Д. Н. Колисниченко
Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание — СПб.: Наука и Техника, 2004. — 400 с.: ил.

Серия «Просто о сложном»

Данная книга является превосходным практическим руководством по созданию и обслуживанию компьютерных сетей. С ее помощью вы узнаете, как спроектировать и настроить сеть в зависимости от своих задач и возможностей, какое оборудование использовать, какие программы применять. Для этого в книге все есть: от монтажа сети и конфигурирования сетевой карты до настройки сервера сети и организации общего подключения локальной сети к Интернету. Доступно и «со знанием дела» описываются все основные сетевые сервисы: DHCP, DNS, WINS, Active Directory и другие, указывается, зачем они нужны и что делают.

Автор обладает огромным опытом создания и сопровождения сетей, а потому не понаслышке знаком со всеми особенностями этого процесса. Своим опытом он делится с вами и рассматривает множество «жизненных ситуаций». Например, вы узнаете, как настроить сеть, чтобы в ней одновременно работали и Windows-машины и Linux-машины, выясните, как организовать доступ к локальной сети (офиса) из удаленного места (дома), а также много другого. Наконец, вы научитесь выявлять и решать возникающие проблемы.

Книга написана простым и доступным языком. Предназначена начинающим сетевым администраторам, а также всем, кто хочет знать, как настраивается компьютерная сеть.

Содержание

Часть I

ВВЕДЕНИЕ В СЕТИ

Глава 1

Сети: основные сведения

1.1. Что и зачем нужно знать прежде, чем начать настраивать сеть

В этой главе мы с вами ознакомимся с основными понятиями и теоретическими сведениями, относящимися к сетям. Как известно, практике должно предшествовать хотя бы минимум теории. Так вот, этот минимум и будет изложен далее в данной главе. Можно ли без него обойтись — наверное можно, но только до определенного уровня. Рано или поздно вам придется решать какие-то проблемы, оптимизировать сеть при настройке и т.п. Не обладая же хотя бы базовым набором сведений о сетевых технологиях, вы себя будете чувствовать абсолютно беспомощными и не сможете ничего предпринять.

В общем, если не терпится — можете сразу переходить к следующим главам, в которых начинается непосредственное описание методики прокладки сети. В случае необходимости вы потом сможете вернуться к данной главе и восполнить недостаток необходимых сведений. Однако, я бы порекомендовал сначала ознакомиться с ними, а потом уже двигаться дальше.

Пусть вам поначалу будет казаться, что вы без тех или иных сведений можете прекрасно обойтись, но вы все равно прочитайте данную главу от начала до конца. Во-первых, вы еще не знаете, что вам пригодится и зачем. Во-вторых, возвращаясь впоследствии к данному теоретическому материалу, вы сможете быстро и уверенно в нем ориентироваться (если что-то забудете). Ну и в-третьих, данная глава является небольшой и долго «мучиться» с теорией вам не придется.

1.2. Что такое компьютерная сеть?

Итак, что мы будем считать сетью? Сеть — это совокупность компьютеров и других сетевых устройств, объединенных между собой средой передачи данных и коммуникационным оборудованием. Это общее определение. При этом в качестве среды передачи могут использовать как провода и кабели различного типа (проводные технологии), так и радиоэфир (беспроводные технологии).

В то же время, в современную компьютерную сеть могут входить не только компьютеры, но и всевозможные другие электрические приборы. Это могут быть сетевой принтер, телевизор и множество всевозможных бытовых приборов. В ближайшем будущем вообще планируется сетевое объединение всех бытовых приборов (через сеть Интернет). Например, уже сейчас существуют прототипы холодильников, которые автоматически заказывают по сети в магазинах различные продукты, когда те подходят к концу. Как говорится: «Вот до чего техника дошла».

1.3. Классификации сетей

1.3.1. По степени географического распространения (LAN, MAN и WAN)

Существует много классификаций сетей. Одной из них является территориальная. Согласно этой классификации, сети бывают трех видов:

- **Локальные** (Local Area Network, NAL) — это относительно небольшие сети масштаба предприятия, дома, офиса и т.п.
- **Муниципальные** (Metropolitan Area Network, MAN) — сети масштаба города.
- **Глобальные** (Wide Area Network, WAN) — сети, охватывающие значительное географическое пространство — регион, страну, континент.

Ясное дело, что для нас основным видом будут локальные сети, хотя мы будем рассматривать и их интеграцию с глобальной сетью Internet.

1.3.2. Одноранговые сети и сети клиент/сервер (иерархические сети)

Существуют две основные архитектуры сети:

- **одноранговая сеть** (peer-to-peer);
- **сеть клиент/сервер** (client/server) или ее еще называют иерархической сетью.

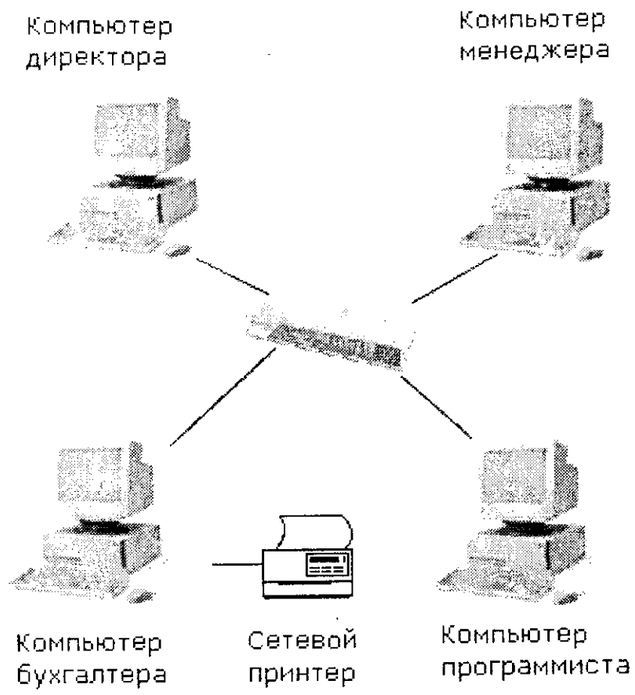


Рис. 1.1. *Локальная сеть*

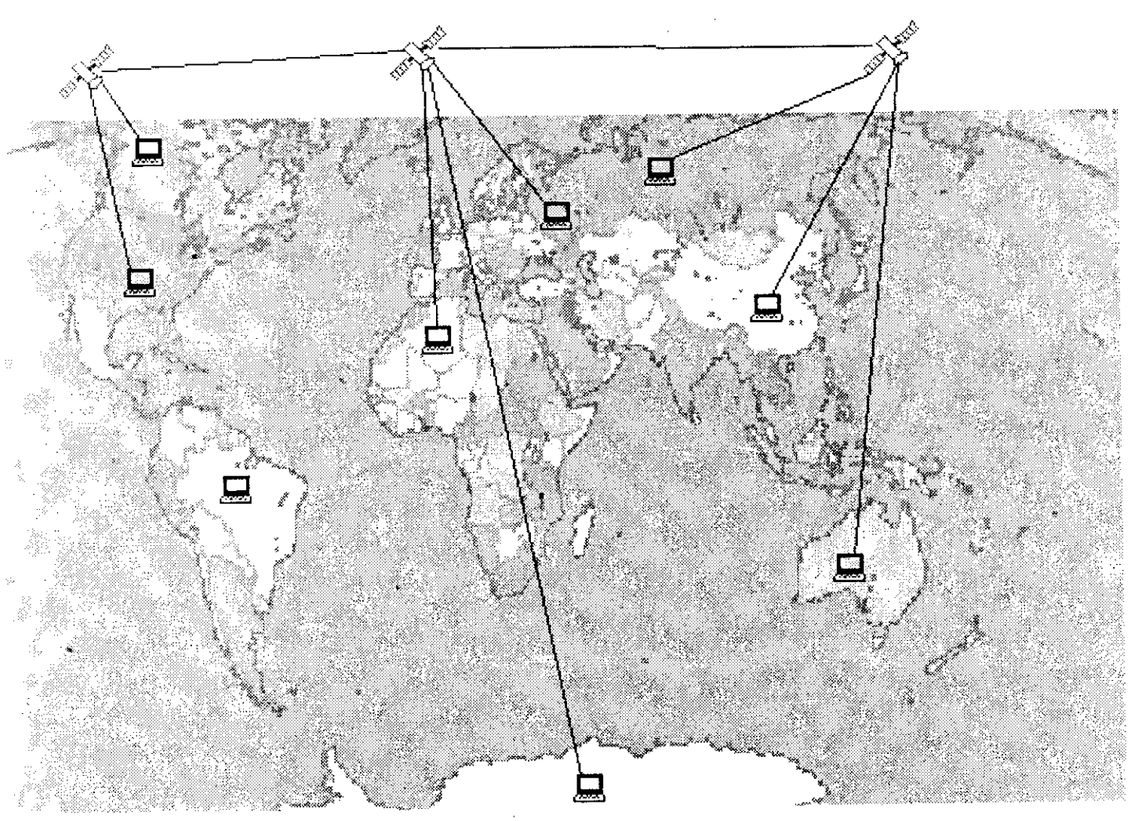


Рис. 1.2. *Глобальная сеть*

Причем вторая практически вытеснила первую. В одноранговой сети все компьютеры равны — имеют один ранг. Любой компьютер может выступать как в роли сервера, то есть предоставлять свои ресурсы (файлы, принтеры) другому компьютеру, так и в роли клиента, другими словами — использовать предоставленные ему ресурсы.

Одноранговые сети

Одноранговые сети преимущественно распространены в домашних сетях или небольших офисах. В самом простом случае для организации такой сети нужно всего лишь пара компьютеров, снабженных сетевыми платами, и коаксиальный кабель (нужна еще пара терминаторов (заглушек), но пока сильно углубляться в детали не будем).

Когда сеть создана физически (компьютеры связаны с помощью коаксиального кабеля), нужно настроить сеть программно. Для этого необходимо, чтобы на компьютерах были установлены сетевые операционные системы (Linux, FreeBSD, Windows NT, Windows 98) или сетевые системы с поддержкой сетевых функций (Windows 95, Windows for Workgroups).

Компьютеры в одноранговой сети объединяются в **рабочие группы**. Каждая рабочая группа имеет свой идентификатор — имя рабочей группы. Если вы сейчас работаете в Windows 9x, узнать имя рабочей группы можете, запустив апплет **Сеть** с **Панели управления** (см. рис. 1.3).

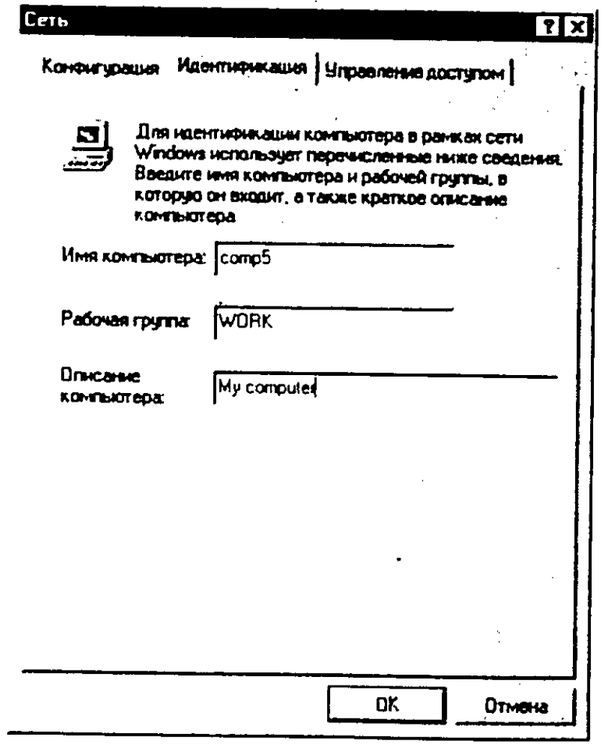


Рис. 1.3. *Идентификатор рабочей группы в ОС Windows 9x*

Для примера допустим, что в вашей одноранговой сети имеется три компьютера A, B, C. Первые два входят в рабочую группу WG1, а компьютер C — в рабочую группу WG2 (см. рис. 1.4).

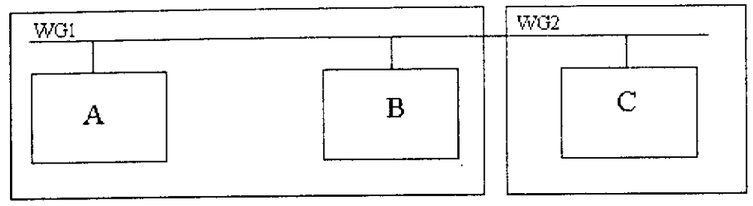


Рис. 1.4. *Схема одноранговой сети*

Даже несмотря на то, что компьютеры входят в один сегмент сети (физически подключены к одному кабелю), компьютеры A и B не будут «видеть» компьютер C, а компьютер C не будет видеть компьютеры A и B. Если выполнить команду поиска компьютера в Windows 9x (**Пуск → Поиск → Найти компьютер**), компьютер «увидит» компьютеры A и B, но будет сообщено, что они находятся в другой рабочей группе — WG1.

Единственное ограничение доступа, которое возможно в одноранговой сети, это использование пароля для доступа к какому-нибудь ресурсу. Для того, чтобы получить доступ к этому ресурсу, например, принтеру, нужно знать пароль. Это называется управлением доступом на уровне ресурсов. В сети клиент/сервер используется другой способ управления доступом — на уровне пользователей. В этом случае можно разрешить доступ к ресурсу только определенным пользователям.

Например, ваш компьютер A через сеть могут использовать два пользователя: Иванов и Петров. К этому компьютеру подключен принтер, который можно использовать по сети. Но вы не хотите, чтобы кто угодно печатал на вашем принтере, и установили пароль для доступа к этому ресурсу. Если у вас одноранговая сеть, то любой, кто узнает этот пароль, сможет использовать ваш принтер. В случае с сетью клиент/сервер вы можете разрешить использовать ваш принтер только Иванову или только Петрову (можно и обоим).

Сети клиент/сервер

Для получения доступа к ресурсу в сети клиент/сервер пользователь должен ввести свой уникальный идентификатор — имя пользователя (login — логин) и пароль (password). Логин пользователя является общедоступной информацией и это правильно: возможно, если кто-нибудь захочет отправить пользователю сообщение по электронной почте, то для этого ему достаточно знать его логин (естественно, и имя сервера электронной почты, который «знает» этого пользователя).

Использование логина и пароля для доступа к ресурсам называется идентификацией. Подтверждение (проверка подлинности) имени пользователя паролем — аутентификацией. Идентификация + аутентификация = авторизация. Иногда понятие аутентификация просто воспринимается как проверка подлинности в широком смысле слова.

После рассмотрения архитектуры одноранговой сети можно прийти к выводу, что единственное преимущество этой архитектуры — это ее простота и дешевизна. Сети клиент/сервер обеспечивают более высокий уровень производительности и безопасности.

В отличие от одноранговой сети, в сети клиент/сервер существует один или несколько главных компьютеров — серверов. Все остальные компьютеры сети называются клиентами или рабочими станциями (workstations). Как я уже писал выше, ***сервер* — это специальный компьютер, который предоставляет определенные услуги другим компьютерам.** Существуют различные виды серверов (в зависимости от предоставляемых ими услуг): серверы баз данных, файловые серверы, серверы печати (принт-серверы), почтовые серверы, Web-серверы и т.д.

Для экономии средств, как правило, один сервер сочетает в себе функции нескольких серверов, например, почтовик может быть также и Web-сервером. Услуги, которые может предоставлять сервер, ограничиваются только его физическими возможностями — чем мощнее сервер, тем больше услуг и с большим качеством он может предоставлять, поэтому в качестве сервера выбирается довольно мощный компьютер. Хотя системные требования к серверу во многом зависят от системных требований операционной системы. Если вам нужен почтовик и маршутизатор на одном компьютере, при использовании Windows 2000 Server будьте готовы приобрести компьютер не ниже Intel Celeron 500...700 MHz/256...512 Мб памяти, а при использовании Linux вполне хватит старенького Intel Pentium 133/128 Мб ОЗУ.

1.4. Какое основное оборудование применяется для построения сетей

Давайте уже в самом начале книги определимся с основными устройствами, которые применяются для создания сетей — с так называемым коммуникационным оборудованием. В дальнейшем мы каждое из них рассмотрим более подробно, когда будем располагать большей информацией о механизме сетевого взаимодействия.

Сейчас же лишь кратко остановимся на том, что это за устройства, для чего они нужны и что они делают. Совсем не обязательно они будут все присутствовать в вашей сети, но определить нужны они вам или нет вы сможете только обладая информацией о них.

Кабель

Как правило, сети (особенно локальные) создаются на основе проводных технологий, то есть устройства соединяются с помощью кабеля. При этом используются различные виды кабеля различной категории. Какой кабель использовать — зависит от технологии, по которой строится сеть. Ну а технология выбирается исходя из необходимой пропускной способности сети и финансовых возможностей. Чем больше пропускная способность — тем лучше (данные передаваться будут быстрее), но и тем дороже.

В дальнейшем, при рассмотрении различных технологий, мы узнаем для какого варианта какой кабель необходим. Но уже сейчас можно сказать, что основным стандартом, по которому строятся сейчас локальные сети, является стандарт Fast Ethernet с пропускной способностью 100 Мбит/с. Для этой сети используется кабель типа «витая пара» пятой категории.

Что такое концентратор (хаб) и зачем он нужен

Первым среди устройств следует отметить **концентратор** (или хаб — от англ. hub). Концентратор — это устройство, к которому подключаются сетевые устройства (компьютеры), и, таким образом, через него осуществляют взаимодействие друг с другом. В зависимости от модели разные концентраторы обладают разным количеством портов и, соответственно, позволяют подключать и объединять в сеть разное количество сетевых устройств.

Когда какому-либо компьютеру в сети необходимо передать что-либо другому компьютеру, он посылает данные концентратору, а тот передает полученные данные во все свои порты, независимо от адресата. Таким образом, все устройства, подключенные к концентратору, будут «видеть» передаваемые данные, даже если те для них не предназначены. Просто все устройства будут игнорировать эти данные, кроме устройства, которому они предназначены.

Если компьютеров (сетевых устройств) много, для их объединения можно использовать несколько концентраторов, соединенных между собой.

У концентраторов есть существенный недостаток — они работают в широковещательном режиме, то есть данные, передаваемые от одного компьютера к другому, передаются всем сразу. Помимо вопросов безопасности загвоздка еще заключается в том, что при использовании большого количества компьютеров сеть может быть перегружена излишним количеством данных. Ведь от одного компьютера концентратор передает данные всем остальным, от второго передает всем остальным, от третьего и т.д. Таким образом в сети ходит очень много ненужных данных,

которые большинством компьютеров игнорируются (кроме адресата) и при этом еще перегружают сеть.

Решить эту проблему позволяют коммутаторы. Однако, наряду с минусом, концентраторы по сравнения с коммутаторами обладают и плюсами. Во-первых, они дешевле (сейчас разница в цене незначительна), а во-вторых, не требуют, в отличие от коммутаторов, никакой настройки. Кроме того, на сегодняшний день пропускная способность сети достаточно велика и излишние данные не производят перегрузки (если, конечно, не используется огромное количество компьютеров).

Коммутатор (switch)

Коммутатор по своим функциям представляет собой концентратор, который пересылает поступившие от одного компьютера данные не всем остальным компьютерам, а только адресату. Благодаря этому, помимо повышения безопасности, снижается нагрузка на сеть.

Нужно сказать пару слов о выборе коммутатора. Раньше основным камнем преткновения для использования коммутаторов была их высокая стоимость. Сейчас можно купить довольно производительные коммутаторы за относительно небольшие деньги. Для своей домашней сети я купил восьмипортовый коммутатор всего за 22 долларов (CANYON 10/100 CN-D08PD1). 16-портовый коммутатор от компании Surecom обойдется вам около 80 долларов, а самый простой 24-портовый от Lantech — чуть более 90 долларов.

Это страшное слово — маршрутизатор

Довольно часто несколько сетей соединяются друг с другом. Например, в одном доме есть своя домовая сеть, в другом — своя, а в третьем — своя. Причем третий дом соединен уже еще с несколькими другими домами. Для объединения сетей и оптимизации пересылаемого трафика (пересылаемых данных) предназначены маршрутизаторы.

Маршрутизатор собирает информацию о топологии межсетевых соединений и на основании этой информации целенаправленно пересылает данные из одной сети в другую. Благодаря этому данные между компьютерами, расположенными в разных сетях, передаются по наиболее оптимальному маршруту.

Маршрутизатор может быть как аппаратным, так и программным. Например, функции маршрутизатора может выполнять один из компьютеров сети, с настроенным соответствующим программным обеспечением.

Мост

Мост — это устройство, выполняющее локализацию трафика. Сейчас поясню, что это означает. Представьте, что у нас есть сеть, довольно большая, скажем 100 компьютеров, при пропускной способности сети в 10 Мбит/с. Да, по современным нормам 100 компьютеров — это не так уж и много, но обратите внимание на пропускную способность. Такая сеть будет работать очень медленно, поскольку она постоянно будет перегружена.

Так вот, мост позволяет разбить нашу сеть на логические сегменты, что позволяет существенно снизить нагрузку на сеть. Представим, что мы разбили нашу сеть на два логических сегмента.

В результате у нас есть две более быстрые сети по 50 компьютеров, а не одна неповоротливая на 100. Потом мы с компьютера А отправляем на компьютер Б данные. Если компьютер Б находится в том же сегменте, что и компьютер А, то данные отправляются непосредственно компьютеру Б. Если же компьютер Б находится в другом сегменте, то данные «переходят» через мост.

Повторитель

Повторитель служит для увеличения общей длины сети. Сигнал, проходящий по кабелю, имеет привычку «затухать», то есть, чем дальше сигнал удаляется от источника, тем он более слаб. Практически все сети (точнее стандарты) имеют такую характеристику как «общая длина сети». Затухание сигнала зависит от используемой среды передачи данных, грубо говоря, от используемого кабеля — при использовании одного вида кабеля сигнал «затухает» быстрее, при другом — медленнее.

А случается ведь и такое, что сигнал передается на максимальное для этой сети расстояние, но, «дойдя» до приемника, он становится настолько слаб, что приемник не может его распознать. Тем более, что по дороге из-за затухания сигнал может видоизмениться, то есть произойдет потеря или искажение информации. Тогда где-то между источником и приемником ставится повторитель. Он получает сигнал еще без искажения и попросту его повторяет — усиливает.

Кроме усиления сигнала повторитель может преобразовывать один тип сигнала в другой. Это бывает необходимым, если мы соединяем различные сети друг с другом. На рис. 1.5 изображен повторитель-конвертер сигналов Ethernet 100TX в Ethernet 100 FX.

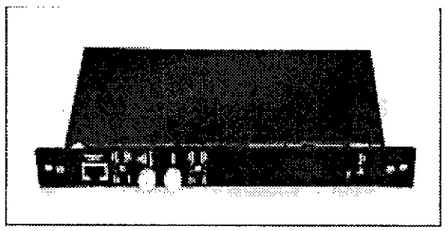


Рис. 1.5. *Повторитель-конвертер сигналов Ethernet 100TX в Ethernet 100 FX производства ЗАО «Русская Телефонная Компания»*

1.5. Какие сервера бывают и для чего они нужны

Для полноты картины рассмотрим несколько различных типов серверов:

1. Сервер локальной сети.
2. Шлюз.
3. Сервер удаленного доступа.

1.5.1. Сервер локальной сети

Сервер локальной сети (рис. 1.6) — это сервер, оказывающий услуги пользователям сети Интранет (Intranet). Не путайте «Интранет» с «Интернет». Сеть Intranet — это внутренняя корпоративная сеть, как правило, без выхода в Интернет. Представьте себе небольшую офисную сеть. Если у вас развито воображение, вы даже можете себе представить большую локальную сеть, размещенную в многоэтажном здании. В такой сети сервер может выполнять самые разнообразные функции, например, быть сервером печати или файловым сервером. Обычно во внутренних сетях серверы выполняют только эти функции. В зависимости от вида деятельности организации, в которой установлен сервер, довольно часто он используется в качестве сервера баз данных.

Если сеть большая, то целесообразно выделить отдельно по серверу для каждого сервиса, например, отдельный файловый сервер и отдельный сервер баз данных. Для сервера баз данных и файлового сервера вообще желательно выделить по одному компьютеру, потому что если нагрузка на сервер баз данных довольно большая, а это в большинстве случаев именно так, то это будет снижать производительность файлового сервера, и наоборот. Если производительность сервера будет низкой, то, как всегда, страдает пользователь. В свою очередь, «страдания» пользователей отразятся ни на ком другом, кроме как на вас — администраторе.

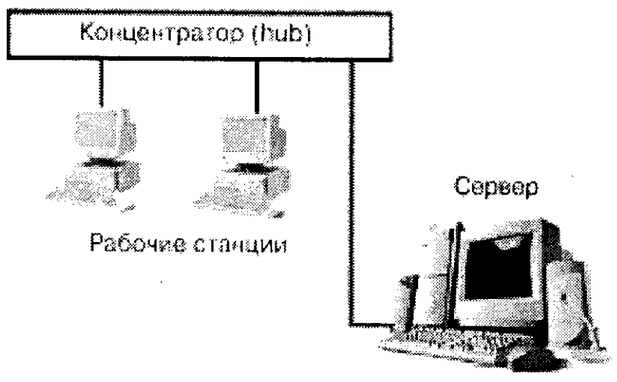


Рис. 1.6. *Сервер локальной сети*

На рис. 1.6 изображена небольшая локальная сеть без выхода в Интернет. Все рабочие станции и сам сервер подключены к центральному устройству сети — концентратору. Вместо концентратора можно использовать (и предпочтительнее использовать) коммутатор (switch). В отличие от коммутатора, концентратор «не знает», к какому порту подключен тот или иной компьютер и когда один из компьютеров передает пакет, то концентратор повторяет этот пакет на все свои порты. Каждый компьютер сети получает этот пакет и проверяет наличие своего IP-адреса в заголовке этого пакета. Если IP-адрес назначения не совпадает с IP-адресом компьютера, который принял этот пакет, то пакет просто игнорируется. Коммутатор же передает пакет только на тот порт, к которому подключен адресат. Благодаря этому, помимо повышения безопасности, снижается нагрузка на сеть.

Вот так пакет доставляется от источника к месту назначения. Кроме концентратора или коммутатора, в большинстве случаев не нужно никакого другого сетевого оборудования, за исключением разве что сетевых плат. В случае большой протяженности сети используются повторители, которые, пропуская через себя сигнал, усиливают его. По своей сути повторитель представляет собой простейший концентратор. Концентратор же, за вычетом некоторых сервисных функций, представляет собой многопортовый повторитель.

1.5.2. Шлюз — сервер для доступа в Интернет

В том случае, если в вашей внутренней сети необходим доступ к Интернет, имеет смысл установить сервер для доступа к всемирной Сети (см. рис. 1.7). Это и есть шлюз. Шлюзом может быть и отдельное устройство, но в локальных сетях с выходом в Интернет обычно устанавливается целый сервер для доступа к Интернет. Это намного удобнее, так как кроме шлюза можно также настроить Web, FTP, SMTP/POP-сервер. В этом случае вы сможете размещать информацию о вашей компании в Интернет и настроить собственный почтовый сервер. Для этих же целей существуют аппаратные преднастроенные решения различных компаний, например, компании Intel. Но возможности администрирования таких устройств довольно ограниченные. Ощутить свободу действий как администратор вы сможете только в случае, когда у вас будет полноценный сервер.

Что же изменилось по сравнению с рис. 1.6? Вы правы, появилась выделенная линия. Обычно подключение сервера (читайте: локальной сети) к Интернет происходит по выделенной линии. В простейшем случае для организации выделенной линии необходим модем, позволяющий работать на выделенных линиях. Я бы порекомендовал использовать ZyXEL U336S. Этот модем поддерживает двух- и четырехпроводные линии, а также синхронную и асинхронную передачу данных. Максимальная скорость передачи 300...480 Кбит/с. Это уже будет считаться рекламой мо-

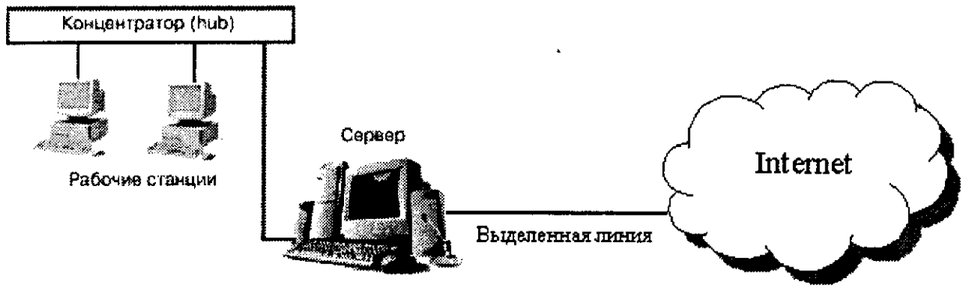


Рис. 1.7. *Сервер для доступа к Интернет (шлюз)*

демов ZyXEL, но я все-таки напишу, что данные модемы работают практически на любых (даже на самых зашумленных) линиях. Конечно, зашумленность выделенной линии вам не грозит, а вот при организации модемного пула, о котором поговорим немного позже, желательно установить все-таки модемы ZyXEL.

В большинстве случаев скорость передачи 300...480 Кбит/с вас не будет устраивать. В этом случае существуют DSL-модемы, обеспечивающие передачу данных со скоростью до 1 Мбит/с. Если позволяют условия расположения вашего офиса, можно купить оборудование Radio Ethernet.

1.5.3. Сервер удаленного доступа

Теперь представьте, что ваша компания немного разрослась и кроме нескольких соседних зданий, соединенных между собой оптоволоконным кабелем, появилось еще несколько филиалов в разных концах города. Нужно обеспечить пользователям удаленных филиалов возможность работать в сети компании. При этом вам не нужно, чтобы эти пользователи находились в сети постоянно. В этой ситуации на сцене появляется сервер удаленного доступа (см. рис. 1.8).

Работа с сервером удаленного доступа выглядит следующим образом. Удаленный пользователь звонит по определенному номеру модемного пула компании. Сервер удаленного доступа аутентифицирует пользователя и предоставляет ему доступ, если аутентификация прошла успешно. При этом удаленному пользователю кажется, что он работает непосредственно в сети компании, если не считать медленного канала передачи данных. Другим (не удаленным) пользователям сети будет казаться, что удаленный пользователь находится где-то рядом — в этом же здании.

Однако, если нужно обеспечить постоянную работу удаленных пользователей в сети компании, то для этого существуют более эффективные решения, например, технология Radio Ethernet.

Обратите внимание, что в сети появилось новое устройство — модемный пул. Это просто совокупность модемов, подключенных к серверу.

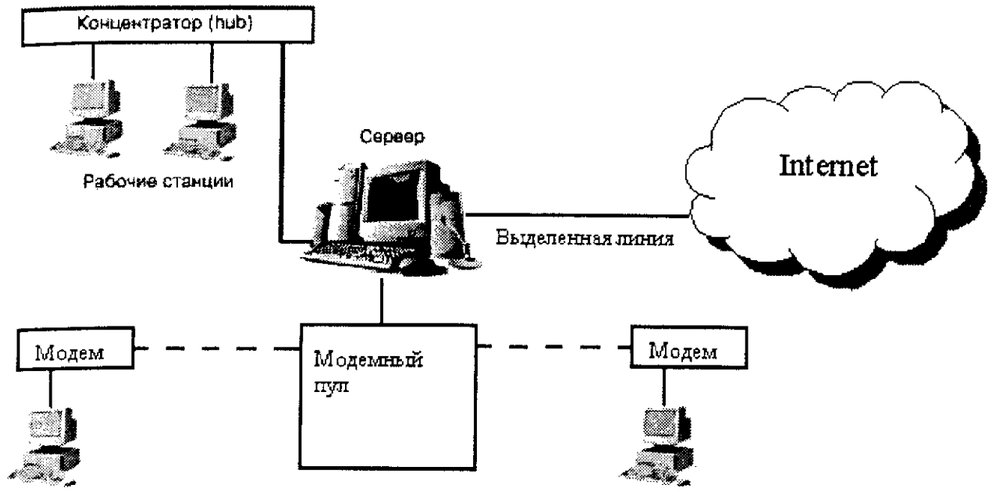


Рис. 1.8. *Сервер удаленного доступа*

Обычно все эти модемы устанавливаются в специальные стойки, но это не обязательное требование — просто ради удобства.

У вас может возникнуть вопрос: как все эти модемы подключаются к серверу, если максимально можно подключить четыре последовательных устройства (а без установки дополнительных контроллеров — только два)? Для этого используется мультипортовая плата, которая обеспечивает подключение большого количества модемов (и других устройств), подключаемых к последовательному порту компьютера. При этом все модемы подключаются к мультипортовой плате, а она, в свою очередь, к компьютеру.

Пунктирной линией на рис. 1.8 обозначено непостоянное (dial-up) подключение пользователя.

Как я уже писал, для модемного пула я рекомендую устанавливать модемы ZyXEL. Модемы Robotics тоже хорошо работают, но ZyXEL — это мой субъективный выбор. В случае с выделенной линией вероятность возникновения каких-либо помех на линии значительно меньше, чем при работе с обыкновенными телефонными линиями. Чтобы обеспечить надежное соединение пользователя, нужно установить профессиональные модемы и правильно настроить их.

О том, как настраивать модемы, вы прочитаете в документации по модему. Лучший модем в этом случае — это модем, который лучше остальных работает на данной линии. Сейчас мы не рассматриваем случай, когда вы являетесь Интернет-провайдером и у вас нет возможности проконтролировать, какой модем установил пользователь. Перед покупкой модема протестируйте его работу на линии — обычно фирма-продавец разрешает сделать это. Когда вы найдете оптимальный вариант по цене и качеству — покупайте.

Тестировать подключение нужно непосредственно на той АТС, к которой подключен пользователь. Не повторяйте распространенной ошибки, когда администратор, настроив сервер удаленного доступа, пытается протестировать соединение, позвонив с другого номера той же АТС. Учитывая качество наших телефонных линий, результаты тестирования на разных АТС будет отличаться. Лучше всего тестировать подключение, находясь на рабочем месте удаленного пользователя.

1.6. Что такое «протокол» и что такое «интерфейс». Наиболее важные протоколы

Теперь пора уже перейти к протоколам, в частности, к протоколу TCP/IP, который лежит в основе сети Интернет. **Протокол — это совокупность правил, определяющих взаимодействие абонентов вычислительной системы (в нашем случае — сети) и описывающих способ выполнения определенного класса функций.** Говоря простым языком, протокол — это набор правил, по которым взаимодействуют компьютеры между собой.

Еще один термин, который мы будем часто употреблять, интерфейс. **Интерфейс — это средства и правила взаимодействия компонент системы между собой.** Чтобы лучше понять значения этих терминов, обратите внимание на рис. 1.9. На этом рисунке изображены две системы (компьютера) — A и B.

Из рис. 1.9 видно, что средства, которые обеспечивают взаимодействие модулей разных уровней в рамках *одной системы* (например, B1 и B2), называются интерфейсом, а средства, обеспечивающие взаимодействие компонент одного уровня *разных систем* (например, A1 и B1), называются протоколом.

Протокол и интерфейс можно сравнить еще и так: разговор двух директоров разных предприятий можно назвать протоколом, а разговор директора и подчиненного одного предприятия можно считать интерфейсом.

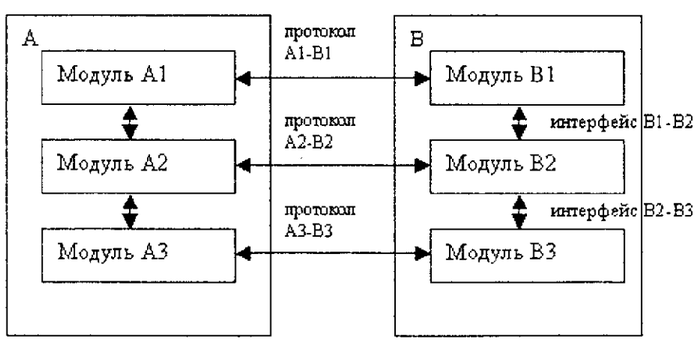


Рис. 1.9. *Протоколы и интерфейсы*

Как вы уже догадались, разговор сотрудников разных предприятий будет протоколом.

Необходимость протоколов обусловлена тем, что в сети могут взаимодействовать компьютера с самым разным программным обеспечением (операционными системами) и самым разным аппаратным устройством. Чтобы все подключенные к сети компьютеры могли понимать друг друга, необходимы общие наборы правил. Такими наборами правил и являются протоколы. Для разного рода взаимодействий используются разные правила, а значит, и разные протоколы. Давайте рассмотрим основные протоколы, используемые в Интернете.

Протокол TCP/IP. Самым главным — святыней всех святынь — является **протокол TCP/IP** (Transmission Control Protocol/Internet Protocol — Протокол Управления Передачей/Интернет протокол). Именно на этом протоколе основана вся сеть Интернет.

Если быть точными TCP/IP — это не один, а два протокола:

- Протокол TCP — является транспортным протоколом, который обеспечивает гарантированную передачу данных по сети.
- Протокол IP — является адресным протоколом, который отвечает за адресацию всей сети. То есть, благодаря использованию протокола IP, каждый компьютер (устройство) в сети имеет свой индивидуальный адрес (IP-адрес). По этим адресам и осуществляется передача данных. Широко используемые в Интернете URL-адреса (www.rambler.ru, www.ozon.ru и т.п) являются лишь словесными обозначениями IP-адресов. Сделано это для удобства, поскольку человеку проще запомнить словесный адрес, нежели числовой IP-адрес. Однако компьютеры работают только с числовыми адресами. Когда вы вводите URL-адрес в командную строку браузера, то он автоматически преобразуется в IP-адрес. Обмен данными в Интернете осуществляется только по IP-адресам.

За сопоставление словесных URL-адресов и числовых IP-адресов отвечает специальная служба — служба DNS. И ошибка в этом деле может привести к тому, что вы будете обращаться к одному серверу, а попадать на другой или вообще никуда не попадать, а наблюдать у себя на экране сообщение об ошибке. Подробнее на рассмотрении протокола TCP/IP и службы DNS мы остановимся чуть позже, когда будем изучать передачу данных в сети Интернет. Сейчас же продолжим рассмотрение других немаловажных протоколов.

Протокол ICMP (Internet Control Message Protocol) — протокол межсетевых управляющих сообщений. С помощью этого протокола компьютеры и устройства в сети обмениваются друг с другом управляющей информацией. К примеру, этот протокол используется для передачи сообщений об ошибках, проверки доступности узла и т.д.

Протокол FTP (File Transfer Protocol) — протокол передачи файлов. Служит для обмена файлами между компьютерами. Например, вам нужно передать файл на сервер или, наоборот, скачать файл с сервера. Для этого вам нужно подключиться к файловому серверу (он же FTP-сервер) и выполнить необходимую вам операцию скачивания или закачки. Подключение к FTP-серверу обычно осуществляется с помощью FTP-клиента. Простейший FTP-клиент входит в состав практически любой операционной системы. Кстати, просматривать FTP-сервера могут и обычные браузеры.

Протокол HTTP (Hyper Text Transfer Protocol) — протокол обмена гипертекстовой информацией, то есть документами HTML. Вы наверное слышали, что HTML является базовым языком создания web-страниц. Так вот, протокол HTTP предназначен для их передачи в сети. Таким образом, протокол HTTP используется Web-серверами. Соответственно браузеры, используемые для блуждания по Интернету, являются HTTP-клиентами.

Протоколы POP и SMTP. Протокол **POP** (Post Office Protocol) — протокол почтового отделения. Этот протокол используется для получения электронной почты с почтовых серверов. А для передачи электронной почты служит протокол **SMTP** (Simple Mail Transfer Protocol) — протокол передачи сообщений электронной почты.

Протокол IMAP. Для чтения почты существует и другой протокол — **IMAP**. Его отличие от протокола POP состоит в том, что пользователь читает сообщения электронной почты, не загружая их на свой компьютер. Все сообщения хранятся на сервере. При удалении сообщения оно удаляется с сервера.

Протокол SLIP (Serial Line Internet Protocol) — протокол подключения к сети Интернет по последовательной линии. Используется для установления связи с удаленными узлами через низкоскоростные последовательные интерфейсы. В настоящее время вытеснен протоколом PPP и практически не используется.

Протокол PPP (Point-to-Point Protocol) — обеспечивает управление конфигурацией, обнаружение ошибок и повышенную безопасность при передаче данных на более высоком уровне, чем протокол SLIP. Поэтому при настройке сервера рекомендуется использовать именно этот протокол. Протокол PPP рассмотрен в RFC 1547 и RFC 1661.

Протокол RIP (Routing Information Protocol) — используется для маршрутизации пакетов в компьютерных сетях. Для маршрутизации также используется протокол OSPF (Open Shortest Path First), который является более эффективным, чем RIP.

1.7. Как осуществляется сетевое взаимодействие

В каком виде информация передается по сети

Любая сеть связи работает с использованием определенного метода коммутации абонентов. Наиболее распространены три метода коммутации:

- коммутация каналов;
- коммутация пакетов;
- коммутация сообщений.

Для использования метода коммутации каналов нужен физический канал для прямой передачи данных между узлами. Физический канал состоит из последовательно соединенных канальных участков. Каналы соединяются между собой коммутаторами, которые устанавливаются межу конечными узлами сети.

Коммутация каналов удобна для телефонных сетей. Для передачи компьютерного трафика был разработан метод коммутации пакетов. Для передачи компьютерных данных сети с коммутацией каналов совершенно не годятся из-за слишком большого коэффициента пульсации трафика. Рассмотрим следующую ситуацию: вы заходите на почтовый сервер и запрашиваете список сообщений. Сервер, в ответ на ваш запрос, порождает относительно небольшой трафик — ведь список содержит небольшой объем информации — кто отправил, дата, тема, размер сообщения.

Просмотрев список сообщений, вы загружаете на свой компьютер сообщение, отправленное вашим другом. Он написал про летний отдых и прислал десяток качественных фотографий общим размером в 10 Мб. Получение этого сообщения порождает интенсивный обмен данных. Просмотрев фотографии, вы, в свою очередь, отправляете ему свои фото, что также создает большую нагрузку на канал связи. Если сеть, в которой вы работаете, использует метод коммутации каналов, то канал между вами и сервером большую часть времени будет простаивать, занимая и без того ограниченные ресурсы коммутатора.

При коммутации пакетов ваши данные будут разбиты на части — пакеты. Вы можете передавать данные без ограничения на их размер — хоть 100 Гб, но размер пакетов ограничен — от 46 до 1500 байт. Пакеты передаются как независимые блоки. На другом компьютере переданные вами данные будут «собраны» воедино. Пакетная передача позволяет сбалансировать нагрузку на канал связи и обеспечить наиболее эффективное его использование.

Мы забыли о сетях с коммутацией сообщений. В чистом виде они сегодня не существуют, поскольку в свое время послужили прототипом сетей с коммутацией пакетов.

Из чего состоит пакет? Пакет состоит из заголовка и поля данных. Заголовок содержит служебную информацию — адрес отправителя, адрес получателя, порт назначения и другая информация. Поле данных содержит передаваемые вами данные. Ясное дело, что не все сразу, а только их часть. Любая сеть накладывает свои ограничения на длину пакетов; например, для сети Ethernet минимальный размер пакета равен 72 байтам, а максимальный — 1526. Думаю, понятно, почему пакет не может быть меньше 72 байтов: если мы не укажем служебную информацию, мы не сможем отправить даже пустой пакет. Мы еще вернемся к устройству пакетов и рассмотрим заголовок пакета подробнее.

Семиуровневая модель взаимодействия открытых систем OSI

В начале 80-х годов международной организацией по стандартизации (ISO — International Organization for Standardization) была разработана *модель взаимодействия открытых систем* (OSI — Open System Interconnection). Почему именно «открытых», думаю, ясно: все мы знаем русский язык, который и является этим *открытым соглашением*. В другой литературе вы можете встретить и другие названия этой модели: сокращенное — модель OSI или более полное — семиуровневая модель взаимодействия открытых систем OSI.

Средства взаимодействия (см. рис. 1.10) в модели OSI делятся на семь уровней:

1. Физический.
2. Канальный.
3. Сетевой.
4. Транспортный.
5. Сеансовый.
6. Представительный.
7. Прикладной.

Благодаря этому задача сетевого взаимодействия разбивается на несколько более мелких задач. Это позволяет при разработке новых способов и инструментов сетевого взаимодействия не разрабатывать их заново целиком и полностью, а использовать уже готовые решения, заменив только некоторые его части.

Непосредственно друг с другом взаимодействуют только физические уровни. Все остальные уровни напрямую взаимодействуют только с выше- и нижележащими уровнями: пользуются услугами нижележащего и предоставляют услуги вышележащему. Друг с другом такие уровни контактируют косвенным образом, через посредство нижележащих уровней.

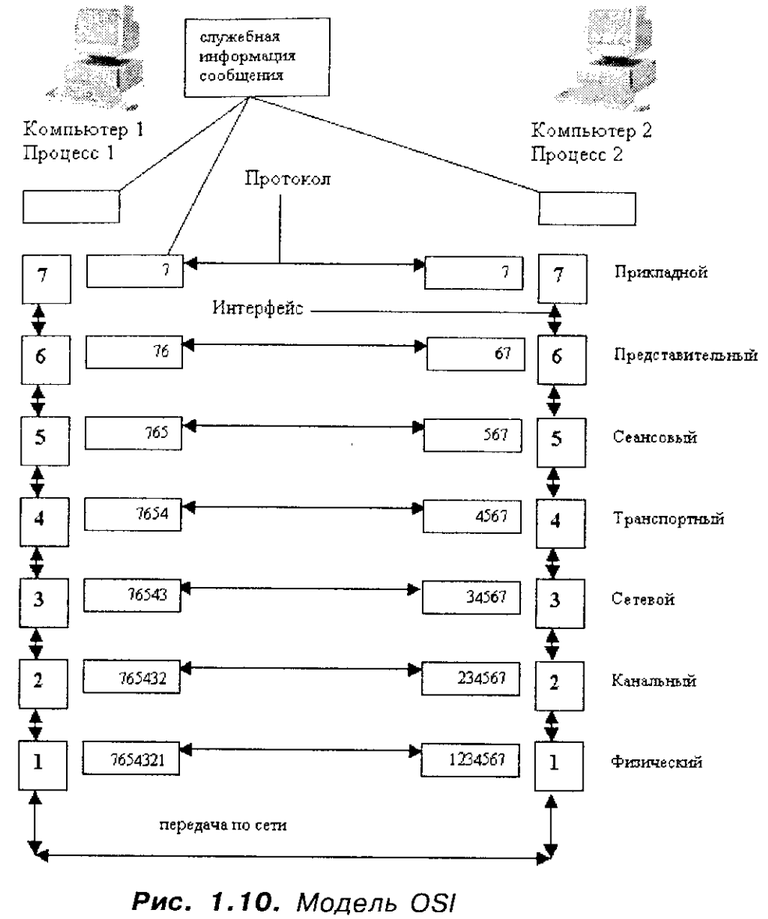


Рис. 1.10. *Модель OSI*

Примечание.

В некоторых случаях сетевого взаимодействия физический уровень как таковой отсутствует, при этом его функции выполняет самый низлежащий уровень.

Из рис. 1.10 видно, что по мере прохождения сообщения через уровни модели OSI к пересылаемым данным добавляется служебная информация, свидетельствующая о прохождении данных через определенный уровень.

Взаимодействие между компьютерами вы обычно осуществляете с помощью каких-либо программных приложений, обладающих специальным набором функций. Эти приложения работают на самом высоком уровне модели взаимодействия — прикладном. Поэтому, когда вы укажете, что хотите записать определенные данные в файл, будет сформировано соответствующее сообщение. В поле данных этого сообщения и будет содержаться передаваемая в файл информация.

После формирования сообщение с прикладного уровня будет передано на представительный уровень. На этом уровне в заголовок добавляются указания для представительного уровня компьютера-адресата. Потом сообщение передается сеансовому уровню, который добавляет свою ин-

формацию и т.д. Как изменяется заголовок видно из рис. 1.10. Процесс вложения одного протокола в другой называется *инкапсуляцией*. В процессе прохождения исходного блока данных (сообщения) по уровням он разбивается на более мелкие фрагменты для пересылки их по сети.

Когда сообщение поступает на компьютер-адресат, оно принимается физическим уровнем и передается вверх с уровня на уровень. Каждый уровень анализирует содержимое заголовка своего уровня, выполняет содержащиеся в нем указания, затем удаляет относящуюся к себе информацию из заголовка и передает сообщение далее вышележащему уровню. Этот процесс называется *декапсуляцией*.

Далее приведено описание уровней взаимодействия.

1.8. Уровни сетевого взаимодействия

Физический уровень (Physical Layer)

Физический уровень передает биты по физическим каналам связи, например, коаксиальному кабелю или витой паре. То есть именно этот уровень непосредственно производит передачу данных.

На этом уровне определяются характеристики электрических сигналов, которые передают дискретную информацию, например: тип кодирования, скорость передачи сигналов. К этому уровню также относятся характеристики физических сред передачи данных: полоса пропускания, волновое сопротивление, помехозащищенность.

Функции физического уровня реализуются сетевым адаптером или последовательным портом. Примером протокола физического уровня может послужить спецификация 100Base-TX (технология Ethernet).

Канальный уровень (Data link Layer)

Канальный уровень отвечает за передачу данных между узлами в рамках одной локальной сети. При этом под узлом понимается любое устройство, подключенное к сети.

Этот уровень выполняет адресацию по физическим адресам (**MAC-адресам**), «вшитым» в сетевые адаптеры предприятием-изготовителем. Каждый сетевой адаптер имеет свой уникальный MAC-адрес, то есть вы не найдете две сетевые платы с одним и тем же MAC-адресом.

Канальный уровень переводит поступившую с верхнего уровня информацию в биты, которые потом будут переданы физическим уровнем по сети. Он разбивает пересылаемую информацию на фрагменты данных — кадры (frames).

На этом уровне открытые системы обмениваются именно кадрами. Процесс пересылки выглядит примерно так: канальный уровень отправляет кадр физическому уровню, который отправляет кадр в сеть. Этот кадр получает каждый узел сети и проверяет, соответствует ли адрес пункта назначения адресу этого узла. Если адреса совпадают, канальный уровень принимает кадр и передает наверх вышележащим уровням. Если же адреса не совпадают, то он просто игнорирует кадр. Таким образом, сеть на канальном уровне является широковещательной.

В используемых в локальных сетях протоколах канального уровня заложена определенная топология. Топологией называется способ организации физических связей и способы их адресации. Канальный уровень обеспечивает доставку данных между узлами в сети с определенной топологией, то есть для которой он разработан. К основным топологиям (см. рис. 1.11) относятся:

1. Общая шина.
2. Кольцо.
3. Звезда.

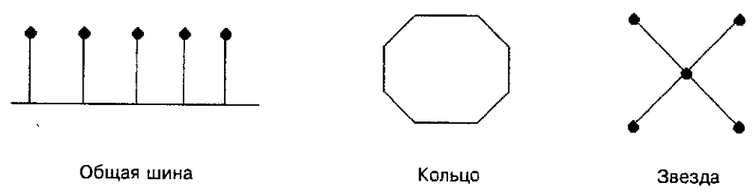


Рис. 1.11. *Основные топологии локальных компьютерных сетей*

Протоколы канального уровня используются компьютерами, мостами, маршрутизаторами. Глобальные сети (в том числе и Интернет) редко обладают регулярной топологией, поэтому канальный уровень обеспечивает связь только между компьютерами, соединенными индивидуальной линией связи.

Для доставки данных через всю глобальную сеть используются средства сетевого уровня (протоколы «точка-точка»). Примерами протоколов «точка-точка» могут послужить PPP, LAP-B. О них речь пойдет далее.

Сетевой уровень (Network Layer)

Данный уровень служит для образования единой транспортной системы, которая объединяет несколько сетей. Другими словами, сетевой уровень обеспечивает межсетевое взаимодействие.

Протоколы канального уровня передают кадры между узлами только в рамках сети с соответствующей топологией. Проще говоря — в рамках одной сети.

Нельзя передать кадр канального уровня узлу, который находится в другой сети. Данное ограничение не позволяет строить сети с развитой структурой или сети с избыточностью связей, а именно такой сетью является Интернет.

Построить одну большую сеть на канальном уровне также невозможно из-за физических ограничений. И хотя, например, спецификация 10Base-T позволяет использовать 1024 узла в одном сегменте, производительность данной сети не будет вас радовать, так как на канальном уровне сеть является широковещательной. То есть пакет данных (кадр) отсылается сразу всем компьютерам в сети. Если в сети немного компьютеров и быстрый канал связи — то это не страшно, нагрузка не будет критичной. А если компьютеров сети очень много (1024) то нагрузка на сеть будет очень велика, а это, в свою очередь, скажется на быстродействии сетевого взаимодействия. Все это приводит к необходимости другого решения для больших сетей. Именно такое решение и призван реализовать сетевой уровень.

На сетевом уровне термин *сеть* следует понимать как совокупность компьютеров, которые соединены в соответствии с одной из основных топологий и использующих для передачи данных один из протоколов канального уровня.

Сети соединяются специальными устройствами — *маршрутизаторами*. Маршрутизатор собирает информацию о топологии межсетевых соединений и на основании этой информации пересылает пакеты сетевого уровня в сеть назначения.

Чтобы передать сообщение от компьютера-отправителя компьютеру-адресату, который находится в другой сети, нужно совершить некоторое количество *транзитных передач между сетями*. Иногда их еще называют хопами (от англ. hop — прыжок). При этом каждый раз выбирается подходящий маршрут.

Сообщения на сетевом уровне называются пакетами. При этом на сетевом уровне работают несколько видов протоколов. Прежде всего — это сетевые протоколы, которые обеспечивают передвижение пакетов по сети, в том числе в другую сеть. Поэтому довольно часто к сетевому уровню относят протоколы маршрутизации (routing protocols) — RIP и OSPF.

Еще одним видом протоколов, работающтх на сетевом уровне, являются протоколы разрешения адреса — Address Resolution Protocol (ARP). Хотя эти протоколы иногда относят и к канальному уровню.

Классические примеры протоколов сетевого уровня: IP (стек TCP/IP), IPX (стек Novell).

Транспортный уровень (Transport Layer)

На пути от отправителя к получателю пакеты могут быть искажены или утеряны. Некоторые приложения самостоятельно выполняют обработку

ошибок при передаче данных, но большинство все же предпочитают иметь дело с надежным соединением, которое как раз и призван обеспечить транспортный уровень. Этот уровень обеспечивает требуемую приложению или верхнему уровню (сеансовому или прикладному) надежность доставки пакетов. На транспортном уровне определены пять классов сервиса:

1. Срочность.
2. Восстановление прерванной связи.
3. Наличие средств мультиплексирования нескольких соединений.
4. Обнаружение ошибок.
5. Исправление ошибок.

Обычно уровни модели OSI, начиная с транспортного уровня и выше, реализуются на программном уровне соответствующими компонентами операционных систем.

Примеры протоколов транспортного уровня: TCP и UDP (стек TCP/IP), SPX (стек Novell).

Сеансовый уровень (Session Layer)

Сеансовый уровень устанавливает и разрывает соединения между компьютерами, управляет диалогом между ними, а также предоставляет средства синхронизации. Средства синхронизации позволяют вставлять определенную контрольную информацию в длинные передачи (точки). Благодаря этому, в случае обрыва связи, можно вернуться назад (к последней точке) и продолжить передачу с места обрыва.

Сеанс — это логическое соединение между компьютерами. Каждый сеанс имеет три фазы:

1. Установление соединения. Здесь узлы «договариваются» между собой о протоколах и параметрах связи.
2. Передача информации.
3. Разрыв связи.

Не нужно путать сеанс сетевого уровня с сеансом связи. Пользователь может установить соединение с Интернетом, но не устанавливать ни с кем логического соединения, то есть не принимать и не передавать данные.

Представительный уровень (Presentation Layer)

Представительный уровень изменяет форму передаваемой информации, но не изменяет ее содержания. Например, средствами этого уровня может быть выполнено преобразование информации из одной кодировки в другую. Также на этом уровне выполняется шифрование и дешифрование данных.

Примером протокола представительного уровня может служить протокол SSL (Secure Socket Layer). Данный протокол обеспечивает секретный обмен данными.

Прикладной уровень (Application Layer)

Данный уровень представляет собой набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к совместно используемым ресурсам. Единица данных называется сообщением.

Примеры протоколов: HTTP, FTP, TFTP, SMTP, POP, SMB, NFS.

1.9. Интернет и модель OSI

При взаимодействии открытой системы и Интернет модель OSI упрощается, так как некоторые протоколы Интернет включают в себя функции нескольких уровней. Если к сети Интернет подключается один пользователь, а не вся сеть, то автоматически исчезают канальный и физический уровни, потому что нет сетевых адаптеров, а значит, нет и физических адресов. В данном случае конечным протоколом будет протокол типа «точка-точка», например, PPP. В этот протокол будут вложены все остальные.

1.10. Адресация в компьютерных сетях. IP-адреса

Вид IP-адреса и способы его назначения

Любому компьютеру в IP-сети (TCP/IP-сети) назначен уникальный адрес, который называется IP-адресом. **IP-адрес** — это 32-разрядное число, которое принято записывать в десятеричном или шестнадцатеричном формате в виде четырех чисел, разделенных точками, например:

1. 111.111.213.232
2. 127.0.0.1
3. 192.168.9.2

При условии, что ваша сеть подключена к Интернет, протокол TCP/IP обеспечивает работу вашей сетевой программы с любым компьютером в мире, как-будто тот находится в локальной сети. Уникальность IP-адреса достигается достаточно просто — IP-адреса назначаются централизованно **Сетевым Информационным Центром** (NIC, Network Information Center).

Для понимания остальной информации нужно отметить, что существуют локальные (LAN, Local Area Networks) и региональные (Wide Area Networks) сети. Сеть Интернет сначала была региональной (Arpanet), а

потом стала глобальной, объединив все региональные сети мира. Если ваша локальная (или даже региональная) сеть не соединена с Интернет, то внутри сети вы можете использовать любые IP-адреса без согласования с NIC. Обычно в локальных сетях используются особые IP-адреса, о которых мы поговорим немного позже.

Любую сеть, независимо от типа — LAN или WAN, можно разделить на подсети. Причины разбиения сети на подсети кроются в ранних версиях протокола IP. Тогда существовало несколько сетей класса A, содержащих несколько миллионов узлов (о классах читайте далее). Помимо всего прочего, в таких сетях очень велика вероятность коллизий, то есть одновременного доступа двух или более узлов к среде передачи данных. Управлять такой сетью крайне неудобно, да и сеть будет перегружена собственным трафиком. Поэтому основной принцип разделения — «разделяй и властвуй».

К другим причинам разделения относят создание маленьких подсетей с использованием разных технологий — Ethernet, Token Ring, FDDI, ATM. Вы не можете смешивать эти технологии в одной сети, однако они могут быть взаимосвязаны с помощью разделения на подсети.

Разделение на подсети может быть также произведено из соображений безопасности. Более подробно об этой и других причинах разделения сети на подсети вы можете прочитать в руководстве IP Sub-networking-HOWTO, которое вы найдете на прилагаемом компакт-диске.

Как я уже писал, каждый компьютер в сети имеет свой уникальный адрес. Но оказывается, что и сеть (подсеть) также имеет свой уникальный адрес. Под сетью можно понимать «пачку» IP-адресов, идущих подряд, то есть 192.168.1.0...192.168.1.255. Самый младший и самый старший адреса резервируются. Младший (192.168.1.0) является адресом сети, а старший является широковещательным (broadcast) адресом сети. Адрес сети может потребоваться, когда нужно указать всю сеть (подсеть), например, при задании маршрутизации для этой сети.

Представьте, что у вас есть две отдельных сети и вам нужно объединить их в одну. Тогда эта одна «большая» сеть станет называться сетью, а две «маленькие» — подсетями. Устройство, которое будет обеспечивать связь этих сетей (маршрутизацию), называется, как уже было отмечено выше, маршрутизатором. Маршрутизатор может быть как аппаратным (отдельное устройство), так и программным.

В роли программного маршрутизатора может выступать любой компьютер с двумя (или более) сетевыми интерфейсами, например, двумя сетевыми платами. В качестве операционной системы может быть установлена любая сетевая операционная система, поддерживающая перенаправление пакетов IPv4-Forwarding. Такой операционной системой может быть Linux, FreeBSD, любая UNIX-система, Windows NT/2000. Маршутизатор можно настроить и на базе Windows 98, но делать это я не рекомендую, поскольку

ку вряд ли он будет работать надежно. Традиционно в роли маршрутизатора используются UNIX-системы, к которым относится и Linux.

Широковещательный адрес используется для передачи сообщений «всем — всем — всем» в рамках сети, то есть когда нужно передать сообщение (пакет) сразу всем компьютерам сети. Широковещательные запросы очень часто используются, например, для построения ARP-таблиц.

Для каждой подсети определена ее маска. Фактически, маска — это размер сети, то есть число адресов в сети. Маску принято записывать в десятично-побайтном виде:

1. 255.255.255.0 — маска на 256 адресов (0...255);
2. 255.255.255.192 — маска на 64 адреса (192...255);
3. 255.255.0.0 — маска на 65536 адресов (256*256)

Классы IP-сетей

В общем случае IP-сети делятся на три класса: A, B, C, D и E.

Сети класса A — это огромные сети. Маска сети класса A: 255.0.0.0. В каждой сети такого класса может находиться 16777216 адресов. Адреса таких сетей лежат в промежутке 1.0.0.0...126.0.0.0, а адреса хостов (компьютеров) имеют вид 125.*.*.*

Сети класса B — это средние сети. Маска такой сети — 255.255.0.0. Эта сеть содержит 65536 адресов. Диапазон адресов таких сетей 128.0.0.0... 191.255.0.0. Адреса хостов имеют вид 136.12.*.*

Сеть класса C — маленькие сети. Содержат 256 адресов (на самом деле всего 254 хоста, так как номера 0 и 255 зарезервированы). Маска сети класса C — 255.255.255.0. Интервал адресов: 192.0.1.0...223.255.255.0. Адреса хостов имеют вид: 195.136.12.*

Класс сети определить очень легко. Для этого нужно перевести десятичное представление адреса сети в двоичное. Например, адрес сети 128.11.1.0 в двоичном представлении будет выглядеть так:

```
10000000 00001011 00000001 00000000
```

А 192.168.1.0:

```
11000000 10101000 00000001 00000000
```

Если адрес начинается с последовательности битов 10, то данная сеть относится к классу B, а если с последовательности 110, то — к классу C.

Если адрес начинается с последовательности 1110, то сеть является сетью **класса D**, а сам адрес является особым — групповым (multicast). Если в пакете указан адрес сети класса D, то этот пакет должны получить все хосты, которым присвоен данный адрес.

Характеристики сетей различных классов *Таблица 1.1*

Класс	Первые биты	Диапазон адресов	Количество узлов
A	0	1.0.0.0...126.0.0.0	16777216 (2^{24})
B	10	128.0.0.0...191.255.0.0	65536 (2^{16})
C	110	192.0.1.0...223.255.255.0	256 (2^{8})
D	1110	224.0.0.0...239.255.255.255	Multicast
E	11110	240.0.0.0...247.255.255.255	Зарезервирован

Адреса **класса E** зарезервированы для будущего применения. В табл. 1.1 приведены сравнительные характеристики сетей классов A, B, C, D и E.

Теперь самое время немного сказать о специальных адресах, о которых я упомянул немного выше. Если весь IP-адрес состоит из нулей (0.0.0.0), то значит, он обозначает адрес того узла, который сгенерировал этот пакет.

Адрес 255.255.255.255 — это широковещательный адрес. Пакет с таким адресом будет рассылаться всем узлам, которые находятся в той же сети, что и источник пакета. Это явление называется ограниченным широковещанием. Существует также другая рассылка, которая называется широковещательным сообщением. В этом случае вместо номера узла стоят все единицы в двоичном представлении (255). Например, 192.168.2.255. Это означает, что данный пакет будет рассылаться всем узлам сети 192.168.2.0.

Особое значение имеет IP-адрес 127.0.0.1 — это адрес локального компьютера. Он используется для тестирования сетевых программ и взаимодействия сетевых процессов. При попытке отправить пакет по этому адресу данные не передаются по сети, а возвращаются протоколам верхних уровней, как только что принятые. При этом образуется как бы «петля». Этот адрес называется **loopback**. В IP-сети запрещается использовать IP-адреса, которые начинаются со 127. Любой адрес подсети 127.0.0.0 относится к локальному компьютеру, например: 127.0.0.1, 127.0.0.5, 127.77.0.6.

Существует также специальные адреса, которые зарезервированы для несвязанных локальных сетей — это сети, которые используют протокол IP, но не подключены к Интернет. Вот эти адреса:

1. 10.0.0.0 (сеть класса A, маска сети 255.0.0.0).
2. 172.16.0.0 — 172.31.0.0 (16 сетей класса B, маска каждой сети 255.255.0.0).
3. 192.168.0.0 — 192.168.255.0 (256 сетей класса C, маска каждой сети 255.255.255.0).

В этой книге я старался использовать именно такие адреса, чтобы не вызвать пересечение с реальными IP-адресами.

Глава 2

Стандарты IEEE

Это больше теоретическая, нежели практическая глава. В ней мы будем рассматривать стандарты, по которым строятся современные сети — стандарты IEEE. Кроме того, в этой главе мы поговорим об истории развития компьютерных сетей, конечно, может не так подробно, как хотелось, но вкратце скажем — этого будем достаточно, чтобы поняли, что и откуда произошло.

Довольно серьезный вопрос, который будет рассматриваться в этой главе — это уровень управления доступом к среде — MAC. На этом уровне даже существуют так называемые аппаратные адреса, MAC-адреса, сетевых устройств. Например, каждая сетевая плата имеет свой уникальный MAC-адрес, по которому можно однозначно ее распознать. Многие сетевые администраторы, создавая программы учета трафика, привязываются именно к MAC-адресам, поскольку эти адреса позволяют однозначно идентифицировать пользователя — ведь IP-адрес можно изменить, а MAC — нет. Для изменения MAC-адреса нужно заменить сетевую плату, что во многих организациях просто невозможно.

Учитывая серьезность как первого, так и второго вопроса, не рекомендую пропускать эту главу или читать ее «по диагонали». Вы же не хотите себя неловко чувствовать, когда зайдет разговор о стандартах IEEE? Вы же не скажете: «А я эту главу пропустил...»???

2.1. Разделение канального уровня

IEEE (Institute of Electrical and Electronic Engineers) — Институт инженеров по радиоэлектронике (США), занимающийся стандартизацией в области информационных технологий.

В 1980 году институтом IEEE был организован комитет 802, занимающийся стандартизацией локальных сетей. В результате работы данного комитета появилась группа стандартов IEEE 802.x. Данные стандарты содержат рекомендации относительно построения нижних уровней локальной сети — физического и канального. Физический и канальный уровни отражают специфику локальных сетей разного вида, в то время как более высокие уровни, например, сетевой, одинаковые как для локальных, так и для глобальных сетей.

Канальный уровень делится на два подуровня:

- MAC (Media Access Control) — уровень управления доступом к среде.
- LLC (Logical Link Control) — уровень логической передачи данных.

Уровень MAC обеспечивает корректное совместное использование общей среды передачи данных. Используя определенный алгоритм, который различается для сетей разного типа, доступ к среде предоставляется тому или иному узлу сети. То есть для каждого типа сети имеется свой алгоритм доступа, заложенный на уровне MAC. В этом алгоритме заложены правила общей среды передачи данных, правила «общения» компьютеров, точнее, правила использования сетевого кабеля (тот, который для передачи данных, а не напряжения!). Если компьютер (или другое сетевое устройство) использует один и тот же алгоритм, что и сеть, к которой он подключается, значит, этот компьютер может работать в этой сети.

После предоставления доступа на уровне MAC, можно «перейти» на более высокий уровень — LLC.

Уровень LLC предназначен для передачи кадров между узлами. Уровень LLC позволяет установить степень надежности передачи данных — одни данные, не очень важные, будут передаваться с небольшой степенью надежности, что позволит увеличить скорость их передачи. Другие данные, очевидно «top secret», будут передаваться с самой большой степенью надежности, что снизит скорость передачи, но будет гарантировать 100%-ю доставку данных при условии неразрывности среды передачи данных. Про степень надежности уровня LLC мы поговорим в следующем пункте.

Стандарты IEEE, лежащие в основе локальных сетей, представлены в табл. 2.1, а структура стандартов IEEE представлена на рис. 2.1.

Комитет 802 института IEEE проанализировал сетевые технологии различных компаний с целью найти общие подходы и принципы. Описание каждой технологии делится на два уровня — канальный и физический. Канальный уровень, как уже отмечалось, был разделен на два подуровня — MAC и LLC. Протокол LLC, как видно из рисунка, общий для всех технологий уровня MAC и не зависит от выбора самой технологии.

Таблица 2.1

Стандарт	Описание
802.1	Объединение сетей (internetworking)
802.2	Протокол LLC (Logical Link Control)
802.3	Локальные сети с методом доступа CSMA/CD (Ethernet)
802.4	Локальные сети с методом доступа Token Bus (Token Bus LAN)
802.5	Локальные сети с методом доступа Token Ring (Token Ring LAN)
802.6	Распределенная городская сеть MAN (Metropolitan Area Network)
802.7	Консультативная группа по широкополосной передаче, что-то наподобие группы технической поддержки (Broadband Technical Advisory Group)
802.8	Консультативная группа по волоконно-оптическим сетям (Fiber Optic Advisory Group)
802.9	Сети с интеграцией звука и данных (Integrated Voice and Data Networks)
802.10	Сетевая безопасность (Network Security)
802.11	Беспроводные сети (Wireless Networks)
802.12	Локальные сети с методом доступа по требованию и с приоритетом (Demand Priority Access LAN)

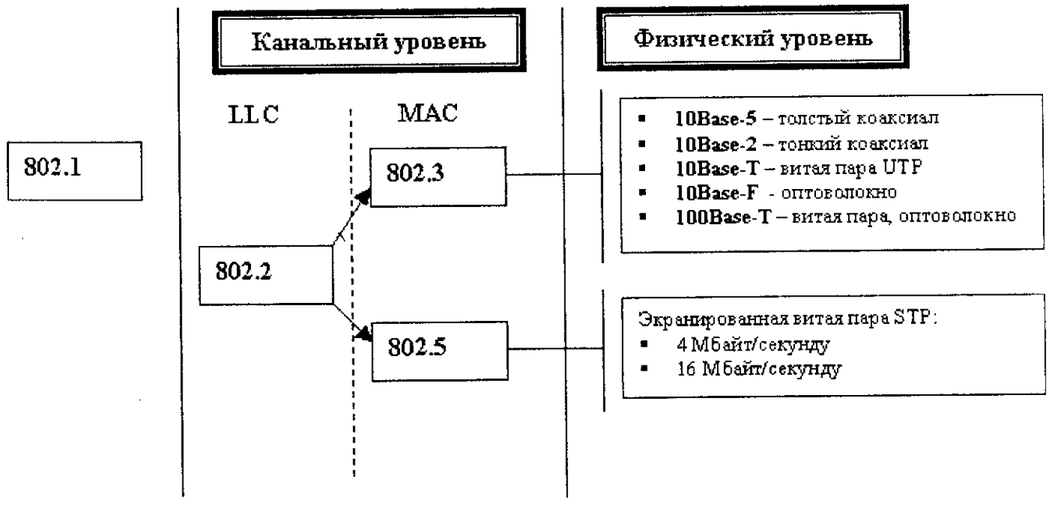


Рис. 2.1. *Структура стандартов IEEE*

2.2. Протокол LLC

Общее описание

LLC (Logical Link Control) — это протокол управления логическим каналом. Как уже отмечалось, как только станция получит разрешение на соединение на уровне MAC, устанавливается логическое соединение между передающей данные станцией и принимающей эти данные станцией. Протокол LLC управляет данным логическим соединением.

Протокол LLC является своеобразным мостом между протоколами сетевого уровня и протоколами уровня MAC. Протоколы сетевого уровня передают протоколу LLC следующую информацию:

- Пакет данных (например, IP, NetBEUI или IPX).
- Адрес узла-назначения.
- Качество передачи данных (степень надежности).

Протокол LLC записывает информацию, переданную сетевым протоколом, в свой пакет, дополняя его при этом служебной информацией. Далее пакет переходит на уровень MAC, где он преобразуется в кадр уровня MAC (например, в кадр Ethernet), дополненный определенными служебными заголовками, характерными для уровня MAC.

Различные компании использовали различные функции протоколов в своих технологиях. Это привело к необходимости включить в уровень LLC три типа процедур управления передачей данных, которые позволяют выбрать степень надежности передачи:

- LLC1 — процедура без установления соединения и без подтверждения.
- LLC2 — процедура с установлением соединения и с подтверждением.
- LLC3 — процедура без установления соединения, с подтверждением.

Стоит отметить, что протокол сетевого уровня может обратиться только к процедурам одного типа.

Процедура без установления соединения и без подтверждения

Это наименее надежный, но наиболее быстрый способ передачи данных. При этом способе передаче данных данные отправляются вслепую. Если узел назначения не может принять данные — например, он загружен или просто выключен, то данные отправляются «в никуда». Наш узел так и не узнает, получил ли данные узел назначения, поскольку процедура LLC1 не предусматривает подтверждения получения данных.

Данный способ передачи данных называется дейтаграммным (UDP, User Datagram Protocol). Кроме всего прочего он позволяет снизить загруженность канала, поскольку пакеты с подтверждением получения не отправляются.

Процедура с установлением соединения и с подтверждением

LLC2 — наиболее надежный способ передачи данных, поскольку сначала устанавливается логическое соединение с узлом назначения, а потом уже передаются данные, причем каждый переданный пакет подтверждается. Установление соединения позволяет исключить невозможность приема данных узлом назначения. Если узел назначения не может принять данные (например, он выключен), то передача будет прервана. Если узел не получил переданный пакет или пакет в результате передачи был поврежден, то пакет будет передан заново.

Процедура без установления соединения, с подтверждением

В некоторых, достаточно редких случаях, потеря времени на установление соединения просто неприемлема и/или просто не нужна, поскольку мы точно знаем, что узел назначения включен и ожидает передачи данных. В то же время, нам нужно знать, получил ли он от нас переданный пакет или нет. Тогда процедуры LLC1 и LLC2 нас не устраивают — нам нужно использовать LLC3.

Какие процедуры использует тот или иной протокол, зависит от его разработчиков. Например, протокол NetBIOS/NetBEUI (разработка Microsoft/IBM) использует процедуры LLC2. Но это, если стек протоколов NetBIOS/NetBEUI работает в режиме восстановления искаженных пакетов, если же стек NetBIOS/NetBEUI работает в дейтаграммном режиме, используются процедуры LLC1.

Стек TCP/IP всегда использует режим работы LLC1, поскольку протокол LLC в этом случае используется просто для извлечения из кадра пакетов различных протоколов — IP, ARP и др.

Глава 3

Сетевые технологии, на основе которых строятся сети

Ничто не стоит на месте, а в процессе своего развития усовершенствуется и видоизменяется. Точно такая же ситуация сложилась вокруг компьютерных сетей. Сначала были одни сети, затем другие — более совершенные. Поначалу, когда компьютерные сети не были стандартизированы, их было несметное количество — практически каждая компания старалась разработать свою сеть (а мы новый дом построим!). Ясное дело, что компьютеры, оснащенные сетевыми адаптерами одной компании, не могли работать в сети, в которой использовались сетевые адаптеры другой фирмы, не говоря уже о типе кабеля. Со временем возникла необходимость стандартизации — чтобы навести порядок в создавшемся хаосе.

Одной из самых «древних» сетей, тем не менее, дожившей до наших дней и даже все еще используемой на некоторых предприятиях, является сеть Ethernet. Она позволяет передавать данные со скоростью 10 Мбитс/с (это теоретически, на практике выходит меньше).

Усовершенствованным потомком сети Ethernet является сеть Fast Ethernet, позволяющая передавать данные со скоростью 100 Мбитс/с. Это технология сегодняшнего дня — она используется в большинстве сетей, в основном с ней вам придется работать. Технология Fast Ethernet идеально подходит для этого самого сегодняшнего дня: она дешева и обеспечивает приемлемую скорость передачи данных.

Все остальные технологии рассматриваются в этой книге или для общего развития — чтобы вы знали, что это такое, или для некоторых экстремальных случаев, когда использовать стандартную технологию — Fast Ethernet — нельзя или нецелесообразно.

3.1. Технология Ethernet

3.1.1. Стандарт Ethernet и его развитие

Технология Ethernet (и ее модификация Fast Ethernet) является наиболее распространенной технологией построения локальных сетей. Общее количество компьютеров, оснащенных сетевыми адаптерами Ethernet, давно превысило 50 миллионов.

Корни сети Ethernet уходят далеко в прошлое: в шестидесятые годы прошлого века. Сейчас поясню: в Ethernet-сетях используется метод доступа CSMA/CD, о котором мы поговорим позже. Несмотря на то, что первая экспериментальная Ethernet-сеть была создана компанией Xerox в 1975 году, сам метод CSMA/CD был опробован во второй половине 60-х годов в радиосети Гавайского университета. Тогда он получил название Aloha.

В 1980 году компании DEC, Intel и Xerox разработали вторую версию стандарта Ethernet — Ethernet II или Ethernet DIX (по первым буквам названий фирм-создателей). Стандарт Ethernet II предусматривал работу сети на основе коаксиального кабеля.

Чуть позже, на основе стандарта Ethernet II, был разработан стандарт IEEE 802.3, который практически совпадает со стандартом Ethernet II. Отличия оригинального стандарта Ethernet от стандарта 802.3 состоят в следующем:

- В оригинальном стандарте уровни MAC и LLC объединены в один уровень — канальный, а в стандарте 802.3 — это два самостоятельных уровня.
- В стандарте IEEE 802.3 отсутствует протокол тестирования конфигурации, который имеется в оригинальном стандарте.
- Есть небольшие отличия в формате кадров.

В принципе, для нас все вышесказанные отличия несущественны, для нас главное — это среда передачи информации, а в качестве нее можно использовать:

- коаксиальный кабель с диаметром 0,5 дюйма, «толстый» коаксиал — стандарт 10Base-5;
- коаксиальный кабель с диаметром 0,25 дюйма, «тонкий» коаксиал — стандарт 10Base-2;
- неэкранированная витая пара (UTP, Unshielded Twisted Pair) — стандарт 10Base-T;
- оптоволоконный кабель — стандарт 10Base-F.

Следующий шаг в развитии технологии Ethernet был сделан в 1995 году. Тогда появился новый стандарт — Fast Ethernet. Главное его отличие от

простого Ethernet — повышенная в десять раз максимальная скорость передачи данных — 100 Мбит/с, против 10 Мбит/с. Хотя стандарт Fast Ethernet не является самостоятельным стандартом: для него не был создан отдельный стандарт IEEE. Стандарт Fast Ethernet описан в документе IEEE 802.3u.

В 1998 году была «запущена» технология Gigabit Ethernet. Скорость передачи данных возросла еще в 10 раз и составила 1000 Мбит/с. Принятие стандарта было поначалу воспринято с большим энтузиазмом, но пыл охладила стоимость оборудования для этого стандарта, поэтому технология Gigabit Ethernet не получила особого распространения. По крайней мере, на просторах СНГ она встречается довольно редко, и мы подробно ее рассматривать не будем. Стандарт Gigabit Ethernet был описан в документе IEEE 802.3z. Как видите, и эта технология не получила отдельного документа IEEE. Почему же так выходит? Да потому, что все эти три технологии — Ethernet, Fast Ethernet и Gigabit Ethernet используют один и тот же метод разделения среды передачи данных — CSMA/CD.

3.1.2. Метод разделения среды передачи данных CSMA/CD

CSMA/CD (Carrier-Sense-Multiply-Access with Collision Detection) — метод коллективного доступа с обнаружением несущей (carrier) и коллизий. Метод CSMA/CD используется в сетях с логической топологией типа «шина». При использовании данной топологии все компьютеры подключены к общей среде передачи данных — как гирлянды на новогодней елке. Ясное дело, что в определенный момент времени обмениваться информацией могут только два компьютера.

Если в момент обмена данных еще один компьютер пытается передать данные по общей шине. Тогда возникает коллизия. Это как параллельный телефон — вы разговариваете по телефону, а кто-то в соседней комнате поднимает трубку и пытается набрать номер. Не подумайте, что этому третьему компьютеру нужно будет ждать, пока первые не завершат полностью обмен информацией. Представьте, если бы так работала сеть, то все пользователи «отдыхали», пока вы скопируете фильм объемом 700 Мб. Инженерами, проектировавшими сеть Ethernet, все предусмотрено на этот случай.

Как же передаются данные по сети Ethernet? Данные «упаковываются» в кадры определенного формата (о форматах кадров мы поговорим чуть позже). Перед передачей кадра передающий его компьютер должен убедиться, что среда передачи данных свободна. Если среда передачи данных свободна, компьютер передает кадр.

Примечание.

Я не смог удержаться, чтобы не сказать, как именно компьютер убеждается в том, что среда передачи данных свободна. Он прослушивает несущую частоту (Carrier-Sense — отсюда первые две буквы в аббревиатуре названия метода). Если среда свободна, то на ней отсутствует несущая частота — 5...10 МГц, в противном случае считается, что среда занята. Практически, несущая — это своеобразный «флажок» занятости среды — если она есть, то среда занята — кто-то передает данные.

Каждый кадр снабжается преамбулой, которая состоит из 7 байтов 10101010 и одного, восьмого, байта со значением 10101011. Преамбула необходима для синхронизации приемника и передатчика. Кроме того, в заголовках кадра находятся сведения об адресах передатчика и приемника.

Переданный компьютером кадр получают абсолютно все компьютеры сети. Компьютер-приемник обнаруживает в заголовках кадра свой адрес, обрабатывает его, то есть передает «вверх», а сам отправляет компьютеру-передатчику ответ, который тоже оформлен в виде кадра.

Предположим, что еще одному компьютеру тоже нужно передать данные. Он проверяет наличие несущей частоты и не начинает передачу данных до тех пор, пока первый компьютер не прекратит передачу кадра. Заметьте: кадра, а не всех данных — иначе бы другому узлу пришлось бы ждать долго и нудно — вспомните пример с фильмом.

По окончании передачи все компьютеры должны немного подождать — это так называемая технологическая пауза, которая равна 9,6 мкс. Данное время также называют межкадровым интервалом. Догадываетесь, зачем эта пауза? За это время другой компьютер может начать передачу кадра. В противном случае первый компьютер узурпировал бы всю среду передачи данных и передавал бы кадр за кадром, а это недопустимо.

Почему же происходит коллизия? Метод обнаружения несущей не гарантирует защиту от коллизий. Предположим, что компьютер 1 только-только начал передавать кадр. Компьютер 2, достаточно удаленный от первого компьютера, проверил наличие несущей. Но несущая еще до него «не дошла» — ведь несущая частота — это сигнал, который передается с определенной скоростью. Поэтому он решает, что среда свободна и начинает передавать кадр. Более того, такое решение могут принять две или более станции. При этом содержимое двух или более кадров смешивается, и разобраться какие данные и кому принадлежали уже невозможно. Попробуйте разбавить лимонад молоком и потом обратно разделить их. Так возникает коллизия.

Все компьютеры наблюдают за сигналами, которые возникают в кабеле. Если сигналы, которые передаются, и наблюдаемые сигналы отличаются, значит, возникла коллизия. Компьютер, который первым обнаружил коллизию, прекращает передачу своего кадра, если он его передавал, и

«бьет тревогу» — отправляет в сеть 32-битную jam-последовательность. Затем данный компьютер делает случайную паузу. Данная пауза равна:

$$N * II$$

Здесь II — это 512 битовых интервалов, один битовый интервал для простого Ethernet (не Fast Ethernet) равен 0,1 мкс.

N — это случайное число из диапазона $0...2^K$, где K — это номер попытки передачи кадра. Максимальное значение K, то есть максимальное число попыток равно 10. После десятой попытки интервал не увеличивается. Если не удается передать кадр после 16-ой попытки, кадры отбрасывается.

3.1.3. Время двойного оборота

Для более надежного обнаружения коллизий время передачи кадра должно быть больше или равно времени двойного оборота. Время двойного оборота (PDV, Path Delay Value) — это время, за которое коллизия распространяется до самого удаленного узла. Выполнится это условие или нет, зависит от следующих факторов:

- длины минимального кадра;
- пропускной способности сети;
- длины среды передачи данных;
- скорости распространения сигнала в кабеле, которая отличается для разных типов кабеля.

Минимальная длина кадра в стандарте Ethernet составляет 46 байт, но еще нужно учитывать служебные поля и преамбулу, поэтому все вместе выходит 72 байта или 576 бит. Время передачи кадра минимальной длины в стандартном Ethernet (скорость 10 Мбит/с) составляет 575 битовых интервалов. Следовательно, время двойного оборота должно быть меньше 575 битовых интервалов (57,5 мкс). За это время сигнал может пройти по толстому коаксиальному кабелю (диаметр 0,5 дюйма) 13280 м, но так как нас интересует двойной оборот, то полученное значение нужно разделить на 2. Выходит 6635 м. Это максимальное расстояния между двумя самыми отдаленными компьютерами сети. Но на практике максимальное расстояние еще меньше, поскольку учитываются дополнительные ограничения.

Одно из самых существенных ограничений — это затухание сигнала. Затухание сигнала уменьшает максимальную длину между наиболее отдаленными компьютерами до 500 (!) метров. Почувствовали разницу: было 6635 метров, а стало всего 500. Это максимальная длина сегмента толстого коаксиального кабеля. При использовании специальных устройств — повторителей, которые увеличивают мощность сигнала и используются

для соединения сегментов сети, максимальное расстояние между самыми отдаленными компьютерами сети составляет 2500 м.

С увеличением скорости уменьшается максимальное расстояние, причем уменьшается оно пропорционально увеличению скорости. Например, в стандарте Fast Ethernet максимальное расстояние составило бы всего 250 метров, а в Gigabit Ethernet — 25. Однако разработчики этих технологий предприняли некоторые меры, благодаря которым удалось увеличить максимальное расстояние. Какие именно, мы узнаем при рассмотрении соответствующих технологий, а пока рассмотрим некоторые характеристики стандарта Ethernet (точнее его MAC-уровня). Характеристики сведены в табл. 3.1.

Характеристики стандарта Ethernet *Таблица 3.1*

Параметр	Значение
Максимальное число станций	1024
Максимальное расстояние между станциями, м	2500
Скорость передачи данных, Мбит/с	10
Межкадровый интервал, мкс	9,6
Длина jam-последовательности, бит	32
Максимальное количество попыток передачи кадра	16
Максимальная длина кадра (с преамбулой), байт	1526
Минимальная длина кадра (с преамбулой), байт	72
Длина преамбулы, байт	8
Минимальная длина паузы после коллизии, bt	0
Максимальная длина паузы после коллизии, bt	524 000

Примечание.

Сокращение «bt» означает «битовых интервалов». Данное сокращение часто используется в англоязычной литературе

3.1.4. КПД или определяем производительность сети Ethernet

Как мы знаем, производительность любой системы на практике оказывается меньше ее максимальной теоретической производительности. Одни системы работают быстрее, другие медленнее, но практически никогда не достигают максимума, хотя некоторые весьма к нему приближаются. Достигнет система пика своей производительности или нет, зависит от множества факторов, возникающих при практическом применении системы.

Точно такая же ситуация сложилась вокруг технологии Ethernet. На практике никогда не достигаются заявленные 10 Мбит/с, хотя при некото-

рых условиях скорость передачи данных достаточно близко приближается к этому значению.

Все мы знаем, что такое КПД (коэффициент полезного действия). Нет, рассчитывать КПД для Ethernet мы не будем. Лучше вычислим полезную пропускную способность данной технологии. Представим, что по сети передается кадр минимальной длины, которая, как вы знаете, равна 72 байтам. Но из этих 72 байтов 8 байтов — это преамбула, то есть служебная информация, которая никакого отношения к нашим данным не имеет. Кроме того, нужно учитывать, что кадр содержит заголовки, что также является служебной информацией. Получается, что кадр минимальной длины «переносит» всего лишь 46 байтов нашей информации (72 − 8 − 18 = 46).

Максимально возможная пропускная способность сети Ethernet при использовании кадров минимальной длины составляет 14880 кадр/с. Нетрудно рассчитать полезную пропускную способность сети Ethernet: 14880 * 46 * 8 = = 5,48 Мбит/с. Полученное значение намного меньше обещанных 10 Мбит/с. Но кадры минимальной длины используются не для передачи нашей информации, а для передачи служебной информации — так называемых квитанций. Для передачи пользовательской информации используются кадры с длиной поля данных 512 байтов. При этом полезная пропускная способность (ППС) составит около 9,3 Мбит/с, что весьма близко к заветным 10 Мбит/с. При использовании кадров максимальной длины ППС составит около 9,76 Мбит/с, что тоже очень близко к 10 Мбит/с. Однако нужно заметить, что ни при использовании кадров нормальной длины, ни при использовании кадров максимальной длины, максимальная пропускная способность не была достигнута.

Данную ситуацию можно сравнить с обыкновенной бутылкой, на которой написано 0,5 литра. Да, в ней находится 0,5 литра жидкости, но в бутылку можно залить еще немного — вы же замечали, что от максимального уровня до крышки еще есть «место», которое никогда не заполняют при разливе. Правда, может сложиться и другая ситуация — на бутылки написано 0,5 литра, как максимальное значение, а жидкость при разливе в нее просто не доливают — вот этого не проверял.

3.1.5. Форматы кадров

Как и любая другая технология, Ethernet в процессе своего развития эволюционировал, поэтому вполне закономерно, что форматы кадров различных версий этого стандарта немного отличаются друг от друга. В этом пункте мы рассмотрим форматы кадров трех «версий»:

- 802.3/LLC (известен как Novell 802.2).
- Raw 802.3 (также известен как Novell 802.3).
- Ethernet DIX (он же Ethernet II).

Знание форматов кадров пригодится вам позже, когда вы уже прочитаете эту книгу и, быть может, еще пару книг по этому направлению. Формат кадра нужно знать при анализе кадра программами-анализаторами сетевого трафика. Считайте, что этот пункт — это некое справочное пособие — нет-нет, да и пригодится.

Формат кадров 802.3/LLC

Данный кадр состоит из восьми полей заголовка:

1. Поле преамбулы (preamble), состоящее из семи байтов со значением 10101010. Поле преамбулы используется для синхронизации приемника и передатчика.
2. Начальный ограничитель кадра (start-of-frame-delimiter) — указывает на начало кадра. Это один байт со значением 10101011.
3. Адрес приемника (destination address, DA). Может состоять из 2 или 6 байтов, но обычно используются 6 байтов для указания адреса компьютера-приемника. Первый бит этого поля указывает, является ли адрес индивидуальным (unicast) или групповым (multicast). Группой кадр предназначается группе узлов, может предназначаться всем узлам сети. В последнем случае адрес состоит из всех единиц и называется широковещательным (broadcast).
4. Адрес передатчика (source address, SA). Состоит из 2 или 6 байтов. На практике обычно используются 6 байтов. Первый бит всегда 0.
5. Длина (L) — задает длину поля данных. Поле «длина» (length) имеет длину 2 байта.
6. Поле данных (Data) — длина этого поля может быть от 0 до 1500 байт. Точнее, размер этого поля колеблется в пределах 46...1497 (1496) байтов, поскольку в поле данных встраивается кадр LLC, который занимает 3 или 4 байта. Об этом будет сказано ниже.
7. Поле заполнения (padding). Данное поле используется в том случае, если длина поля данных меньше 46 байт, например, равна 0. В этом случае поле заполнения будет содержать столько байтов, сколько нужно, чтобы обеспечить минимальную длину кадра. Например, если поле данных содержит 10 байтов, а поле заполнения будет содержать 46 − 10 = 36 байтов.
8. Поле контрольной суммы (Frame Check Sequence, FCS). Длина этого поля — 4 байта.

В поле данных (Data) данного кадра включается кадр подуровня LLC с флагами начала и конца кадра. Формат кадра LLC следующий:

- Флаг 01111110;
- поле DSAP (Destination Service Access Point) — точка входа сервиса назначения, 1 байт;

- поле SSAP (Source Service Access Point) — точка входа сервиса-источника, 1 байт;
- управляющее поле (Control), 1 или 2 байта;
- Данные;
- Флаг 01111110.

Поле данных кадра LLC используется для передачи пакетов протоколов IP, IPX и др. Данное поле необязательно и может отсутствовать.

Формат кадров Raw 802.3

Кадр Raw 802.3 также называется кадром Novell 802.3. Это практически тот же кадр, что и 802.3/LLC, но без заголовка LLC, то есть в этом кадре отсутствуют следующие поля:

- DSAP — адрес сервиса назначения;
- SSAP — адрес сервиса-источника;
- Control — управляющее поле.

Во всем остальном данный кадр аналогичен первому, за тем лишь исключением, что размер поля данных находится в пределах 46 — 1500 байтов, а не 1497 (1496) байтов, как в первом типе кадра, поскольку кадр LLC в поле данных не включается — его вообще нет.

Примечание.

Вам интересно, почему произошла такая путаница с полями кадров? Долгое время компания Novell вообще не использовала уровень LLC в своих операционных системах. Это обусловлено использованием протокола IPX, точнее его особенностями. Когда же без использования протокола LLC уже было не обойтись, компания начала использовать обыкновенные кадры 802.3/LLC, обозначив их как 802.2 в своих ОС, хотя на самом деле данный кадр является комбинацией 802.2 и 802.3.

Кадр 802.3/LLC *Таблица 3.2*

DA	SA	L	DSAP	SSAP	Control	Data	FCS
6	6	2	1	1	1 или 2	46...1497 или 1496	4

Кадр Raw 802.3 *Таблица 3.3*

DA	SA	L	Data	FCS
6	6	2	46...1497 или 1496	4

Формат кадров Ethernet DIX (Ethernet II)

Кадр Ethernet DIX имеет точно такую же структуру, как и Raw 802.3, но поле «длина» используется не для указания длины поля данных, а для указания типа протокола верхнего уровня, который «упаковал» свой пакет в данный кадр.

При передаче IP-пакетов через сети Ethernet, Fast Ethernet и Gigabit Ethernet используются именно кадры Ethernet DIX.

1.3.6. Общие характеристики сети Ethernet

Перед тем как перейти к рассмотрению новой технологии — Fast Ethernet, рассмотрим сводную таблицу спецификаций стандартов Ethernet (табл. 3.4).

Сводная таблица характеристик стандартов Ethernet *Таблица. 3.4*

Параметр сравнения	10Base-2	10Base-5	10Base-T	10Base-F
Максимальное число компьютеров в сегменте	30	100	1024	1024
Максимальная длина сегмента	185 м	500 м	100 м	2000 м
Максимальное расстояние между компьютерами	925	2500	500	2500 (2740 дл 10Base-FB)
Максимальное число концентраторов (повторителей)	4	4	4	4 (5 для 10Base-FB)
Кабель	RG-58	RG-8 или RG-11	UTP категори 3, 4 или 5	оптоволоконный кабель

3.2. Fast Ethernet — технология сегодняшнего дня

3.2.1. Fast Ethernet, как следующий шаг в развитии Ethernet

Скорость передачи данных в 10 Мбит/с, которую обеспечивал стандартный Ethernet, устраивала пользователей примерно лет пятнадцать — с момента появления технологии Ethernet и до появления новых компьютеров, использующих шину PCI. До появления шины PCI на рынке использовались две шины — ISA и EISA. Первой оснащались недорогие, пользовательские компьютеры. Вторую шину можно было встретить на более дорогих компьютерах, которые использовались в роли сервера сети. Пропускная способность первой шины — 8 Мбайт/с, а второй — 32 Мбайт/с. Разница, как вы видите, в 4 раза. Для сравнения 10 Мбит/с — это примерно 1,25 Мбайт/с (на практике это всего 1 Мбайт/с).

Шина PCI обеспечивает пропускную способность (опять же таки — теоретическую, которая на практике редко когда достигается) 133 Мбайт/с. Соотношения пропускной способности шин ISA/EISA/PCI и сети Ethernet: 1/8, 1/32 и 1/133, соответственно. Если с первыми двумя соотношениями можно было мириться, то с третьим уже никак.

Хотя, как вы догадались, дело не в простых математических расчетах. Шина PCI не просто же так появилась. Для создания более высокоскоростной шины были свои предпосылки. Первая, и самая весомая, — это увеличение объема обрабатываемых данных. Нормальный графический ролик нельзя создать на шине EISA — скорость будет слишком мала. Также увеличился объем пользовательских документов: новые версии программного обеспечения, новые возможности, и, как следствие, увеличение объема самих документов. Что и говорить, а проект средней сети в Corel Draw 10 занимает около 10 Мбайт, а небольшой видеоролик минут на 7-9 — около 29 Мбайт, о фильмах я уже вообще молчу. Не было бы «больших» документов, не появилась бы и шина PCI, и технология Fast Ethernet, которая обеспечивает в 10 раз бо́льшую производительность, чем Ethernet.

В 1992 начались разработки нового стандарта. На рынке информационных технологий, как и на любом другом, не обойтись без конкуренции, поэтому за разработку нового стандарта взялись две группы инженеров. Первая группа — это инженеры компаний 3Com, SynOptics и некоторых других. Вторая — фирмы Hewlett-Packard и AT&T. Первая группа организовала так называемый Fast Ethernet Alliance.

В результате конкуренции было разработано две независимые технологии:

- Fast Ethernet (3Com и SynOptics);
- 100VG-Any LAN (HP и AT&T).

Обе технологии стали стандартами IEEE осенью 1995 года. Первая технология была представлена в качестве стандарта IEEE 802.3u, а вторая — 802.12.

Чем же отличаются эти две технологии? Первая использует метод доступа CSMA/CD, а вторая технология использует совершенно новый метод доступа по требованию — Demand Priority. Первая технология сохранила совместимость с технологией Ethernet, благодаря чему завоевала бо́льшую популярность на рынке информационных технологий. Представьте себе, на сколько меньше была стоимость перехода на новую технологию: не нужно было менять сетевые адаптеры на всех компьютерах сети, а переход на Fast Ethernet можно было сделать последовательно. На наших просторах, ясное дело, более популярна Fast Ethernet.

3.2.2. Стандарты Fast Ethernet

В качестве среды передачи данных Fast Ethernet использует:

- неэкранированную витую пару категории 5 (четырехжильный кабель) или экранированная витая пара STP тип 1 — стандарт 100Base-TX;
- неэкранированную витую пару (UTP, Unshielded Twisted Pair) категорий 3, 4 или 5 (восьмижильный кабель) — стандарт 100Base-t4;
- оптоволоконный кабель — стандарт 100Base-FX.

Каждый стандарт подразумевает использование кабеля определенного типа. В настоящее время обычно используется восьмижильный кабель типа UTP — неэкранированная витая пара пятой категории.

3.3. Разные специальные сетевые технологии

3.3.1. Технология Token Ring

Стандарт Token Ring был разработан компанией IBM и стал основным конкурентом Ethernet, правда, не у нас, а там, на западе, и в США.

Скорость передачи данных в сетях Token Ring составляет 4 или 16 Мбит/с. Стандарт Token Ring использует неэкранированную (UTP) или экранированную (STP) витую пару как среду передачу данных. Максимальная длина кольца составляет 4000 м, а максимальное количество станций в сети Token Ring — 260.

