, когда необходимо изменить способ IP-адресации, а также уточнить IP-адреса DNS-серверов и добавить маршруты. Изменить настройки протокола очень просто, и, что самое главное, это можно сделать «на ходу», то есть без перезагрузки компьютера.

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. 30.1) находится несколько ссылок, позволяющих получить доступ к разным функциям. В частности, чтобы получить доступ к настройкам сетевого адаптера, необходимо использовать ссылку **Изменение параметров адаптера**. При ее нажатии откроется окно, содержащее список всех сетевых подключений, которые используются на компьютере (рис. 30.11).

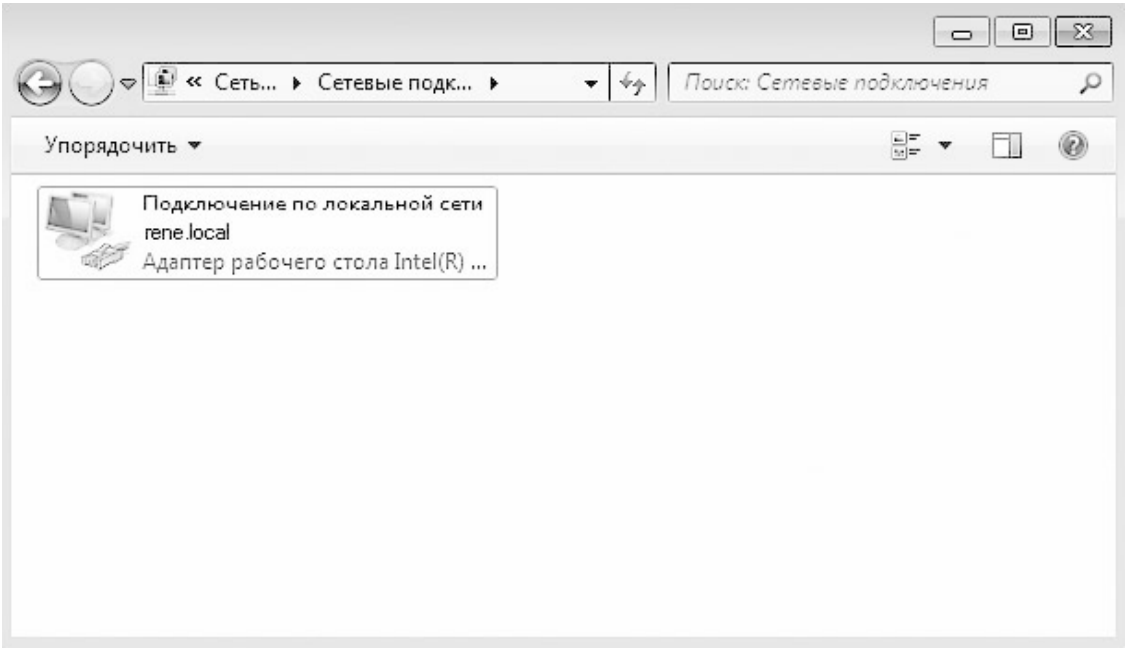

Рис. 30.11. Список сетевых подключений

Их количество зависит от количества установленных сетевых адаптеров, а также программно эмулируемых адаптеров. 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. 30.12).