В отличие от Ethernet, где используется метод доступа к среде CSMA/CD, в сетях Token Ring используется маркерный метод доступа, который заключается в следующем:

- компьютер имеет право передавать информацию, если он получил маркер — разрешение на передачу;
- один и только один компьютер в определенный момент времени имеет право на передачу информации;
- маркер передается по кругу (кольцу) — отсюда и название технологии (Token — маркер, Ring — кольцо).

Данный метод вообще исключает возможность возникновения коллизии — ни одна станция не будет пытаться получить доступ к среде без маркера.

В сетях Token Ring используются следующие типы пакетов:

- Маркер — компьютер не имеет права начинать передачу данных, пока не получит маркер.
- Пакет, содержащий данные или команды управления сетью.
- Пакет прекращения передачи — получив данный пакет, компьютер сразу же прекращает передачу данных.

3.3.2. Технология FDDI

FDDI (Fiber Distributed Data Interface) — оптоволоконный интерфейс распределенных данных. Сеть FDDI стала первой сетью, использующей оптоволоконный кабель в качестве среды передачи данных. Работы над созданием этой сети начались еще в 80-ые годы прошлого столетия. В 1988 году группа института ANSI приняла начальную версию стандарта FDDI, обеспечивающую скорость передачи данных до 100 Мбит/с с максимальной длиной кольца передачи данных до 100 км.

Технология FDDI во многом похожа на технологию Token Ring — ее разработчики взяли от Token Ring все лучшее и усовершенствовали это. В основном FDDI используется как магистральная сеть передачи информации, например, для соединения нескольких зданий одной компании в единую сеть.

Несмотря на преимущества технологии FDDI — большую скорость передачи данных и большое расстояние передачи этих данных, она до сих пор не пользуется популярностью. Основная причина — высокая стоимость оборудования для сети FDDI — за последние 15 лет существенно цены не изменились, и до сих пор остаются достаточно высокими. Например, трансивер сети FDDI, преобразующий электрический сигнал в оптический, обойдется в несколько тысяч долларов — из расчета, что один оптоволоконный порт стоит около 750 долларов, а один порт на витой паре — около 450 долларов. Вот и посчитайте: восемь оптоволоконных портов вам обойдутся в 6000 долларов.

Сравнительные характеристики сетей Token Ring, FDDI и Ethernet представлены в табл. 3.5.

Сравнительные характеристики сетей FDDI, Token Ring и Ethernet *Таблица 3.5*

Характеристика	Ethernet	Fast Ethernet	Token Ring	FDDI
Скорость передачи данных, Мбит/с	10	100	4 или 16	100
Топология	Шина/Звезда	Шина/Звезда	Звезда/Кольцо	Двойное кольцо
Метод доступа	CSMA/CD	CSMA/CD	Маркер	Часть времени оборота маркера
Среда передачи данных	Толстый коаксиал, тонкий коаксиал, витая пара категории 3, оптоволокно	Витая пара категорий 3,4, оптоволокно	Экранированная и неэкранированная витая пара, оптоволокно	Оптоволокно, неэкранированная витая пара категории 5
Максимальное количество компьютеров	1024	1024	260	500
Максимальная длина сети	2500 м	200 (272 для оптоволокна)	4000 м	200 км — 100 км на кольцо

3.3.3. Технология Gigabit Ethernet — следующий шаг развития Ethernet

В ходе развития технологии Fast Ethernet возникала необходимость в быстрой магистральной технологии. Представьте, что у нас есть два здания с общим числом компьютеров около двух сотен. Эти два здания нужно объединить в одну сеть. Не объединишь их же тем же Fast Ethernet — магистраль между зданиями будет очень «узкой», внутри здания скорость передачи данных будет довольно высокой, а между зданиями — очень низкой.

Единственной магистральной технологией до 1996 года была FDDI. Но вы сами знаете стоимость FDDI-оборудования — она довольно высока даже для витой пары, не говоря уже про оптоволокно (примерно 750 долларов за порт).

Летом 1996 года была создана группа 802.3z института IEEE. Основным заданием этой группы стала разработка технологии, совместимой с Ethernet и Fast Ethernet, но со скоростью передачи данных в 1000 Мбит/с.

Окончательная версия стандарта 802.3z была принята летом 1998 года. Новая технология была названа Gigabit Ethernet.

Что же общего у новой технологии с Ethernet и Fast Ethernet? Во-первых, были сохранены форматы кадров Ethernet. Во-вторых, по-прежнему использовался метод доступа CSMA/CD. В-третьих, используются те же кабели, что и для технологий Ethernet и Fast Ethernet: коаксиал, витая пара и оптоволокно.

Минимальный размер кадра (без преамбулы) был увеличен с 64 до 512 байтов, а время двойного оборота — до 4095 битовых интервалов, что позволяет увеличить диаметр сети до 200 м.

Максимальная длина кабеля зависит от самого кабеля. Для многодомного оптико-волоконного кабеля (стандарт 1000Base-SX) предельная длина кабеля составляет:

- 220 м, при использовании кабеля 62,5/125;
- 500 м, при использовании кабеля 50/125.

Для однодомного оптоволокна (стандарт 1000Base-LX) максимальная длина кабеля равна 5000 м. В качестве среды передачи данных можно использовать твинаксиальный кабель, но в этом случае максимальная длина кабеля равна всего 25 метров.

Примечание.

Буква «S» в спецификации Gigabit Ethernet означает передачу информации на небольшие расстояния (s — short, короткий), а буква «L» — передачу информации на значительные расстояния (l — long, длинный).

Теперь поговорим о стоимости оборудования. Стоимость оборудования для организации сети Gigabit Ethernet не очень высока по сравнению с FDDI, но заоблачная относительно обыкновенной Fast Ethernet (см. табл. 3.6).

Сравнительная таблица стоимости оборудования Fast Ethernet и Gigabit Ethernet *Таблица 3.6*

Fast Ethernet		Gigabit Ethernet	
Наименование	**Цена**	**Наименование**	**Цена**
Сетевой адаптер LANTECH 10/100 : Realtek 8139	$4,5	Сетевой адаптер LANTECH 10/100/ 1000 Gigabit Ethernet 1000LX (UTP)	$32
		Сетевой адаптер 3Com 3C996-SX Gigabit SX Server fiber	$570
Коммутатор LANTECH 24 порта FE2400	$93	Коммутатор 24port Planet GSW-2400S WEB-SMART Gigabit 10/100/1000	$730

Как вы видите, стоимость одного коммутатора Gigabit Ethernet почти в восемь раз больше, чем Fast Ethernet, не говоря уже о стоимости кабеля — одно дело проложить 100 метров витой пары, а другое — 100 метров оптоволокна. Хотя на коммутаторе можно сэкономить: в продаже имеются 24-портовые коммутаторы, в которых только 2 порта поддерживают Gigabit Ethernet. В принципе, это оптимальное решение: вам же нужна только магистраль, а это 1-2 порта. Зачем платить за все 24 порта? 24-портовый коммутатор с двумя портами Gigabit Ethernet стоит в пределах 300...400 долларов в зависимости от фирмы-производителя и выполняемых ним функций.

На небольших и средних предприятиях, а также в домашних сетях технология Gigabit Ethernet не нашла применения. И дело даже не в стоимости оборудования: не так уж она и высока. Просто пока у рядовых пользователей не будет в распоряжении достаточно мощная для Gigabit Ethernet техника, потребности в этой технологии не будет. Подумайте: стоит ли использовать Gigabit Ethernet со скоростью 1000 Мбит/с, если скорость шины PCI — 133 Мбит/с. Все равно больше, чем позволяет шина PCI, вам компьютер не примет и не передаст. Поэтому в ближайшие пять лет дома коммутаторы Gigabit Ethernet вы не увидите...

3.3.4. Беспроводные технологии

Технология Radio Ethernet — беспроводная сеть Ethernet

Технология Radio Ethernet позволяет передавать ваши данные «по воздуху». Для передачи используется направленная радиоантенна — отсюда и название Radio Ethernet. Данная технология пользуется достаточной популярностью у домашних пользователей, как средство доступа к Internet.

Честно говоря, я немного разочаровался в этой технологии: как только на улице плохая погода (дождь, сильный ветер), скорость передачи информации падает в десятки раз. Пару раз вообще не было связи из-за плохой погоды. Поэтому, если вам нужно действительно надежное и постоянное соединение с Internet, лучше используйте выделенную линию — хотя скорость и не такая высокая, как в случае с Radio Ethernet, зато надежно. И не нужно слушать продавцов Radio Ethernet, мол, кабель своруют. А антенну, что украсть не могут? Ее еще быстрее украдут, поскольку кабель выделенной линии находится в относительно защищенных местах, а антенна — на самом открытом месте на крыше дома — иначе она не сможет принимать и передавать радиосигнал.

Технологию Radio Ethernet следует применять в следующих случаях:

- Когда нужно обеспечить связь мобильных абонентов, например, мобильных пользователей или передвижных офисов. Второй случай больше подходит, поскольку антенна Radio Ethernet довольно большая и пользователю с ней будет неудобно, учитывая, что она в несколько раз больше его ноутбука. А вот на крышу микроавтобуса антенну установить можно.
- Когда невозможно провести выделенную линию — и такое случается. Иногда данное удовольствие стоит так дорого, что проще купить радиоантенну.
- Когда связь нужна именно сейчас, то есть, у вас нет времени ждать, когда вам проведут выделенную линию. Или же Radio Ethernet можно использовать временно — пока у вас нет выделенной линии.

При использовании Radio Ethernet нужно помнить о том, что это все-таки радиосигнал, который может искажаться по пути к провайдеру. Поэтому среднее (и рекомендуемое) расстояние до провайдера — до 15 километров. Максимальное расстояние — до 50 метров, но это в идеальных условиях (например, на открытой местности — в поле)

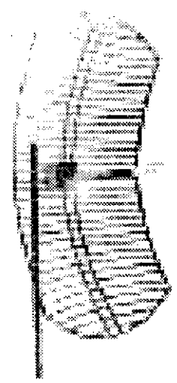


Рис. 3.1. *Параболическая направленная радиоантенна (24 dBi Parabolic Grid Antenna)*

Средняя скорость передачи данных — до 6 Мбит/с. Ясное дело, что у вас она будет ограничена провайдером — если у самого провайдера канал всего в 4 Мбит/с, то 6 Мбит/с у вас быть никак не может. Максимальная скорость передачи данных — 11 Мбит/с (чуть выше, как у обычного Ethernet). Что радует, так это число компьютеров такой сети, которое неограниченно.

Для подключения клиента к сети Radio Ethernet нужно следующее оборудование:

- PCMCIA Radio Card 11 Mbit/sec — сетевая радиокарта 11 Мбит/с.
- ISA Adapter Card — PCMCIA переходник для радиокарты.

- 24 dBi Parabolic Grid Antenna, 2.4-2.4835 GHz — направленная параболическая радиоантенна.
- WRC 600 (4.0 dB per 100 ft. @ 2.4 GHz) — высокочастотный кабель.
- N-Type Connector for WRC600 Cable — разъем для кабеля.
- Standard Lucent ORINOCO WaveLan Jumper Cable — переходник для фирменного разъема.

Стоимость клиентского оборудования обычно не превышает 250 долларов. Многие провайдеры вообще предоставляют оборудование в аренду, то есть вам вообще ничего не нужно за него платить: вы платите только за Internet. Тогда при отключении или смене провайдера вам нужно будет отдать оборудование.

Сеть WiFi

Сеть WiFi — это беспроводная сеть, позволяющая связать вместе огромный спектр различных устройств. Клиентами сети WiFi могут быть компьютеры, КПК (карманные ПК), мобильные телефоны, ноутбуки. Сети WiFi описаны в стандарте IEEE 802.11. Идея WiFi заключается в следующем: доступ к Интернету по WiFi осуществляется через так называемые точки доступа, радиус действия которых составляет всего 100 м.

Точки доступа связываются с центральным маршрутизатором, который и обеспечивает связь со всемирной паутиной. Точки доступа обычно устанавливаются в многолюдных местах: гостиницах, кафе, Интернет-клубах. У нас WiFi не очень распространена, но на Западе эта технология уверенно развивается и со временем получить доступ к Интернету по WiFi с помощью ноутбука можно будет практически в любой точке Европы.

Для работы по WiFi вам понадобится специальная WiFi-карта. Современные модели ноутбуков, КПК и мобильных телефонов уже оснащены WiFi-адаптерами, а для более старых ноутбуков вам понадобится WiFi-адаптер, например, Nokia D211 (см. рис. 3.2).

Что же касается безопасности, то данную технологию лучше не использовать для критически важных объектов, поскольку имеются сведения (`http://www.hardwareportal.ru/cgi-bin/news_show.pl?id=23yv80Cx`), что WiFi-сеть легко «заклинить» при помощи обыкновенного КПК.

Если вы заинтересовались в приобретении WiFi-карты Nokia D211, прочитать детальные технические характеристики можно по адресу `http://www.nokia.com/nokia/0,,1449,00.html`

Рис. 3.2. *WiFi-адаптер Nokia D211*

3.3.5. Технология PowerLine — сеть через электрическую розетку

Что это такое и как работает

Все, кто хотя бы один раз в жизни прокладывал сеть собственными руками, скажут, что это занятие не из приятных. Одно дело — проектировать сеть, совсем другое — заниматься монтажом оборудования и прокладыванием кабелей. Конечно, когда все компьютеры находятся в одной комнате, особых проблем с кабелем, как правило, витой парой не возникает. Но когда нужно объединить в сеть два, три, четыре, пять или более этажей, невольно начинаешь думать: «Кто бы за меня все это сделал???».

Конечно же PowerLine! PowerLine (Powerline Communications) — это семейство технологий связи, использующее в качестве физической среды передачи информации существующую сеть электропитания (220 В или 120 В).

Выходит, чтобы объединить в одну единую сеть целый жилой дом, не нужно прокладывать кабели, монтировать различные сетевые устройства и заботиться о том, чтобы однажды ночью они не исчезли вместе с кабелем. Среда передачи данных уже есть — это обычная электропроводка. И количество этажей не играет особой роли. Удобно? Еще бы. Кроме этого, мы получаем еще одно преимущество: безопасность передачи данных — перехватить данные в электросети не так уж просто, если сравнивать с обычной Ethernet-сетью. К тому же используется аппаратное шифрование потока данных, о котором мы поговорим позже.

Вам мало одного дома? Вы хотите подключить еще один? Технология Powerline позволяет передавать данные на расстояние до десяти километром. Естественно, если мы что-то приобретаем, то нужно что-то отдать взамен. В нашем случае мы жертвуем скоростью передачи.

Если объекты находятся на расстоянии более двух километров, скорость передачи данных падает до 0,05 Kbps (максимум 50 Kbps). Поэтому для связи удаленных объектов целесообразнее использовать другие технологии, например, Gigabit Ethernet — дорож,е зато надежнее или RadioEthernet — дешево и сердито.

Скорость передачи данных и расстояние

В зависимости от расстояния между объектами изменяется скорость передачи данных:

- **Высокоскоростной обмен** (High baud rate). В этом режиме обеспечивается передача данных на расстоянии до нескольких сотен метров. Скорость передачи данных обратно пропорционально зависит от

расстояния, минимальная скорость передачи в высокоскоростном режиме — 100 Kbps, максимальная — 14 Mbps (практически никогда не достигается). Данный вариант идеально подходит для создания небольшой SOHO-сети или объединения в одну сеть компьютеров друзей, живущих в одном доме. Однако подключить сразу все желаемые PLC-устройства мы не сможем: может не хватить полосы пропускания, а она для PLC-устройств составляет не более 10 Mbps. Да, видео в реальном времени передавать не получится, но для передачи файлов с приемлемой скоростью — вполне хватить. О максимальной скорости, а также о полосе пропускания мы еще поговорим чуть позже.

- **Среднескоростной обмен** (Medium baud rate) — предназначен для передачи информации на средние расстояния — до двух-трех километров. При этом максимальная скорость передачи данных в этом режиме составляет 50 Kbps, а минимальная — 0,05. В принципе, если подумать, 50 Kbps — это не так уж и мало, если учесть, что существующие линии телефонной связи, особенно аналоговые, еле обеспечивают надежную передачу данных на скорости 33,6 Kbps. Мой модем, подключенный к аналоговой АТС, работает по такому сценарию: сначала подключается на скорости 33,6 Kbps, затем (минут через 15-20) сбрасывает скорость до 28,8 Kbps, потому скорость то понижается (до 21 Kbps), то повышается (до 28,8 Kbps).
- **Низкоскоростной обмен** (Low baud rate). Обеспечивает передачу данных на расстояние более 10 километров. Максимальная скорость передачи — 0,05 Kbps. Данный режим будет полезен для передачи какой-нибудь служебной информации небольшого объема.

Как подключиться к электросети?

Предположим, что у нас есть самый обыкновенный компьютер, снабженный самым обыкновенным Ethernet-адаптером (имеется в виду FastEthernet). Как можно его подключить в PLC-сеть? Неужели прямо в розетку? Почти: для подключения компьютера к электросети используется специальный адаптер — Powerline to Ethernet adapter. Вот он-то и подключается к электросети, а Ethernet-адаптер подключается к нему. На рис. 3.3 изображен пример небольшой домашней сети, состоящей из трех компьютеров, использующей технологию Powerline.

Один из компьютеров подключается непосредственно к среде передачи данных, то есть к электропроводке, используя адаптер Powerline to Ethernet. На данном компьютере должен быть установлен Ethernet-адаптер. Другие два компьютера подключены в нашу домашнюю сеть через самый обыкновенный Ethernet-коммутатор (switch), который, в свою очередь, подключается к электросети с помощью адаптера Powerline to Ethernet. Далее, к одному из компьютеров подключен модем. Если правильно настроить программное обеспечение, этот компьютер будет выступать в роли Internet-шлюза и все компьютеры получать доступ к Internet.

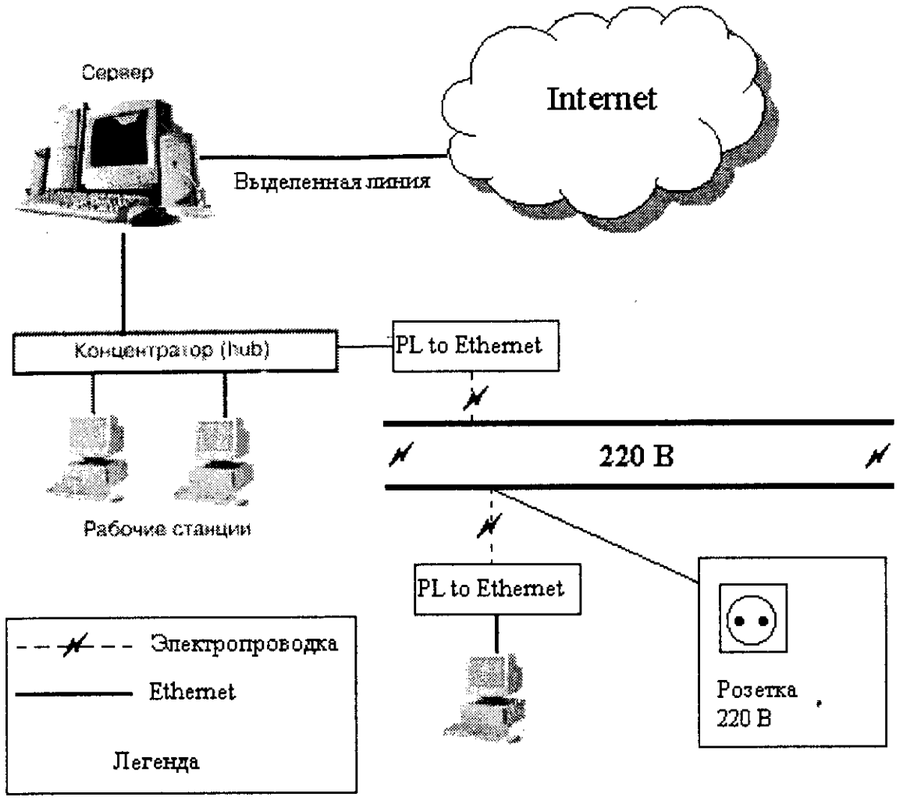


Рис. 3.3. *Пример небольшой сети с использованием технологии Powerline*

На вашем компьютере нет сетевой платы? Не беда: кроме адаптера Powerline to Ethernet существуют адаптеры Powerline to USB, позволяющие использовать USB-порт компьютера вместо сетевой платы. Такой адаптер целесообразнее использовать на одиночных компьютерах, как в нашем случае. Во-первых, не нужно покупать сетевую плату, а во-вторых, адаптер Powerline to USB стоит дешевле, чем адаптер Powerline to Ethernet (цена зависит от модели и производителя).

А что делать, если у вас старенький компьютер без USB-порта? Тогда есть два выхода: или купить специальный USB-адаптер, или специальную PowerLine PCI-карту. В первом случае у вас появится так необходимый вам USB-порт, к которому можно подключить адаптер Powerline to USB, а во втором — вы будете подключаться к электросети с помощью купленной вами Powerline PCI-платы. PLC-устройства, выполненные в виде PCI-платы, являются самыми дешевыми, но наименее распространенными.

Устройства производства Planet Technology

Рассмотрим два устройства производства Planet Technology:

- Powerline to Ethernet converter (PL-101E);
- USB to Powerline Network Adapter (PL-101U).

Первое устройство позволяет подключаться к электросети с помощью сетевого адаптера, а второе представляет собой сетевой адаптер, подключаемый к USB, и способный работать по электросети — такой себе набор 2 в 1. Устройства представлены на рис. 3.4 и 3.5 соответственно.

Оба устройства поддерживают спецификации HomePlug PowerLine Alliance v1.0 и USB Spec 1.1. Основные технические характеристики:

- Максимальная скорость до 14 Mbps;
- Для надежности передачи данных используют кодирование с ключом 56 бит (DES);
- Максимальное расстояние — до 90 м;
- Метод сетевого доступа — CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance — метод коллективного доступа с избежанием коллизий);
- Поддержка QoS (Quality of Service, IEEE 802.3u);
- Полоса занимаемых частот для обмена данными: 4,3 — 29,9 MHz;
- Схема модуляции — OFDM, прямая коррекция ошибок (FEC, Forward Error Correction).

Стоимость каждого устройства — около $130.

Примечание.

56-битная система шифрования окажется бесполезной, если вы забудете изменить пароль по умолчанию. Данный пароль должен быть одинаковым на всех устройствах вашей сети.

Рис. 3.5. *USB to Powerline Network Adapter (PL-101U)*

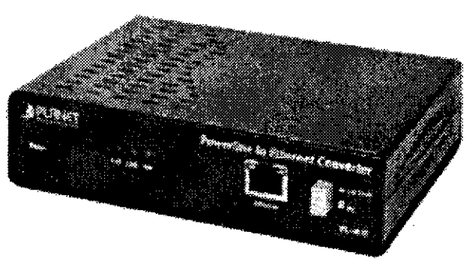


Рис. 3.4. *Powerline to Ethernet converter (PL-101E)*

Выбор устройства

Табл. 3.7 поможет вам выбрать ваше PLC-устройство.

Технические характеристики PCL-устройств *Таблица 3.7*

Наименование	Производитель	Модель	Индикаторы LAN/USB	Чипсет	Цена, $
Powerline to Ethernet	Planet Technology	PL-101E	Link-LAN, 100 Mbps	Intellion INT5130A/100A	130
USB to Powerline Network Adapter	Planet Technology	PL-101U	Нет	Intellion INT5130A/100A	130
Ethernet to Power line bridge	Dynamix	PL-E	Link-LAN, 100 Mbps	Intellion INT5130A/100A	155
Home Plug USB adapter	Dynamix	PL-U	Нет	Intellion INT5130A/100A	155
Powerline bridge (OEM)	Surecom	PLB11	Link, 10, 100 Mbps, Col	Intellion INT51X1A	110
Powerline USB adapter (OEM)	Surecom	PLU11	Нет	Intellion INT51X1A	100
HomePlug USB adapter	Surecom	NE-6201/A1	Нет	Intellion INT5130A/100A	110
HomePlug Ethernet bridge	Surecom	NE-6211/A1	Link-act	Intellion INT5130A/100A	110

Примечание.

В табл. 3.7 указана приблизительная цена, которая может измениться в зависимости от различных факторов.

Тестирование

К сожалению, у меня не получилось раздобыть все перечисленные в табл. 3.7 устройства, поэтому ограничимся теми, что были: Powerline to Ethernet converter (PL-101E) и USB to Powerline Network Adapter (PL-101U).

Установка устройства происходит без проблем. USB-адаптер операционная система Windows 2000 определила как Safely Remove Hardware, после чего был проинсталлирован драйвер с компакт-диска.

Ethernet-устройства вообще не требуют никакого драйвера, нужно только изменить пароль по умолчанию (обычно это слово «HomePlug»). Напомню, что пароль должен быть одинаковым на всех PLC-устройствах.

На прилагаемом компакт-диске также находилась программа конфигурации, позволяющая изменить параметры устройства, а также оценить скорость передачи данных между устройствами.

Несмотря на то, что заявленная максимальная скорость передачи данных равна 14 Mbps, на практике она составляла 5-6 Mbps.

При передаче файла объемом 10 Мб наилучший результат был следующим: 5,55 Mbps. Всего было сделано 10 попыток в идеальных условиях: оба устройства находились в пределах одной квартиры, и не было включено ни одно устройство, способное создавать помехи — даже холодильник был временно отключен.

При включении водонагревателя, холодильника и микроволновой печи скорость передачи этого же файла составила 3,14 Mbps. Очень даже неплохо, учитывая, что сигнал преодолел сопротивление в 70 Ом и несколько автоматов-выключателей.

В отличие от PLC-устройств типа HomePlug, существует еще один тип подобных устройств — HomePNA, позволяющие для передачи данных использовать обычные телефонные линии. А что если подключить наши HomePlug (PLC)-устройства к телефонной линии? Они работают, причем их работа оценивается утилитой мониторинга, как «Excellent», то есть с максимальной скоростью. В то же время, мы можем набрать номер и нормально разговаривать по телефону — качество голосовой связи не пострадало.

Теоретически, можно подключить PLC-устройства и к радио, то есть к ретрансляционной сети. Однако я не стал этого делать.

В начале пункта мы акцентировали внимание не только на удобстве, но и на надежности. Мол, самые надежные и самые безопасные... Неужели нет способа «завалить» PLC-сеть? Способ есть: соедините сетевым кабелем два устройства Ethernet to PL и увидите, что будет. Если боитесь экспериментировать, скажу, что в результате блокируется работа всех устройств в подсети.

Выводы

Теперь подытожим все вышесказанное. PowerLine-устройства являются самыми удобными в плане внедрения в уже существующую среду передачи информации — электросеть. В отличие от устройств HomePNA, использующих для передачи информации телефонные кабели, PLC-устройства являются более удобными, поскольку телефонный провод есть не в каждой комнате, а вот розетка, наверняка найдется.

Хотя заявленная пропускная способность 14 Mbps, на практике она составляет 6 Mbps, это не так уж и мало. Сравнивать PLC-устройства с сетью FastEhternet не стоит — они находятся в разных весовых категориях. Гораздо корректнее сравнивать PowerLine-устройства с RadioEthernet и другими беспроводными сетями.

Что лучше RadioEthernet или PowerLine сказать однозначно тоже нельзя: это зависит от того, как вы хотите использовать данные технологии. Если вы хотите объединить в сеть несколько компьютеров друзей, находящихся

в одном доме, лучшим выбором окажется PowerLine. А если объекты находятся на расстоянии более 1 километра, использовать PowerLine вряд ли целесообразно: при таком расстоянии скорость передачи данных будет очень низкой.

Используемое 56-битное шифрование DES создает дополнительный барьер при перехвате информации. Также стоит отменить, что шифрование выполняется на аппаратном уровне и вам не нужно заботиться о различных программных средствах для шифрования трафика, как в случае с Ethernet-сетью.

Стоимость PowerLine-устройств на сегодняшний день пока высока. Например, чтобы объединить в сеть два компьютера, вам понадобится минимум $200. При использовании FastEhternet вам понадобятся всего лишь два сетевых адаптера ($5-10 каждый) и до 100 метров витой пары пятой категории (от $20 за 100 метров).

Как известно, если нужно соединить сетью два компьютера, можно обойтись без концентратора/коммутатора, поэтому итоговая стоимость такой сети 40-50 долларов: в четыре раза ниже, чем стоимость PowerLine-сети. Однако, мы не учли стоимость прокладки кабеля (если вы будете заниматься этим сами, то стоимость будет определяться временем, потраченным на монтаж такой сети) и возможного ремонта помещения, если придется прокладывать кабель через стену.

Кроме стоимости ограничивает распространение PLC-устройств максимальная полоса пропускания. Да, мы можем объединить в сеть компьютеры, которые расположены на разных этажах и даже в разных подъездах (если это жилой дом), но мы не можем объединить в сеть *все* компьютеры, находящиеся в одном доме. Ограниченная полоса пропускания не позволяет работать с относительно высокой скоростью более чем десяти-пятнадцати PLC-устройствам.

Монтаж сети

Еще раз повторюсь, что сегодняшним стандартом, на основе которого строятся 90% (а то и более) локальных сетей, является Fast Ethernet. Эта технология является сегодня наиболее оптимальной как по техническим, так и ценовым параметрам.

Остальные технологии следует использовать в каких-то особых случаях, например, вам нужно, чтобы сеть строилась на толстом коаксиальном кабеле, чтобы была меньше вероятность его повреждения или пробоя изоляции (в этом случае придется пожертвовать скоростью передачи). В общем предыдущая глава как раз и была направлена на то, чтобы вы определились, какая же вам все-таки технология нужна. И если никаких особых условий у вас нет, то используйте Fast Ethernet — и будете довольны.

Далее в этой главе рассмотрены различные варианты монтажа сети в зависимости от той или иной технологии. Отдельно рассмотрено построение сети по технологии Fast Ethernet.

4.1. Построение сети Ethernet

Как мы уже знаем, существует несколько спецификаций сетей Ethernet в зависимости от используемой среды передачи данных:

- коаксиальный кабель с диаметром 0,5 дюйма, «толстый» коаксиал — стандарт 10Base-5;
- коаксиальный кабель с диаметром 0,25 дюйма, «тонкий» коаксиал — стандарт 10Base-2;
- неэкранированная витая пара (UTP, Unshielded Twisted Pair) — стандарт 10Base-T;
- оптоволоконный кабель — стандарт 10Base-F.

Помню, в свое время на лекции по сетевым технологиям студентам был задан вопрос: что означает слово Base в названии спецификации? Тогда ради интереса я узнал его назначение. Число 10 — это скорость передачи в Мбит/с. Слово `Base` — это метод передачи данных на одной, базовой (отсюда и `base`) частоте 10 МГц. Последний символ — это тип кабеля.

4.1.1. Тонкий коаксиал: 10Base-2

Необходимое оборудование

Начнем со спецификации 10Base-2. Это самый простой и самый дешевый способ объединить в сеть несколько компьютеров.

В качестве среды передачи информации используется коаксиальный кабель с внешним диаметром около 5 мм. Как правило, такой кабель имеет маркировку:

- RG-58/U
- RG-58 A/U
- RG-58 C/U

Компьютеры к кабелю подключаются с помощью Т-образных BNC коннекторов. «Ножка буквы Т» подключается к сетевому адаптеру, а «концы буквы Т» — к концам разрыва кабеля. К концам кабеля подключаются специальные заглушки — терминаторы с сопротивлением 50 Ом.

Основная задача терминаторов — это поглощение распространяющихся по кабелю сигналов и отраженных сигналов. Если ваш сегмент кабеля не будет оснащен терминаторами, то одни узлы будут получать очень мощные сигналы, а другие — очень слабы. Терминаторы согласовывают величину сигнала, поэтому их еще называют *согласующими терминаторами.*

Простейшая сеть стандарта 10Base-2 приведена на рис. 4.1.

Оборудование, которое нам понадобится для объединения в сеть 10Base-2 трех компьютеров, приведено в табл. 4.1. На рис. 4.2, 4.3 и 4.4 можно увидеть, как выглядят сетевые комплектующие.

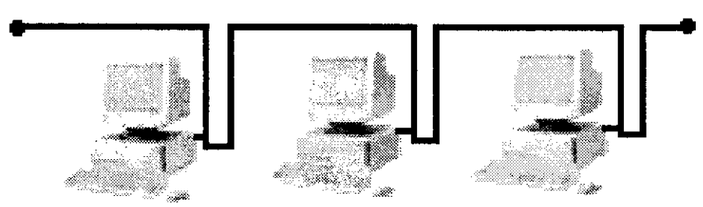


Рис. 4.1. *Простейшая сеть стандарта 10Base-2*

Оборудование, необходимое для создания сети 10Base-2 *Таблица 4.1*

Наименование	Количество	Ед. изм.	Цена	Сумма
Компьютеры	3	шт.	–	–
Сетевые адаптеры 10Mbit, PCI, BNC+RJ45	3	шт.	5	15
Кабель RG-58	10	м.	0,25	2,5
BNC терминатор	2	шт.	0,5	1
BNC коннектор	3	шт.	0,5	1,5

Итого: 20 вечнозеленых единиц.

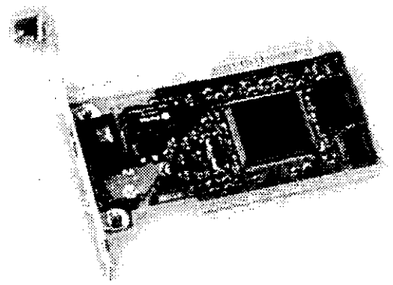


Рис. 4.2. *Сетевой адаптер Intel EtherExpress 10/100 Pro Plus*

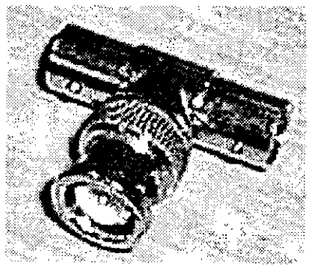


Рис. 4.3. *T-коннектор*

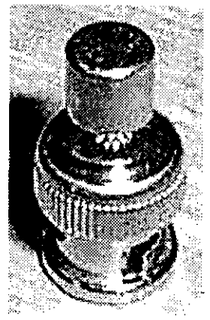


Рис. 4.4. *BNC-терминатор без заземления*

Как видите, стоимость построения такой сети весьма незначительна, но за все приходится расплачиваться: если где-то мы экономим, то это обязательно где-нибудь и проявится. В технологии 10Base-2 это проявляется плохой помехозащищенностью тонкого коаксиала и большой вероятностью обрыва кабеля, если кабель проложен вне помещения. В этом случае лучше использовать для прокладки кабеля защитные короба. Хотя есть и положительные моменты при использовании тонкого коаксиала — разрыв кабеля диагностируется очень просто — сеть просто перестает работать.

Правила построения сети 10Base-2

При построении сети стандарта 10Base-2 нужно придерживаться следующих правил:

- Правило 5-4-3: в сети 10Base-2 может быть не более 5-ти сегментов, 4-х повторителей и 3-х нагруженных сегментов, то есть таких сегментов, в которых имеются компьютеры (2 сегмента должны быть «пустыми»). Данное ограничение связано с задержками распространения сигнала.

- Максимальная длина сегмента без повторителей составляет 185 метров.
- Сегмент должен иметь на концах терминаторы.
- Минимальное расстояние между компьютерами — 1 метр (на кабеле имеется специальная разметка каждый метр).

Напомню, что повторитель (repeater) — это устройство, повышающее длину сегмента путем его разбиения на несколько сегментов. Кроме того, повторители увеличивают сигнал и повышают надежность сети. Например, если сеть 10Base-2 не использует повторителей, то при обрыве кабеля вся сеть будет недоступна. Если же повторитель разбивает сеть на два сегмента, то будет недоступен только тот сегмент, в котором произошел обрыв кабеля.

10Base-2, как домашняя сеть

Вы хотите использовать 10Base-2 в качестве домашней сети? Сразу хочу вас отсоветовать! Не надо! Я, конечно, понимаю, что это самый дешевый вариант, а всю зарплату или хотя бы ее половину на построение сети выкладывать не хочется (один коммутатор стоит 20-30 долларов). Но не делайте то, о чем пожалеете — это выброшенные на ветер деньги, все равно потом будете переделывать. Сеть 10Base-2 — это давно забытое старое. Сейчас объясню почему. Для чего вам нужна домашняя сеть? Правильно, обменяться с соседями фильмами и поиграть в сетевые игры. Ну, может еще организовать небольшой шлюз для доступа всего подъезда к Internet.

Начнем с фильмов. Реальная скорость передачи по сети 10Base-2, как показывает практике, не превысит 6-7 Мбит/с. И это при условии, что только вы один будете копировать этот фильм, и вообще, что никто кроме вас не будет пытаться ничего передать. Теперь считаем: 7 Мбит/с — это приблизительно 0,875 Мбайт/с. Средний фильм занимает 650 Мбайт. Рассчитываем время: 650 / 0,875 = 743 секунды. Это около 12 минут. Многовато, вам так не кажется? Моя домашняя сеть со включенной службой QoS в Windows XP способна скопировать 1,2 Гб за 3 минуты 50 секунд — ради интереса сам время замерил. После отключения QoS стало еще быстрее.

Если построить 100-мегабитную сеть на основе витой пары и коммутатора (switch), то такая сеть будет в меньшей мере подвержена коллизиям, чем сеть на коаксиале. Это означает, что если весь ваш подъезд играет в Counter Strike по сетке, то в Internet вы нормально не поработаете (при условии, что сеть 10Base-2).

4.1.2. Толстый коаксиал: 10Base-5

Необходимое оборудование

Сеть стандарта 10Base-5 использует «толстый» коаксиальный кабель с внешним диаметром 0,5 дюйма. Такими являются кабели с маркировками RG-8 и RG-11.

Сегмент без повторителя может быть не более 500 метров и обязательно должен содержать на концах терминаторы 50 Ом (см. рис. 4.5).

Рис. 4.5. *BNC-терминатор с заземлением*

Компьютер подключается к кабелю с помощью специального устройства — трансивера (см. рис. 4.6), предназначенного для приема и передачи информации (transceiver = transmitter & receiver). Кроме приема и передачи информации трансивер используется для определения коллизий.

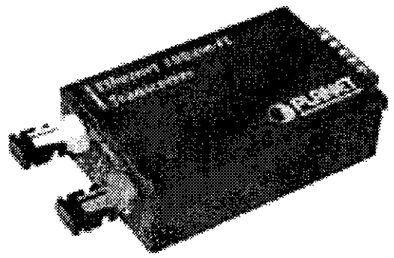


Рис. 4.6. *Трансивер Planet ET-118*

Трансивер подключается к кабелю и питается от сетевого адаптера. Сетевой адаптер подключается к трансиверу кабелем AUI (Attachment Unit Interface). Длина такого кабеля не может превышать 50 метров. Для использования AUI нужно, чтобы сетевой адаптер был оснащен специальным разъемом — DB-15.

К одному сегменту можно подключить не более 100 трансиверов, причем минимальное расстояние между трансиверами не должно быть меньше 2,5 метра. На кабеле RG-8 (11) через каждые 2,5 метра имеется разметка для подключения трансивера.

Стоит ли строить сеть 10Base-5?

Как и 10Base-2, сеть 10Base-5 давно морально устарела. Прежде всего, современного пользователя не устроит скорость передачи данных — 10 Мбит/с. Даже если данный параметр для вас не критичен, то уже проще и дешевле построить сеть Fast Ethernet: во-первых, быстрее, во-вторых, проще, в-третьих, практичнее.

Если быть более конкретным, то к основным недостаткам 10Base-5 можно отнести:

- Требование специальных сетевых адаптеров с разъемом DB-15.
- Высокая стоимость оборудования: кроме стоимости сетевого адаптера вам еще придется заплатить за трансиверы. А трансивер нужен для каждого компьютера. Стоит он немало — от 25 до 30 долларов. Помните, пример с тонким коаксиалом: тогда стоимость всей сети из трех компьютеров обошлась в 35 долларов, а тут только три трансивера будут стоить минимум 75 долларов. Подумайте: за 25 долларов можно купить коммутатор сети Fast Ethernet (8-портовый) и подключить к нему все компьютеры сети!
- Высокая стоимость кабеля.
- Требование специального инструмента для прокладки кабеля: с помощью молотка и отвертки кабель вы не обожмете. Инструмент тоже денег стоит.
- Сложность прокладки кабеля из-за его жесткости.

Конечно, есть и обратная сторона медали: в отличие от «тонкого» коаксиала, «толстый» коаксиал значительно труднее повредить, рабочую станцию можно перемещать в пределах кабеля AUI (его максимальная длина — 50 метров). Но эти два достоинства полностью перекрываются вышеперечисленными недостатками.

4.1.3. Витая пара: стандарт 10Base-T

Необходимое оборудование

Вот на эту технологию нужно обратить особое внимание, поскольку витая пара очень часто используется на наших просторах, я бы даже сказал, что это стандарт де-факто для построения локальных сетей на территории бывшего СНГ. На популярности витой пары сказывается относительно небольшая стоимость построения такой сети, гибкость и надежность. Конечно, стоимость сети 10Base-T выше, чем сети 10Base-2, но чего стоит только тот факт, что при обрыве кабеля будет отключен от сети только один компьютер, а все остальные будут работать, как ни в чем не бывало.

Стандарт 10Base-T как и вышеописанные уже устарел, но он все же достаточно часто встречается на разных предприятиях, где сеть строилась 5-10 лет назад. Несмотря на то, что вы вряд ли будете создавать сеть 10Base-T, разобраться с этим стандартом просто необходимо: ведь это своеобразный прототип сети 100Base-TX, которая является стандартом современных сетей.

Сети данного стандарта (10Base-T) используют две неэкранированные витые пары (UTP, Unshielded Twisted Pair). Кабель, необходимый для построения данной сети, имеет маркировку UTP3 или UTP 3-cat.

Компьютеры сети 10Base-T объединяются в сеть специальным устройством — концентратором (другое название — хаб, hub, concentrator). Концентратор — это многопортовый повторитель, то есть он повторяет сигналы на всех отрезках витой пары, поэтому получается единая среда передачи данных — логическая шина.

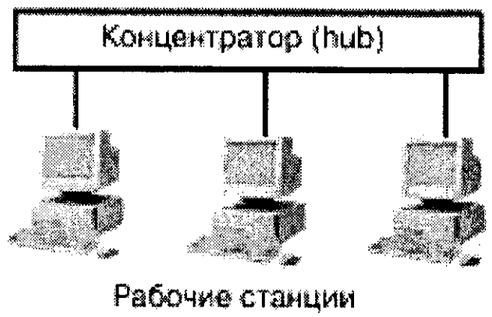


Рис. 4.7. *Сеть стандарта 10Base-T*

Предположим, что первая рабочая станция отправляет третьей станции кадр. Концентратор получает сигнал и повторяет его на все свои порты, то есть кадр получают все станции — точно так же, если бы они были подключены к одному общему кабелю, как в сети 10Base-2/5.

Кроме функций повторителя, концентратор используется для обнаружения коллизии. Сейчас поясню как. У каждого порта концентратора есть Rx-входы и Tx-выходы. Когда станция отправляет сигнал, он поступает на Rx-вход концентратора соответствующего порта, к которому подключен компьютер. Потом концентратор повторяет полученный сигнал на все Tx-выходы, чтобы их получили все компьютеры в сети. Вы уже догадались, как обнаруживается коллизия? Если концентратор обнаруживает сигналы на двух или более Rx-входах (возникла коллизия), то он пересылает jam-последовательности на все Tx-выходы.

Иерархическое соединение концентраторов

Концентраторы можно соединять друг с другом с помощью тех же портов, которые используются для подключения компьютеров. Желательно соединять концентраторы с помощью одного и того же порта. Например, если вы подключили один конец кабеля к порту номер 1 первого концентратора, то другой конец нужно подключить тоже к первому порту другого концентратора (рис. 4.8).

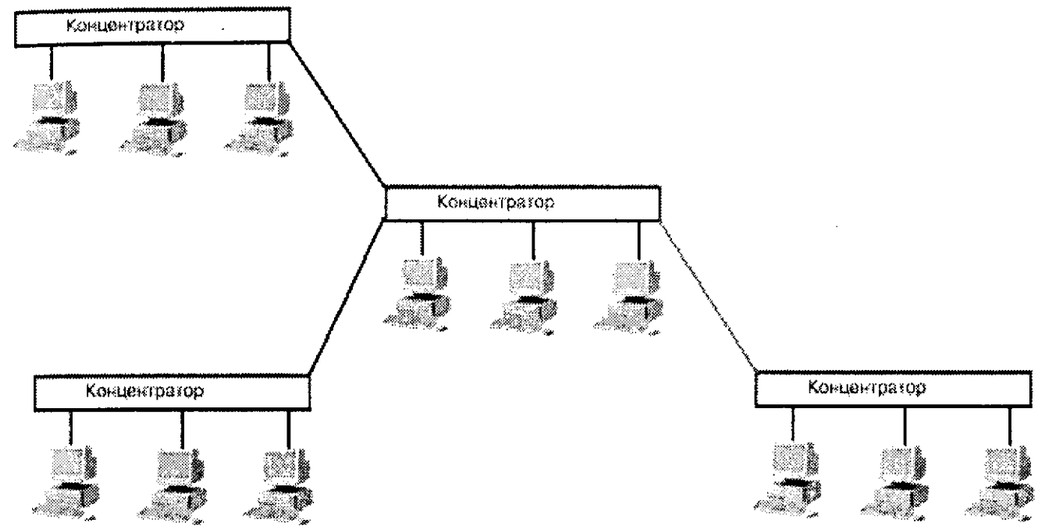


Рис. 4.8. *Иерархическая структура концентраторов*

При построении сети 10Base-T нужно помнить правило «четырех хабов»: между двумя конечными компьютерами не должно быть более трех концентраторов.

Максимальное количество компьютеров в сети 10Base-T — 1024. Этого количества можно достичь с помощью схемы максимального количества узлов (рис. 4.9).

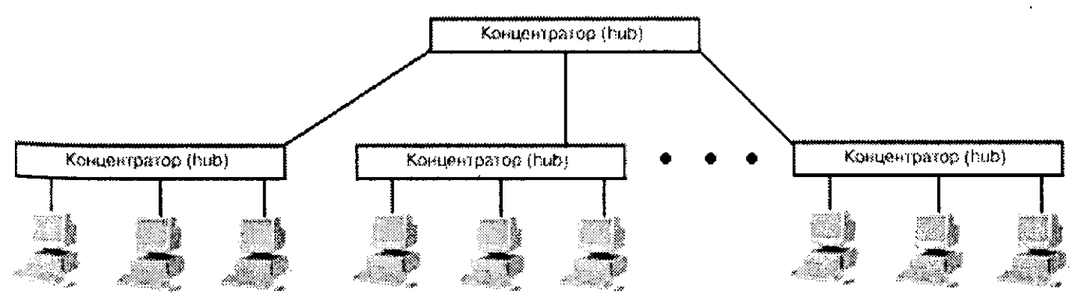


Рис. 4.9. *Схема максимального количества узлов*

Как видно из рисунков, для обеспечения данной схемы нужен один корневой концентратор, к которому будут подключены концентраторы нижнего уровня. На нижнем уровне нужно расположить достаточное количество концентраторов — с общим количеством портов 1024.

Схема максимального количества полностью соответствует правилу 4-х хабов. При построении такой большой сети нужно помнить, что максимальное расстояние между двумя самыми удаленными узлами — 2500 метров.

Построение сети 10Base-T

Перед построением сети поговорим о ее характеристиках. Для ясности они сведены в табл. 4.2.

Характеристики сети 10Base-T *Таблица 4.2*

Параметр	Значение
Максимальная скорость передачи данных	10 Мбит/с
Максимальное расстояние между двумя узлами сети (между компьютером и концентратором)	100 м
Максимальное количество станций	1024

Конечно, это не все характеристики сети 10Base-T, но все остальные в данный момент для нас не столь важны.

Для построения сети 10Base-T нам понадобится оборудование, перечисленное в табл. 4.3. Для сравнения с сетью 10Base-2 будем считать, что у нас есть три компьютера.

Сразу нужно сделать несколько примечаний. Во-первых, цены в таблице усредненные — в некоторых городах они могут быть ниже, в других — выше. Во-вторых, витую пару третьей категории достаточно сложно найти, поэтому вместо нее можно использовать пятую категорию, цена приведена именно пятой категории. В-третьих, стоимость концентратора зависит от количества портов. Количество портов концентратора должно быть больше или равно количеству компьютеров сети, иначе будут «лишние» компьютеры, которые не удастся подключить к сети.

Оборудование, необходимое для создания сети 10Base-T *Таблица 4.3*

Наименование	Количество	Ед. изм.	Цена	Сумма
Компьютеры	3	шт.	-	-
Сетевые адаптеры 10Mbit, PCI, RJ45	3	шт.	5	15
Коннекторы RJ-45	6	шт.	0,3	1,8
Витая пара UTP категории 5	10	м	0,35	3,5
Концентратор 5 портов	1	шт.	20	20
Инструмент для обжимки кабеля	1	шт.	15	15

Общая стоимость: 55,3 долларов США

В приведенном примере количество компьютеров (3) меньше количества портов (5). Покупая концентратор, подумайте о расширении сети: будут ли подключаться к сети дополнительные компьютеры. Иногда дешевле взять концентратор с большим количеством портов, чем нужно — «про запас», чем покупать со временем еще один концентратор. Концентратор на восемь портов будет стоить всего на 2-5 долларов дороже, чем пятипортовый, зато со временем вам не придется еще выкладывать 20 долларов за еще один концентратор.

Также можно сэкономить на сетевых платах — если у вас они интегрированы в материнскую плату, то, разумеется, платить вам за них не нужно. Практически все современные компьютеры оснащаются встроенной сетевой платой. Конечно, встроенные сетевые платы — это вам не сетевой адаптер Intel, но для сети небольшого офиса возможностей встроенных адаптеров вполне достаточно.

И, наконец, последнее замечание. Можно сэкономить на инструменте для обжимки кабеля. Обжать витую пару можно при желании обыкновенной отверткой и пассатижами. Если кто-то попытается возразить, мол, это невозможно, буквально пару месяцев назад (сейчас май 2004 года) у меня сломался инструмент для обжимки, а дело было в 100 км от города. Пришлось обжимать отверткой.

В результате компьютерный класс на 8 компьютеров работал на скорости 100 Мбит/с (!). Ни один компьютер не был обжат специальным инструментом. Свою домашнюю сеть я ради интереса тоже обжимал отверткой, не подумайте, что ради экономии — просто хотел повторить тот эксперимент. Инструмент для обжимки кабеля показан на рис. 4.10, а также на рис. 4.11 (другой вариант).

Теперь приступим к построению сети. Установите сетевые платы в компьютеры, настройка самих плат будет обсуждаться в следующей части. Коннекторов RJ-45 (рис. 4.12) нам понадобится в два раза больше, чем компьютеров — витую пару нужно обжимать с обеих концов: ведь с од-

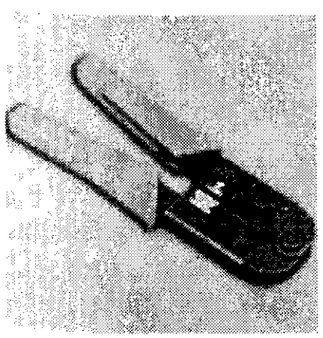


Рис. 4.10. *Инструмент для обжима разъемом RJ-45*

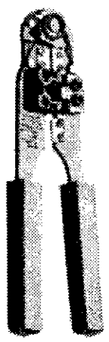


Рис. 4.11. *Еще один инструмент для обжима*

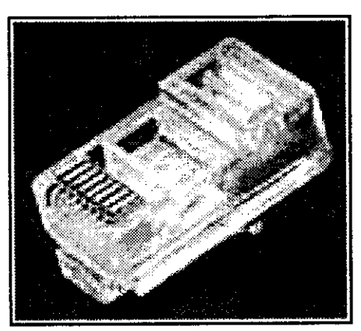


Рис. 4.12. *Коннектор RJ-45*

ной стороны будет сетевая плата, а с другой — концентратор. Я вообще рекомендую купить на 1-2 больше, чтобы потом не бегать по несколько раз в магазин, если обожмете кабель неправильно. Если вы в первый раз обжимаете кабель, то вероятность ошибки очень велика.

Теперь о кабеле. Вы можете купить четырех- или восьми-жильную витую пару. Все жилы (проводки) витой пары нумеруются цветовым кодом — дабы не перепутать провода. Скорее всего, у вас будет восьмижильный кабель с маркировкой, соответствующей стандарту 568B (ли EIA/TIA-568B, ATA&T 258A). В зависимости от типа кабеля разводка жил кабеля выполняется поразному (табл. 4.4, 4.5). Сначала рассмотрим нумерацию контактов коннектора RJ-45 (их еще называют «джеками» или «вилками»).

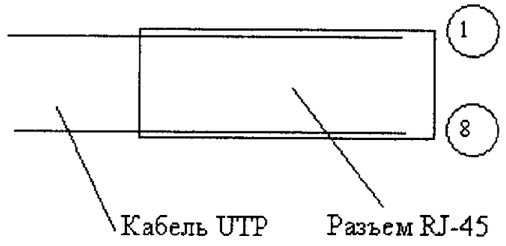


Рис. 4.13. *Нумерация контактов разъема RJ-45*

Таблица 4.4
Разводка восьмижильного кабеля

Контакт	Цвет провода
1	Бело-оранжевый
2	Оранжевый
3	Бело-зеленый
4	Синий
5	Бело-синий
6	Зеленый
7	Бело-коричневый
8	Коричневый

Таблица 4.5
Разводка четырехжильного кабеля

Контакт	Цвет провода
1	Бело-оранжевый
2	Оранжевый
3	Бело-синий
6	Синий

Если вы правильно обжали кабель, на вашей сетевой плате и на вашем хабе должны загореться соответствующие индикаторы после подключения компьютера к концентратору. Если же индикаторы не загораются, проверьте разводку кабеля, а также надежность обжатия — возможно, вы плохо обжали один из контактов. Такое иногда случается при использовании дешевого или изношенного инструмента. В таком случае приходится воспользоваться плоской отверткой для обжатия одного-двух плохо обжатых контактов.

После подключения кабеля к концентратору, при условии, что он включен, а также включен подключаемый компьютер, на передней панели концентратора должны загореться две лампочки: первая свидетельствует о том, что порт подключен и работает, а вторая — о том, что используется скорость 100 Мбит/с. Для каждого порта имеется своя собственная пара лампочек. Если загорается только первая лампочка, значит порт работает на скорости 10 Мбит/с. Причиной этому может быть плохая обжимка кабеля или устаревший сетевой адаптер, который не поддерживает Fast Ethernet.

4.1.4. Оптоволокно: 10Base-F

Данный стандарт использует оптоволоконный кабель в качестве среды передачи данных. Дешевый оптоволоконный кабель при полосе пропускания до 800 МГц обеспечивает передачу данных на расстояние до 1 километра. Стандарт 10Base-F используется, если скорость передачи данных не столь важна (10 Мбит/с — это предел для данной технологии), но важно расстояние и повышенная помехозащищенность кабеля.

Сеть 10Base-F с принципиальной точки зрения похожа на сеть 10Base-T: сетевые адаптеры, концентраторы и отрезки кабеля, соединяющие концентратор и компьютеры. Только вместо витой пары используется оптоволоконный кабель. По-прежнему действует правило четырех хабов.

Стандарт 10Base-FL обеспечивает максимальное расстояние между компьютером и концентратором до 2000 метров. Максимальная длина сети — 2500 м.

Стандарт 10Base-FB используется только для соединения концентраторов (повторителей). Между узлами такой сети можно установить до пяти концентраторов 10Base-FB, при этом обеспечивается максимальная длина сети до 2740 метров.

4.2. Сеть Fast Ethernet — оптимальное решение

4.2.1. Оборудование, необходимое для сети Fast Ethernet

Коаксиальный кабель в технологии Fast Ethernet не используется, благодаря чему все три стандарта 100Base-* имеют иерархическую структуру, основанную на концентраторах и/или *коммутаторах*. Вообще вместо концентратора предпочтительнее использовать коммутатор (switch).

В отличие от коммутатора, концентратор «не знает», к какому порту подключен тот или иной компьютер и когда один из компьютеров передает пакет, то концентратор повторяет этот пакет на все свои порты. Каждый компьютер сети получает этот пакет и проверяет наличие своего IP-адреса в заголовке этого пакета. Если IP-адрес назначения не совпадает с IP-адресом компьютера, который принял этот пакет, то пакет просто игнорируется. Коммутатор (рис. 4.14) же передает пакет только на тот порт, к которому подключен адресат. Благодаря этому, помимо повышения безопасности, снижается нагрузка на сеть.

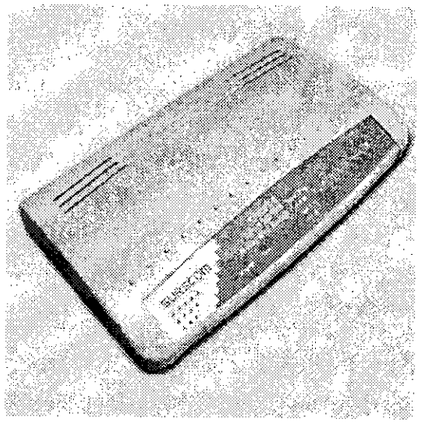


Рис. 4.14. *Коммутатор Surecom Switchhub 808x8 портов*

Стоимость организации сети Fast Ethernet будет примерно такой же, что и Ethernet (10Base-T), поэтому предпочтительнее использовать именно Fast Ethernet. Для организации Fast Ethernet нам понадобится следующее оборудование:

- Сетевые адаптеры Fast Ethernet — по количеству компьютеров.
- Коннекторы RJ-45 — в два раза больше, чем количество компьютеров.
- Витая пара категории 5 (лучше использовать именно пятую категорию).
- Коммутатор с количеством портов больше и равным количеству компьютеров.
- Инструмент для обжимки витой пары (как уже отмечалось, его вполне может заменить плоская отвертка).

4.2.2. Разработка оптимальной топологии сети

Разрабатывая сеть, необходимо хотя-бы примерно прикинуть, сколько и откуда-куда будет происходить передача данных. В соответствии с этим необходимо наиболее оптимально осуществить расположение и подключение сетевых устройств. Чтобы не было задержек с передачей данных

(сеть не. «тормозила»). Если у вас несколько компьютеров и один концентратор (или коммутатор), то тут и выбирать-то не из чего — просто подключаете все компьютеры к концентратору и все.

А если у вас сеть из большого количества компьютеров с несколькими концентраторами, то здесь уже есть о чем призадуматься. В простейшем случае можно подключить все компьютеры к концентраторам, а их соединить между собой. Это хорошо, если все компьютеры выступают примерно в одинаковой роли.

Ну а если у вас компьютерный клуб и на одном из компьютеров размещены фильмы? Поток данных по сети при трансляции фильмов довольно существенный (тем более, если фильмы будут смотреть сразу с нескольких компьютеров). В этом случае необходимо позаботиться, чтобы расположение компьютера с фильмами в сети было таким, которое бы обеспечивало наибольшее быстродействие.

Кстати говоря, не стоит оставлять без внимания тот факт, что в один компьютер можно вставить несколько сетевых карт и таким образом обеспечить сразу несколько каналов доступа из сети к этому компьютеру. Данной возможностью воспользовались в одном из знакомых компьютерных клубов. В результате топология сети у них выглядит как показано на рис. 4.15.

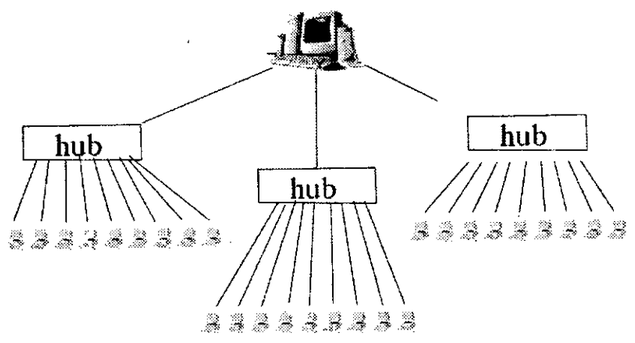


Рис. 4.15. *Топология сети*

Таким образом нагрузка на сеть (в направлении к компьютеру с фильмами) была оптимизирована. А теперь представьте, если компьютер с фильмами располагался внизу, вместо одного из обычных компьютеров, а фильм попытались бы смотреть из разных сегментов сети. Оцените, какие перегрузки сети будут.

Примечание.

Кстати говоря, на компьютере с фильмами в вышеупомянутом компьютерном клубе был также настроен программный мост (на основе Windows Server 2003). Что оптимизировало нагрузку на сеть в целом, не давая пакетам данных, передаваемых внутри каждого из сегментов, выходить за пределы этого сегмента.

4.2.3. Последовательность действий для создания сети Fast Ethernet

Последовательность действий для создания сети Fast Ethernet:

1. Установить сетевые адаптеры (если сетевые адаптеры интегрированы в материнскую плату, этот шаг, разумеется, пропускаем).
2. Обжать оба конца кабеля UTP-5 в соответствии с табл. 4.6.
3. Соединить обжатым кабелем сетевой адаптер и концентратор (коммутатор). На современных концентраторах/коммутаторах обычно имеется два индикатора для каждого порта. Первый LNK/ACT свидетельствует о том, что к этому порту подключен компьютер. Второй, 100M, говорит о том, что данный порт будет работать со скоростью 100 Мбит/с. Если вы используете кабель категории 5 и ваши сетевые адаптеры поддерживают 100 Мбит/с, а индикатор 100M не загорается, значит, вам нужно заново обжать кабель — возможно один из контактов не обжат или плохо обжат.

Примечание.

Если индикатор LNK/ACT не горит, значит, вы плохо обжали кабель, и порт вообще не будет использоваться. Если LNK/ACT мигает, значит, порт принимает пакеты.

4.2.4. Обжимка кабеля

Теперь поговорим о том, как правильно обжать кабель. Кабель нужно обжать, чтобы иметь возможность передавать по нему информацию. Ведь по сути, витая пара — это восемь (или четыре) проводов, а в концентратор (хаб) нужно вставить одну вилку — RJ. Эта вилка часто называется джеком. При обжимке каждый провод становится на свое место в вилке. Ясное дело, что провода нужно расположить в правильной последовательности, для чего нам помогут таблиц 4.4 и 4.5. Поскольку чаще используется восьмижильный кабель, таблица его обжимки (4.4) повторяется — чтобы вы лишний раз не листали книгу.

Разводка восьмижильного кабеля *Таблица 4.6*

Контакт	Цвет провода	Контакт	Цвет провода
1	Бело-оранжевый	5	Бело-синий
2	Оранжевый	6	Зеленый
3	Бело-зеленый	7	Бело-коричневый
4	Синий	8	Коричневый

4.2.5. Правила построения сети Fast Ethernet

Обжимка кабеля — это не самое сложное при построении сети Fast Ethernet. При организации такой сети нужно учитывать четыре класса ограничений:

- Максимальную длину сегмента.
- Максимальную длину сегмента с использованием повторителей.
- Максимальную длину сети.
- Максимальное число повторителей.

Максимальная длина сегмента

Как вам уже известно, сеть Fast Ethernet имеют топологию «звезда». Данная топология подразумевает подключение компьютеров сети с помощью сегментов кабеля к центральной точке. Так вот максимальная длина этих сегментов указана в табл. 4.7. Например, для витой пары пятой категории она составляет 100 метров.

Максимальная длина сегментов *Таблица 4.7*

Стандарт	Кабель	Макс. длина сегмента, м
100Base-TX	UTP категория 5	100
100Base-T4	UTP категория 3,4,5	100
100Base-FX	Оптоволокно 62,5/125 мкм	2000

Максимальная длина сегмента с использованием повторителей

Повторители (читайте концентраторы, поскольку повторитель — это простейший концентратор) бывают двух классов: первого (I) и второго (II). Разница в использовании типов кодирования сигнала. Повторители первого класса поддерживают любой тип сигнала, используемый в Fast Ethernet, а повторители второго класса — только один, определенный тип сигнала. Визуально отличить повторитель первого класса от повторителя второго класса очень просто. Так как он поддерживает все типы сигналов (точнее, типы кодирования сигнала), то он будет портами всех трех типов: TX, T4 и FX. Повторитель второго класса оснащен каким-то одним типом порта: или TX, или T4, или FX.

Повторители второго класса вносят меньшую задержку при передаче сигнала, поэтому максимальное количество повторителей второго класса в одном домене коллизий (это часть сети, все узлы которой распознают коллизию) равно 2. В то время как повторитель первого класса может быть только одним. Максимальное расстояние между повторителями второго класса — 5 метров.

Максимальная длина сети

Максимальную длину сети легко вычислить. Но сначала скажем, что это такое. Максимальная длина сети — это расстояние между двумя наиболее удаленными ее узлами. Для витой пары максимальную длину сети легко вычислить: два повторителя второго класса, максимальная длина сегмента и расстояние между повторителями:

$$2 \times 100 + 5 = 205 \text{ метров.}$$

Что же касается повторителей первого класса, то максимальная длина сети зависит от типа используемых кабелей (см. табл. 4.8).

Максимальная длина сети, основанная на повторителях класса I — *Таблица 4.8*

Витая пара	200
Оптоволокно	272
Один сегмент на оптоволокне и несколько — на витой паре	260
Несколько сегментов на оптоволокне и несколько — на витой паре	272

Максимальное число повторителей

При выборе повторителя сети Fast Ethernet нужно учитывать, к какому классу этот повторитель относится. Существуют два класса повторителей Fast Ethernet. Повторители первого класса поддерживают два типа кодирования данных — 4B/5B и 8B/6T. Повторители второго класса поддерживают какой-то один тип кодирования: или 4B/5B, или 8B/6T. Поэтому первый класс повторителей поддерживает порты всех стандартов — 100Base-TX, 100Base-t4 и 100Base-FX. Повторители второго класса могут поддерживать только один какой-то тип портов — или 100Base-TX, или 100Base-t4, или 100Base-FX.

Первый класс повторителей из-за поддержки обоих типов кодирования данных вносит большую задержку в распространение сигнала, чем второй тип повторителей — 70 битовых интервалов против 46. Поэтому в одном домене коллизий не может быть более одного повторителя первого класса. Что же касается повторителей второго класса, то их может быть в одном домене коллизий не более двух, причем они должны быть соединены кабелем не длиннее пяти метров.

Домен коллизий — это часть сети Fast Ethernet (или просто Ethernet), все узлы которой распознают коллизию, вне зависимости от того, в каком месте сети возникла коллизия.

Характеристики сети на базе повторителей первого класса приведены в табл. 4.9.

Характеристики сети на базе повторителей первого класса — *Таблица 4.9*

Кабель	Максимальная длина сегмента, м	Максимальный диаметр сети, м
Витая пара	100	200
Оптоволокно	136	272
Один сегмент на оптоволокне и несколько на витой паре	100 для витой пары, 160 для оптоволокна	260
Несколько сегментов на витой паре и несколько на оптоволокне	100 для витой пары и 136 для оптоволокна	272

4.3. Сеть из двух компьютеров

При организации небольшой домашней сети, состоящей всего из двух компьютеров, этот вопрос будет очень актуален. Как можно объединить в сеть два компьютера? Для этого существует много способов, но в домашних условиях возможны следующие варианты:

- С помощью нуль модема.
- С использованием модемов.
- По инфракрасному порту.
- С использованием PLC-адаптеров.
- С помощью Fast Ethernet-сети.

С помощью нуль модема

Такой способ вряд ли можно назвать рациональным. Ведь скорость передачи данных с использованием нуль модема очень мала, а расстояние передачи данных невелика. Уже проще записать нужные данные на дискету или CD-R и перенести на другой компьютер, чем использовать нуль модем, поэтому данный способ сразу отпадает. Мы о нем вспомнили ради традиции: помните, в Norton Commander была возможность передачи данных по последовательному порту?

С использованием модемов

Данный способ подходит, если нам нужно передавать данные на значительные расстояния, скажем, в пределах города, где организация сети не столько невозможна, сколько экономически нецелесообразна. Скорость передачи данных по нашим телефонным линиям будет приблизительно равна 28,8 Кб/с, что достаточно для обмена небольшими объемами данных. Передать фильм по такому каналу вряд ли удастся — скорее оборвется соединение, чем вы успеете передать хотя бы 100 Мб информации. Да и за телефон платить накладно.

По инфракрасному порту

Данный способ обладает теми же недостатками данных, что и последовательный порт — маленькая скорость передачи данных и небольшое расстояние (в пределах 1 метра). Данный способ нужно применять, если нет другой возможности обмена данными. Например, для связи КПК или ноутбука с компьютером. Кроме того, далеко не все стационарные компьютеры оснащены инфракрасным портом, который придется покупать отдельно. С ноутбуками и КПК, как правило, проблем нет. Инфракрасный порт отсутствует или на самых старых или на самых дешевых моделях.

С использованием PLC-адаптеров

Учитывая небольшую скорость обмена данными, данный способ тоже отпадает, хотя единственное его преимущество — это экономия на прокладке кабеля и стоимости самого кабеля. Пока PLC-адаптеры довольно дороги (в пределах 100 долларов), что очень дорого для домашнего пользователя. Вам же нужен не один адаптер, а несколько — по количеству компьютеров.

С помощью Fast Ethernet-сети

Сразу могу вас обрадовать: вам не нужен коммутатор или концентратор — вы можете сэкономить около 20 долларов. Все, что вам нужно, чтобы ваша небольшая сеть работала со скоростью 100 Мбит/с — это наличие 100 мегабитных сетевых адаптеров. Этот вариант с экономической точки зрения является самым оптимальным, особенно учитывая, что скорость передачи данных равна 100 Мбит/с.

Идея работы без концентратора заключается в следующем: один конец кабеля, соединяющего два компьютера, вы обжимаете как обычно, а другой — перекрестно. Разумеется, с помощью такого кабеля вам уже не удастся подключить компьютер к концентратору, но ведь у вас его нет! Нормальная и перекрестная разводка кабеля для удобства представлена в табл. 4.10.

Нормальная и перекрестная разводка кабеля *Таблица 4.10*

Контакт	Нормальная разводка	Перекрестная
1	Бело-оранжевый	Бело-зеленый
2	Оранжевый	Зеленый
3	Бело-зеленый	Бело-оранжевый
4	Синий	Синий
5	Бело-синий	Бело-синий
6	Зеленый	Оранжевый
7	Бело-коричневый	Бело-коричневый
8	Коричневый	Коричневый

Уточним список оборудования для мини-сети из двух компьютеров:

- Два сетевых адаптера 100 Мбит/с.
- Кабель витая пара пятой категории.
- Два коннектора RJ-45.

После обжимки кабеля один конец нужно подсоединить к одному компьютеру, а другой — к другому. Если вы правильно обжали кабель, сеть уже должна работать.

Часть III

БАЗОВАЯ НАСТРОЙКА СЕТИ (ОДНОРАНГОВАЯ СЕТЬ)

Глава 5

Сетевые операционные системы

5.1. Windows for Workgroups

Это довольно старая операционная система, не соответствующая требованиям к современным сетевым операционным системам. Вообще-то ее и операционной системой можно назвать с большой натяжкой — это всего лишь надстройка над операционной системой DOS с функциями поддержки одноранговых сетей.

В сети типа клиент/сервер данная операционная система работать не сможет: она не сможет использовать ресурсы этой сети, хотя при желании можно добиться, чтобы клиенты сети клиент/сервер с выделенным сервером на базе Windows NT/2000 Server смогли использовать ресурсы компьютера, работающего под управлением Windows for Workgroups. Но в большинстве случаев это не стоит потраченного времени — проще купить компьютер с процессором Pentium 100-166 примерно за 100 долларов и установить на него Windows 98.

Данную операционную оболочку можно установить на компьютер, который и продать нельзя — никто не купит, и выбросить жалко. Как правило, это система с процессором Intel 80386. Если у вас 486-й процессор и хотя бы 8 Мб памяти, целесообразно установить Windows 95. Системные требования операционной оболочки Windows for Workgroups:

- Процессор Intel 80386 SX/DX или 80486.
- Оперативная память 2...8 Мб.

5.2. Windows 95

Данную операционную систему нельзя в полной мере назвать сетевой. Это скорее операционная система с поддержкой сетевых функций. Но по сравнению с Windows for Workgroups, Windows 95 намного лучше — хотя бы потому, что она может работать в сети клиент/сервер. Это означает, что компьютер под управлением Windows 95 может быть членом домена Windows NT/2000. Ресурсами этого компьютера смогут пользоваться другие компьютеры сети Microsoft, равно как и пользователь, работающий за этим компьютером, сможет использовать ресурсы сети Microsoft.

Системные требования очень низки. Мне удавалось устанавливать Windows 95 на компьютер с процессором Intel 80386 DX и оперативной памятью 8 Мб. Хотя для более или менее уверенной работы понадобится процессор Intel 80486 66 MHz и 8...12 Мб оперативной памяти. Если у вас компьютер с процессором Pentium, лучше установить Windows 98.

5.3. Windows 98/ME

Вот данная операционная система является действительно сетевой. Данную операционную систему лучше устанавливать на компьютер с процессором Intel Pentium. На 486-ой процессор Windows 98 лучше не устанавливать — уж больно медленно. Хотя, если у вас новое поколение 486-го процессора — 586 DX-5 133 MHz, можно установить и Windows 98. Требования к оперативной памяти — 8 Мб. Я бы порекомендовал не менее 16 Мб, а лучше 24 или 32 Мб.

Что лучше Windows 98 или Windows Millennium Edition? Лично мне больше нравится классика — Windows 98, несмотря на все новшества Windows ME. Windows 98 работает стабильнее, мне больше нравится ее поведение в сети, чего не скажешь о Windows ME. Если мне не верите, установите Windows ME — проверите на собственном опыте. У меня Windows ME не задержалась и двух недель.

5.4. Windows NT Workstation 4.0

Данная операционная система очень стабильная и надежная. Ее стабильность нельзя даже и сравнивать с Windows 9x. Надежность Windows NT достигается благодаря новой технологии ядра (NT — New Technology). Работа в сети тоже не вызывает каких-либо нареканий.

Вот только «классическая» Windows NT, особенно если вы работали с Windows 98/2000/XP, вам не очень понравится. Для того чтобы «привести ее в чувства», следует установить следующие обновления: SP 3 (service Pack 3), SP5, SP6. Четвертый сервис-пак устанавливать не нужно, поскольку он вносит больше ошибок, чем исправляет. При установке сервис-паков обратите внимание на версию операционной системы и ее язык: на русскую Windows NT английский сервис-пак вы не установите.

Минимальные требования к компьютеру:

- процессор Intel Pentium;
- оперативная память 32 Мб.

Устанавливать Windows NT на компьютер с 16 Мб оперативной памяти не имеет смысла, если вы планируете работать в сети. Если отключить все сетевые сервисы, в принципе, Windows NT будет работать на 16 Мб оперативной памяти, но: каждый сервис-пак увеличивает требование к системе. Если вы установите SP3, вам понадобится минимум 32 Мб для работы без сети. Если у вас всего 32 Мб, вы можете отключить ActiveDesktop, добавляемый третьим сервис-паком, тогда при работе в сети вы не будете ощущать «эффекта торможения».

Если вы планируете использовать файловую систему NTFS, для нормальной работы вам понадобится не менее 64 Мб оперативной памяти и процессор с частотой не менее 166 МГц.

При установке Windows NT у вас могут возникнуть определенные проблемы, особенно, если вы никогда ее раньше не устанавливали. Первая проблема — это медленная установка операционной системы. На компьютере с процессором Intel Celeron 700 МГц и 128 Мб оперативной памяти копирование файлов занимает около 80 минут. Существенно (раза в 4) уменьшить время установки можно, если перед запуском программы установки Windows NT (файл `winnt.exe`) нужно запустить программу SmartDrive (файл smartdrv.exe) — так установка операционной системы пройдет заметно быстрее.

Если вы планируете установить Windows NT на файловую систему FAT, а не NTFS4, то проследите, чтобы FAT был 16-разрядным: Windows NT не поддерживает файловую систему FAT32. Точнее, поддерживает, но после установки. Для поддержки FAT32 нужно установить один из сервис-паков (Service Pack). Какой именно — не помню.

Если вы запускаете программу установки Windows NT с FAT-раздела (который тоже должен быть FAT16!), не забудьте перед установкой выполнить команду LOCK. Данная программа разрешает прямой доступ к диску приложениям — без этого Windows NT установить невозможно.

И, наконец, последний совет. Чтобы отказаться от создания всем известных «трех дискет», которые так и хочет создать программа установки Windows NT, нужно запустить программу установки с параметрами /b и /s. Первый параметр, собственно, и есть отказ от создания этих устано-

вочных дискет, а второй параметр задает каталог, в котором находится дистрибутив Windows NT.

Итак, общая последовательность действий при установке Windows NT:

1. Обеспечиваем кэширование чтения и записи для жесткого диска:

```
C:\...\smartdrv
```

2. Разрешаем прямой доступ к диску:

```
lock
```

3. Запускаем программу установки. Дистрибутивный каталог — c:\i386ws.rus:

```
c:\i386ws.rus\winnt.exe /b /s:c:\i386ws.rus
```

Ну а дальше — вы сами справитесь. Там нет ничего сложного. Кроме, разве что, серийного номера. Если вы его забыли, то подойдет 112-111111.

5.5. Windows NT Server 4.0

Windows NT Server — это одна из наиболее распространенных и популярных серверных операционных систем на территории бывшего СНГ. Несмотря на появление Windows 2000/2003 Server, многие организации не спешат их устанавливать, поскольку Windows NT Server до сих пор справляется с возложенными на него задачами.

Это очень надежная и в некоторой мере универсальная операционная система. Она может выступать в роли:

- Первичного контроллера домена;
- Резервного контроллера домена;
- Сервера DNS;
- Сервера DHCP (не должен быть контроллером домена);
- Web-сервера;
- Почтового и файлового сервера;
- Сервера удаленного доступа;
- Маршрутизатора;
- Шлюза.

Установка Windows NT 4.0 Server практически аналогична Windows NT 4.0 Workstation (см. выше). При установке системы вам нужно выбрать тип сервера:

- Primary Domain Controller — первичный контроллер домена;
- Backup Domain Controller — резервный контроллер домена;

- Stand-Alone Server — независимый сервер (может быть DHCP-сервером, DNS-сервером, Web-сервером и т.д.).

Если вы установили неправильный тип сервера, изменить вы его не сможете — вам нужно будет переустанавливать систему, поэтому будьте очень внимательны.

Системные требования:

- Процессор с частотой не менее 166 МГц.
- Оперативная память не менее 64 Мб (при использовании NTFS — 128 Мб).

5.6. Windows 2000 Pro, Server

Windows 2000 — по сути, это пятая версия операционной системы Windows NT, ставшая еще более надежной. Что же еще нового появилось в Windows 2000, по сравнению с Windows NT:

- улучшенный графический интерфейс пользователя;
- поддержка PnP (Plug and Play);
- большая база данных драйверов;
- обновленная версия файловой системы NTFS — NTFS5.

Но самое главное (с нашей точки зрения) — это служба каталогов Active Directory. Что это такое, вы узнаете в сответсвующей главе этой книги.

Системные требования:

- Процессор с частотой не менее 300 МГц (для более или менее комфортной работы).
- Оперативная память не менее 64 Мб для Windows 2000 Pro и 128 Мб для Windows 2000 Server. Рекомендуется 128-128 и 256-512, соответственно. При использовании файловой системы NTFS (что очень актуально для сервера), можете добавить еще 64 Мб. Тут можно использовать количественный принцип: чем больше, тем лучше.

В принципе, если у вас нет особой необходимости устанавливать Windows 2000 Pro, лучше установить Windows 98 — будет быстрее. Под «особой необходимостью» имеется в виду следующее:

- Поддержка службы каталогов Active Directory.
- Особые требования к безопасности данных, подразумевающие использование файловой системы NTFS.
- Поддержка SMP (если у вас два или более процессора).

О сервере можно сказать то же самое: если вам не нужна служба каталогов, можно использовать Windows NT Server 4.0. Данная операционная система вполне будет справляться с возложенными на нее задачами и при этом системные требования будут заметно скромнее.

5.7. Windows XP

С момента своего появления Windows XP завоевала большую популярность. Почему? Что в этой операционной системе такого особенного? Домашним пользователям захотелось чего-то новенького. Windows XP с лихвой оправдала их ожидания — на фоне Windows 98/ME/2000 данная операционная система очень выделяется. Большую роль сыграл обновленный, внешне более привлекательный и более продуманный интерфейс пользователя. На втором месте — поддержка большого количества самых разнообразных устройств: от Web-камер до Flash-накопителей.

Что же касается корпоративных пользователей, то им не оставили другого выбора. В одно время Windows XP продавалась параллельно с Windows 98. Руководители могли выбирать: покупать «классику» — Windows 98 или более новую операционную систему Windows XP. Сейчас Windows 98 не продается, поэтому, покупая новый компьютер, вы получаете Windows XP. Домашние пользователи не ограничены Windows XP — они могут купить компьютер без программного обеспечения и установить на него все что захочется, например, Linux или же собственноручно написанную операционную систему.

Windows XP — это операционная система для рабочих станций. «В природе» не существует серверной версии Windows XP. Версия Windows XP Professional отличается от Windows XP Home не только названием: она поддерживает SMP, то есть, если у вас многопроцессорная система, вам нужно покупать только Windows XP Professional.

Минимальные системные требования Windows XP:

- Процессор с частотой не менее 400 МГц.
- Оперативная память не менее 128 Мб.

Рекомендуемые системные требования:

- Процессор с частотой не менее 700 МГц.
- Оперативная память не менее 256 Мб.

Обычно при установке Windows XP проблем не возникает. Но у меня был очень интересный случай, когда Windows XP отказывалась устанавливаться на только что купленный компьютер. Конфигурация компьютера довольно прилична — AMD Duron 1,6 GHz/256 MB DDR400/HDD 40 GB Samsung/

Video 64 MB GeForce4 MX-440. Да, не самая мощная машинка, но для Windows XP — в самый раз. Компакт диск с Windows XP был лицензионным, поэтому не будем грешить на пиратскую копию.

После загрузки с компакт-диска все пошло, как нужно. До первой перезагрузки. А после перезагрузки я увидел синий экран с абракадаброй (Windows XP была русской) и одной понятной фразой — UNMOUNTABLE_BOOT_VOLUME. То есть невозможно примонтировать загрузочный том. Интересно. Windows XP ставилась на раздел FAT32 размером 1,5 Гб. Второй раздел был отформатирован как NTFS — его размер около 38 Гб. Для установки Windows XP нужен раздел размером хотя бы 1,2 Гб, то есть все требования программы установки были выполнены.

После различных вариантов разбивки диска (переформатировали его несколько раз) результат был тот же. Все опции SETUP тоже в норме. Попробовали ставить Windows 98 — установилась без проблем. Но это же не выход, нужно было установить именно Windows XP. Проблема оказалась в старом шлейфе IDE (ATA33), на котором решил сэкономить сборщик, установив его в новый компьютер. После замены шлейфа Windows XP установилась без проблем.

Вообще нужно заметить, что Windows XP очень чувствительна именно к шлейфам. Ваша система будет загружаться быстрее, если жесткий диск и CD-ROM подключить на один шлейф, а не на разные (при условии, что у вас установлены только один жесткий диск и один CD-ROM). Вот так вот.

5.8. Linux

Linux — это самая универсальная операционная система, известная мне. Она может устанавливаться как на рабочей станции, так и на сервере. Причем на Linux можно настроить абсолютно любой тип сервера: от обыкновенного DNS-сервера до контроллера домена сети Microsoft (PDC).

При установке Linux у начинающих пользователей, как правило, возникают определенные проблемы. Сейчас мы рассмотрим установку классического дистрибутива — Red Hat Linux. В этой книге, которая лишь косвенно относится к Linux, мы не можем рассмотреть установку всех популярных дистрибутивов — Linux Mandrake, ALT Linux, ASP Linux. Если вы заинтересовались, рекомендую свои книги:

- Linux-сервер своими руками, 2-е изд.
- Самоучитель Linux: установка, настройка, использование, 3-е изд.

Настройка сетевого адаптера (сетевой карты) и одноранговой сети

Первые четыре главы были теоретико-практическими. Вы познакомились с основными сетевыми технологиями и сразу же, «не отходя от кассы», узнали, как построить сеть, использующую ту или иную технологию. Дальнейшая настройка вашей сети будет происходить во второй части этой книги, но читать ее нет смысла, пока вы не ознакомитесь с протоколом TCP/IP, не разберетесь с маршрутизацией и не освоите другие «киты», необходимые для полноценной настройки сети.

6.1. Выбор сетевого адаптера

При нынешнем многообразии выбора сетевых плат (да и другого железа), невольно задаешь себе вопрос: какой сетевой адаптер выбрать? Что лучше, а что хуже? Переплачивать ведь никому не хочется.

Интегрированные сетевые адаптеры

В последнее время наблюдается тенденция интегрирования сетевых плат в материнскую плату. Производители материнских плат стараются удешевить свою продукцию, поэтому зачастую встроенное железо (это относится и к видеоплатам, и к звуковым платам) не очень качественное. Помню, был случай, когда пришлось оснащать целый компьютерный класс отдельными сетевыми адаптерами.

А дело было так: руководство одного университета, дабы сэкономить деньги, закупило дешевые тайваньские материнские платы с сомнительной репутацией. На борту материнских плат был сетевой адаптер. После настройки систем оказалось, что данные сетевые адаптеры более 11 Мбит/с не дают — это максимум, что можно было с них выжать.

Пришлось заменить эти платы дешевыми PCI-адаптерами Realtek 8139 — цена этого адаптера чуть больше 4 долларов. Не самый лучший выбор, но, по крайней мере, скорость существенно возросла.

Дешевые и дорогие сетевые адаптеры

В любом компьютерном магазине можно купить сетевую плату Realtek 8139 — обычно производства компаний Surecom или Lantech. Стоимость таких сетевых адаптеров не превышает 5-6 долларов (а зачастую и того меньше). Данные сетевые адаптеры могут работать как в режиме 100 Мбит/с, так и в режиме 10 Мбит/с, то есть их можно использовать как в сети Fast Ethernet, так и в обычной Ethernet-сети (10Base-T).

Они поддерживают управление питанием (ACPI, Advanced Configuration and Power Interface) и функцию WOL (Wake On LAN). Что можно сказать об этих сетевых адаптерах? Довольно неплохие адаптеры, возможностей которых вполне хватит для организации небольшой сети — домашней или сети небольшого предприятия.

Если же вам нужна надежность, вы часто работаете с мультимедиа-информацией, причем эта информация частенько «гуляет» по вашей сети, могу посоветовать сетевые адаптеры фирмы Intel. Такие сетевые платы стоят от 28 долларов и не всегда есть в наличии — их нужно заказывать. Это объясняется тем, что данные сетевые адаптеры не пользуются большим спросом из-за их большой стоимости.

Сравните, десять сетевых адаптеров Realtek обойдутся в 45 долларов, а 10 адаптеров Intel — 300 долларов. Но эти адаптеры оправдывают себя. Не пожалейте денег и купите хотя бы один такой адаптер. Ясное дело, что установить его нужно будет на сервер.

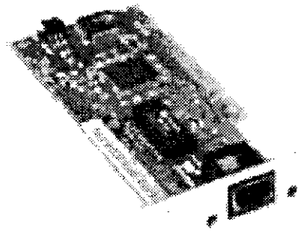


Рис. 6.1. *Сетевой адаптер Intel Express 10/100 Pro Plus Management Adapter*

Технологии и стоимость адаптера

Цена сетевого адаптера зависит от поддерживаемых им технологий и среды передачи данных. Например, обыкновенная сетевая плата для технологии Fast Ethernet 100Base-t4/TX, как уже было замечено, стоит около 5 долларов. Сетевая плата для того же Fast Ethernet, но для стандарта 100Base-FX, использующего оптоволоконный кабель, стоит в пределах 100 долларов (например, PCI Fiber Card-SC-Type (VIA) SURECOM EP-320FX-C 100Base-FX — 113 долларов).

Парадоксально, но сетевые платы для более старых технологий могут стоить дороже, чем для новых. Например, Ethernet-плата 3Com 10 Мбит/с, способная работать как на витой паре, так и на коаксиале, стоит в пределах 10-11 долларов, в то время как адаптер для Fast Ethernet стоит 5. Конечно, это при покупке в магазине. На руках (то есть по объявлению) можно купить и дешевле, но на меньше чем на 5 долларов рассчитывать не приходится. Вот и считайте: нужен ли вам старый Ethernet?

При покупке сетевого адаптера нужно убедиться, поддерживает ли он выбранную вами технологию и тип кабеля, чтобы не случилось, что вы купили адаптер с BNC-разъемом под коаксиал, а у вас витая пара.

USB-адаптеры

Для ноутбуков, не оснащенных сетевой платой, лучшим выбором станет внешние адаптеры USB-to-Ethernet. Такой адаптер стоит в пределах 20...35 долларов и с ним сможет работать любой ноутбук, оснащенной шиной USB.

При выборе адаптера обратите внимание, какая шина ему необходима: если у вас старый ноутбук, оснащенный только USB 1.0, то и покупать нужно сетевой адаптер для USB 1.0. Если вы купите адаптер для шины USB 2.0, а у вас USB 1.0, гарантии, что он будет работать, нет никакой.

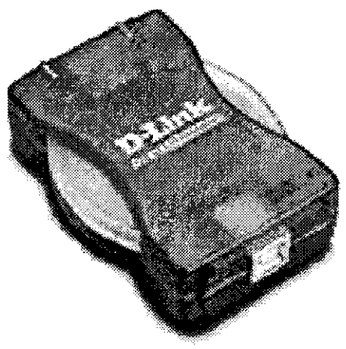


Рис. 6.2. *Сетевой адаптер USB to Ethernet DLink DU E100*

Установите сетевой адаптер в свободный PCI-слот на вашей материнской плате. Все современный сетевые адаптеры и операционные системы поддерживают технологию Plug and Play, поэтому вам не придется самостоятельно указывать IRQ и адрес порта ввода/вывода.

6.2. Настройка сетевой карты и настройка простейшего сетевого взаимодействия

6.2.1. Настройка сетевой карты в Windows 95/98

Установку драйвера сетевого адаптера в операционных системах Windows 95/98/ME рекомендуется производить с установочного диска производителя, даже если в операционной системе имеется драйвер для вашей сетевой платы. В операционных системах Windows 2000, Windows XP и Linux лучше воспользоваться стандартным драйвером, предложенным операционной системой.

Для определенности мы будем использовать следующую конфигурацию сети для всех операционных систем:

- IP-адрес: 192.168.1.5
- Маска сети: 255.255.255.0
- Имя компьютера: comp5
- Рабочая группа: WORK

Конечно, вы можете назначить любой другой адрес, также совсем необязательно использовать сеть класса C. Однако, чтобы облегчить себе жизнь, при настройке компьютеров желательно нумеровать их по порядку, например, 192.168.1.1, 192.168.1.2 и т.д., а к имени компьютера приписывать его порядковый номер, например, comp1, comp2.

В качестве имени компьютера можно также использовать имя рабочей группы с порядковым номером, например, если имя рабочей группы WORK, компьютеры можно называть `work1`, `work2` и т.д. Сеть класса C идеально подходит для небольшой SOHO-сети. Сети класса C могут содержать до 255 компьютеров — вряд ли у вас будет больше.

Настраиваем адаптер

При загрузке операционная система обнаружит новое устройство и предложит вам его установить (рис. 6.4). Нажмите кнопку **Далее**. Операционная система предложит вам найти лучший драйвер или воспользоваться драйвером, имеющимся в составе операционной системы. Конечно же выбирайте первый вариант. Поиск может производиться на гибких дисках, съемных дисках, CD-ROM или по указанному пути — если вы знаете местонахождение драйвера.

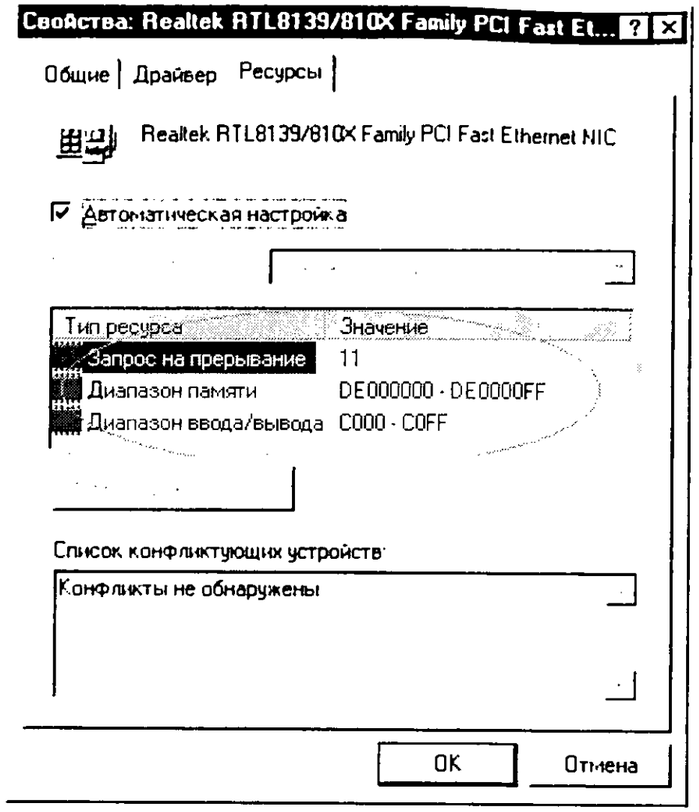


Рис. 6.3. *Ресурсы сетевого адаптера Realtek RTL8139*

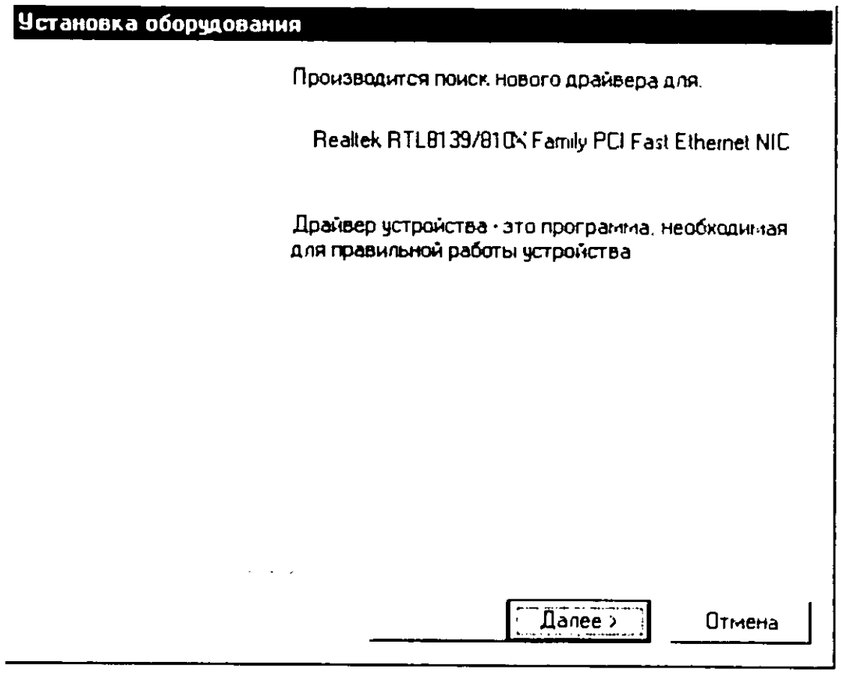


Рис. 6.4. *Обнаружено новое устройство*

Второй вариант (установку стандартного драйвера) нужно выбирать, если у вас нет нужного драйвера. Однако следует помнить, что не всегда операционная система может предложить подходящий драйвер — базы драйверов операционных систем Windows 95/98 безнадежно устарели. Если вы устанавливаете такой же старый сетевой адаптер, вполне вероятно, что операционная система найдет драйвер. Из личного опыта знаю, что Windows 95/98 редко когда находит подходящие драйверы — и это касается не только сетевых плат. Поэтому лучше найти, например, в Internet, драйвер для нужного вам устройства, если у вас его нет. Могу порекомендовать два отличных инструмента для поисков драйверов:

- http://www.drivers.ru/
- http://www.google.com

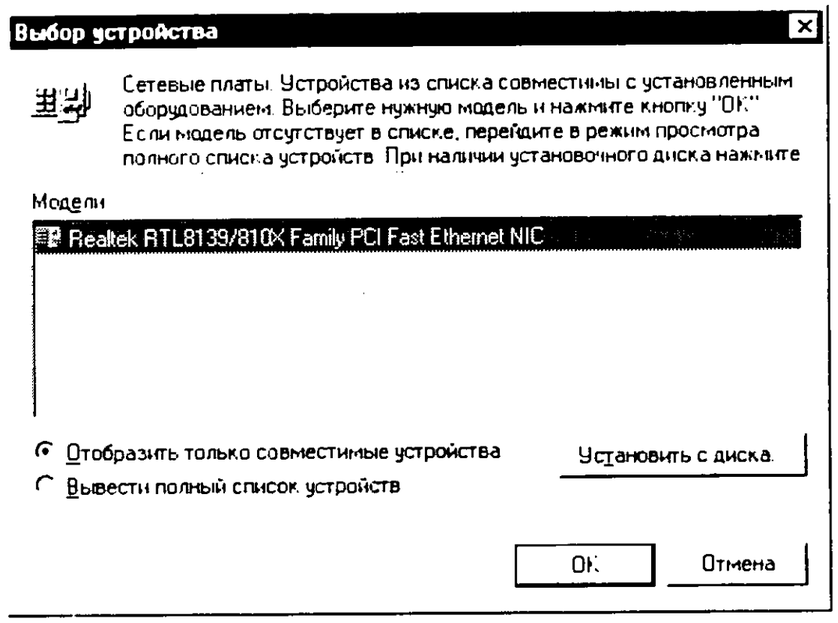


Рис. 6.5. *Операционная система нашла драйвер*

Примечание.

На вышеприведенном рис. 6.5 операционная система Windows 98 нашла драйвер только потому, что данное устройство уже было установлено в системе ранее, а установка драйвера производилась с диска производителя устройства.

Следующий этап — это непосредственная установка файлов драйвера (рис. 6.6). Просто нажмите кнопку **Далее** и немного подождите. Во время установки операционная система может запросить установочный диск — или диск с самой Windows 98 или диск с драйвером. Поэтому не уходите от компьютера слишком далеко: у вас есть шанс почувствовать себя DJ-ем (шутка).

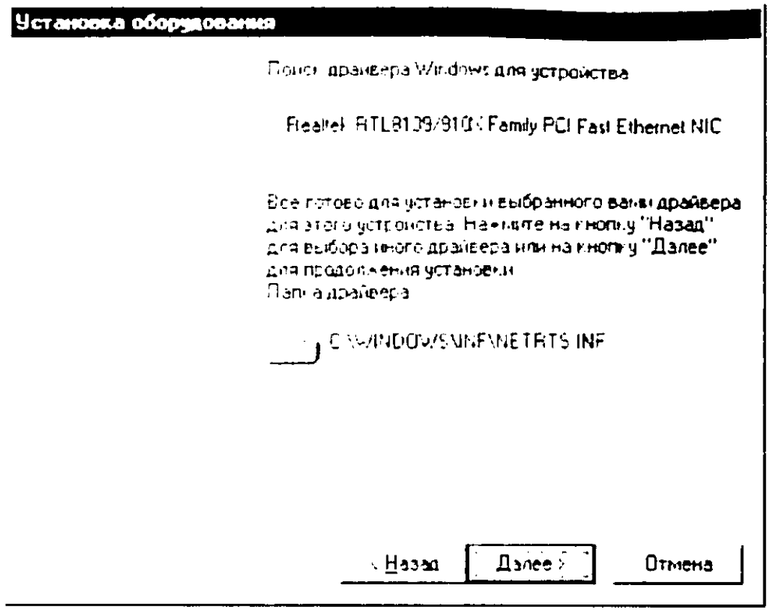


Рис. 6.6. *Установка файлов драйвера*

После установки устройства операционная система предложит вам перезагрузить компьютер — не отказывайтесь: если надо, то надо. После загрузки убедимся, что наша сетевая плата появилась в списке устройств (рис. 6.7).

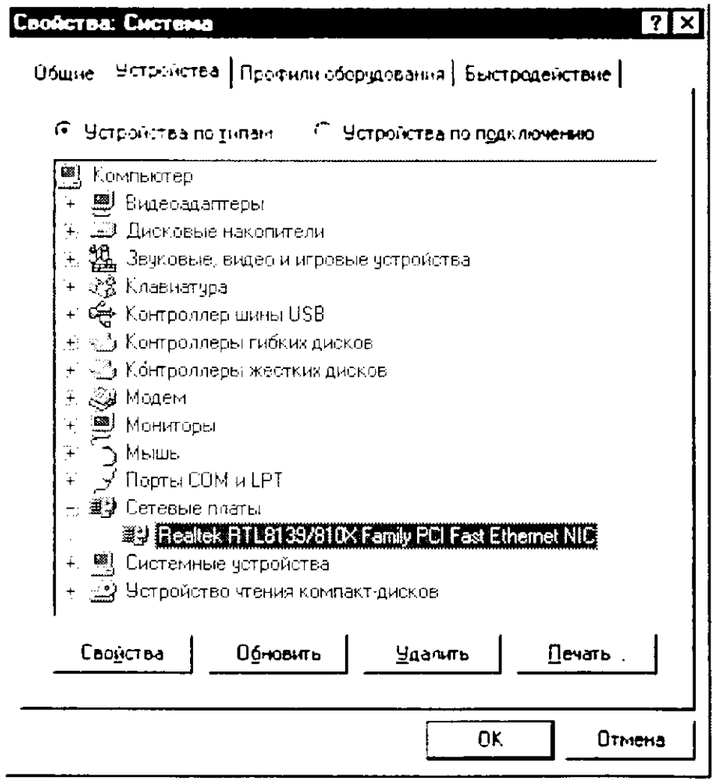


Рис. 6.7. *Наш сетевой адаптер в списке устройств Windows 98*

Примечание.

Для открытия списка устройств вы используете Панель управления (**Панель управления ®Система**)? Запомните комбинацию клавиш Win+Break — так аплет **Система** с Панели управления будет открываться существенно быстрее.

Теперь мы можем просмотреть сведения о файлах драйвера нашего сетевого адаптера. Выделите сетевой адаптер в списке устройств и нажмите кнопку **Свойства**. Затем перейдите на страничку **Драйвер** и нажмите кнопку **Сведения о файле драйвера** (рис. 6.8).

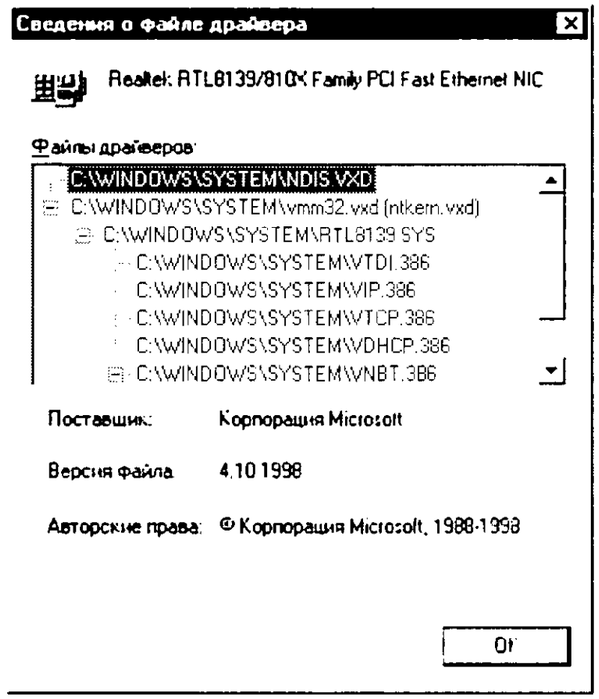


Рис. 6.8. *Сведения о файле драйвера сетевой платы*

Настройка сети

Теперь приступим к непосредственной настройке сети. Откройте апплет **Сеть** с **Панели управления**. При правильной настройке вы должны увидеть конфигурацию сети, показанную на рис. 6.9.

Если сеть на данном компьютере никогда не настраивалась и никогда не устанавливался сетевой адаптер, то конфигурация сети будет пуста (рис. 6.10).

Более надежный способ проверки правильности конфигурации сети — это программа **ipconfig**. Откройте окно **Сеанса MS DOS (Пуск → Сеанс MS DOS)** и введите команду **ipconfig**.

Сейчас настройка сети довольно-таки странна: непонятно откуда взявшийся IP-адрес 169.254.81.180 и сеть класса B. Это параметры по умол-

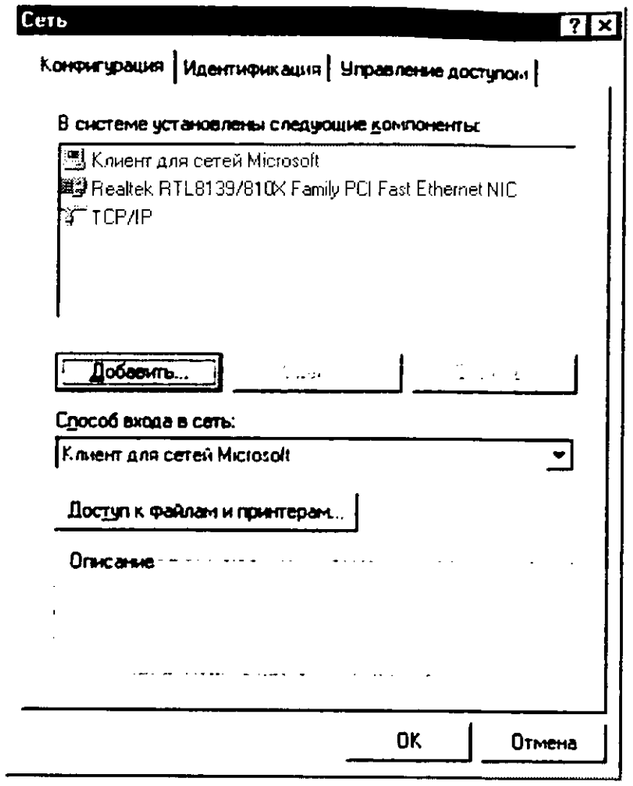


Рис. 6.9. *Правильная конфигурация сети после установки сетевой платы*

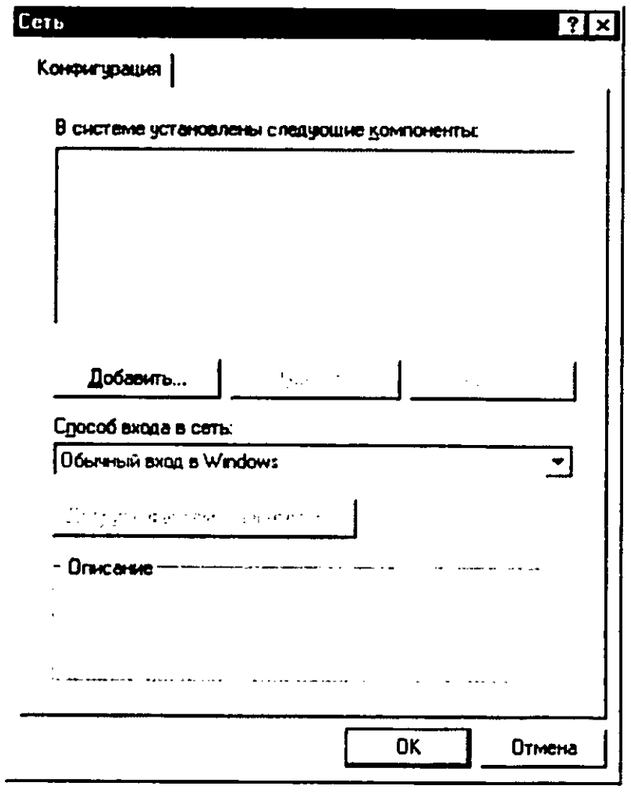


Рис. 6.10. *Пустая конфигурация сети*

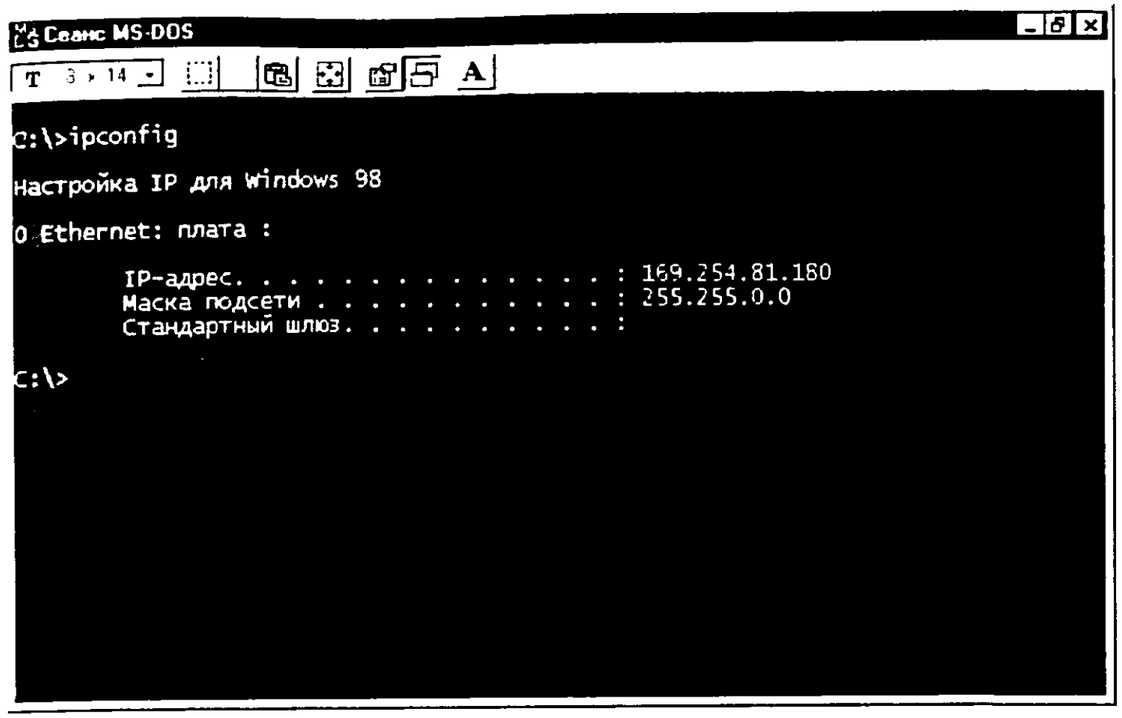


Рис. 6.11. *Программа ipconfig*

чанию, которые, ясное дело, нас не устраивают. Как мы уже договорились, будем использовать IP-адрес 192.168.1.5 и сеть класса C.

Примечание.

Параметры сети по умолчанию находятся в разделе реестра Windows 9x HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\DHCP\DhcpInfo00. Это так называемые параметры DHCP. Протокол DHCP будет подробно рассмотрен далее в этой книге.

Перейдите к окну конфигурации сети (см. рис. 6.10) и откройте свойства протокола TCP/IP. На вкладке **IP-адрес** выберите опцию **Указать IP-адрес явным образом** и укажите IP-адрес 192.168.1.5 и маску сети 255.255.255.0.

Все остальные опции пока оставьте по умолчанию. Конфигурация сети будет записана в раздел HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans\0000 реестра Windows (рис. 6.13). После изменения конфигурации сети Windows предложит перезагрузить систему, не отказывайтесь (рис. 6.14).

После перезагрузки системы проверим конфигурацию сети. Для этого будем использовать две программы — **ipconfig** и **ping**. Откройте окно сеанса MS DOS и сначала введите команду **ipconfig**. Результат представлен на рис. 6.15.

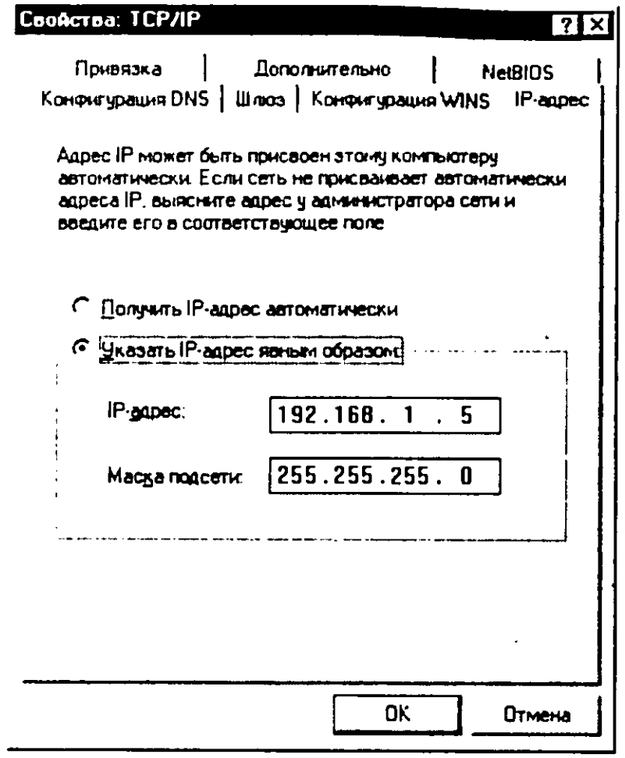


Рис. 6.12. *Указание IP-адреса*

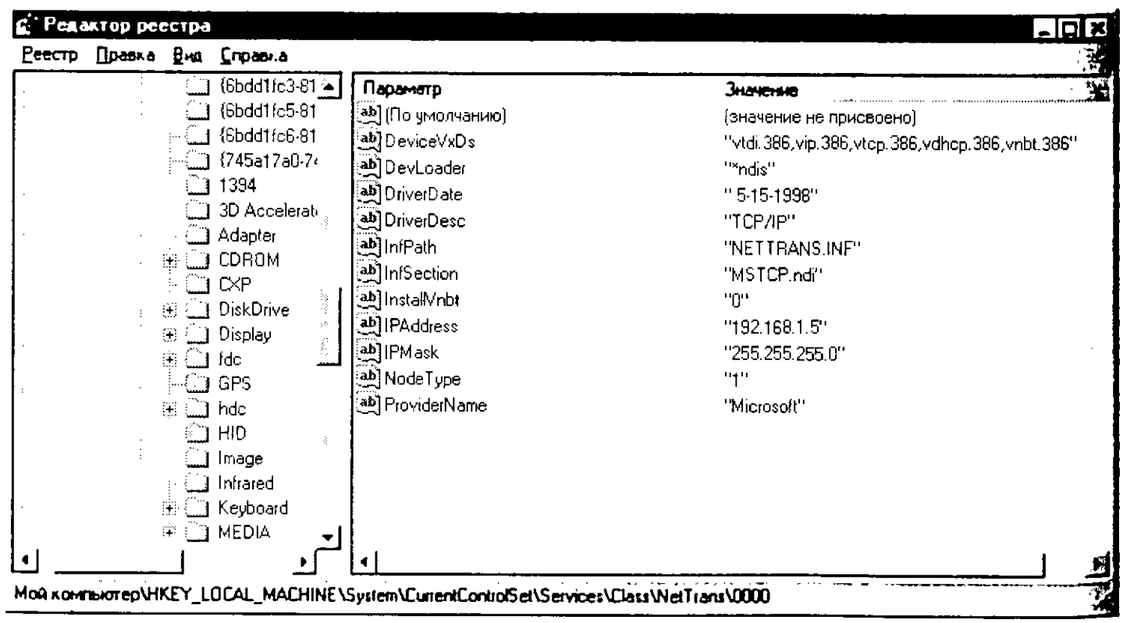


Рис. 6.13. *Конфигурация сети в реестре Windows*

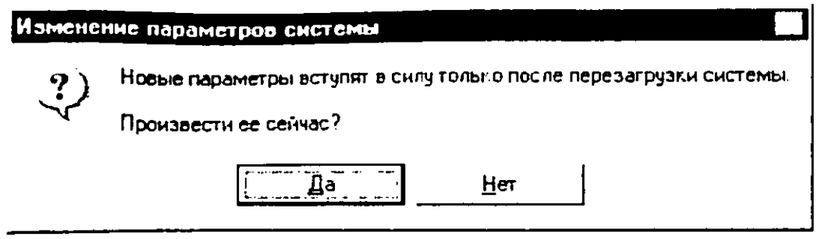


Рис. 6.14. *Перезагрузка компьютера*

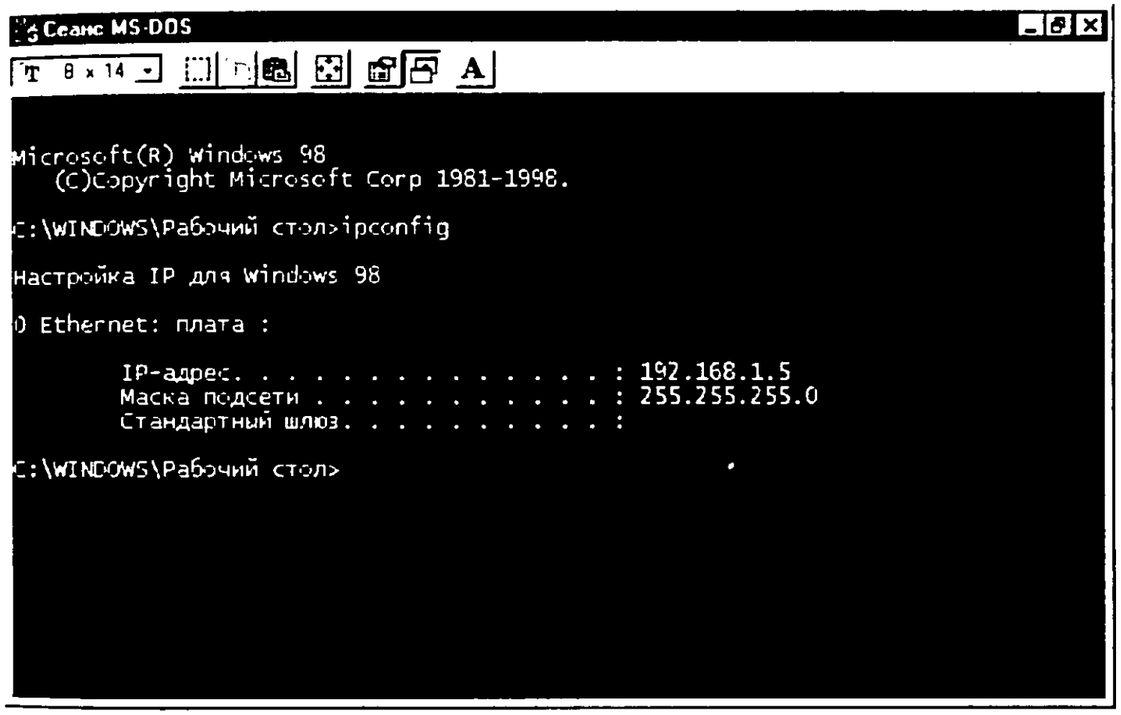


Рис. 6.15. *Конфигурация сети — программа ipconfig*

Почему мы используем программу **ipconfig**, если сразу можно было бы пропинговать узел? Программа **ipconfig** очень полезна при выявлении дублирования IP-адреса. Если вы указали IP-адрес, который уже используется другим узлом в этой подсети, то программа отобразит указанный вами IP-адрес, но маска сети будет 0.0.0.0:

```
Настройка IP для Windows 98
0 Ethernet: плата :
        IP-адрес. . . . . : 192.168.1.5
        Маска подсети . . . . . : 0.0.0.0
        Стандартный шлюз. . .   . :
```

Теперь с нашей конфигурацией все в порядке. Можно попробовать «пропинговать» узел. Для этого введите команду в командной строке сеанса MS DOS:

```
ping 192.168.1.5
```

Если все в порядке, вы получите ответ на каждый запрос программы **ping**:

```
Обмен пакетами с 192.168.1.5 по 32 байт:
Ответ от 192.168.1.5: число байт=32 время<10мс TTL=128
Ответ от 192.168.1.5: число байт=32 время=1мс TTL=128
Ответ от 192.168.1.5: число байт=32 время<10мс TTL=128
Ответ от 192.168.1.5: число байт=32 время<10мс TTL=128
```

Статистика Ping для 192.168.1.5:

```
Пакетов: послано = 4, получено = 4, потеряно = 0 (0% потерь),
```

Приблизительное время передачи и приема:

```
наименьшее = 0 мс, наибольшее =  1 мс, среднее = 0 мс
```

Вот теперь можно пересесть на другой компьютер и попробовать пропинговать с него только что настроенный узел. Скорее всего будет все Ок. Если же программа **ping** сообщит, что узел 192.168.1.5 недоступен, то это будет связано с:

- физическим повреждением среды передачи данных, проверьте сетевой кабель и его подключение к коммутатору или повторителю;
- неправильной настройкой компьютера, на котором запущена программа ping — с нашим компьютером уж точно все в порядке.

Теперь установим имя компьютера и рабочей группы. Откройте апплет **Сеть** и перейдите на вкладку **Идентификация**. Далее введите имя компьютера и рабочей группы (рис. 6.16), после чего перезагрузите машину.

Я же все делал правильно... — возможные неполадки и их устранение

Казалось бы, нет ничего сложного в настройке сети в такой простой операционной системе, как Windows 95/98. Однако на практике все бывает не так просто. Помню, у меня был компьютер, на котором был установлен модем — для доступа к Internet. Модем работал нормально, выполняя возложенную на него задачу — доступ к всемирной Сети.

Спустя некоторое время появилась необходимость подключить компьютер к локальной сети. Драйвер сетевого адаптера был установлен корректно, сетевой адаптер отображался в списке устройств, конфигурация

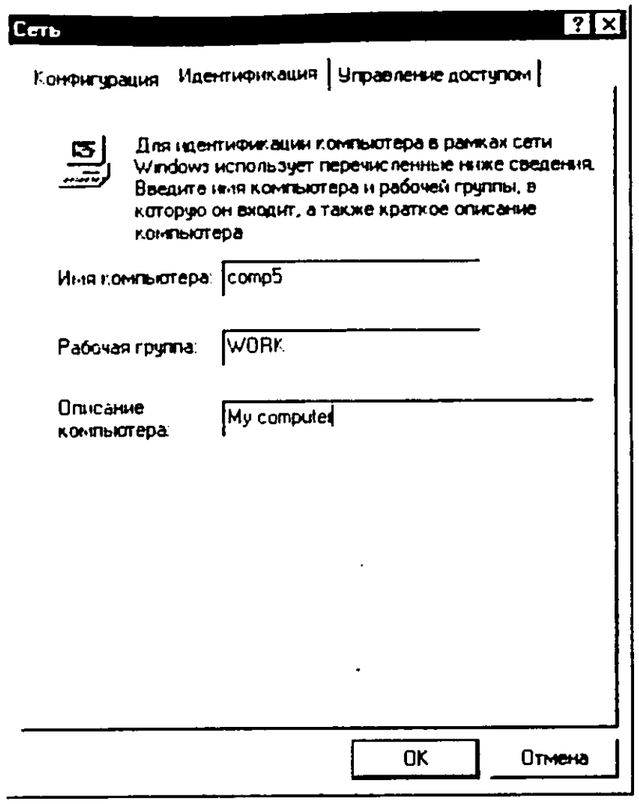


Рис. 6.16. *Установка имени компьютера и рабочей группы.*

сети в аплете **Сеть** Панели управления также была правильной. Но я не то что не мог получить доступ к этому компьютер из локальной сети, я даже не мог пропинговать его локально — команда **ping**, выполнявшаяся на этом компьютере, сообщала что «узел недоступен». Я ввел команду **ipconfig**. Оказалось, что в системе присутствует только контроллер удаленного доступа — это тоже своеобразная сетевая плата для доступа к удаленной сети.

Как оказалось, такое случается довольно часто с операционными системами Windows 95/98 — на языке Microsoft — это «feature», то есть неотъемлемая особенность работы. Лечится это горе довольно просто. Вы должны очистить всю конфигурацию сети: удалить все протоколы, все клиенты, все сетевые адаптеры, включая контроллер удаленного доступа.

Перед перезагрузкой компьютера убедитесь, что сетевой адаптер удален из списка устройств (модем удалять не нужно). После перезагрузки компьютера сконфигурируйте сеть, как было показано выше. А потом добавьте контроллер удаленного доступа. Для этого отройте Панель управления, выберите апплет **Сеть**, нажмите кнопку **Добавить**, выберите компонент **Сетевая плата** и снова нажмите кнопку **Добавить** (рис. 6.17).

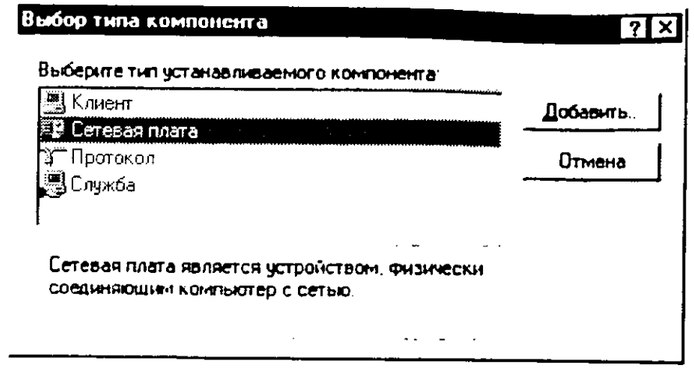


Рис. 6.17. *Добавление сетевой платы*

Выберите изготовителя — компанию Microsoft и сетевую плату **Контроллер удаленного доступа** (рис. 6.18). Измененная конфигурация сети будет такой, как показано на рис. 6.19.

Настройки контроллера удаленного доступа изменять не нужно — оставьте так, как есть.

Примечание.

Настройки удаленного доступа изменять нужно только в том случае, если того требует ваш провайдер. Подробнее вы можете узнать только у него.

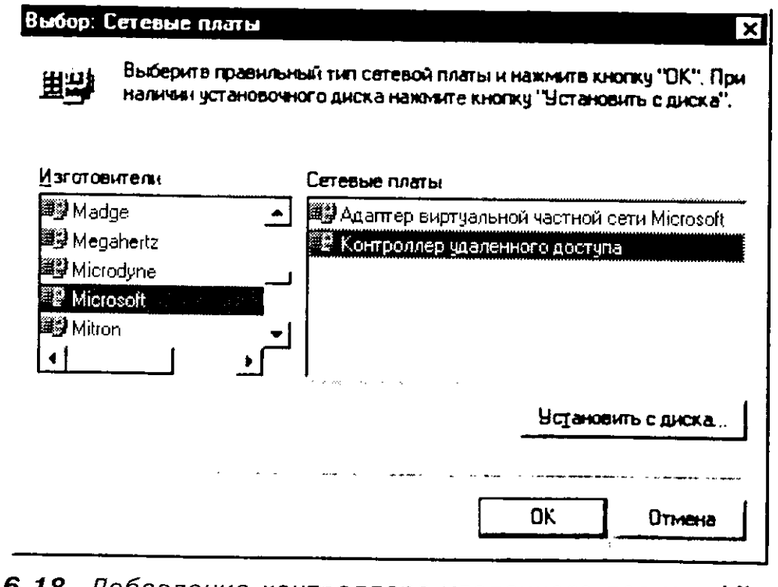


Рис. 6.18. *Добавление контроллера удаленного доступа Microsoft*

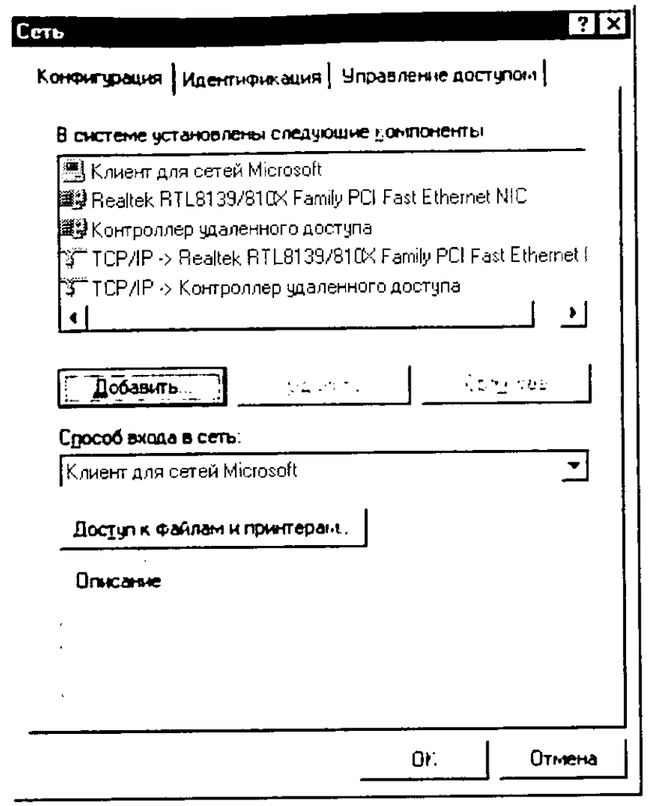


Рис. 6.19. *Конфигурация сети*

Теперь самое время перезагрузить компьютер. После перезагрузки можно проверить конфигурацию сети программой **ipconfig**. Она будет примерно такой:

```
Настройка IP для Windows 98

0 Ethernet: плата :
    IP-адрес. . . . . . . . . . . .: 192.168.1.5
    Маска подсети . . . . . . . . .: 255.255.255.0
    Стандартный шлюз. . . . . :
1 Ethernet: плата :
    IP-адрес. . . . . . . . . . . . : 0.0.0.0
    Маска подсети . . . . . . . . . : 0.0.0.0
    Стандартный шлюз. . . . . :
```

Кстати говоря, если вам по каким-то причинам неудобно использовать программу **ipconfig**, вы можете использовать ее аналог с графическим интерфейсом — **winipcfg**. Ее окно продемонстрировано на рис. 6.20.

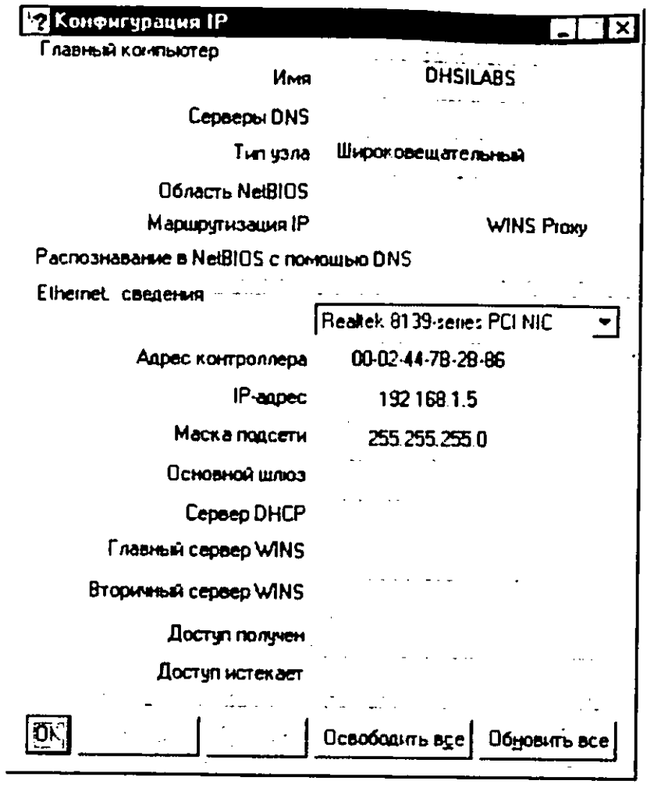


Рис. 6.20. *Программа winipcfg*

Неправильная работа с контроллером удаленного доступа — это далеко не единственный камень преткновения, но сейчас мы не будем рассматривать всевозможные причины сетевых неполадок — они обсуждаются в главе **Поиск неисправностей**.

6.2.2. Настройка сетевой карты и сетевого взаимодействия в Windows ME

Установка и настройка сетевой карты

Установка сетевого адаптера в Windows ME очень схожа на установку сетевой платы в Windows 98. Однако есть свои отличия, но мы не будем на них останавливаться отдельно, а опишем процесс установки от начала и до конца.

При загрузке операционная система обнаружит новое устройство и попытается установить для него драйвер. База драйверов операционной системы Windows ME существенно больше, чем в операционных системах Windows 95/98. Но все же лучше использовать драйвер производителя, если таковой имеется, тем более, что поиск драйвера в операционной системе Windows ME более гибок и производится быстрее, чем в Windows 98.

После установки драйвера сетевого адаптера нужно как обычно перезагрузить компьютер. Когда компьютер загрузится, нажмите Win+Break, чтобы убедиться в наличии сетевого адаптера в списке устройств (рис. 6.21).

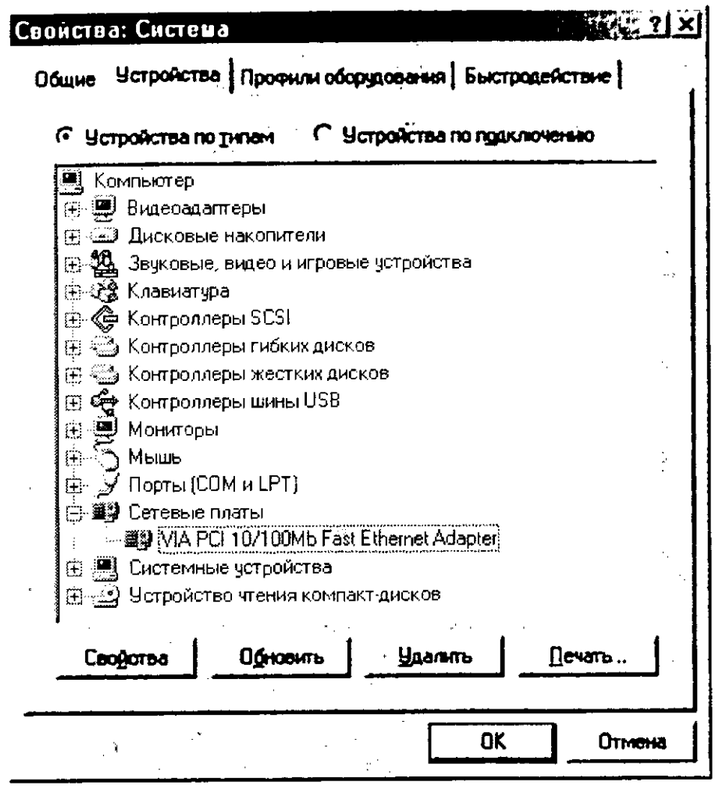


Рис. 6.21. *Список устройств Windows ME*

Чтобы просмотреть информацию о драйвере устройства, выделите сетевой адаптер в списке устройств и нажмите кнопку **Свойства**. Затем перейдите на страничку **Драйвер** и нажмите кнопку **Сведения о файле драйвера**. В результате вы получите нужную информацию (рис. 6.22).

Конфигурирование сетевого адаптера как устройства в Windows ME практически ничем не отличается от Windows 98. Как и в Windows 98 вам не придется вводить ни IRQ, ни диапазон ввода/вывода, ни другие аппаратные ресурсы. Но в Windows ME появилась одна очень удобная опция — **Управление электропитанием**. Перейдите на одноименную страницу свойств сетевого адаптера (рис. 6.23).

На этой странице вы найдете две опции:

- Разрешить выключение этого устройства.
- Разрешить этому устройству пробуждать компьютер.

Рис. 6.22. Сведения о файле драйвера сетевого адаптера

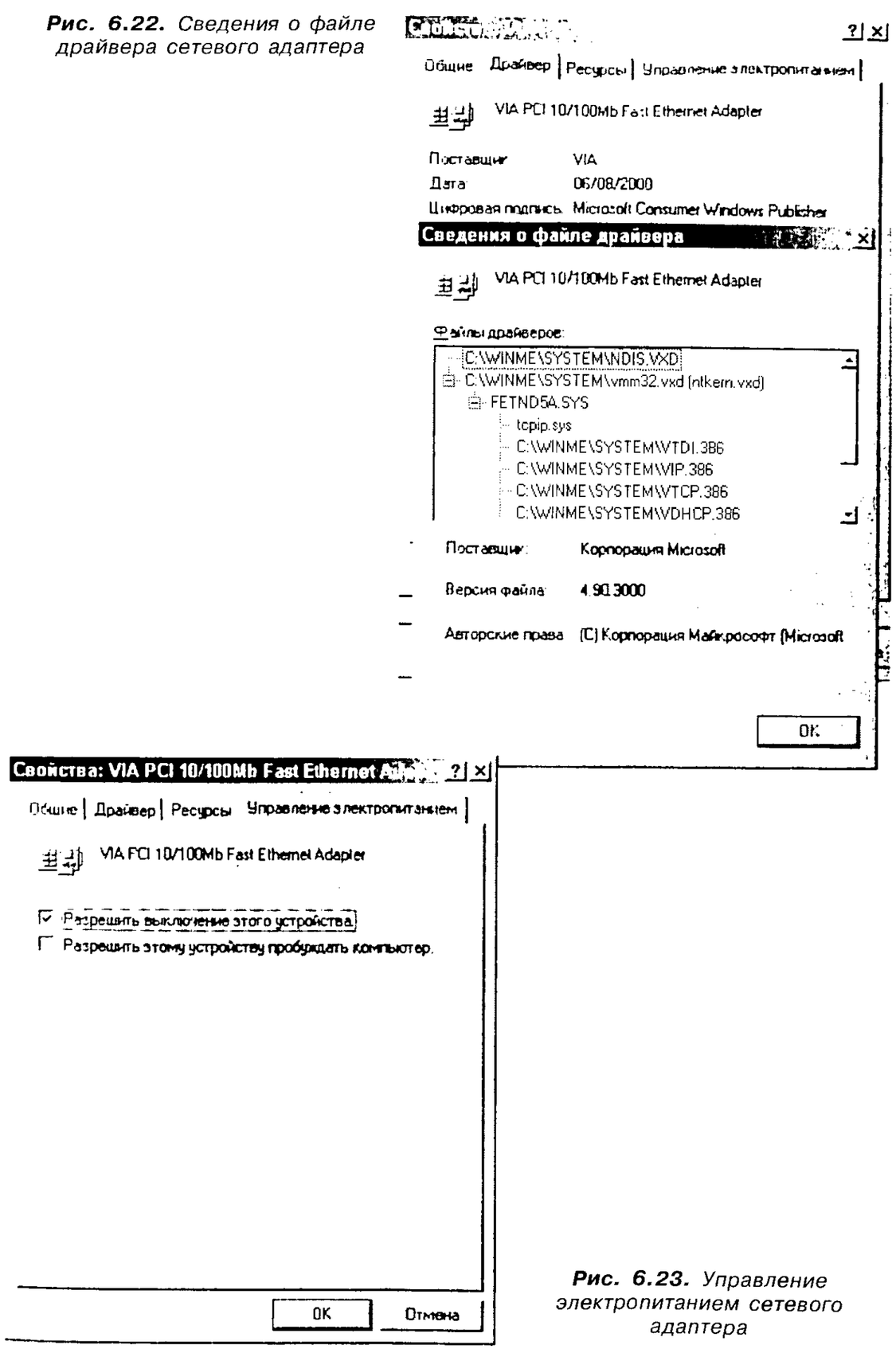


***Рис. 6.23.** Управление электропитанием сетевого адаптера*

Думаю, они в особенных комментариях не нуждаются. Нужно, правда, заметить, что последняя как бы реализует функцию WOL (Wake On LAN) — пробуждение по сети. Как только будет получение прерывания от этого устройства (сетевой платы), компьютер сразу же «проснется».

Первоначальная конфигурация сети будет такой как показано на рис. 6.24.

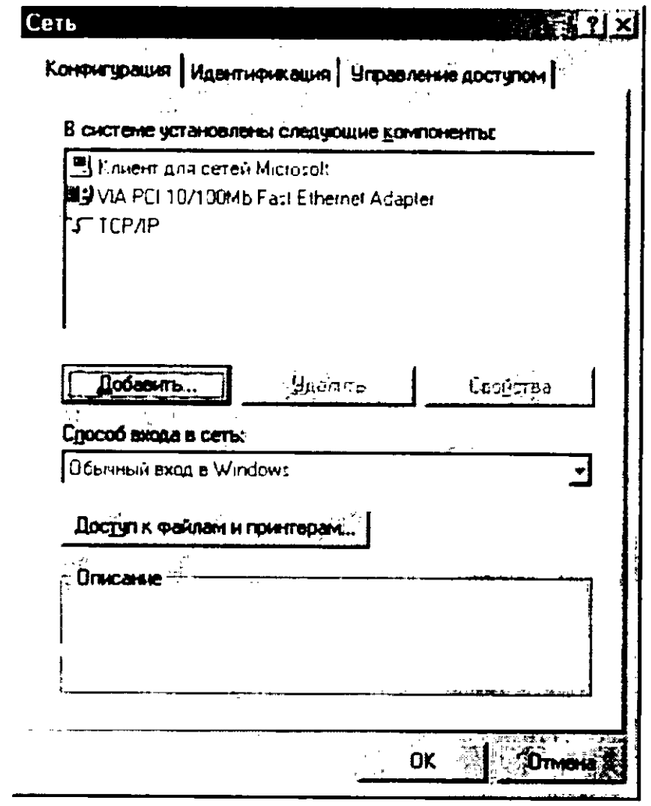


***Рис. 6.24.** Первоначальная конфигурация сети*

Теперь откройте окно сеанса MS DOS и введите программу **ipconfig**. Если вы читали предыдущий пункт, вы уже знакомы с этой программой. Вывод программы будет следующим:

```
C:\WINME\Рабочий стол>ipconfig
Конфигурация IP-адресов Windows
0 Ethernet: плата :
    Состояние носителя. . . . : Отключен
    IP-адрес. . . . . . . . . . . . . : 0.0.0.0
    Маска подсети . . . . . . . . : 0.0.0.0
    Стандартный шлюз. . . . . :
```

Это означает, что наш сетевой адаптер корректно установлен в системе, но параметры сети еще не указаны.

Настройка сети

Самое время настроить сеть. Откройте апплет **Сеть** с Панели управления. Установим свойства протокола TCP/IP, как показано на рис. 6.25.

Как и договаривались, будем использовать IP-адрес 192.168.1.5 и маску сети 255.255.255.0. Все остальные параметры изменять пока не нужно. После этого дважды нажмите **Ок** и согласитесь на перезагрузку компьютера (рис. 6.26).

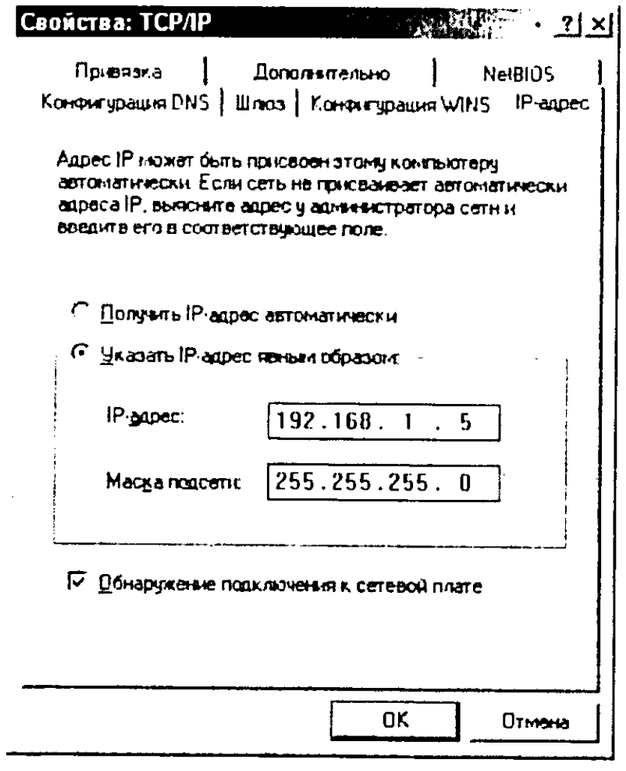


Рис. 6.25. *Параметры протокола TCP/IP*

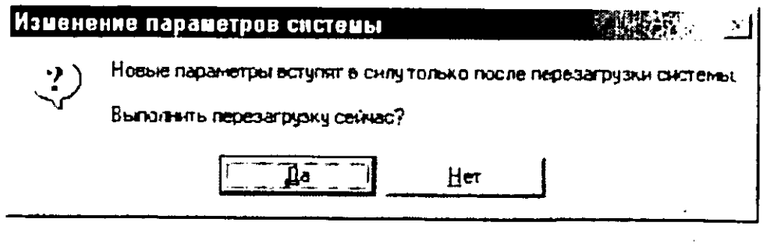


Рис. 6.26. *Перезагрузить?*

После перезагрузки компьютера нужно протестировать созданную нами конфигурацию сети. Мы будем использовать программу **ipconfig** — проверки самой конфигурации и программу **ping** — для того, чтобы проверить соединение. Вывод программы **ipconfig** будет таким:

```
C:\WINME\Рабочий стол>ipconfig
Конфигурация IP-адресов Windows
0 Ethernet: плата :
     IP-адрес. . . . . . . . . . . : 192.168.1.5
     Маска подсети . . . . . . . . : 255.255.255.0
     Стандартный шлюз. . . . . :
C:\WINME\Рабочий стол>ping 192.168.1.5
```

А программа **ping** в результате своей работы выведет следующее:

```
Обмен пакетами с 192.168.1.5 по 32 байт:
Ответ от 192.168.1.5: число байт=32 время<10 мс TTL=128
Ответ от 192.168.1.5: число байт=32 время<10 мс TTL=128
Ответ от 192.168.1.5: число байт=32 время<10 мс TTL=128
Ответ от 192.168.1.5: число байт=32 время<10 мс TTL=128
Статистика Ping для 192.168.1.5:
    Пакетов: послано = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время передачи и приема:
    наименьшее = 0 мс, наибольшее =  0 мс, среднее =  0 мс
```

Небольшая информация для справки. Текущая сетевая конфигурация для нашей сетевой платы хранится в разделе HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans\0000 реестра Windows ME (рис. 6.27).

Если вы не читали предыдущий пункт, можете спросить: «А зачем мы используем ipconfig — ведь, если ping не проходит, то настройки неправильны?». Так-то оно так, но программа **ipconfig** позволяет проверить дублирование IP-адреса. Если он дублируется, то есть в вашей подсети есть еще один компьютер с таким же именем, то в выводе ipconfig маска сети будет 0.0.0.0.

Вы успешно «пропинговали» свой компьютер? Тогда самое время пересесть за другой, соседний, и «пропинговать» только что настроенный компьютер. В большинстве случаев все будет в порядке. Если же «пинги» не доходят до узла 192.168.1.5 (который мы только что настроили), значит, тут возможны два варианта:

- Повреждена физическая среда передачи данных — проверьте кабель, не поврежден ли он. Если нет, проверьте подключение к коммутатору или повторителю. Также стоит проверить, правильно

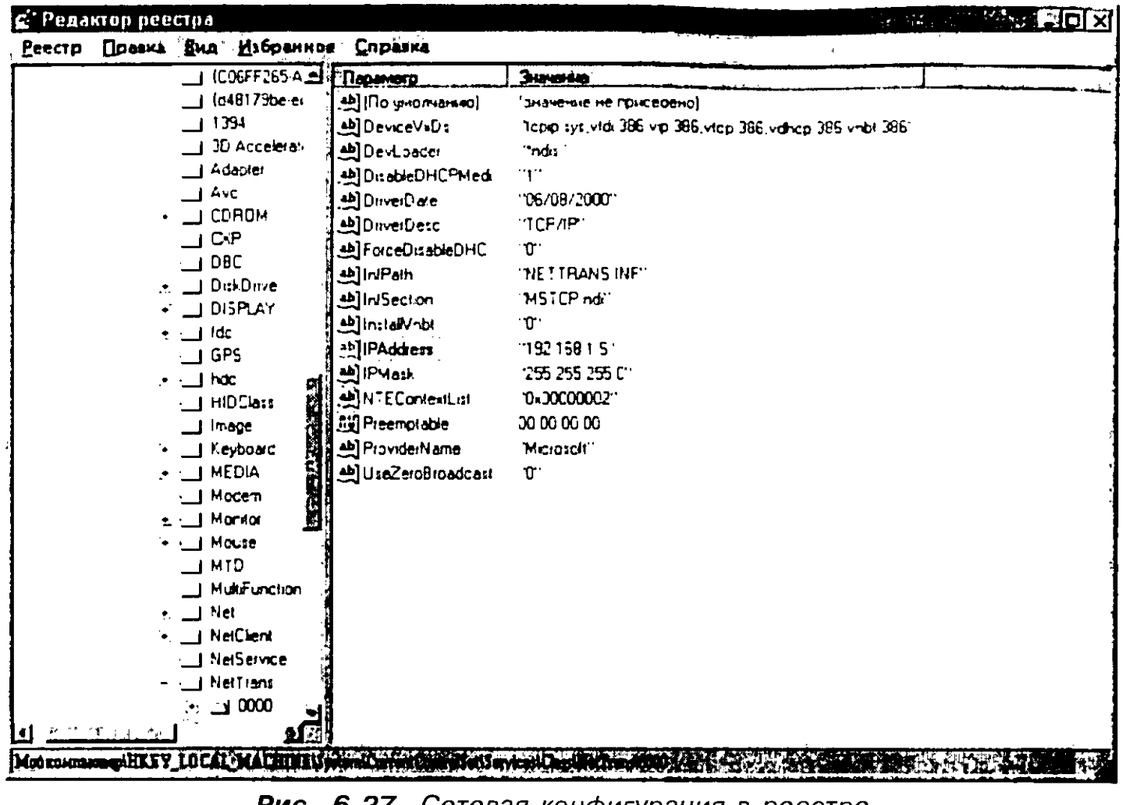


Рис. 6.27. *Сетевая конфигурация в реестре*

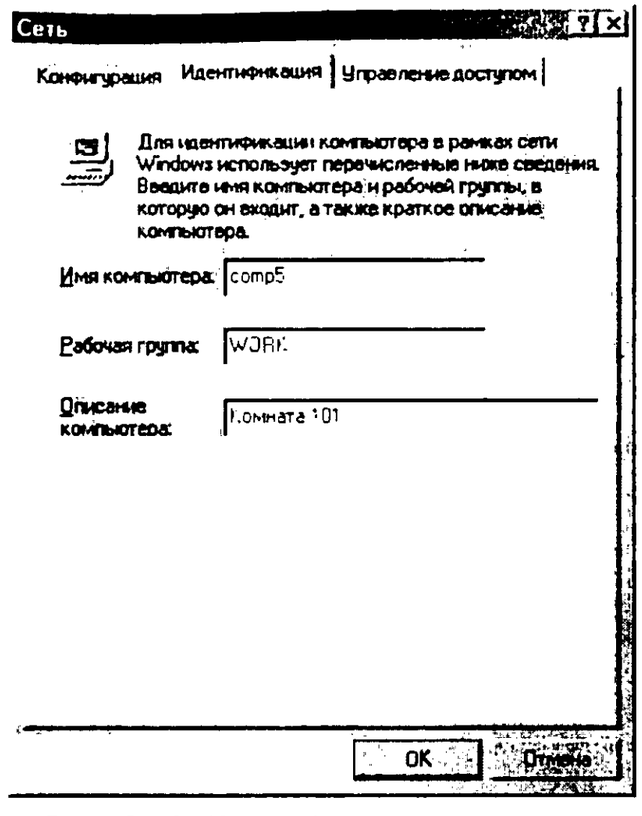


Рис. 6.28. *Идентификация компьютера*

ли обжат кабель. Если кабель обжат неправильно, на повторителе (или коммутаторе) не будет гореть соответствующий индикатор. Также проверьте включен ли сам повторитель.

- Неправильные настройки второго компьютера. Проверить это можно, пропинговав другом компьютер со своего, только что настроенного.

После настройки сетевого адаптера и протокола TCP/IP нужно установить имя компьютера и рабочей группы — COMP5 и WORK, соответственно. Для этого откройте апплет **Сеть** с Панели управления и перейдите на страничку **Идентификация**. Затем введите указанные параметры (рис. 6.28) и перезагрузите машину.

Сеть не настраивается!

Вы делаете все правильно, шаг за шагом, а ваш узел все равно не доступен, а программа **ipconfig** хоть и видит вашу сетевую плату, но в упор не хочет изменять ни IP-адрес, ни сетевую маску. Ее вывод следующий:

```
Конфигурация IP-адресов Windows
0 Ethernet: плата :
      IP-адрес. . . . . . . . . . . . : 0.0.0.0
      Маска подсети . . . . . . . . . : 0.0.0.0
      Стандартный шлюз. . . . . :
```


Не спешите переустанавливать Windows и удалять все протоколы (он у нас всего один) и сетевые адаптеры (тоже один). В свойствах протокола TCP/IP отключите режим **Обнаружение подключения к сетевой плате**. Сеть у вас не будет настраиваться до тех пор, пока компьютер не будет по настоящему подключен к коммутатору или повторителю. А он просто может быть выключен или вы пока еще не подключили сетевой кабель к нему (только обжали, или даже еще не обжимали).

Если вы читали предыдущий пункт, могу вас обрадовать: в Windows ME нет такой «feature», когда невозможно настроить сетевой адаптер, если был установлен контроллер удаленного доступа или другой сетевой адаптер, до тех пор, пока все не удалишь и не настроишь заново. Во всяком случае, мною данная особенность замечена не была.

6.2.3. Настройка сетевой карты и сетевого взаимодействия в Windows NT 4.0

Сегодня редко кто устанавливает Windows NT — домашние и корпоративные пользователи уже давно перешли на Windows 2000 или Windows XP. Сборщики компьютеров поголовно устанавливают Windows XP или,

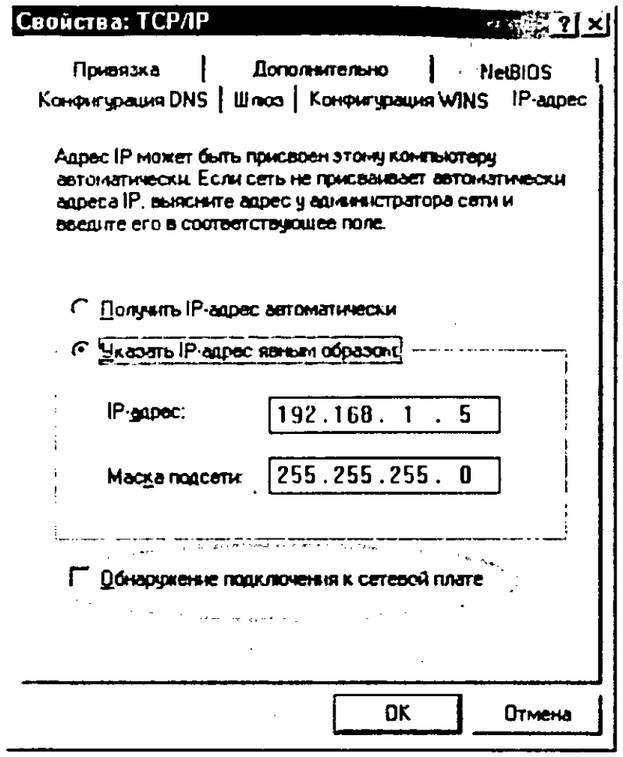


Рис. 6.29. *Обнаружение подключения к сетевой плате*

в крайнем случае, Windows 98, несмотря на то, что она давно уже не продается (к счастью, «Реаниматоров» на наш век хватит).

Однако Windows NT (как Workstation, так и Server) была очень распространена в 1997...1999 годах, особенно часто она устанавливалась на рабочие станции средних и больших предприятий. Поэтому, если в вашей сети более 10 компьютеров, то вероятность «встретить» NT 4.0 довольно велика — хотя бы один компьютер, да и найдется. Как и любой нормальный Windows, NT тоже нуждается в периодической переустановке, а это означает, что рано или поздно вам придется настраивать эту систему «с нуля».

Что же касается установки Windows NT, позволю себе несколько советов. Во-первых, перед запуском программы установки Windows NT (файл winnt.exe) нужно запустить программу SmartDrive (файл smartdrv.exe) — так установка операционной системы пройдет заметно быстрее.

Во-вторых, если вы планируете установить Windows NT на файловую систему FAT, а не NTFS4, то проследите, чтобы FAT был 16-разрядным: Windows NT не поддерживает файловую систему FAT32. Точнее, поддерживает, но после установки. Для поддержки FAT32 нужно установить один из сервис-паков (Service Pack). Какой именно — не помню.

В-третьих, если вы запускаете программу установки Windows NT с FAT-раздела (который тоже должен быть FAT16!), не забудьте перед установкой выполнить команду LOCK. Данная программа разрешает прямой доступ к диску приложениям — без этого Windows NT установить невозможно.

И, наконец, последний совет. Чтобы отказаться от создания всем известных «трех дискет», которые так и хочет создать программа установки Windows NT, нужно запустить программу установки с параметрами /b и /s. Первый параметр, собственно, и есть отказ от создания этих установочных дискет, а второй параметр задает каталог, в котором находится дистрибутив Windows NT.

Итак, общая последовательность действий при установке Windows NT:

1. Обеспечиваем кэширование чтения и записи для жесткого диска:

   ```
   C:\...\smartdrv
   ```

2. Разрешаем прямой доступ к диску:

   ```
   lock
   ```

3. Запускаем программу установки. Дистрибутивный каталог — c:\i386ws.rus:

   ```
   c:\i386ws.rus\winnt.exe /b /s:c:\i386ws.rus
   ```

Ну а дальше — вы сами справитесь. Там нет ничего сложного. Кроме, разве что, серийного номера. Если вы его забыли, то подойдет 112-111111.

Все иллюстрации в этой книге соответствуют русской версии Windows NT Workstation 4.0. Во время установки операционная система сама распознала мой сетевой адаптер. Скажем прямо, такое бывает не часто, поэтому лучше не надеяться на то, что вам повезет так же, как и мне, а приготовить диск с драйвером сетевой платы для Windows NT 4.0. Напомню, что установку нового устройства в Windows NT нужно производить, зарегистрировавшись в системе как Администратор или как пользователь, относящийся к группе администраторов.

Чтобы установить сетевую плату, отройте **Панель управления** Windows NT и выберите апплет **Сеть** (рис. 6.30).

В окне **Сеть** перейдите на вкладку **Адаптеры** и нажмите кнопку **Добавить**. Конечно, можно попытаться найти в списке ваш сетевой адаптер (рис. 6.31), но, скорее всего, его там не будет, поскольку база драйверов Windows NT устарела так же, как и сама операционная система.

Поэтому лучше сразу вставить диск с драйвером и нажать кнопку **Установить с диска**. Дальше, я думаю, вы справитесь без моей помощи.

Когда драйвер сетевой платы установлен, и она отображается на вкладке **Адаптеры** окна **Сеть** (см. рис. 6.32), можно приступить к настройке сети.

На вкладке **Компьютер** (см. рис. 6.30) можно задать имя компьютера и имя рабочей группы. Как мы договорились, наш компьютер будет называться COMP5, а рабочая группа — WORK. Поэтому смело нажимайте кнопку **Из-**

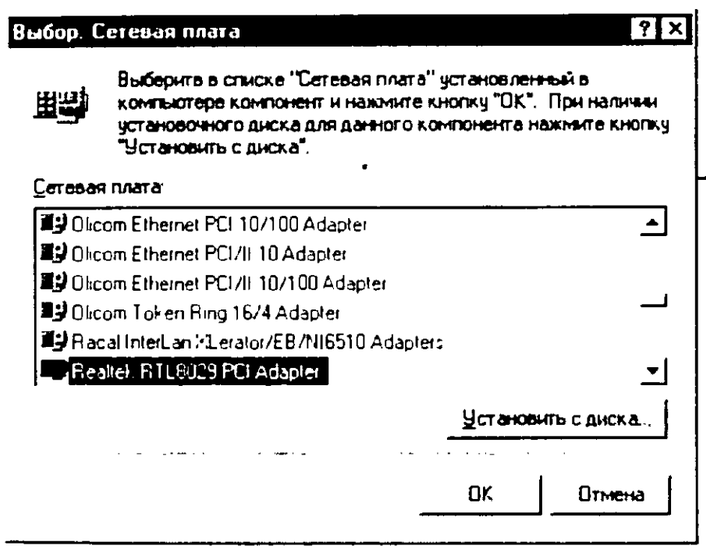


Рис. 6.31. *Выбор сетевого адаптера*

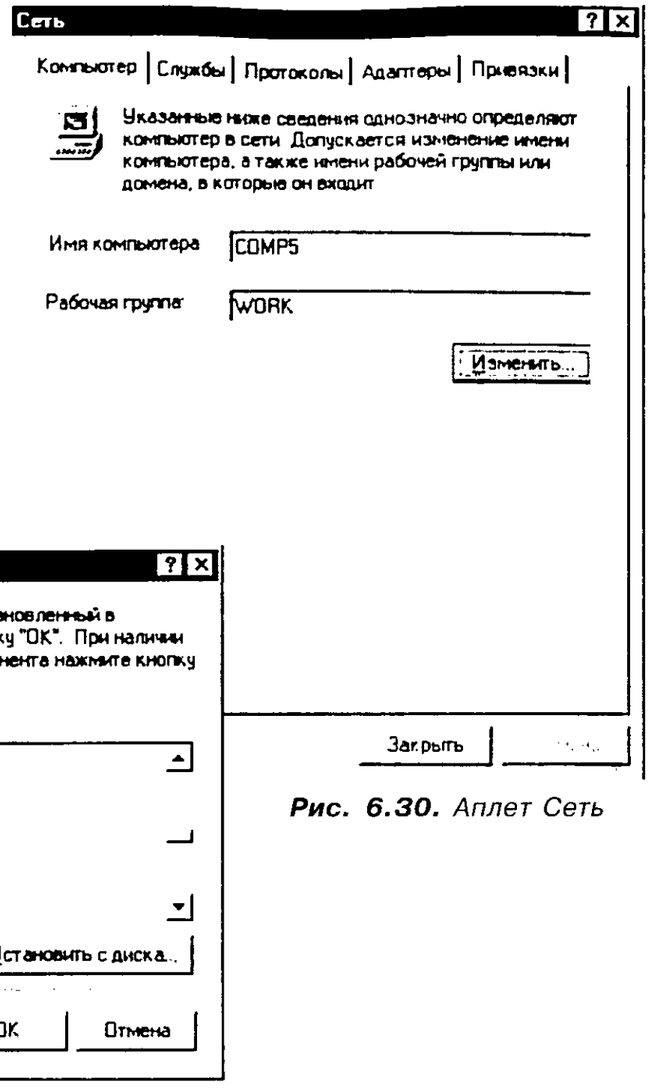


Рис. 6.30. *Аплет Сеть*

менить и вводите новые параметры, если, конечно, они вас устраивают — ведь имена компьютера и рабочей группы у вас будут другими.

На страничке **Службы** отображаются установленные сетевые службы (см. рис. 6.33). Здесь же можно настроить все сетевые службы, но пока мы не будем этого делать, а займемся настройкой протокола TCP/IP.

На страничке **Протоколы** перечислены установленные протоколы. Выделите протокол TCP/IP и нажмите кнопку **Свойства** (рис. 6.34).

Сейчас от нас требуется всего лишь установить IP-адрес компьютера и сетевую маску. Ни дополнительные параметры, ни параметры DNS, ни маршрутизации мы изменять пока не будем — оставим все как есть (рис. 6.35). В дальнейшем мы разберемся с каждым параметром.

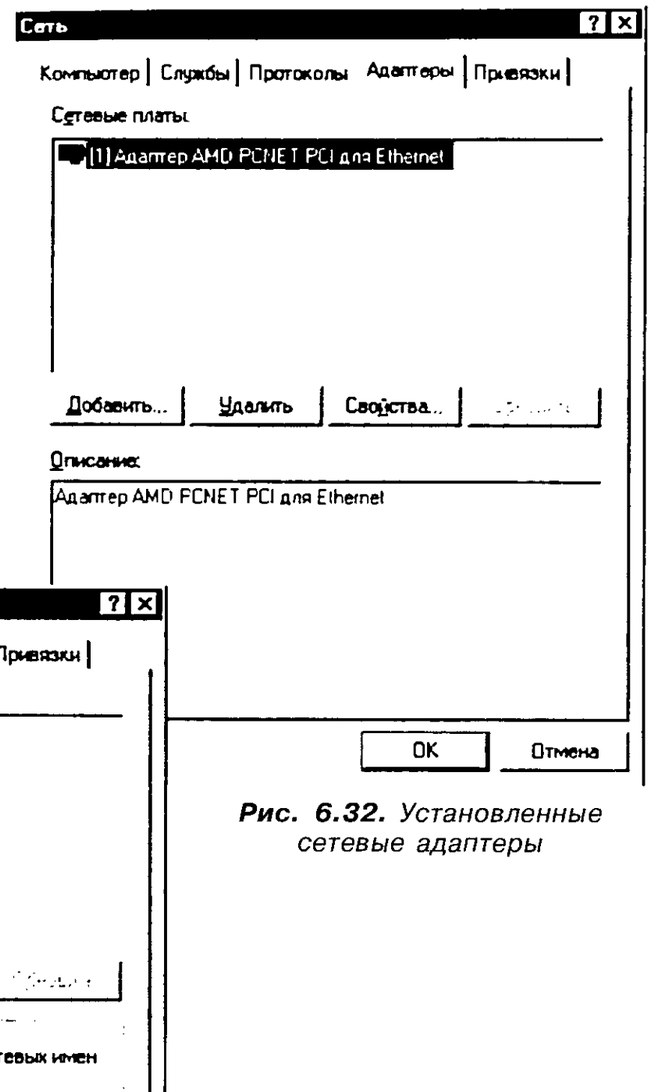


Рис. 6.32. *Установленные сетевые адаптеры*

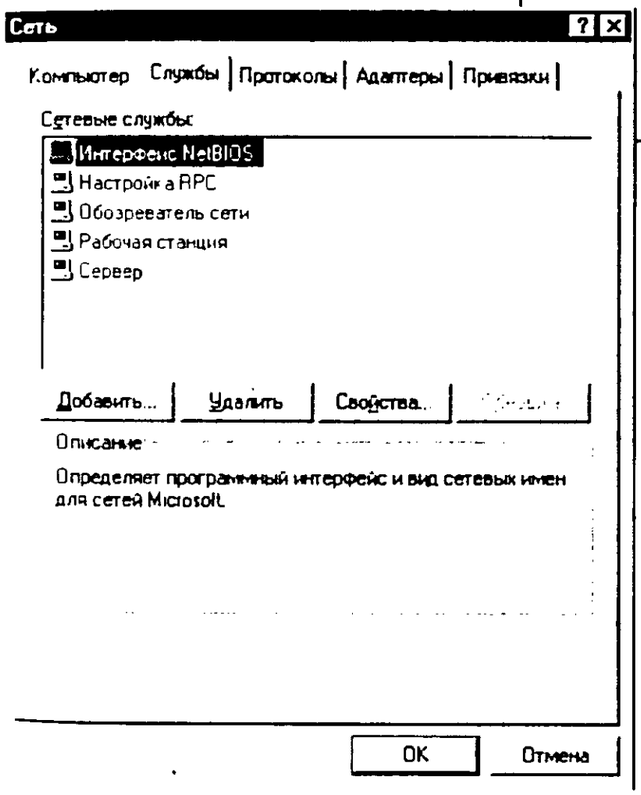


Рис. 6.33. *Сетевые службы*

Установите IP-адрес 192.168.1.5 и маску сети 255.255.255.0. Дважды нажмите Ок, и можно приступить к тестированию сети. Перезагружать Windows NT не нужно, хотя в какой-то книге, написанной сертифицированным специалистом Microsoft, рекомендуется перезагрузить компьютер после изменения настроек сети.

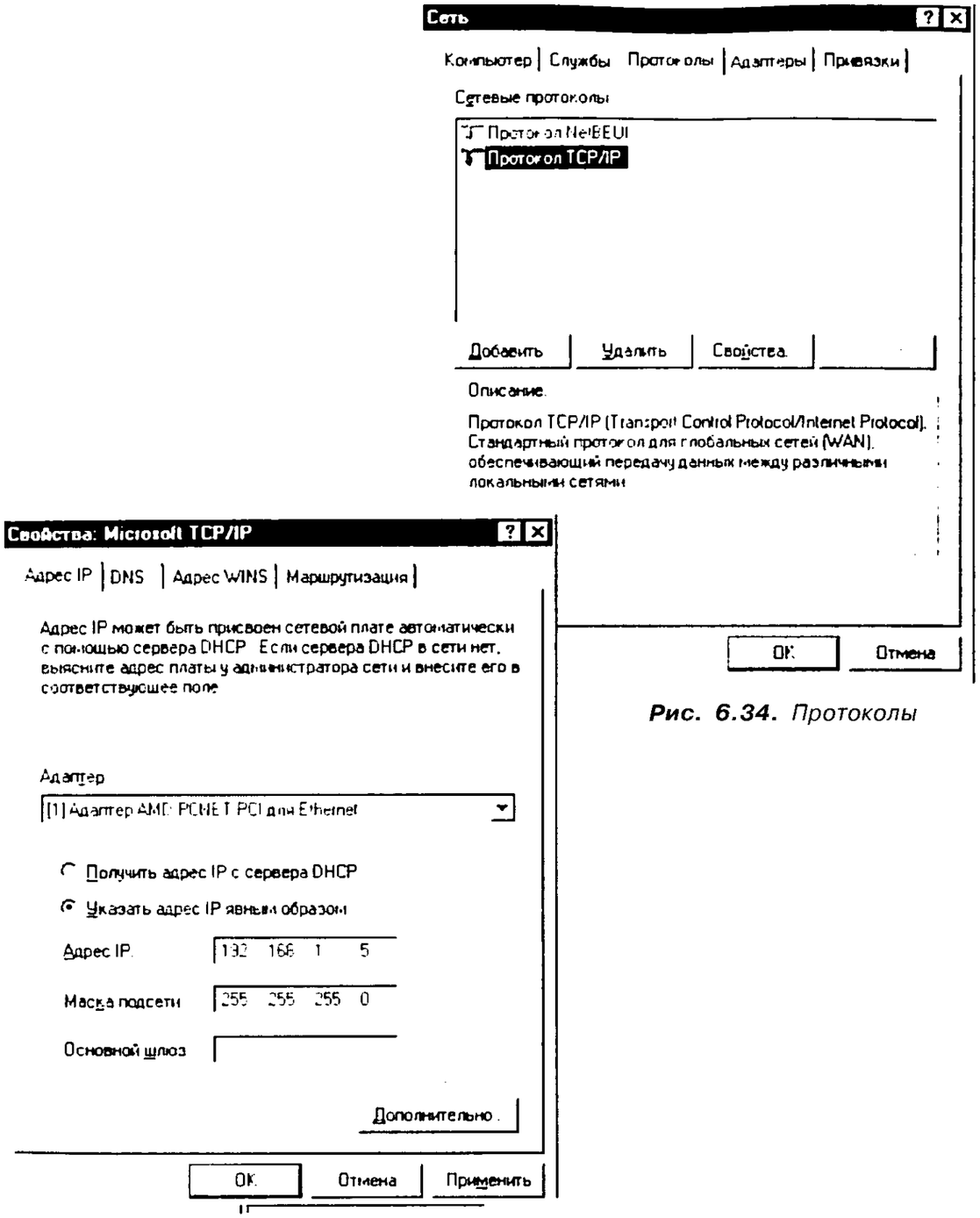


Рис. 6.34. *Протоколы*

Рис. 6.35. *Параметры протокола TCP/IP*

Следовать или нет этой рекомендации — дело ваше. У меня все заработало без перезагрузки, поэтому, чтобы зря не терять время — попробуйте «пропинговать» сами себя:

```
ping 192.168.1.5
```

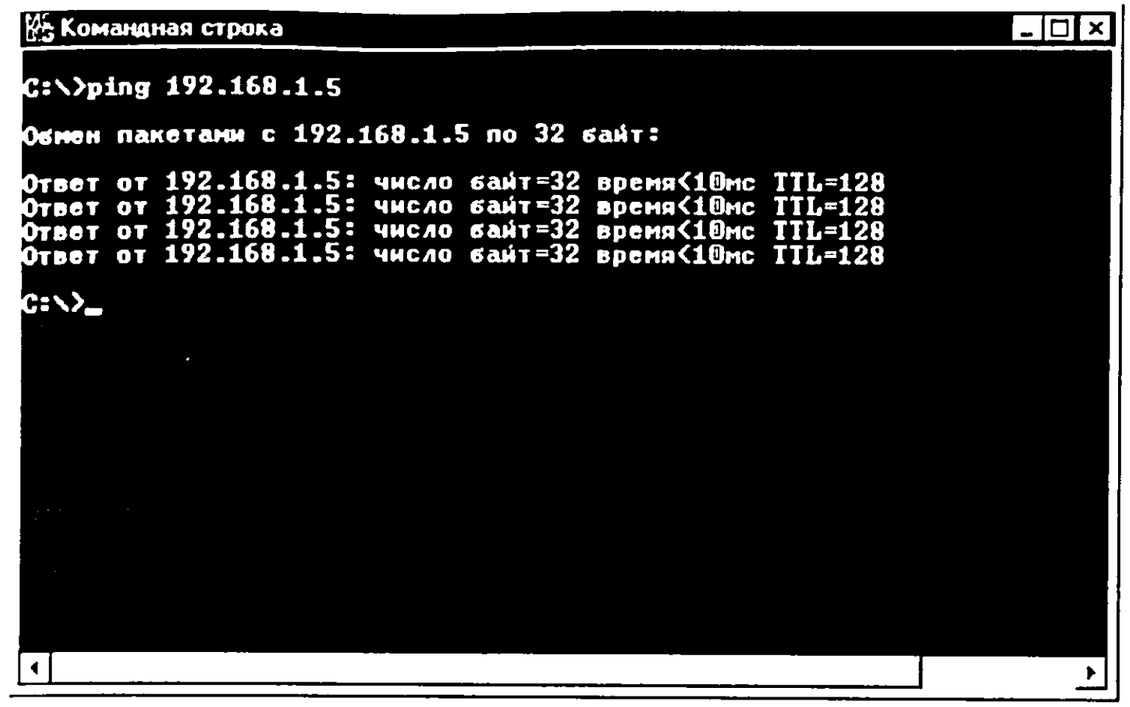



Рис. 6.36. *Программа ping*

Если ответ получен (рис. 6.36), значит, все нормально — теперь можно попробовать пропинговать другой узел. Если другой узел не отвечает, то следует проверить:

- Физическую среду передачи данных — возможно, ваш сетевой кабель поврежден или просто отключен.
- Настройки удаленного компьютера. А может, он вообще выключен?

Если же ответ от «самого себя» не получен, то сначала попробуйте перезагрузить компьютер. Если это не помогает, удалите сетевой адаптер, установите его снова и повторите настройку сети заново. Сеть опять не настраивается? Тогда убедитесь в исправности самого сетевого адаптера — возможно, он неисправен. Лучше средство — возьмите заведомо исправный сетевой адаптер, установите его в системный блок и попытайтесь настроить сеть, используя новый сетевой адаптер.

Также не помешает проверить конфигурацию сети программой **ipconfig**. При правильной настройке вывод **ipconfig** будет следующим:

```
Microsoft(R) Windows NT(TM)
(C) 1985-1996 Microsoft Corp.
C:\>ipconfig
Настройка протокола IP для Windows NT
```

```
Адаптер Ethernet AMDPCN1:
        Адрес IP . . . . . . . . . . . . : 192.168.1.5
        Маска подсети. . . . . . . . . . : 255.255.255.0
        Основной шлюз. . . . . . . . . . :
```

Если сетевая маска равно 0.0.0.0, значит, указанный вами IP-адрес уже используется в вашей локальной сети: операционная система обнаружила это и заблокировала ваш компьютер, дабы не возник конфликт IP-адресов.

6.2.4. Настройка сетевой карты и сетевого взаимодействия в Windows 2000

Windows 2000 — это та же NT, но с более расширенными функциями, фактически — это пятая версия Windows NT. Наиболее важными функциями Windows 2000 являются: поддержка PnP (самонастраивающихся устройств), служба каталогов ActiveDirectory, расширенная база драйверов устройств и дружественный интерфейс пользователя. Конечно, это далеко не все новшества в Windows 2000 (или как любят сокращать американцы, да и не только — W2K), но в данный момент для нас важны именно вышеперечисленные функции.

Операционная система сама обнаружит сетевой адаптер и установит для него драйвер с цифровой подписью Microsoft (!) — вы только увидите соответствующее сообщение. Если у вас относительно свежая Windows 2000, вполне может случиться, что драйвер устройства, предложенный операционной системой, будет более свежим, чем драйвер изготовителя, находящийся на прилагаемом к устройству компакт-диске.

Если у вас есть возможность загрузить новую версию драйвера от изготовителя устройства, не спешите ею воспользоваться — это нужно делать только в том случае, если устройство некорректно работает со стандартным драйвером. Данное правило касается всех устройств, а не только сетевых адаптеров.

После установки драйвера операционной системой, вы можете приступать к работе с устройством, но прежде его нужно настроить. Нажмите Win + Break, откроется окно **Свойства системы**. Перейдите на страничку **Оборудование** и нажмите кнопку **Диспетчер устройств**. Убедитесь, что ваш сетевой адаптер работает корректно — это сразу будет видно: если драйверы установлены некорректно, возле иконки устройства будет знак предупреждения — восклицательный знак в желтом треугольнике.

Что делать, если есть проблемы с драйвером устройства. Попробуйте удалить устройство и перезагрузить компьютер. Возможно, при повторной установке устройства, проблема будет устранена. Если же этого не

произошло, загрузите драйвер изготовителя и попробуйте его установить. Проблема должна быть устранена.

Если вам опять не повезло, значит нужно проверить само устройство: установите его на другой компьютер. Устройство работает на другом компьютере нормально? Тогда возможен один из двух вариантов:

- Ваше устройство А конфликтует с другим устройством Б, установленном в компьютере. Ваша задача — выяснить, с каким именно. Если вы определили причину, создайте два профиля оборудования: один, который включает в себя все устройства компьютера, кроме устройства А, а второй — все устройства, кроме устройства Б. При загрузке вы будете выбирать один из профилей. Ясное дело, что одновременная работа этих двух устройств невозможна. Если же вам нужны оба устройства данного типа, попробуйте найти или специальные драйверы, или купить другое устройство.

  В моей практике был один случай, когда клиент жаловался на то, что периодически в компьютере отказывается работать звуковая плата. Компьютер привезли в офис, поставили на «тест-драйв». В течение двух суток Winamp не умолкал (музыкальный проигрыватель, если кто не знает) — все было нормально. Как только клиент забрал компьютер домой, у него возникла опять та же проблема. Причина была в следующем: встроенная звуковая плата конфликтовала с USB-принтером. Когда работал принтер, звуковая плата отказывалась работать. В Интернете был найден специальный «патч», который разрешил конфликт устройств. Но такой «патч» можно найти далеко не для каждого устройства. Просто изготовитель принтера знал о подобной проблеме (фирма-то известная, можете представить себе, сколько пользователи мучались с этим принтером?) и выложил на сайте программку, устраняющую проблему.

- Возможно, нужно переустановить Windows 2000 — не забывайте, это все-таки Windows, хотя и самый надежный (может после NT 4). Но не спешите переустанавливать всю систему — вероятность ошибки в самой ОС невелика — вы просто потеряете время. Переустанавливать систему можно только, если другие средства не помогают или у вас есть подозрения, что ошибка заключается именно в самой системе.

Вернемся к настройке сетевого адаптера. Откройте папку **Сеть** и удаленный доступ к сети. Выберите **Соединение по локальной сети**, щелкнув по нему правой кнопкой мыши. Из появившегося меню выберите **Свойства** (рис. 6.38).

Сейчас будем конфигурировать только протокол TCP/IP. Выберите его и нажмите кнопку **Свойства**. В появившемся окне введите IP-адрес 192.168.1.5, маску сети 255.255.255.0 (рис. 6.39).

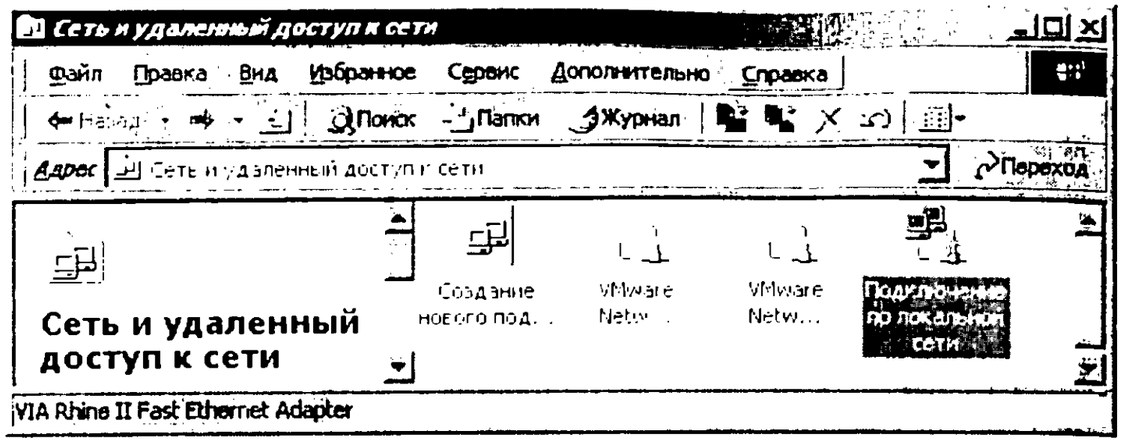


Рис. 6.37. *Сеть и удаленный доступ к сети*

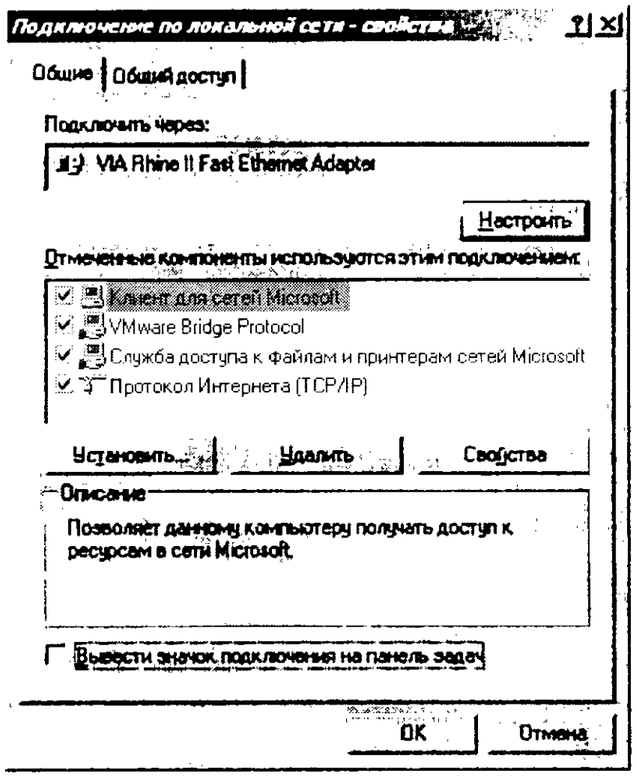


Рис. 6.38. *Свойства соединения по локальной сети*

Другие параметры, например, DNS, вводить не будем, поскольку данные возможности у нас еще не настроены — мы ведь еще не настраивали DNS-сервер своими руками? Вот когда настроем, тогда и можно будет прописать заветный адрес на всех компьютерах.

Следующий шаг — откройте окно **Свойства системы** (Win+Break). Перейдите на страничку **Имя компьютера** и установите имя компьютера COMP5 и имя рабочей группы WORK. После чего нужно перезагрузить машину.

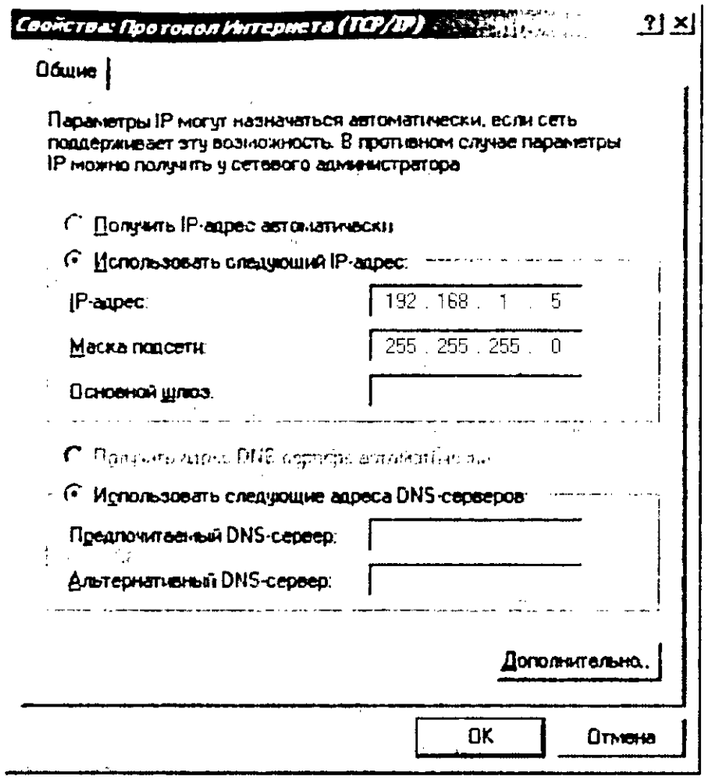


Рис. 6.39. *Свойства протокола TCP/IP*

После перезагрузки можно будет проверить работу сетевого адаптера. Как именно, вы уже знаете, поэтому мы не будем на этом подробно останавливаться. Напомню, что для тестирования работы сетевого адаптера нужно использовать команды **ipconfig** и **ping**.

6.2.5. Настройка сетевой карты и сетевого взаимодействия в Windows XP

Первичная настройка

Почему мне нравится Windows 2000 и XP? Да потому, что в большинстве случаев эти операционные системы «знают» практически все установленные у вас устройства. Поэтому о драйвере для сетевого адаптера можете забыть — XP справится с этой задачей самостоятельно. Конечно, с одной стороны, драйвер производителя — лучше, но стандартные драйверы Windows XP тоже отлично работают — во всяком случае с драйверами для сетевых плат у меня проблем не было.

Windows XP — это потомок Windows NT, поэтому не нужно забывать о правах пользователей. Настройку сети нужно производить, зарегистрировавшись как Администратор, или как пользователь, относящийся к группе администраторов.

Все же убедимся, что наш сетевой адаптер установлен корректно. Вдруг у вас какой-то экзотический адаптер, для которого у XP нет стандартного драйвера или он работает некорректно. Откройте окно диспетчера устройств. Для этого нажмите Win + Break, перейдите на страничку **Оборудование** и нажмите кнопку **Диспетчер устройств**.

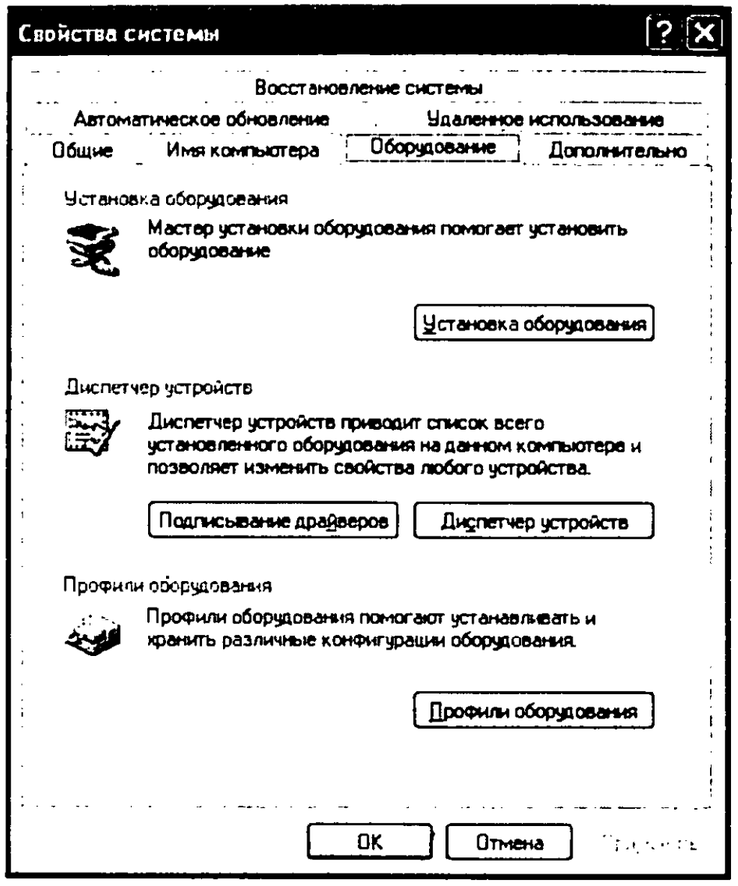


Рис. 6.40. *Свойства системы*

В окне Диспетчера устройств выберите раздел **Сетевые платы** — вы увидите ваш сетевой адаптер (или сетевые адаптеры, если у вас их несколько) (рис. 6.41).

Дважды щелкните на интересующем вас сетевом адаптере. Вы увидите свойства сетевой платы. На страничке **Общие** вы можете увидеть общее состояние устройства, его тип и размещение. Если в области **Состояние устройства** у вас значится «Устройство работает нормально», значит все нормально (рис. 6.42), можно приступать к дальнейшей настройке устройства.

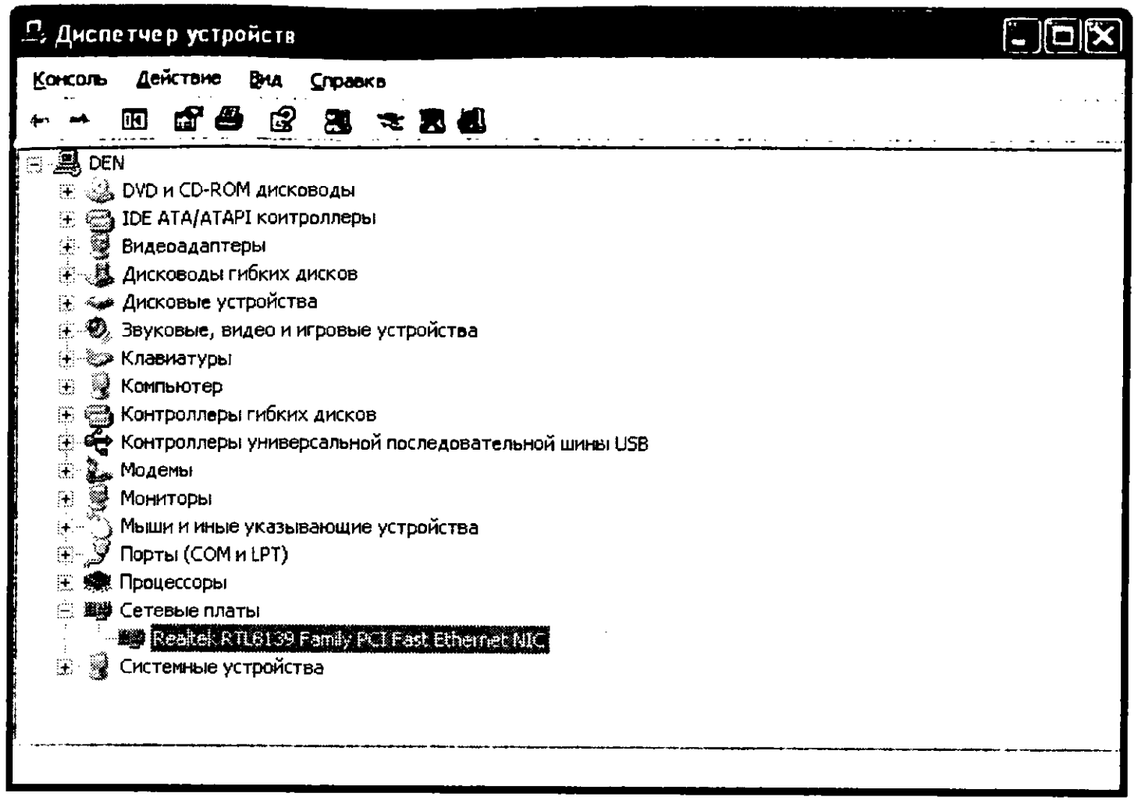


Рис. 6.41. *Диспетчер устройств*

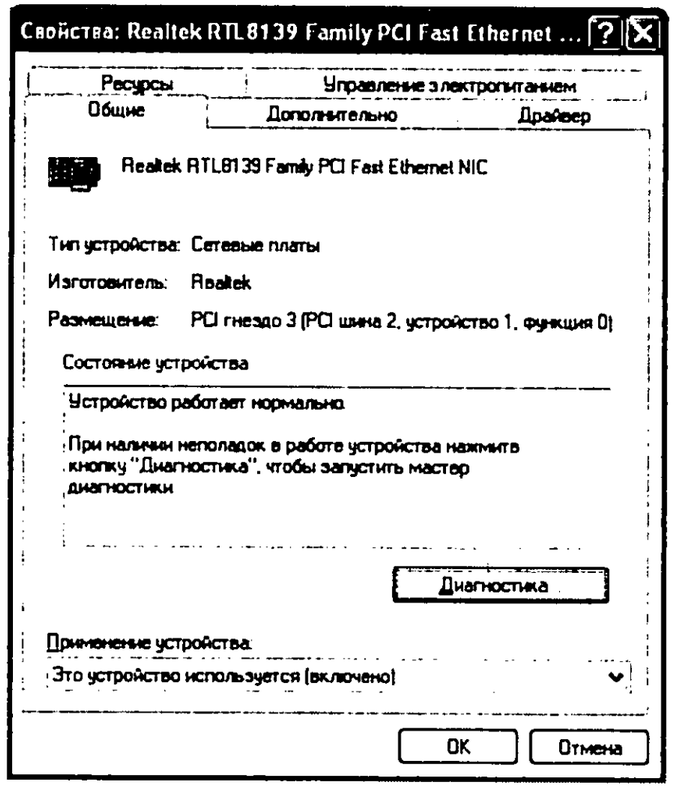


Рис. 6.42. *Состояние сетевой платы*

Настройка сети

Теперь приступим к настройке сети. Откройте Панель управления и переключитесь к классическому виду, поскольку он более удобен. Затем выберите апплет **Сетевые подключения** (рис. 6.43).

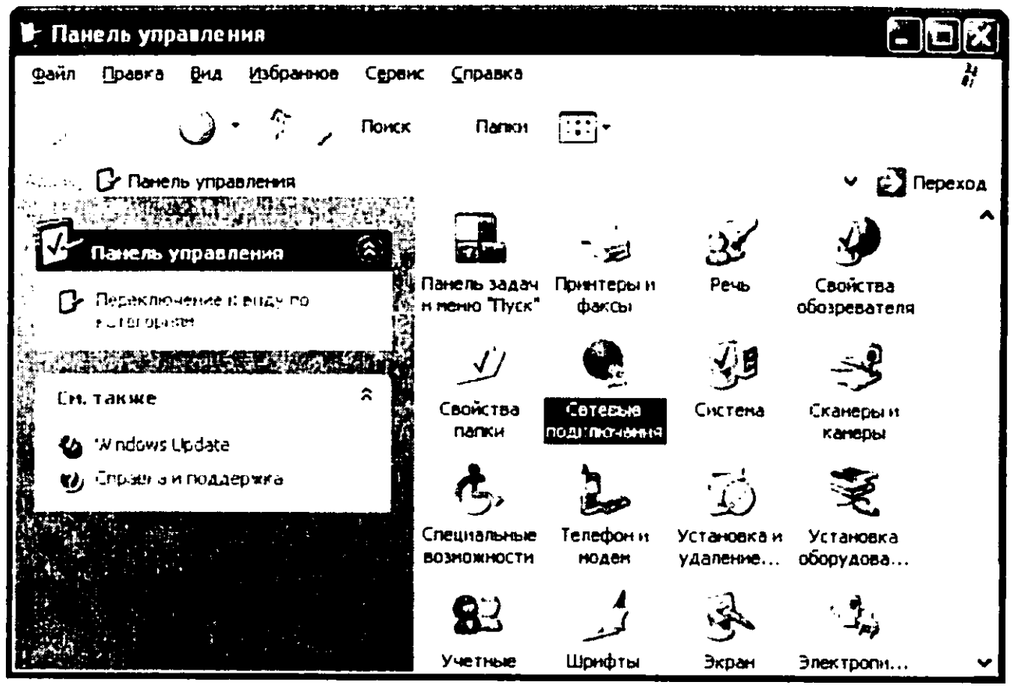


Рис. 6.43. *Панель управления Windows XP*

В папке **Сетевые подключения** отображаются абсолютно все сетевые подключения — от простого PPP-подключения к Internet до подключения к VPN-сети, если такие имеются (рис. 6.44). В этой же папке находится наше подключение к локальной сети с помощью сетевого адаптера.

Выберите сетевой адаптер и щелкните по ссылке **Изменение настроек подключения**. По умолчанию для любого сетевого адаптера используются следующие компоненты (рис. 6.45):

- Клиент для сети Microsoft.
- Служба доступа к файлам и принтерам сетей Microsoft.
- Планировщик пакетов QoS.
- Протокол Интернета (TCP/IP).

Первые два компонента пока трогать не будем — о них мы еще поговорим, но только не в этой главе. Протокол TCP/IP — это знакомый нам компонент, а вот что такое Планировщик пакет QoS? Это такой зверь, который «отъедает» примерно 20% канала передачи данных. Да, ваш канал становится «уже» на 20%. Подробнее о QoS и об его отключении мы поговорим после настройки протокола TCP/IP.