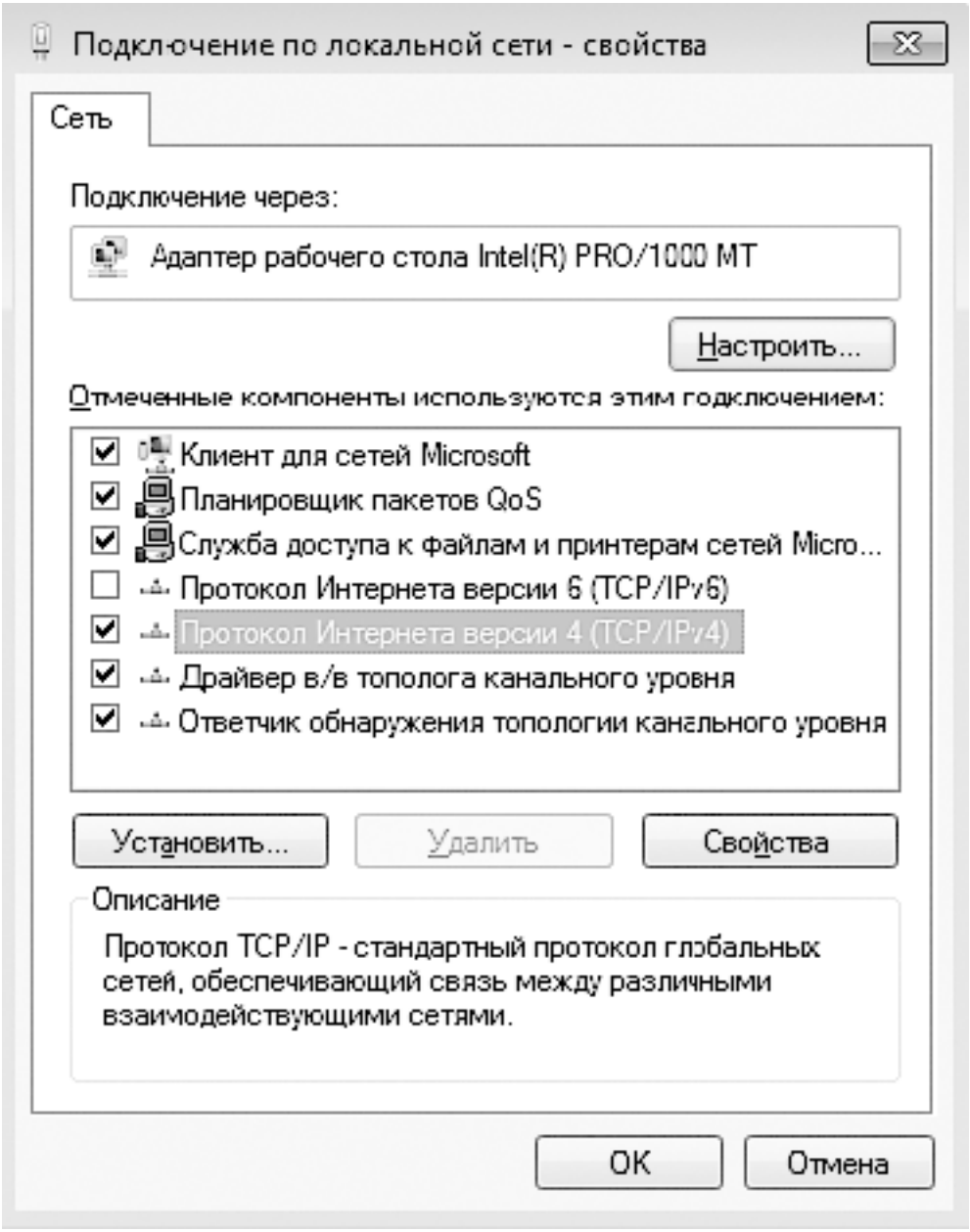

Рис. 30.12. Свойства сетевого подключения

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. 30.13).

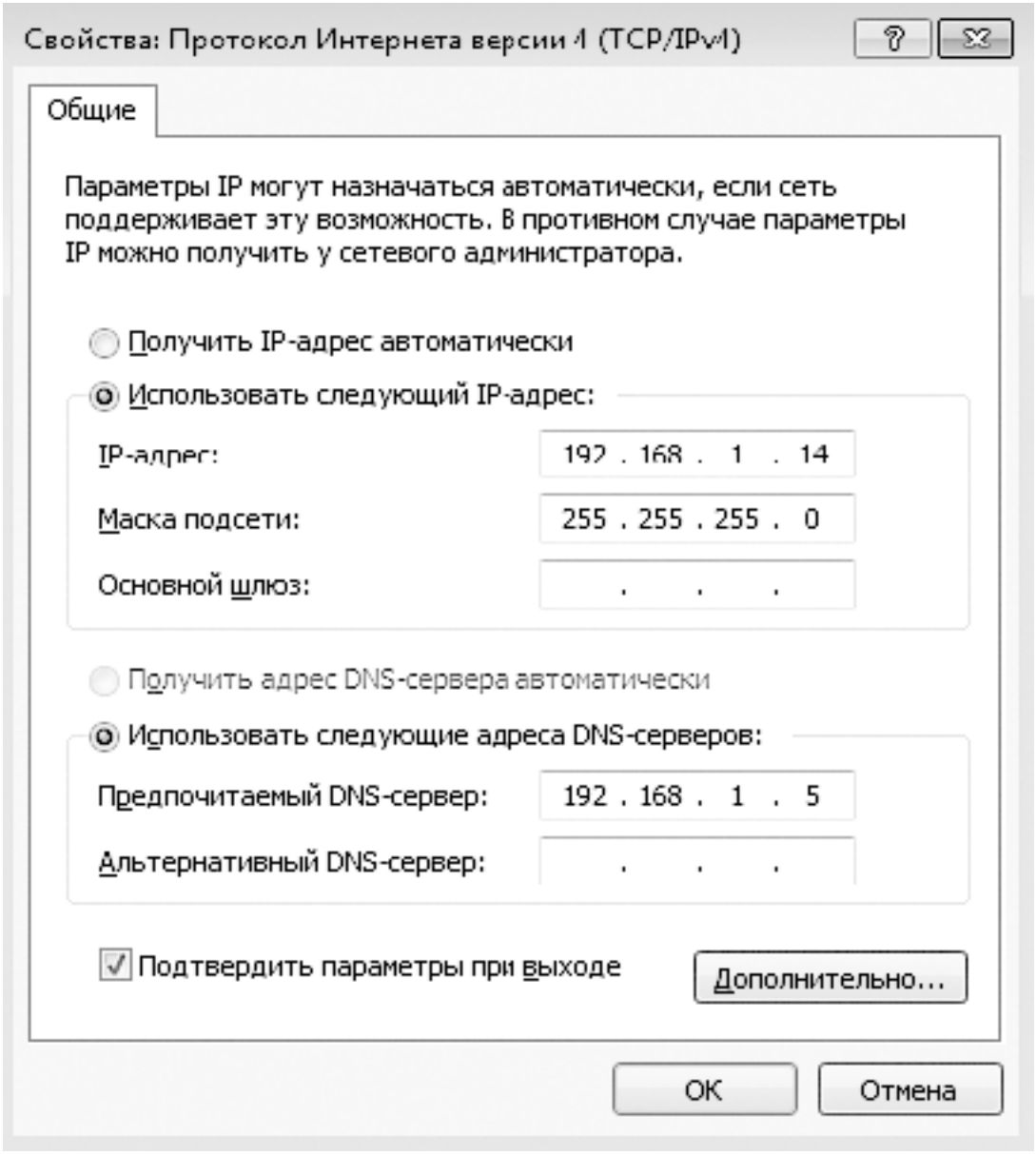

Рис. 30.13. Настройки протокола

Здесь вы можете вносить все необходимые изменения, но главное – не ошибитесь, поскольку от этого зависит, будет ли компьютер виден в сети.