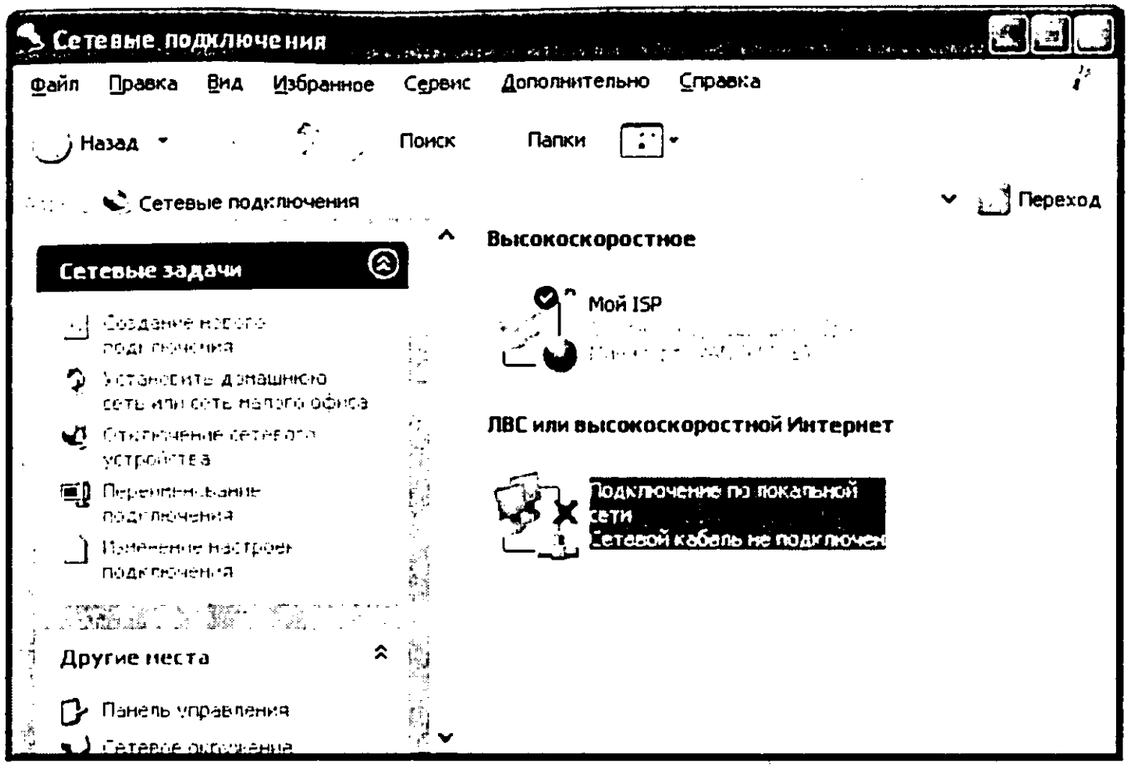


Рис. 6.44. *Сетевые подключения*

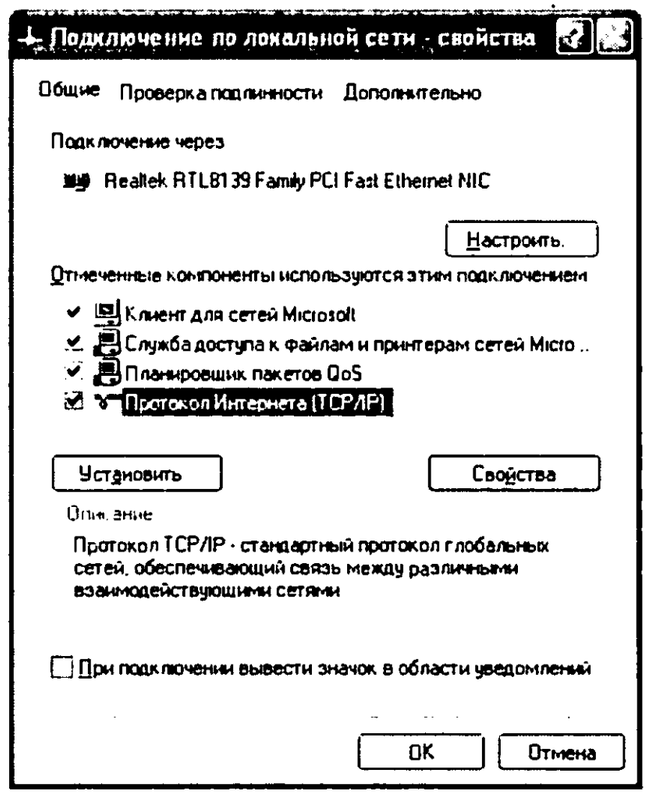


Рис. 6.45. *Компоненты подключения*

Настройка протокола TCP/IP

Настройка протокола TCP/IP в Windows XP упрощена до невозможного: просто выберите опцию **Использовать следующий IP-адрес**, введите IP-адрес 192.168.1.5 и все (рис. 6.46)! Даже сетевую маску XP введет за вас. IP-адрес шлюза вводить не нужно, во всяком случае пока.

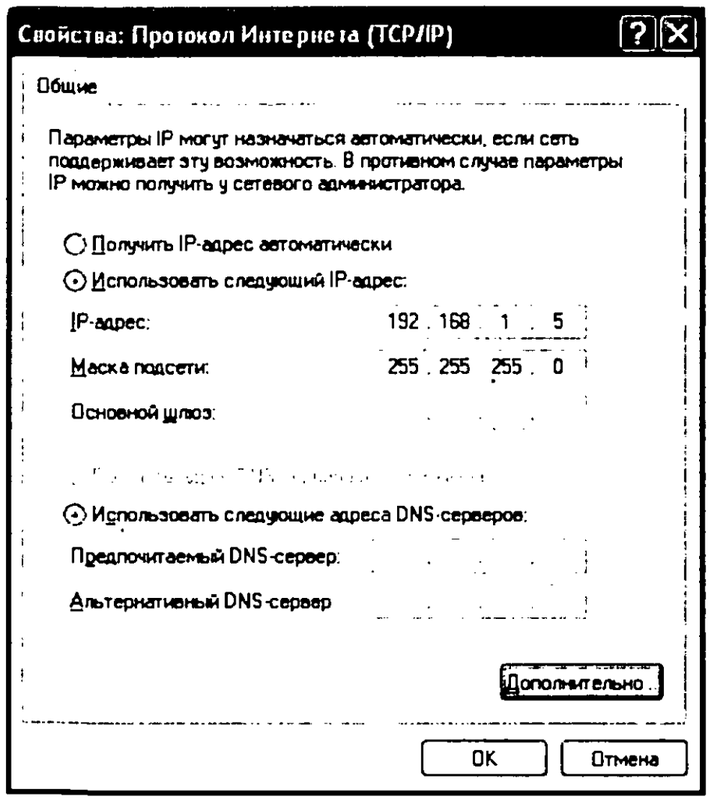


Рис. 6.46. *Свойства TCP/IP*

Кнопка **Дополнительно** содержит дополнительные параметры TCP/IP, о которых мы поговорим в других главах этой книги.

После настройки протокола TCP/IP нужно установить имя компьютера и рабочей группы. Для этого откройте окно **Свойства системы** (нажмите Win+Break) и перейдите на вкладку **Имя компьютера**. Затем нажмите кнопку **Изменить** и установите имя компьютера и рабочей группы — COMP5 и WORK, соответственно (см. рис. 6.47).

На этом базовая настройка сети завершена. Я обещал, что мы поговорим о планировщике QoS.

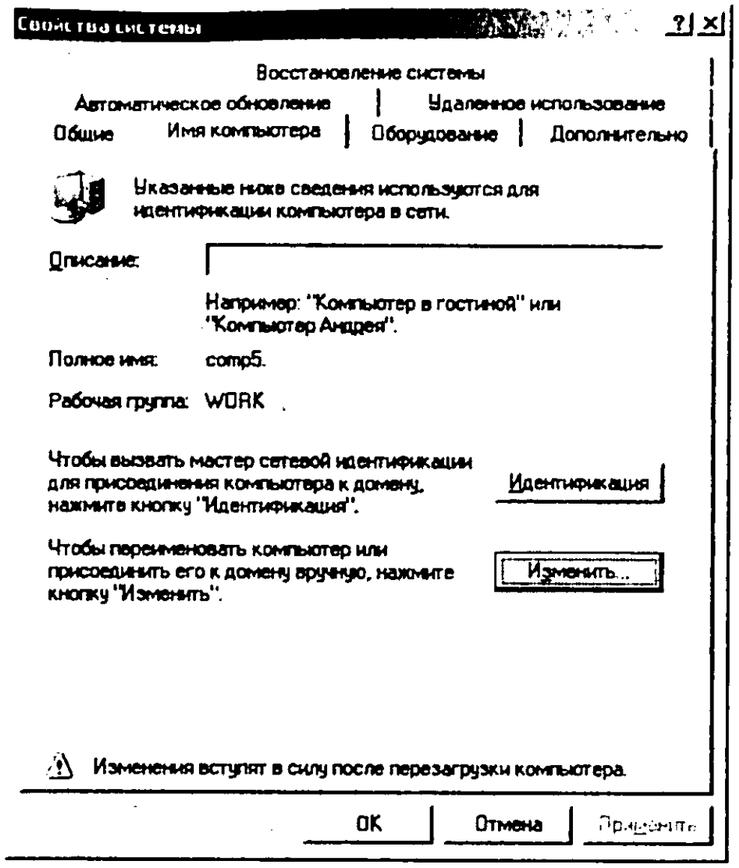


Рис. 6.47. *Установка имени компьютера и рабочей группы*

Планировщик Quality of Service и как его отключить, чтобы сеть быстрее работала

Именно так расшифровывается аббревиатура QoS. В описании компонента сказано: «Этот компонент обеспечивает управление сетевым трафиком, включая скорость передачи и приоритеты». Не очень понятно, правда? С одной стороны, вещь — полезная. Но! Основная задача QoS — улучшить распределение трафика между сетевыми программами, которые используют специальный программный интерфейс — QoS API. А такие программы нужно занести в Красную книгу программного обеспечения. Нет, не потому, что они — вымирающий вид, а потому, что встречаются они довольно редко. Даже если у вас и есть одна такая программа, включать ради нее QoS — это непозволительная роскошь.

По умолчанию QoS резервирует для служебных целей 20% канала передачи данных. Чтобы наш канал снова стал полноценным, как это было в предыдущих версиях Windows (9x/ME/NT), нужно проделать следующие действия:

1. Запустите редактор Групповых политик. Проще всего это сделать, выбрав команду меню Пуск, Выполнить и ввести команду **gpedit.msc**.
2. В окне **Групповые политики** (см. рис. 6.48) перейдите к разделу **Конфигурация компьютера → Административные шаблоны → Сеть → Диспетчер пакетов QoS**.
3. В правой части окна выберите **Ограничить резервируемую пропускную способность** (щелкните по этой надписи дважды) (рис. 6.49).
4. Несмотря на то, что ограничение не задано, выберите опцию Включить и установите значения ограничения 0%.
5. Нажмите кнопку **Применить**.
6. Убедитесь, что для всех ваших соединений **включен** Планировщик пакетов QoS и перезагрузите компьютер.

Если ограничение пропускной способности не задано или выключено, по умолчанию операционная система будет «отъедать» 20% трафика. Не верите? Перейдите на вкладку **Объяснение** окна свойств QoS и прочитайте объяснение службы (рис. 6.50).

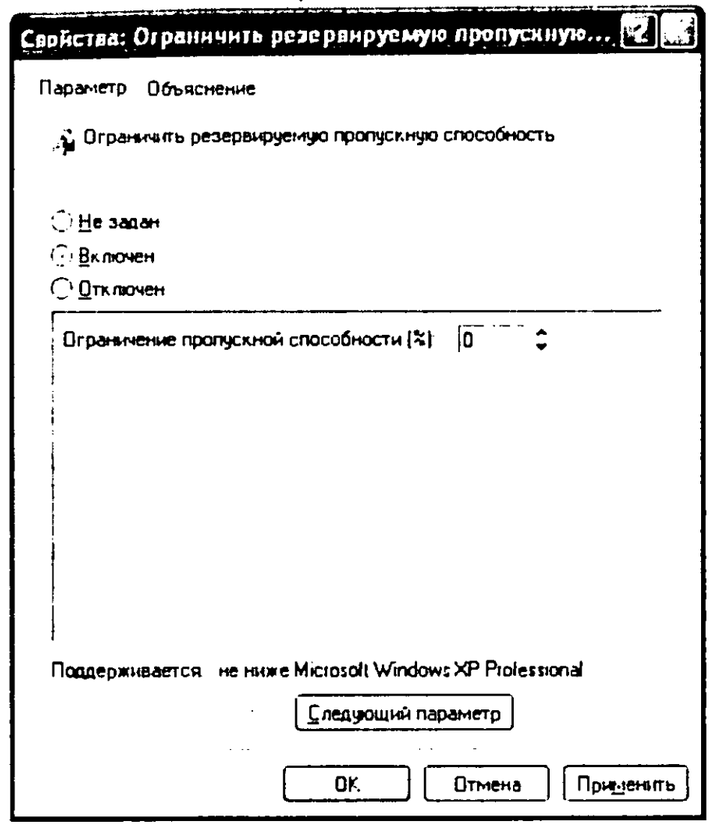


Рис. 6.49. *Ограничение пропускной способности*

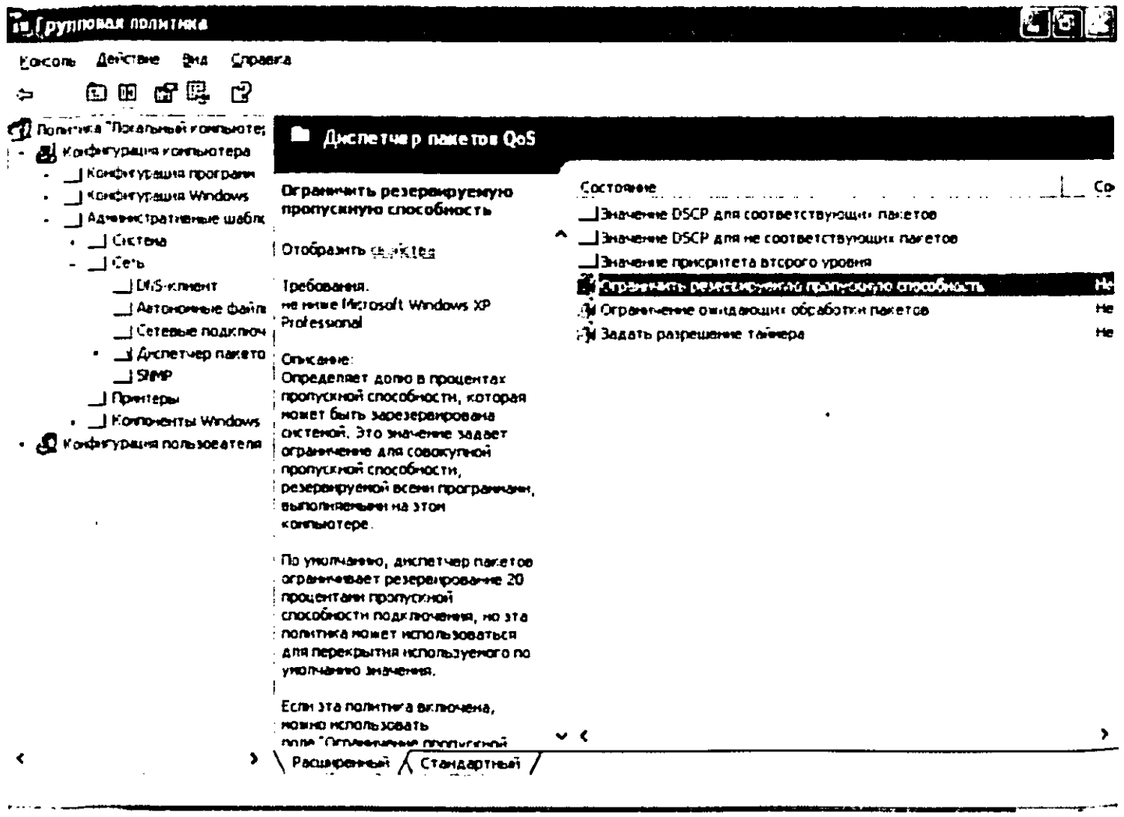


Рис. 6.48. *Групповые политики*

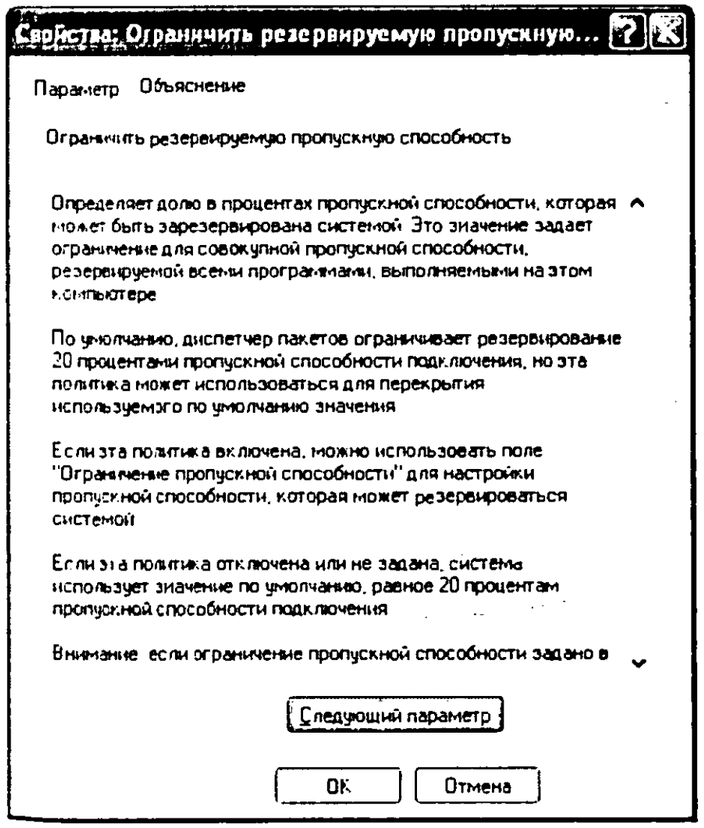


Рис. 6.50. *Объяснение QoS*

6.2.6. Настройка сетевой карты и сетевого взаимодействия в Windows 2003 Server

Нельзя сказать, что установка сетевого адаптера в Windows 2003 Server чем-то принципиально отличается от установки сетевого адаптера в предыдущих версиях — Windows 2000 и Windows XP, но для полноты описания данный пункт просто необходим. Даже по той причине, что в основном на момент написания этих строк довольно трудно найти русскую версию Windows 2003 Server — в основном доступны английские версии с поддержкой русского языка. Вот именно такая версия описывается в этой книге, учитывая особенности каждого читателя — ведь не каждый читатель свободно владеет английским.

Итак, самостоятельно заниматься установкой драйвера устройства вам не придется. Windows 2003 обладает еще более большей базой драйверов, поэтому вероятность установки стандартного драйвера еще выше — она приближается к 99%.

Откройте папку **Network Connection (Сетевые соединения)**, показанную на рис. 6.51. Для этого выберите пункт **Network Connections** из меню **Start → Settings (Пуск → Настройки)**.

После этого щелкните правой кнопкой мыши по иконке **Local Area Connection (Соединение по локальной сети)** и из контекстного меню выберите пункт **Properties (Свойства)**. Свойства показаны на рис. 6.52.

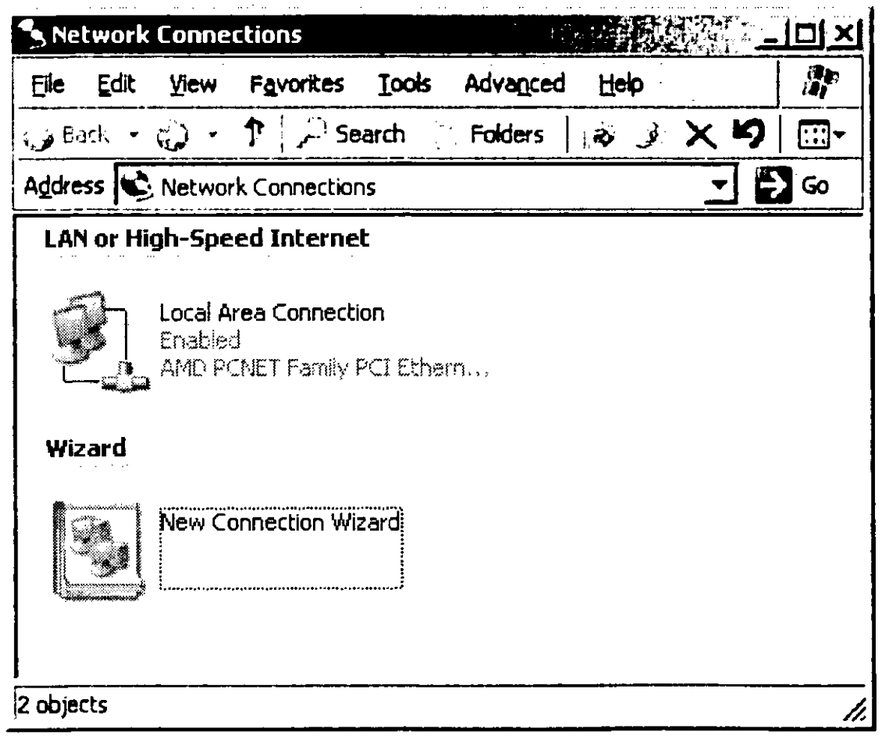


Рис. 6.51. *Network Connections*

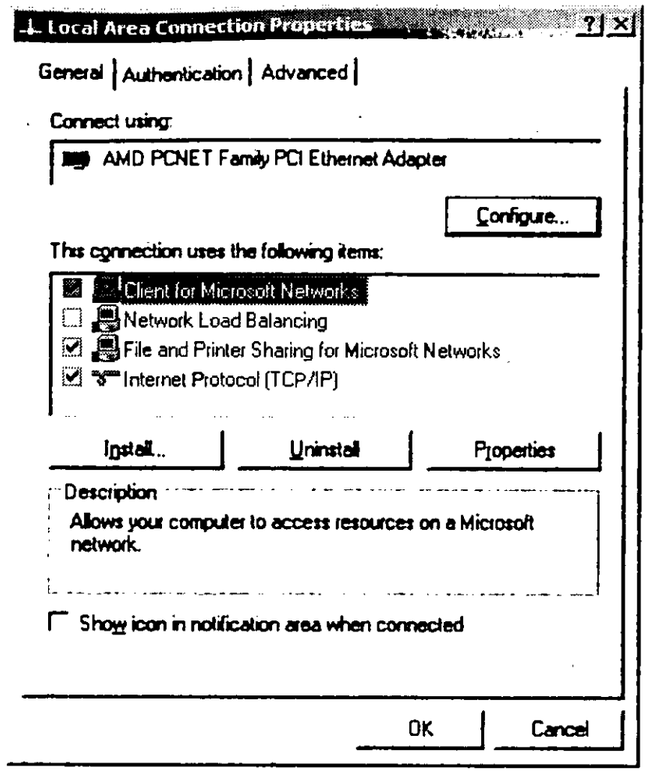


Рис. 6.52. *Свойства LAN Area Connection*

Далее выберите **Internet Protocol (TCP/IP)** и нажмите кнопку **Properties (Свойства)**. В появившемся окне **Internet Protocol (TCP/IP) Properties** (см. рис. 6.53) в поле **IP address** введите IP-адрес 192.168.1.5, а в поле **Subnet mask** — введите 255.255.255.0. Никакие другие параметры изменять не нужно — просто нажмите **Ок**.

Убедимся, что IP-адрес принят и в локальной сети нет больше компьютеров с таким же IP-адресом. Для этого откройте Командную строку (**Start → Programs → Accessories → Command Prompt**), введите команду **ipconfig**. Примерный ответ показан на рис 6.54.

Напомню, что если IP-адрес занят, в поле **IP Address** вы увидите установленный вами IP, а в поле **Subnet Mask** — 0.0.0.0. Если все нормально, с помощью команды **ping** пропингуем адрес 192.168.1.5 (см. рис. 6.55).

Теперь самое время установить имя компьютера и рабочей группы. Для этого откройте показанное на рис. 6.56 окно **Свойства системы (System Properties)** (нажмите Win+Break), перейдите на страничку **Computer Name** и нажмите кнопку **Change**. В открывшемся окне введите нужные значения (рис. 6.57). На этом базовая настройка Windows 2003 Server завершена.

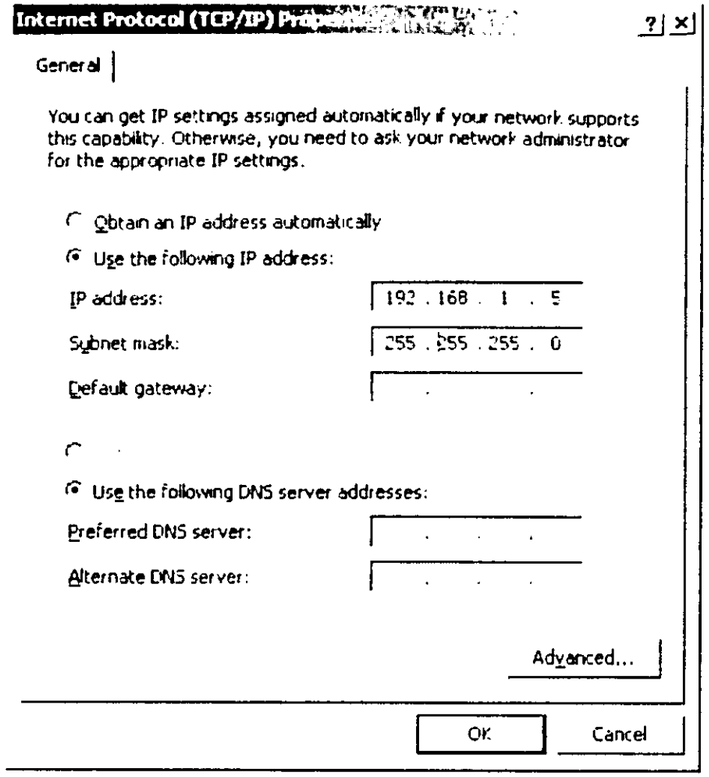


Рис. 6.53. *Свойства Internet Protocol (TCP/IP)*

Рис. 6.54. *Команда ipconfig в Windows 2003 Server*

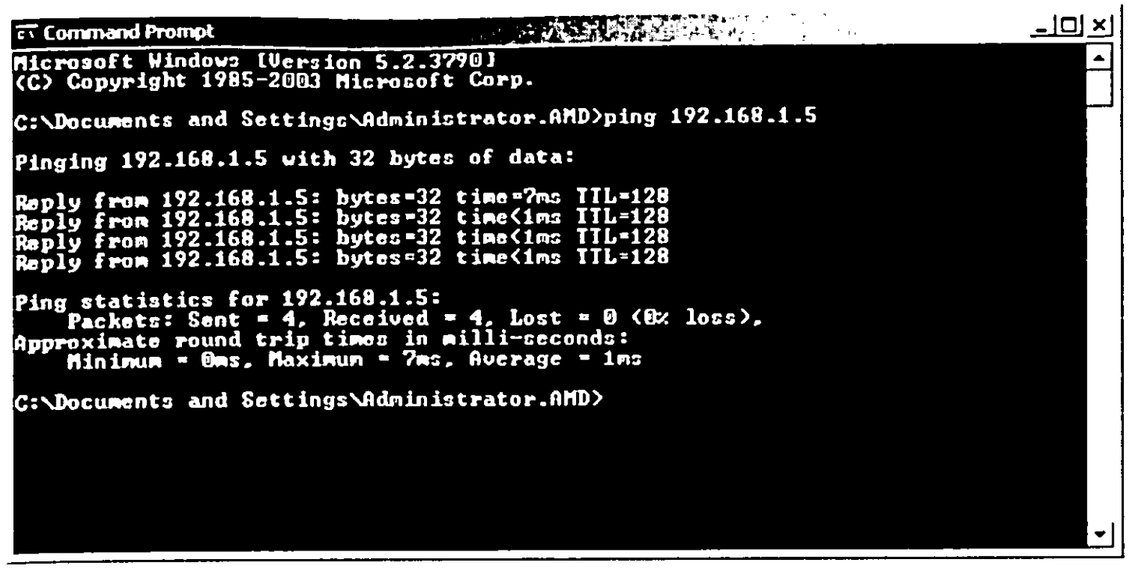


Рис. 6.55. *Команда ping в Windows 2003 Server*

Рис. 6.56. *Свойства системы*

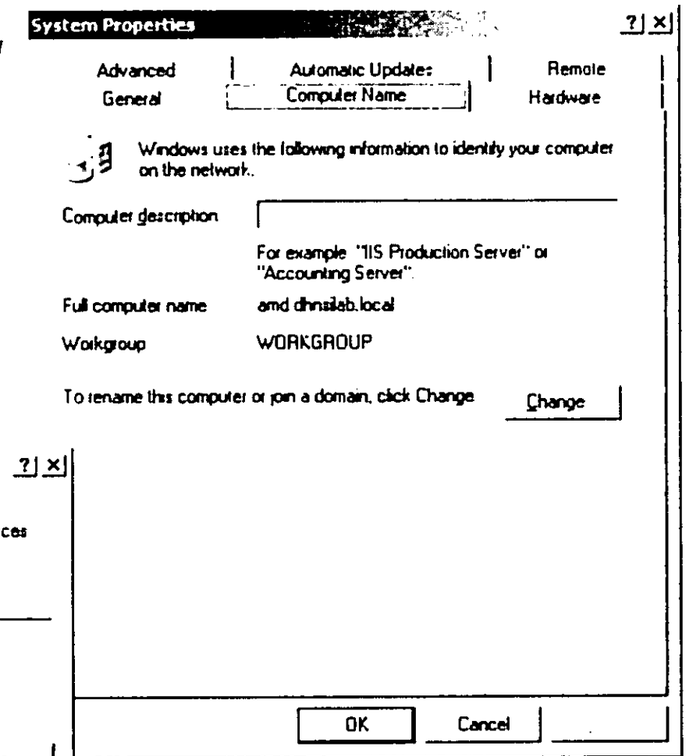


Рис. 6.57. *Изменение имени компьютера и рабочей группы*

6.2.7. Настройка сетевой карты и сетевого взаимодействия в Linux

С одной стороны, описывать настройку Windows проще: несмотря на то, что есть различные версии Windows — 95/98, ME, NT, 2000, XP — метод настройки сети один-единственный для каждой конкретной версии Windows. Тем более, что настройки 95/98 и ME, NT Workstation и NT Server, 2000 и XP практически ничем не отличаются друг от друга. А с Linux дело обстоит хуже.

Во-первых, существует много различных дистрибутивов Linux — Red Hat, Mandrake, ALT Linux, ASP Linux, Debian, SuSe — сейчас я все и не вспомню. А программы-конфигураторы и их названия отличаются друг от друга. Во-вторых, в Linux не существует единого способа настройки. Что я имею в виду? Все мы привыкли настраивать сеть в Windows через апплет **Сеть** с Панели Управления. В Linux сеть (и многое другое) настраивается с помощью программ-конфигураторов.

Мало того, что в разных дистрибутивах, как уже отмечалось, названия этих программ (а и сами эти программы) — разные. В некоторых дистрибутивах вообще может не быть программ конфигураторов. Мне встречались и такие дистрибутивы — там вообще сеть настраивается «ручками» — с помощью команд операционной системы, которые после успешной настройки должны быть прописаны в сценарии автозагрузки системы — чтобы не вводить их каждый раз при загрузке.

Да, совсем забыл: названия конфигураторов или сами конфигураторы могут изменяться в зависимости от версии дистрибутива. Например, конфигуратор **redhat-config-network** появился в RedHat, начиная с восьмой версии дистрибутива. До этого использовался конфигуратор **netconfig**.

В дистрибутиве Mandrake конфигуратор **netconf** был, кажется, до восьмой версии, а параллельно ему использовался конфигуратор **draknet**. Начиная с восьмой, если мне не изменяет память, конфигуратор netconf вообще не используется в Mandrake — его полностью вытеснил **draknet**.

Описать в книге настройку абсолютно всех дистрибутивов — это означает объять необъятное. Поэтому ограничимся лишь тремя дистрибутивами: Red Hat 9-10, Mandrake 9-10 и ALT Linux 2.2. Почему именно эти дистрибутивы?

Red Hat — это своеобразный стандарт в мире Linux. В данной книге будет описываться девятая версия этого дистрибутива. Настройка девятой версии очень похожа на настройку предыдущей, восьмой версии, поэтому мы убиваем двух зайцев, описав две версии дистрибутива. Настройка седьмой версии отличается от восьмой версии, не говоря уже про шестую версию. Не исключено, что у кого-то до сих пор установлена версия 7.2 или 7.3 — это очень хорошие и стабильные версии, у меня до сих пор дома установлена версия 7.3 и я не жалуюсь на нее. Еще раз говорю, что описать все версии просто нереально, поэтому седьмую и шестую версии рассматривать не будем.

Linux Mandrake — это популярный французский дистрибутив, который является достойной альтернативой Red Hat Linux. Сейчас, конечно, для меня нет никакой разницы с каким дистрибутивом работать, но при первом знакомстве с Mandrake (тогда это был Mandrake 7.0) он мне показался более простым в настройке и более дружелюбным, нежели Red Hat. Что же касается версий дистрибутива, то можно сделать аналогичные замечания, как и в случае с Red Hat. В книге будет рассматриваться только последняя версия.

Почему такое отношение к Linux? Потому что в отличие от Windows, где не хотят переходить на новую версию, потому что привыкли к старой или просто не позволяет сделать это финансовое положения, Linux стараются установить только последнюю версию. Да и в каком магазине можно купить, скажем, шестую версию Red Hat или седьмой Mandrake? К тому же, чем Linux новее, тем он лучше, чего не скажешь о Windows.

ALT Linux рассматривается в этой книге, потому что это лучший, на мой взгляд, отечественный дистрибутив Linux. Не хочу обидеть разработчиков ASP Linux и другие отечественные команды — их дистрибутивы тоже ничего, но я решил ограничиться ALT Linux, тем более, что под рукой была свежая версия этого дистрибутива, которую я без проблем установил и настроил не только на стационарном компьютере, но и на ноутбуке.

И еще: описывая настройку сети, я надеюсь, что вы уже имеете хотя бы какие-нибудь представления о Linux и немного умеете работать в этой операционной системе, или когда-то работали, а сейчас хотите возобновить в памяти кое-какие моменты. Если Linux для вас — загадка, а настроить его все же нужно, потому что начальство требует, я рекомендую свои книги (издательство «Наука и Техника», 2004):

- Linux-сервер своими руками, изд. 2.
- Самоучитель Linux: установка, настройка, использование, изд. 3.

Конечно, я буду стараться делать небольшие примечания для новичков, но это не панацея. Чтобы освоить Linux, вам нужна полноценная книга. Вспомните себя, когда вы осваивали Windows. Скорее всего, у вас была какая-нибудь книга, которая стала для вас фундаментальной. Вот сейчас вам нужна такая же книга по Linux.

Настройка в дистрибутиве Red Hat Linux

При установке дистрибутива программа установки сама распознает установленный сетевой адаптер — в моей практике не было случая, чтобы сетевой адаптер был не опознан (это не касается внешних USB-адаптеров). Вам нужно указать только параметры сетевого соединения (рис. 6.58).

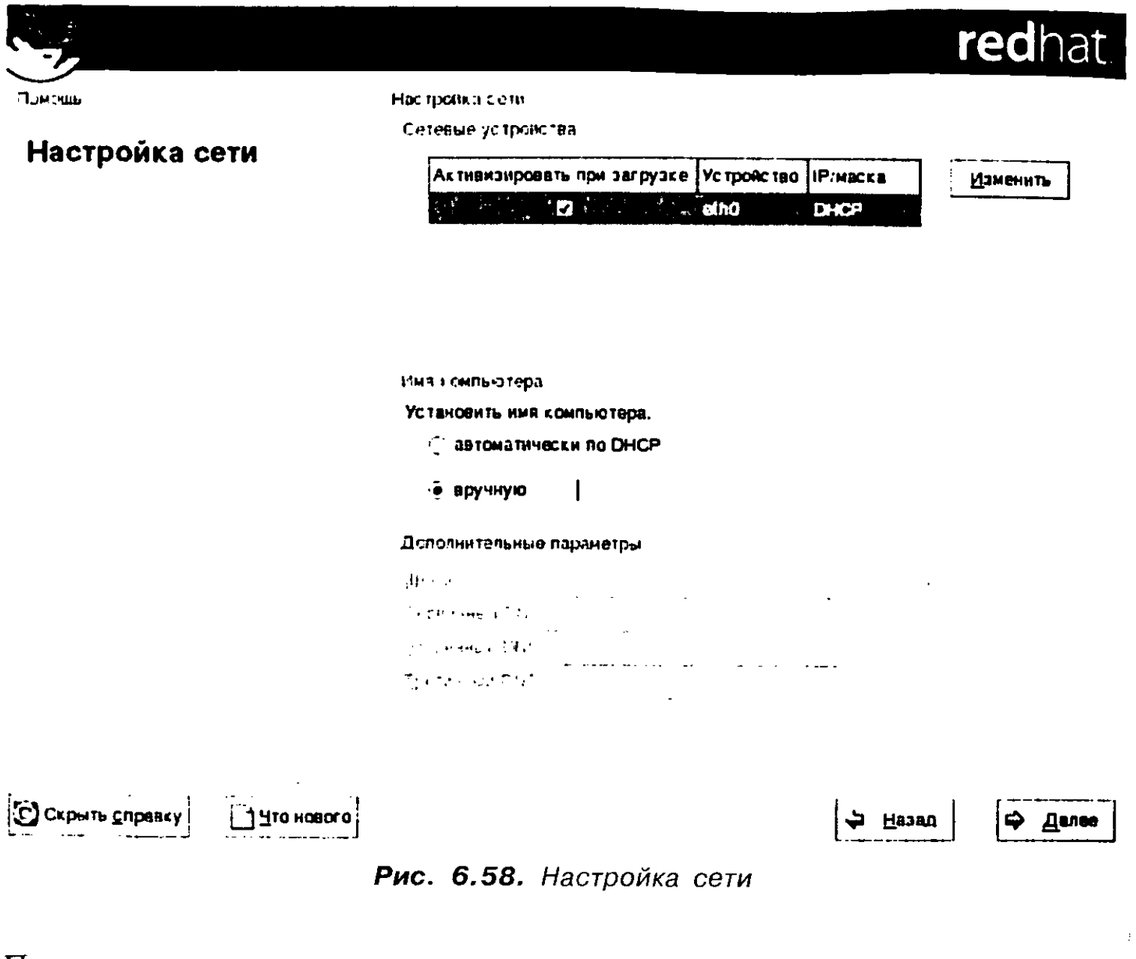


Рис. 6.58. *Настройка сети*

Программа установки распознает все сетевые устройства. В данном случае был найден только сетевой адаптер — устройство `eth0`. Нумерация устройств в Linux начинается с 0, поэтому `eth0` — это *первый* сетевой адаптер.

Примечание.

Запомните следующие имена сетевых интерфейсов и устройств — они вам пригодятся при настройке сети:

- ethN (N — целое число от 0) — сетевой адаптер Ethernet.
- pppN (N — целое число от 0) — соединение PPP (Point to Point Protocol).
- /dev/modem — модем. /dev/modem — это всего лишь символическая ссылка на последовательный порт, то есть устройство /dev/ttySN.
- /dev/ttySN — (N от 0 до 3) — это последовательный порт, /dev/ttyS0 соответствует COM1 в Windows, /dev/ttyS3 — COM4.

Вернемся к настройке сети. Выберите нужный вам адаптер и нажмите кнопку **Изменить**. В появившемся окне (рис. 6.59) введите IP-адрес 192.168.1.5 и сетевую маску 255.255.255.0. Обязательно выключите режим **Configure using DHCP** — мы настраиваем интерфейсы вручную, а не с помощью DHCP. Также следует включить режим **Activate On Boot** — тогда

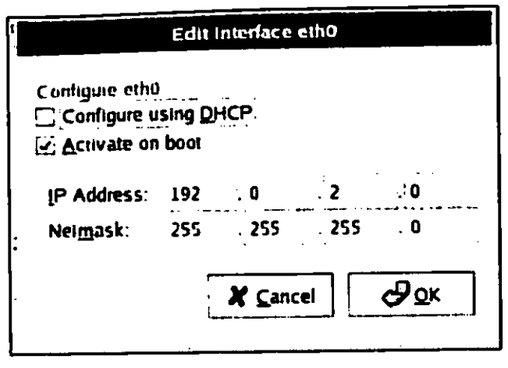


Рис. 6.59. *Редактирование сетевого интерфейса*

наш интерфейс будет «поднят» при загрузке системы. Данный режим нужно включать для всех постоянных соединений, например, соединение по локальной сети или по выделенной линии.

Для непостоянных соединений, например, для коммутируемого модемного соединения, данный режим включать не нужно, поскольку модем сразу же начнет набирать номер провайдера, а счетчик-то у провайдера тикает.

Вернувшись в окно настройки сети (рис. 6.58), определите имя компьютера — COMP5. А затем нажмите кнопку **Далее**. Все, сеть настроена.

А что же делать, если сеть нужно настроить уже после установки системы или изменить параметры какого-нибудь сетевого соединения? Для этого используется конфигуратор **redhat-config-network**. О нем мы еще поговорим, а сейчас займемся установкой сетевого адаптера в системе — мы должны сообщить системе, что мы установили новое устройство и хотим его настроить.

Обычно при запуске системы запускается утилита поиска нового оборудования — **kudzu**, которая и сообщит вам о «находке». Если вы не запускаете **kudzu** автоматически — в самом же деле, ведь не каждый день устанавливаешь новое оборудование, а запуск **kudzu** занимает много времени — то запустите **kudzu** из командной строки (от имени пользователя root).

Kudzu самостоятельно определит новое устройство и установит его: пропишет модуль (драйвер) устройства в файл `/etc/modules.conf` (или `/etc/conf.modules` — имя файла зависит от версии дистрибутива) и добавит модуль в состав ядра (выполнит команду insmod). Запустите **kudzu** из командной строки.

Kudzu сообщит вам, что найден сетевой адаптер, и предложит его настроить (рис. 6.60). Нельзя отказываться от такого предложения, поэтому нажимаем кнопку Настроить и ждем, пока устройство будет сконфигурировано. После этого конфигуратор **kudzu** запустит конфигуратор сети.

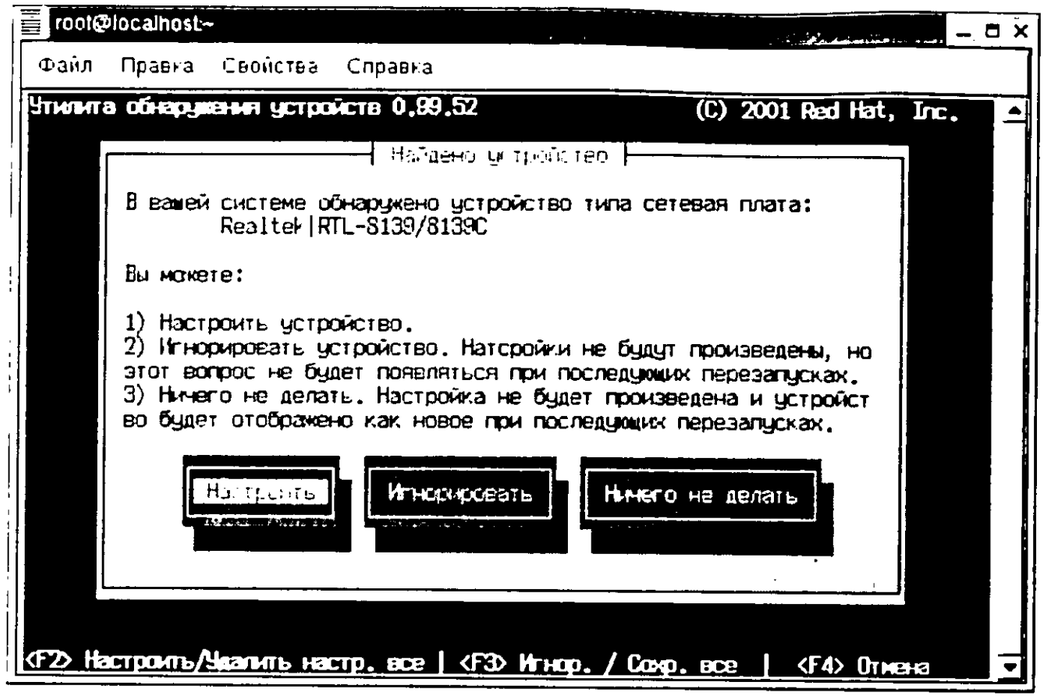


Рис. 6.60. *Поиск нового оборудования*

Какой именно, это зависит от версии дистрибутива. Например, в Red Hat 7.3 — это программа **netconfig**. От предложения конфигуратора **netconfig** тоже не стоит отказываться — он предлагает настроить сеть, точнее найденную сетевую плату (рис. 6.61).

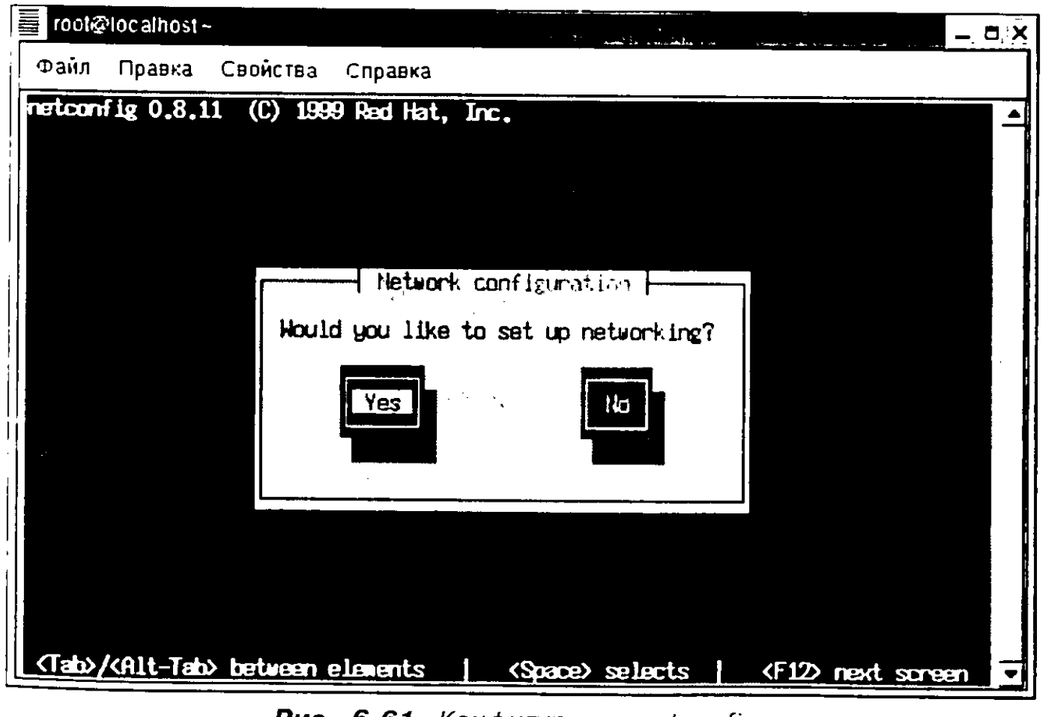


Рис. 6.61. *Конфигуратор netconfig*

Напомню параметры сетевого соединения: IP-адрес 192.168.1.5 (я его уже повторял столько раз, что, наверное, вы уже его давно запомнили, но, как говорится, заикание — мать повторения), сетевую маску — 255.255.255.0. Шлюз по умолчанию (Default gateway IP) и первичный сервер DNS (Primary nameserver) пока указывать не нужно — ведь мы их еще не настроили — у нас их просто пока нет (рис. 6.62).

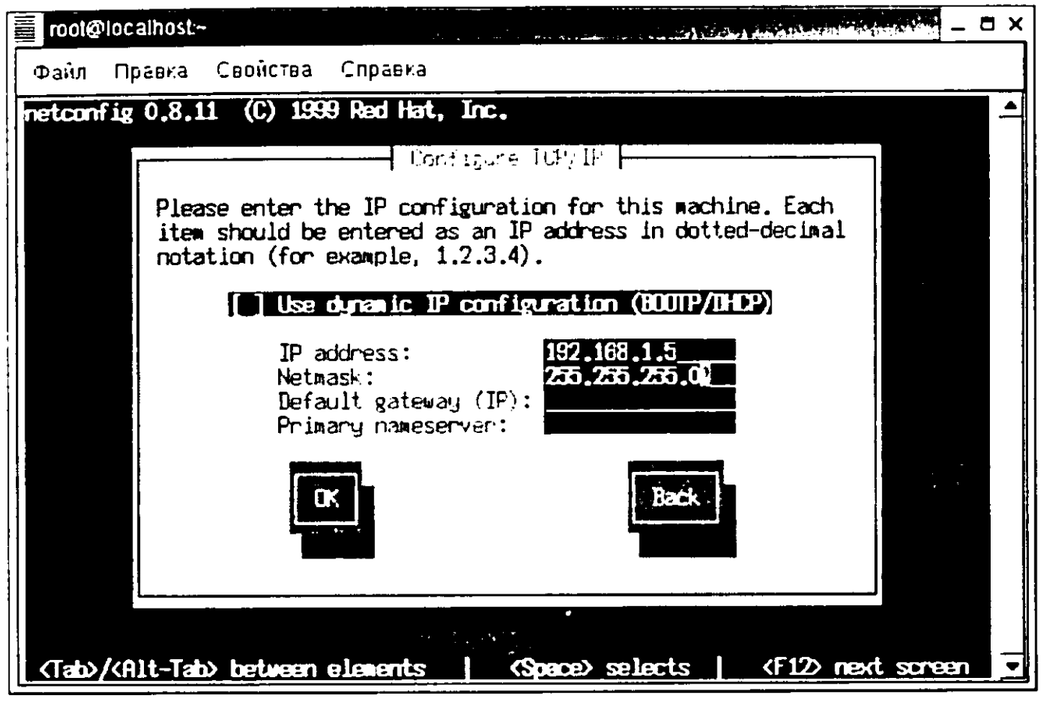


Рис. 6.62. *Параметры интерфейса eth0*

Нажимаем Ok и наблюдаем за работой конфигураторов **kudzu** и **netconfig**. Первый должен был добавить нужный нам модуль в файл `/etc/modules.conf`, а второй — настроить интерфейс `eth0`. Проверяем работу **kudzu**. Для этого в любом редакторе или средстве просмотра открываем файл `/etc/modules.conf` (можно просто использовать команду `cat /etc/modules.conf`). Последняя строка — это имя модуля, добавленного утилитой **kudzu** (рис. 6.63).

Теперь проверим, что же сделал конфигуратор **netconfig**. Запускаем программу **ifconfig**. И что мы видим? Только интерфейс `lo`!

```
lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:18 errors:0 dropped:0 overruns:0 frame:0
      TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:1512 (1.4 Kb)  TX bytes:1512 (1.4 Kb)
```

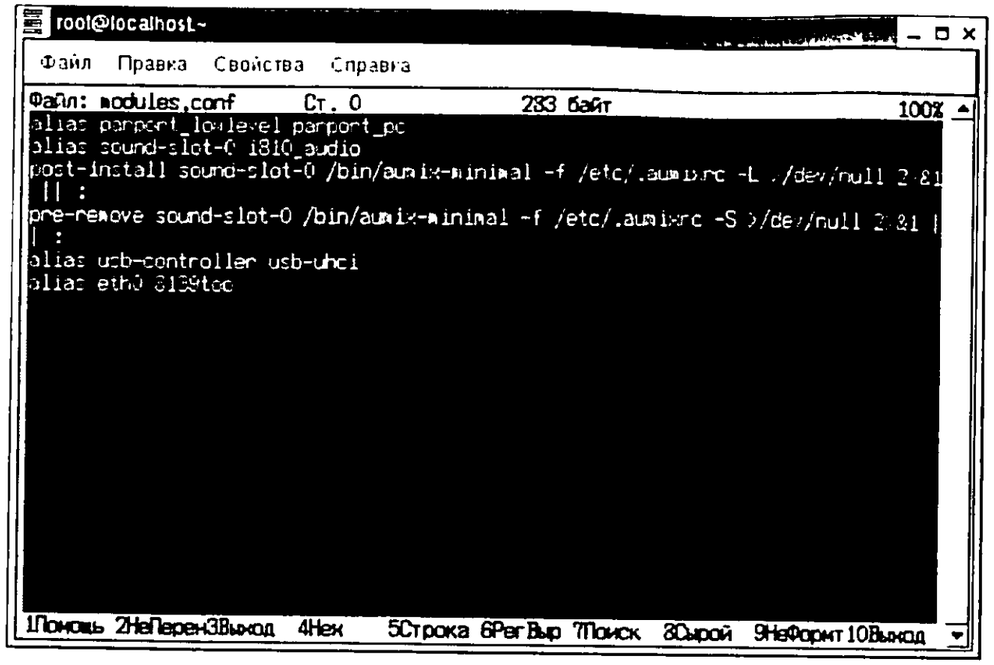


Рис. 6.63. *Модуль 8139too добавлен!*

А где же интерфейс eth0? Все нормально: конфигуратор настроил интерфейс, но пока его не «поднимал». Чтобы запустить («поднять») интерфейс, введите команду:

```
ifconfig eth0 up
```

и получите результаты, показанные на рис. 6.64.

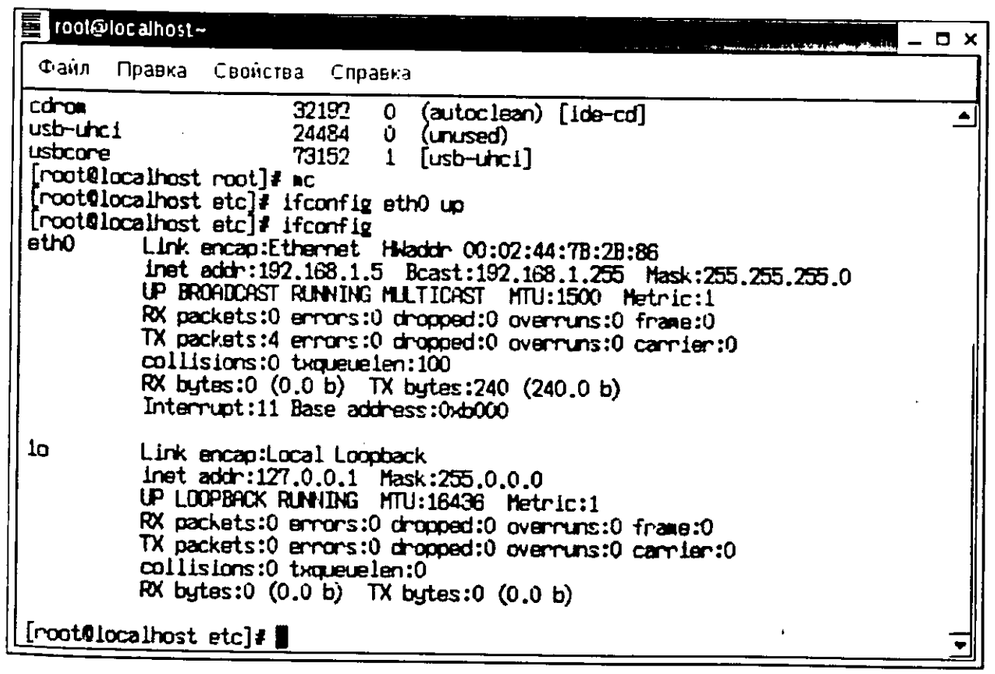


Рис. 6.64. *Интерфейс eth0 поднят!*

Вот, собственно, и все. Для изменения параметров сетевого соединения удобнее использовать графический конфигуратор **redhat-config-network**. Для его запуска нужно сделать следующее. Прежде всего, убедитесь, что данный конфигуратор у вас вообще установлен. Для этого откройте терминал (если вы работаете в консоли, ничего открывать не нужно) и введите команду

```
rpm -qa | grep redhat-config-network
```

Данная команда (**rpm –qa**) выводит список установленных пакетов на стандартный ввод программы grep, которая выполняет роли фильтра — ищет указанную строку (**redhat-config-network**). Если вывод данной команды содержит строку **redhat-config-network** — вы ее должны увидеть — то это означает, что пакет установлен. В противном случае вам нужно установить пакет. Для этого зарегистрируйтесь в системе как пользователь root или просто введите команду **su** (сокр. от superuser). Далее нужно ввести пароль пользователя root. После этого вставьте установочный (дистрибутивный) диск в CD-ROM и введите команду:

```
rpm -ihv redhat-config-network
```

Примечание.

Чтобы просмотреть список всех установленных в вашей системе конфигураторов, в командной строке введите **redhat-config-** и нажмите два раза клавишу «Tab». Можно также использовать команду:

```
rpm -qa | grep redhat-config-
```

Подождите, пока пакет будет установлен. Теперь все готово для настройки сети. Если система X-Window не запущена, ее нужно запустить, поскольку **redhat-config-network** — это графический конфигуратор и для ее работы нужна X-Window. Если X-Window не запускается автоматически, введите команду **startx**. Если же X-Window запускается при загрузке системы, для перехода в графический режим нажмите комбинацию клавиш Alt+F7.

Затем откройте терминал и введите команду **redhat-config-network**. Напомню, что запускать программу нужно от имени пользователя root. Конфигуратор обладает настолько понятным интерфейсом, что дальше вы справитесь без моего напутствия. Вы не забыли параметры сети: IP-адрес 192.168.1.5, маска сети 255.255.255.0. Имя компьютера — COMP5. Имя рабочей группы в Linux не используется — мы будем его указывать только при настройке пакета Samba (когда необходимо, чтобы Linux-машина работала в Windows-сети).

После изменения настроек сети перезагружать компьютер не нужно — это вам не Windows. Лучше сразу протестировать настройки. Сначала нужно убедиться, что сетевой интерфейс функционирует без ошибок. Для этого в Windows использовалась программа **ipconfig**. В Linux для этих целей используется программа **ifconfig** (сокр. от interface configuration).

Введите команду:

```
ifconfig
```

В ответ получите примерно следующее:

```
eth0      Link encap:Ethernet  HWaddr 00:02:44:7B:2B:86
          inet addr:192.168.1.5  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:11 Base address:0xb000
          Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1512 (1.4 Kb)  TX bytes:1512 (1.4 Kb)
```

Последний интерфейс — это интерфейс обратной петли (127.0.0.1). Он нас не интересует, поэтому не обращайте на него внимания. Что же выводит программа **ifconfig**? В первых двух строчках выводится тип адаптера (Ethernet), его MAC-адрес — HWaddr (физический адрес адаптера).

```
eth0 Link encap:Ethernet  HWaddr 00:02:44:7B:2B:86
     inet addr:192.168.1.5  Bcast:192.168.1.255  Mask:255.255.255.0
```

В третьей строке — параметры интерфейса:

```
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Они означают, что интерфейс запущен и используется, MTU интерфейса равно 1500, метрика — 1 (о метрике мы будем говорить при рассмотрении маршрутизации).

Примечание.

MTU (Maximum Transfer Unit) — максимальная единица передачи данных. Практически все протоколы позволяют использовать в кадре поля переменной длины, это касается даже заголовка кадра. Максимально допустимое значение длины поля — это как раз и есть MTU.

Далее следует статистика — сколько пакетов принято/передано, сколько байтов принято/передано, а также сколько коллизий было с участием этого интерфейса.

Убедившись, что с интерфейсом все в порядке, можно попробовать пропинговать самого себя, а также соседний узел. Что делать, если пинг «не доходит», вы уже знаете из предыдущих пунктов, поэтому я не вижу смысла повторяться. Лучше рассмотрим пару примеров использования команды **ifconfig**. Пробовать их не нужно, поскольку вся настройка производится через конфигуратор:

`ifconfig eth0 192.168.1.1 up` — «поднимаем» сетевой интерфейс.

А более корректно это будет выглядеть так:

```
/sbin/ifconfig eth0 ${IPADDR} broadcast ${BROADCAST}
netmask ${NETMASK}
```

Широковещательный адрес (broadcast) — это как адрес сети, но с 255 вместо последнего нуля. Если адрес сети 192.168.1.0, то широковещательный адрес будет 192.168.1.255.

Настройка в дистрибутивах ALT Linux

В дистрибутивах ALT Linux и Mandrake Linux для настройки сети используется один и тот же конфигуратор — **draknet** (ну, может быть дизайн чуть-чуть отличается), в остальном — это один и тот же конфигуратор. Но все же, чтобы вы не терялись, настройку сети в ALT Linux и Mandrake Linux будем производить параллельно, не ограничиваясь фразой «по аналогии».

Начнем с ALT Linux. Запустите конфигуратор **draknet** (рис. 6.65). Я рекомендую запускать его из терминала, поскольку по окончании настройки (и во время самой настройки) вы сможете увидеть диагностические сообщения. Напомню, что запуск конфигуратора нужно производить в системе X Windows, поскольку это графический конфигуратор, и от имени пользователя root (в случае необходимости для получения прав суперпользователя можно использовать команду **su**, как это было показано на примере Red Hat Linux).

Оставим автоопределение настроек сети в покое. Лучше будем использовать режим эксперта (Expert mode). Не бойтесь этого слова — эксперт. Даже если вы и не являетесь экспертом в области сетевых технологий, данный режим поможет вам лучше настроить сеть, указав некоторые параметры, которые в обыкновенном режиме принимаются по умолчанию.

Следующий шаг — это выбор типа соединения, которое вы хотите настроить (рис. 6.66). Можно сразу настроить несколько (или даже все, если это нужно) соединений. Мы сейчас будем настраивать только одно соединение — по локальной сети (LAN connection).

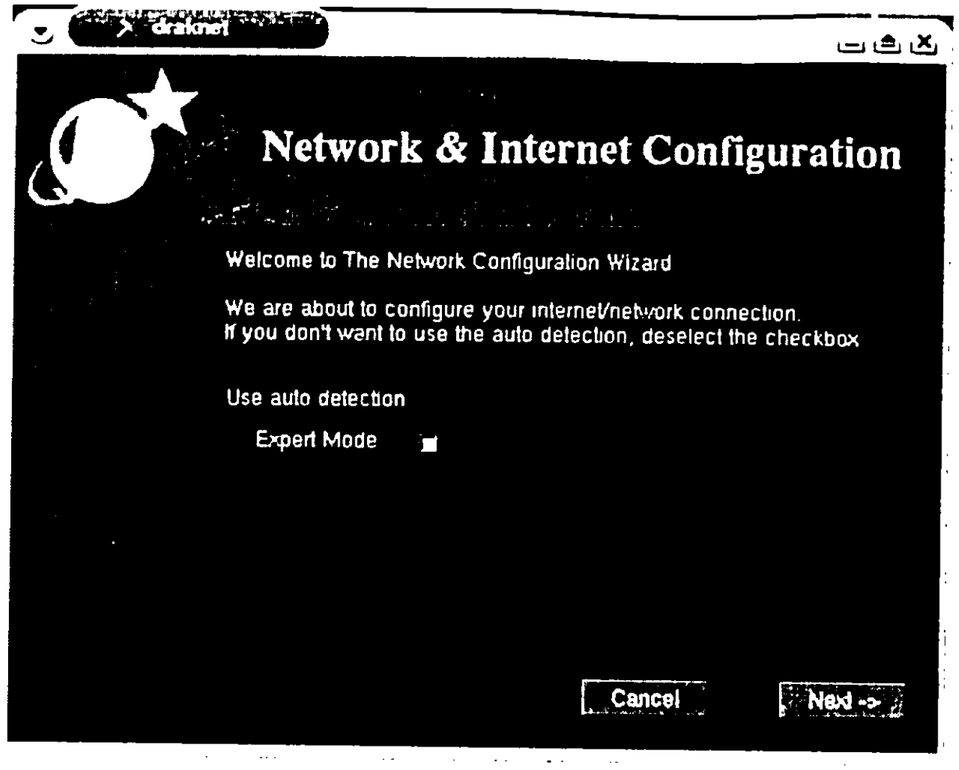


Рис. 6.65. *Конфигуратор draknet*

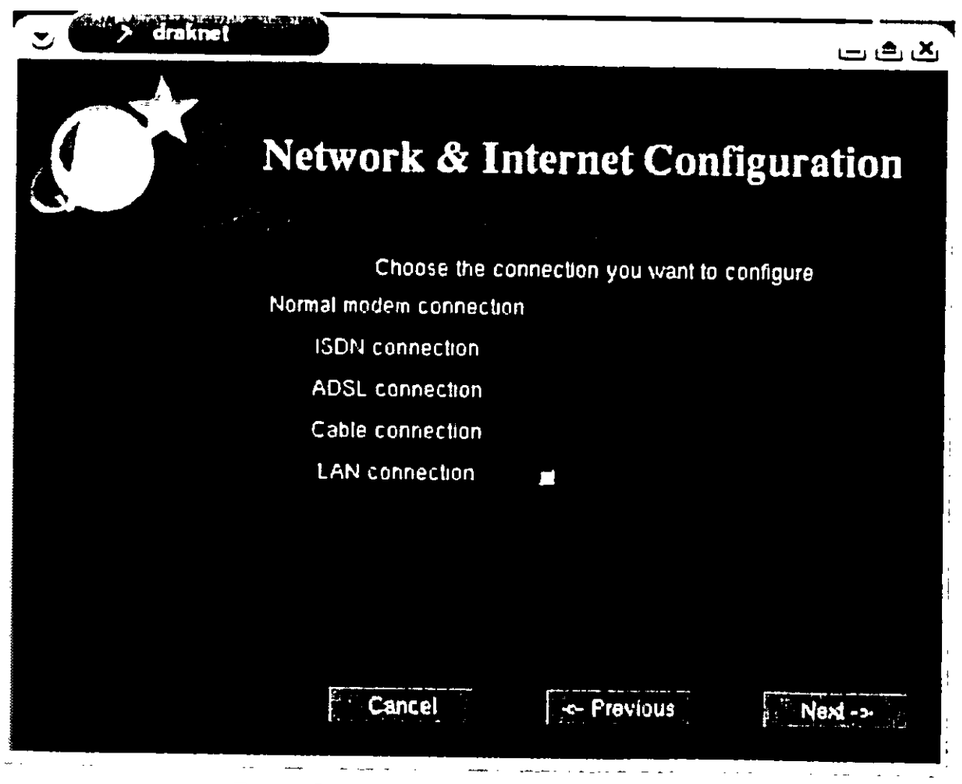


Рис. 6.66. *Выбор типа соединения*

После этого конфигуратор draknet «опознает» ваш сетевой адаптер (даже, если **kudzu** уже это сделал!) и спросит, есть ли у вас еще один сетевой адаптер (рис. 6.67). Отвечаем **No** (если у вас есть еще одна сетевая плата, то нужно выбрать Yes) и нажимаем кнопку **Next** (Далее).

Затем нужно ввести уже известные нам (на этот раз я их повторять не буду) IP-адрес и сетевую маску. Потом нужно установить два параметра соединения (рис. 6.68):

- **Automatic IP (bootp/dhcp)** — не нужно включать этот параметр, поскольку мы настраиваем интерфейс вручную.
- **Start at boot** — а этот режим обязательно нужно включить, в этом случае интерфейс будет «поднят» при загрузке системы.

Следующий шаг — это ввод имени компьютера (COMP5, на рис. 6.69 — имя моего домашнего компьютера), IP-адреса сервера DNS и шлюза — эти два адреса пока вводить не нужно.

Следующий шаг мастера — это ввод прокси-серверов для протоколов HTTP и FTP (рис. 6.70). Поскольку данные прокси мы не настраивали (пока), ничего вводить не нужно.

Затем конфигуратор поздравит вас с успешной настройкой интерфейса. Если вы запустили конфигуратор из терминала, то после завершения его работы вы увидите диагностические сообщения, как показано на рис. 6.71.

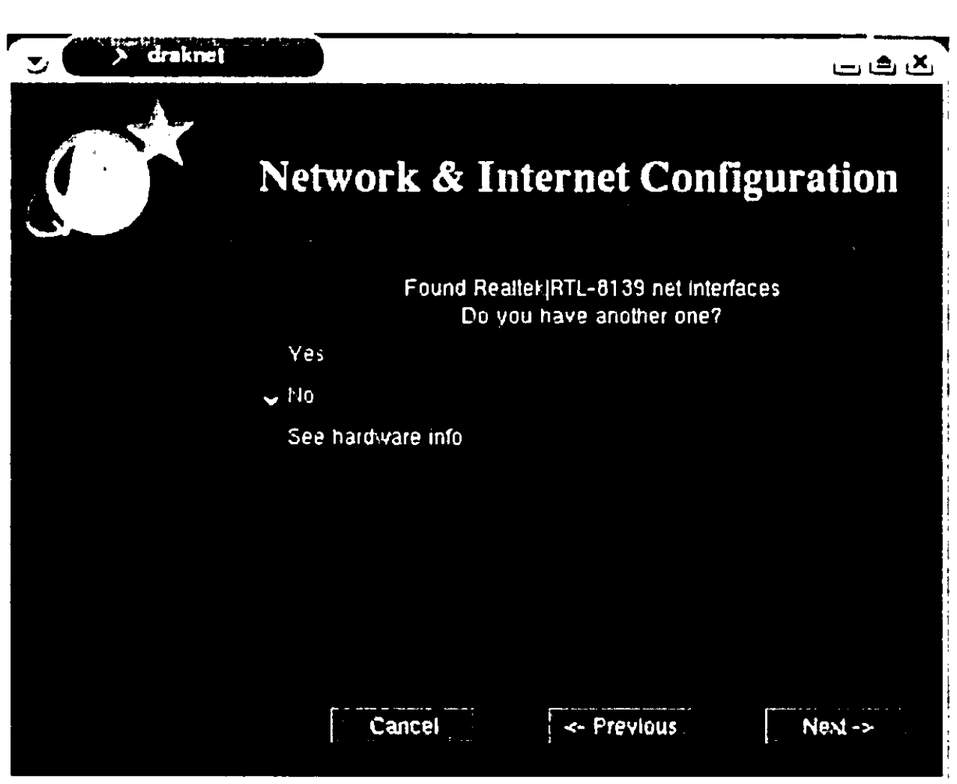


Рис. 6.67. *Сетевой адаптер опознан*

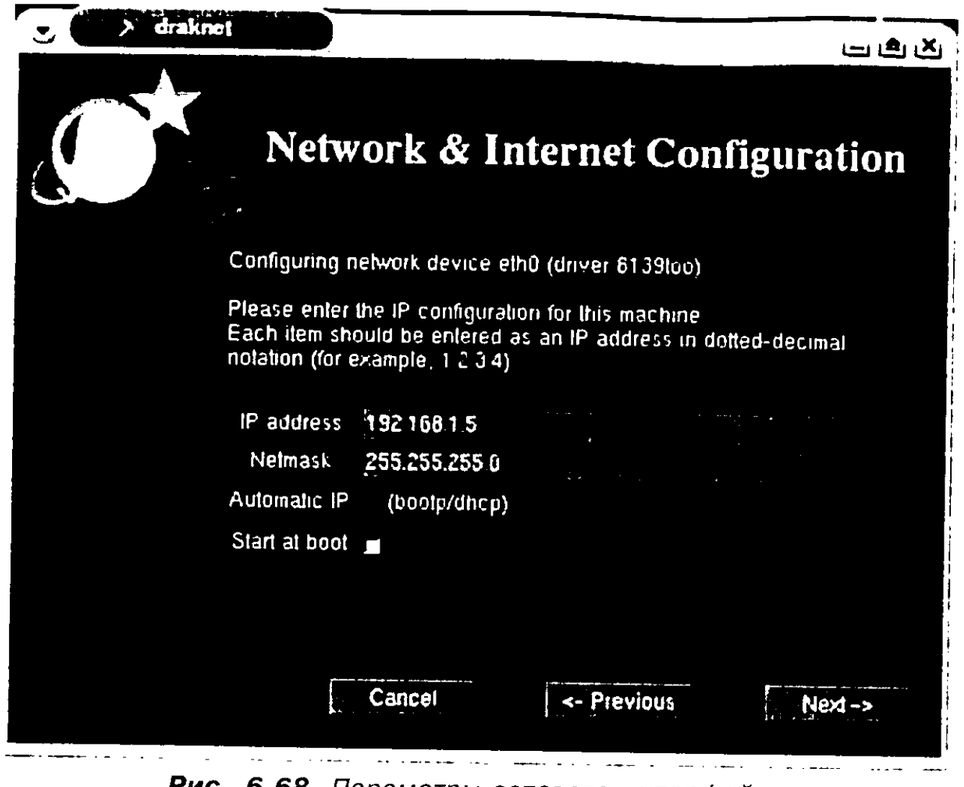


Рис. 6.68. *Параметры сетевого интерфейса*

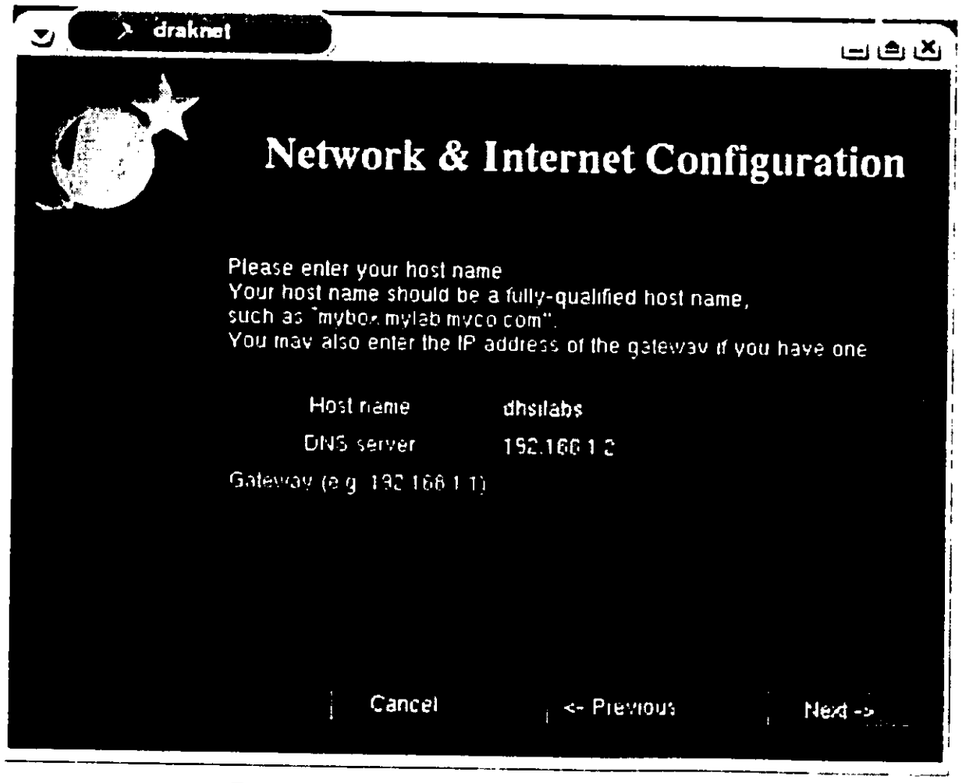


Рис. 6.69. *Ввод имени компьютера*

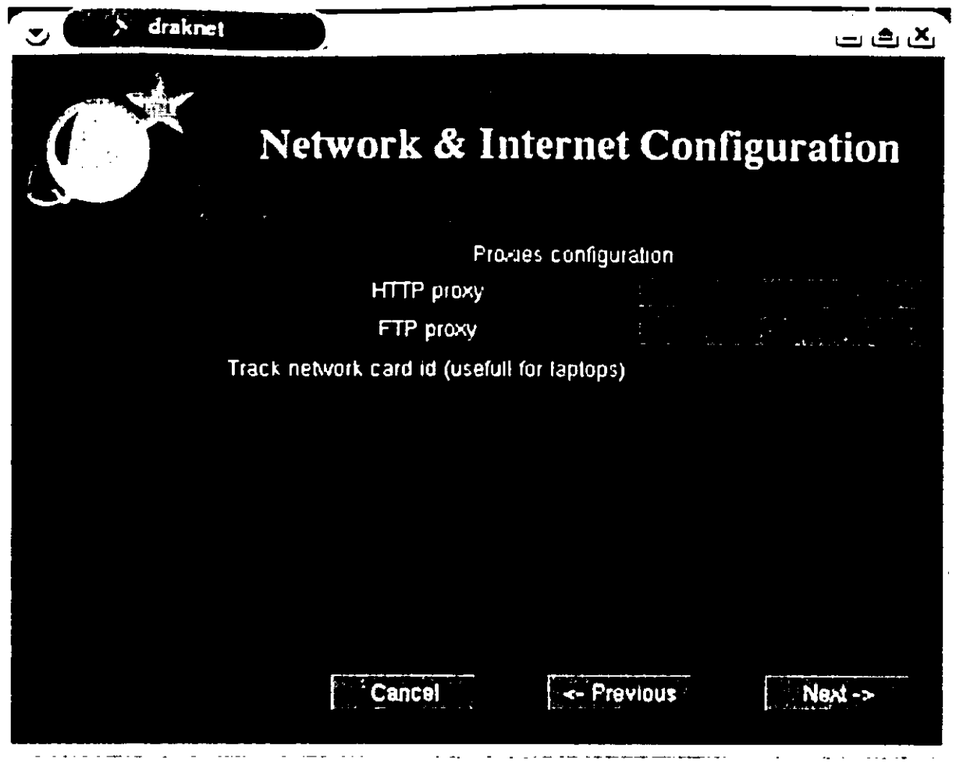


Рис. 6.70. *Ввод имени прокси-сервера*

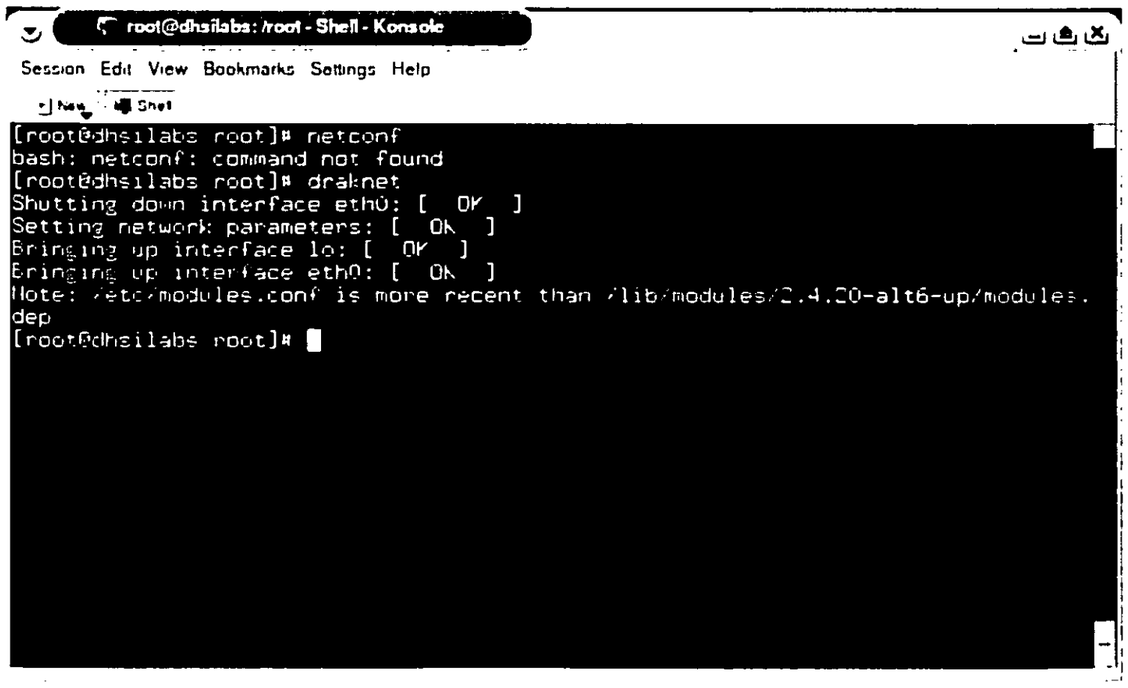


Рис. 6.71. *Диагностические сообщения*

Сначала конфигуратор останавливает интерфейс `eth0`:

```
Shutting down interface eth0
```

У вас, скорее всего, не будет этого сообщения, поскольку до запуска конфигуратора сеть на данном компьютере уже была настроена. Затем сказано, что параметры сети установлены:

```
Setting network parameters
```

Следующие два сообщения говорят о том, что интерфейсы `lo` и `eth0` запущены:

```
Bringing up interface lo
Bringing up interface eth0
```

Вам остается сделать следующее:

- ввести команду **ifconfig**, дабы убедиться, что сетевой интерфейс поднят
- пропинговать сначала наш интерфейс, а потом любой другой компьютер вашей сети: ping 192.168.1.5 (рис. 6.72).

Что делать, если пинг «не проходит», вы уже знаете, поэтому не будем тратить на объяснение время.

Примечание.

После изменения настроек сети перезагружать компьютер не нужно, однако рекомендуется перезагрузить сервер X Window.

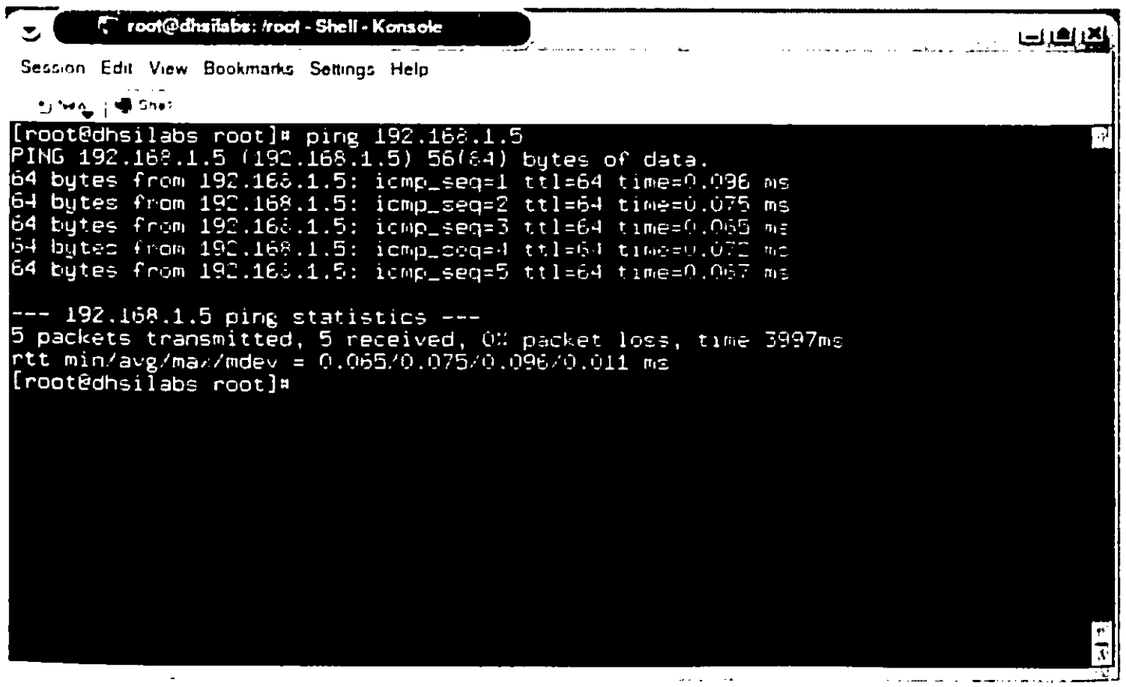


Рис. 6.72. *Команда ping 192.168.1.5*

Настройка в дистрибутиве Mandrake Linux

В Linux Mandrake настройка сети практически аналогична дистрибутиву ALT Linux. Для настройки сети запустите конфигуратор DrakConf (он же Центр управления Mandrake, Mandrake Control Center). Для его запуска выберите и дважды щелкните по иконке Manadrake Control Center на вашем рабочем столе или введите команду **drakconf** в командной строке. Конфигуратор DrakConf (рис. 6.73) может работать не только в графическом, но и в текстовом режиме (в консоли без запуска системы X Window). Если вы не зарегистрированы как пользователь root, конфигуратор сообщит вам об этом и попросит ввести пароль пользователя root.

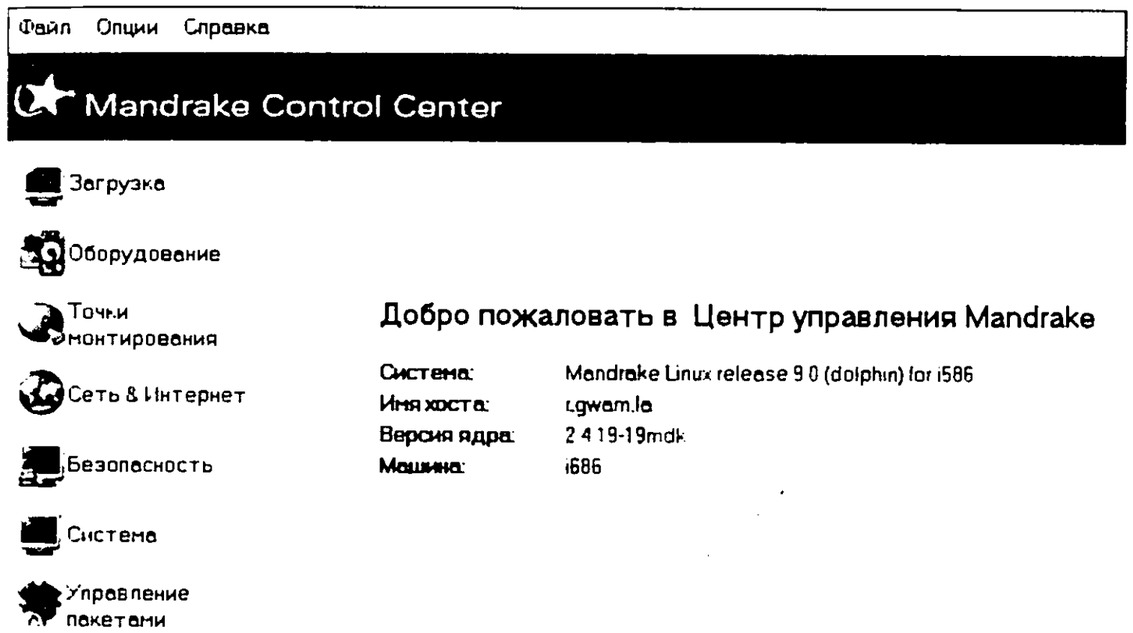


Рис. 6.73. *Mandrake Control Center*

Для настройки сети выберите пункт **Сеть&Интернет** из меню, расположенного в левой части окна. Будет запущен конфигуратор **drakconnect**. (рис. 6.74).

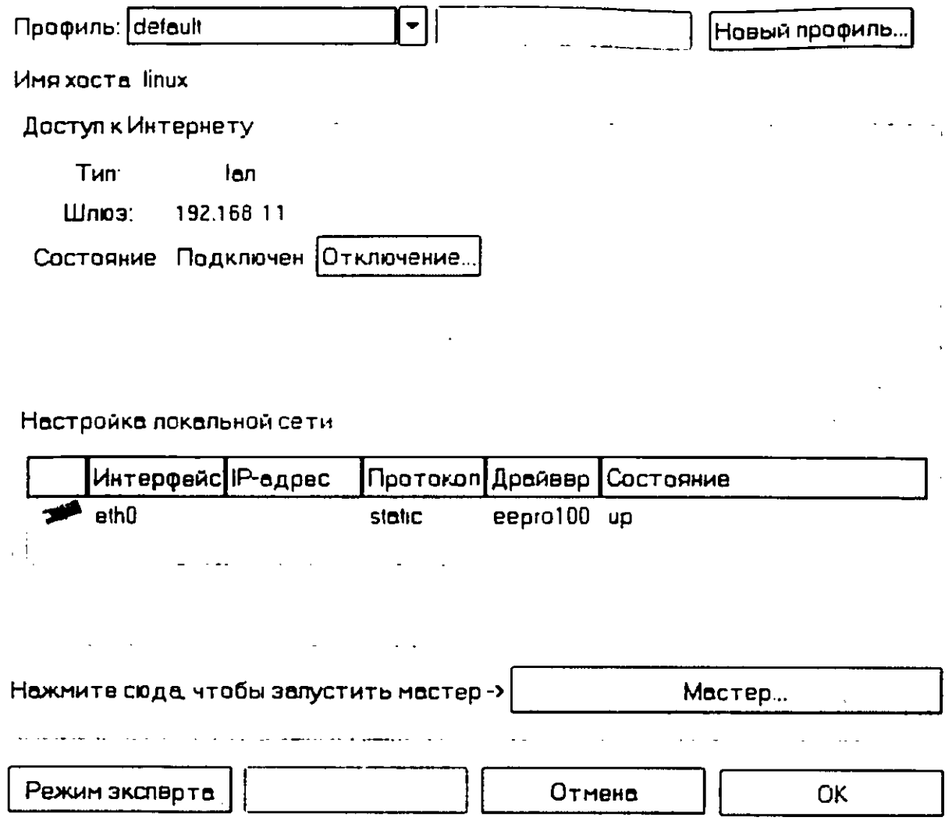


Рис. 6.74. *Конфигуратор drakconnect*

Изюминкой конфигуратора **drakconnect** является использование профилей настроек. Почему это удобно? Например, у вас ноутбук и вы работаете дома и в офисе. Параметры вашей сети, ясное дело, отличаются от параметров корпоративной сети.

При переходе из домашней в корпоративную сеть и обратно, вам не придется настраивать сеть заново: достаточно выбрать нужный профиль из списка. Создать новый профиль можно, нажав кнопку **Новый профиль**, а для удаления профиля используется кнопка **Удалить профиль**.

Настраивать сеть можно в двух режимах — в режиме Мастера и Эксперта. Режим мастера полностью аналогичен вышеописанному мастеру ALT Linux (только дизайн немного изменен, а так все одно и то же), а режим эксперта позволяет настроить соединение без мастера.

После настройки сетевого соединения не забудьте пропинговать свой узел и удаленный узел.

Простая идентификация узлов (компьютеров)

В этой главе рассматривается простая идентификация узлов локальной сети, а именно, как IP-адреса преобразуются в символьные имена и обратно. Почему простая? Да потому, что мы будем использовать штатные средства операционной системы, а не сервер DNS. Если не настраивать идентификацию узлов, то сеть работать будет, но для обращения к какому-нибудь компьютеру нужно будет использовать не символьное имя, а IP-адрес, например, http://192.168.1.1/ Не очень удобно, правда?

7.1. Имена и IP-адреса компьютера

Компьютеру проще работать с числами, нежели с символьными именами. Человеку, например, намного проще запомнить символьное имя ivanov, чем адрес 192.168.57.51. Правда? Тут уже сказывается психология человека — символьное имя сопоставляется с неким образом - Ивановым, а не какими-то абстрактными числами. Компьютер же просто так устроен, что ему «удобнее» оперировать с числами.

Проблема разрешения имен, то есть преобразования IP-адреса компьютера в символьное имя и обратно, волновала разработчиков сетей давно — с момента появления первых сетей. Сначала для разрешения имен использовался файл `hosts`. В этом файле хранилась следующая информация:

- IP-адрес;
- имя;
- псевдонимы узла.

Например:

```
127.0.0.1       localhost
192.168.1.1     gateway
192.168.1.5     dhsilabs
```

В пределах одной организации и при условии, что компьютеров немного, скажем 5...10 или меньшее количество, файл `hosts` должен устраивать всех. Вы его заполняете, например

```
192.168.1.1     comp1
...
192.168.1.N     compN
```

и копируете на все компьютеры вашей сети — от `comp1` до `compN`. При добавлении нового компьютера в сеть, вам нужно добавить строку:

```
192.168.1.N+1   compN+1
```

в файл hosts и опять скопировать данный файл на все компьютеры от 1 до N+1. Не очень удобно, неправда ли? Но, неужели у вас каждый день добавляются новые компьютеры в вашу сеть? Обычно сеть небольшого предприятия — это от 2 до 10 компьютеров, причем новые компьютеры редко подключаются к сети. В этом случае файл `hosts` должен полностью удовлетворить ваши требования.

Другое дело, когда нужно разрешать имена в глобальной сети или сети большого предприятия, где состав сети может модифицироваться каждый день, что и происходит на практике. Не будем трогать глобальные сети — и так ясно, что файл `hosts` для них не подходит.

В большом предприятии состав сети может изменяться несколько раз в день, например, пользователь перешел из одного раздела в другой и перенес свой компьютер (ноутбук) или же просто добавлен компьютер в один из разделов. Как тогда? Копировать файл `hosts` на все 300 компьютеров? Конечно, можно настроить систему так, чтобы она сама копировала файл `hosts` с главного компьютера — компьютера администратораг — на локальный компьютер. Но это не выход: что делать, если на протяжении рабочего дня был добавлен компьютер в один из разделов? Перезагружать все три-четыре сотни компьютеров или они временно (до следующего дня) не смогут получить доступ к новому компьютеру?

В глобальной сети возникает еще и проблема иерархии узлов. Вы можете представить, что компьютеры компаний IBM, Microsoft, Compaq, Intel и других крупных компаний смешаны — находятся в одном адресном пространстве глобальной сети? Не знаю, как вам, мне это довольно трудно сделать.

7.2. Требования к системе имен

Итак, мы пришли к выводу, что нам необходима служба разрешения имен, которая бы обеспечивала — это только минимальные требования:

- централизованное хранение базы данных IP-адресов и символьных имен;
- иерархическую структуру узлов разных сетей;
- преобразование IP-адреса в символьное имя и обратно.

Обратите внимание на последовательность наших требований к системе разрешения имен. Прежде всего, нас интересует централизованное хранение базы данных, которая содержит IP-адреса и символьные имена компьютеров — чтобы нам не приходилось вручную загружать каждый день обновления файла `hosts`. Компьютер-клиент обратится к компьютеру-серверу, на котором запущена система разрешения имен, и «узнает» IP-адрес нужного компьютера, указав символьное имя, или, наоборот, его символьное имя, указав IP-адрес. Все компьютеры будут работать с одной и той же копией базы данных — как только администратор добавит новую запись, содержащую сведения о новом компьютере, все компьютеры сети при необходимости сразу же смогут обратиться к новому компьютеру, зная его имя или IP-адрес.

Второе требования к системе разрешения имен — это иерархическая структура базы данных. Помните, пример с компаниями Microsoft, IBM, Compaq и Intel? Предположим, что на компьютере-сервере имеется четыре каталога — Microsoft, IBM, Compaq, Intel. В каждом из этих каталогов находится файл `hosts`, в котором содержится информация о узлах этих компаний. Тогда компьютер-клиент подает запрос, наподобие `GET_IP comp.ibm`. Компьютер-сервер анализирует запрос: GET_IP — нужен IP-адрес. ibm — нужно смотреть каталог IBM, переходит в этот каталог, открывает соответствующий файл `hosts`, просматривает его, находит запись, содержащую IP-адрес компьютера comp (если она есть вообще) и возвращает найденный IP.

Само преобразование имен — это третье, последнее требование. Почему оно указано последним, а не первым? Да потому, что само разрешение имени — это задача несложная и с ней можно справиться, используя только файл `hosts`. А вот первые два требования обеспечивают комфорт управления сетью, чего мы, собственно, и добивались.

Как вы уже догадались, наша абстрактная система разрешения имен давным-давно реализована на практике — это DNS (Domain Name System) — доменная система имен. О DNS поговорим в одной из следующих глав (когда будем рассматривать иерархическую сеть), а сейчас вернемся к файлу `hosts`.

7.3. Файл hosts

Практически в каждой сетевой операционной системе существует свой файл `hosts`. Если это Windows, то вы найдете его в каталоге, в котором установлена Windows, а если Linux, то файл `hosts` будет расположен в каталоге `/etc`.

Начнем с Linux. Откройте файл `/etc/hosts`. Его формат следующий:

```
IP-адрес имя  (*) псевдонимы
```

Примечание.
(*) Допускается указание полного доменного имени, например, comp5.firma.com

Пример файла `/etc/hosts` приведен в листинге 7.1.

Листинг 7.1. Файл /etc/hosts

```
127.0.0.1       localhost.localdomain localhost
192.168.1.1     dhsilabs
192.168.1.2     comp2
192.168.1.3     comp3
192.168.1.4     comp4
192.168.1.5     comp5
```

По умолчанию в Windows 9x/ME данный файл не создается. Вместо него в каталоге Windows (у вас он может называться по-другому) вы найдете файл `hosts.sam` (сокращенное от hosts sample) — пример файла `hosts`. Этот файл нужно скопировать в файл `hosts` или создать новый файл вручную. Формат этого файла:

```
IP-адрес имя
```

В качестве имени допускается полное доменное имя. Пример файла c:\windows\hosts приведен в листинге 7.2

Листинг 7.2. Пример файла c:\windows\hosts

```
127.0.0.1       localhost
192.168.1.1     dhsilabs
192.168.1.2     comp2
192.168.1.3     comp3
192.168.1.4     comp4
192.168.1.5     comp5
```

В Windows 2000/XP данный файл находится в каталоге `%WINDIR%\System32\Drivers\Etc`. Формат данного файла такой же, как и в Windows 9x.

Настройка простейшей Windows-сети. Рабочие группы и общие ресурсы

8.1. Что такое рабочая группа?

В этой главе мы рассмотрим одноранговую сеть Microsoft. Как вы знаете, одноранговая сеть — это сеть без выделенного сервера. Любой компьютер в сети может выступать как в роли клиента, так и в роли сервера, то есть использовать общие ресурсы или предоставлять ресурсы в общее использование. Компьютеры одноранговой сети объединяются в рабочие группы.

В одном физическом сегменте может быть несколько рабочих групп, то есть вам необязательно разбивать сеть на подсети — отдельная подсеть для рабочей группы не нужна. Использование рабочих групп — это идеальное решение для небольшой домашней или офисной сети. Например, у вас могут быть рабочие группы `Buhgalteria` и `Programmers` — бухгалтерия и программисты. Первая объединяет компьютеры бухгалтерии, а вторая — компьютеры программистов.

Ограничение доступа к общим ресурсам происходит на уровне ресурсов. Например, вам нужно предоставить общий доступ к диску D. При этом вы можете выбрать уровень доступа:

- Только чтение.
- Полный.
- Определяется паролем.

В первом случае все пользователи сети могут только читать файлы, расположенные на вашем диске D. Во втором случае все пользователи сети получают полный доступ к файлам на диске D — они могут записывать на диск новые файлы, удалять уже имеющиеся, просматривать интере-

сующие их файлы и т.д. В последнем случае для доступа к ресурсу вы определяете два пароля — один для чтения, а второй — для записи.

Если пользователь обращается к ресурсу, следовательно, выполняется операция чтения ресурса и ему нужно указать пароль для чтения. Если пользователь хочет записать файлы на диск D или же модифицировать имеющийся на нем файл, ему нужно будет ввести пароль, разрешающий запись ресурса. Все пользователи сети будут знать пароль для чтения, но лишь некоторые — пароль для записи.

Неудобство данного метода заключается в том, что невозможно контролировать доступ каждого пользователя отдельно. Например, пароль для записи знают три человека. Кто-то модифицировал ваш квартальный отчет, причем, при этом допустил множество ошибок. Как узнать, кто это сделал? Узнав, что он допустил ошибки, этот человек может и не признаться — вот вам первый человеческий фактор. Второй человеческий фактор заключается в том, что пользователи, знающие пароль для записи, могут «поделиться» ним с другими пользователями, которые его не знают.

Для небольшой офисной сети одноранговая сеть, как уже отмечалось, довольно приемлемое решение. Думаю, если в вашей организации работает не очень много человек, выяснить, кто модифицировал файл не очень сложно: достаточно собраться всем вместе. Ну а дальше дело техники.

Достоинства одноранговой сети — это ее простота и дешевизна. Любой пользователь с уровнем знаний большим, чем у оператора компьютерного набора, справится с администрированием такой сети (если операции по предоставлению ресурсов в общее пользование можно вообще назвать администрированием). А экономия заключается в том, что вам не придется выделять отдельный компьютер для сервера, покупать серверную операционную систему и нанимать на работу администратора (хотя, если вы читаете эту книгу, последнее необязательно).

8.2. Создание рабочей группы

Узнав, что такое рабочая группа, перейдем к практике, а именно к созданию рабочей группы. Предположим, что у нас есть два компьютера бухгалтеров BUH1, BUH2 и три компьютера программистов — PRG1, PRG2, PRG3. Первые два компьютера мы хотим объединить в группу BUHGALT, а остальные — в группу PROGRAMMERS. Длина имени рабочей группы не должна превышать 15 символов.

Рабочие группы в Windows 9x/ME

Если наши компьютеры (или один из них) работают под управлением Windows 9x/ME, выполните следующие действия. Прежде всего, нам

нужно активизировать службу доступа к файлам и принтерам, если это еще не сделано. Откройте апплет **Сеть** с Панели управления. Если на вкладке **Конфигурация** (рис. 8.1) в самом конце списка есть служба доступа к файлам и принтерам, значит, она установлена.

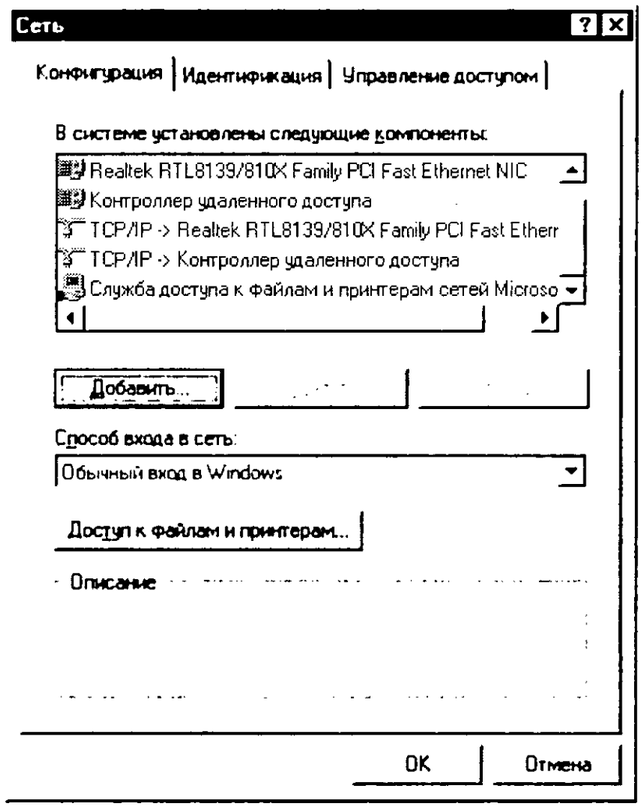


Рис. 8.1. *Конфигурация системы*

В противном случае вам нужно нажать кнопку **Добавить**. В окне **Выбор типа компонента** выберите **Служба**, а в следующем окне нужно выбрать из списка службу доступа к файлам и принтерам сети Microsoft (рис. 8.2).

После перезагрузки компьютера снова откройте апплет **Сеть**. На странице **Конфигурация** нажмите кнопку **Доступ к файлам и принтерам** и выберите нужный тип доступа к ресурсам этого компьютера (рис. 8.3): будут ли пользователи сети получать доступ только к файлам этого компьютера или только к принтерам, подключенным к этому компьютеру, или же и к файлам, и принтерам.

Затем перейдите на вкладку **Идентификация** (рис. 8.4). На этой вкладке введите имя компьютера — BUH1 для первого или BUH2 — для второго компьютера. В поле **Рабочая группа** введите имя рабочей группы — BUHGALT. Теперь перейдите на вкладку **Управление доступом** (рис. 8.5) и выберите режим **На уровне ресурсов**. Этим мы указываем, что мы хотим организовать одноранговую сеть.

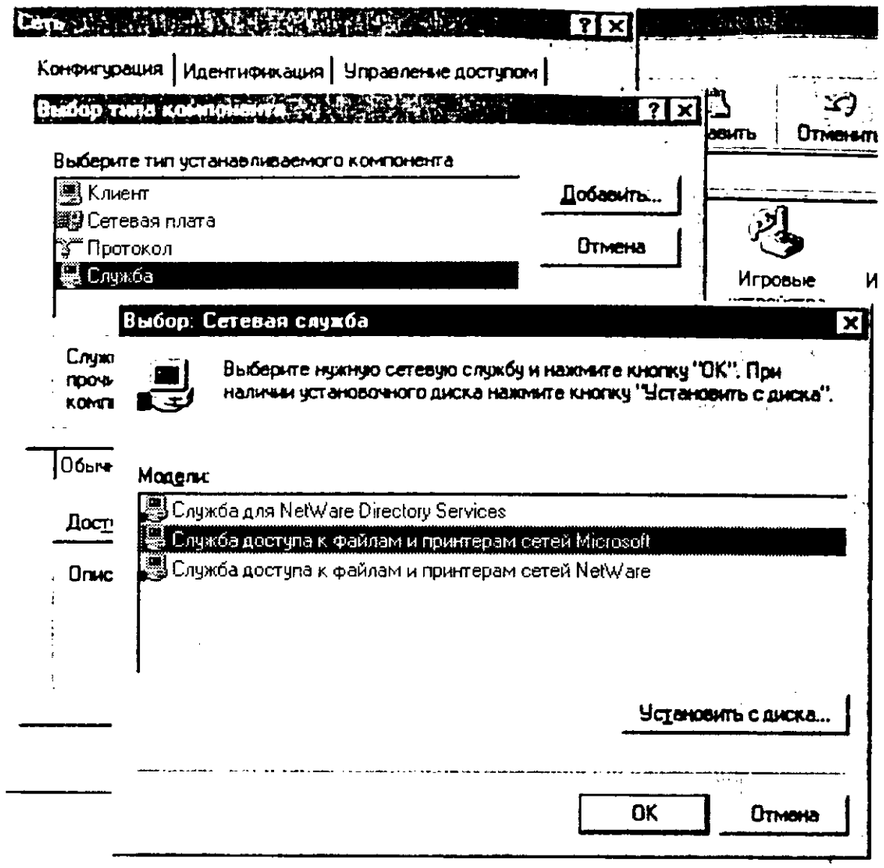


Рис. 8.2. *Установка службы доступа к файлам и принтерам Microsoft*

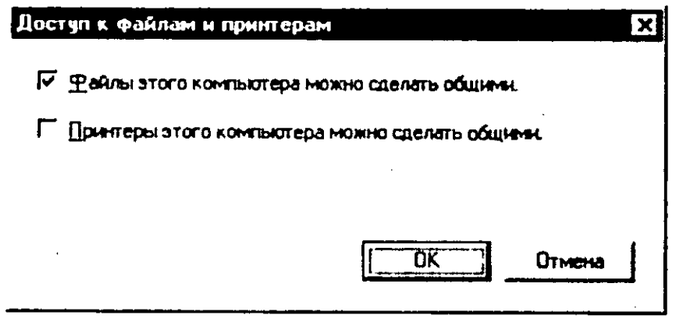


Рис. 8.3. *Доступ к файлам и принтерам*

Все, нажимаем Ок и перезагружаем компьютер. Если нам нужно добавить к группе новый компьютер — BUH3, выполняем для него те же действия. При вводе имени рабочей группы не допустите ошибок, иначе будет создана совершенно иная рабочая группа, членом которой будет единственный компьютер BUH3.

С компьютерами PRG1, PRG2, PRG3 нужно поступить аналогичным образом, только вместо имени BUHGALT нужно ввести имя рабочей группы PROGRAMMERS.

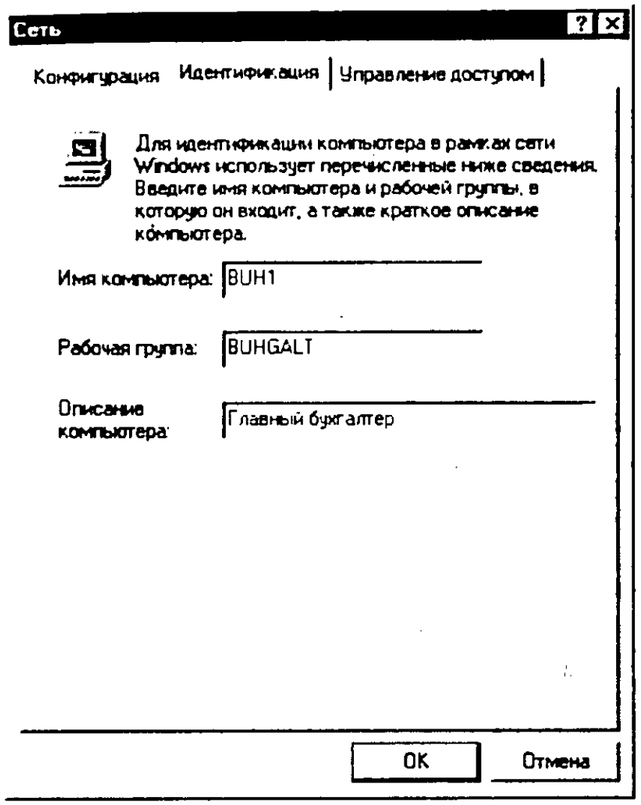


Рис. 8.4. *Идентификация*

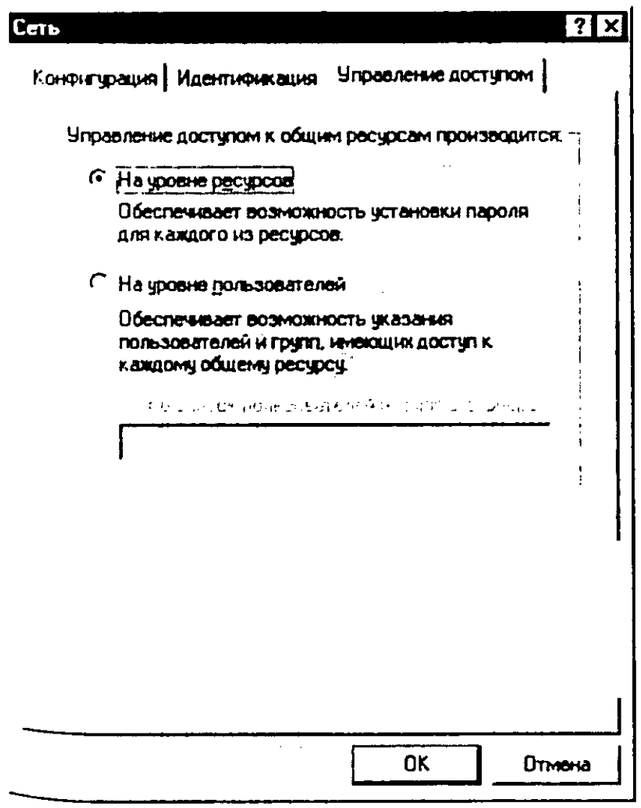


Рис. 8.5. *Управление доступом*

Рабочие группы в Windows NT 4.0

Если ваши компьютеры работают под управлением Windows NT, откройте апплет **Сеть** с Панели управления. На странице **Компьютер** нажмите кнопку **Изменить** и введите нужные вам имя компьютера и имя рабочей группы (рис. 8.6).

Рабочие группы в Windows 2000/XP

Служба доступа к файлам и принтерам в Windows 2000 и Windows XP устанавливается по умолчанию, если вы, конечно, не отключили ее при установке. На всякий случай откройте свойства соединения по локальной сети (**Пуск → Настройка → Сетевые подключения → Соединение по локальной сети → Свойства**) и убедитесь, что служба доступа к файлам и принтерам включена (см. рис. 8.7).

Если службы вообще нет в списке, нажмите кнопку **Установить**, выберите тип компонента **Служба**, а затем — службу доступа к файлам и принтерам.

Для создания группы откройте свойства системы, щелкнув на пиктограмме **Мой компьютер** и выбрав пункт меню **Свойства**. Перейдите на вкладку **Имя компьютера**, затем нажмите кнопку **Изменить** и введите имя компьютера и рабочей группы (рис. 8.8).

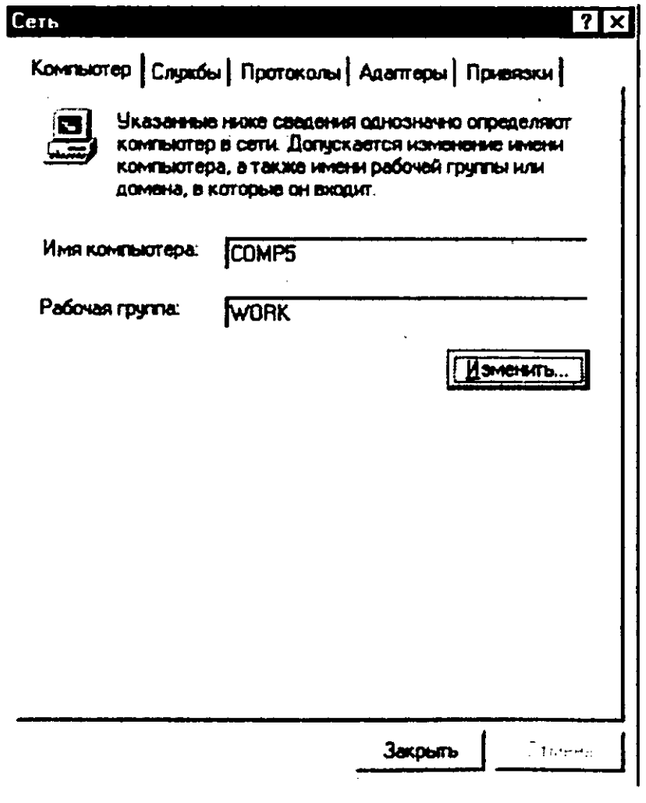


Рис. 8.6. *Имя компьютера и рабочей группы в Windows NT*

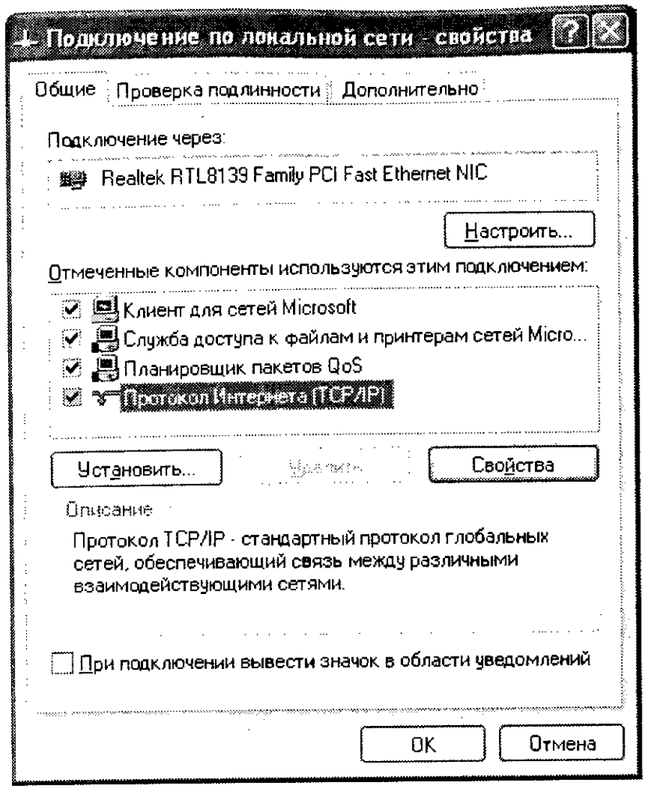


Рис. 8.7. *Компоненты соединения в Windows XP*

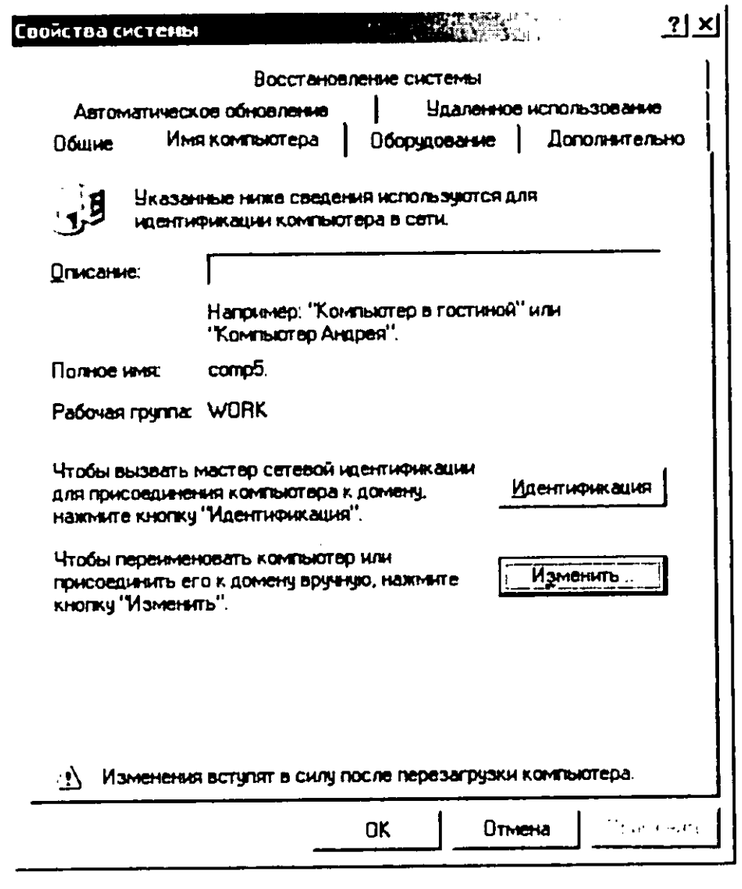


Рис. 8.8. *Имя компьютера и рабочей группы в Windows XP*

8.3. Предоставление общего доступа к ресурсам

Для более эффективного управления доступом к ресурсам компьютера я рекомендую открывать доступ не к целым дискам, а к отдельным каталогам. Тогда можно будет более или менее разграничивать доступ. Например, к каталогу `Music` назначить доступ только чтение, к каталогу `Uploads` — полный доступ, а к каталогу `Отчеты` — доступ по паролю.

Предоставление общего доступа из Windows 9x/ME

Предоставить доступ (иногда говорят «расшарить ресурс» — от англ. слова «share») к ресурсу в Windows 9x/ME проще простого. Для этого выберите нужный вам каталог (можно выбрать целый диск), щелкнув по нему правой кнопкой мыши, затем выберите команду **Свойства** и перейдите на вкладку **Доступ** (рис. 8.9).

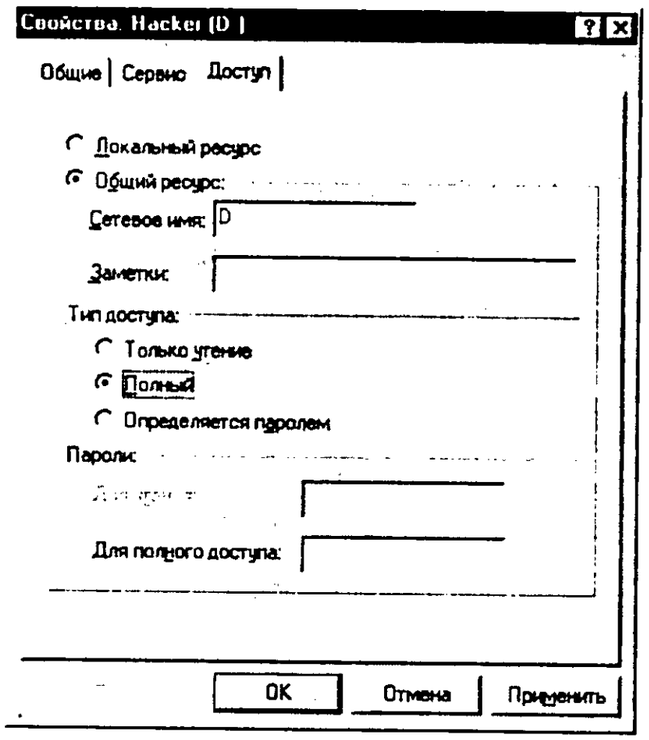


Рис. 8.9. Свойства ресурса

Вам нужно указать сетевое имя (оно может отличается от названия каталога или диска), а также определить режим доступа:

- **Только чтение** — ресурс будет доступен только для чтения.
- **Полный доступ** — можно будет указать пароль, разрешающий полный доступ к ресурсу. Тогда пользователям станут доступны все операции с файлами: создание, изменение, удаление, чтение и т.д. Если пароль не нужен, просто ничего не нужно вводить в поле ввода пароля.
- **Определяется паролем** — в этом случае нужно указать два пароля — один для чтения, а другой — для полного доступа. Причем обязательно нужно указать оба пароля, даже если они будут одинаковыми.

После этого нажмите Ок и общий ресурс будет доступен пользователям сети. В окне **Мой компьютер** общий ресурс будет представлен особой пиктограммой — папкой, лежащей на ладони.

Существует возможность подключить общий ресурс как локальный диск. При этом вы будете работать с таким ресурсом как с обыкновенным диском. Чтобы подключить сетевой диск, выполните следующие действия:

1. Щелкните на пиктограмме **Мой компьютер** правой кнопкой мыши и выберите команду **Подключить сетевой диск.**
2. Затем введите сетевой путь и выберите имя диска. Сетевой путь состоит из имени компьютера, содержащего общий ресурс, и имени самого ресурса. Например, путь для общего ресурса D на компьютере COMP1 выглядит так: \\COMP1\D.
3. Хотите ли вы, чтобы сетевой диск подключался автоматически при входе в систему? Если да, включите соответствующий режим (рис. 8.10).

Существует более простой способ подключения сетевого диска, который мы рассмотрим в следующем пункте.

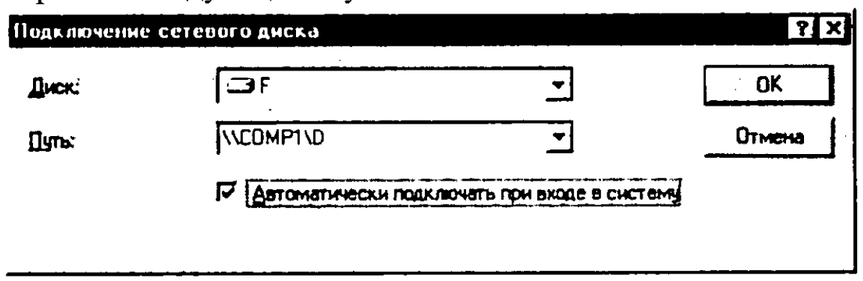


Рис. 8.10. Подключение сетевого диска

Предоставление общего доступа из Windows NT 4.0

Сразу нужно отметить, что настройка прав доступа к общим ресурсам в Windows NT намного сложнее, чем аналогичная операция в Windows 9x или Windows XP. Поэтому не нужно читать данный пункт «по диагонали», если вы действительно хотите разобраться с правами доступа.

Щелкните правой кнопкой на нужном вам каталоге, выберите команду **Свойства** и перейдите на вкладку **Доступ** (рис. 8.11).

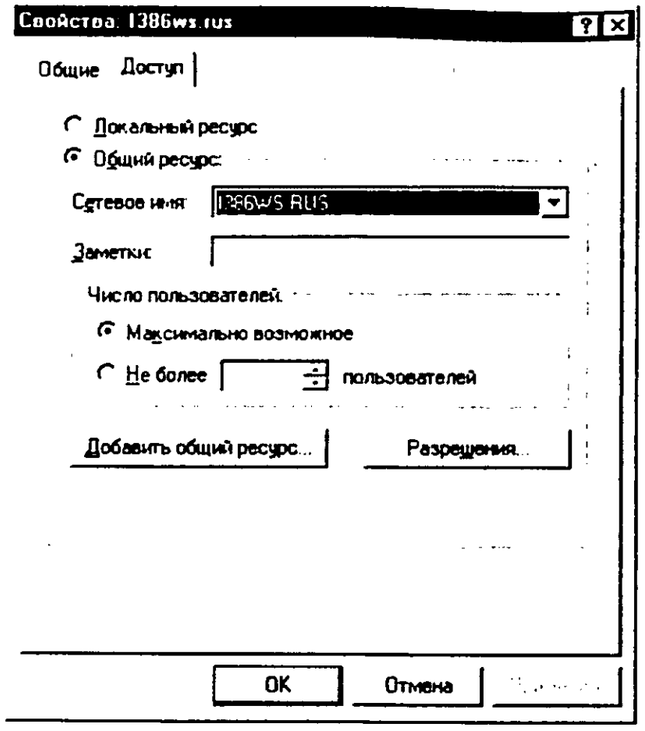


Рис. 8.11. *Определение параметров общего доступа к каталогу I386WS.RUS*

На этой вкладке вам нужно определить следующие параметры:

- **Сетевое имя ресурса**;
- **Заметки** — это просто примечание, содержащее описание ресурса;
- **Количество пользователей**, которые могут одновременно получать доступ к ресурсу.

Если в конце имени ресурса поставить знак доллара $, то этот ресурс не будет виден в сети. Обратиться к нему можно, только явно указав его имя в строке адреса Проводника. Это относится ко всем версиям Windows, а не только к Windows NT.

Если вы хотите предоставить персональный доступ какому-нибудь определенному пользователю, нажмите кнопку **Разрешения**. В результате откроется окно (рис. 8.12), в котором перечислены зарегистрированные в системе пользователи, которым разрешено пользоваться данным ресурсом.

Из вышеприведенного рисунка видно, что доступ к ресурсу могут получить абсолютно все пользователи, зарегистрированные в системе. Чтобы добавить определенного пользователя в список, нажмите кнопку **Добавить**.

В появившемся окне (рис. 8.13) вы увидите список групп. Вы можете выбрать любую из них. После этого пользователи данной группы получат доступ к компьютеру. Каждый из пользователей будет использовать

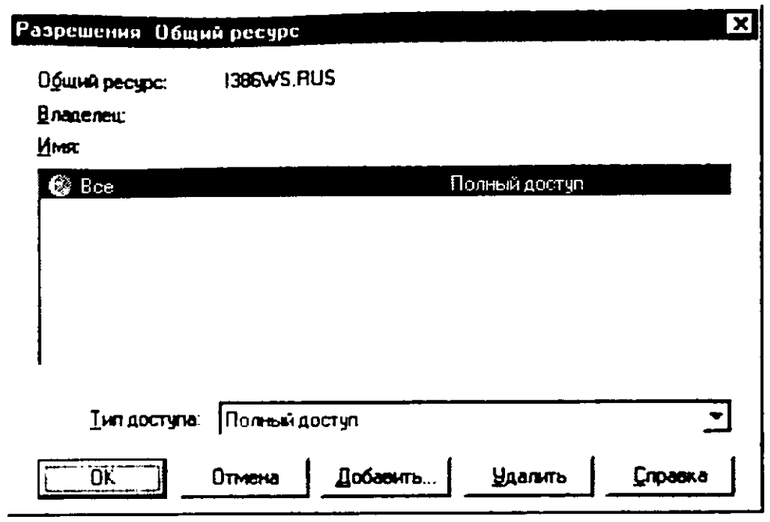


Рис. 8.12. *Кто получит доступ к ресурсу?*

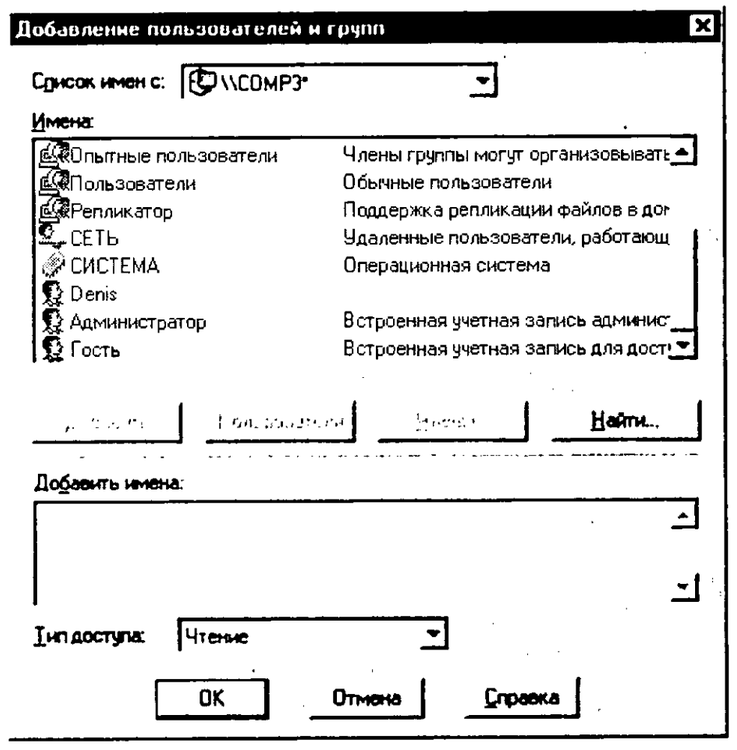


Рис. 8.13. *Добавление пользователей или групп*

собственный пароль доступа к системе. Если вас интересует какой-то конкретный пользователь, нажмите кнопку **Пользователи** и в конце списка вы увидите имена пользователей, зарегистрированных в системе.

Если нужного вам пользователя нет в списке, его нужно добавить. Для управления учетными записями пользователей используется утилита **Диспетчер пользователей** (рис. 8.14), вызвать которую можно из меню **Пуск → Программы → Администрирование (Общее)**.

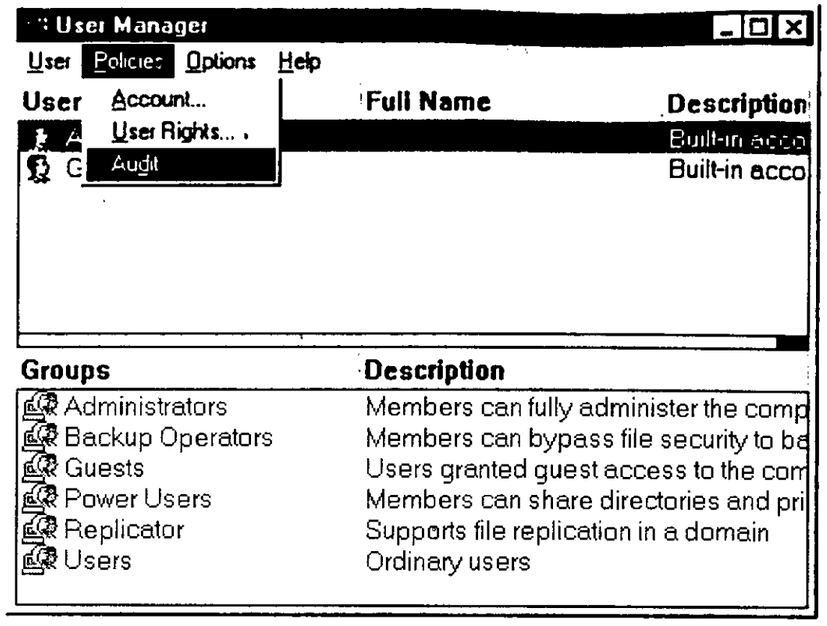


Рис. 8.14. *Диспетчер пользователей*

Для добавления пользователя используется команда меню **Пользователи → Добавить пользователя**. В появившемся окне нужно ввести имя пользователя, его пароль, а также нажать кнопку **Группы**, чтобы определить, к какой группе будет принадлежать пользователь (рис. 8.15). Можно добавить свою локальную группу, но я рекомендую использовать стандартные — `Администраторы` или `Пользователи`. Своего пользователя, под которым вы будете работать в системе, можно отнести к группе `Администраторы`, всех остальных — к группе `Пользователи`.

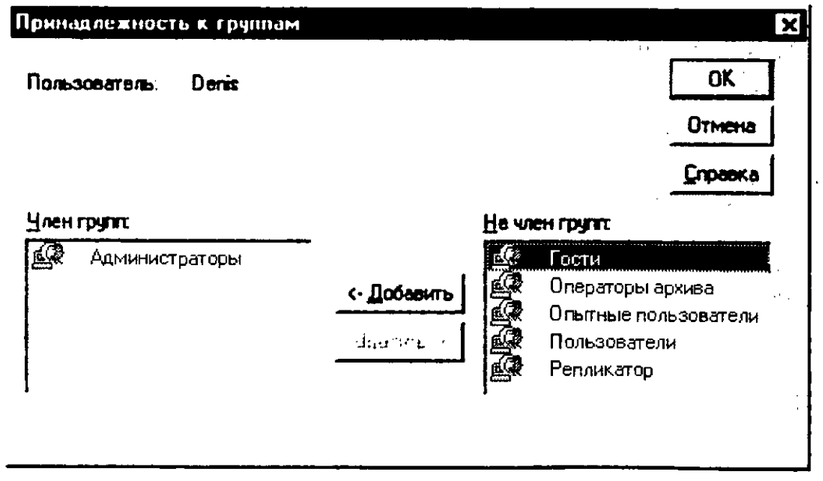


Рис. 8.15. *Определение принадлежности пользователя к локальной группе*

Добавив пользователя нужно вернуть к окну определения разрешений. Заново нажмите **Добавить**, а затем нажмите кнопку **Пользователи**. Только что добавленный пользователь должен появиться в списке. Выберите его, нажмите кнопку **Добавить**. Имя пользователя должно появиться в списке **Добавить имена**, например, `COMP3\Denis`. Теперь дважды нажмите кнопку **Ок**, а затем кнопку **Применить**. Все, доступ к ресурсу предоставлен. В окне **Мой компьютер** общий ресурс будет представлен особой пиктограммой — папкой, лежащей на ладони.

Теперь начинается самое интересное. Подойдите к другому компьютеру и попытайтесь получить доступ к общему ресурсу компьютера, работающего под управлением Windows NT. Вы получите диалоговое окошко, в котором нужно будет ввести имя пользователя и его пароль (рис. 8.16)!

Помните, я подчеркивал, что пользователь должен быть зарегистрирован в системе. Даже если вы выбираете группу Все, то это еще не означает, что доступ к ресурсу получат все пользователи сети. Здесь имеется в виду все пользователи, которые зарегистрированы в системе. Что же делать, если нужно предоставить общий доступ всем пользователям сети. Здесь есть два выхода. Или создать учетные записи пользователей для всех пользователей вашей сети, или же создать одного пользователя, задав для него простой пароль, например, «1» или «123».

Имя этого пользователя и пароль вы сообщаете всем пользователям вашей сети, чтобы они могли работать с вашим компьютером. Первый способ рекомендуется с точки зрения безопасности. Второй — более простой, для использования. Можно также включить пользователя `Гость` (это можно сделать в утилите Диспетчер пользователей) и задать для него простой пароль — это как один из вариантов второго способа. Как лучше — решайте сами.

Как видите, безопасность в Windows NT — на первом месте. Если пользователя нет в системе, то он не получит доступ даже на чтение ресурса.

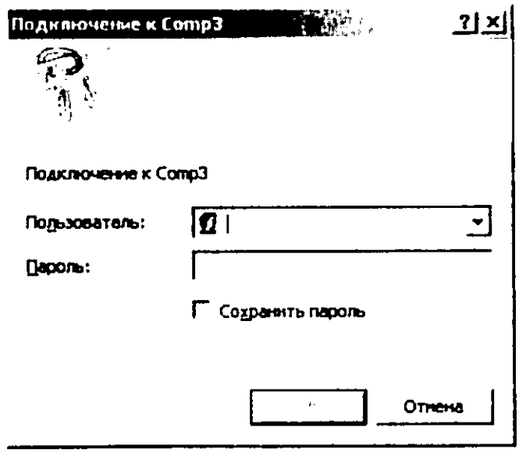


Рис. 8.16. *Ввод имени пользователя и его пароля*

Как-то непривычно, неправда ли? Концепция общего доступа Windows NT как-то не вписывается в концепцию одноранговых сетей, но зато она более практична с точки зрения безопасности.

Сейчас немного обобщим «технологию» предоставления общего доступа:

1. Откройте окно свойств каталога и перейдите на страницу **Доступ**.
2. Укажите имя ресурса, заметки и максимальное число одновременно работающих с ресурсом пользователей.
3. Нажмите кнопку **Разрешения**, чтобы определить, кому будет предоставлен доступ и режим доступа:
   - Только чтение.
   - Изменение.
   - Полный доступ.
   - Нет доступа.

Теперь предположим, что нам нужно подключить сетевой ресурс. Пусть на компьютере COMP5 есть общий ресурс D. Его сетевое имя будет \\COMP5\HACKER (D). Для подключения этого ресурса выполните следующие действия:

1. Щелкните правой кнопкой мыши по пиктограмме **Мой компьютер** и выберите команду **Подключить сетевой диск**.
2. В открывшемся окне (рис. 8.17) выберите имя диска (E:), а также укажите имя сетевого ресурса. Если вы не помните имя, в области **Общие каталоги** вы можете выбрать нужный вам компьютер и его общий ресурс.
3. Нажмите кнопку Ok. Теперь вы можете работать с общим ресурсом как с обыкновенным локальным диском E.

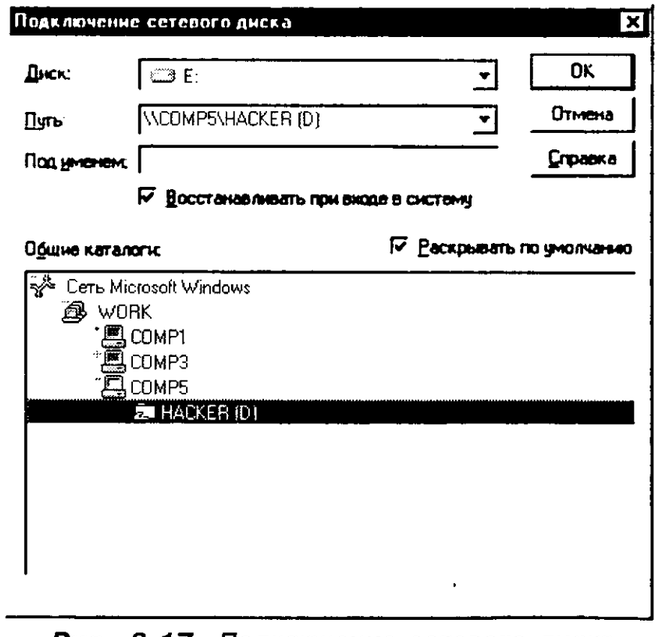


Рис. 8.17. *Подключение сетевого диска*

Предоставление общего доступа из Windows XP

В Windows XP предоставление доступа еще проще. Выберите ресурс, щелкнув по нему правой кнопкой мыши, затем выберите команду **Свойства**. В появившемся окне (рис. 8.18) отметьте всего два режима:

- **Открыть общий доступ к этой папке** — по умолчанию открывается в режиме только чтение.
- **Разрешить изменение файлов по сети** — а это полный доступ.

При попытке открыть общий доступ к целому диску, то есть к корневому каталогу, вы получите соответствующее предупреждение, которое, однако, не запрещает вам сделать задуманное. Из соображений безопасности не нужно предоставлять полный доступ к целому диску, особенно, если на этом диске установлена операционная система или программное обеспечение.

Подключение сетевого диска аналогично его подключению в других операционных системах от Microsoft. Для этого щелкните правой кнопкой по пиктограмме **Мой компьютер** и выберите команду **Подключить сетевой диск** (рис. 8.19). Если вы забыли имя сетевого ресурса, нажмите кнопку **Обзор** и выберите нужный вам ресурс (рис. 8.20).

Подключить сетевой диск можно по-другому. Находясь в папке **Сетевое окружение**, выберите команду меню **Сервис → Подключить сетевой диск**.

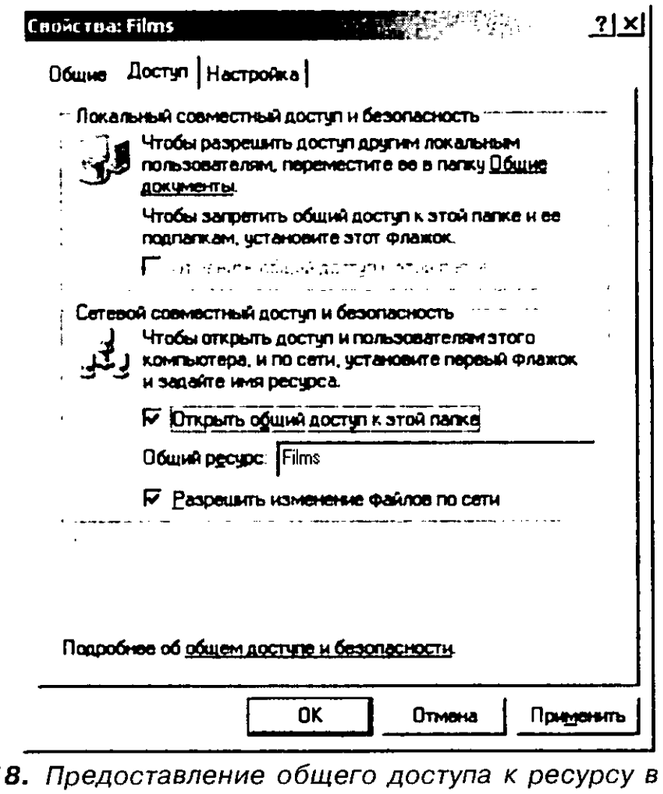


Рис. 8.18. *Предоставление общего доступа к ресурсу в Windows XP*

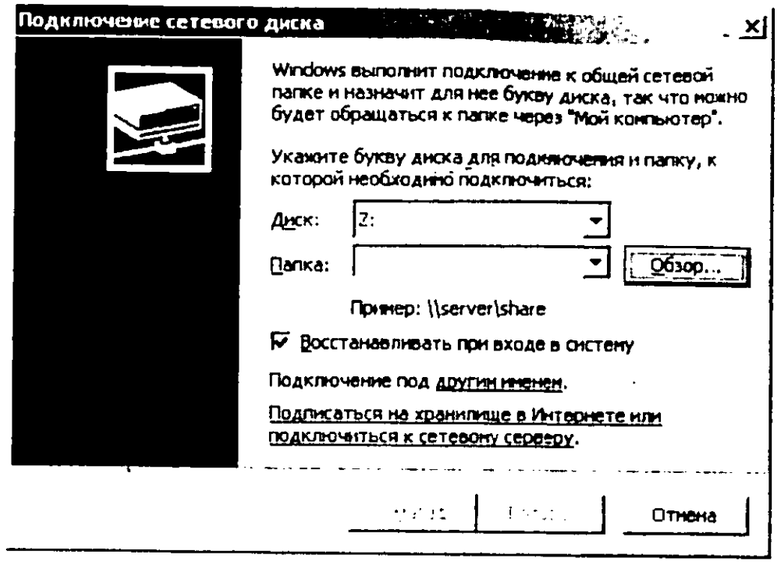


Рис. 8.19. *Подключение сетевого диска*

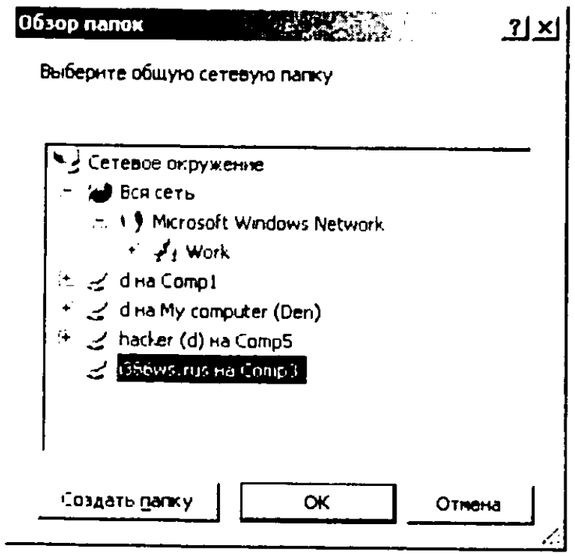


Рис. 8.20. *Обзор сети*

8.4. Просмотр общих ресурсов сети

Просмотр ресурсов сети — компьютеров, общих каталогов, дисков, принтеров — осуществляется с помощью системной папки Сетевое окружение, которая обычно расположена на рабочем столе Windows. Внешний вид этой папки зависит от настроек компьютера и от версии операционной системы.

В Windows 9x, Windows NT, Windows 2000 по умолчанию отображаются компьютеры рабочей группы. Чтобы просмотреть общие ресурсы того или

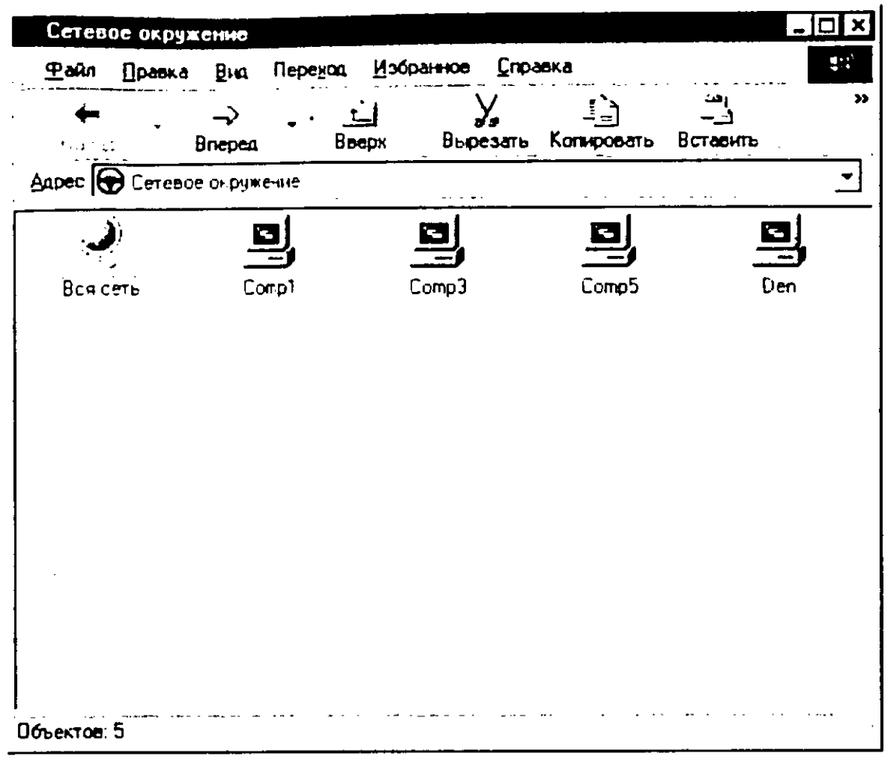


Рис. 8.21. *Сетевое окружение в Windows 98*

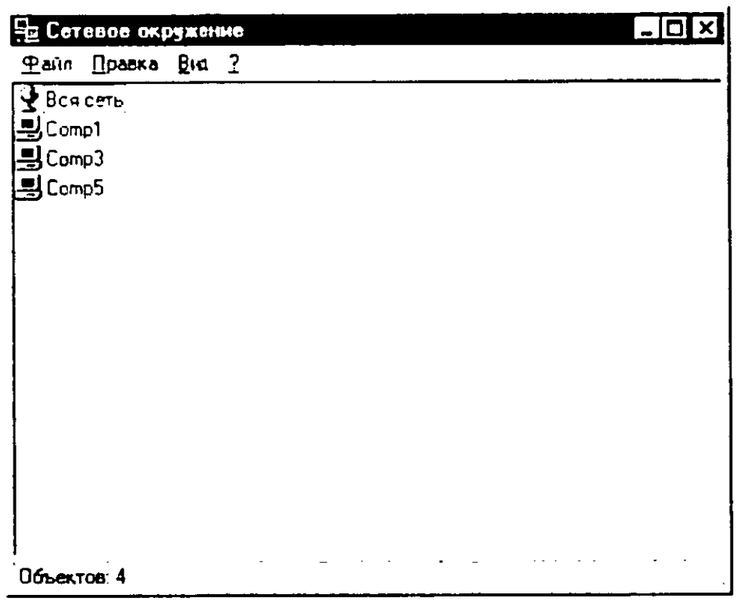


Рис. 8.22. *Сетевое окружение в Windows NT*

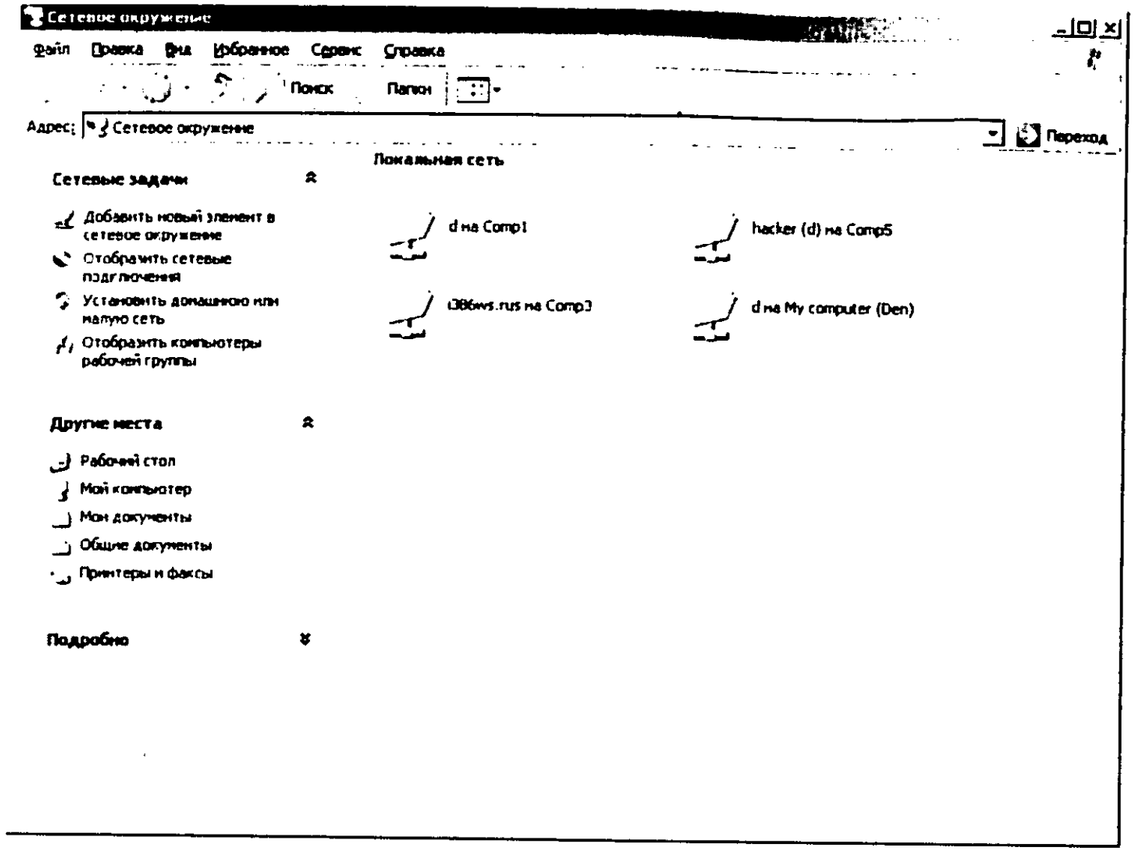


Рис. 8.23. *Сетевое окружение в Windows XP*

иного компьютера, дважды щелкните на пиктограмме этого компьютера. Если вам нужно просмотреть компьютеры другой рабочей группы, дважды щелкните на пиктограмме **Вся сеть**, затем выберите нужную вам рабочую группу (в некоторых системах может быть промежуточный выбор — **Сеть Microsoft**, а только затем — выбор рабочей группы).

В Windows XP по умолчанию отображаются не компьютеры, а общие ресурсы. Чтобы просмотреть компьютеры рабочей группы, выберите команду **Отобразить компьютеры рабочей группы** в области **Сетевые задачи**. В области **Другие места** выберите **Microsoft Windows Network**, чтобы просмотреть другие рабочие группы вашей сети.

Чтобы подключить сетевой диск, находясь в папке **Сетевое окружение**, щелкните по сетевому ресурсу правой кнопкой мыши и выберите команду **Подключить сетевой диск**. Появится окно подключения сетевого диска, в котором поле **Путь** уже будет заполнено — вам останется выбрать только имя сетевого диска.

8.5. Сетевая печать. Настройка сетевого принтера

До этого мы рассматривали только общий доступ к файлам. Но Windows может также предоставлять общий доступ к принтерам, подключенным к компьютеру. В Windows 9x/ME для предоставления доступа к принтерам, убедитесь, что включена опция **Принтеры этого компьютера можно сделать общими** в окне **Доступ к файлам и принтерам** (см. рис. 8.3).

Для предоставления принтера в общее пользование нужно перейти в папку **Принтеры** (в Windows XP она называется **Принтеры и факсы**). Сделать это можно, выбрав **Пуск → Настройка → Принтеры**. Щелкните по нужному вам принтеру правой кнопкой мыши и выберите команду **Доступ** (рис. 8.24).

В открывшемся окне вам нужно только включить режим **Общий ресурс** — все остальные параметры можно не изменять. Если нужно, можете указать пароль для доступа к принтеру.

Для подключения сетевого принтера запустите мастер установки принтера. На запрос мастера о типе принтера выберите **Сетевой принтер**. На рис. 8.25 показан Мастер установки принтера в Windows XP, а на рис. 8.26 — Мастер установки принтера в Windows 98.

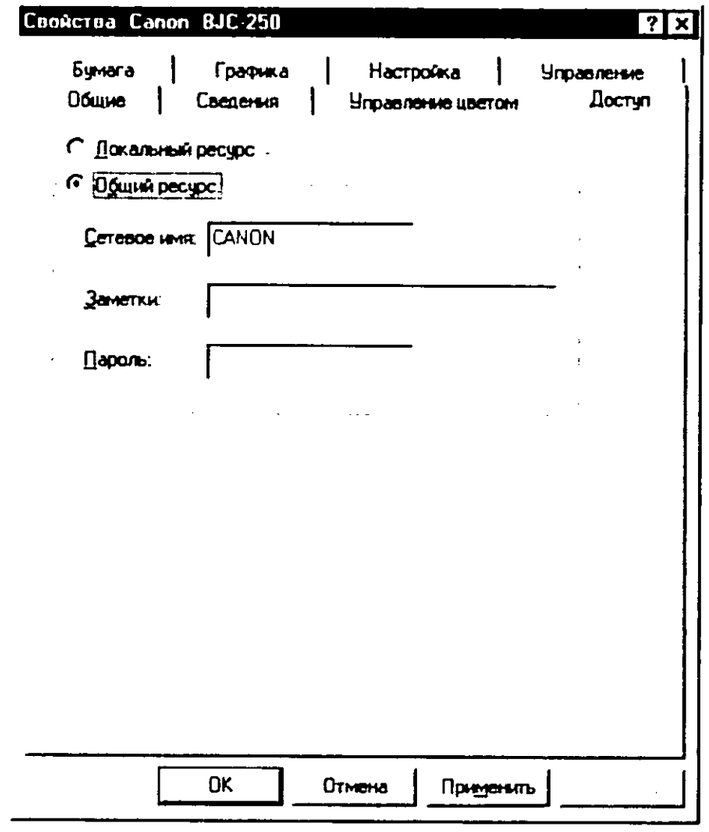


Рис. 8.24. *Предоставление общего доступа к принтеру*

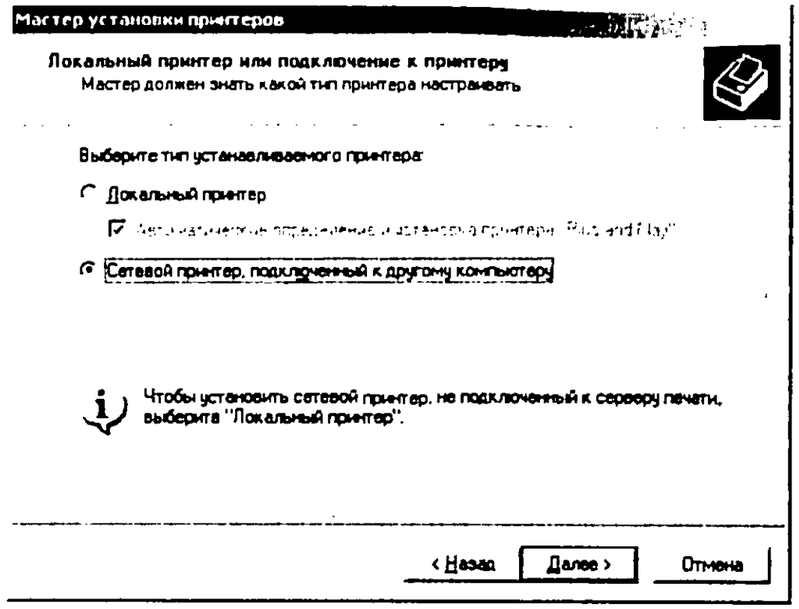


Рис. 8.25. *Мастер установки принтера в Windows XP*

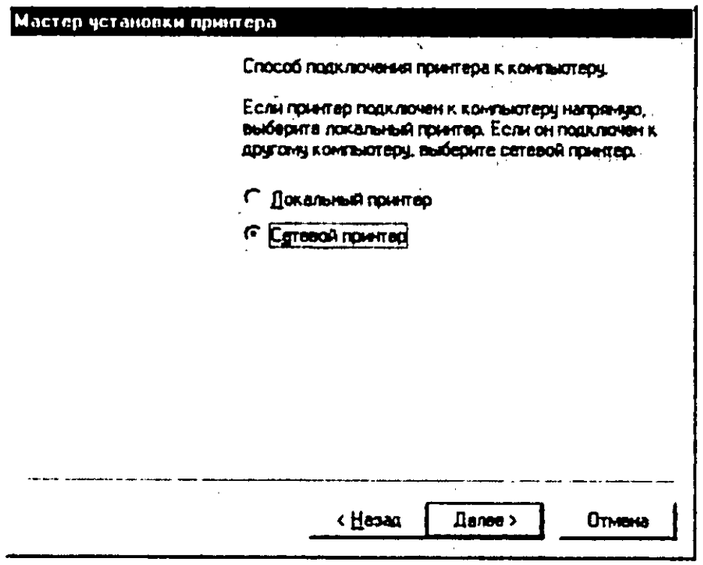


Рис. 8.26. *Мастер установки принтера в Windows 98*

Если вы точно помните имя принтера, например, `\\computer\printer`, можно сразу его ввести (рис. 8.27). В том случае, если вы не помните имя, выберите опцию **Обзор** (рис. 8.28).

В появившемся окне выберите нужный вам принтер, нажмите кнопку **Далее** — ну а дальше дело техники. Вам разве что придется указать драйвер принтера, а если такого драйвера не будет в базе данных драйверов операционной системы, нужно будет вставить диск с драйвером.

Впоследствии, для использования сетевого принтера при распечатке документов в диалоге печати выбирайте сетевой принтер (рис. 8.29).

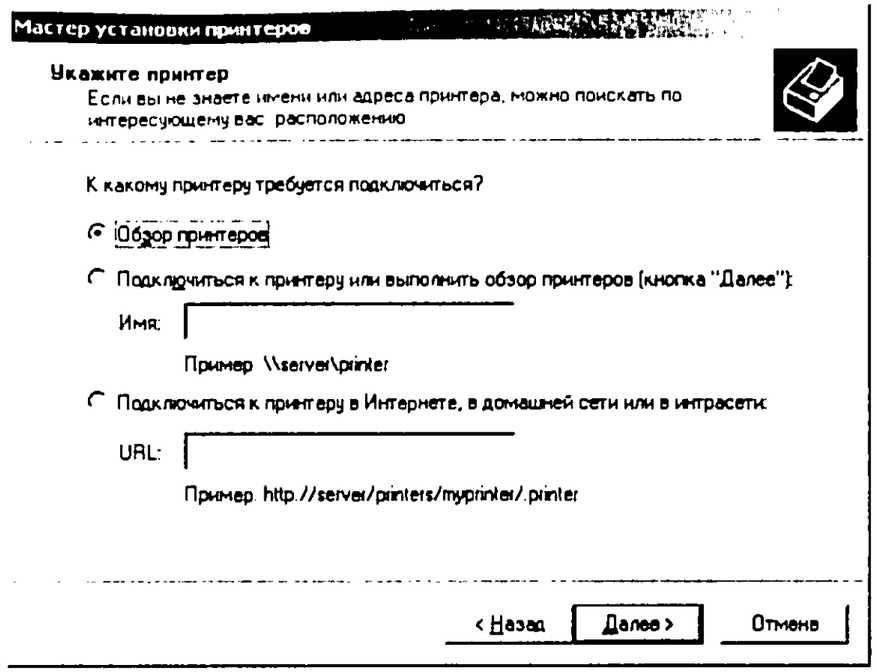


Рис. 8.27. *Ввод имени принтера*

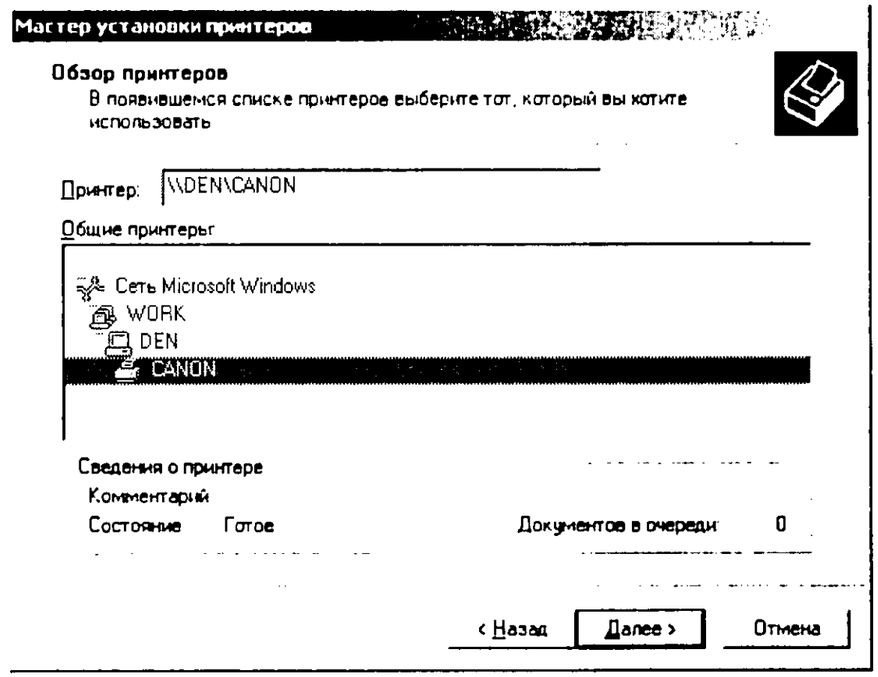


Рис. 8.28. *Обзор сети*

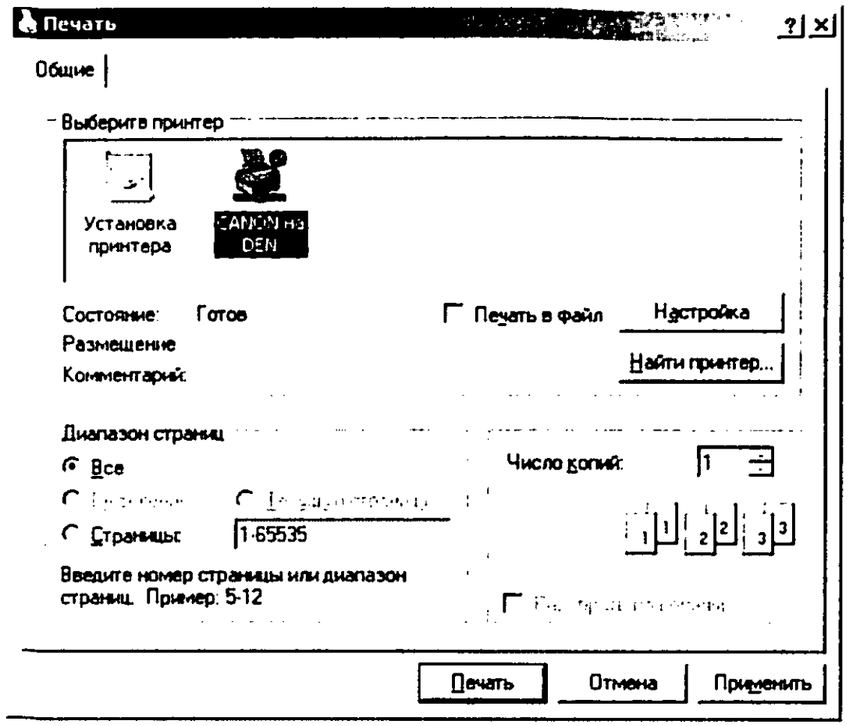


Рис. 8.29. *Диалог печати*

Часть IV

НАСТРОЙКА СЕРВЕРА СЕТИ. ИЕРАРХИЧЕСКАЯ СЕТЬ

Одноранговые сети более просты, как в настройке, так и в эксплуатации, однако использование данных сетей недопустимо с точки зрения безопасности в средних и больших компаниях. Почему, вы, наверное, догадываетесь. Если в небольшой сети, где работают только «свои», можно вообще отказаться от паролей для доступа к ресурсам, то в большой сети это недопустимо.

Даже если не отказываться от паролей, в небольшой сети их будет немного, например, один пароль для записи на сетевой диск, выбранный для централизованного хранения документов, другой — для доступа к Интернету, третий — для печати на сетевом принтере.

В большой сети сетевых ресурсов намного больше — 20, 50, 100. Попробуйте запомнить пароль для доступа к каждому ресурсу. Тем более, что пароли одинаковые и их знают все сотрудники. Попробуйте потом определить, кто из них стер квартальный отчет???? Когда доступ к ресурсу производится с аутентификацией по имени и паролю, как в сети клиент/сервер, то тогда можно однозначно определить, кто и когда получил доступ к тому или иному сетевому ресурсу.

Кроме того, сети клиент/сервер позволяют организовать централизованное управление сетью, что также немаловажно.

Глава 9

Система DNS

9.1. Как работает DNS?

Принцип работы

Думаю, что не нужно в очередной раз рассказывать о преобразовании IP-адреса в имена компьютеров и том, что выполняет служба DNS. Данному вопросу посвящены целые тома. Мы же давайте займемся непосредственно настройкой сервера DNS, который будет работать под управлением рассматриваемых в книге операционных систем — Linux, Windows NT Server 4.0, Windows 2000 Server и Windows 2003 Server.

Перед началом настройки сервера DNS разберемся, как он работает. Некоторую информацию вы уже знаете, но, как говорится, повторение — мать учения (или заикания). Система имен DNS — это иерархическая древообразная система. В этом дереве существует корень — он обозначается «.» (root). Список корневых серверов должен быть у каждого сервера: он содержится в файле `named.ca`. Этот файл может называется и по-другому — в зависимости от настроек сервера. Существует определенное количество доменов верхнего уровня. Наиболее известные вы знаете: com, gov, net, org и другие (в том числе и домены стран — ru, ua, fr и др).

Допустим, что пользователь вводит в окне браузера адрес **http://server**. Однако адресация в локальной сети (так же как и в Интернет) построена на основе IP-протокола. Поэтому для того, чтобы установить соединение с компьютером `server` компьютеру пользователя необходимо знать его IP-адрес, поэтому операционная система пользователя пытается разрешить (перевести) имя компьютера в IP-адрес. С этой целью она сначала использует свои стандартные средства (тот же файл `hosts`), а потом обращается к службе DNS.

Примечание.

Если быть предельно точным, то к DNS-серверу обращается не сама операционная система, а ее модуль, который называется DNS-клиентом или ресолвером. DNS-клиент может быть встроен в приложение, но чаще всего — это библиотечная программа.

Рассмотрим теперь интернет-адрес www.yahoo.com (на самом деле абсолютно неважно это интернет-адрес или адрес в локальной сети — все то же самое). Сервер DNS сначала пытается разрешить имя данного компьютера, используя свой собственный кэш имен. Если требуемое имя компьютера в нем отсутствует, то сервер DNS обращается к одному из корневых серверов DNS, о которых мы поговорим позже.

Запрос обрабатывается рекурсивно: корневой сервер обращается к серверу, который отвечает за домен com, а тот, в свою очередь, к серверу DNS домена yahoo.com. Сервер DNS домена yahoo.com возвращает IP-адрес компьютера www — 64.58.76.222 или все адреса, которые сопоставлены этому имени (многие сетевые операционные системы, в том числе и Linux, позволяют одному имени сопоставлять несколько IP-адресов).

Примечание.

На самом деле, если выполнить разрешение имени www.yahoo.com, сервер DNS возвратит следующие адреса:
64.58.76.222
64.58.76.228
64.58.76.223
64.58.76.176
64.58.76.224
64.58.76.177
64.58.76.227
64.58.76.179

А официальное имя компьютера `www.yahoo.com` (это его каноническое имя — о канонических именах и как их использовать будет сказано ниже) — `www.yahoo.akadns.net`

Иерархическая структура системы DNS

Как уже было отмечено, существует домен корневого уровня, который обозначается «.». Следующий уровень иерархии — это домены верхнего уровня. Вся структура службы DNS является иерархической. Существуют домены первого, второго, третьего, n-го уровней. Рассмотрим доменное имя компьютера `www.department.firma.isp.ru`. Здесь доменом первого уровня является `ru`, `isp` — второго, `firma` — третьего, а `department` — четвертого уровня. Иерархическая структура системы DNS уже рассматривалась в пятой главе этой книги, поэтому сейчас подробно останавливаться на ней не будем.

Полное доменное имя

Полным доменным именем узла называется его имя, дополненное справа именем домена. Например, если наш узел называется server и принадлежит домену `firma.com`, то его полным доменным именем будет имя `server.firma.com`.

Зоны ответственности

При настройке сервера DNS мы будем говорить о так называемых зонах. Не стоит путать зону с доменом. Зона ответственности (или просто зона) — это определенная часть пространства имен, за которое отвечает сервер DNS. В одной зоне может быть несколько доменов, а один сервер DNS может обслуживать несколько зон. Каждая зона подчинена определенному домену, который называется корневым доменом зоны.

Пусть у нас есть домен `firma.com`. Кроме этого домена на предприятии есть два отделения, которым принадлежат свои собственные домена — `dep1` и `dep2`. Наш сервер DNS обслуживает как домен `firma.com`, так и его поддомены — `dep1.firma.com` и `dep2.firma.com`. Все эти три домена составляют зону ответственности сервера DNS. Домен firma.com будет корневым доменом зоны. Обычно имя зоны совпадает с именем корневого домена.

Типы серверов DNS

Существует три основных типа серверов DNS, которые отличаются возложенными на них задачами:

- основной сервер DNS;
- резервный (вторичный) сервер DNS;
- кэширующий сервер DNS.

Основной сервер DNS управляет зоной полномочий. Если нужно добавить/удалить домен или узел или как-то иначе модифицировать зону, изменения нужно производить на основном сервере DNS. Через определенное время, которое зависит от настроек сервера, основной сервер передаст зону резервному серверу DNS. Данное явление называется трансфером зоны.

Что же касается резервных серверов, то должен быть хотя бы один резервный сервер DNS. Тому есть несколько причин:

- если клиентов много, то наличие резервного сервера DNS позволит снизить нагрузку на основной сервер DNS и ускорить доступ физически отдаленных от основного сервера клиентов к базе данных доменных имен;
- надежность — вдруг что-то случится с основным сервером DNS — не будут же клиенты ждать, пока вы устраните ошибку. А что делать, если вы уехали в отпуск? Сеть не будет работать?

Абсолютно все DNS-серверы кэшируют запросы, полученные от клиентов — так повторный запрос будет выполнен быстрее. Существует особый вид сервера DNS — кэширующий сервер. Серверы данного типа не отвечают за зоны, а только перенаправляют запросы клиентов, получают ответы, кэшируют их и отправляют клиентам.

Существует три типа запросов:

- рекурсивный;
- итеративный;
- обратный (инверсный).

Вернемся к нашему примеру, когда нужно разрешить имя `www.yahoo.com`. Клиент посылает серверу *рекурсивный* запрос. Сервер просматривает свое пространство имен и не находит имени `www.yahoo.com`. Тогда он посылает вышестоящему серверу итеративный запрос, который и устанавливает IP-адрес имени `www.yahoo.com`.

Обратный запрос — это запрос преобразования IP-адреса в доменное имя. Для разрешения таких запросов был создан специальный домен `in-addr.arpa`. Имена узлов в этом домене совпадают с их IP-адресами, указанными в обратном порядке. Если IP-адрес узла 192.168.1.1, то в домене `in-addr.arpa` ему будет соответствовать имя `1.1.168.192.in-addr.arpa`.

9.2. Сервер DNS под управлением Linux

9.2.1. Настройка сервера DNS

Установка DNS-сервера BIND

Учитывая, что на обращение к серверу DNS провайдера требуется 10...15, а иногда и все 30 секунд (это зависит от загрузки сети и от скорости соединения), установка сервера DNS в локальной сети с выходом в Интернет является просто необходимой. Обычно сервер DNS устанавливается на шлюзе, который используется для выхода в Интернет. Прежде чем приступить к настройке сервера, нужно определить, запущен ли он:

```
ps -ax | grep named
```

Если сервер DNS запущен, то его нужно остановить (командой **kill** или **ndc**), а если он вообще не установлен, то вам придется установить пакеты **bind** и **bind-utils**.

Примечание.

Для установки девятой версии BIND требуются:
- ядро 2.4 или выше;
- библиотека OpenSLL.

Обратите внимание, что исполнимый файл называется `named`, а сам пакет — **bind**. BIND (Berkley Internet Nameserver Deamon) — это наиболее известный и используемый DNS-сервер, настраиваемый в Linux. Для работы сервера должен быть активизирован сервис **network**. Я надеюсь, вы не забыли, как это сделать?

Практическая настройка DNS-сервера

Теперь приступим к непосредственной настройке сервера и рассмотрим ее на примере. Для этого обратимся к файлу `/etc/named.conf`, в котором содержится основная информация о параметрах сервера (см. листинг 9.1).

Листинг 9.1. Файл named.conf

```
logging {
    category cname {null; };
    };

options {
    directory «/var/named»;
    };

zone «.» {
    type hint;
    file «named.ca»;
    };

zone «dhsilabs.com» {
    type master;
    file «dhsilabs.com»;
    notify no;
    };

zone «0.0.127.in-addr.arpa» {
    type master;
    file «named.local»;
    };

zone «1.168.192.in-addr.arpa» {
    type master;
    file «192.168.1»;
    notify yes;
    };
```

Основной рабочий каталог сервера — /var/named. Указанные без начального обратного слэша имена файлов будут искаться относительно этого каталога. То есть именно в нем сервер будет искать файлы dhsilabs.com, named.local, 192.168.1, named.ca (см. листинги 9.1, 9.3, 9.4) . Обслуживаемая сервером зона (домен) — dhsilabs.com.

Давайте рассмотрим поподробнее листинг 10.1. Сначала в нем были определены опции протоколирования — блок **logging**. Затем идет задание параметров самого сервера — блок **options**. Параметр **directory** определяет корневой каталог сервера — /var/named. Помимо параметра **directory** в блоке **options** могут задаваться и другие параметры (такие как **forwarders**, **forward** и др.), о которых сказано будет несколько позже (см. п. 9.3). Для функционирования сервера достаточно и одного параметра **directory**.

После блока параметров должны быть перечислены зоны, обслуживаемые сервером. Мы будем обслуживать зону (домен) dhsilabs.com. Информация об этой зоне хранится в файле /var/named/dhsilabs.com. Позже мы займемся созданием этого файла. С помощью этого файла наш сервер будет преобразовывать имена компьютеров в IP-адреса. Для обратного преобразования служит файл /var/named/192.168.1.

Зоны «.» и «0.0.127.in-addr.arpa» — особые. Я не буду их подробно описывать: их назначение вы поймете из дальнейшего текста книги. Файл named.local — это файл обратного соответствия, предназначенный для преобразования IP-адресов в имена, то есть, в частности, он используется для преобразования адреса 127.0.0.1 в имя localhost.

Файл named.ca — это файл, в котором перечислен начальный набор корневых DNS-серверов. Он содержит информацию о корневых серверах DNS. При разрешении имени в IP-адрес или наоборот полученная информация кэшируется и остается в памяти сервера определенное время. В свой работе, если нужно разрешить имя в IP-адрес (или наоборот), ваш DNS-сервер сначала будет искать необходимую ему информацию в кэше. Если ее там не окажется, то сервер обратится к одному из корневых серверов DNS, IP-адреса которых находятся в файле named.ca.

Файл named.ca необходимо регулярно обновлять, чтобы он всегда содержал свежие данные (первый раз его нужно обновить сразу же после установки сервера, несмотря на то, что этот файл будет только что создан). Немного позже я отдельно опишу его обновление.

Файл dhsilabs.com непосредственно служит для преобразования имен в IP-адреса (см. листинг 9.2).

Листинг 9.2. Файл dhsilabs.com

```
@     IN  SOA den.dhsilabs.com. hostmaster.dhsilabs.com. (
          93011120    ; серийный номер
          10800       ; обновление каждые 3 часа
          3600        ; повтор каждый час
          3600000     ; хранить информацию 1000 часов
          86400)      ; TTL записи - 24 часа
      IN  NS  den.dhsilabs.com.
      IN  A   192.168.1.1
      IN  MX  150 den.dhsilabs.com.

den   IN  A       192.168.1.1
      IN  HINFO   INTEL CELERON (LINUX)
      IN  MX  100 den
      IN  MX  150 evg.dhsilabs.com.
ns    IN  CNAME   den.dhsilabs.com.
www   IN  CNAME   den.dhsilabs.com.
ftp   IN  CNAME   den.dhsilabs.com.
mail  IN  CNAME   den.dhsilabs.com.

evg   IN  A       192.168.1.2
      IN  MX  100 den.dhsilabs.com.

localhost     IN  A       127.0.0.1
```

Попробую объяснить все как можно быстрее и проще. Свое объяснение оформлю в виде табл. 9.1.

Записи DNS *Таблица 9.1*

Запись	Описание
NS	Обозначает сервер имен (name server)
A	Задает IP-адрес, соответствующий имени компьютера
PTR	Задает имя компьютера, соответствующее IP-адресу
MX число	Определяет почтовик, который будет обслуживать наш домен. Числовой параметр возле записи MX является приоритетом данного почтового сервера. Чем меньше число, тем выше приоритет
CNAME	Определяет каноническое имя узла, то есть если вы в окне браузера введете http://www.dhsilabs.com, то обращение будет произведено к den.dhsilabs.com
HINFO	Сведения об аппаратном обеспечении. Рекомендую не заполнять эту запись или использовать заведомо неправильные данные. Чем меньше информации имеет о вашей сети злоумышленник, тем сложнее ему будет атаковать ее
TXT	Прочие сведения. Содержит произвольный текст

Обратите внимание на точку в конце:

```
@    IN  SOA den.dhsilabs.com. hostmaster.dhsilabs.com. (
```

Если точка не указана, то к имени будет добавлено имя домена (то есть dhsilabs.com).

Листинг 9.3. Файл named.local

```
@    IN  SOA dhsilabs.com. root. dhsilabs.com. (
           199609203    ;серийный номер
           28800        ;обновление каждые 8 часов
           7200      ;повтор каждые 2 часа
           604800    ;хранить информацию 168 часов (1 неделю)
           86400)       ;TTL записи - 24 часа
         NS  dhsilabs.com.
1        PTR localhost.
```

Файл 192.168.1 или файл обратного соответствия представлен в листинге 9.4.

Листинг 9.4. Файл обратного соответствия (192.168.1)

```
 @    IN  SOA den.dhsilabs.com. hostmaster.dhsilabs.com. (
           93011120      ; серийный номер
           10800         ; обновление каждые 3 часа
           3600          ; повтор каждый час
           3600000       ; хранить информацию 1000 часов
           86400 )       ; TTL записи - 24 часа
 @    IN  NS  den.dhsilabs.com
 1    IN  PTR den.dhsilabs.com
 2.1.168.192  IN  PTR evg.dhsilabs.com
```

Запись PTR используется для преобразования IP-адреса в имя.

Если указан не весь IP, например:

```
 1    IN  PTR den.dhsilabs.com
```

то к нему будет добавлен адрес подсети 1.168.192. Внимание! IP-адреса указываются в обратном порядке!

Для установки файла корневого кэша следует установить пакет **caching-nameserver**, но я рекомендую получить и установить самую новую версию. Для этого подключитесь к Интернет, запустите сервер DNS, а затем выполните команду

```
 # nslookup | tee ns
```


В ответ на приглашение программы **nslookup** введите две команды

```
 > set q=ns (или set type=ns)
 > .
```

На экране вы увидите список корневых серверов DNS, который будет помещен в файл `ns`. Для преобразования файла `ns` в формат `named.ca` воспользуйтесь следующей программкой на **awk** (см. листинг 9.5).

Листинг 9.5. Сценарий reformat

```
#!/bin/awk
awk ' BEGIN {
/root/ { print «. IN NS « $4».» }
/internet/ { print $1".» « 999999 IN A « $5 }
END '
```

Использовать ее нужно как **reformat <source file> <output file>**, то есть:

```
reformat ns named.ca
```

Теперь осталось скопировать `named.ca` в каталог `/var/named` и на этом — все.

А теперь покажу, как то же самое можно было сделать проще. Для этого следует воспользоваться программой **dig**, выполнив команду:

```
dig @a.root-servers.net . ns > named.ca
```

или

```
dig @198.41.0.4 . ns > named.ca
```

После этого остается просто заменить старый файл `named.ca` новым файлом `named.ca.new`. Как видите, второй способ намного проще, но и первый знать не помешает.

Обычно файл `named.ca` содержит примерно такую информацию:

```
.     6D IN NS        G.ROOT-SERVERS.NET.
.     6D IN NS        J.ROOT-SERVERS.NET.
.     6D IN NS        K.ROOT-SERVERS.NET.
.     6D IN NS        L.ROOT-SERVERS.NET.
.     6D IN NS        M.ROOT-SERVERS.NET.
.     6D IN NS        A.ROOT-SERVERS.NET.
.     6D IN NS        H.ROOT-SERVERS.NET.
.     6D IN NS        B.ROOT-SERVERS.NET.
.     6D IN NS        C.ROOT-SERVERS.NET.
```

```
.       6D IN NS        D.ROOT-SERVERS.NET.
.       6D IN NS        E.ROOT-SERVERS.NET.
.       6D IN NS        I.ROOT-SERVERS.NET.
.       6D IN NS        F.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
G.ROOT-SERVERS.NET.     5w6d16h IN A    192.112.36.4
J.ROOT-SERVERS.NET.     5w6d16h IN A    198.41.0.10
K.ROOT-SERVERS.NET.     5w6d16h IN A    193.0.14.129
L.ROOT-SERVERS.NET.     5w6d16h IN A    198.32.64.12
M.ROOT-SERVERS.NET.     5w6d16h IN A    202.12.27.33
A.ROOT-SERVERS.NET.     5w6d16h IN A    198.41.0.4
H.ROOT-SERVERS.NET.     5w6d16h IN A    128.63.2.53
B.ROOT-SERVERS.NET.     5w6d16h IN A    128.9.0.107
C.ROOT-SERVERS.NET.     5w6d16h IN A    192.33.4.12
D.ROOT-SERVERS.NET.     5w6d16h IN A    128.8.10.90
E.ROOT-SERVERS.NET.     5w6d16h IN A    192.203.230.10
I.ROOT-SERVERS.NET.     5w6d16h IN A    192.36.148.17
F.ROOT-SERVERS.NET.     5w6d16h IN A    192.5.5.241
```

Если вы настраиваете сервер DNS только для своей внутренней сети (intranet), которая не имеет выхода в Интернет, не спешите обновлять файл кэша! Он вам вообще не нужен. Вы также должны удалить зону, описывающую корневой кэш в файле `named.conf`.

Теперь остается сделать пару завершающих штрихов. Отредактируйте файл `/etc/resolv.conf` таким образом: с помощью директивы **search** укажите домены для поиска, а в качестве сервера по умолчанию — 127.0.0.1. Можно также указать и адрес реального интерфейса:

```
search subdomain.domain.com domain.com
nameserver 127.0.0.1
```

Как вы уже догадались, сервером DNS по умолчанию является первый сервер из списка **nameserver**. Напомню, что в списке может быть не более четырех серверов. Список доменов используется для поиска компьютера в том случае, если указано только имя узла без домена.

Например, если вы введете в окне броузера `http://host`, сначала будет выполнена попытка обращения к узлу `host.subdomain.domain.com`, а потом, если узел не будет найден, к узлу host.domain.com. Если и этот узел не будет найден, вы получите соответствующее сообщение. И еще: проверьте порядок разрешения имен в файле `/etc/hosts.conf`. Порядок должен быть задан так: **order hosts,bind**. Несмотря на то, что сейчас мы используем DNS, лучше сначала все же искать в файле `hosts`.

9.2.2. Кэширующий сервер DNS

Настройка кэширования на DNS-сервере

Кэширующий сервер, как правило, не обслуживает домен, а используется для повышения скорости работы соединения. Для настройки кэширующего сервера используется параметр **forwarders**, задаваемый в файле `named.conf` (в блоке **options**).

Рассмотрим пример: допустим, ваш сервер для разрешения какого-нибудь имени пытается добраться до одного из корневых серверов. А если у вас коммутируемое соединение да и модем на 14400? Сейчас выглядит смешно, но иногда бывают и такие ситуации, например, в моей системе спокойно уживаются два модема — один 56K V.90, а второй именно на 14K. В любом случае, если у вас нет собственного домена, а сервер DNS запущен на вашей машине, которую вы используете в гордом одиночестве, то с помощью вышеупомянутой директивы можно существенно повысить скорость соединения.

Способ очень прост: можно заставить провайдера проделать за вас всю «грязную» работу. В обычной ситуации в процессе разрешения какого-нибудь имени ваш сервер будет последовательно запрашивать несколько удаленных корневых DNS-серверов, с каждым из которых надо установить соединение, отправить запрос и получить ответ.

Создание у себя кэширующего DNS-сервера позволит возложить всю эту работу на DNS-сервер провайдера. При этом ваш DNS-сервер будет отсылать в сеть только один запрос на разрешение имени (DNS-серверу провайдера) и получать только один окончательный ответ. Это особенно полезно, если у вас плохое соединение с Интернет.

Для того, чтобы насладиться такой возможностью, следует в файл `named.conf` добавить следующие параметры (в блоке **options**):

```
forward first;
forwarders {
 192.168.99.1;
 192.168.99.2;
    };
```

Здесь я рассматриваю конкретный пример, вы же у себя замените адреса 192.168.99.1 и 192.168.99.2 на адреса DNS-серверов вашего провайдера. Параметр **forwarders** задает заключенный в фигурные скобки список IP-адресов, соответствующих DNS-серверам, которым ваш DNS-сервер будет переадресовывать запросы вместо того, чтобы отвечать на них самому. IP-адреса перечисляются через точку с запятой.

Параметр **forward** может принимать одно из двух следующих значений:

- **only** — ваш DNS-сервер никогда не должен предпринимать попыток обработать запрос самостоятельно;
- **first** — ваш DNS-сервер должен пытаться сам обработать запрос, если указанные далее параметром **forwarders** сервера DNS не были найдены.

Использование параметра **forward** бессмысленно без использования параметра **forwarders**.

Таким образом, вернемся к настройке сервера, весь файл `named.conf` примет следующий вид, приведенный в листинге 9.6.

Листинг 9.6. Файл named.conf кэширующего сервера DNS

```
options {
     directory «/var/named»;
     forward first;
     forwarders {
         192.168.99.1;
         192.168.99.2;
     };
     // Раскомментируйте следующую строку, если вы
     // работаете через firewall и система не работает
     // query-source port 53;
};

zone «.» {
     type hint;
     file «named.ca»;
     };

zone «0.0.127.in-addr.arpa» {
     type slave;
     file « named.local «;
     };
```

Обратите внимание, что в примере уже не поддерживается зона `dhsilabs.com`.

Возможные проблемы и их решения

Как правило, кэширующий сервер используется на отдельной машине, которая подключается к Интернет по коммутируемому соединению. Нужно учитывать, что сервер DNS сразу требует обращения к какому-нибудь сетевому ресурсу. В нашем же случае, если соединение не установлено, то устройство `ppp0` существовать не будет, а `named` будет страшно ругаться на то, что сеть недоступна. При этом недоступным окажется даже интерфейс **lo**, а программа **nslookup**, если она нам понадобится без существования сети, просто «подвиснет», ожидая ответа от сервера DNS.

Есть два способа решить данную проблему. Какой использовать — это решать вам. Первый заключается в том, что при установлении соединения сценарий **ppp-on**, будет запускать программу **ndc** с параметром **start** (см. ниже), а сценарий **ppp-off** будет останавливать сервер DNS командой **ndc stop**.

Второй способ основывается тоже на использовании сценариев **ppp-on и ppp-off**, но в этом случае сервер DNS всегда будет запущен. Принцип работы заключается в подмене файла корневого кэша `named.ca`. Сервер DNS содержит пустой файл корневого кэша, и при установке соединения сценарий **ppp-on** скопирует вместо пустого файла нормальный файл кэша. Сценарий **ppp-off** при разрыве соединения перезапишет нормальный файл `named.ca` пустым файлом с таким же именем. При использовании этого способа в ваших протоколах (журналах) будут регулярно появляться сообщения примерно такого содержания:

```
Jan 5 16:10:11 den named[10147]: No root nameserver for
class IN
```

Для полноты картины хочу отметить, что если вы используете NFS, и у вас возникают проблемы с монтированием удаленных файловых систем, запускайте сервер **named** после запуска **nfsd** и **mountd**.

9.2.3. Настройка дополнительного (вторичного) сервера DNS

Вы когда-нибудь обращали внимание, что у любого уважающего себя провайдера есть два сервера DNS — первичный (primary или master) и вторичный (secondary или slave)? Так вот, сейчас и мы займемся настройкой вторичного сервера DNS.

Примечание.

Практически у каждого провайдера работают два сервера DNS. Наличие двух серверов обеспечивает, если можно так выразиться, избыточность разрешения имени. Например, с первичным сервером что-нибудь случилось, произошел сбой, что бывает очень редко, или же просто первичный сервер не в

состоянии обработать большое количество запросов клиентов. Тогда система разрешения имен операционной системы, получив отказ от первичного сервера DNS, обращается к вторичному.

Например, вам нужно создать вторичный сервер, который будет обслуживать домен `domain.com`. С этой целью внесите следующие изменения в файл `named.conf` дополнительного сервера:

```
zone «domain.com» {
     type slave;
     file «domain.com»;
     masters { 192.168.1.1; 192.168.1.2; };
     };
```

IP-адреса основных серверов DNS вашей сети указываются внутри подсекции **master** через точку с запятой. Вторичный сервер, в отличие от кэширующего, всегда должен иметь тип **slave**.

9.2.4. Команды управления сервером DNS

Для управления сервером DNS используется программа **ndc**. Ее можно использовать с параметрами **start**, **stop**, **reload**, **restart**:

- Параметр **start** — запускает сервер.
- Параметр **stop** — останавливает сервер.
- Параметр **reload** — перезагружает файлы зоны, если в них произошли изменения.
- Параметр **restart** — перезапускает сервер DNS.

9.2.5. Просмотр DNS-зоны. Использование nslookup

Программа **nslookup** используется для просмотра зоны DNS и входит в состав Linux (и всех вариантов UNIX), а также Windows NT.

В данном случае зону следует понимать как домен и читать «для просмотра домена». В зоне содержится различная информация о компьютерах в домене. Зоны бывают разные: одни содержат информацию о компьютерах в домене и служат для преобразования имени компьютера в IP-адрес и наоборот (см. листинг 10.1), другие содержат информацию о корневых серверах — зона «.». Последняя зона относится к типу **hint** — подсказка. Зоны для разрешения имен обычно имеют тип **master** (главный), а зоны вторичных серверов относятся к типу **slave** (подчиненный).

Просмотр зоны — это просмотр информации, которую содержит зона. Обычно просмотр зоны разрешается только определенным, доверенным хостам. Итак, запустите **nslookup**:

```
# nslookup
Default Server: myserver.domain.com
Address: 127.0.0.1
>
```

Для того, чтобы получить информацию от сервера, нужно установить тип запроса **set q=<type>** (или **set type=<type>**). Перечень типов представлен в табл. 9.2.

Типы запросов *Таблица 9.2*

Тип	Описание
soa	Начало полномочий
a	Преобразование имени в IP-адрес узла
aaaa	Отображение IPv6-адреса узла
ns	Отображение информации о сервере DNS
ptr	Преобразование IP-адреса в имя узла
wks	Распространенные службы
hinfo	Информация о «железе» узла
mx	Информация о почтовых серверах домена
txt	Отображение записи общего назначения
cname	Отображение канонического имени
any	Отображение всех ресурсных записей

Теперь рассмотрим несколько практических примеров. Например, вы знаете имя узла — www.server.com. Давайте посмотрим, какая информация будет выведена при указании типа **any**:

```
>set q=any
>server.com
Server: myserver.domain.com
Address: 127.0.0.1
Non-authoritative answer:
server.com nameserver = comp1.server.com
server.com nameserver = comp2.server.com
server.com nameserver = comp3.server.com
Authoritative answers can be found from:
server.com nameserver = comp1.server.com
server.com nameserver = comp2.server.com
```

```
server.com nameserver = comp3.server.com
comp1.server.com internet address = 323.111.200.1
comp2.server.com internet address = 323.111.200.2
comp3.server.com internet address = 323.555.200.3
```

Теперь получим сведения о зоне и почтовиках.

```
>server comp1.server.com
Default Server: comp1.server.com
Address: 323.111.200.1
>server.com.
Server: comp1.server.com
Address: 323.111.200.1
server.com internet address = 123.111.200.2
server.com nameserver = comp1.server.com
server.com nameserver = comp2.server.com
server.com nameserver = comp3.server.com
server.com
origin = comp2.server.com
mail addr = root.server.com
serial = 19
refresh = 10800 (3 hours)
retry = 7200 (2 hours)
expire = 86400 (1 day)
minimum ttl = 3600 (1 hour)
server.com preference = 10, mail exchanger =mail.server.com
comp1.server.com internet address = 323.111.200.1
comp2.server.com internet address = 323.111.200.1
comp3.server.com internet address = 323.111.200.3
mail.server.com internet address = 323.111.200.17
```

А сейчас посмотрим информацию о других узлах в этой сети:

```
ls server.com.
[comp2.server.com]
server.com. 323.111.200.2
server.com. server = comp1.server.com
server.com. server = comp2.server.com
server.com. server = comp3.server.com
mail 323.111.200.17
gold 323.111.200.22
www.ie 323.111.200.11
```



```
jersild 323.111.200.25
comp1 323.111.200.1
comp3 323.111.200.3
parasit3 323.111.200.20
www.press 323.111.200.30
comp1 323.111.200.1
www 323.111.200.2
```

Теперь вам понятно, почему не нужно вообще использовать запись HINFO? Если при реальной атаке злоумышленник выяснит, какая операционная система используется на компьютерах в вашей сети, ему будет проще нанести удар. Я не отрицаю, существует много способов выяснить тип ОС, но зачем же сообщать это самому?

Примечание.

В записи HINFO обычно указывается информация об аппаратном обеспечении, платформе компьютера и его операционной системе.

Несколько замечаний:

1. IP-адреса использовались учебные.
2. Не всегда все так просто: иногда настройки сервера DNS и *firewall* не разрешат вам просмотреть некоторую информацию о зоне, например ту, которую мы получали с помощью команды **ls server.com**.

Разрешить передачу зоны (трансфер зоны) определенным узлам, а значит, запретить всем остальным, вы можете с помощью директивы **allow-transfer**. В следующем примере трансфер зоны разрешен узлам 10.1.1.1 и 10.1.2.1. Другими словами, на узлах 10.1.1.1 и 10.1.2.1 можно будет использовать команду **nslookup ls** для просмотра зоны.

```
options{
allow-transfer
{
10.1.1.1;
10.1.2.1;
};
};
```

Вторичный сервер DNS не передает никакой информации о зоне, поэтому обязательно укажите следующую строку в его файле конфигурации (в секции options):

```
allow-transfer { none; }
```

9.2.6. Оптимизация настроек сервера DNS

Как любой хороший администратор, вы хотите, чтобы ваш сервер DNS быстро обслуживал запросы клиентов. Но к вашему серверу могут подключаться пользователи не из вашей сети, например, из сети конкурирующего провайдера. Тогда ваш сервер будет обслуживать «чужих» клиентов. Непорядок! Опция **allow-query** в файле `/etc/named.conf` позволяет указать адреса узлов и сетей, которым можно использовать наш сервер DNS:

```
allow-query { 192.168.1.0/24; localhost; };
```

В данном примере мы позволяем использовать наш сервер узлам из сети 192.168.1.0 и узлу localhost. Целесообразно разрешить рекурсивные запросы только из сети 192.168.1.0 и узлу localhost:

```
allow-recursion { 192.168.1.0/24; localhost; };
```

Обычно взлом любой сети начинается со сбора информации — о структуре сети, об установленном программном обеспечении и версиях этого ПО и т.д. Мы можем заставить сервер DNS сообщать не номер своей версии, а произвольное сообщение:

```
version «Made in USSR»;
```

Все вышеперечисленные опции должны быть указаны в секции **options** файла конфигурации `/etc/named.conf`:

```
options {

allow-query { 192.168.1.0/24; localhost; };
allow-recursion { 192.168.1.0/24; localhost; };
allow-transfer { 10.1.1.1; 10.1.2.1; };

version «Made in USSR»;

}
```

9.2.7. Защита сервера DNS

Настройка и запуск DNS-сервера в chroot-окружении

Из соображений безопасности рекомендуется запускать все сетевые сервисы в так называемом chroot-окружении. Сейчас поясню, что это такое. Создается файловая система, повторяющая структуру корневой файловой системы, но на этой файловой системе будут только те файлы, которые необходимы для запуска нашего сетевого сервиса. Взломав сетевой сервис и получив доступ к корневой файловой системе, злоумышленник не сможет повредить всей системе в целом, поскольку он получит доступ только к файлам, которые принадлежат данному сетевому сервису. Одни сетевые сервисы могут работать в chroot-окружении, а другие — нет. Сервис BIND как раз относится к первой группе.

Теперь разберемся, как все это организовывается. Вам не нужно создавать отдельный раздел на диске для каждого сетевого сервиса: нужно только создать каталог, например, root-dns, в который вы скопируете все файлы, необходимые для запуска сервера DNS. Потом, при запуске сервиса, будет выполнена команда **chroot** для этого сервиса, которая подменит файловую систему. А так как в каталоге `root-dns`, который станет каталогом /, имеются все необходимые файлы для работы BIND, то для сервиса запуск и работа в chroot-окружении будут совершенно прозрачными.

Сразу нужно сказать, что настраивать chroot-окружении мы будем для девятой версии BIND, поскольку это значительно проще, чем для восьмой версии. В отличие от восьмой версии, где для настройки chroot-окружения нужно было копировать все бинарные файлы или библиотеки, необходимые для запуска BIND, для работы девятой версии достаточно скопировать только файлы конфигурации и зон, обслуживаемых сервером.

Начнем настраивать chroot-окружение для нашего сервера DNS. Создадим каталоги корневой файловой системы сервера DNS — каталоги `root-dns`:

```
mkdir -p /root-dns
mkdir -p /root-dns/etc
mkdir -p /root-dns/var/run/named
mkdir -p /root-dns/var/named
```

Остановим сервер DNS, если он запущен:

```
service named stop
```

Переместим файл конфигурации `/etc/named.conf` и файлы зон в каталог `/root-dns`:

```
mv /etc/named.conf /root-dns/etc/
mv /var/named/* /root-dns/var/named/
chown named.named /chroot/etc/named.conf
chown -R named.named /root-dns/var/named/*
```

Нам еще понадобится файл `/etc/localtime` для правильной работы сервера DNS со временем:

```
cp /etc/localtime /root-dns/etc/
```

Защитим от редактирования и удаления файл конфигурации `named.conf`:

```
chattr +i /root-dns/etc/named.conf
```

Примечание.

Не забудьте снять атрибут «i» перед редактированием файла конфигурации (**chattr –i /root-dns/etc/named.conf**).

Удалим каталоги `/var/named` и `/var/run/named` — они нам больше не нужны:

```
rm -rf /var/named/
rm -rf /var/run/named/
```

Добавим в файл `/etc/sysconfig/named` строку:

```
ROOTDIR=«/root-dns/»
```

Все, теперь можно запустить сервер **named**:

```
service named start
```

Выполните команду **ps –ax | grep named**. Если вы увидите примерно следующее:

```
5380  ?     S   0:00 named -u named -t /root-dns/
5381  ?     S   0:00 named -u named -t /root-dns/
5382  ?     S   0:00 named -u named -t /root-dns/
5383  ?     S   0:00 named -u named -t /root-dns/
```

значит, все сделали правильно.

Мы запустили сервер DNS в chroot-окружение, но на этом данная глава не заканчивается.

Использование подписей транзакций. Механизм TSIG

В девятой версии BIND появилась возможность создавать подписи транзакций (TSIG — Transaction SIGnatures). Механизм TSIG работает так: сервер получает сообщение, подписанное ключом, затем подпись проверяется, если она «правильная», сервер отправляет ответ, подписанный тем же ключом.

Механизм TSIG очень эффективен при передаче информации о зоне, уведомлений об изменении зоны и рекурсивных сообщений. Согласитесь, проверка подписи надежнее, чем проверка IP-адреса. Злоумышленник может вывести вторичный сервер DNS банальной атакой на отказ, и, пока администратор будет «подымать» вторичный сервер, он заменит свой IP-адрес адресом вторичного сервера. При использовании TSIG задача злоумышленника значительно усложняется: ведь ему придется «подобрать» 128-битный MD5-ключ, а вероятность такого подбора стремится к нулю.

Итак, приступим к настройке. Остановим сервис **named**, если он запущен:

```
service named stop
```

Сгенерируем общие ключи для каждой пары узлов. Общие ключи используются при «общении» первичного и вторичного серверов DNS.

```
[root@dns]# dnssec-keygen -a hmac-md5 -b 128 -n HOST ns1-ns2
Kns1-ns2.+157+49406
```

Мы используем алгоритм HMAC-MD5, 128-битное шифрование, `ns1-ns2` — это имя ключа. После выполнения этой команды будет создан файл `Kns1-ns2.+176+40946.private`. Откройте его в любом текстовом редакторе. Вы увидите примерно следующее:

```
Private-key-format: v1.2
Algorithm: 157 (HMAC_MD5)
Key: ms7dfts87Cjhj7FD9lk7a3==
```

Ключ «`ms7dfts87Cjhj7FD9lk7a3==`» и будет тем секретом, который будет передаваться между серверами. Запишите данный ключ на бумаге (которую потом нужно будет уничтожить) и удалите файлы:

```
rm -f Kns1-ns2.+157+49406.key
rm -f Kns1-ns2.+157+49406.private
```

Добавим в файл `/etc/named.conf` (или `/root-dns/etc/named.conf`) первичного и вторичного серверов DNS следующие строки:

```
key ns1-ns2 {
algorithm hmac-md5;
secret «ms7dfts87Cjhj7FD9lk7a3==»;
};
```

Укажем серверу BIND использовать ключ `ns1-ns2`. Для этого в файле `named.conf` первичного сервера DNS добавим опцию **server**. Как это сделать для первичного и вторичного серверов DNS, показано в листингах 9.7 и 9.8.

Листинг 9.7. Фрагмент файла named.conf первичного сервера DNS

```
key ns1-ns2 {
algorithm hmac-md5;
secret «ms7dfts87Cjhj7FD9lk7a3==»;
};
```

```
# прописываем вторичный сервер DNS – 192.168.1.2:
server 192.168.1.2 {
keys { ns1-ns2; };
};

options {
# разрешаем передачу зоны вторичному серверу DNS
allow-transfer { 192.168.1.2; };
…
};

….
```

Листинг 9.8. Фрагмент файла named.conf ВТОРИЧНОГО сервера DNS

```
key ns1-ns2 {
algorithm hmac-md5;
secret «ms7dfts87Cjhj7FD9lk7a3==»;
};

# прописываем первичный сервер DNS – 192.168.1.1:
server 192.168.1.1 {
keys { ns1-ns2; };
};

options {
# никому не передаем зону
allow-transfer { none };
…
};

….
```

Можно также настроить передачу зоны «по ключу». Для этого в файле конфигурации первичного сервера DNS замените строку

```
allow-transfer { 192.168.1.2; };
```

строкой

```
allow-transfer { key ns1-ns2; };
```


Нам осталось только «спрятать» файлы конфигурации *обоих* серверов DNS от посторонних глаз — ведь они содержат ключи в открытом виде.

```
chmod 600 named.conf
```

Запускаем сервис named:

```
service named start
```

Теперь о безопасности вашего BIND позаботится TSIG.

9.3. Сервер DNS под управлением Windows 2000/2003 Server

Настройка сервера DNS под управлением Windows 2000 Server полностью аналогична настройке в Windows 2003 Server, поэтому эти две операционные системы объединены в один пункт. Сразу хочу отметить, что настраивать сервер DNS под управлением Windows 2000/2003 — сплошное удовольствие. Менеджер DNS стал намного удобнее и понятнее по сравнению с Windows NT 4.0. Давайте договоримся, если в данном пункте сказано Windows 2000, то подразумевается также и Windows 2003 Server.

9.3.1. Установка сервера Microsoft DNS

Для установки сервера отройте Панель управления и откройте окно **Add/Remove Programs (Установка и удаление программ)**. Затем перейдите в раздел **Add/Remove Windows Components (Установка и удаление компонент Windows)**. Откроется окно **Windows Components Wizard** (рис. 9.1), в котором нужно выделить пункт **Networking Options** и нажать кнопку **Details**.

После этого откроется окно **Networking Services** (см. рис. 9.2). В нем нужно отметить пункт **Domain Name System (DNS)** и нажать кнопку **OK**.

После установки сервера DNS лучше перезагрузить машину, даже если операционная система не будет этого требовать — так рекомендует Microsoft. После перезагрузки системы выполните команду меню **Start → Programs → Administrative Tools → DNS** (в Windows 2003 — **Start → Settings → Control Panel → Administrative Tools → DNS**). Откроется окно с названием DNS (рис. 9.3).

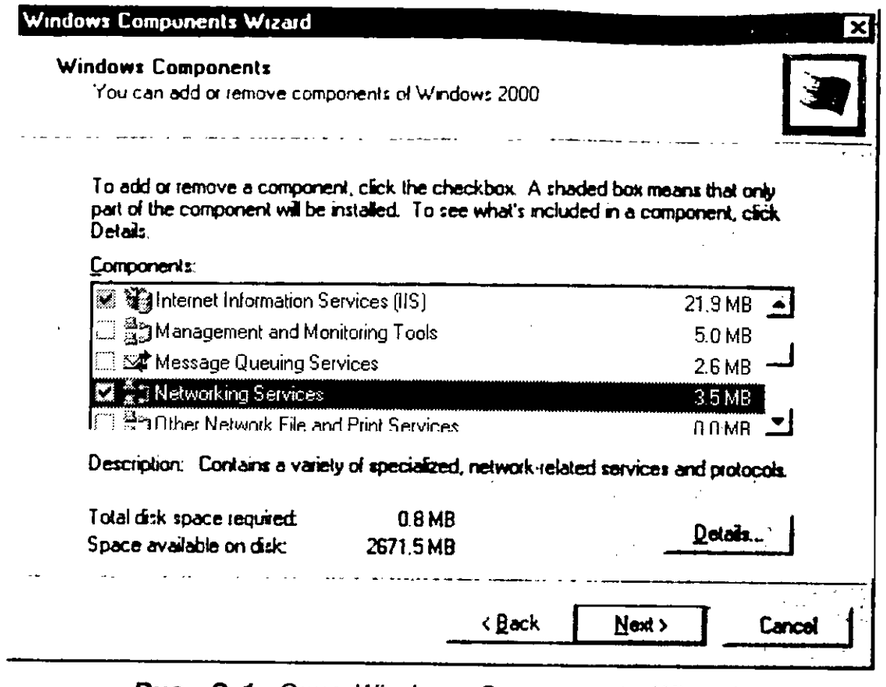


Рис. 9.1. *Окно Windows Components Wizard*

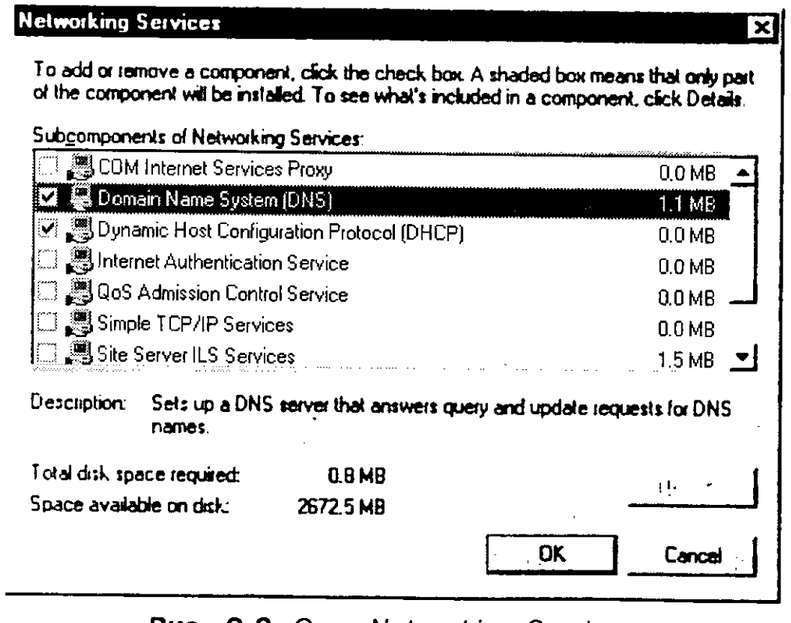


Рис. 9.2. *Окно Networking Services*

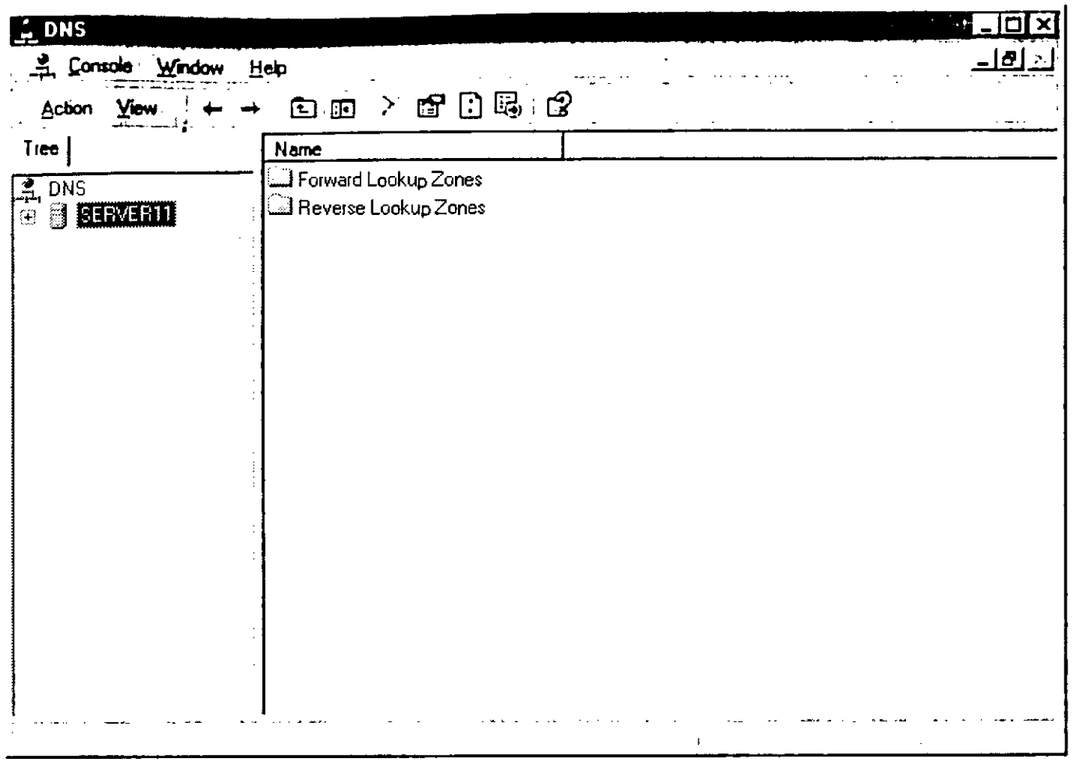


Рис. 9.3. *Управление сервером DNS*

9.3.2. Создание зоны ответственности

Если мы настраиваем первичный (главный) сервер DNS, нам нужно создать первичную зону. Для этого выделите ваш сервер (на рис. 9.4 это SERVER11) и выполните команду меню **Action → New Zone**.

Нужно выбрать тип зоны **Standard Primary**, поскольку службу Active Directory мы еще не устанавливаем.

Затем нам нужно уточнить тип зоны (см. рис. 9.5) — прямая (для преобразования имени в IP-адрес) или обратная (для преобразования IP-адреса в имя). Как правило, сначала создается прямая зона, а потом обратная.

После этого нужно ввести имя зоны, например, firma.com (рис. 9.6).

Следующий шаг — это выбор имени файла зоны. По умолчанию используется имя «имя_зоны.dns». Используйте это имя. Созданный файл будет сохранен в каталоге `%SystemRoot%\system32\dns`.

После этого система попросит вас проверить введенные данные (рис. 9.7):

- Имя зоны;
- Тип зоны;
- Тип преобразования;
- Имя файла.

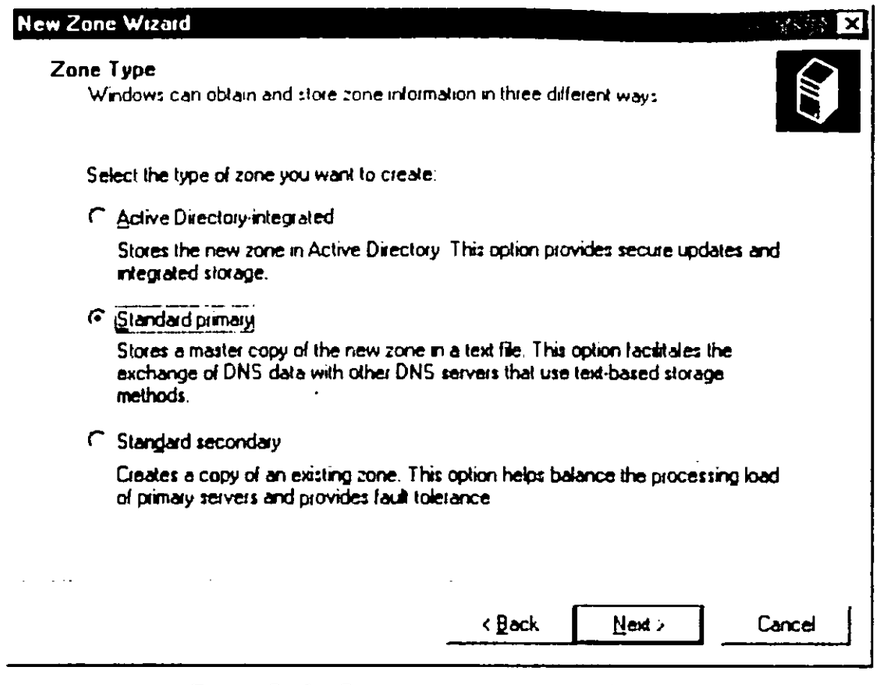


Рис. 9.4. *Создание первичной зоны*

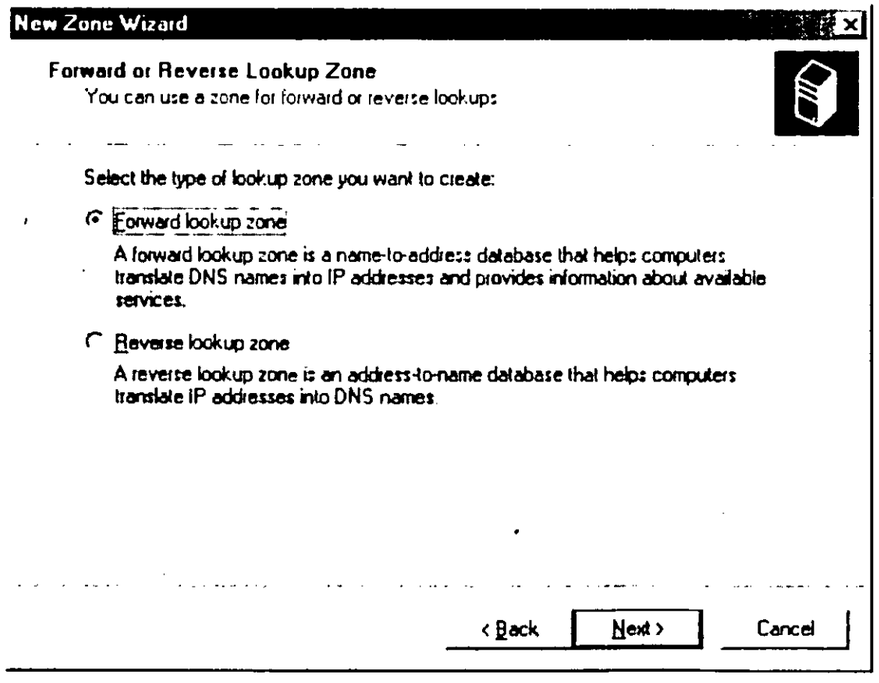


Рис. 9.5. *Выбор типа зоны*

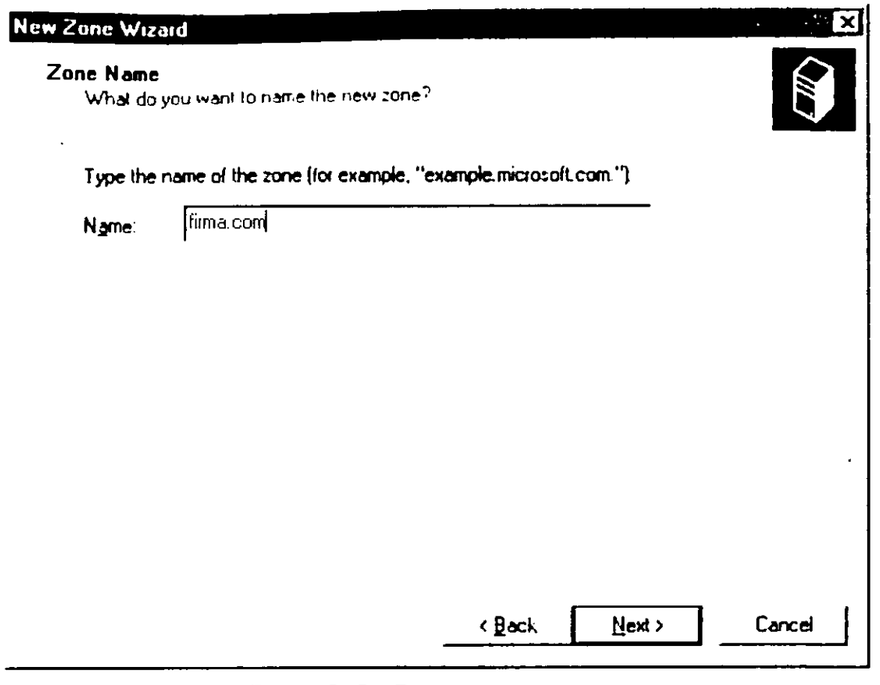


Рис. 9.6. *Ввод имени зоны*

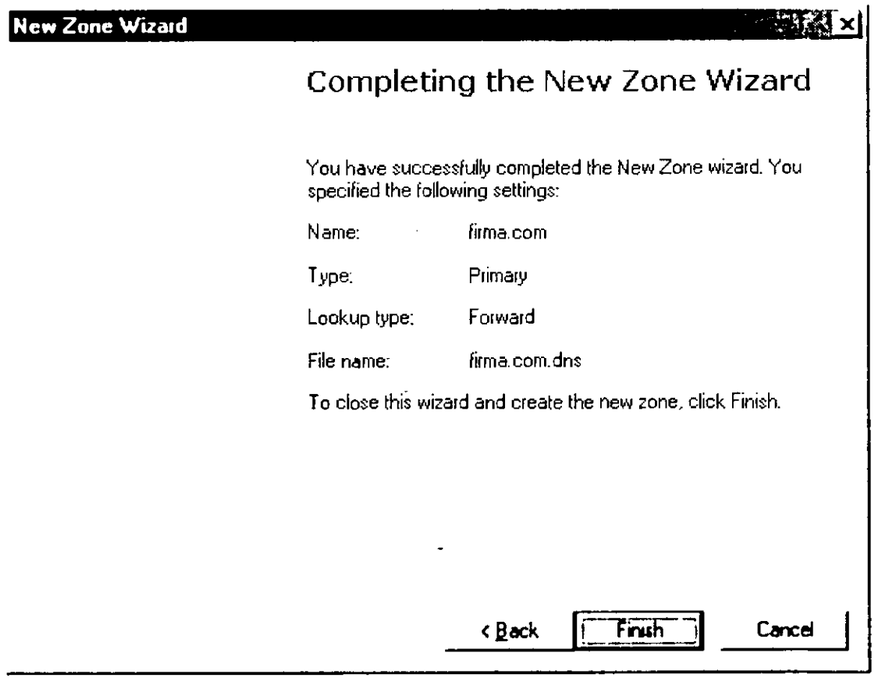


Рис. 9.7. *Принять параметры?*

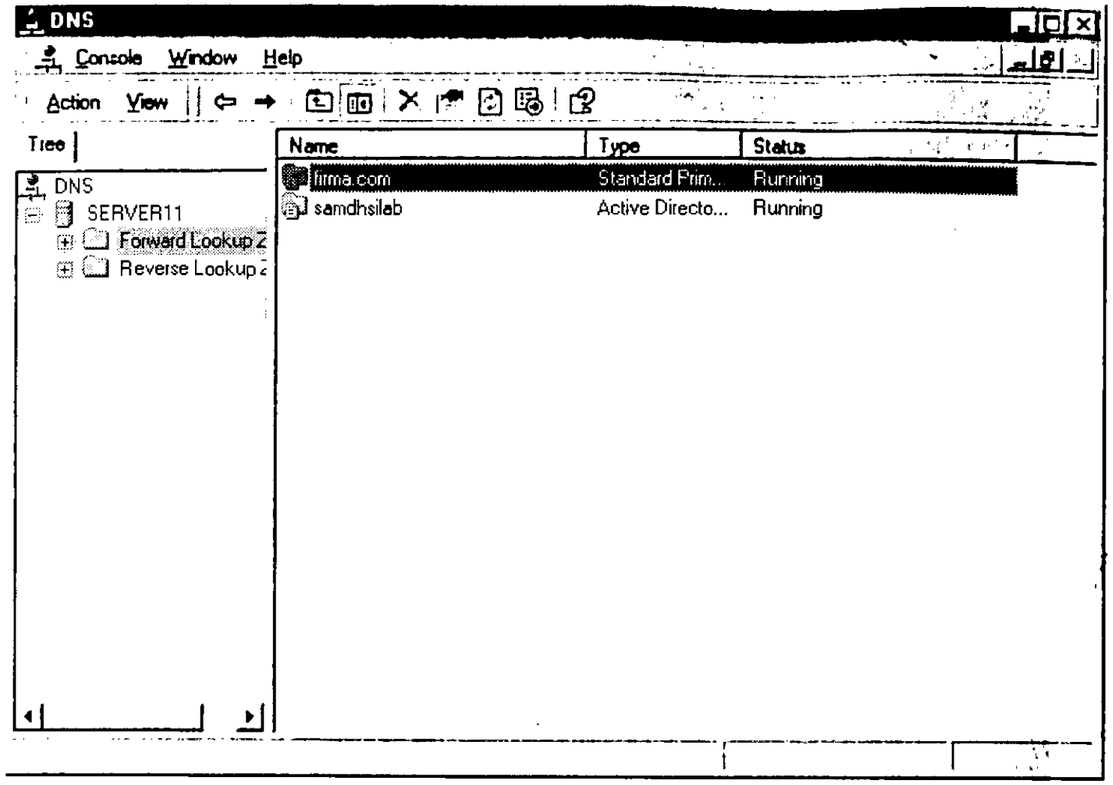


Рис. 9.8. *Созданная зона*

Если введенные вами параметры точны, нажмите кнопку **Finish**. Созданная зона показана на рис. 9.8.

Теперь нужно создать обратную зону. Для ее создания повторите все шаги заново, только установите тип преобразования *обратный* (см. рис. 9.5). Помните, как нужно создавать обратную зону в Windows NT. Там нужно было указать специальное имя обратной зоны, например, 1.168.192.in-addr.arpa.

Если вы ошибетесь хотя бы в одном символе, зона уже не будет считаться обратной для заданной подсети. В Windows 2000 такого неудобства нет: вы просто выбираете тип зоны (обратная) и указывается адрес вашей подсети — 192.168.1.0. Система сама создаст нужный файл (1.168.192.in-addr.arpa): вам нужно только нажать кнопку **Next** (рис. 9.9).

Как и при создании первичной зоны, после указания имени зоны, система попросит вас ввести имя файла обратной зоны. Лучше не изменять имя файла, предложенного по умолчанию. Обратная зона будет создана после нажатия кнопки **Finish** в окне проверки правильности ввода информации (рис. 9.10).

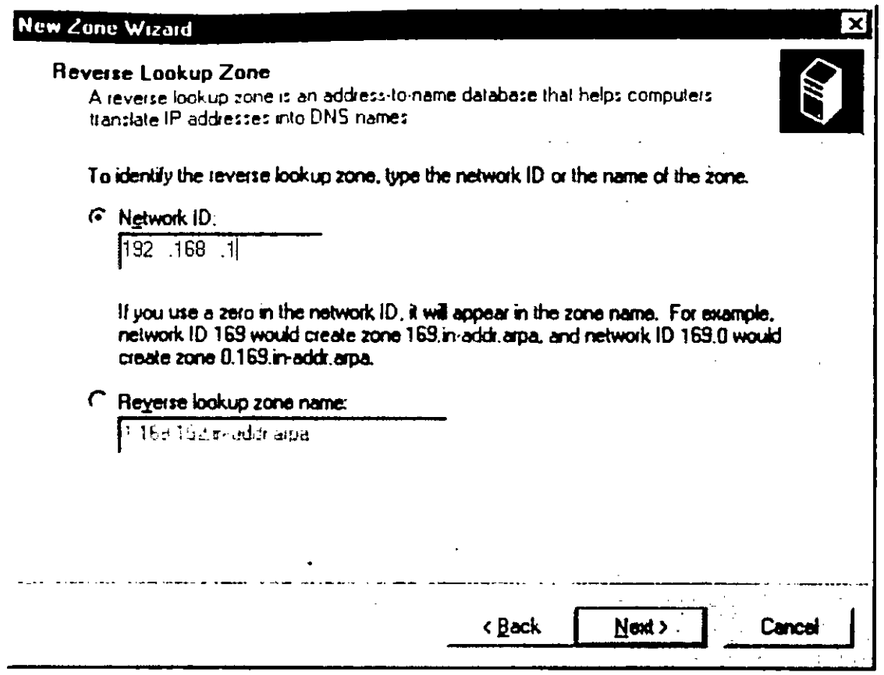


Рис. 9.9. *Создание обратной зоны*

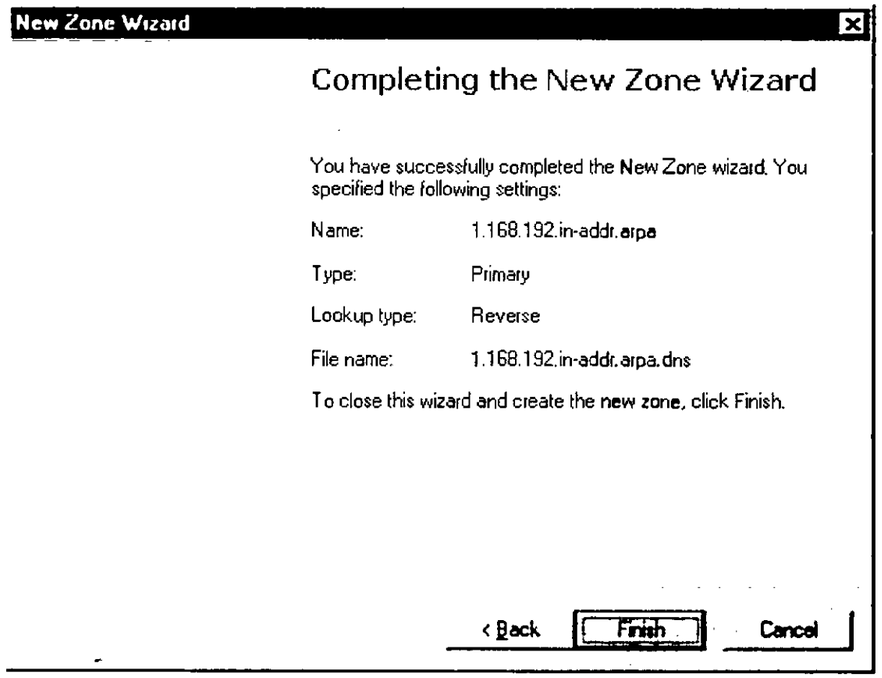


Рис. 9.10. *Информация об обратной зоне*

9.3.3. Настройка зоны

Добавление доменов

Если вы хотите добавить в зону поддомен, сначала «откройте» зону. Для этого выберите в левой части окна нужную вам зону, дважды щелкнув по ней. После этого в меню **Action** выберите команду **New domain**.

Добавление узлов

Для добавления узла «откройте» зону и выполните команду **Action → New host.**

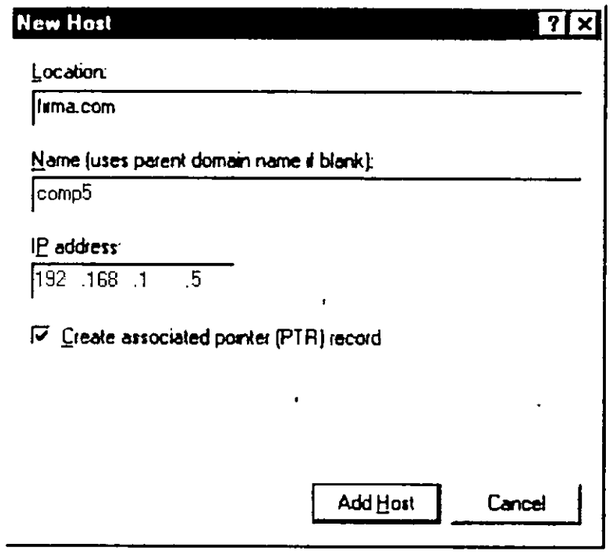


Рис. 9.11. *Добавление узла*

Введите имя узла и его IP-адрес. Обязательно отметьте режим **Created associated pointer (PTR) record**, чтобы система создала соответствующую запись также и в обратной зоне. В прямую зону будет помещена запись типа:

```
имя  A   IP-адрес
```

а в обратную:

```
IP-адрес PTR имя
```

Другие команды меню Action

Если выделить зону и посмотреть в меню **Action**, там будет еще две команды: **New alias** и **New Mail Exchanger**, позволяющие создать ресурс непосредственно. Первая создает запись CNAME, а вторая — MX. Если вам нужна какая-либо другая ресурсная запись, выберите команду **New resource record**.

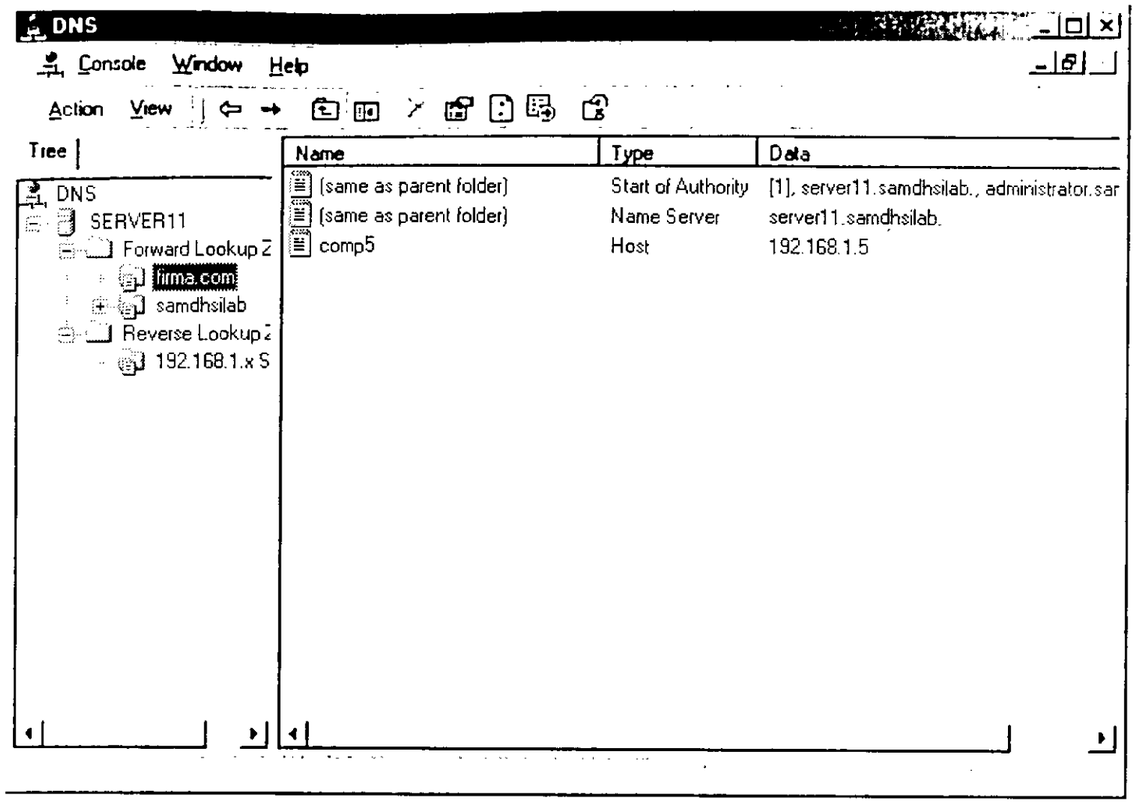


Рис. 9.12. *Содержимое прямой зоны*

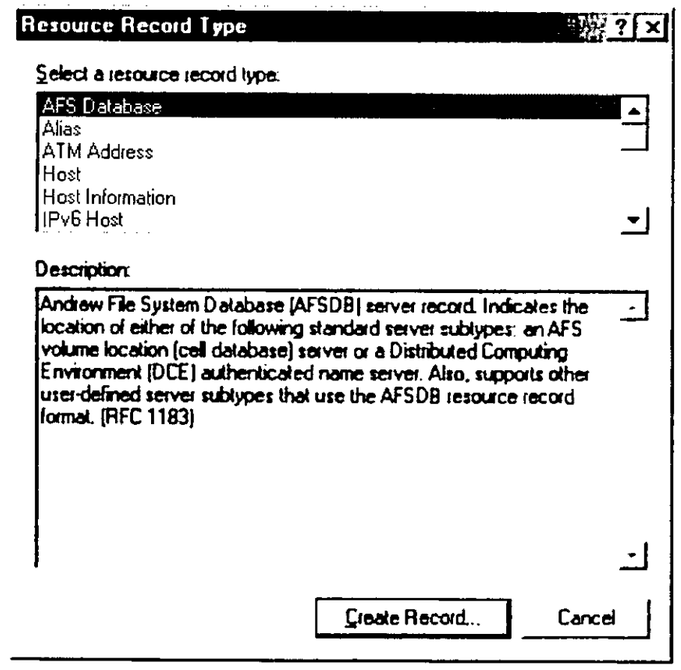


Рис. 9.13. *Создание ресурсных записей*

Создание ресурсной записи проиллюстрировано на рис. 9.13. Узнать для чего используется та или иная ресурсная запись можно в предыдущем пункте.

Свойства зоны

Выделите интересующую вас зону и выполните команду **Action → Properties**. В открывшемся окне можно будет установить свойства зоны (см. рис. 9.14):

- **General** — общие свойства зоны;
- **Start of Authority** — начало полномочий;
- **Name servers** — информация о серверах имен;
- **WINS** — интеграция WINS и DNS. WINS будет рассматриваться в следующей главе;
- **Zone Transfer** — информация о передаче зоны: кому, когда и как.

Со свойствами зоны должно быть все понятно. Все, кроме динамического обновления. Включать или нет? По умолчанию динамическое обновление (Dynamic update) выключено (No). Разберемся, что это такое.

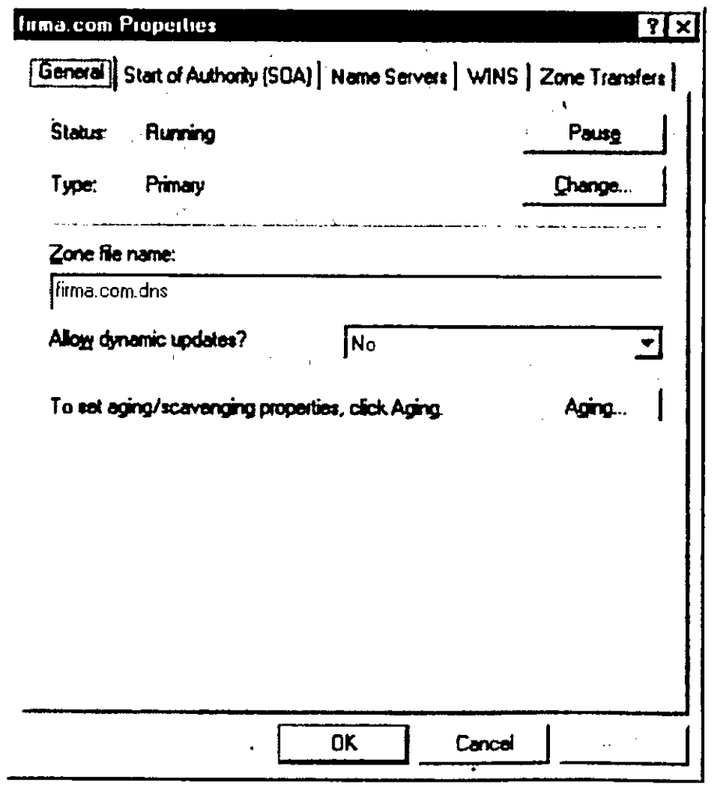


Рис. 9.14. *Свойства зоны*

Динамическое обновление позволяет DNS-клиентам изменять записи DNS-сервера. Например, клиент с IP-адресом 192.168.1.77 был статически «прописан» на сервер DNS под именем `manager`. Если пользователь изменяет имя компьютера (пусть новое имя будет `director`), то изменение автоматически будет отображено в базе DNS. То есть IP-адрес 192.168.1.77 уже будет связан с именем `director`.

Включать динамическое обновление можно, если у вас в сети работает сервер DHCP. В противном случае лучше не позволять пользователям такой свободы.

Свойства сервера

Свойства сервера часто изменять вам не придется. Лично я изменял свойства своего сервера всего один раз, когда ради эксперимента превратил его из первичного сервера в резервный. Для изменения свойств сервера (рис. 9.15) выделите сервер в левой части окна и выберите команду **Action → Properties**.

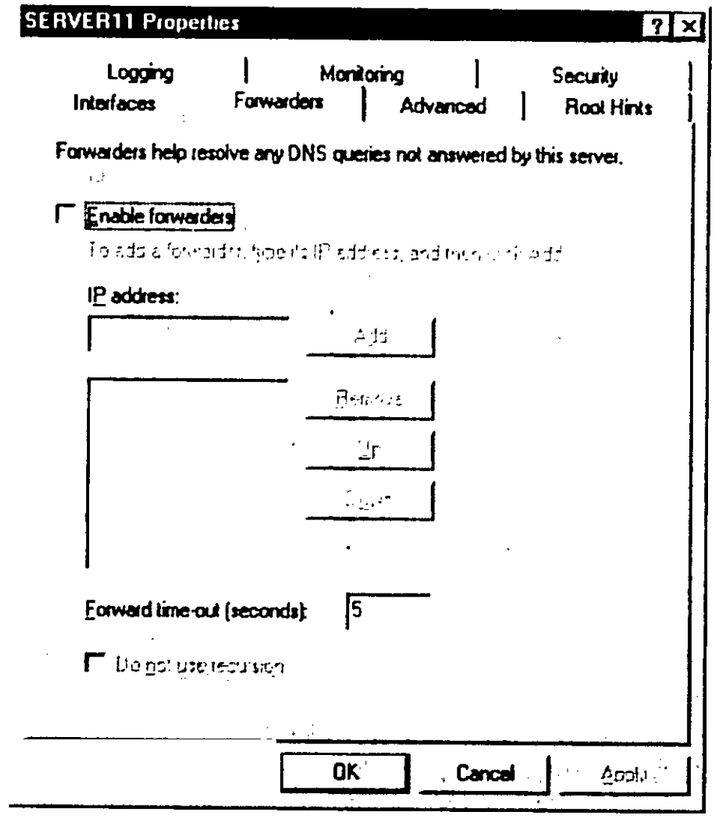


Рис. 9.15. *Свойства сервера*

9.3.4. Дополнительные возможности

Вторичный сервер DNS

Для настройки вторичного сервера DNS выполните те же операции, что и для настройки основного: то есть установите службу MS DNS Server. После этого создайте зону firma.com, но при создании зоны укажите ее тип — **Secondary** (Вторичная). Затем укажите IP-адрес первичного (основного сервера DNS). В качестве имени основного DNS-сервера в поле **Server** лучше указать его IP-адрес. А в поле **Zone** — имя зоны, то есть firma.com.

Кэширующий сервер

Для настройки кэширующего сервера выполните команду **DNS → New server**. Затем введите IP-адрес сервера. Создавать зоны не нужно! Просто откройте окно свойств нового сервера. Для этого щелкните правой кнопкой по серверу и выберите команду **Properties**.

Затем перейдите на вкладку **Forwarders** и включите режим **Use Forwarder(s)**. Затем вам остается указать только IP-адреса серверов DNS вашего провайдера.

9.4.5. Проверка работы сервера

Для проверки работы нашего сервер используется программа **nslookup**, которая входит в состав Windows NT. Запускать программу нужно в окне командной строки, открыть которое можно с помощью команды меню **Start → Programs → Command Prompt**.

Запустите программу **nslookup**, указав IP-адрес нашего сервера:

```
nslookup 192.168.1.111
```

Попробуем узнать IP-адрес компьютера comp5:

```
> comp5
Name: comp5.firma.com
Address: 192.168.1.5
```

Для того чтобы узнать имя компьютера, нужно указать его IP-адрес.

Чтобы увидеть текущие установки программы nslookup, введите команду **set all**. При тестировании обычно нужно изменить тайм-аут и количество попыток:

- set ti=8 // тайм-аут равен 8 секунд
- set ret=6 // 6 попыток

9.5. Настройка клиентов

Прежде всего, разрешите вас поздравить: вы только что настроили первый в своей сети сервер! Ведь до этого у нас было только несколько компьютеров, которые можно было только пропинговать, да и то только по IP-адресу. Теперь мы перешли на новый уровень — от одноранговой сети до сети клиент/сервер.

Ясное дело, что другие компьютеры и не подозревают, что в нашей сети появился сервер DNS. Поэтому нужно сообщить им об этом. Итак, перейдем к настройке клиентов.

Windows 9x/ME

Запустите апплет **Сеть** с Панели управления. Затем выберите протокол TCP/IP и нажмите кнопку **Свойства**. В открывшемся окне перейдите на страничку **Конфигурация DNS** (рис. 9.16).

В поле **Имя компьютера** нужно ввести имя этого компьютера, то есть компьютера-клиента. В нашем случае это comp5. В поле **Домен** нужно ввести имя нашего домена — firma.com. Затем в поле **Порядок просмотра серверов DNS** вводим адрес нашего DNS-сервера — 192.168.1.1 и нажимаем кнопку **Добавить**. Причем, если у вас два сервера, то сначала нужно вводить первичный сервер DNS, а только затем — резервный. В поле **Порядок просмотра доменных суффиксов** можно ввести имя нашего домена. Нажимаем кнопку Ок и перезагружаем компьютер.

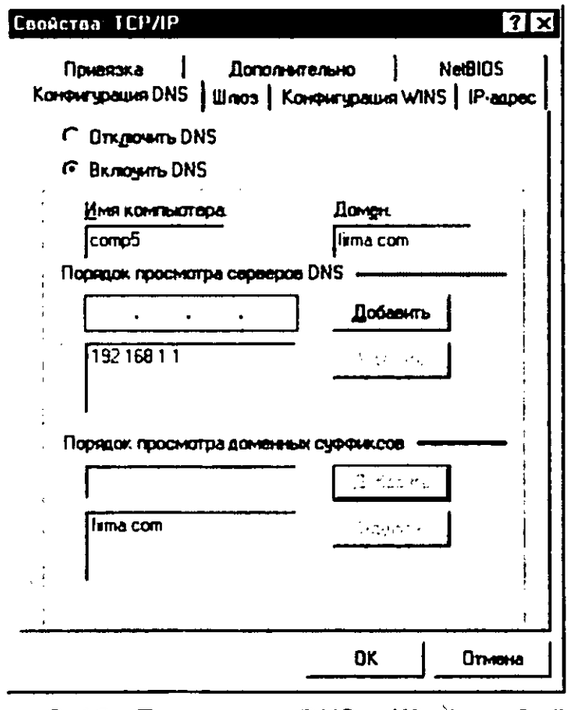


Рис. 9.16. *Параметры DNS в Windows 9x/ME*

Windows NT

Запустите Панель управления и откройте апплет Сеть (Network). Потом перейдите на вкладку **Протоколы** (Protocols), выберите протокол TCP/IP, нажмите кнопку **Свойства** и в открывшемся окне перейдите на вкладку **DNS** (см. рис. 12.1). Далее, все так же, как и в Windows 9x — вводим имя этого компьютера (comp5), вводим имя домена (firma.com) и добавляем IP-адрес сервера DNS — 192.168.1.1.

Windows XP

Откройте папку **Сетевые подключения** (**Пуск** → **Настройка** → **Сетевые подключения**), затем выберите **Подключение по локальной сети** — щелкните по нему правой кнопкой мыши и выберите команду **Свойства**. Затем выберите протокол TCP/IP и нажмите кнопку **Свойства**. В открывшемся окне введите адреса первичного и резервного (если он есть) серверов (см. рис. 9.17).

Добавить DNS-суффикс можно, нажав кнопку **Дополнительно** и перейдя на вкладку **DNS** (см. рис. 9.18).

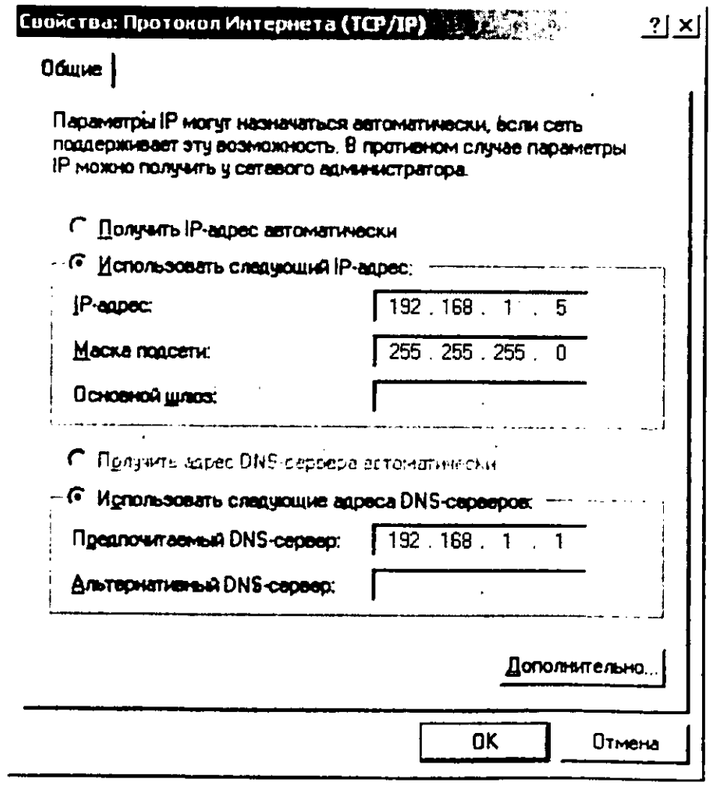


Рис. 9.17. *Настройки DNS в Windows XP*

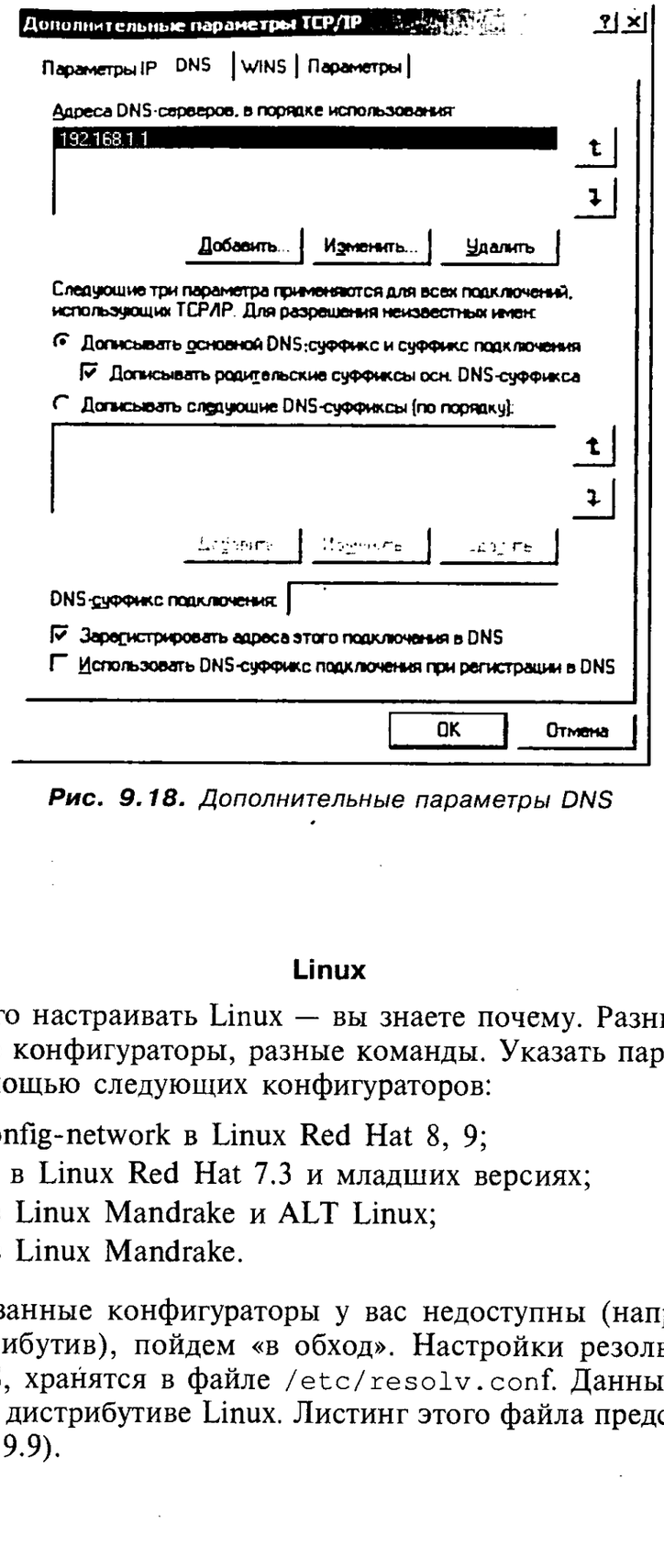


Рис. 9.18. *Дополнительные параметры DNS*

Linux

Сложнее всего настраивать Linux — вы знаете почему. Разные дистрибутивы, разные конфигураторы, разные команды. Указать параметры DNS можно с помощью следующих конфигураторов:

- redhat-config-network в Linux Red Hat 8, 9;
- netconfig в Linux Red Hat 7.3 и младших версиях;
- draknet в Linux Mandrake и ALT Linux;
- netconf в Linux Mandrake.

Если же указанные конфигураторы у вас недоступны (например, у вас другой дистрибутив), пойдем «в обход». Настройки резолвера, то есть клиента DNS, хранятся в файле `/etc/resolv.conf`. Данный файл имеется в любом дистрибутиве Linux. Листинг этого файла представлен ниже (см. листинг 9.9).

Листинг 9.9. Файл /etc/resolv.conf

```
search firma.com
nameserver 192.168.1.1
nameserver 192.168.1.2
```

Директива **search** позволяет указать список DNS-суффиксов, но мы ее будем указывать для указания домена. Можно вместо нее использовать менее универсальную директиву **domain**, но мы не станем этого делать. После это директивы следуют директивы **nameserver**, указывающие сервера имен. Всего можно указать четыре сервера имен.

Теперь откройте файл `/etc/hosts.conf` (см. листинг 9.10).

Листинг 9.10. Файл /etc/hosts.conf

```
order hosts,bind
multi on
```

В этом файле указывается порядок разрешения имен. В данном случае сначала используется файл /etc/hosts, а уже затем — сервер DNS. Вы можете изменить этот порядок. Вторая строка разрешает использовать сразу несколько IP-адресов. Не жадничайте и не отключайте эту возможность.

9.6. Выбор операционной системы сервера DNS

Сервер DNS будет одинаково хорошо работать — как под управлением Linux, так и под управлением Windows 2003 Server. При выборе операционной системы нужно учитывать множество факторов, не зависящих от операционной системы. Скорее всего, у вас небольшая сеть, в которой уже есть сервер, например, Windows 2000 Server или Windows NT 4 Server. Вот на базе этой операционной системы и нужно настраивать DNS-сервер.

Вы же будете выделять отдельный компьютер только для DNS-сервера. Это целесообразно делать, если у вас большое предприятие или вы являетесь Internet-провайдером. В таком случае я бы посоветовал использовать Linux: во-первых, данная операционная система бесплатна и вам не придется платить деньги за дополнительный сервер, а во-вторых, требования к системным ресурсам у этой операционной системы значительно ниже, чем у Windows 2000 Server. Пусть даже Windows 2000 Server будет выполнять функции только DNS-сервера: для его нормальной работы понадобится компьютер с частотой не ниже 700 МГц и оперативной памятью 256...512 Мб.

В качестве Linux-сервера, выполняющего функции DNS-сервера и маршрутизатора, вполне подойдет старенький Pentium с частотой 133...200 МГц и памятью 64-128 Мб. Такой компьютер, благодаря стараниям Microsoft, нельзя даже использовать в качестве печатной машинки.

С другой стороны, если у вас большая сеть, вы будете заинтересованы в использовании службы Active Directory. В этом случае целесообразно интегрировать службы DNS и Active Directory. В этом случае, разумеется, о Linux придется забыть...

Как вы видите, не все зависит только от операционной системы. Выберите оптимальное решение, подходящее именно для вашей сети.

Глава 10

Служба WINS

В этой главе мы поговорим о именах сети Microsoft и службе WINS. Может возникнуть вопрос: «А чем же эти имена отличаются от имен DNS?» И этот вопрос совершенно уместен — потому что на первый взгляд непонятно для чего они вообще нужны. Компания Microsoft во многом поступает по принципу «а мы новый дом построим», поэтому она создала службу WINS, которая во многом напоминает службу DNS. Но только это «свой» DNS, от Microsoft.

Первоначально WINS был разработан для преобразования имен в сетях Microsoft. Если бы Windows была бы единственной операционной системой, то наверняка, о DNS мы так бы и не услышали — был бы только WINS. Но так как Microsoft не удалось завоевать все сети мира, в операционных системах Microsoft есть программы резолверы, которые используют службы DNS и WINS (от своего еще никто не отказывался), даже выпущен сервер DNS от Microsoft, чтобы серверные операционные системы Microsoft ничем не уступали другим операционным система по функциональности.

Второй вопрос, который может возникнуть, таков: «Что будет, если не настроить WINS?» Да ничего особенного. Если вы строите сеть с нуля, то просто прочитайте эту главу — настраивать вам ничего не придется — хватит одной службы DNS. Читать эту галву нужно для общего развития. Если же кто-то до вас настраивал сеть с использованием WINS (лет эдак пять-шесть назад WINS настраивалась в больших сетях — сейчас же используется DNS), то вам придется не просто прочитать эту главу, а прочитать ее внимательно, чтобы разобраться что и зачем используется.

10.1. Протокол NetBIOS

Служба WINS (Windows Internet Name Service) чем-то напоминает службу DNS, но она используется для разрешения имен сети Microsoft, то есть компьютеров, которые работают под управлением операционной системы Windows. Основная задача WINS — это разрешение имен (то есть преобразование символьного имени в IP-адрес и наоборот). Про остальные функции WINS мы поговорим позже, а сейчас приступим к рассмотрению протокола NetBIOS, без которого не имеет смысла рассматривать службу WINS.

Стандарт NetBIOS разработан компанией Sytek Corp. в далеком 1983 году. Компания Sytek разрабатывала данный стандарт не просто так, а по заказу IBM. Как данный стандарт оказался на вооружении у Microsoft, думаю, говорить не стоит: все мы слышали о периоде сотрудничества компаний IBM и Microsoft, когда они работали над разработкой операционной системы.

Стандарт NetBIOS определяет одноименный протокол, работающий на сеансовом и транспортном уровне. Протокол NetBIOS выполняет следующие функции:

- регистрацию сетевых имен;
- проверку сетевых имен;
- начало и завершения сеанса;
- передачу данных сеанса (если он ориентирован на соединение);
- передачу датаграмм сеанса (если он не ориентирован на соединение);
- мониторинг и управление сетевым адаптером.

Имя NetBIOS — это 16-байтный адрес, уникальный в данной сети. Имя NetBIOS используется для идентификации в сети ресурса NetBIOS: компьютера, группы, пользователя и т.д.

Просмотреть все имена NetBIOS вашей сети можно с помощью команды **nbtstat −n**. Результат действия этой команды продемонстрирован на рис. 10.1.

Имена NetBIOS используются в следующих системах:

- Операционной системе Windows NT — все сетевые службы NT используют NetBIOS.
- Оболочке или все-таки операционной системе — как кому нравится — Windows for Workgroups.
- LAN Manager.
- LAN Manager для UNIX.

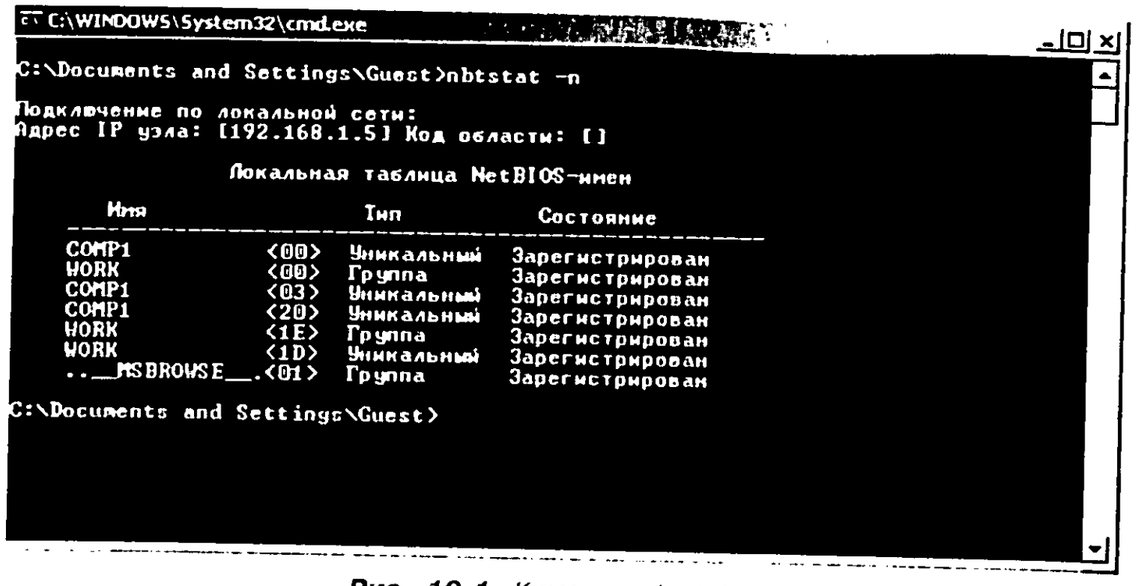


Рис. 10.1. *Команда nbtstat -n*

10.2. Разрешение имен NetBOIS

Рассмотрим, как выполняется разрешение имен NetBIOS в сети Microsoft:

- Когда клиент запрашивает имя NetBIOS, IP-адрес, соответствующий данному имени, ищется в первую очередь в локальном кэше имен NetBIOS. Если IP-адрес не обнаружен, будет выполнено разрешение имени без использования NetBIOS.
- Если IP-адрес не обнаружен в локальном кэше, выполняется три попытки доступа к основному серверу NetBIOS. Если сервер NetBIOS не доступен, выполняется попытка доступа к резервному серверу NetBIOS. Если ответ от сервера получен, и он нашел в своей базе данных нужного IP-адреса, возвращается найденный IP-адрес.
- Если IP-адрес не найден, выполняется широковещательный запрос в локальную сеть. Если имя NetBIOS обнаружено в локальной сети, возвращается IP-адрес.
- Если IP-адрес не найден в локальной сети, то система обращается к локальному файлу LMHOSTS. Он находится в каталоге `%SystemRoot%\System32\Drivers\Etc`. Если имя найдено в файле LMHOSTS, возвращается IP-адрес.
- Если имя не найдено в файле LMHOSTS, Windows NT при условии включенного режима **Enable DNS for Windows resolution** (свойства протокола TCP/IP, вкладка **WINS Address** — см. рис. 10.2) будет искать IP-адрес в файле Hosts. Он также находится в каталоге %SystemRoot%\System32\Drivers\Etc.

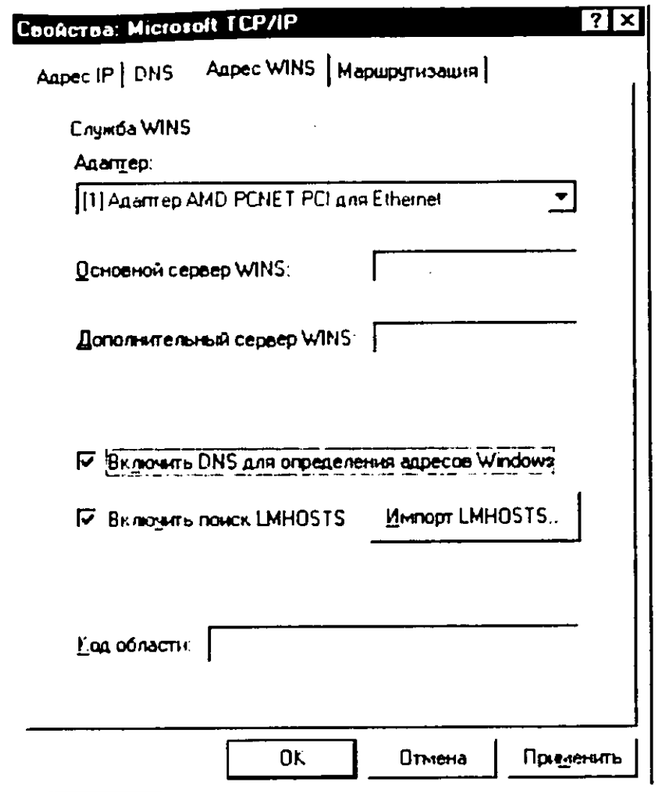


Рис. 10.2. *Свойства WINS*

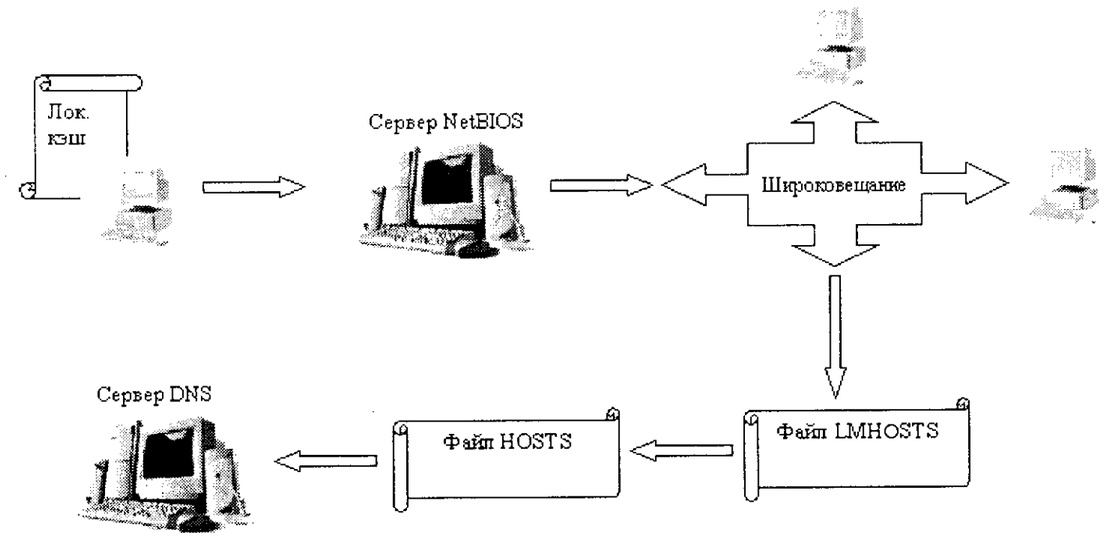


Рис. 10.3. *Схема разрешения имени NetBIOS*

- Если IP-адрес не найден в файле Hosts, будет выполнена попытка обращения к серверу DNS. Если сервер не отвечает, то будет произведено несколько повторных запросов с интервалами 5, 10, 20, 40 секунд.
- Если сервер DNS не в состоянии разрешить имя компьютера, клиенту будет сообщено, что компьютер с данным именем не удалось обнаружить.

Схема разрешения имени NetBIOS показана на рис. 10.3.

10.3. Файл LMHOSTS

Файл LMHOSTS используется при разрешении имен NetBIOS в самую последнюю очередь, если считать, что использование DNS при разрешении Windows-имен выключено. LMHOSTS — это обыкновенный текстовый файл, который можно редактировать в любом текстовом редакторе, например, Блокноте. В каталоге %SystemRoot%\System32\Drivers\Etc находится пример этого файла с подробным описанием всех опций — LMHOSTS.SAM.

Пример файла LMHOSTS:

```
192.168.1.10 Director     # Director's comp
192.168.1.2  Den          # Second director's comp
192.168.1.1  Main         #PRE # Main Server
```

В файле LMHOSTS можно использовать ключевые слова. Они начинаются со знака решетки, после которого не должен следовать пробел или пробельный символ, поскольку знак # будет воспринят как комментарий. Ключевые слова файла LMHOSTS описаны в табл. 10.1.

Файл LMHOSTS просматривается последовательно, поэтому для ускорения поиска узлов наиболее часто используемые узлы нужно расположить в начале файла. Это не касается записей #PRE — их нужно расположить в конце списка, поскольку они при инициализации будут загружены в кэш.

Утилита **nbtstat** позволяет управлять локальным кэшем NetBIOS:

- **nbtstat -c** — отображает состояние кэша;
- **nbtstat -R** — загружает кэш имен PRE-записями из файла LMHOST;
- **nbtstat -n** — отображает список всех имен NetBIOS.

Ключевые слова файла LMHOSTS *Таблица 10.1*

Ключевое слово	Описание
#PRE	Данную запись нужно поместить в локальный кэш имен и не удалять ее оттуда. Загрузка имен из файла LMHOSTS в кэш имен выполняется при инициализации, но ее можно выполнить принудительно — с помощью утилиты nbtstat, о чем будет сказано ниже
#DOM:[имя_домена]	Ассоциирует запись с указанным доменом. Данное слово используется при просмотре ресурсов сети, синхронизации учетных записей пользователей и регистрации в сети
#MH	Используется, если компьютер оснащен несколькими сетевыми интерфейсами
#INCLUDE	Загружает и просматривает записи из другого файла, который имеет такой же формат, что и LMHOSTS
#NOFNR	Запрещает использование прямых запросов при работе со старыми версиями LAN Manager
#BEGIN_ALTERNATE #END_ALTERNATE	Используется для указания альтернативных мест расположения файлов LMHOSTS

10.4. Служба WINS

Сервер WINS — это усовершенствованный сервер имен NetBIOS, разработанный компанией Microsoft. Основная задача данного сервера — снизить объем широковещательного трафика, вызванного при широковещательном разрешении имени NetBIOS.

Сетевой трафик снижается за счет того, что запросы клиентов поступают непосредственно на сервер, без использования широковещания. Если серверу удалось разрешить имя, то адрес сразу же отправляется клиенту, если нет, то никакого широковещания не происходит. Широковещание допускается лишь в том случае, если сервер WINS недоступен.

Второе преимущество WINS — это динамическая база данных соответствия имен IP-адресам, в результате чего отпадает необходимость в файле LMHOSTS.

Рассмотрим процесс разрешения имени с использованием сервера WINS:

1. При запуске в среде WINS, клиент регистрируется на сервере — называет серверу свое имя и свой IP-адрес. Сервер WINS задается в конфигурации клиента.
2. Когда клиенту нужно разрешить имя, он направляет свой запрос непосредственно к серверу WINS.
3. Если имя найдено в базе данных WINS, IP-адрес направляется к клиенту. База данных WINS динамическая, поэтому она всегда содержит самые свежие данные, и ее не нужно обновлять вручную, как базу данных сервера DNS.

Использовать WINS-сервер целесообразно, если ваша сеть работает под управлением Windows NT Server. Тогда можно немного снизить время разрешения имени NetBIOS, за счет отказа от использования сервера DNS, который используется в последнюю очередь, и существенно снизить широковещательный трафик — это особо актуально для небольших сетей, использующих технологию Ethernet/Fast Ethernet. Если ваша сеть ориентирована на работу с Internet, целесообразно использовать только DNS-сервер, интегрировав его при необходимости с протоколом DHCP.

10.5. Настройка сервера и клиента WINS

Итак, определим требования к серверу WINS. Сервером WINS может быть любой сервер под управлением Windows NT Server, причем не обязательно контроллер домена.

Клиентом службы WINS могут быть компьютеры под управлением следующих операционных систем:

- LAN Manager 2.2 для MS DOS;
- клиент Microsoft для MS DOS;
- Windows for Workgroups 3.11;
- Windows 9x/ME;
- Windows NT 4.0 Workstation;
- Windows NT Server 4.0;
- Windows 2000;
- Linux с пакетом Samba.

Сначала настроим клиент — так проще. В Windows 9x/ME откройте апплет **Сеть** с Панели управления. Затем откройте свойства протокола TCP/IP и перейдите на вкладку **Конфигурация WINS**. Включите режим **Включить распознавание WINS** и добавьте WINS-сервер (см. рис. 10.4).

В Windows NT нужно открыть апплет **Сеть** с Панели управления, перейти на вкладку **Протоколы**, открыть свойства протокола TCP/IP и перейти на вкладку **Адрес WINS** (см. рис. 10.2). На этой страничке нужно задать IP-адреса основного и резервного (если он есть) серверов WINS.

В Windows 2000/XP откройте свойства соединение по локальной сети, затем свойства протокола TCP/IP и нажмите кнопку **Дополнительно**. Затем перейдите на вкладку **WINS**. На это страничке можно задать IP-адреса серверов WINS (рис. 10.5).

Теперь приступим к настройке сервера. Сначала нужно установить службу WINS. Для этого откройте апплет **Сеть** с Панели управления и перейдите на вкладку **Services (Службы)**, показанную на рис. 10.6. Все действия, как всегда, нужно выполнять от имени администратора.

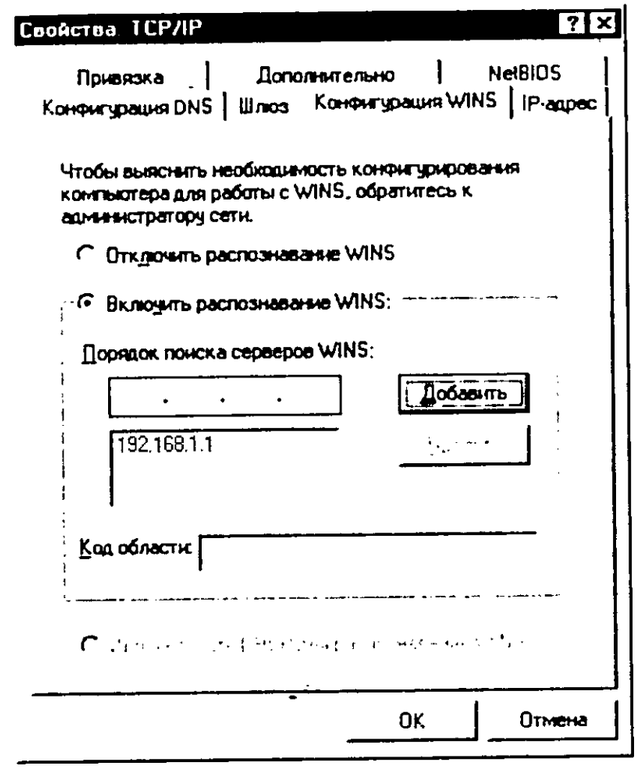


Рис. 10.4. *Конфигурация WINS в Windows 9x/ME*

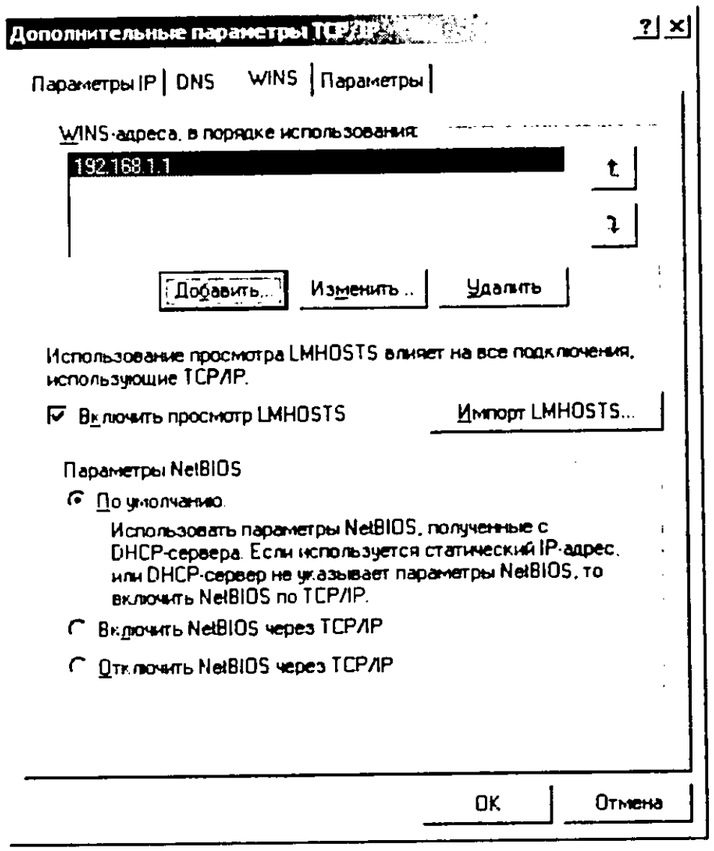


Рис. 10.5. *Конфигурация WINS в Windows 2000/XP*

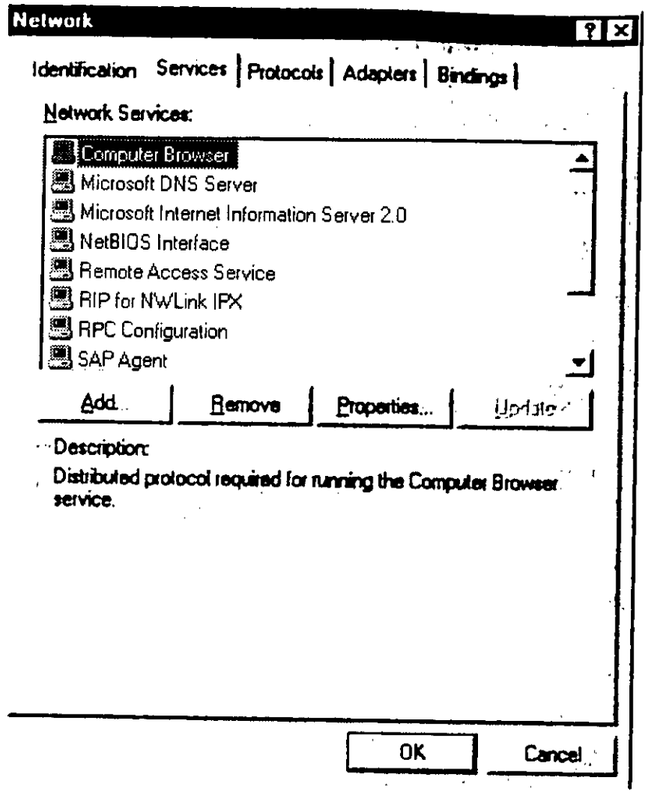


Рис. 10.6. *Сетевые службы*

Затем нажмите кнопку **Add** (**Добавить**) и выберите из списка службу **Windows Internet Name Service** (рис. 10.7). Система попросит вас ввести имя дистрибутивного каталога Windows NT Server. После этого нажмите Ok. Система попросит перезагрузить компьютер — без этого никак.

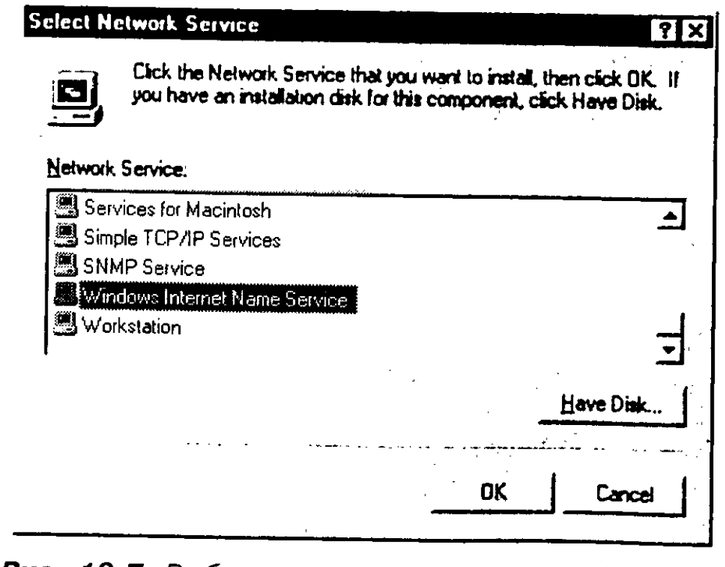


Рис. 10.7. *Выбор устанавливаемой сетевой службы*

После перезагрузки системы выполните команду меню **Start** → **Programs** → **Administrative Tools (Common)** → **WINS Manager**. Окно программы WINS Manager при первом запуске будет выглядеть так, как показано на рис. 10.8:

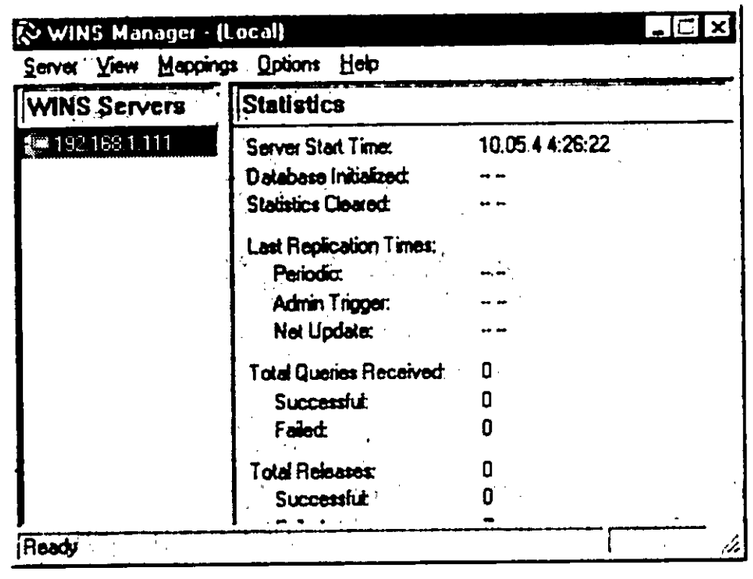


Рис. 10.8. *WINS Manager*

Для начала просмотрим базу данных ресурсов WINS: выполните команду меню **Mappings** → **Show database** (рис. 10.9).

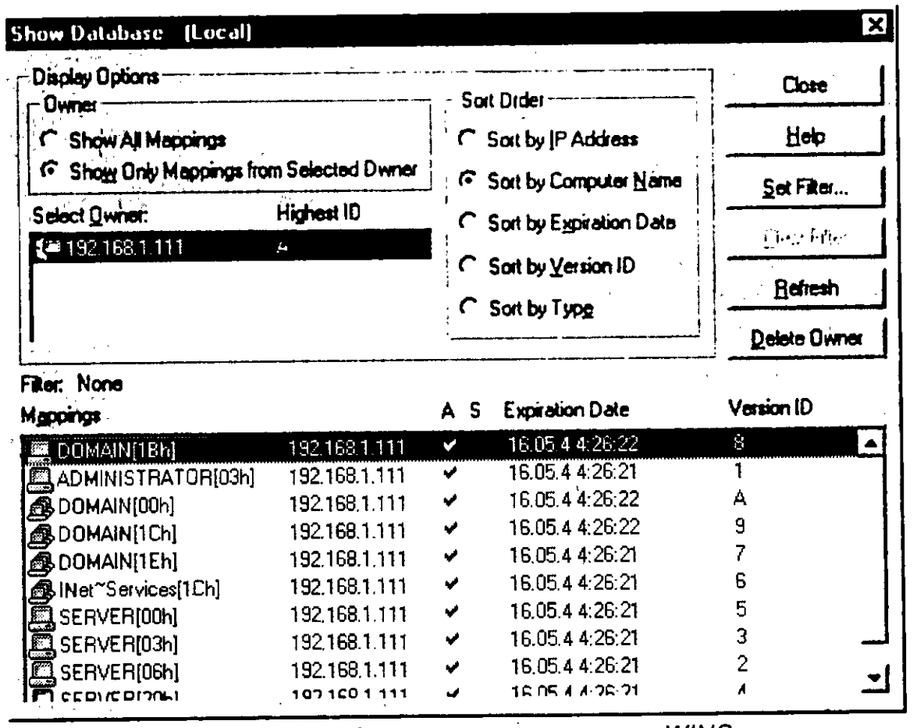


Рис. 10.9. *База данных ресурсов WINS*

Как вы уже знаете, ресурсом сети Microsoft является домен, рабочая группа, пользователь, компьютер и т.д. В окне **Show database** отображаются все эти ресурсы, но возле каждого стоит определенный код. Данный код — это зарезервированное имя службы. Список зарезервированных имен представлен в табл. 10.2.

Зарезервированные имена NetBIOS *Таблица 10.2*

Зарезервированное имя	Описание
Имя_компьютера[00h]	Данное имя зарезервировано для службы «Рабочая станция» клиента WINS
Имя_компьютера[03h]	Это имя зарезервировано для службы Messenger клиента WINS
Имя_компьютера[20h]	Данное имя зарезервировано для службы «Сервер» клиента WINS
Имя_пользователя[03h]	Имя, под которым пользователь зарегистрирован в системе
Имя_домена[1bh]	Имя домена, зарегистрированное главным контроллером домена (PDC)

Некоторые узлы вашей сети могут не поддерживать службу WINS. Как правило, операционные системы данных узлов не поддерживают WINS. К таким операционным системам можно отнести:

- Операционную систему DOS с системой LAN Manager, младше версии 2.2.
- Операционную систему Linux без пакета Samba.
- Операционную систему UNIX со старой версией системы LAN Manager.

Для таких узлов нужно задать статические записи в базе данных службы WINS. Для этого в меню **WINS Manager** выберите команду **Mappings → Static Mappings**. В появившемся окне (рис. 10.10) нажмите кнопку **Add Mappings**. Затем введите имя узла, его IP-адрес, а также выберите тип имени (рис. 10.11).

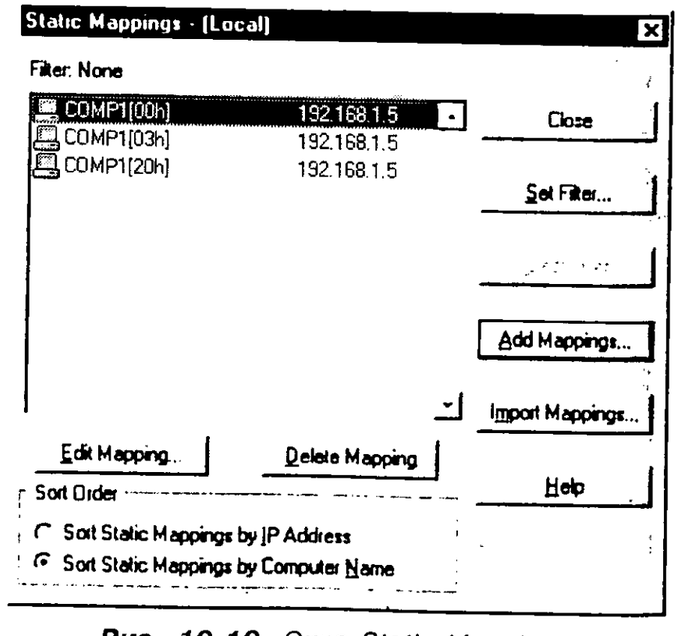


Рис. 10.10. *Окно Static Mappings*

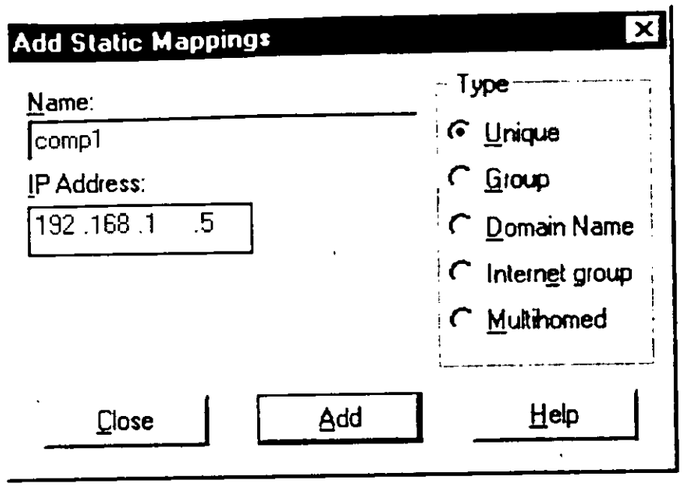


Рис. 10.11. *Добавление статической записи*

Завершим процесс добавления статических записей, нажмите кнопку **Close**. Сейчас нужно поговорить о типе узла:

- **Unique** — уникальное имя, которое соответствует одному IP-адресу.
- **Group** — IP-адреса членов группы не хранятся в базе данных WINS, для взаимодействия с членами группы используется широковещание. Если ваша цель — снизить сетевой трафик за счет сокращения широковещания, не используйте этот тип записи.
- **Domain name** — имя домена, группа доменов может содержать до 25 IP-адресов.
- **Internet Group** — позволяет задать межсетевую группу с целью добавления в нее общих сетевых ресурсов (например, принтеров) с целью упрощения их поиска. Такая группа может содержать не более 25 членов.
- **Multihomed** — применяется для компьютера с несколькими сетевыми интерфейсами, но одним уникальным именем. Обычно можно использовать для UNIX-маршрутизатора, не являющимся клиентом WINS.

Служба DHCP — автоматическое управление IP-адресами и настройками устройств сети

11.1. Что такое DHCP и для чего он нужен?

DHCP — это протокол настройки узла, который автоматически назначает IP-адреса компьютерам. Настроенный DHCP-сервер централизовано назначает IP-адреса в вашей сети и автоматически конфигурирует рабочие станции. Использование DHCP избавит вас от некоторых проблем, проявляющихся при ручной настройке TCP/IP. Во-первых, сразу же исключается проблема дублирования адреса. Например, у вас сеть из 77 компьютеров и вы можете забыть, какой адрес вы использовали, а какой нет.

При использовании DHCP вы просто задаете диапазон, из которого DHCP-сервер будет «раздавать» IP-адреса, а обо всем остальном он позаботится сам. Во-вторых, вам не нужно подходить к каждому компьютеру при его настройке. По умолчанию многие операционные системы ориентированы именно на использование DHCP, а не на ручное конфигурирование. Поэтому вам вообще не придется настраивать клиенты сети.

В-третьих, при конфигурировании клиента сервер DHCP может передавать ему дополнительные параметры, например, IP-адреса DNS- или WINS-серверов, а также IP-адрес шлюза. Фактически, настройка всей сети сводится к правильной настройке DHCP-сервера. Если у вас большая сеть, правильно настроить DHCP — в ваших же интересах, тогда при изменении параметров сети, таких как IP-адреса DNS или WINS-серверов, вам не придется подходить к каждому компьютеру.

Единственное, что может вас отпугнуть от DHCP — это сеть с фиксированным доступом к Internet. Как тогда определить, кто работал в Internet, если IP-адреса каждый день разные? Во-первых, многие прокси-серверы позволяют производить аутентификацию с использованием имени

пользователя, что, с одной стороны, даже надежнее, чем идентификация компьютера по IP-адресу. А во-вторых, если вариант с использованием имен пользователей вас не устраивает, многие прокси-серверы позволяют привязываться к MAC-адресу (аппаратному адресу сетевого адаптера), который является уникальным: в природе нет двух сетевых адаптеров с одинаковым MAC-адресом. Об использовании MAC-адресов и сервера DHCP мы поговорим чуть позже.

Возможно, вы подумали, что в одной сети должен быть только один сервер DHCP, потому что в противном случае между серверами возникнет конфликт, а пострадавшим опять окажется клиент, который зависнет при загрузке. А вот и не так — в одной сети может быть несколько серверов DHCP. И это не только не отразится на производительности сети, но даже повысит надежность сети, если, например, один из серверов выйдет из строя.

Протокол DHCP подробно описан в RFC 1533, 1534, 1541, 1542, а протокол BOOTP описан в RFC 1532.

11.2. Настройка сервера DHCP в Windows NT Server

Требования к серверу DHCP

Настройка DHCP в Windows NT ничуть не сложнее и ничуть не легче, чем в любой другой операционной системе, например, Linux. Настройка сервера DHCP в любой операционной системе заключается в том, что нужно установить сетевой сервер DHCP (в Linux — это демон dhcpd), задать область видимости сервера — диапазон обслуживаемых адресов, задать дополнительные параметры, например, имя сервера DNS, и активизировать настройки.

К серверу DHCP на базе операционной системы Windows NT Server есть определенные требования. Во-первых, сервер DHCP не должен быть первичным контроллером домена. Во-вторых, IP-адрес самого сервера DHCP должен быть статическим, то есть назначенным администратором вручную.

Как уже отмечалось, в одной сети может быть несколько серверов DHCP, и они не будут конфликтовать друг с другом. Если у вас небольшая сеть, скажем, сеть класса C, то одного сервера должно вполне хватить. Если у вас несколько подсетей, желательно организовать DHCP-сервер в каждой подсети.

Установка сервера DHCP

Для установки сетевой службы DHCP нужно выполнить следующие действия. Прежде всего, нужно зарегистрироваться в системе как Administrator. Затем откройте Панель управления и запустите апплет **Сеть** (Network). Перейдите на вкладку **Services** и нажмите кнопку **Add**. В появившемся окне выберите из списка службу **Microsoft DHCP Server** (рис. 11.1).

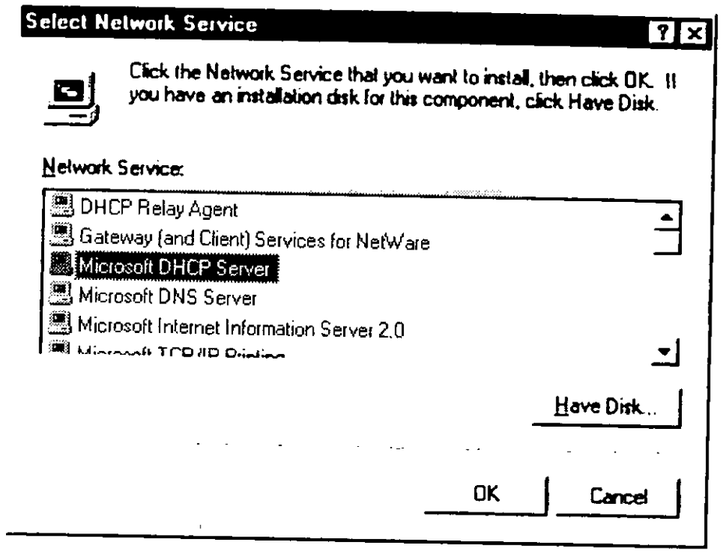


Рис. 11.1. *Установка сетевой службы*

После этого операционная система, как обычно, запросит путь к дистрибутивному каталогу. Укажите его и нажмите кнопку Ок. Потом система отобразит сообщение о том, что если некоторые сетевые адаптеры используют DHCP, то нужно задать для них статические адреса — до настройки DHCP-сервера (рис. 11.2). Так как у нас до этого не было сервера DHCP, следовательно, ни один из компьютеров сети его не использовал, это сообщение можно проигнорировать.

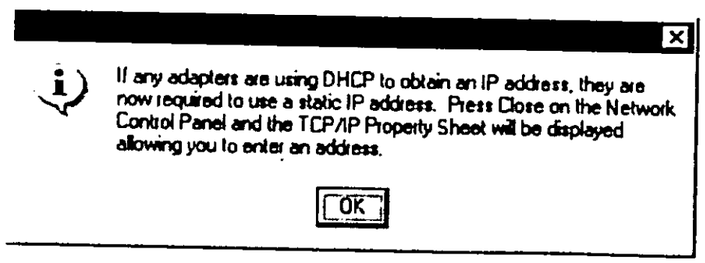


Рис. 11.2. *Требование задать статические IP-адреса*

Настройка DHCP

Перезагрузите компьютер, а после перезагрузки, зарегистрировавшись как Administrator, запустите утилиту **DHCP Manager** (**Start → Programs → Administrative Tools (Common) → DHCP Manager**). При первом запуске вы увидите окно, показанное на рис. 11.3.

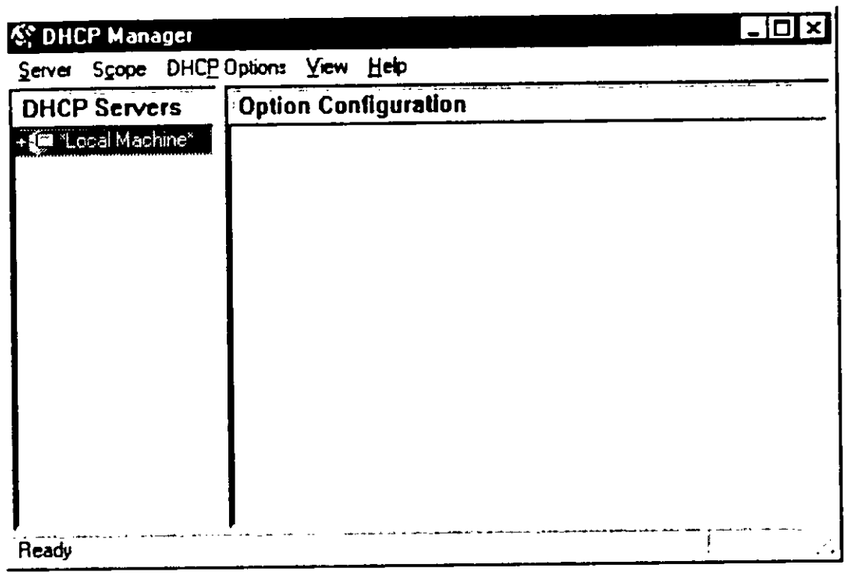


Рис. 11.3. *Окно DHCP Manager*

Теперь можно приступить непосредственно к настройке. Дважды щелкните на ***Local Machine*** в левой части окна DHCP Manager и выполните команду меню **Scope → Create**. Вы увидите окно **Create Scope**, в котором нужно будет указать следующие параметры (рис. 11.4):

- **Start Address** — начальный адрес области видимости DHCP-сервера, например, 192.168.1.10 — это начальный адрес диапазона адресов;
- **End Address** — конечный адрес диапазона адресов;
- **Exclusion Range** — диапазон, который будет исключен из области видимости сервера;
- **Lease Duration** — время действия полученного IP-адреса;
- **Name** — имя диапазона, которое будет отображено в левой части окна DHCP Manager;
- **Comment** — комментарий.

Например, нам нужно, чтобы наш сервер «раздавал» адреса из диапазона 192.168.1.10...192.168.1.24. Установите поле **Start Address** равным первому адресу диапазона, а поле **End Address** — последнему. Но в то же время нам нужно исключить некоторые адреса, например, адреса 192.168.1.13... 192.168.1.16.

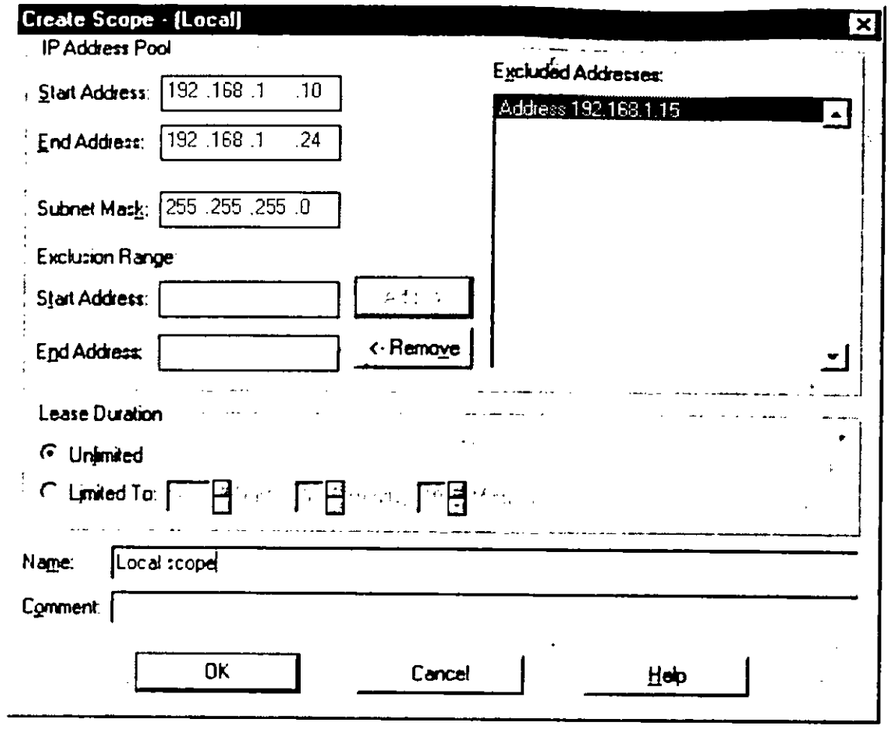


Рис. 11.4. *Создание диапазона*

В области **Exclusion Range** установите поле **Start Address** равным 192.168.1.13, а поле **End Address** — 192.168.1.16, затем нажмите кнопку **Add**. Если нужно исключить только один адрес, введите его в поле **Start Address** и нажмите кнопку **Add**. Для удаления адреса из исключаемого диапазона используется кнопка **Remove**.

В области **Lease Duration** можно указать время действия полученного IP-адреса:

- **Unlimited** — без ограничения времени;
- **Limited to** — можно указать количество дней, часов и минут, на протяжении которых клиент может распоряжаться полученным адресом.

После того как вы нажмете кнопку Ок, программа спросит вас, хотите ли вы активизировать созданный диапазон. По умолчанию созданный диапазон не активизируется, поэтому нажмите кнопку **Yes**. Не нажимайте «Enter», поскольку ответ по умолчанию — **No**, чтобы не получилось такой ситуации, что будто бы активизировали диапазон, а ничего не работает.

Примечание.

Активизировать или деактивизировать диапазон можно с помощью соответствующих команд меню Scope окна DHCP Manager.

После создания и активизации диапазон будет выглядеть так, как показано на рис. 11.5.

На этом настройка не заканчивается — нам нужно указать дополнительные параметры, а именно IP-адреса шлюза и сервера DNS.

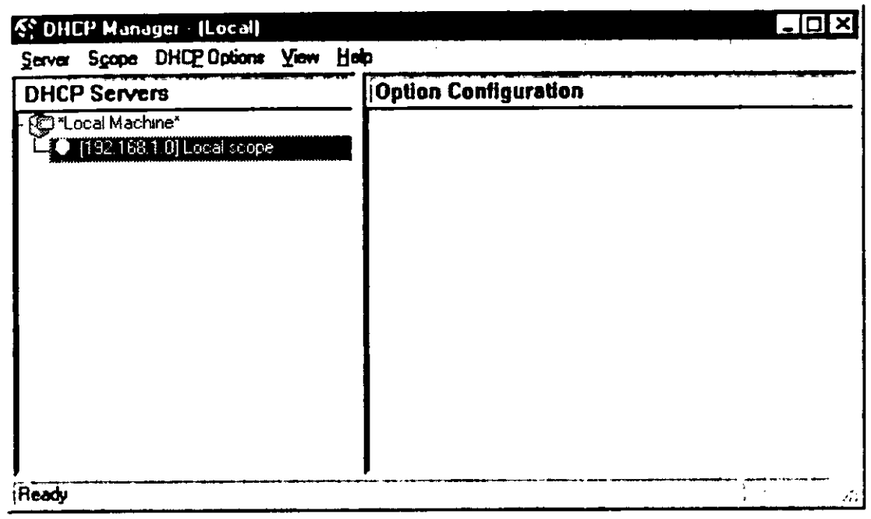


Рис. 11.5. *Только что созданный диапазон*

Для этого в меню **DHCP Options** выберите команду **Scope**. Данная команда изменяет параметры выделенного диапазона. Команда **Global** изменяет глобальные параметры сервера, а команда **Default** задает значения опций по умолчанию.

В левой части окна DHCP Options (рис. 11.6) выберите опции:

- 003 Router;
- 006 DNS Servers.

Можно выбрать другие опции, например, WINS/NBNS Servers, но мы этого делать не будем. Еще довольно полезной в сетях Microsoft оказывается опция **Domain Name**, позволяющая задать имя домена.

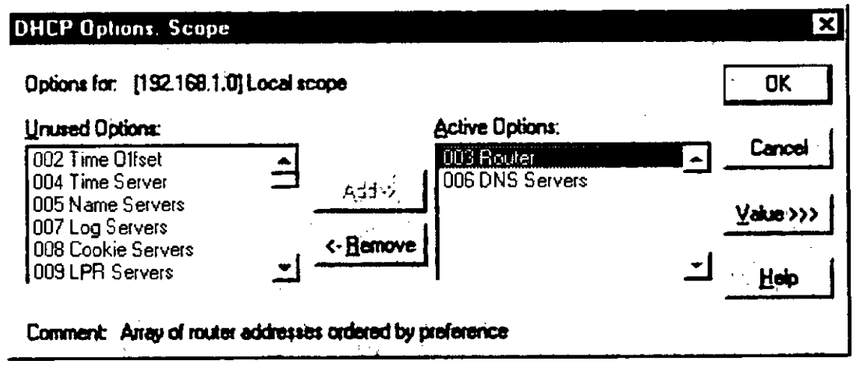


Рис. 11.6. *Опции диапазона*

В правой части окна выделите опцию **003 Router** и нажмите кнопку **Value**, а затем **Edit Array**. В появившемся окне введите IP-адрес шлюза и нажмите кнопку **Add**, затем нажмите кнопку Ok. Если вы не помните IP-адрес шлюза, а помните имя, можно указать имя в поле **Server name**, а затем нажать кнопку **Resolve**.

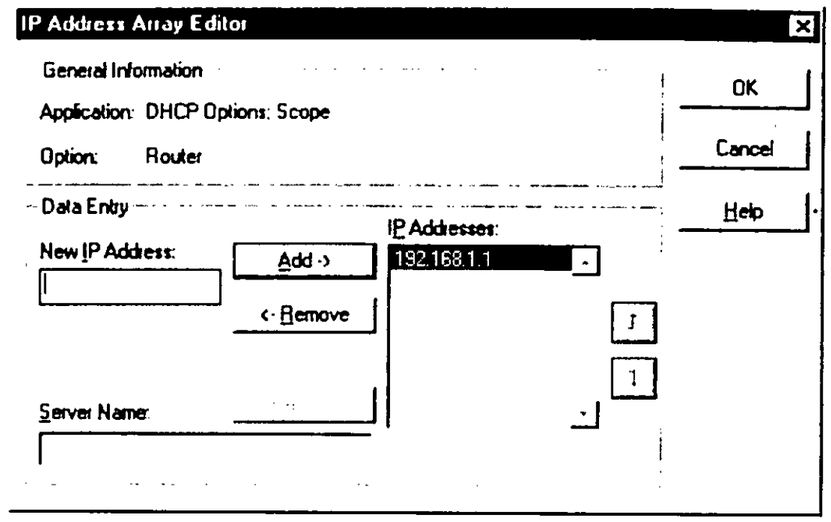


Рис. 11.7. *Опции диапазона — 003 Router*

«Бронирование» IP-адресов

Как и билеты на самолет, IP-адреса можно «забронировать». Бронирование IP-адреса позволяет назначить один и тот же IP-адрес одному и тому же клиенту. Как правило, идентификация клиентов выполняется по MAC-адресу сетевого адаптера, который уникален.

Для резервирования IP-адреса выполните команду **Scope → Add reservation**. В появившемся окне (рис. 11.8) нужно ввести IP-адрес, MAC-адрес, имя клиента и комментарий.

Узнать MAC-адрес можно с помощью утилиты **TCPNetView**, которая описана в пункте, посвященном Linux, или же с помощью программы **ipconfig**, запущенной на компьютере, адрес для которого нужно зарезервировать. MAC-адрес нужно вводить без дефисов.

Если у вас несколько DHCP-серверов, и все они используют одну и ту же резервацию, клиент гарантировано получит свой IP-адрес.

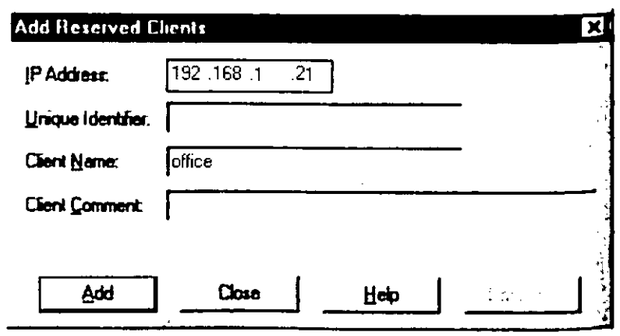


Рис. 11.8. *Бронирование IP-адреса*

11.3. Настройка сервера DHCP в Windows 2000/2003 Server

Установка сервера

Настройка DHCP-сервера в Windows 2000/2003 Server значительно проще, в основном благодаря улучшенному интерфейсу пользователя Windows 2000 Server. В этом вы убедитесь сами — на настройку DHCP-сервера вы потратите не более пяти минут, не считая времени, затраченного на установку самого сервера.

Установка сервера выполняется не через апплет **Сеть (Network)**, как в Windows NT, а с помощью аплета **Add/Remove Programs (Установка и Удаление программ)** с Панели управления. Запустите этот апплет и перейдите в раздел **Windows Components**. В окне **Windows components wizard** (рис. 11.9) выберите **Networking services** и нажмите кнопку **Next**.

Затем выберите **Dynamic Host Configuration Protocol (DHCP)** и нажмите **Next** (рис. 11.10).

После установки DHCP желательно перезагрузить компьютер. После перезагрузки зарегистрируйтесь в системе как Administrator и запустите утилиту **DHCP,** показанную на рис. 11.11. Для этого выполните **Start → Programs → Administrative Tools → DHCP** или **Start → Settings → Control Panel → Administrative Tools → DHCP**.

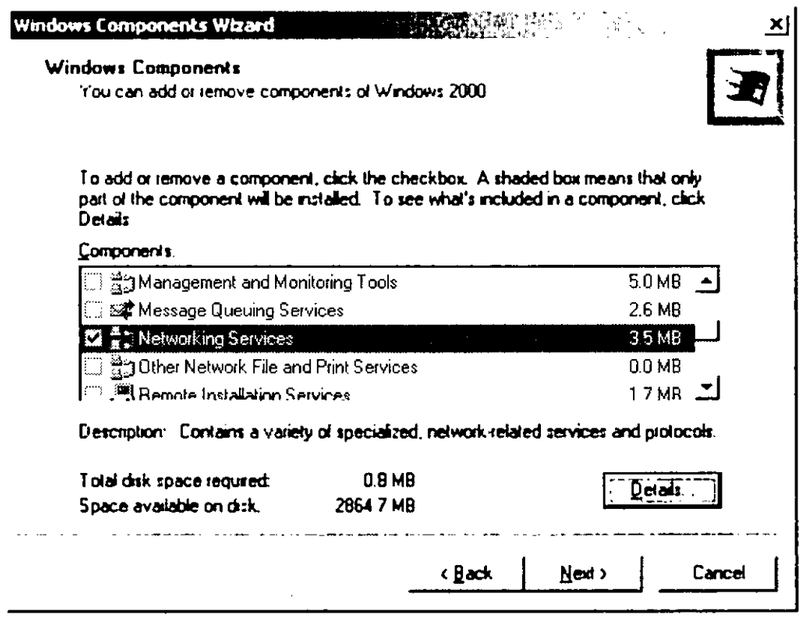


Рис. 11.9. *Окно Windows components wizard*

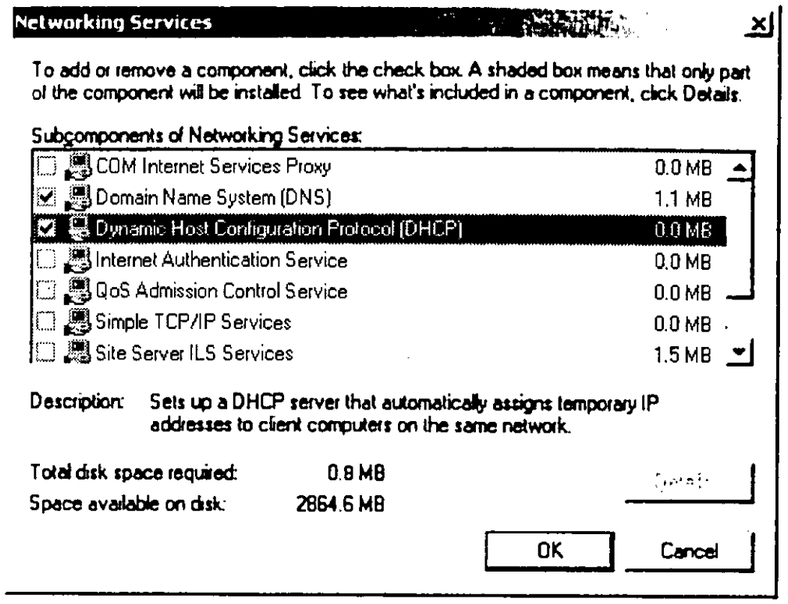


Рис. 11.10. *Установка DHCP*

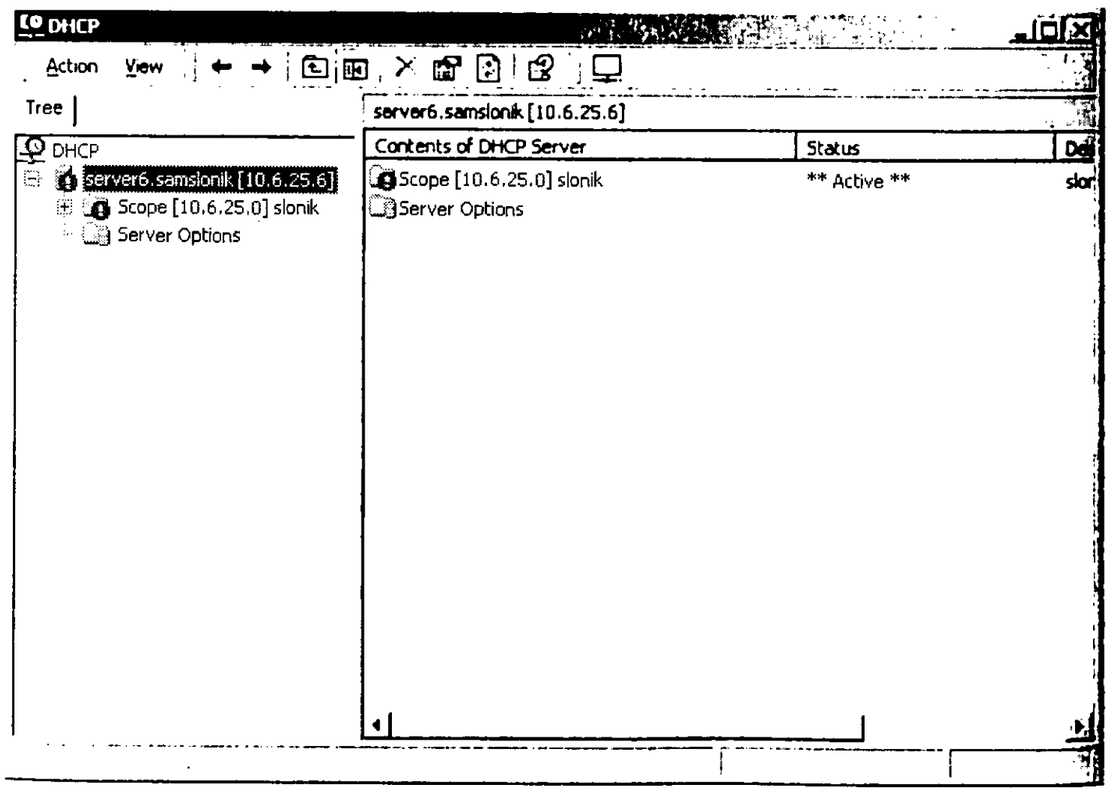


Рис. 11.11. *Утилита DHCP*

Создание диапазона

Для добавления диапазона выделите сервер и выполните команду меню **Action → New scope**. Затем нужно будет ввести имя диапазона, комментарий и нажать **Next**. В следующем окне нужно ввести параметры самого диапазона — начальный и конечный адреса и маску подсети (см. рис. 11.12).

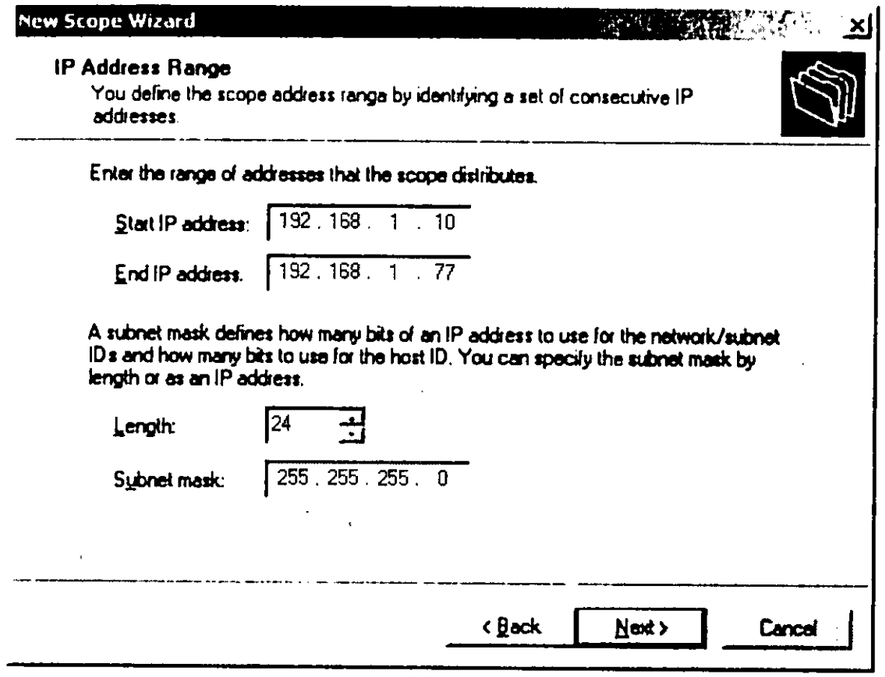


Рис. 11.12. *Параметры диапазона*

В следующем окне нужно ввести исключения из диапазона — IP-адреса отдельных компьютеров или целые диапазоны IP-адресов, как это мы делали в Windows NT. Исключения могут понадобиться для компьютеров, для которых IP-адреса назначены статически, например, если операционная система компьютера не поддерживает DHCP или же по другой причине (рис. 11.13).

Затем нужно указать время действия IP-адреса: дни, часы, минуты. После этого программа спросит вас, не желаете ли вы указать дополнительные опции: соглашайтесь. Программа предложит вам указать IP-адрес шлюза (шлюзов) и серверов WINS (рис. 11.14).

Последний вопрос программы — активизировать диапазон или нет. Тут уж решайте сами — нужен вам в данный момент сервер или вы хотите запустить его позже.

Наверное, вам захочется указать опцию **006 DNS Servers**, чтобы на всех DHCP-клиентах вашей сети автоматически «прописывались» DNS-серверы вашей сети. Для этого выделите диапазон и выполните команду

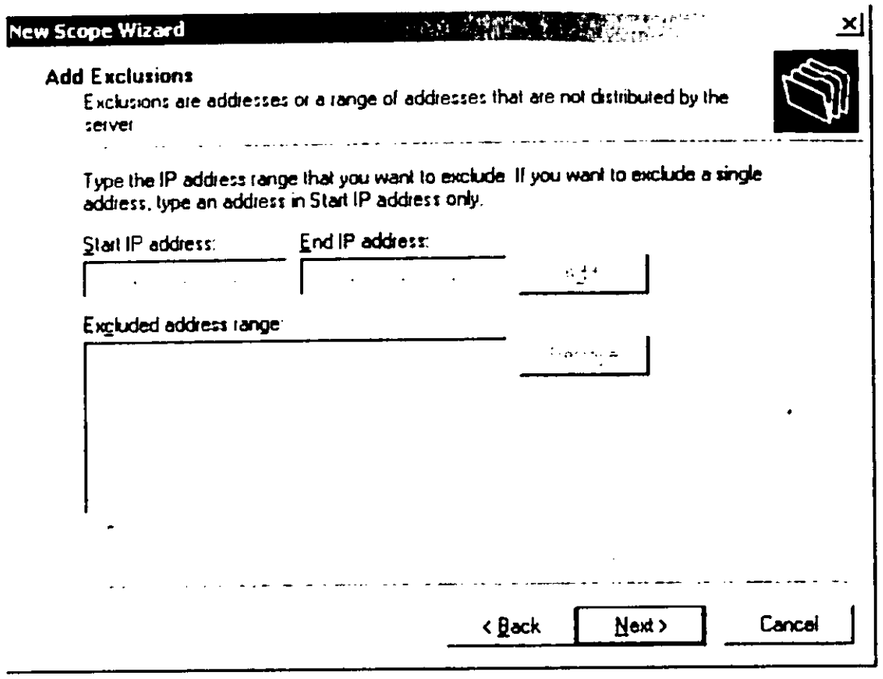


Рис. 11.13. *Исключения*

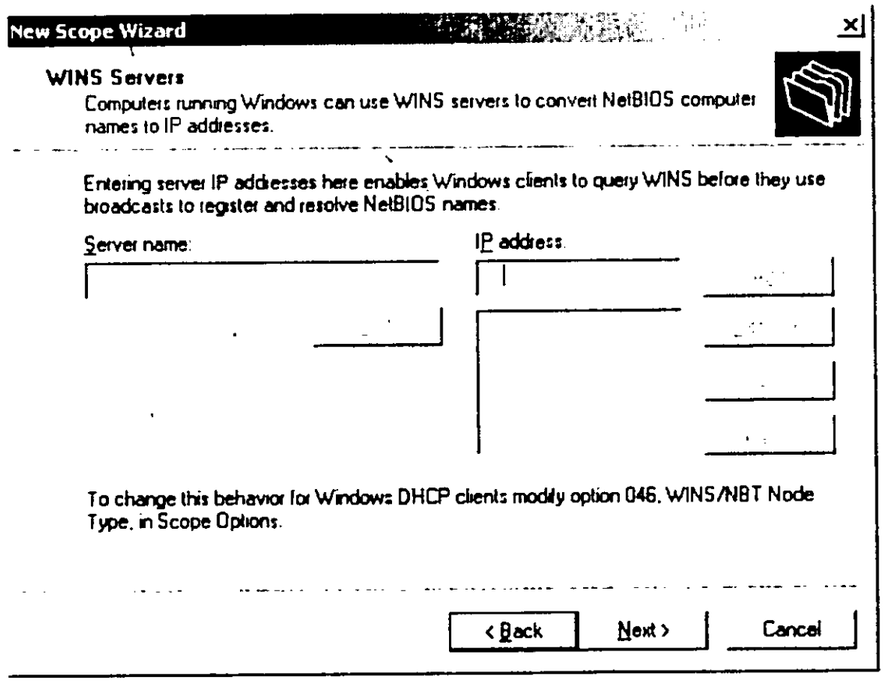


Рис. 11.14. *Задание WINS-сервера*

меню **Action → Configure Options**. В появившемся окне (рис. 11.15) вы сможете сконфигурировать дополнительные опции — сервер DNS, сервер имен и др.

На этом настройка DHCP-сервера завершена.

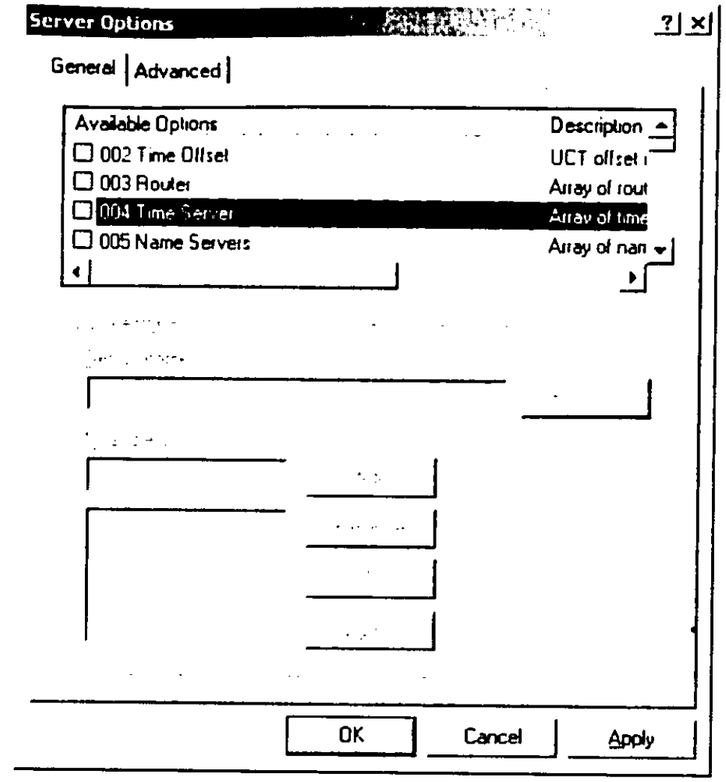


Рис. 11.15. *Дополнительные опции*

11.4. Настройка DHCP в Linux

11.4.1. Состав и установка DHCP

DHCP в Linux реализован в виде демона сервера (**dhcpd**) и демона клиента (**dhcpcd** или **pump** (в Red Hat)). Демон **dhcpd** запускается на сервере и непосредственно отвечает за назначение и отбор IP-адресов клиентам, при входе и выходе их из сети. Клиентский демон, как явствует из названия, запускается на стороне клиента.

DHCP при установке Linux обычно не устанавливается, однако входит в состав дистрибутивов. В любом случае вы всегда можете скачать последнюю версию с сайта `www.isc.org`. Установите пакет **dhcp** и включите поддержку динамических IP-адресов командой **echo «1» > /proc/sys/net/ipv4/ip_dynaddr.**

Конфигурационным файлом для **dhcpd** является `/etc/dhcpd.conf`. При запуске DHCP-сервера происходит выделение IP-адресов согласно содержащимся в файле `/etc/dhcpd.conf` установкам. Выделенные адреса **dhcpd** регистрирует в файле `dhcpd.leases`, который обычно находится в каталоге `/var/dhcpd`.

11.4.2. Простейшая конфигурация DHCP

Сейчас давайте рассмотрим простейшую конфигурацию, которую будем постепенно наращивать (см. листинг 11.1). Описание опций приведено непосредственно в самом листинге. Обратите внимание на то, что, чтобы внесенные вами в файл `/etc/dhcp.conf` изменения вступили в силу, демон **dhcpd** необходимо остановить и запустить снова. При этом используйте команду **/etc/rc.d/init.d/dhcpd stop** для останова демона и команду **/etc/rc.d/init.d/dhcpd start** для его запуска.

Листинг 11.1. Файл /etc/dhcpd.conf

```
# описание сети, указывающее какая из подсетей будет
# обслуживаться. Указывается сетевой адрес и маска сети
subnet 192.168.1.0 netmask 255.255.255.0 {

# маршрутизатор по умолчанию
option routers 192.168.1.1;

# маска подсети 255.255.255.0
option subnet-mask 255.255.255.0;

# установка домена по умолчанию и сервера NIS,
# если таковой используется
option nis-domain «domain.ua»;
option domain-name «domain.ua»;

# адрес DNS сервера, который будут использовать клиенты
option domain-name-servers 192.168.1.1;

# диапазон, из которого будут назначаться IP-адреса
# для клиентов
# 192.168.1.50-192.168.1.250
range 192.168.1.10 192.168.1.254;

# сказать клиентам, чтобы отдали адрес через 21600 секунд
# (6 часов)
# после получения адреса
default-lease-time 21600;

# забрать адрес самому через 28800 секунд (8 часов)
max-lease-time 28800;
}
```


11.4.3. Расширенные настройки DHCP

Назначение статических адресов

Теперь будем постепенно усложнять конфигурацию. Существуют ситуации, когда определенным клиентам при их подключении должен выделяться один и тот же фиксированный IP-адрес. С помощью DHCP это можно сделать, если знать MAC-адрес клиента. MAC-адрес — это уникальный адрес, который имеет каждая сетевая карточка. Этот адрес индивидуален для каждой сетевой карты и назначается ей при изготовлении. Чтобы связать какой-то MAC-адрес с определенным IP-адресом, используется конструкция **host**:

```
host myhost {
hardware ethernet xx:xx:xx:xx:xx:xx;
fixed-address 192.168.1.9;
}
```

Ее нужно вставить в ту конструкцию подсети **subnet**, которой принадлежит назначаемый IP-адрес. Данная конструкция означает, что компьютеру с аппаратным адресом xx:xx:xx:xx:xx:xx будет назначен IP-адрес 192.168.1.9. Например:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    # прочие опции
    # …
    #
    host myhost {
        hardware ethernet 00:40:C7:34:90:1E;
        fixed-address 192.168.1.9;
            }
```

Данный пример показывает, что аппаратному адресу 00:40:C7:34:90:1E будет сопоставлен IP-адрес 192.168.1.9. Обратите внимание, что IP-адрес хоста myhost 192.168.1.9 относится к подсети 192.168.1.0 и включен в инструкцию **subnet** подсети 192.168.1.0, а не какой-либо другой сети!

Встает вопрос: «Как узнать MAC-адрес клиента?». Существует довольно удобная утилита для просмотра всех MAC-адресов сетевых адаптеров в вашей сети — программа **TCPNetView**. Эта программа разработана Александром Горлачем и загрузить ее вы можете по адресу `http://www.enet.ru/~gorlach/netview/`. Правда, есть одно «но»: эта программа работает под Windows. В любом случае, если вы будете использовать эту программу, при настройке сервера вам не придется подходить к каждо-

му компьютеру, чтобы узнать его MAC-адрес. Существуют также и утилиты под Linux, способные показать сразу все MAC-адреса, например, **Trafshow**. Но по сравнению с Trafshow, TCPNetView несколько удобнее (см. рис. 11.16).

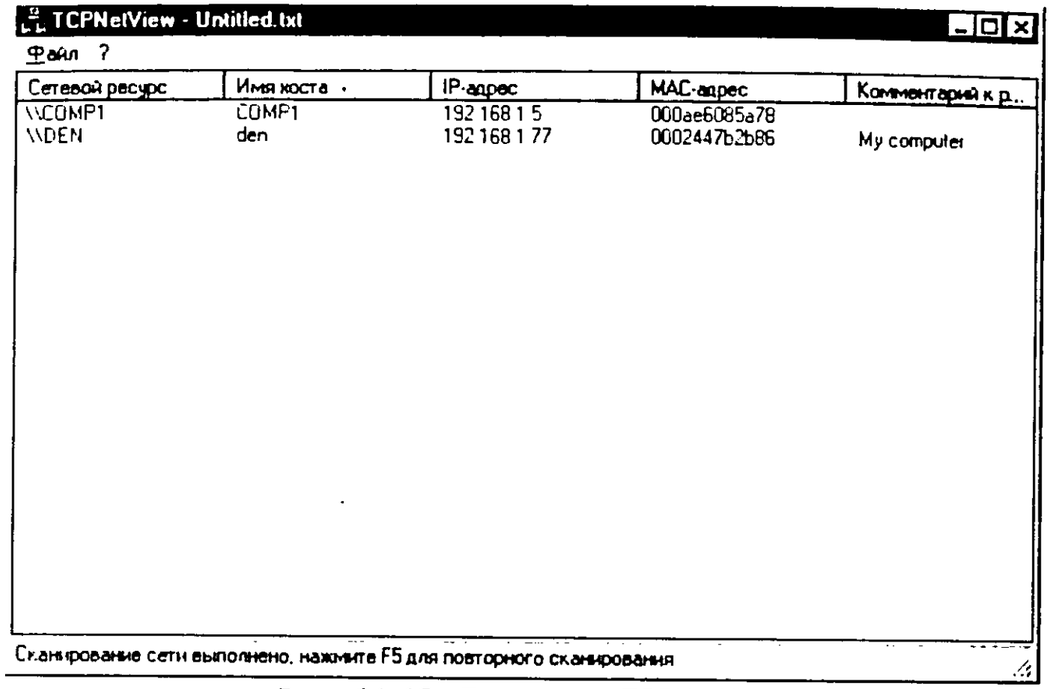


Рис. 11.16. *Программа TCPNetView*

Поддержка WINS

Теперь предположим, что вам необходимо обеспечить поддержку **WINS**, а на вашей машине установлен сервер **Samba**. В этом случае в конструкцию **subnet** нужно включить следующие директивы:

```
option netbios-name-servers 192.168.1.1;
option netbios-dd-server 192.168.1.1;
option netbios-node-type 8;
```

Примечание.

Служба **WINS** (Windows Internet Name Service) используется для разрешения (перевода) имен **NetBIOS** в IP-адреса. Сервер **WINS** — это усовершенствованный сервер имен **NetBIOS**, разработан Microsoft для снижения широковещательного трафика.

Пакет **Samba** предназначен для использования протокола **SMB** (Server Message Block), который также еще называется протоколом **NetBIOS**. С помощью пакета **Samba** ваша машина, работающая под управлением Linux, ничем не будет отличаться от рабочей станции или сервера сети Microsoft.

Вот практически и все. Правда, еще можно добавить пару незначительных опций:

```
# определяем широковещательный адрес
option broadcast-address 192.168.2.255;

# включаем IP-Forwarding
option ip-forwarding on;

# можно добавить глобальную опцию:
server-identifier server.domain.ua;
```

Дополнительную информацию можно получить, введя команду **man dhcpd.conf**.

Расширенная версия файла dhcpd.conf

Окончательный вариант конфигурационного файла приведен в листинге 11.2.

Листинг 11.2. Конфигурационный файл /etc/dhcpd.conf (окончательный вариант)

```
# Подсеть 192.168.1.0, маска сети 255.255.255.0
subnet 192.168.1.0 netmask 255.255.255.0 {

# маршрутизатор по умолчанию
option routers 192.168.1.1;

# маска подсети 255.255.255.0
option subnet-mask 255.255.255.0;

# установка домена по умолчанию и сервера NIS,
# если таковой используется
option nis-domain «domain.ua»;
option domain-name «domain.ua»;

# задание широковещательного адреса
option broadcast-address 192.168.2.255;

# включение IP-Forwarding
option ip-forwarding on;
```

```
# глобальная опция server-identifier:
server-identifier server.domain.ua;

# адрес DNS сервера, который будут использовать клиенты
option domain-name-servers 192.168.1.1;

# диапазон адресов для клиентов
# 192.168.1.50-192.168.1.250
range 192.168.1.10 192.168.1.254;

# сказать клиентам, чтобы отдали адрес
# через 21600 секунд (6 часов)
# после получения адреса
default-lease-time 21600;

# забрать адрес самому через 28800 секунд (8 часов)
max-lease-time 28800;
option netbios-name-servers 192.168.1.1;
option netbios-dd-server 192.168.1.1;
option netbios-node-type 8;

#описание трех клиентов клиентов (dhcp50, dhcp51, dhcp52)
# и их аппаратных адресов
     host dhcp50 {
         hardware ethernet 00:40:C7:34:90:1E;
# обратите внимание на то, что вы должны использовать
# IP-адрес из указанного
# ранее диапазона адресов 192.168.1.50-250.
         fixed-address 192.168.1.50;
                  }
     host dhcp51 {
         hardware ethernet 00:40:C7:34:90:1F;
         fixed-address 192.168.1.51;
                  }
     host dhcp52 {
         hardware ethernet 00:40:C7:34:90:2A;
         fixed-address 192.168.1.52;
                  }
}
```


11.5. DHCP-клиенты

Если в вашей сети все IP-адреса прописаны статически, то толку от настройки DHCP-сервера не будет: ни один клиент к нему не обратится, и он будет работать вхолостую. Чтобы клиенты могли получать IP-адреса от DHCP-сервера, нужно настроить протокол TCP/IP определенным образом.

В Windows 9x/ME

В Windows 9x/ME откройте апплет **Сеть** с Панели Управления, затем откройте свойства протокола TCP/IP. На вкладке IP-адрес установите режим **Получить IP-адрес автоматически**. Все, нажмите Ок и перезагрузите компьютер.

В Windows NT

В Windows NT отройте апплет **Сеть (Network)** с Панели управления и перейдите на страничку **Protocols**. Выделите протокол TCP/IP и нажмите кнопку **Свойства (Properties)**. В окне свойств TCP/IP выберите опцию **Получить IP-адрес с сервера DHCP** и нажмите Ок. После этого перезагрузите компьютер.

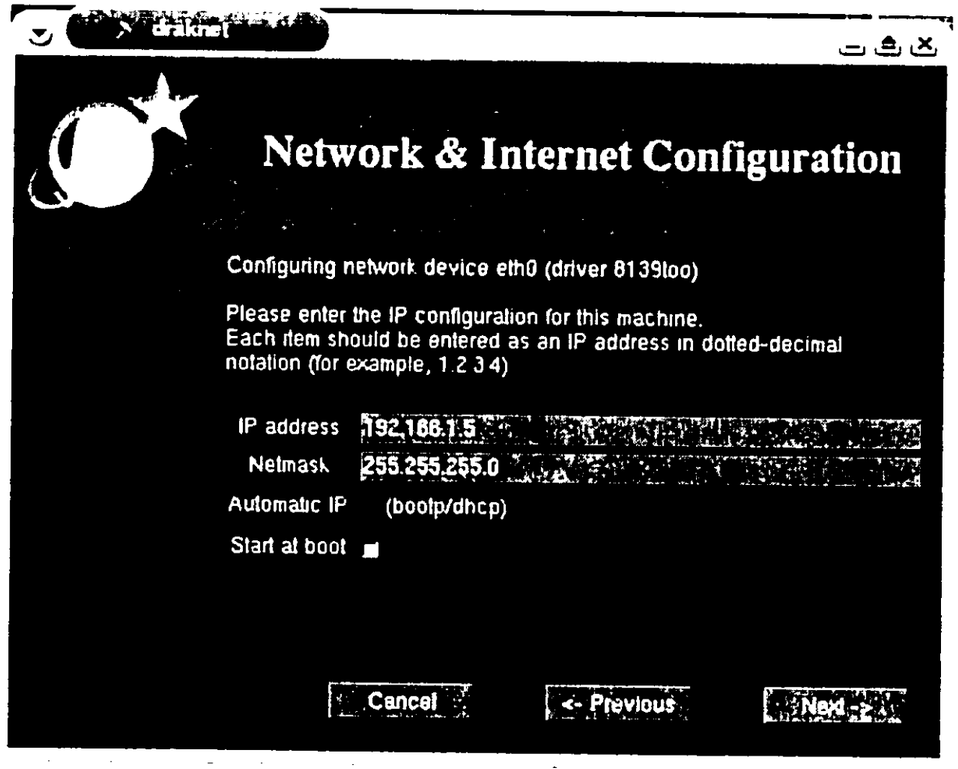


Рис. 11.17. *Конфигуратор draknet*

В Windows 2000

В Windows 2000 откройте папку **Сеть и удаленный доступ к сети**. Выберите **Соединение по локальной сети**, щелкнув по нему правой кнопкой мыши. Из появившегося меню выберите **Свойства**. Выберите протокол TCP/IP и нажмите кнопку **Свойства**. В окне **Свойства: Протокол Интернета (TCP/IP)** выберите **Получить IP-адрес автоматически**. Затем нужно перезагрузить компьютер.

В Windows XP

В Windows XP откройте панель управления и запустите апплет **Сетевые подключения**. Выберите подключение по локальной сети, затем выберите протокол TCP/IP и нажмите кнопку **Свойства**. Дальше нужно выбрать опцию **Получить IP-адрес автоматически**.

В Linux

В Linux запустите конфигуратор сети, например, **draknet** (см. рис. 11.17) и выберите использование протокола DHCP вместо статического указания IP-адреса (Automatic IP).

Как сделать так, чтобы в одной сети были и Windows-машины и Linux-машины

В этой главе вам предстоит настроить пакет **Samba**, предназначенный для использования протокола **SMB** (Server Message Block), который также еще называется протоколом **NetBIOS**. С помощью пакета Samba ваш компьютер, работающий под управлением Linux, ничем не будет отличаться от рабочей станции или сервера сети Microsoft. Дополнительную документацию по этому поводу можно найти по адресу `http://www.samba.org`, а также на всевозможных форумах.

С помощью Samba вы сможете следующее:

- Предоставлять доступ к разделам Linux для рабочих станций Windows.
- Получать доступ к ресурсам сети Microsoft.
- Распечатывать документы на сетевых принтерах сети Microsoft, а также позволить использовать свой принтер в качестве сетевого.

12.1. Установка Samba

При установке, на первом этапе, нужно установить пакеты **samba**, **samba-common** и **samba-client**:

```
# rpm -ih /mnt/cdrom/Mandrake/RPMS/samba*
```

При этом, если вы используете другой дистрибутив (не Mandrake, как указано в примере), перейдите в нужный каталог.

Серверный пакет **samba** состоит из двух основных программ — **smbd** и **nmbd**. Первая из них является носителем протокола **SMB**, а вторая обеспечивает поддержку имен **NetBIOS**. Сразу же после их настройки ваш компьютер будет отображаться в сети.

После установки сервисы **smbd** и **nmbd** конфигурируются как автозапускаемые, то есть вам не придется самостоятельно производить никаких действий по их запуску. Возможно, вас не устраивает такой вариант (например, в тех случаях, если обращение к ним будет производиться редко, и вы хотите освободить память). В этой ситуации никто не мешает добавить их в файл конфигурации суперсервера `/etc/xinetd.conf` и запускать «по востребованию». При этом не забудьте только отключить их автозагрузку с помощью конфигуратора системы.

В этой главе будет рассмотрена настройка пакета Samba «вручную», то есть не прибегая к помощи конфигуратора. Вы же можете использовать конфигруатор **netconf** (см. рис. 12.1), но в этом случае есть одно «но»: если вы будете настраивать Samba или любую другую службу сервера в другом дистрибутиве (не Red Hat или Mandrake), привычного вам конфигуратора может и не быть, поэтому вы должны знать хотя бы назначение и расположение системных файлов той или иной службы сервера.

Если же вы все-таки решили использовать конфигуратор, запустите **netconf** и, перейдя на вкладку **Server Tasks**, выберите конфигурирование Samba (см. рис. 12.1).

С помощью конфигуратора **netconf** вы можете полностью настроить пакет Samba — от указания общих параметров (см. рис. 12.2) до определения общих ресурсов (см. рис. 12.3).

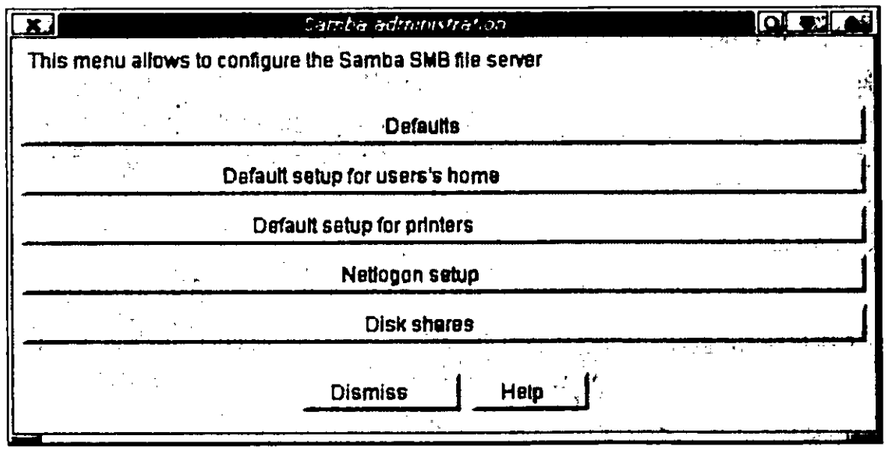


Рис. 12.1. *Конфигурирование Samba*

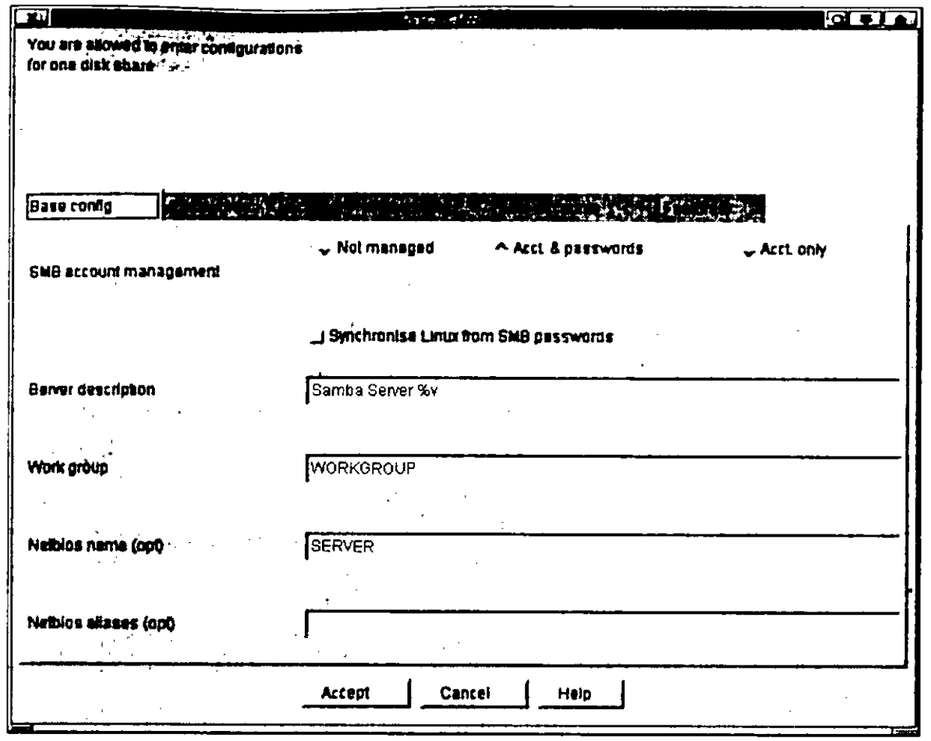


Рис. 12.2. *Общие параметры*

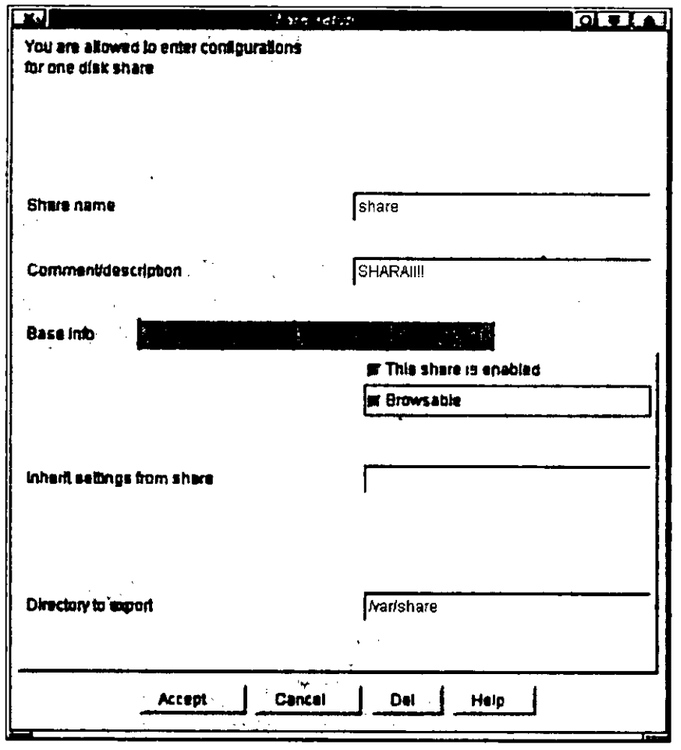


Рис. 12.3. *Определение общих ресурсов*

12.2. Настройка сервера Samba

Основным конфигурационным файлом сервера Samba является файл `/etc/smb.conf`. Именно в нем задаются все используемые и предоставляемые ресурсы. Формат данного файла напоминает формат INI-файла программ для Windows, например `win.ini`.

Файл `/etc/smb.conf` состоит из нескольких секций, в начале каждой из которых в квадратных скобках указывается ее имя. Параметры в каждой секции указываются в виде записей **Имя=Значение**.

Секция [GLOBAL]

Основной является секция **[global]**, ее пример приведен в листинге 12.1.

Листинг 12.1. Пример секции global

```
[global]
workgroup = WORK
comment = Linux Server
guest account = guest
security = share
printing = bsd
printcap name = /etc/printcap
load printers = yes
client code page = 866
character set = koi8-r
encrypt passwords = Yes

log file = /var/log/samba/log.%m
max log size = 50
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
dns proxy = no
wins support = yes
domain master = yes
interfaces = 192.168.1.1/24 192.168.2.1/24
```

Параметр **workgroup** определяет рабочую группу или имя домена NT. Параметр **comment** аналогичен параметру **NT Description** для ОС Windows NT или **Description** (Описание компьютера) для ОС Windows 9x. Параметр **guest account** задает имя пользователя. Указание **guest** в качестве пользователя означает, что пользователи получают доступ без регистрации. Вернее, регистрация все же происходит, но используется гостевая учетная запись.

Следующий параметр — параметр **security** может принимать три значения:

- **share** — при каждом доступе будет запрашиваться имя пользовательского ресурса;
- **user** — для аутентификации будет использоваться имя пользователя и пароль, которые используется для входя в сеть Windows. Это значение используется по умолчанию;
- **server** — для проверки пароля будет использоваться сервер NT.

Записи **printing** и **printcap name** относятся к подсистеме печати. Первая из них задает систему печати типа **BSD**, а вторая — указывает, где расположен файл, содержащий информацию о принтерах. О настройке принтеров мы поговорим немного позже.

Параметры **client code page** и **character set** необходимы для корректного отображения русскоязычных имен файлов файловой системы Windows.

В ОС Windows NT, начиная с Service Pack 3, передача паролей по сети происходит в закодированном виде. Последние версии Samba позволяют поддерживать эту возможность. Для этого нужно установить значение параметра **encrypt password** равным **yes**. Если ваша версия Samba не поддерживает данную возможность, то вы можете отключить использование закодированных паролей в Windows.

Учитывая, что вам придется вручную изменять параметр реестра всех рабочих станций Windows, мне кажется, что проще обновить Samba. Но если вас все же интересует, какой именно параметр реестра Windows нужно изменить, я укажу его:

- В разделе реестра ОС Windows NT: `[NT HKEY_LOCAL_MACHINE\System\Current ControlSet\Services\Rdr\Parameters]` нужно создать ключ **EnablePlainTextPassword** типа DWORD и установить его значение, равное 1.
- В ОС Windows 9x вам нужно создать тот же ключ, но в разделе `[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\Parameters]`.
- В ОС Windows 2000 нужно внести изменения в раздел реестра `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkStation\Parameters]`.

Параметры **log file** и **max log size** определяют имя файла протокола (журнала) и его максимальный размер. Опции сокетов задаются с помощью параметра **socket option**. Прежде, чем задавать опции сокета, рекомендую прочитать справочное руководство по файлу `smb.conf`.

Если в вашем компьютере установлено несколько сетевых интерфейсов, то вы можете сконфигурировать пакет Samba так, чтобы он использовал все интерфейсы. Как это сделал я, показано в листинге 12.1.

Секция [HOMES]

Теперь перейдем к следующей секции, которая определяет параметры совместно используемых ресурсов. Данная секция называется **[homes]**. Пример содержимого этой секции приведен в листинге 12.2.

Листинг 12.2. Секция [homes]

```
[homes]
comment = Home
browseable = yes
writable = yes
```

Параметр **browseable=yes** (см. листинг 12.2) разрешает отображение совместно используемых ресурсов в сети Microsoft. Параметр **writable=yes** разрешает запись в каталоги (вместо этого параметра может использоваться параметр **read only=no**).

Секция [PUBLIC]

Теперь создадим общий каталог (см. листинг 12.3). Делается это в секции **[public]**.

Листинг 12.3. Секция [public]

```
[public]
comment = Public Directory
path = /home/samba
read only = no
```

Практические примеры настройки

Ваших знаний уже достаточно, чтобы самому произвести дальнейшую настройку. В качестве завершения этого раздела я приведу пару практических примеров (см. листинг 12.4). Обратите внимание, что в файле `smb.conf` комментарии могут обозначаться либо решеткой (#), либо точкой с запятой (;).

Листинг 12.4.

```
;  Каталог NETLOGON для входа в домен
[netlogon]
comment = Samba Netlogon Service
path = /var/netlogon
; Не устанавливайте значение yes
case sensitive = no
guest ok = yes
locking = no
writable = yes
browseable = yes

; Профиль для совместно используемых ресурсов
[Profiles]
path = /usr/local/samba/profiles
browseable = no
printable = no
guest ok = yes

; Каталог, используемый пользователем admin
; Пользователь admin должен существовать на сервере Samba
[admin]
comment = admin's directory
path = /home/admin
valid users = admin root
read only = no
```


12.3. Доступ к SMB-ресурсам из Linux

12.3.1. Программа smbclient

Будем смотреть правде в глаза, ОС Windows разрабатывалась для домохозяек. Каждая домохозяйка, чтобы просмотреть ресурсы сети Microsoft, использует пиктограмму «Сетевое окружение» на рабочем столе Windows. А теперь представьте, что эта домохозяйка работает в ОС Linux и хочет просмотреть ресурсы сети. Скорее всего, у нее возникнут определенные трудности. Попробуем их сейчас решить.

Для просмотра ресурсов сети Microsoft используется программа **smbclient**. Допустим, вы хотите подключиться к общему каталогу `share` компьютера `nt_ws1`. При этом допустим, что ваше имя пользователя *user* и пароль *123456*. В этом случае использование команды **smbclient** выглядит следующим образом:

```
$ smbclient //nt_ws1/share -U user%123456
```

Если пароль не нужен, то указывается только имя пользователя без знака процента.

После подключения к общему ресурсу, если точнее, к каталогу, вы можете использовать те же команды, что и при работе с клиентом **ftp** (см. табл. 12.1).

Команды программы smbclient *Таблица 12.1*

Команда	Описание
Dir	Выводит список файлов в каталоге
cd [каталог]	Выполняет переход в заданный каталог на сервере (учтите, что именно на сервере, а не на клиентском компьютере). В том случае, если каталог не указан, то **smbclient** просто выдаст имя текущего каталога
get [файл] [локальное имя]	Получает указанный файл из общего ресурса и сохраняет его на локальном компьютере. Если указано локальное имя, то полученный с сервера файл будет сохранен на клиентском компьютере под этим именем
put [файл] [удаленное имя]	Копирует файл на удаленный компьютер (сервер) и сохраняет его там под именем, указанном в поле удаленное имя. Соответственно, если это имя не указано, то файл при сохранении переименовываться не будет
rm [каталог] **rmdir** [каталог]	Удаляет указанный каталог на удаленном компьютере (сервере)
md [каталог] **mkdir** [каталог]	Создает указанный каталог на удаленном компьютере (сервере)
mput [файлы]	Копирует все указанные файлы на удаленный компьютер (сервер)
del [файлы]	Удаляет на сервере указанные файлы, если, конечно, пользователь обладает на это правами
help	Помощь
exit или **quit**	Завершение сеанса работы программы **smbclient**

12.3.2. Программа smbmount. Доступ через монтирование

Использовать программу **smbclient** не очень удобно. Гораздо удобнее использовать программу **smbmount**, которая умеет монтировать удаленный общий ресурс как обычную файловую систему. При этом впоследствии использовать общий ресурс становится гораздо приятнее и удобнее. Ниже приведен пример команды, которая монтирует общий ресурс `customers` компьютера `nt`, используя имя пользователя *user*. Точка монтирования — каталог `/mnt/customers`, идентификатор пользователя (UID) равен 500, а группы (GID) — 100:

```
smbmount //nt//customers" -U user -c 'mount /mnt/customers
-u 500 -g 100'
```


Для этих же целей можно воспользоваться командой:

```
smbmount //nt/customers/ /mnt/customers -U user
```

Примечание.

Использовать команду **smbmount** имеет право только пользователь root. Для того, чтобы обычный пользователь мог использовать эту программу, следует установить для нее атрибут **Setuid root**, однако такое решение является небезопасным. Выходом из этого положения может послужить запуск программы **smbmount** при загрузке системы. Добавьте в сценарии автозагрузки вызов программы **smbmount** для монтирования файловых систем совместного использования, с которыми вы работаете чаще всего. После этого обычные пользователи смогут работать с удаленными ресурсами как с обычной локальной файловой системой.

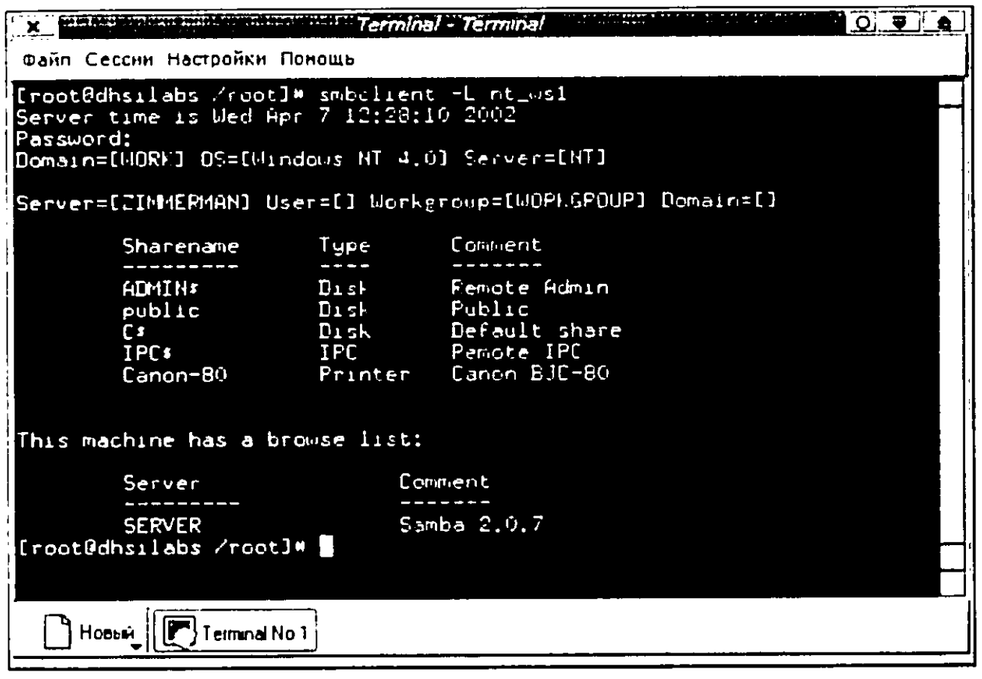


Рис. 12.4. *Общие ресурсы*

Просмотреть общие ресурсы компьютера можно с помощью опции **-L** (см. рис. 12.4). Список **Browse list** (см. рис. 12.4) показывает другие SMB-сервера в сети с доступными ресурсами. Опция **-I** разрешает программе **smbclient** работать с именами DNS. Например, если домен называется `domain.ru`, то просмотреть общие ресурсы компьютера `nt_ws1` можно командой:

```
$ smbclient -L -I nt_ws1.domain.ru
```

12.3.3. Программа LinNeighborhood — правильный выбор

Доступ к совместно используемым ресурсам осуществляется с помощью программ **smbclient** и **smbmount**. Как их использовать, вы уже знаете. Не очень удобно, не правда ли? Конечно, если вы работаете в текстовом режиме и система **X Window** у вас не установлена — другого выхода у вас нет. Но если **X Window** у вас установлена, бороздить просторы сети Microsoft гораздо приятнее с помощью программы **LinNeighborhood** (**Сетевое окружение Linux**).

Установите программу **LinNeighborhood** (пакет и имя команды для запуска называются так же). Запустите ее и наслаждайтесь!

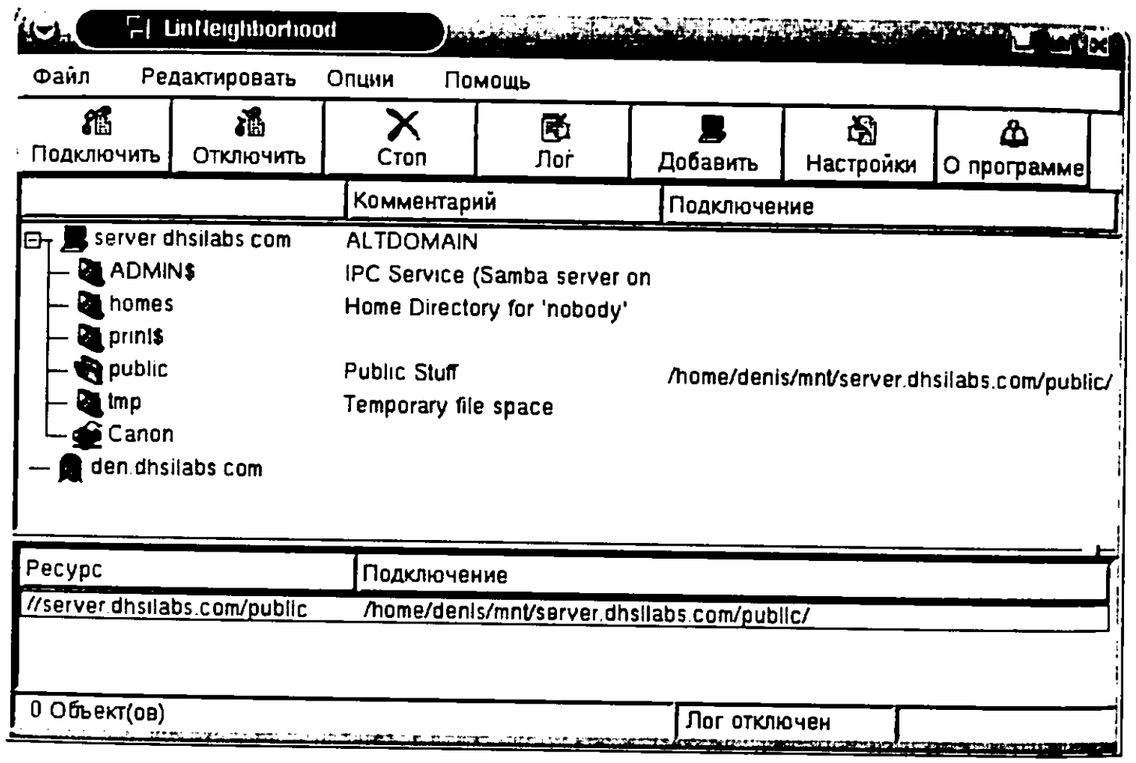


Рис. 12.5. *Программа LinNeighborhood*

В верхней части окна отображаются все узлы в Сети, а в нижней — подключенные общие ресурсы, которые мы подключили в данный момент.

Вы видите, что в сети находятся две машины. Первая — это контроллер домена server.dhsilabs.com, а вторая — это моя машина den.dhsilabs.com.

Сервер «расшарил» такие ресурсы:

1. ADMIN$
2. Homes
3. Print$
4. public
5. tmp
6. Принтер Canon

Ресурс **public** в данный момент подключен к каталогу `/home/denis/mnt/server.dhsilabs.com/public`. С этим каталогом можно работать как с обыкновенным каталогом файловой системы. Подключение обычно производится к каталогу:

```
/home/<имя_пользователя>/mnt/<имя_сервера>/<имя_ресурса>
```

Чтобы подключить ресурс, выделите его и нажмите кнопку **Подключить** или дважды щелкните на нужном вам ресурсе. Появится окно **Диалог подключения**, в котором нужно указать необходимые параметры подключения (см. рис. 12.6).

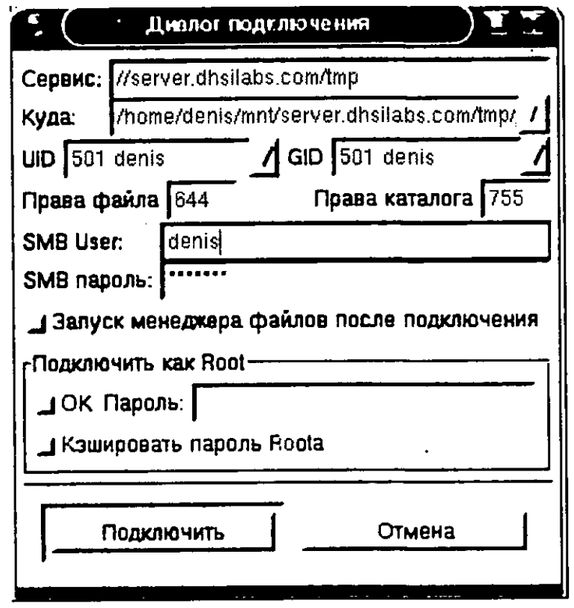


Рис. 12.6. *Диалог подключения*

Обычно вам просто нужно указать имя пользователя и пароль, если они вообще нужны — ведь вы можете подключаться с помощью гостевой записи к общему каталогу.

Кнопка **Добавить** позволяет добавить любимую машину, то есть машину, которую вы часто используете (см. рис. 12.7). Совсем необязательно, чтобы машина находилась в одной с вами рабочей группе.

Нажав на кнопку **Настройка**, вы можете определить параметры программы, но предлагаемые параметры вполне приемлемы для большинства

пользователей. Единственное, что нужно указать, так это имя рабочей группы (см. рис. 12.8).

Для сканирования все сети можно использовать команду меню **Опция → Просмотреть всю сеть**.

Рис. 12.7. *Добавление любимой машины*

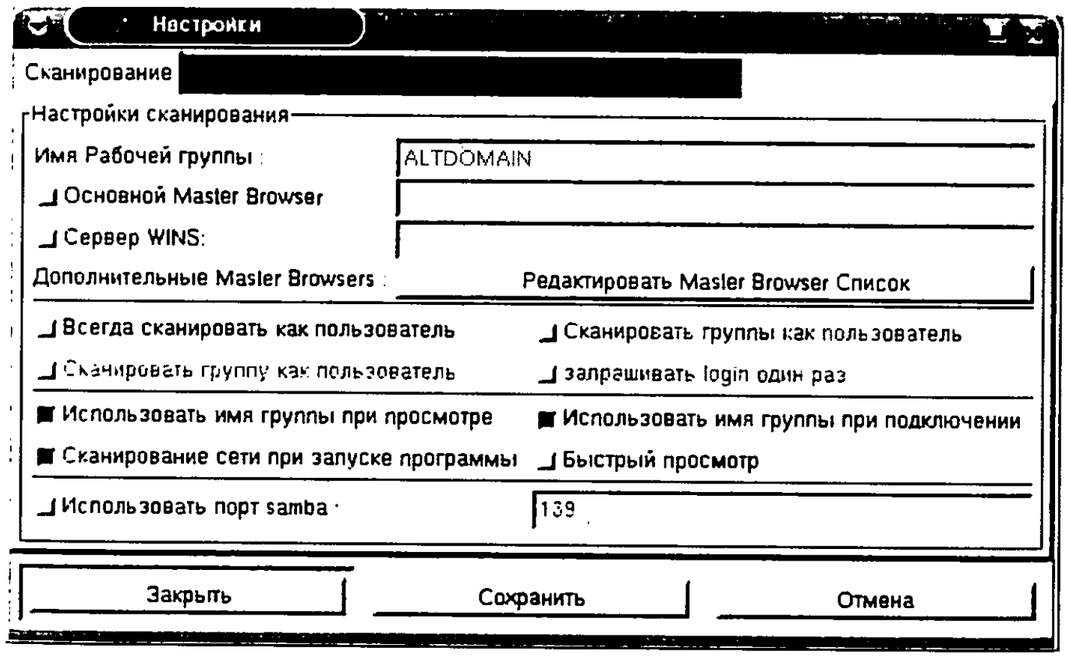


Рис. 12.8. *Параметры программы*

12.4. Доступ к принтеру Linux для Windows-машин

Для обеспечения поддержки печати мы уже сделали почти все возможное. Параметр секции **[global] load printers** загружает принтеры из файла `/etc/printcap` (см. листинг 12.1). Используется система печати BSD. Теперь осталось определить секцию **[printers]** файла `smb.conf` (см. листинг 12.5).

В этой секции задаются глобальные параметры для всех принтеров, поэтому нет необходимости указывать их отдельно для каждого принтера.

Листинг 12.5. Секция [printers]

```
[printers]
     comment = All Printers
     security=server
     path = /var/spool/lpd/lp
     browseable = no
     printable = yes
     public = yes
     writable = no
     create mode = 0700
```

Некоторые параметры, используемые в этой секции, (**browseable, writable, comment**) имеют те же значения что и в секции **[homes].** Параметр **path** задает буферный каталог, в который файлы будут копироваться перед печатью (так называемый *спул* принтера). Параметр **public** в значении **yes** разрешает печать из под гостевой учетной записи, то есть всем желающим. Чтобы запретить печать из под гостевой учетной записи, укажите **public=no.** В этом случае доступ к принтеру будут иметь только зарегистрированные на сервере пользователи. Вместо параметра **public** иногда используется его синоним — параметр **guest ok**. Параметр **writable** установлен в значении **no** для того, чтобы в буферный каталог принтера (спул) могли записываться только печатаемые файлы.

Возможно, вам потребуется разрешить печать только одному или нескольким определенным пользователям на каком-то определенном принтере. Сделать это можно так, как это показано в листинге 12.6.

Листинг 12.6. Разрешение печати определенному пользователю

```
[admprn]
     valid user = root admin administator
     path = /home/admin
     printer = canon
     public = no
     writeable = no
     printable = yes
```

Подключение к Windows-компьютеру сетевого принтера, подключенного к Linux-серверу или Linux-станции, осуществляется аналогично подключению обыкновенного сетевого принтера, подключенного к рабочей

станции Windows. В операционной системе Windows 98 для этого проделайте следующие действия:

1. Выполните команду меню **Пуск → Настройка → Принтеры**.
2. Активизируйте мастера **Установки принтера**.
3. Выберите тип принтера: **сетевой**.
4. Укажите путь к принтеру или нажмите на кнопку «Обзор» для автоматического выбора ресурса (см. рис. 12.9).
5. Далее установка сетевого принтера аналогична установке локального.

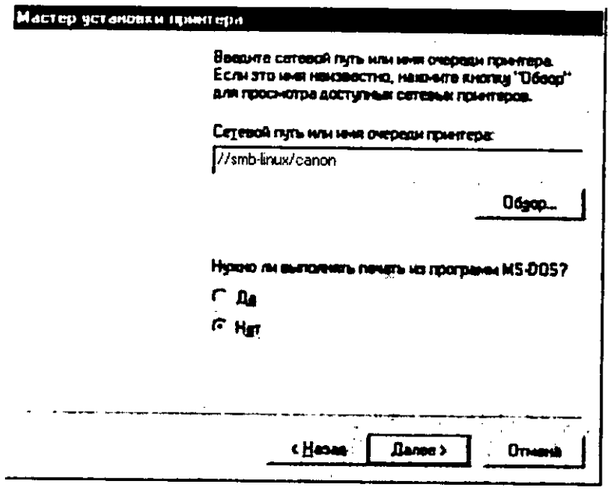


Рис. 12.9. *Подключение сетевого принтера*

12.5. Доступ к Windows-принтеру с компьютеров, работающих под Linux

Прежде всего, вам нужно создать правильные записи в файле `/etc/printcap`. С форматом этого файла вы можете ознакомиться в листинге 12.7.

Листинг 12.7. Файл printcap

```
# /etc/printcap
#
# //nt_ws1/hp5m via smbprint
#
lp:\
# просто комментарий
     :cm=HP 5MP Postscript hp5m on nt_ws1:\

# имя устройства, открываемого для вывода
     :lp=/dev/lp0:\

# директория спула принтера (на локальной машине)
     :sd=/var/spool/lpd/lp:\

# файл учета использования принтера
     :af=/var/spool/lpd/lp/acct:\

# максимальный размер файла.
# Если указано значение "ноль", то ограничение снимается
     :mx#0:\

# имя фильтра
     :if=/usr/bin/smbprint:
```

В листинге 12.7 приведено (в комментариях) описание полей файла `printcap`, но, я думаю, не помешает отдельно привести их перечень:

cm ..... задает комментарий;

lp ..... имя устройства, открываемого для вывода;

sd ..... директория спула принтера на локальной машине;

af..... файл учета использования принтера;

mx ..... максимальный размер файла. Если указано значение «ноль», то ограничение снимается;

if ..... имя входного фильтра.

Возвращаясь к настройке доступа, убедитесь, что каталог для спула принтера существует и разрешен для записи. Также нужно указать существующее устройство для вывода. В листинге 12.7 этим устройством является `/dev/lp0`.

В пакет Samba входит сценарий **smbprint**. С помощью этого сценария можно распечатывать документы на сетевом принтере, используя сервисы SMB. Возможно, в состав вашего пакета он не входит, поэтому я воссоздал его в листинге 12.8. Этот листинг частично позаимствован из руководства по пакету Samba.

Листинг 12.8. Сценарий smbprint

```
#!/bin/sh -x
# (c) Andrew Tridgell
# Этот скрипт является фильтром для системы печати,
# использующей файл /etc/printcap
```

```
# Он использует программу smbclient для печати файла
# на сетевом принтере,
# который подключен к рабочей станции Windows.
#
# smb:lp=/dev/null:sd=/usr/spool/smb:sh:if=/usr/local/samba/smbprint
#
# Запись создает unix-принтер, названный "smb",
# который будет печатать с помощью этого скрипта.
# Вам необходимо создать директорию спула
# /usr/spool/smb с соответствующими правами и владельцем.

# Установите здесь имя сервера и принтер, на который
# вы хотите печатать.

# Далее скрипт был изменен Майклом Гамильтоном
# (Michael Hamilton)
# так что сервер, сервис и пароль могут быть считаны из файла
# /usr/var/spool/lpd/PRINTNAME/.config
#
# Для того, чтобы это работало, запись в /etc/printcap должна
# включать файл учета использования (af=...):
#
#cdcolour:\
#    :cm=CD IBM Colorjet on 6th:\
#    :sd=/var/spool/lpd/cdcolour:\
#    :af=/var/spool/lpd/cdcolour/acct:\
#    :if=/usr/local/etc/smbprint:\
#    :mx=0:\
#    :lp=/dev/null:
#
# Файл /usr/var/spool/lpd/PRINTNAME/.config должен содержать
#    server=PC_SERVER
#    service=PR_SHARENAME
#password="password"
#
#Например,
#    server=PAULS_PC
#    service=CJET_371
#    password=""
```



```
#
# Файл для отладочной информации, можно изменить на /dev/null
#
logfile=/tmp/smb-print.log

# logfile=/dev/null
spool_dir=/var/spool/lpd/lp
config_file=$spool_dir/.config

eval 'cat $config_file'

echo "server $server, service $service" >> $logfile

(
    echo translate
    echo "print -"
    cat
) | /usr/bin/smbclient "\\\\$server\\$service" $password -
U $user -N -P >> $logfile
```

Теперь вы можете печатать на сетевом принтере. Но тем не менее, я все же рекомендую прочитать руководство по пакету Samba для получения более подробной информации о печати на сетевых принтерах.

12.6. Пример файла smb.conf

В листинге 12.9 приведен пример моего файла `/etc/smb.cof`. Скорее всего, он и у вас тоже будет корректно работать.

Листинг 12.9. Файл smb.conf

```
[global]
workgroup = WORK
comment = Linux Server
guest account = guest
security = share
printing = bsd
printcap name = /etc/printcap
load printers = yes
client code page = 866
```

```
character set = koi8-r
encrypt passwords = Yes
log file = /var/log/samba/log.%m
max log size = 50
# Следующие строки я закомментировал, потому что они
# характерны только для моей конфигурации
# socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
# dns proxy = no
# wins support = yes
# domain master = yes
# interfaces = 192.168.1.1/24 192.168.2.1/24

[admin]
comment = admin's directory
path = /home/admin
valid users = admin root
read only = no

[homes]
comment = Home
browseable = yes
writable = no

[public]
comment = Public Directory
path = /home/samba
read only = no

[printers]
comment = All Printers
path = /var/spool/lpd/lp
browseable = no
printable = yes
writable = no
create mode = 0700
guest ok = yes
```


12.7. Конфигуратор SWAT

Конфигуратор **SWAT** (Samba Web-based Administrative Tool) предназначен для настройки пакета Samba через Web-интерфейс. Как и другие конфигураторы, например, **netconf** или **linuxconf**, SWAT предоставляет удобный графический интерфейс для администрирования сервера Samba. Основным преимуществом данного конфигуратора является то, что вам не нужно находиться за компьютером, который вы администрируете. Администрировать сервера Samba вы можете из любого компьютера вашей сети. Как и при работе с другими конфигураторами, при работе со SWAT вам не нужно знать ни формат конфигурационных файлов, ни их название, ни расположение.

Для установки SWAT нужно установить пакет **samba-swat**. Обычно данный пакет находится на втором компакт-диске вашего инсталляционного набора Linux. Установите пакет командой:

```
rpm -ihv samba-swat-2.2.1a-4.i386.rpm
```

После установки пакета проследите за тем, чтобы в вашем файле `/etc/services` была следующая запись:

```
swat 901/tcp
```

Конфигуратор SWAT для своей работы использует протокол TCP и порт 901. Тем не менее вы можете назначить любой другой порт. При изменении номера порта не забудьте изменить номер порта в файле `/etc/inetd.conf` или `/etc/xinetd.conf`.

Если вы используете суперсервер **inetd**, добавьте в файл `/etc/inetd.conf` следующую строку (если ее там нет):

```
swat stream  tcp nowait.400  root     /usr/sbin/swat swat
```

При использовании суперсервера **xinetd** в каталог `/etc/xinetd.conf` будет добавлен файл **swat** следующего содержания (см. листинг 12.10):

Листинг 12.10. Файл /etc/xinetd.conf/swat

```
# default: off
# description: SWAT is the Samba Web Admin Tool. Use swat \
#        to configure your Samba server. To use SWAT, \
#        connect to port 901 with your favorite web browser.
service swat
{
     disable = no
     port        = 901
```

```
        socket_type = stream
        wait        = no
        only_from   = 127.0.0.1
        user        = root
        server      = /usr/sbin/swat
        log_on_failure += USERID
}
```

Если вы хотите конфигурировать сервер Samba с любого компьютера вашей сети, закомментируйте запись only_from= 127.0.0.1 или установите любые другие параметры доступа к SWAT.

Теперь нужно перезапустить суперсервер. Для этого введите команду:

```
/etc/init.d/xinetd restart
```

Можно также воспользоваться командой:

```
killall -HUP xinetd
```

При использовании **inetd** перезапустить суперсервер можно командой:

```
killall -HUP inetd
```

Все! Настройка SWAT завершена и теперь можно приступить к конфигурированию Samba с помощью SWAT. Для этого запустите свой любимый браузер и введите URL:

```
http://host:901
```

После установления соединения вы увидите окно, запрашивающее имя пользователя и пароль (см. рис. 12.10).

Введите имя пользователя и пароль. Потом вы увидите основное окно конфигуратора (см. рис. 12.11).

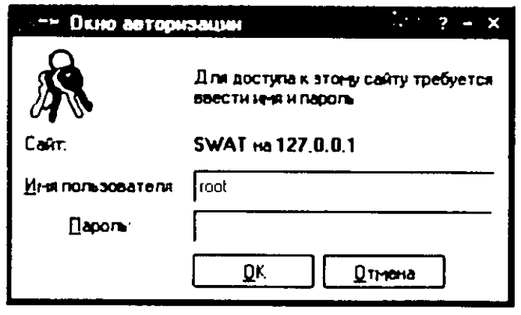


Рис. 12.10. *Окно авторизации*

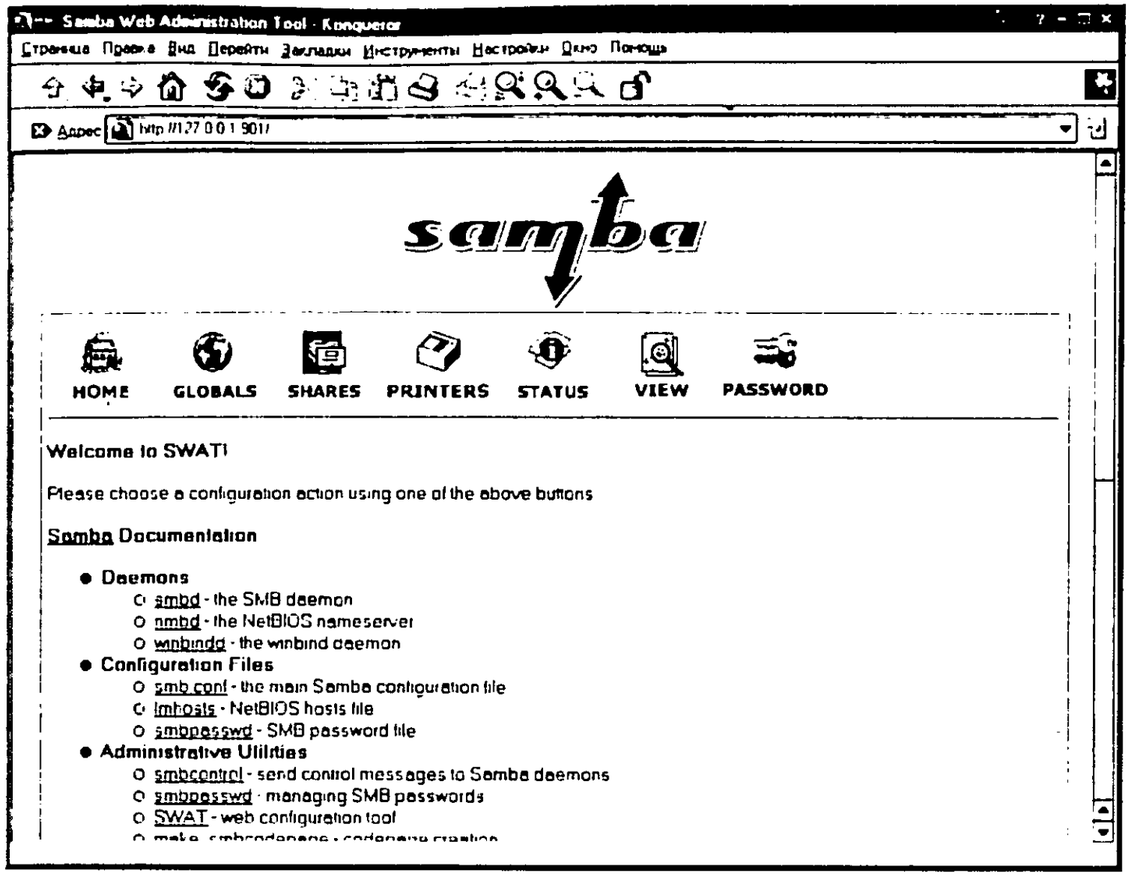


Рис. 12.11. *Samba Web Administration Tool*

Как видно из рис. 12.11, что в конфигураторе SWAT все самое нужно находится «под рукой» администратора: от документации до паролей пользователей.

В разделе **Globals** определяются значения глобальных переменных (см. рис. 12.12). Вы можете получить подсказку по тому или иному параметру, перейдя по ссылке **Help**. Установить значение по умолчанию можно, нажав на кнопку **Set Default**.

В разделе **Shares** определяются общие ресурсы, а в разделе **Printers** — общие принтеры. Состояние сервера Samba можно посмотреть в разделе **Status** (см. рис. 12.13). Здесь же можно запустить, остановить и перезапустить сервисы SMB и NMB. В этом разделе можно завершить любое соединение с сервером Samba, а также просмотреть состояние соединения.

В разделе **Passwords** определяются пользователи, которые имеют доступ к серверу Samba.

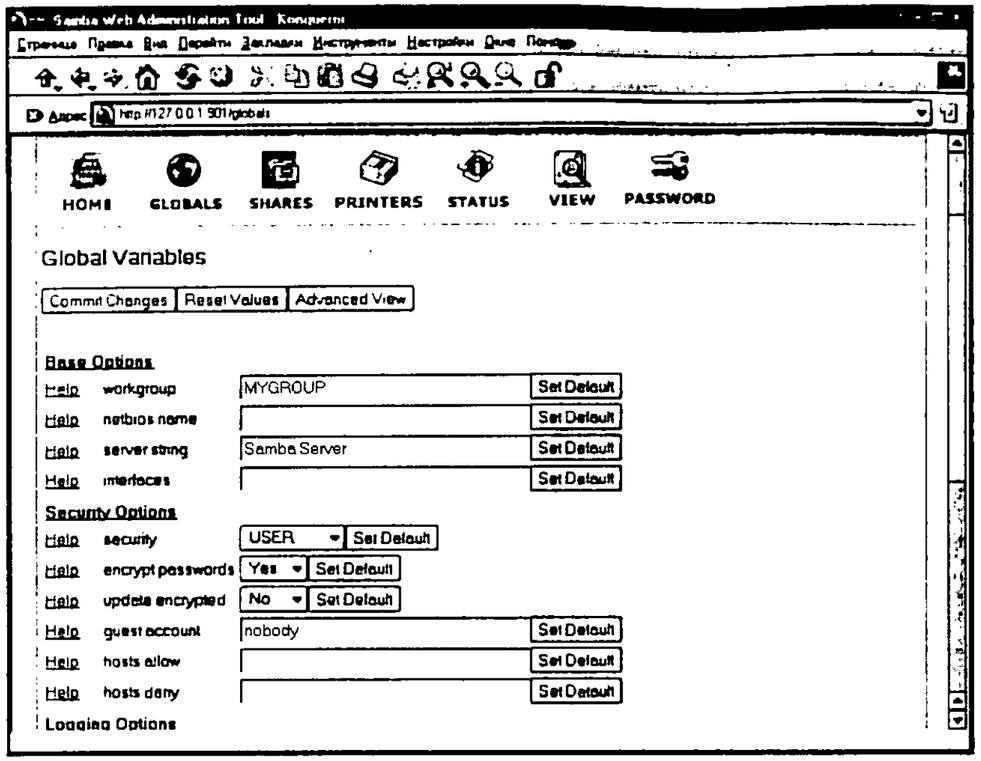


Рис. 12.12. *Глобальные переменные Samba*

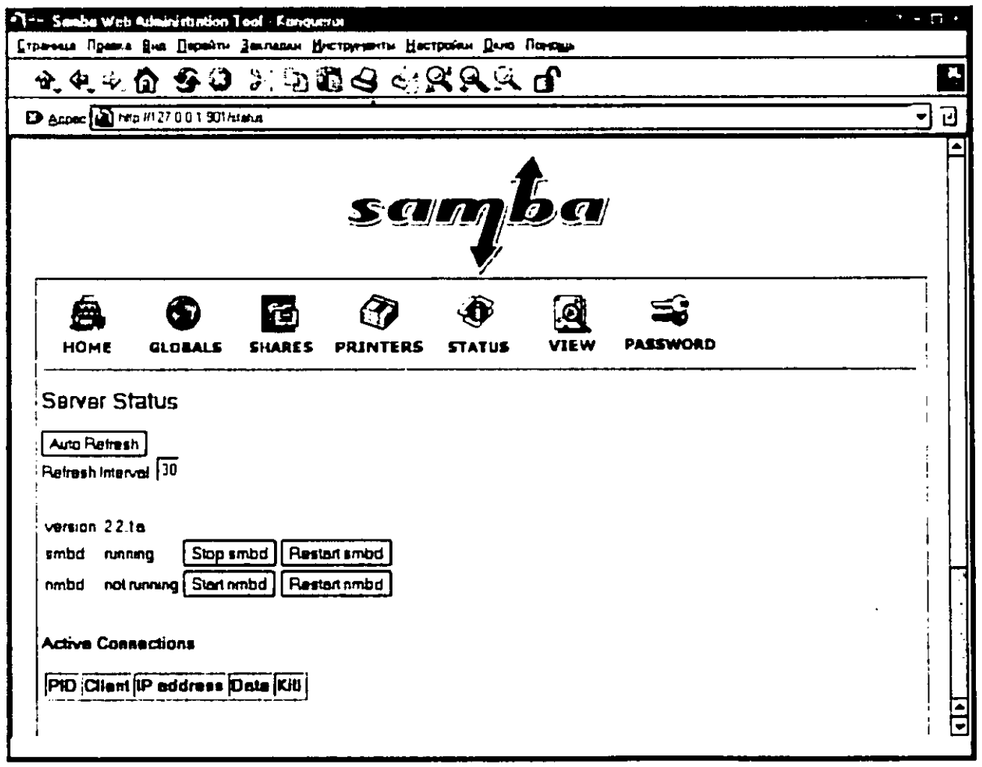


Рис. 12.13. *Раздел Status*

12.8. Совместное использование каталогов в Linux Mandrake 9.1...10

Конфигуратор **diskdrake-fileshare** позволяет очень быстро настроить пакет **Samba** для разрешения совместного использования каталогов («расшаривания» каталогов). Убедитесь, что запущены сервисы **nfs** и **smb**, если это не так, запустите их:

```
service nfs start
service smb start
```

Запустите конфигуратор **diskdrake-fileshare** (см. рис. 12.14), выберите опцию «Разрешить всех пользователей» и нажмите Ок.

Если вы выберите опцию «Выборочно», то разделять каталоги смогут только пользователи, входящие в группу **fileshare**.

Как только вы разрешите совместное использование каталогов, пользователи смогут расшарить их в своем файловом менеджере, например, в **Konqueror** для расшаривания каталога нужно щелкнуть на нем правой кнопкой мыши и выбрать пункт меню **Share**.

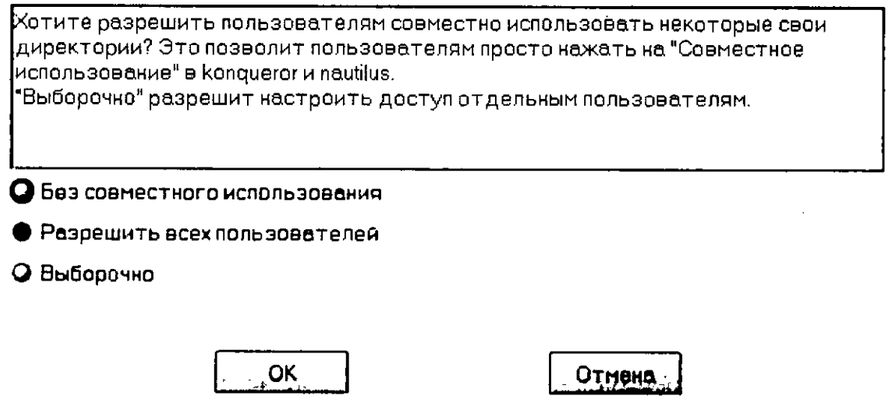


Рис. 12.14. *Конфигуратор diskdrake-fileshare*

12.9. Защита Samba

Вряд ли стоит разрешать доступ к нашему Samba-серверу всем желающим. Целесообразно разрешить доступ только определенным пользователям, которые должны быть зарегистрированы на сервере Samba. Напомню, что для создания пользователя используется команда **adduser**, а для изменения его пароля — **passwd**.

```
adduser -s /bin/false samba-user
passwd samba-user
```

Первая команда создает пользователя сервера Samba под именем `samba-user`. Параметр **-s** устанавливает оболочку для этого пользователя — `/bin/false`. Оболочку `/bin/false` рекомендуется использовать из соображений безопасности для всех пользователей, которые не нуждаются в работе с консолью системы. Даже если кто-то узнает пароль пользователя `samba-user`, он ничего не сможет сделать, потому что «оболочка» `/bin/false` не позволяет вводить команды.

Samba использует свой файл паролей — `/etc/samba/smbpasswd`. В нем всего три поля: логин пользователя, UID (User ID) и хешированный пароль. Для добавления пользователя в файл `/etc/samba/smbpasswd` и изменения его пароля, в Samba используется команда **smbpasswd**:

```
smbpasswd samba-user
New SMB password:
Retype new SMB password:
Added user samba-user
Password changed for user samba-user
```

Совет: если вы хотите добавить всех пользователей из файла `/etc/passwd` в файл `/etc/samba/smbpasswd`, то используйте для этого следующую команду:

```
cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
```

Не забудьте изменить права доступа к файлу `/etc/samba/smbpasswd`:

```
chmod 600 /etc/samba/smbpasswd
```

Осталось только сделать небольшие изменения в секции [global] файла конфигурации `smb.conf`:

```
security = user
```

12.10. Оптимизация Samba

Ваш Samba-сервер медленно работает и вы уже устали от постоянных жалоб пользователей? Лучшим выходом из данной ситуации будет покупка нового винчестера. Лучше всего покупать SCSI-винчестер со скоростью 10000 оборотов в минуту. В крайнем случае подойдет IDE-диск, поддерживающий режим ATA133 и работающий со скоростью 7200 оборотов в минуту. При покупке такого винчестера обратите внимание на следующие факторы:

- ваша материнская плата должна поддерживать режим ATA133;

- у вас должен быть специальный кабель для подключения жесткого диска (если материнская плата поддерживает ATA100/133, такой кабель у вас будет);
- покупайте винчестер с большим объемом кэша: на рынке можно найти несколько моделей винчестеров, различающихся маркировкой, но в одном случае вы получаете 2 Мб кэша, а во втором — 640 Кб (или 1 Мб, но все равно меньше, чем в более дорогой модели).

Если же денег на покупку такого винчестера нет, попробуем оптимизировать наши настройки. Во-первых, установите значение **Yes** для опции **wide links** в файле конфигурации `smb.conf` — это должно повысить производительность сервера, если в общих каталогах имеются ссылки.

Во-вторых, в дистрибутиве Red Hat Linux есть демон **bdflush**. Он занимается записью буферов, содержащих модифицированные данные файловой системы, на диск. Настройки по умолчанию не очень эффективны:

```
30 64 64 256 500 3000 60 0 0
```

Попробуем немного оптимизировать настройки **bdflush**. Для этого откройте файл `/etc/sysctl.conf` и добавьте в него следующую строку:

```
vm.bdflush = 80 500 64 64 15 6000 6000 0 0
```

Этим мы говорим демону, чтобы он записывал буферы на диск, когда буфер кэша файловой системы заполнен на 80 процентов.

После этого нужно перезапустить сервис **network**:

```
service network restart
```

Если вам нельзя ни на секунду останавливать сервис **network**, вместо модификации файла `/etc/sysctl.conf` введите следующую команду:

```
sysctl -w vm.bdflush="80 500 64 64 15 6000 6000 0 0"
```

Чтобы заставить ваш Samba-сервер работать быстрее, попробуем поэкспериментировать с кэшированием памяти: мы будем использовать минимум 60 процентов памяти для кэша.

```
sysctl -w vm.buffermem = "60 10 60"
```

Примечание.

Последние два параметра (10 и 60) сейчас не используются. Значения по умолчанию — «2 10 60».

Очень рекомендую внимательно прочитать главу 4 — в ней описана программа **hdparm**, позволяющая «выжать» из жесткого диска все, на что он способен.

Глава 13

Служба каталогов Active Directory

13.1. Что такое Active Directory?

Объяснить чем же является служба каталогов Active Directory лучше всего на примере базы SAM, которая использовалась в Windows NT 4.0. В базе данных SAM, содержалась информация об учетных записях пользователей, включая их пароли, и компьютерах, входящих в состав домена NT. Информация о сетевых ресурсах — сетевых дисках, принтерах — хранилась отдельно на каждом компьютере, к которому этот ресурс подключен.

В базе данных Active Directory хранится информация не только о пользователях и компьютерах домена, но и о других сетевых ресурсах — дисках, принтерах. Причем в базе данных хранятся не только имена этих ресурсов, но и другие атрибуты, упрощающие поиск этого ресурса.

Например, вы только что устроились на работу и не знаете, в какой комнате (на каком этаже) находится цветной струйный принтер, но последний нужен вам для выполнения вашего задания. Вам достаточно задать атрибуты поиска (например, принтер цветной) и база данных Active Directory сообщит вам имя этого ресурса, информацию об его состоянии и его атрибуты (например, местонахождение). Останется подключить этот сетевой принтер к своему компьютеру, распечатать задание и перейти в нужную комнату, чтобы его забрать.

Удобно? Без службы каталогов вам бы пришлось самостоятельно просматривать все сетевые принтеры в надежде найти подходящий.

Итак, **Active Directory — это база данных, содержащая полную информацию о сети (доменах, компьютерах, пользователях, сетевых ресурсах), и совокупность программ, предназначенных для управления этой базой данных.**

Для управления базой данных Active Directory предназначены следующие утилиты, которые вы сможете найти в папке Administrative Tools:

- **Active Directory Users and Computers** (см. рис. 13.3) — управление каталогом Active Directory (пользователи и компьютеры);
- **Active Directory Domain and Trust** (см. рис. 13.1) — управление доменами и доверительными отношениями;
- **Active Directory Sites and Services Manager** (см. рис. 13.2) — Менеджер узлов и служб Active Directory.

Также в состав Active Directory входят и другие программы, выполняющие служебные функции по обслуживанию каталога. Как правило, такие программы запускаются в фоновом режиме.

Кроме программ, служба Active Directory включает в себя интерфейсы прикладного программирования (API): Active Directory Services Interface-ASDI и C LDAP API. Данные интерфейсы позволяют пользователям, в том числе и администраторам, запрашивать информацию из базы данных и управлять базой данных. За выполнение запросов и обновление базы данных отвечает программа DSA (Directory System Agent). Все зап-

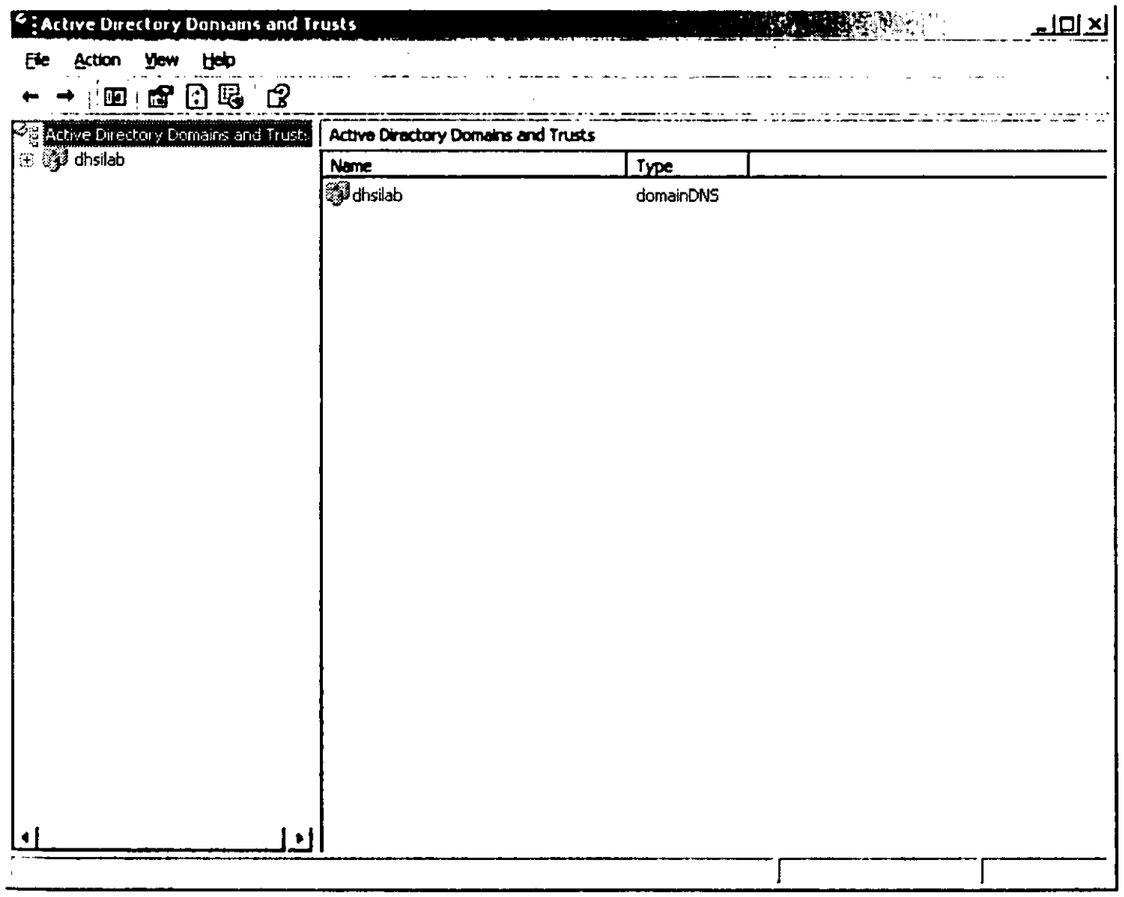


Рис. 13.1. *Утилита Active Directory Domain and Trust*

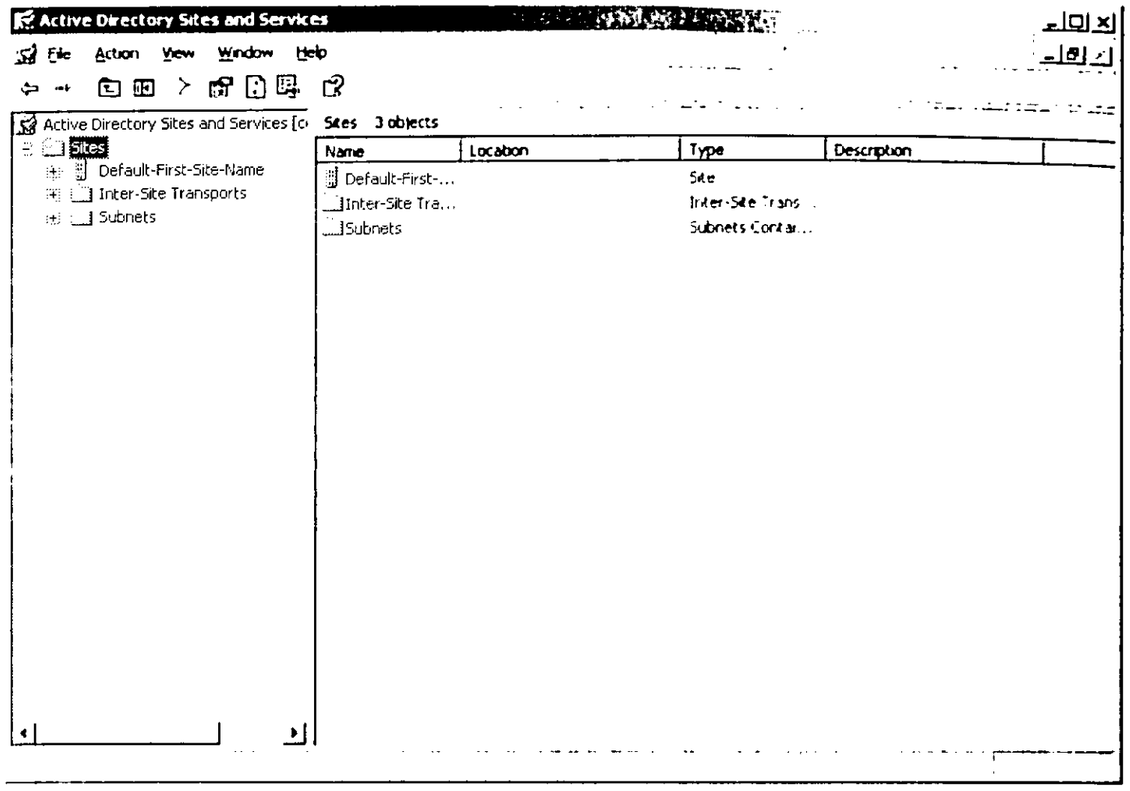


Рис. 13.2. *Утилита Active Directory Sites and Services Manager*

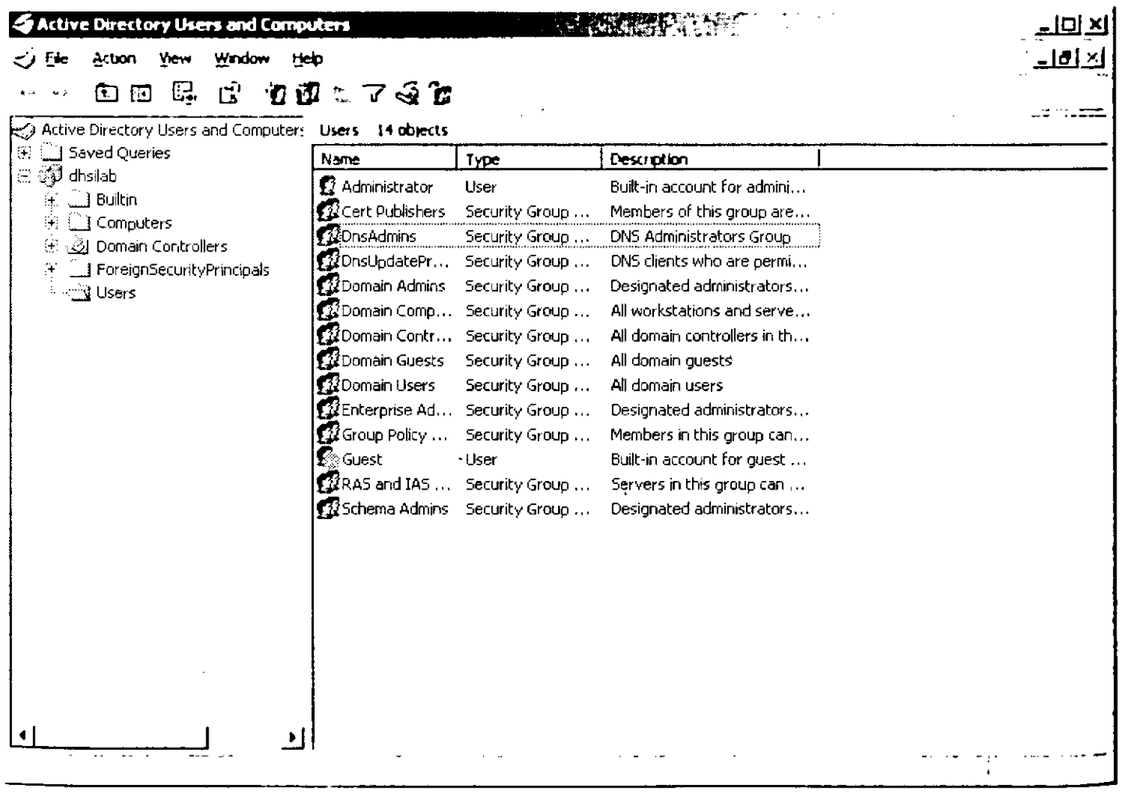


Рис. 13.3. *Утилита Active Directory Users and Computers*

росы к базе данных выполняются через DSA — это позволяет избежать многих проблем, связанных с несоответствием форматов данных в программах и базе данных.

Служба Active Directory выполняет следующие функции:

- **Единый вход в систему** — после входа в домен вам не нужно указывать имя пользователя и пароль для подключения к каждому ресурсу. В принципе, данная возможность была реализована и в Windows NT.
- **Иерархическая структура службы каталогов** — упрощает поиск нужного вам объекта.
- **Открытая схема каталогов** — если в Windows NT база SAM могла содержать только записи двух типов — пользователей и компьютеров, то Active Directory может содержать записи любых типов, которые определяются самим администратором. Вы можете создать запись любого типа — операционная система, процессор и даже мышь. В итоге вы быстро найдете все компьютеры, на которых установлена ОС Windows XP Home и которые оснащены мышками Genius.
- **Распределенная база данных** — повышает отказоустойчивость всей службы каталогов.
- **Программируемость** — служба каталогов содержит интерфейсы прикладного программирования.
- **Масштабируемость** — управление может быть как централизованным, так и децентрализованным.

13.2. Представление объектов в базе данных

Первой «службой каталогов» была файловая система. Основным объектом этой службы был файл (напоминаю, что каталог — это тоже файл). Файлам свойственны следующие атрибуты: имя, расширение (тип файла), дата создания, дата модификации, размера, атрибуты доступа (только чтение, архивный, скрытый, системный), признак каталога и др. По мере усложнения файловой системы появляются новые атрибуты — владелец, группа, более расширенные права доступа.

Что-то подобное наблюдается и в службе каталогов Active Directory. Вот только объектом намного больше и у каждого из них есть свои атрибуты. Например, объекту `Пользователь` свойственны следующие атрибуты (рис. 13.4):

- Имя, под которым он зарегистрирован в системе — логин;
- Фамилия, имя, должность, название отдела и другая персональная информация о пользователе;

Рис. 13.4. *Свойства пользователя*

- Адрес;
- Телефон;
- Группы пользователей — список групп, в которых входит этот пользователь;
- Список серверов, к которым пользователь может получить доступ;
- Местонахождение профиля пользователя и его домашнего каталога;
- Сведения об удаленном доступе к серверу (Dial-up).

13.3. Дерево и лес доменов

Прежде чем сказать, что такое дерево доменов, поговорим о пространстве имен. Служба Active Directory работает в одном пространстве имен, которое объединяет все объекты вашей сети — от пользователя до сведений об операционной системе каждого компьютера. Для обеспечения нормальной работы сети вам потребуется создать сначала хотя бы один домен. Затем, по мере расширения, еще один, а потом — еще один.

Дерево доменов — это объединение нескольких доменов, причем это объединение использует одно и то же пространство имен. **Лес** — это совокупность деревьев доменов, при этом пространство имен у каждого дерева свое. Деревья и леса обеспечивают иерархическую схему службы каталогов, что упрощает использование и управления службой каталогов. На рис. 13.5. представлено дерево доменов, а на 13.6 — лес.

Что же касается доменов, то домен он и в Африке домен — этим я хочу сказать, что домен в Windows 2000 остался таким же доменом, как и в Windows NT 4.0. Вы можете администрировать его по-прежнему — создавать учетные записи пользователей и управлять ресурсами домена.

Что существенно стало лучше — так это транзитивные доверительные отношения между доменами. Теперь для установки доверительных отношений вам не нужно согласовывать свои действия с администраторами других доменов.

Напомню, что при транзитивных отношениях, если вы устанавливаете между доменами A и B, то оба домена будут доверять друг другу. Если же отношения не транзитивные, то если домен A доверяет B, то это еще не означает, что B доверяет A.

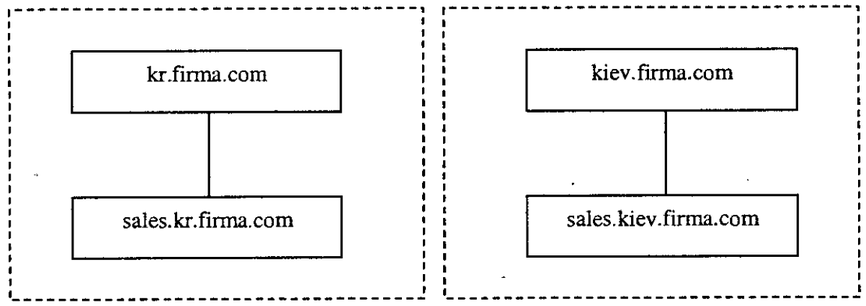


Рис. 13.5. *Дерево доменов — одно пространство имен*

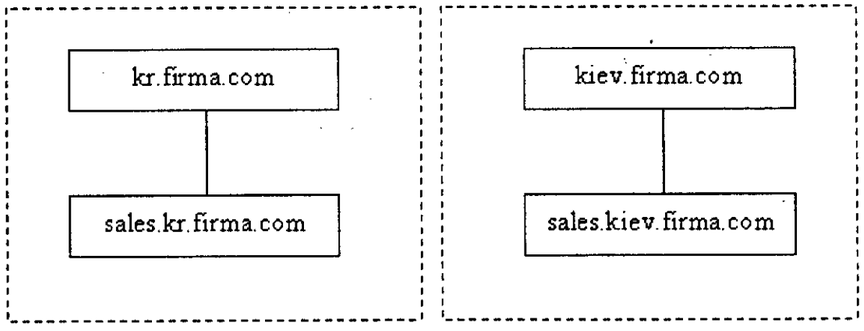


Рис. 13.6. *Лес — два разных пространства имен*

13.4. Установка службы Active Directory

Настраивать Active Directory имеет смысл на контролере домена, также проверьте, чтобы разделы этого сервера были отформатированы под NTFS — иначе начинать установку Active Directory нет смысла (у вас должен быть хотя бы один довольно «просторный» NTFS-раздел).

Запустите утилиту конфигурации вашего сервера (она находится в папке Administrative Tools). В левой части окна выберите Active Directory (рис. 13.7).

Вы можете сейчас настроить ваш сервер как первичный контроллер домена. Если контроллер домена уже есть в сети, можно создать дополнительный контроллер домена, новый дочерний домен (child domain), дерево доменов (domain tree) или лес (forest). Мы договорились, что будем создавать первичный контролер домена, предполагая, что в сети его еще нет. В нижней части окна (прокрутите полоску прокрутки) вы увидите ссылку **Start**. Нажмите ее для запуска мастера установки Active Directory (рис. 13.8).

Первый вопрос мастера — тип нашего сервера:

- **Domain controller for a new domain** — контролер домена для нового домена;
- **Additional domain controller for an existing domain** — дополнительный контролер домена для существующего домена.

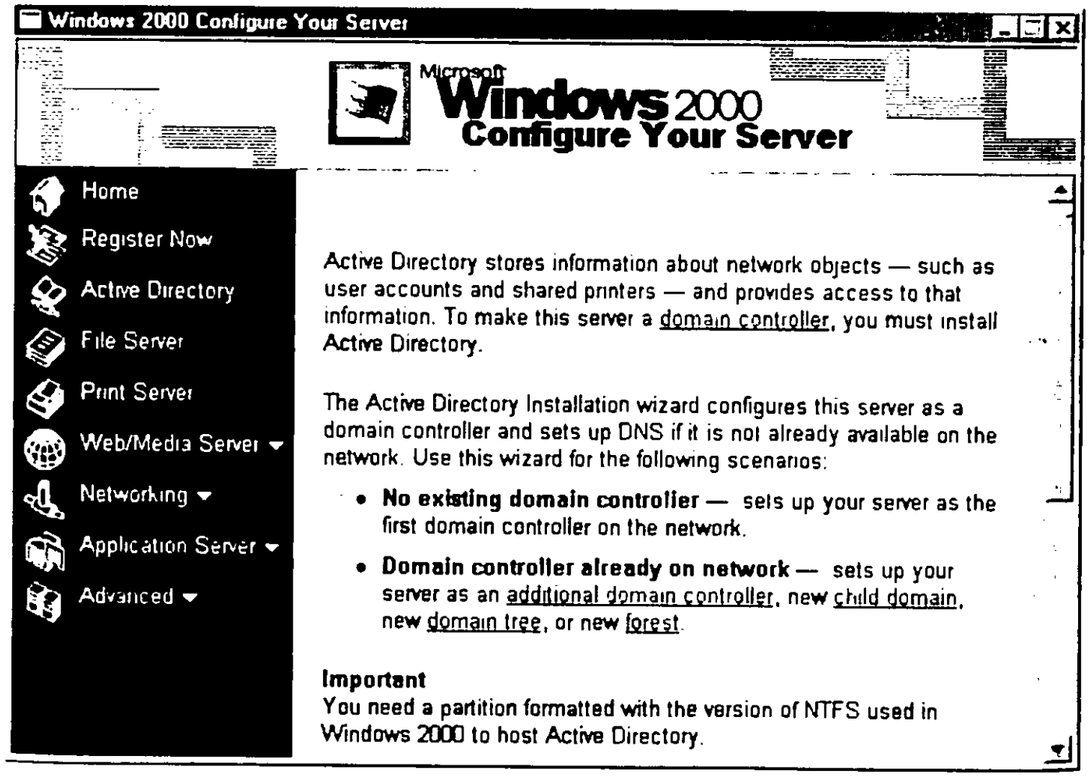


Рис. 13.7. *Как устанавливать Active Directory?*

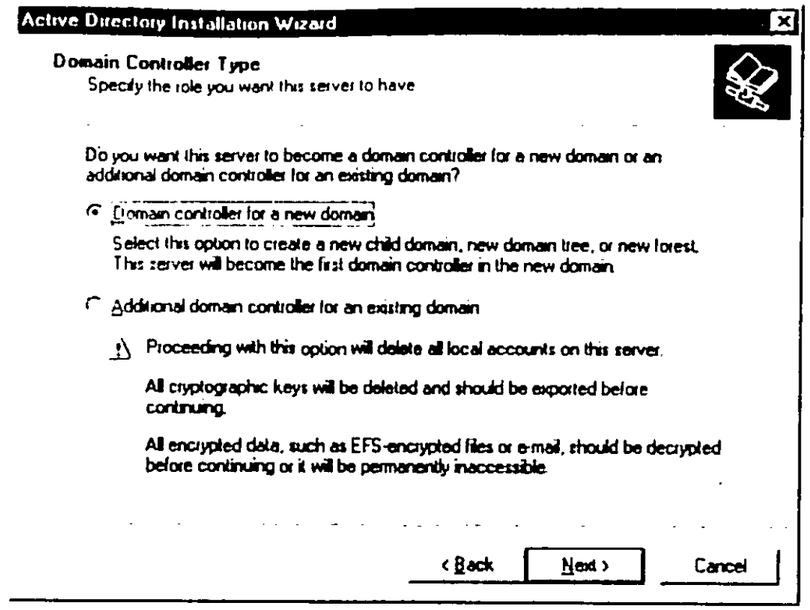


Рис. 13.8. *Мастер установки Active Directory*

Нам нужно выбрать, ясное дело, первый вариант. Если вы все же выбираете второй (поскольку PDC уже существует), не забудьте экспортировать все криптографические ключи, которые будут удалены, если вы нажмете **Next**. Также будут удалены все учетные записи пользователей.

Следующий вопрос — создать новое дерево или подсоединиться к существующему дереву? Нам нужно выбрать **Create a new domain tree** — создать новое дерево (рис. 13.9) и нажать **Next**.

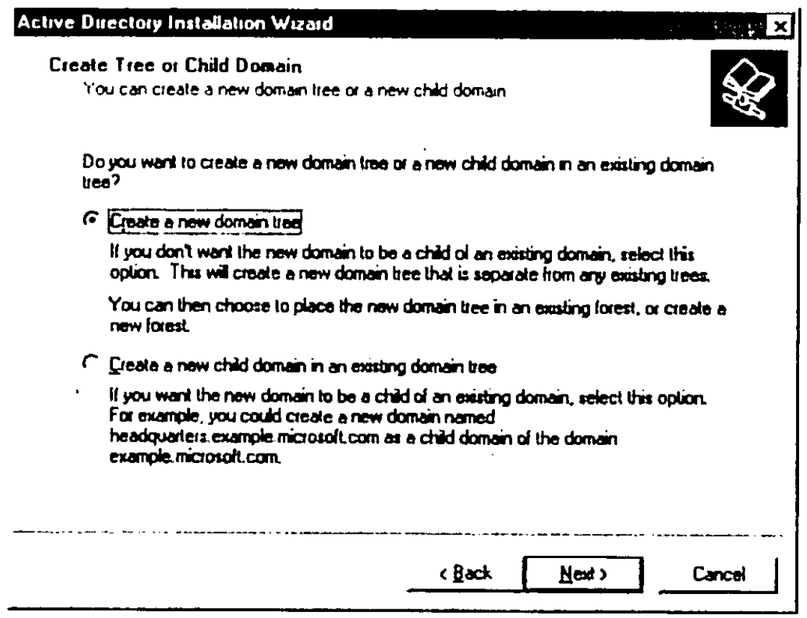


Рис. 13.9. *Создание нового дерева доменов*

Следующий шаг — вам нужно ввести имя будущего домена. Вам нужно ввести полное DNS-имя, например, `firma.com`. Если у вас сеть без выхода в Интернет, можно обойтись простым именем, например, `firma`.

Если вы выбрали присоединение к существующему дереву (см. рис. 13.9), то вам нужно будет ввести полное доменное имя существующего дерева.

После этого нужно будет ввести NetBIOS-имя вашего нового домена. Вообще-то вы здесь можете ничего не вводить, а принять все по умолчанию. Данная опция служит лишь для совместимости с предыдущими версиями Windows.

Следующий этап — это выбор местонахождения базы данных и файлов журналов Active Directory. Из соображений безопасности и первое, и второе должны быть расположены на NTFS-разделах. Причем, обратите внимание, на разных разделах.

На рис. 13.10 использован один раздел — такое допускается, но настоятельно рекомендуется размещать операционную систему, базу данных и файлы протоколов Active Directory на разных NTFS-разделах. В принципе можно разместить их на FAT-разделе, но из практики известно, что NTFS-разделы «падают» значительно реже, чем их FAT-сородичи.

А вот размещение папки `Sysvol` обязательно должно быть на NTFS-разделе. Тут уж никуда не денешься — требование безопасности.

После этого мастер сообщит вам, что в вашей сети не найден DNS-сервер (рис. 13.11), который обслуживает ваш домен и предложит настроить DNS автоматически. Соглашайтесь (рис. 13.12).

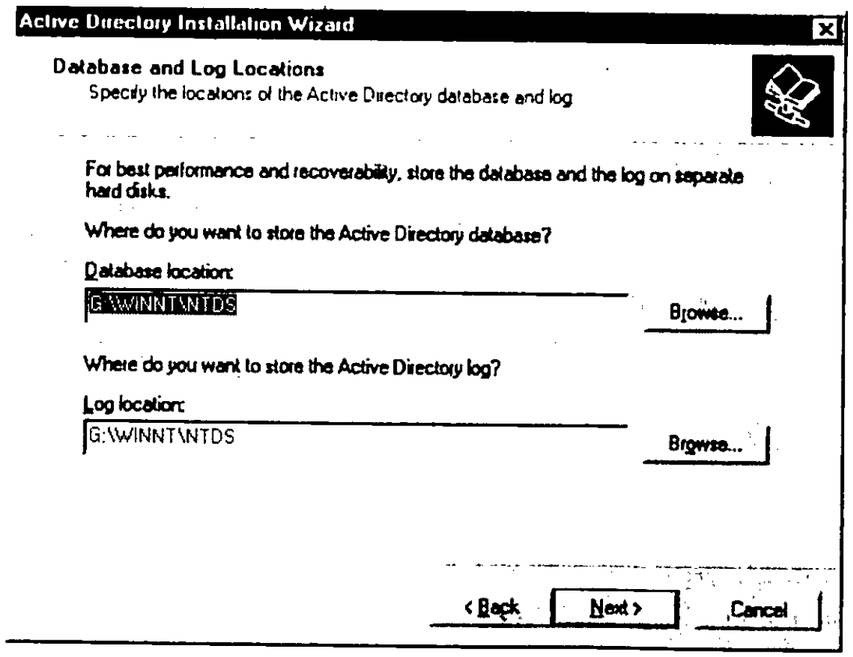


Рис. 13.10. *Размещение базы данных и файлов протокола Active Directory*

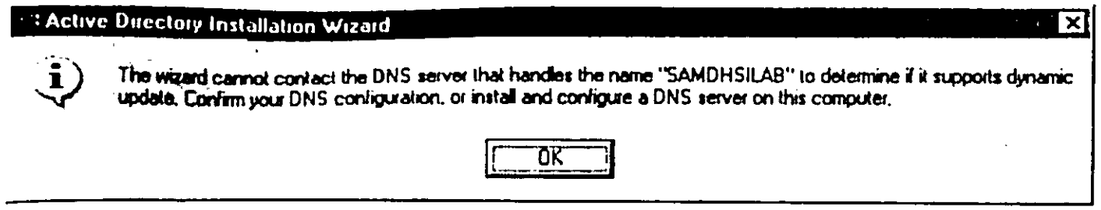


Рис. 13.11. *Нужный DNS-сервер не найден*

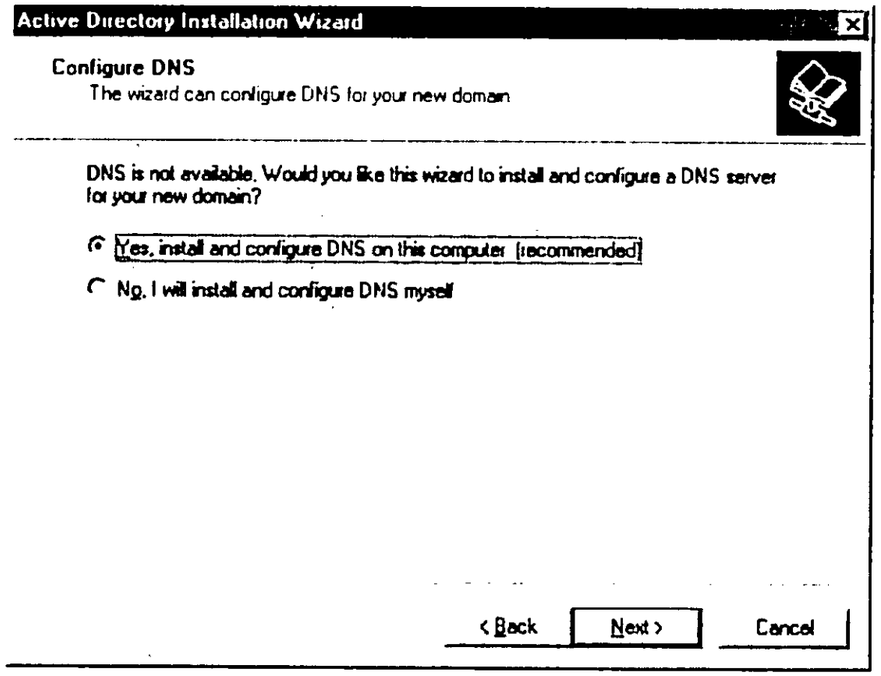


Рис. 13.12. *Тут нужно выбрать Yes (для установки DNS-сервера)*

Следующий шаг — вам нужно выбрать тип разрешений (рис. 13.13) для службы удаленного доступа (RAS):

- **Permissions compatible with pre-Windows 2000 Server** — разрешения совместимы со старыми версиями Windows NT Server — на всякий случай лучше выбрать этот вариант;
- **Permissions compatible only with Windows 2000 server** — разрешения будут совместимы только с серверами Windows 2000.

После этого вам нужно ввести пароль администратора (рис. 13.14) — только постарайтесь его не забыть и не записывать на желтом листике, прикрепленном к монитору.

Вслед за этим вы увидите окно с обобщенной информацией — параметрами, которые вы указали. Если вы согласны, нажмите **Next** для установки Active Directory (см. рис. 13.15).

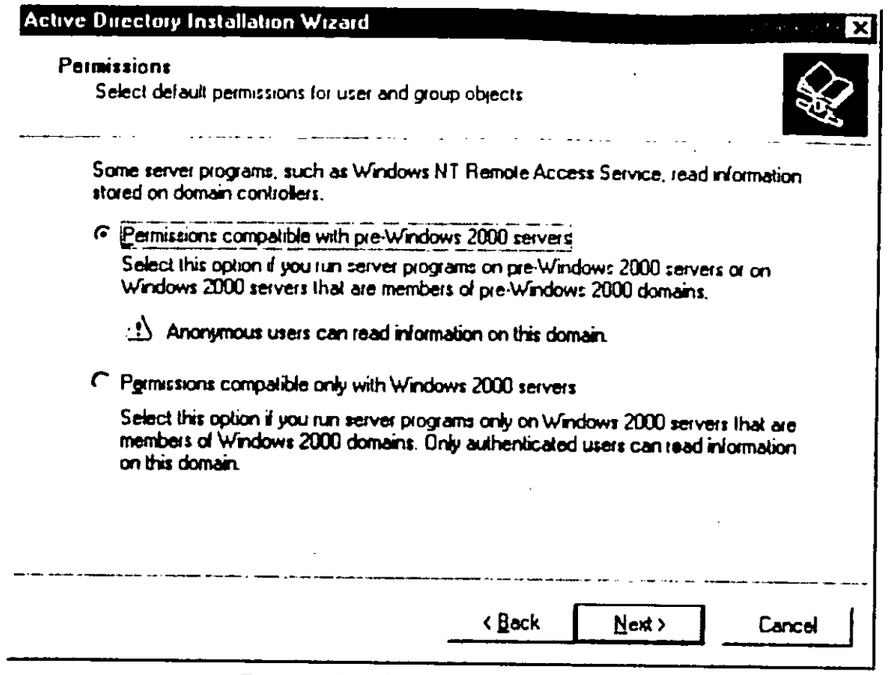


Рис. 13.13. *Тип разрешений*

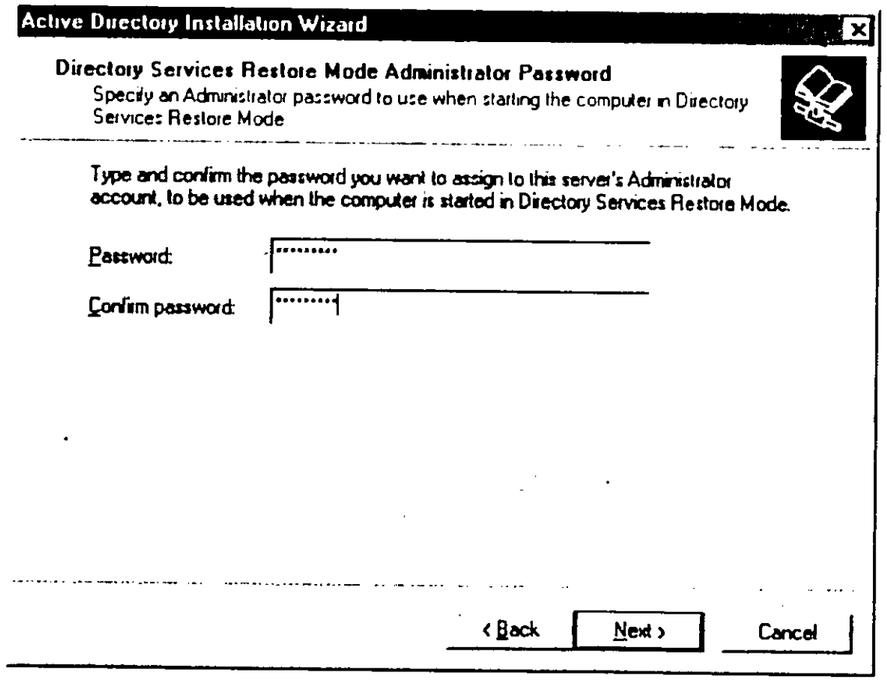


Рис. 13.14. *Ввод пароля администратора*

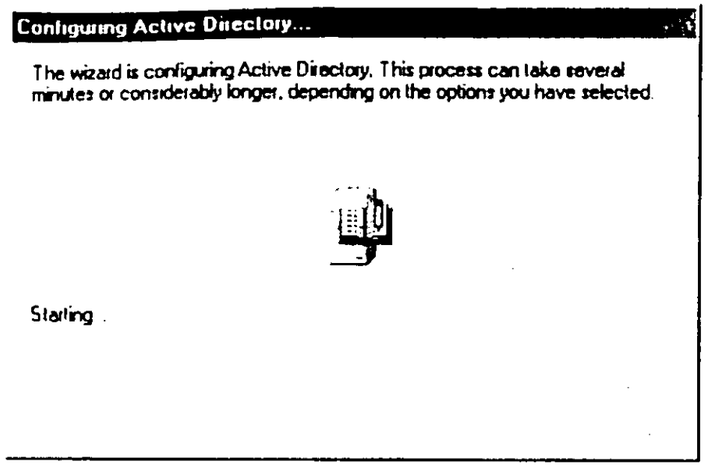


Рис. 13.15. *Начало установки Active Directory*

Вот теперь можно пойти пить кофе. На рис. 13.15 сказано «подождите несколько минут». Понятие «несколько минут» очень расплывчатое, особенно у Microsoft. А после перезагрузки компьютера вы вообще успеете сбегать в ближайшую булочную — за булкой к очередной чашке кофе. Причем можно не спешить — все равно успеете.

После того, как компьютер все-таки загрузится, можно приступить к обычной настройке сервера с помощью утилиты **Directory Management**.

Глава 14

Маршрутизация и управление трафиком в сетях

Данная глава выходит за рамки элементарных знаний о сетях и предназначена уже для приобретения более специализированных навыков, предназначенных для оптимизации сети. В этой главе описывается каким образом и с помощью каких программных инструментов можно оптимизировать трафик (передачу данных) в развитых, разветвленных сетях, а также сетях, состоящих из нескольких подсетей.

14.1. Подсети и маршрутизация

14.1.1. Маршрутизаторы, мосты и шлюзы

Представим, что у нас есть две сети, которые нужно объединить для решения общих задач пользователями этих сетей. Для объединения сетей будем использовать специальное устройство, пересылающее пакеты из одной сети в другую, и наоборот. Процесс пересылки пакетов будем называть маршрутизацией, а устройство, объединяющее две сети, маршрутизатором.

Мы уже раньше говорили о маршрутизаторах, но делали это на популярном уровне. Если же быть более формальным, терминам маршрутизация и маршрутизатор можно дать следующие определения:

Маршрутизация (routing) — процесс передачи пакетов данных между двумя подсетями.

Маршрутизатор (router) — устройство для пересылки пакетов. Маршрутизатор собирает информацию о топологии межсетевых соединений и на

основании этой информации пересылает пакеты сетевого уровня в сеть назначения. Маршрутизатор может быть программным и аппаратным.

Для объединения сетей могут также использоваться другие устройства — мост и шлюз. **Мост** (bridge) — устройство для соединения двух или более физических сетей. Мосты передают пакеты порту, к которому подключен адресат. Однако в отличие от большинства коммутаторов Ethernet, мосты не передают фрагменты пакетов при возникновении коллизий и пакеты с ошибками, поскольку все пакеты буферизуются перед их пересылкой в порт адресата.

Шлюз (Gateway) — межсетевой преобразователь. Выполняет функции, аналогичные мосту, но используется для связи сетей разных типов, например, LAN и WAN (то есть, например, для связи локальной сети с Интернетом).

Какая же разница между этими устройствами, выполняющими похожие функции? Маршрутизатор, в отличие от моста, зависит от протокола. В этой главе мы будем говорить об IP-маршрутизации и об IP-маршрутизаторах. Мост же просто передают пакеты из одной подсети в другую, не задумываясь ни о формате кадра, ни о протоколе.

Обычно для устройства, которое связывает две локальные сети, используется термин «маршрутизатор», а для устройства, которое соединяет вашу локальную сеть с Интернет, — шлюз, хотя оба эти устройства выполняют одну и ту же функцию — маршрутизацию пакетов.

Кроме маршрутизации пакетов шлюз может также выполнять (и часто это делает) преобразование адресов (NAT): он преобразует реальные Интернет-адреса в адреса нашей сети (например, 192.168.1.x) и обратно. Таким образом, создается иллюзия, что любой узел нашей сети подключен к Интернет напрямую, без шлюза. Другие узлы Интернет тоже «думают», что наш узел — вполне самостоятельный узел с реальным IP-адресом.

Что немаловажно — функции шлюза прозрачны и незаметны для пользователей. Однако это верно, если этим самым пользователям не приходится настраивать компьютеры самостоятельно — тогда они точно увидят поле Gateway address в окне настройки.

14.1.2. Аппаратные и программные маршрутизаторы

Маршрутизатор может быть как аппаратным, так и программным. Аппаратный маршрутизатор — это самостоятельное устройство, внешне напоминающее концентратор или модем, подключающееся непосредственно к сети. Такие маршрутизаторы (рис. 14.1) стоят немалых денег, поэтому руководство предприятий частенько заменяют аппаратные маршрутизаторы программными.

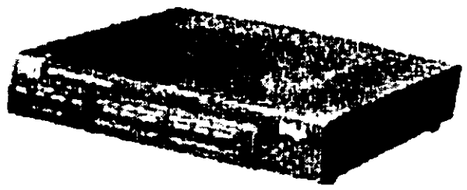


Рис. 14.1. *Аппаратный маршрутизатор Intel Express 9545 HDSL2*

Программный маршрутизатор — это обыкновенный компьютер, операционная система которого может выполнять перенаправление IP-пакетов (IPv4 Forwarding). К числу таких операционных систем относятся:

- Linux/UNIX;
- Windows NT;
- Windows 2000/2003;
- Windows XP.

В принципе, маршрутизатор можно реализовать и на базе Windows 98, но вы ведь не хотите, чтобы обе сети простаивали несколько часов в день из-за того, что какая-то программа выполнила некорректную операцию и была закрыта вместе с операционной системой?

14.1.3. Таблицы маршрутизации в IP-сетях

В качестве примера программного маршрутизатора в этой главе мы будем рассматривать Windows NT 4.0 Server. Это глава сугубо теоретическая — будете ли вы использовать эту операционную систему или нет, важно, чтобы вы поняли сам принцип маршрутизации.

В этой книге (в следующих частях) мы будем рассматривать другие операционные системы в качестве маршрутизатора — Windows 2000/2003 Server, Linux. Если вы заинтересовались, как сделать из Windows 98 маршрутизатор, я вам расскажу чуть позже, однако ответственности за такой маршрутизатор я не несу.

Итак, рассмотрим, как выполняется маршрутизация. Представим, что компьютер А отправляет пакет компьютеру Б. Если оба эти компьютеры находятся в одной сети, то, ясное дело, что никакой маршрутизатор не нужен — пакет должен быть отправлен сразу компьютеру Б. Кто же принимает решение перенаправить пакет или нет? Решение принимается как узлом А, так и маршрутизатором сети. Общий алгоритм выглядит так:

1. Сначала определяется в какой подсети находится компьютер Б.
2. Если компьютер Б находится в нашей, локальной, сети пакет просто отправляется компьютеру Б.

3. Если же компьютер Б находится в другой сети, IP-уровень компьютера А просматривает имеющуюся в его памяти таблицу маршрутизации, в которой может находиться путь к узлу Б.
4. Если маршрута к узлу Б нет в таблице маршрутизации компьютера А, то пакет отправляется маршрутизатору по умолчанию — пусть он сам решает, что делать с этим пакетом.
5. Маршрутизатор просматривает свою таблицу маршрутизации. Если же маршрут к узлу Б снова не найден, то маршрутизатор отправляет пакет другому маршрутизатору — М2, который для него является маршрутизатором по умолчанию.
6. Маршрутизатор М2 просматривает свою таблицу маршрутизации и т.д.
7. При обнаружении следующего маршрута пакет отправляется на следующий маршрутизатор — это явление называется переходом или транзитом (hop). Если пакет так и не достиг узла Б, компьютеру А отправляется сообщение об ошибке.

Рассмотрим рис. 14.2. Из рисунка видно, что маршрутизатор соединяет три сети:

- 192.168.1.0
- 192.168.2.0
- 192.168.3.0

У маршрутизатора есть три сетевых интерфейса, например, три сетевые платы:

- 192.168.1.1
- 192.168.2.1
- 192.168.3.1

Вы уловили суть? Маршрутизатор явно присутствует в каждой из этих сетей. То есть для компьютеров конкретной сети маршрутизатор — это локальный узел. Только для первой сети это узел с адресом 192.168.1.1, для второй — с адресом 192.168.1.2, а для третьей — 192.168.1.3.

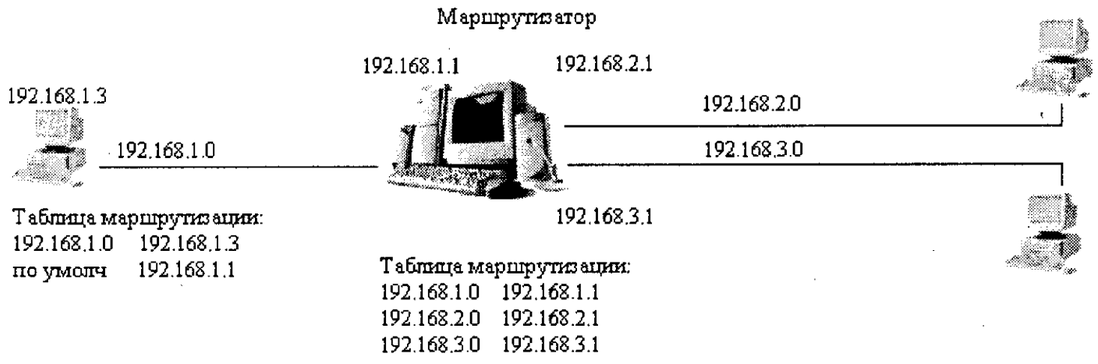


Рис. 14.2. *Соединение трех сетей*

Что же происходит, когда компьютер 192.168.1.3 пытается отправить пакет компьютеру 192.168.3.5, то есть лежащему в сети 192.168.3.0? Компьютер 192.168.1.3 просматривает свою таблицу маршрутизации. Сначала он находит запись:

```
192.168.1.0  192.168.1.3
```

Данная запись означает, что для сети 192.168.1.0 он сам себе маршрутизатор. То есть он самостоятельно будет отправлять пакет, если адресат пакета принадлежит сети 192.168.1.0. Но адресат пакета принадлежит другой сети — 192.168.3.0. Наш компьютер не нашел соответствующей записи в своей таблице маршрутизации, поэтому он ищет запись «по умолч» и оправляет пакет по указанному адресу — адресу маршрутизатора по умолчанию — 192.168.1.1.

Маршрутизатор 192.168.1.1 анализирует пакет, определяет адрес подсети и отправляет этот пакет узлу 192.168.3.5.

Как вы думаете, зачем нужна запись:

```
192.168.1.0  192.168.1.3
```

Правильно, если бы не было этой записи, то даже для отправления пакета локальному узлу пришлось бы задействовать маршрутизатор по умолчанию. Представляете, во сколько раз возросла бы нагрузка на маршрутизатор?

Приведенные на рисунке таблицы маршрутизации упрощены до невозможного. На самом деле таблица маршрутизации операционной системы Windows NT выглядит так, как показано в табл. 14.1.

Таблица маршрутизации ОС Windows NT *Таблица 14.1*

Network Address	Netmask	Gateway address	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.1	1
...	...	...	...	...

Ясное дело, что у вас, на практике, адреса будут другими, да и записей будет больше. Нам сейчас нужно разобраться с назначением полей таблицы маршрутизации:

- **Network address (Сетевой адрес)** — это адрес сети-назначения.
- **Netmask (Маска)** — это сетевая маска сети-назначения. Данное поле обязательно не для всех маршрутиазторов. Некоторые маршрутизаторы не имеют этого поля, но это только минус маршрутизатору. Отсутствие поля «Маска» говорит о том, что маршрутизатор не так гибок в настройка, как этого бы хотелось.

- **Gateway address (Адрес шлюза)** — это адрес шлюза для данной сети.
- **Interface (Интерфейс)** — это адрес интерфейса, через который будет отправлен пакет.
- **Metric (Метрика)** — это число маршрутизаторов на пути пакета до того, как он достигнет назначения, то есть сколько пересадок пакету нужно будет сделать на своем пути. Но обычно это поле используется маршрутизатором по-другому. Это своеобразный признак непосредственного подключения к сети. Метрика 1 (или 0 на некоторых маршрутизаторах) говорит о том, что данная сеть подключена непосредственно к порту маршрутизатора.

Маршрутизаторы, отличные от Windows NT, например, Linux-маршрутизаторы или аппаратные маршрутизаторы имеют несколько другую таблицу маршрутизации. Первое, на что обращаешь внимание — это на изменения имен полей:

- Поле **Netmask** может называться **Destination**.
- Поле **Netmask** может называться просто **Mask**, а может вообще отсутствовать.
- Поле **Gateway address** во многих маршрутизаторах называется просто **Gateway**.

Но названия полей никак не влияют на их назначение. Вот пример таблицы маршрутизации Linux:

```
Kernel IP routing table
Destination   Gateway Genmask Flags    Metric   Ref  Useface
192.168.1.1   0.0.0.0 255.255.255.0    U    0    0    12 eth0
127.0.0.1     0.0.0.0 255.0.0.0   U    0    0    1    lo
```

Как вы видите, поле **Netmask** называется **Genmask**, поле **Network Address** — как **Destination**. Обратите внимание, что появились новые поля:

- Flags.
- Ref.
- Use.

Кроме того, поле **Iface** (**Interface** на маршрутизаторе Windows NT) содержит не адрес интерфейса, а его символьное имя. В Linux различным интерфейсам присваиваются символьные имена (см. табл. 14.2):

Символьные имена сетевых интерфейсов в Linux *Таблица 14.2*

Имя	Описание
lo	Интерфейс обратной петли, то есть 127.0.0.1
ethN (где N – целое число)	Сетевая плата Ethernet. N – это номер сетевой платы, например, eth0, eth1
pppN (N – целое число)	PPP-интерфейс, например, выделенная линия или просто коммутируемое соединение

Предположим, что у нашего Linux-маршрутизатора есть три сетевых платы — eth0, eth1 и eth2. Этим сетевым платам присвоены IP-адреса 192.168.1.1, 192.168.2.1, 192.168.3.1. Так вот, в таблицу маршрутизации Linux вносятся символьные имена интерфейсов вместо IP-адресов. Чтобы узнать, какой адрес, какому интерфейсу присвоен, достаточно ввести команду **ifconfig**, предварительно зарегистрировавшись в системе, как пользователь root.

Вывод программы **ifconfig** выглядит следующим образом:

```
eth0 Link encap:Ethernet  HWaddr 00:02:44:7B:2B:86
     inet addr:192.168.1.5  Bcast:192.168.1.255
Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:0 errors:0 dropped:0 overruns:0 frame:0
     TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:100
     RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
     Interrupt:11 Base address:0xb000

lo   Link encap:Local Loopback
     inet addr:127.0.0.1  Mask:255.0.0.0
     UP LOOPBACK RUNNING  MTU:16436  Metric:1
     RX packets:18 errors:0 dropped:0 overruns:0 frame:0
     TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:0
     RX bytes:1512 (1.4 Kb)  TX bytes:1512 (1.4 Kb)
```

Вернемся к новым полям, которые появились на Linux-маршрутизаторе: **Flags**, **Ref** и **Use**. Поле **Flags** может принимать следующие значения:

- **U** — маршрутизатор активен и свободен;
- **H** — признак использования специального маршрута к указанному узлу;
- **G** — маршрут проходит через промежуточный маршрутизатор;
- **D** — маршрут получен из сообщения Redirect протокола ICMP. Данный признак никак не влияет на процесс маршрутизации, а только указывает, откуда появилась запись, чтобы вы ее случайно не удалили, мол, я такой записи не вносил.

Примечание.

Поле **Flags** на некоторых аппаратных маршрутизаторах называется **Status**. Ясное дело, что поле **Status** будет принимать значения, отличные от значений поля **Flags**. Какие именно? Тут уже нужно читать руководство по вашему маршрутизатору.

Поля **Ref** (иногда называется **Refcnt**) и **Use** — сугубо статистические. Поле **Ref** указывает, сколько раз на данный маршрут ссылались, а поле **Use** — сколько пакетов было передано по данному маршруту.

Как просмотреть таблицу маршрутизации:

- в Linux — команда **route**.
- в Windows (во всех версиях) — команда **route print**.

14.1.4. Статическая маршрутизация

Маршрутизация бывает статической или динамической. Предположим, что у нас есть два маршрутизатора и три подсети, которые объединяются этими маршрутизаторами. При *статической маршрутизации* вы должны самостоятельно (вручную) добавить в таблицу маршрутизации каждого маршрутизатора сведения об имеющихся подсетях.

Причем добавлять информацию нужно обо всех подсетях, поскольку если в маршрутизатор M1 добавить сведения о сети 2, а в маршрутизатор M2 не добавить информацию о сети 1, пользователи сети 1 смогут отправлять пакеты в сеть 2, а получать пакеты от пользователей сети 2 не смогут, равно как и пользователи сети 2 не смогут отправлять пакеты в сеть 1.

Если маршрутизаторов не очень много, то заполнить вручную их таблицы маршрутизации — не такая уж сложная задача. Но если таких маршрутизаторов много, они расположены на значительном расстоянии, а удаленное администрирование невозможно по причине отсутствия маршрутизации пакетов, то редактировать вручную таблицы маршрутизации — не очень приятное занятие. К тому же при добавлении/модификации/удалении записи таблицы маршрутизации вам придется опять редактировать таблицу каждого маршрутизатора.

14.1.5. Динамическая маршрутизация

Динамическая маршрутизация позволяет автоматизировать управление таблицами маршрутизации всех маршрутизаторов сети. Для этого используются два протокола управления маршрутизацией:

- RIP (Routing Information Protocol);
- OSPF (Open Shortest Path First).

Протокол RIP

Из-за своей специфики протокол RIP не используется в глобальных сетях, но нас сейчас интересуют локальные сети, поэтому далее будет рассматриваться именно протокол RIP.

Протокол RIP предназначен для обмена следующей информацией:

- Идентификатором сети (network ID);
- Метрикой.

Метрика (количество транзитов) — это количество маршрутизаторов на пути пакета до достижения нужной сети (идентификатора сети).

Максимальное количество «пересадок» — 15. Если метрика больше 15, то такая сеть считается недоступной. Метрика может модифицировать маршрутизатором в зависимости от загруженности или скорости канала. Если канал медленный или же сильно загружен, метрика может быть специально завышена. Поскольку при выборе маршрута протокол RIP использует именно метрику — чем меньше метрика, тем лучше маршрут, а медленный или перегруженный маршрут выбран не будет.

Примечание.

Протокол RIP работает на основе протокола UDP, порт 520.

RIP-маршрутизаторы обычно пересылают свою таблицу маршрутизации каждые 30 секунд. Вернемся к нашему примеру с тремя подсетями. Маршрутизатор сети 1 — M1 каждые 30 секунд посылает широковещанием свою таблицу маршрутизации. Таблица маршрутизация — это специальные RIP-пакеты, которые воспринимают только RIP-маршрутизаторы.

Маршрутизатор сети 2 — M2 принимает таблицу маршрутизации сети 1. Маршрутизатор M2 добавляет новые записи в свою таблицу маршрутизации. Если записи уже есть, сравниваются метрики. Если метрика новой записи меньше, чем метрика старой, старая запись удаляется, а новая заносится в таблицу маршрутизации. Точно также маршрутизатор M2 посылает сведения о сетях 2 и 3. Маршрутизатор M1 принимает эти данные и заносит их в свою таблицу маршрутизации.

Статические и динамические маршрутизаторы могут работать в одной сети. Но нужно помнить, что статический маршрутизатор не обменивается информацией о маршрутах, поэтому статический маршрут нужно добавить вручную как на статическом, так и на динамическом маршрутизаторе.

Некоторые аппаратные RIP-маршрутизаторы не передают статические маршруты, то есть те маршруты, которые вы добавили вручную. В этом случае нужно будет точно также, вручную, настроить удаленные маршрутизаторы, то есть добавить в их таблицы статические маршруты. Узнать, передает ли ваш аппаратный маршрутизатор статические маршруты или нет, можно в руководстве по вашему маршрутизатору. Желательно узнать это еще до покупки маршрутизатора...

Недостатки протокола RIP

Протокол RIP разрабатывался для небольших, локальных сетей. Точнее во времена первой версии протокола RIP существенно больших сетей еще не было — это один из старейших протоколов маршрутизации (к слову, он был разработан компанией Xerox). Из-за особенностей данного протокола его нельзя применять в глобальных сетях:

- Максимальное количество переходов равно 15: в глобальных сетях количество маршрутизаторов может быть больше 15.
- При передаче таблицы маршрутизации последняя передается полностью. А ведь она может содержать сотни записей. Поскольку данные «упаковываются» порциями по 512 байт, то передача одной такой таблицы может вызвать приличный поток RIP-пакетов. А учитывая еще и тот факт, что передача таблиц осуществляется каждые 30 секунд, приходим к выводу, что несколько RIP-маршрутизаторов могут в течение довольно небольшого времени забить медленный канал глобальной сети, который к тому же, как правило, обладает небольшой пропускной способностью. Скорость 1...2 Мбит/с довольно высока для глобальных каналов связи, но недопустимо мала для локальной сети — нам даже 10 Мбит/с не хватает...

Протокол RIP-2

Вторая версия протокола RIP представляет собою усовершенствованную первую версию. Главное отличие заключается в том, что кроме идентификатора сети и метрики передается еще и маска сети. Благодаря этому маршрутизация стала более гибкой, но как плата — возрос объем передаваемых по сети данных.

Протокол OSPF

Один из самых популярных протоколов маршрутизации. В его основе заложен специальный математический алгоритм, который позволяет высчитывать оптимальные маршруты. Этот протокол является топологическим, то есть учитывающим состояние канала. Протокол OSPF является достаточно сложным протоколом. По сравнению с RIP он обладает следующими достоинствами:

- Возможностью управления несколькими маршрутами.
- Возможностью разделения сети на сегменты, которые будут предоставлять друг другу только высокоуровневые данные маршрутизации.

Этот протокол рекомендуется использовать в сетях с разветвленной структурой, в которой может возникать большое количество дублирующихся маршрутов.

14.1.6. Маршрутизация и перенаправление трафика

Не следует путать понятия «маршрутизация» и «перенаправление трафика». Маршрутизация представляет собой сложный процесс просчета и выбора наиболее оптимального на данный момент маршрута. При этом используется большое количество входной информации, основывающейся на предыдущем опыте работы маршрутизатора, а также на текущем состоянии сети. Значительная часть этой информации предоставляется соседними узлами. При этом существенную роль (и проблему) играет синхронизация таблиц маршрутизации у соседних узлов.

Перенаправление трафика же является простой операцией, направляющей пакеты данных в соответствии с определенным условием. Никакого выбора и расчета при этом не производится. Условно говоря, перенаправление является простейшим методом статической маршрутизации.

14.2. Маршрутизация в Windows

14.2.1. Статическая маршрутизация

Перед прочтением этой и следующей главы я настоятельно рекомендую прочесть еще раз шестую главу, в которой изложены теоретические сведения о маршрутизации. В этих же главах (20 и 21) будет изложена только практическая часть, то есть вы уже должны знать, что делаете, точнее, что хотите сделать.

Как вы знаете, маршрутизация бывает двух типов: статическая и динамическая. Сначала мы поговорим о статической маршрутизации в Windows. При статической маршрутизации вы должны самостоятельно (вручную) добавить в таблицу маршрутизации каждого маршрутизатора сведения об имеющихся подсетях. Причем добавлять информацию нужно обо всех подсетях, поскольку если в маршрутизатор M1 добавить сведения о сети 2, а в маршрутизатор M2 не добавить информацию о сети 1, пользователи сети 1 смогут отправлять пакеты в сеть 2, а получать пакеты от пользователей сети 2 не смогут, равно как и пользователи сети 2 не смогут отправлять пакеты в сеть 1.

Статическая запись включает в себя следующие компоненты:

- **адрес сети** — адрес или имя сети получателя, если задано имя сети, то поиск адреса сети производится в файле %WinDir%\System32\Drivers\Etc\Networks.
- **сетевая маска** — маска подсети для сети получателя.
- **адрес шлюза** — через этот интерфейс будут направлены пакеты в сеть получателя, если задан не IP-адрес, а имя, то поиск имени будет производиться в файле %WinDir%\System32\Drivers\Etc\Hosts.

В таблице маршрутизации по умолчанию содержатся следующие записи:

- **0.0.0.0** — маршрут по умолчанию к любой сети, которая не описана в таблице маршрутизации;
- **широковещание в сети** — используется для широковещания (broadcast) во всей сети;
- **широковещание в подсети** — используется для широковещания (broadcast) в локальной подсети;
- **loopback (интерфейс-заглушка)** — используется для тестирования конфигурации и сетевых программ (127.0.0.1);
- **локальная сеть** — используется для отправки пакетов другим компьютерам локальной сети;
- **локальный узел** — адрес локального компьютера.

Просмотреть таблицу маршрутизации можно с помощью команды **route print**. Добавить статическую запись в таблицу маршрутизации можно с помощью следующих команд:

```
route add сеть mask сетевая_маска шлюз
route -p add сеть mask сетевая_маска шлюз
```

Вторая команда отличается от первой тем, что добавляет постоянный маршрут. Постоянный маршрут хранится в реестре Windows, непостоянные маршруты хранятся в оперативной памяти, поэтому теряются при перезагрузке компьютера.

Например, для добавления маршрута, который будет связывать нашу сеть с сетью 192.168.5.0 через компьютер 192.168.5.1 (это шлюз) нужно использовать команду:

```
route -p add 192.168.5.0 mask 255.255.255.0 192.168.5.1
```

Для удаления или изменения статических записей используются следующие команды:

```
route delete сеть шлюз
route change сеть шлюз
```

Для изменения информации о маршруте по умолчанию можно использовать апплет **Network (Сеть)** с Панели управления. Откройте этот апплет, перейдите на вкладку **Protocols (Протоколы)**, затем выберите протокол TCP/IP и нажмите кнопу **Properties (Свойства)**. В открывшемся окне (рис. 14.3) нужно добавить/удалить адрес основного шлюза (Default Gateway).

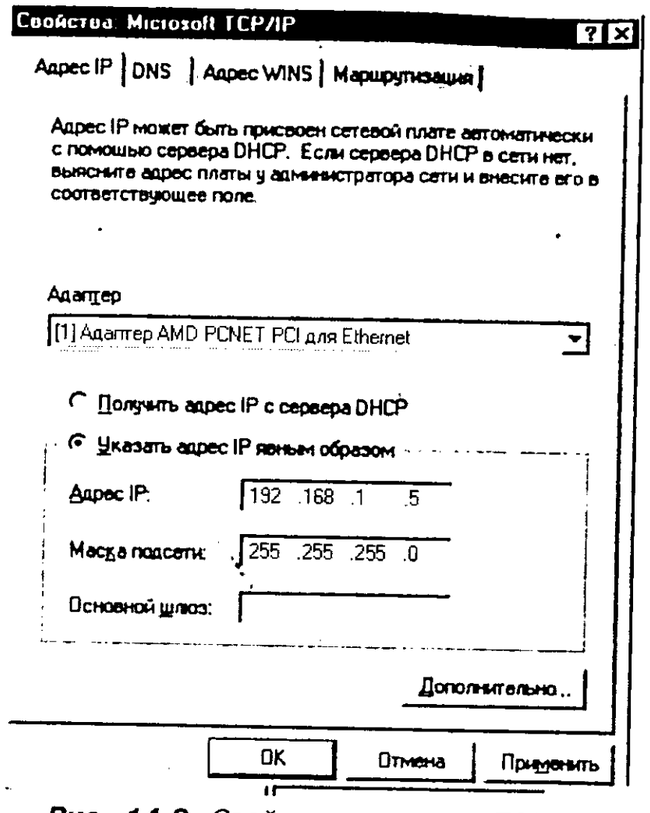


Рис. 14.3. *Свойства протокола TCP/IP*

14.2.2. Динамическая маршрутизация

Разобравшись со статической маршрутизацией, теперь перейдем к динамической. Динамическая маршрутизация основывается на протоколах RIP или OSPF. Для включения динамической маршрутизации откройте апплет **Network (Сеть)** панели управления, откройте свойства протокола TCP/IP, перейдите на вкладку **Routing (Маршрутизация)**, показанную на рис.14.4, и установите флажок **Enable IP Forwarding (Включить перенаправление IP)**.

Примечание.
Не забудьте зарегистрироваться как администратор!

Затем нам нужно установить службу RIP. Для этого в окне **Network (Сеть)** перейдите на вкладку **Services (Службы)** и нажмите кнопку **Добавить**. В открывшемся окне (рис. 14.5) добавьте сервис **RIP for Internet Protocol**.

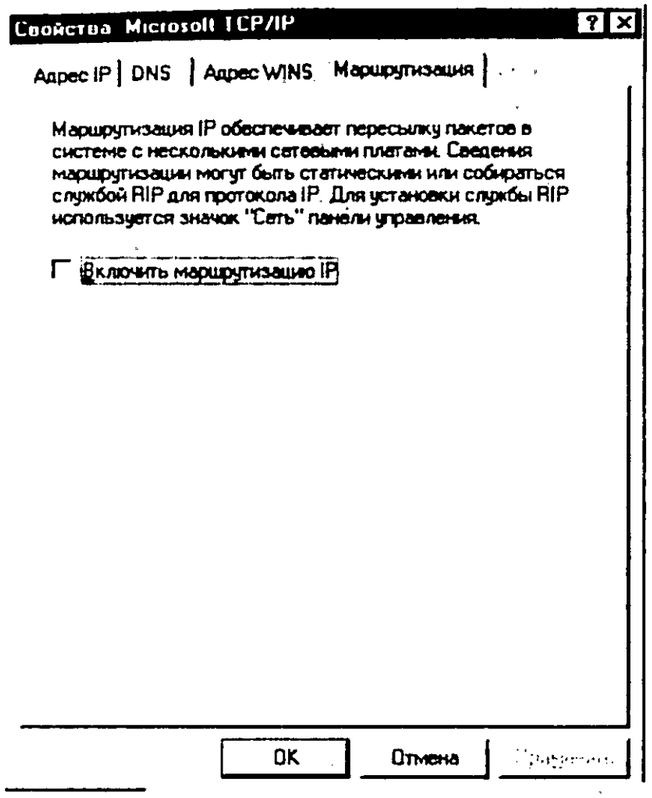


Рис. 14.4. *Вкладка «Маршрутизация»*

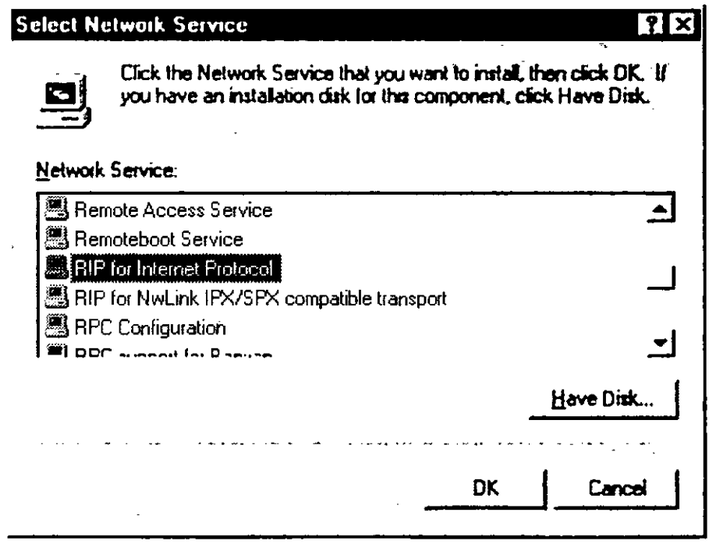


Рис. 14.5. *Установка службы RIP for Internet Protocol*

14.2.3. Особенности операционных систем

Наверное, вы заметили, что данная глава называется «Маршрутизация в Windows». Просто Windows. Без уточнения ее версии. А ведь Windows Windows'у — рознь. Однако настройка маршрутизации выполняется одинаково во всех версиях Windows. Принципиально, можно настроить маршрутизатор и на базе Windows 98. Было бы желание. Однако, стоит ли это делать?

Если вам нужен маршрутизатор только для самоутверждения, мол, я на Windows 98 маршрутизатор настроил, тогда можно. А если для ежедневного использования, тогда сразу можете забыть об этой идее. Почему? Да потому что Windows 98 не очень надежна для этой задачи. Если вам все еще интересно, как превратить Windows 98 в маршрутизатор, запустите редактор реестра (regedit.exe), перейдите в секцию HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP, создайте в ней ключ, содержащий символьное значение (String Value) как показано на рис. 14.6. Имя ключа EnableRouting, значение — «1» (без кавычек).

После перезагрузки компьютера, если вы все сделали правильно, программа **winipcfg** сообщит вам о включенной маршрутизации IP (рис. 14.7).

Теперь с помощью команды **route** вы сможете добавлять статические записи. Динамической маршрутизации в Windows 98 нет.

Если же вам нужен действительно надежный маршрутизатор, установите Windows NT 4.0 Workstation. Во-первых, данная операционная система

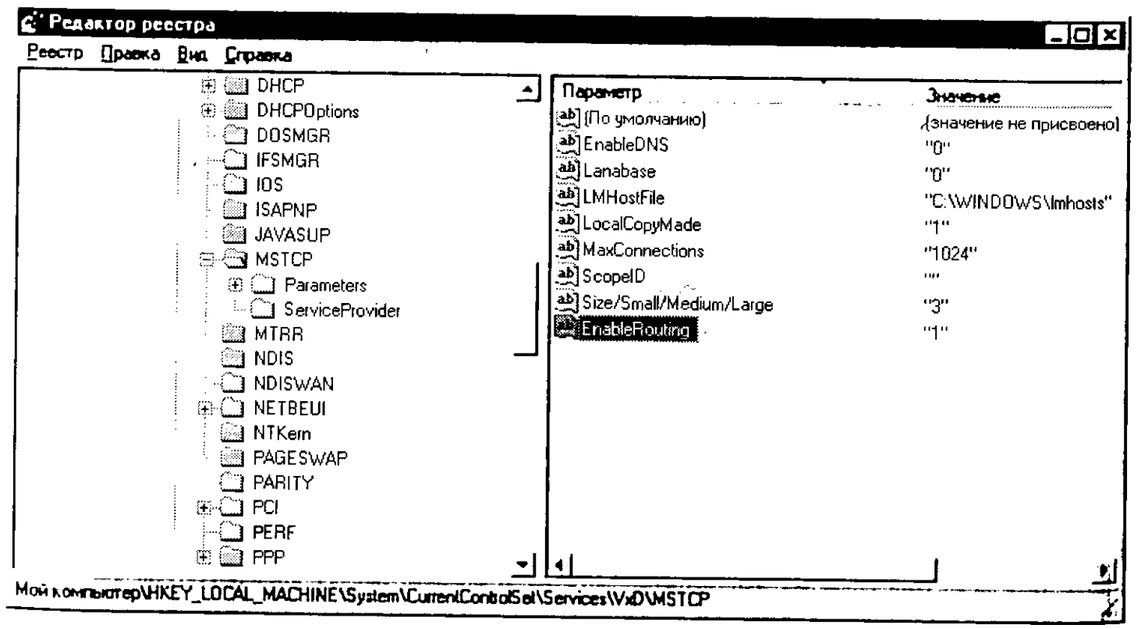


Рис. 14.6. *Редактор реестра*

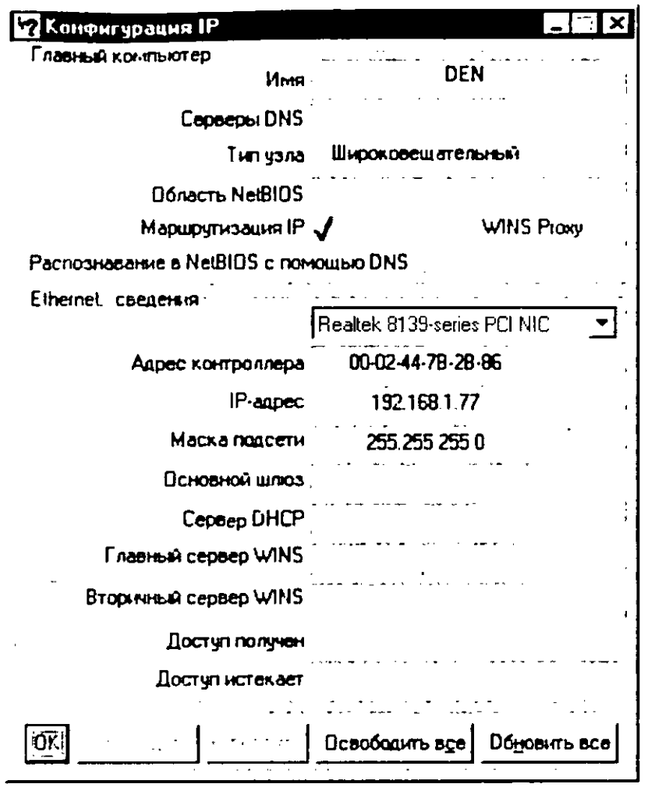


Рис. 14.7. *Программа winipcfg — маршрутизация включена*

не очень требовательна к системным ресурсам (по сравнению с Windows 2000 и Windows 2003 Server).

Для нормальной работы маршрутизатора на базе Windows NT вполне хватит следующей конфигурации Pentium 133, 32 Мб ОЗУ, жесткий диск 500...1024 Мб. Вы со мной не согласны? Маршрутизатор — это такой компьютер, за которым постоянно не работают пользователи. Фактически, его нужно настроить один раз и забыть. Никакого «офиса», никаких других пользовательских приложений. Чтобы «переложить» пакет с одного интерфейса на другой, 32 Мб оперативной памяти вполне достаточно. NTFS на маршрутизаторе также не нужна.

Если же вы все-таки отформатировали жесткий диск под NTFS, вам понадобится еще 32 Мб оперативной памяти. На 32-х тоже будет работать, но загрузка маршрутизатора будет выполняться очень медленно — знаю из собственного опыта.

Windows NT 4.0 — очень надежная операционная система, ее непросто «завалить». Если отключить все неиспользуемые службы (чтобы было меньше «дыр»), NT-маршрутизатор будет служить вам верой и правдой многие годы. Вот только есть одна проблемка.

Несмотря на то, что при включении маршрутизации за вкладке **Маршрутизатора** пишется **Для установки службы RIP используется значок Сеть**,

установить службу RIP мне так и не удалось — ее просто нет в списке служб. Причем я использовал разные версии Windows NT (разные версии сборки и разные языки). Поэтому, видимо, от динамической маршрутизации придется отказаться или же установить Windows NT 4.0 Server — там со службой RIP нет никаких проблем. Но тогда вам понадобится еще 32 Мб оперативной памяти для нормальной работы сервера.

Устанавливать Windows 2000 или Windows 20003 Server только для маршрутизации я не вижу смысла — это все равно, что из пушки по воробьям стрелять. Если же этот компьютер будет использоваться также для решения других задач, например, как шлюз, Web-сервер, контроллер домена, тогда можно.

14.3. Маршрутизация в Linux

14.3.1. Программы маршрутизации в Linux

Программа routed

Стандартной программой маршрутизации в Linux является демон **routed**. Этот демон, как правило, выявляет конфигурацию динамически и не требует конфигурирования. Обнаруженные маршруты он заносит в маршрутную таблицу ядра.

В своей работе демон **routed** использует протокол RIP. Чтобы воспользоваться протоколами RIP-2 или OSFP, вы должны использовать программу-демон **gated** (см. ниже). Демон **routed** может работать либо в режиме сервера (-s), либо в режиме подавления сообщений. Во втором режиме он будет только получать от соседей маршрутную информацию, но сам ее отсылать не будет.

Чтобы вручную внести какой-либо маршрут используется команда **route**. Эта команда используется для задания статических маршрутов. Дальше рассмотрим небольшой пример.

Пусть, у вас есть две сетевые платы `eth0` и `eth1`:

```
ifconfig eth0 192.168.1.1 up
ifconfig eth0 192.168.2.1 up
```

И вам нужно обеспечить маршрутиризацию между подсетями 192.168.1.0 и 192.168.2.0. С этой целью объявляем, что машины, которые находятся в вашем локальном сегменте 192.168.1.* «сидят» на первом интерфейсе и общаться с ними нужно напрямую:

```
route add net 192.168.1.0 192.168.1.1 netmask 255.255.255.0 0
```


А с машинами с адресами 192.168.2.* будем разговаривать через `eth1`:

```
route add net 192.168.2.0 192.168.2.1 netmask 255.255.255.0 0
```

Последний параметр — это метрика. Ее можно понимать как «расстояние до шлюза-назначения» или «сколько пересадок между шлюзами придется сделать пакету по пути и обратно». Т.к. адреса 192.168.1.1 и 192.168.2.1 являются нашими собственными адресами, то метрика равна 0.

Сетевые пакеты для IP-адресов, которые не лежат в нашей локальной сети, будем отправлять на машину 192.168.1.11, а она сама будет разбираться, что с ними делать:

```
route add default 192.168.1.11 1
```

Другими словами, сейчас мы объявили маршрут по умолчанию. Обратите внимание на значение метрики = 1.

Как видите, мы все сделали без всяких конфигураторов — все просто и логично. Только не забудьте добавить вызовы команды route в сценарий автозапуска системы, поскольку при перезагрузке правила маршрутизации ядра теряются.

Кстати говоря, данный статический маршрут по сути представляет собой обычное правило перенаправления трафика. Поэтому его с успехом можно реализовать средствами бастиона IPTables:

```
iptables -P FORWARD DROP
iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.2.0/24 -j ACCEPT
iptables -A FORWARD -s 192.168.2.0/24 -d 192.168.1.0/24 -j ACCEPT
```

Вот более сложный пример, приведенный в документации по IPTables. В данном примере у нас имеется одно единственное соединение с Internet и мы не хотим, чтобы кто-либо вошел в нашу сеть извне.

```
## Загрузим модули для отслеживания соединений(не нужно
## если они встроены в ядро)
# insmod ip_conntrack
# insmod ip_conntrack_ftp

## Создадим цепь block, которая будет блокировать
# соединения извне.
# iptables -N block
# iptables -A block -m state –state ESTABLISHED,
# RELATED -j ACCEPT
# iptables -A block -m state –state NEW -i ! ppp0 -j
```

```
# ACCEPT
# iptables -A block -j DROP
## Весь входящий и маршрутизированный трафик
# будет проходить через block
# iptables -A INPUT -j block
# iptables -A FORWARD -j block
```

Программа gated — правильный выбор

В последнее время демон **gated** используется чаще, чем стандартный **routed**. Объясняется данная тенденция тем, что **gated** более гибок в конфигурировании и обладает большими возможностями. В частности, им поддерживаются протоколы RIP-2 и OSFP.

Программа **gated** была разработана группой американских университетов для работы сети NFSNET. Она позволяет организовать многофункциональный шлюз, обслуживающий как внутреннюю, так и внешнюю маршрутизацию. На данный момент Gated поддерживает следующие протоколы маршрутизации:

- RIP версий 1 и 2;
- HELLO;
- OSPF версии 2;
- EGP версии 2;
- BGP версии 2, 3 и 4.

Табл. 14.3. поможет вам сравнить возможности демонов **routed** и **gated**.

Протоколы, поддерживаемые gated и routed *Таблица 14.3*

Демон	Протоколы внутренних маршрутизаторов			Протоколы внешних маршрутизаторов	
	RIP	HELLO	OSPF	BGP	EGP
routed	V1	-	-	-	-
gated, версия 2	V1	+	-	V1	+
gated, версия 3	V1, V2	+	V2	V2, V3	+

Рассмотрим классическое подключение локальной сети к Интернету. Пусть адрес нашей локальной сети: 143.100.100.0, на шлюзе установлены две сетевые платы с IP-адресами 143.100.100.1 и 143.100.200.1 — данная информация нам понадобится для настройки **gated**.

В нашей сети есть машина с IP-адресом 143.100.100.5, на которой также установлен **gated**. Настроим **gated** сначала на этой рабочей станции, а потом — на сервере. Для настройки может использоваться утилита **gdc**, поставляемая вместе с самим **gated**.

Настройка **gated** осуществляется путем редактирования файла конфигурации /etc/gated.conf. Содержимое этого файла для рабочей станции приведено в листинге 14.1.

Листинг 14.1. Файл конфигурации /etc/gated.conf для рабочей станции

```
# Это IP-адрес рабочей станции
interface 143.100.100.5 passive ;
# используем протокол RIP (Route Internet Protocol)
rip yes;
```

На этом настройка рабочей станции завершена, и мы можем перейти к серверу (см. листинг 14.2).

Листинг 14.2. Файл конфигурации /etc/gated.conf для рабочей станции

```
# Описываем интерфейсы и протокол
interface 143.100.100.1 passive ;
interface 143.100.200.1 passive ;
rip yes;

export  proto rip interface 143.100.100.1
{
    proto direct
    {
            announce 143.100.200.0 metric 0 ;
    } ;
} ;
export proto rip interface 143.100.200.1
{
    proto rip interface 143.100.100.1
    {
            announce all ;
    } ;
} ;
```

Теперь разберемся, что же делает директива **export**. Первая директива **export** объявляет подсеть 143.100.100.0 (наша сеть) через интерфейс 143.100.100.1. При этом считается, что это шлюз в данную подсеть. Другими словами, считается, что интерфейс 143.100.100.1 принадлежит узлу, входящим в эту сеть. Директива **proto direct** говорит о том, что пакеты для подсети нужно посылать непосредственно на интерфейс, а нулевая метрика означает, что интерфейс стоит на шлюзе в подсеть.

Вторая директива **export** сообщает всем узлам подсети через интерфейс 143.100.200.1 все маршруты, которые данный шлюз получает из подсети 143.100.100.1 через интерфейс 143.100.100.1.

При написании директив **export** внешняя конструкция всегда определяет интерфейс, через который сообщается информации, а внутренняя — определяет источник, через который эту информацию будет получать **gated**.

Рассмотрим пример из документации по **gated**. В данном примере нашу сеть через подсеть подключают к Интернет (см. листинг 14.3).

Листинг 14.3. Подключение к Internet через подсеть

```
rip yes;
export proto rip interface 136.66.12.3 metric 3
{
    proto rip interface 136.66.1.5
    {
            announce all ;
    } ;
} ;
export proto ripinterface 136.66.1.5
{
    proto rip interface 136.66.12.3
    {
            announce 0.0.0.0 ;
    } ;
} ;
```

Первая директива **export** говорит о том, что **gated** получает все, что передается в подсеть, связывающую данную сеть с Internet через интерфейс 136.66.12.3 (имеются в виду только маршруты, а не данные).

Вторая директива export определяет место назначения: куда по умолчанию нужно отправлять информацию из сети, чтобы она достигла адресата, который расположен за пределами локальной сети. Адрес 0.0.0.0, соответствующий любой машине за интерфейсом 136.66.12.3, определяется через интерфейс 136.66.1.5 для всей локальной сети.

После настройки **gated** нужно перезапустить:

```
service gated restart
```


14.3.2. Расширенные средства маршрутизации. Комлекс iproute2

Начиная с версии ядра 2.2 была значительно переработана сетевая подсистема Linux, в нее было добавлено много расширенных возможностей, таких как управление трафиком, маршрутизация на основе правил и т.д. Доступ к данным возможностям предоставляется пакетом **iproute2**, входящим в состав большинства современных дистрибутивов.

В случае необходимости можно скачать этот пакет с сайта `ftp://ftp.inr.ac.ru./ip-routing/`.

Команда ip — Общее описание

Утилита **ip**, входящая в состав **iproute2**, объединяет в себе все возможности команд **ifconfig**, **arp** и **route**. Формат ее вызова такой:

ip [Опции] Объект [Команда [Аргументы команды]]

Вы можете указать следующие опции:

-s ..... вывод статистической информации;
-f..... указывается перед идентификатором протокола;
-r ..... разрешать IP-адреса в имена узлов;
-V ..... печать версии программы.

О параметре –f нужно поговорить подробнее. С его помощью можно выбрать протокол:

-f inet ..... протокол IPv4;
-f inet6..... протокол IPv6;
-f link..... сетевое устройство.

Параметр **Объект** позволяет выбрать объект, с которым будем работать:

адрес..... IPv4 или IPv6 адрес устройства;
link..... устройство;
neighbour ..... ARP-адрес;
route ..... маршрутизация;
rule ..... база данных правил маршрутизации;
madress ..... широковещательный адрес;
tunnel ..... туннель через IP.

Параметр **Команда** описывает действие над **Объектом**.

ip link ..... конфигурация сетевого устройства;
ip link set..... изменение параметров сетевого устройства;
ip link show .... просмотр параметров сетевого устройства.

Изменение параметров сетевого устройства

При изменении параметров мы можем задать следующие аргументы:

up ..... включить;
down ..... выключить;
arp on или **arp off** ..... изменение флага NOARP на устройстве;
dynamic on или **dynamic off** ..... изменяет флаг DYNAMIC на устройстве;
multicast on или **multicast off** ..... изменяет флаг MULTICAST на устройстве;
name ..... изменяет имя устройства;
mtu *Число* ..... изменяет значение MTU на устройстве;
address *Адрес* ..... изменяет адрес на устройстве;
broadcast *Адрес* ..... изменяет широковещательный адрес на устройстве.

Просмотр параметров сетевого устройства

Команду **ip link show** лучше всего рассматривать на примерах. Для получения информации о состоянии устройства `eth0` введите команду:

```
# ip link ls dev eth0
eth0:  mtu 1500 qdisc cbq qlen 100
link/ether 00:44:67:91:31:1d brd ff:ff:ff:ff:ff:ff
```

Получить статистику устройства `eth0` можно командой:

```
#ip -s link ls dev eth0
2: eth0:  mtu 1500 qdisc cbq qlen 100
link/ether 00:44:67:91:31:31 brd ff:ff:ff:ff:ff:ff
RX: bytes  packets  errors  dropped overrun mcast
xxxxxxxx   xxxxxx 0        0        0        0
TX: bytes  packets  errors  dropped carrier collsns
xxxxxxxx   xxxxxx 0        0        0        132934
```

Вместо xxxxxxxx xxxxxx вы увидите количество принятых (RX) / переданных (TX) байтов и пакетов.

Операции над адресами. Команда ip address

Команда **ip address** управляет адресами на устройстве. Для данной команды **Объект** — это IPv4 или IPv6 адрес. Команда **ip address** показывает

адреса и их свойства, а также добавляет новые адреса, как это показано в ледующеме примере:

```
ip addr add 192.168.0.1/24 brd + dev eth0 label eth0:Alias
```

Данная команда добавляет адрес 192.168.0.1/24 с маской подсети 255.255.255.0 со стандартным широковещательным адресом и именем `eth0:Alias`.

Помимо стандартного используются еще следующие варианты команды **ip address**:

- Команда **ip address delete** предназначена для удаления адресов. Для удаления адреса 192.168.0.1/24 с устройства `eth0` введем команду **`ip addr del 192.168.0.1/24 dev eth0`**;
- Команда **ip address show** — выводит информацию об адресе.

Управление таблицей маршрутизации

Команда **ip route** управляет таблицей маршрутизации и может применяться в следующих вариантах:

- **ip route add** — добавить новый маршрут;
- **ip route change** — изменить маршрут;
- **ip route replace** — заменить маршрут.

Например, добавление маршрута к сети 192.168.0.0/24 через 192.168.1.1 выглядит следующим образом:

```
ip route add 192.168.0.0/24 via 192.168.1.1
```

Динамическая маршрутизация

Команда **ip route** позволяет добавить динамический маршрут: шлюз будет выбираться в зависимости от нагрузки на данный шлюз. Всегда будет выбираться шлюз с минимальной нагрузкой. В данном случае у нас есть два устройства — `ppp0` и `ppp1`. Маршрут по умолчанию — через устройство `ppp0`, но если этот маршрут недоступен, будет использоваться `ppp1`:

```
ip route add default scope global nexthop dev ppp0 nexthop dev ppp1
```

Для удаления маршрута используйте команду **ip route delete**:

```
ip route del default scope global nexthop dev ppp0 nexthop dev ppp1
```

Управление правилами маршрутизации

Для решения этой задачи предназначена команда **ip rule**. Маршрутизация производится в зависимости от:

- адреса получателя;
- адреса источника;
- IP-протокола;
- транспортного протокола.

По умолчанию используются три таблицы правил маршрутизации:

- **Local** — содержит таблицы для локальных и широковещательных адресов;
- **Main** — самая обыкновенная таблица маршрутизации;
- **Default** — пустая таблица по умолчанию.

Аргументы команды **ip rule**:

- адрес-источник;
- адрес-назначение;
- имя интерфейса, с которого получен пакет;
- метка пакета, которая устанавливается брандмауэром;
- идентификатор таблицы маршрутизации, ним может быть номер или строка из файла `/etc/iproute2/rt_tables`;
- приоритет таблицы (число).

Вот несколько примеров. Пересылать пакеты с сети 192.168.0.0/24 согласно таблицы `main`:

```
ip ru add from 192.203.80.0/24 table main prio 100
```

Предположим, что у нас есть два канала в Интернет — у одного провайдера и у другого:

- ppp1 с адресом 193.168.99.99, который связан с 193.168.99.100;
- ppp2 с адресом 193.168.100.99, связанный с 195.1.1.1.

Пользователь `ivanov` хочет, чтобы мы его пакеты отправляли через **ppp2** (второго провайдера):

```
# echo 200 ivanov >> /etc/iproute2/rt_tables
# ip rule add from 192.168.0.10 table ivanov
# ip rule ls
0: from all lookup local
32765: from 192.168.0.10 lookup ivanov
32766: from all lookup main
32767: from all lookup default
```


Теперь для этого пользователя назначим маршрут по умолчанию и очистим кэш-таблицы маршрутизации, чтобы наши изменения вступили в силу:

```
# ip route add default via 195.1.1.1 dev ppp2 table ivanov
# ip route flush cache
```

Рассмотрим еще один практический пример: направим весь трафик на порт 21 через устройство `eth1`:

```
# iptables -A PREROUTING -i eth0 -t mangle -p tcp –dport
21 -j MARK –set-mark 2
```

Теперь нужно создать правила для помеченных пакетов:

```
# echo 202 21.tbl >> /etc/iproute2/rt_tables
# ip rule add fwmark 2 table 21.tbl
# ip route add default via 192.168.0.10 dev eth1 table 21.tbl
# ip route flush cache
```

ЧАСТЬ 4. ПОДКЛЮЧАЕМ ЛОКАЛЬНУЮ СЕТЬ К ИНТЕРНЕТУ. ОБЩИЙ ВЫХОД В ИНТЕРНЕТ

В этой части мы рассмотрим с вами как настроить подключение вашей локальной (офисной или домашней) сети к Интернету. При этом изначально нужно, чтобы один из компьютеров был подключен к Интернету (обладал возможностью доступа в Интернет). Причем неважно как: с помощью модема, по ADSL-каналу, по выделенной линии или как либо еще. Сути это не меняет — меняется только максимально допустимая скорость доступа из вашей сети в Интернет.

Смысл всех настроек, описанных в данной части книги, заключается в том, чтобы разрешить всем компьютерам сети пользоваться подключением к Интернету, настроенном на одном из компьютеров. Кроме того, описывается как с этого самого компьютера (его называют шлюзом) производить управление и контроль над доступом к Интернету, осуществляемого через него из локальной сети с других компьютеров.

При этом будем считать, что изначально вы уже настроили подключение к Интернету с одного компьютера, который будет выступать у вас в качестве шлюза. Каким образом настроить подключение к Интернету с отдельного компьютера я считаю описывать излишним. Настройка модемного соединения описана в любом самоучителе (или справочной системе операционной системы), а настройка любого другого соединения (ADSL или выделенной линии) производится под контролем самого провайдера или даже им самим. Так что никаких проблем быть не должно. В любом случае вы всегда сможете получить квалифицированную помощь у своего провайдера.

Далее рассмотрены два варианта настроек — на основе системы Windows и на основе системы Linux. В связи с этим хочется сделать небольшое, но существенное замечание. Если вы хотите добиться наибольшей скорости сетевого взаимодействия и наибольшего уровня контроля за Интернет-

трафиком, то рекомендуется в качестве шлюза использовать Linux-компьютер. Если у вас уже имеется сервер локальной сети, работающий под Windows, то, понятное дело, переделывать его не хочется. Да оно и не нужно. Можно просто в качестве сервера локальной сети использовать Windows-сервер, а в качестве сервера общего доступа в Интернте — Linux-машину. Тем не менее, данная рекомендация не является обязательной.

Если вы все-таки решитесь настраивать Linux-сервер, то настоятельно рекомендую прочесть книгу «Linux-сервер своими руками», написанную мною и вышедшую уже вторым изданием в издательстве «Наука и Техника». В гл. 17 хотя и описано, как на основе Linux настроить шлюз (сервер для подключения локальной сети к Интернету), но сделано это просто в виде частного примера, без особых пояснений.

Для полного понимания дела нужна отдельная книга по данной теме. Поэтому если соберетесь настраивать Linux-сервер, может быть не сразу — но обязательно прочитайте книгу «Linux-сервер своими руками». Ее объем свыше 700 страниц и в ней вы найдете все необходимые пояснения и описания. Это я пишу не в качестве рекламы, а качестве объяснения того, что подробно описать настройки Linux-сервера в данной книге я просто не могу, так как это отдельная тема. Если что-то подробно не рассмотрено, это не значит, что я что-то упустил или ухожу от ответа. Просто я это рассмотрел в отдельной книге, специально посвященной данной теме.

Глава 15

Подключаем локальную сеть к Интернету через Windows-сервер. Программы WinGate и WinRoute

15.1. Организуем общий доступ к Интернету

15.1.1. На компьютере под управлением Windows 98 / Windows Millennium

Сразу необходимо оговориться, что ОС Windows 98 Second Edition и Windows Millennium являются мало приспособленными для организации на их основе сервера-шлюза доступа в Интернет локальной сети. Поверьте мне, лучше установить другую операционную систему. Иначе вам не избежать ни «тормозов», ни «сбоев», ни проблем с безопасностью. Если я вас не отговорил — пеняйте на себя.

Итак, в Windows 98 Second Edition и Windows Millennium Edition есть мастер домашней сети. С помощью этого мастера мы можем организовать доступ к Интернет целой домашней сети, то есть таким образом мы предоставляем наше имеющееся соединение в общее пользование. Мастер настраивает общее соединение и создает дискету, с помощью которой можно настроить все остальные компьютеры вашей сети. Остальные компьютеры сети (ваши клиенты) должны работать под управлением Windows 95 или Windows 98 SE/ME.

Для установки мастера запустите панель управления и откройте апплет **Установка/удаление программ**. Затем перейдите на вкладку **Установка Windows**, выделите компонент **Связь** и нажмите кнопку **Состав**. Вы увидите окно, в котором нужно будет выделить компонент **Общий доступ к подключению Интернета** и нажать OK (рис. 15.1). Перед этим не забудьте вставить в CD-ROM диск с дистрибутивом Windows.

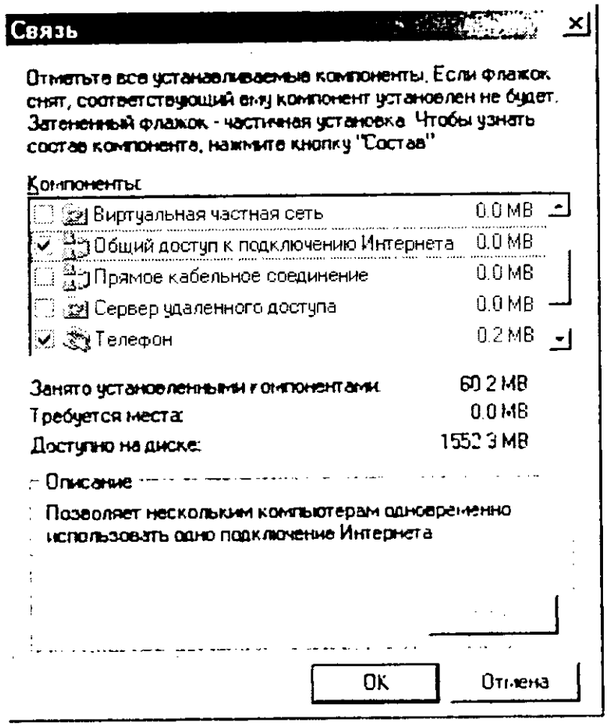


Рис. 15.1. *Установка мастера домашней сети*

После установки мастера нужно перезагрузить компьютер, а перед его запуском (после перезагрузки) желательно создать соединение, с помощью которого мы будем подключаться к Интернет. Для запуска мастера выполните команду главного меню **Пуск → Программы → Стандартные → Связь → Мастер домашней сети**.

Первый вопрос мастера связан с соединением к Интернет (рис. 15.2), а именно, вам нужно уточнить какое соединение будет использовано для общего доступа. Вам нужно выбрать опцию **Да, данный компьютер использует**, а затем опцию **Прямое подключение к поставщику услуг Интернета с помощью устройства** и выбрать настроенное соединение с Интернетом (рис. 15.3).

Затем вам нужно выбрать устройство для подключения к домашней сети — сетевой адаптер (рис. 15.4). Если он у вас один, то ничего выбирать вообще не нужно, а только нажать кнопку **Далее**.

Следующее окно очень важно. И не только потому, что в нем задаются имя пользователя и пароль. Тут вам предстоит решить, разрешить ли установку соединения по требованию одного из компьютеров (рис. 15.5).

В следующем окне нужно ввести имя компьютера (это поле уже будет заполнено) и ввести имя рабочей группы. Почему Microsoft рекомендует имя MSHOME я так до сих пор и не понял, поэтому лучше выбрать имя

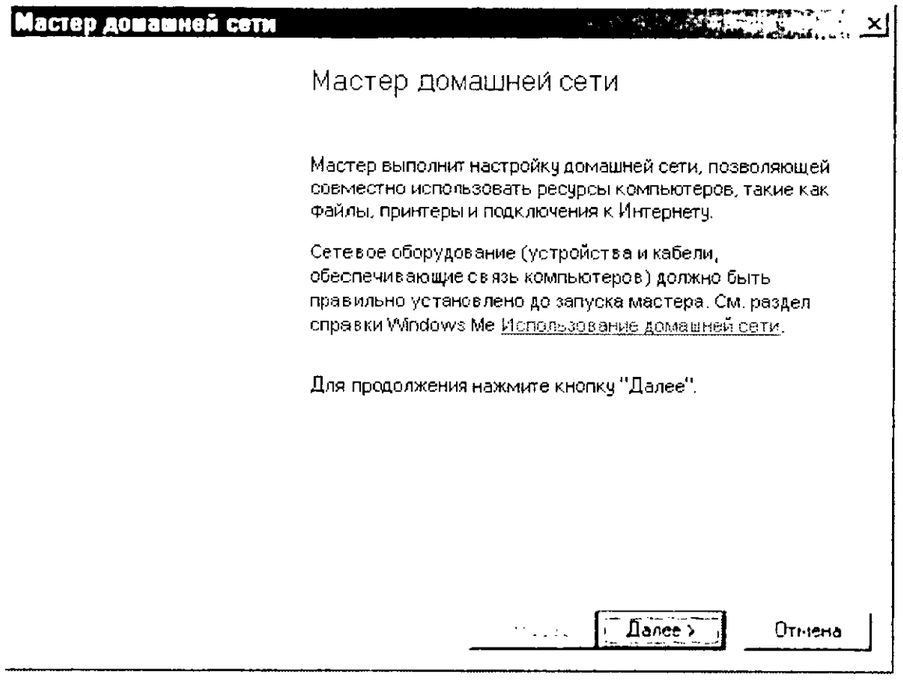


Рис. 15.2. *Мастер домашней сети*

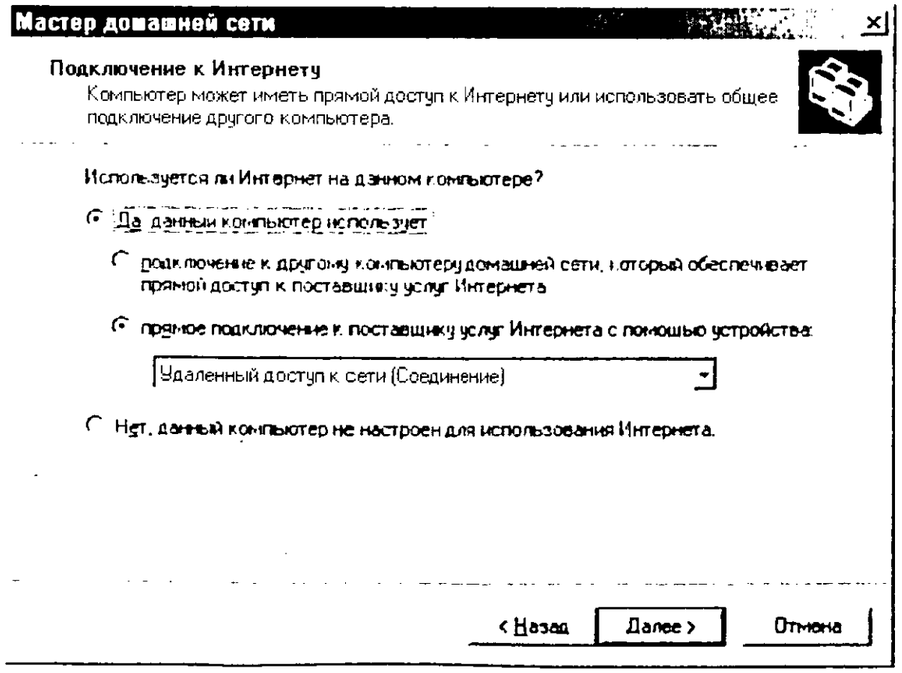


Рис. 15.3. *Выбор соединения для общего доступа*

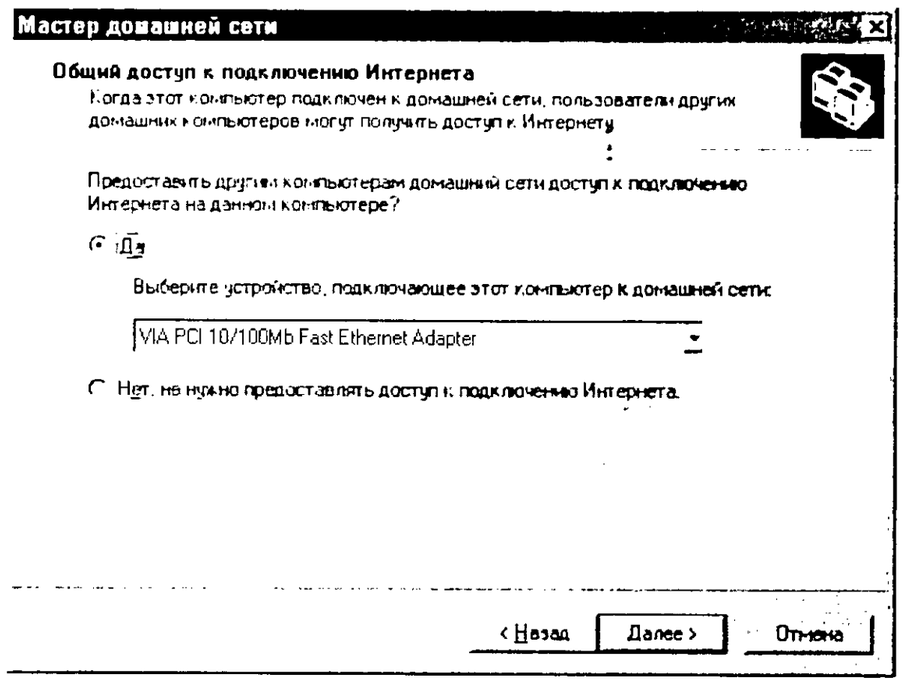


Рис. 15.4. *Выбор сетевого адаптера*

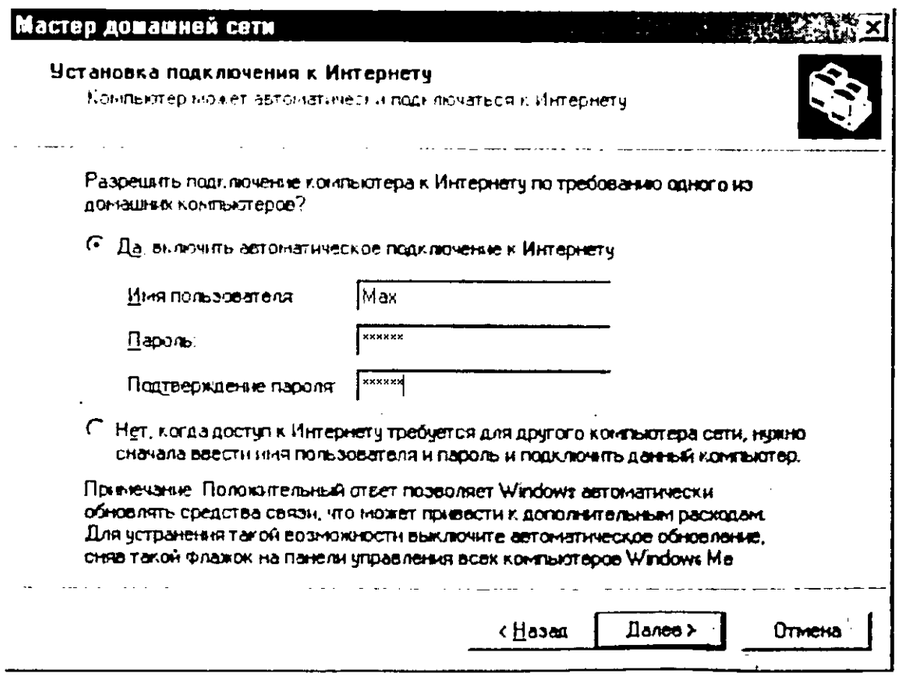


Рис. 15.5. *Разрешить установления соединения по требованию домашних компьютеров?*

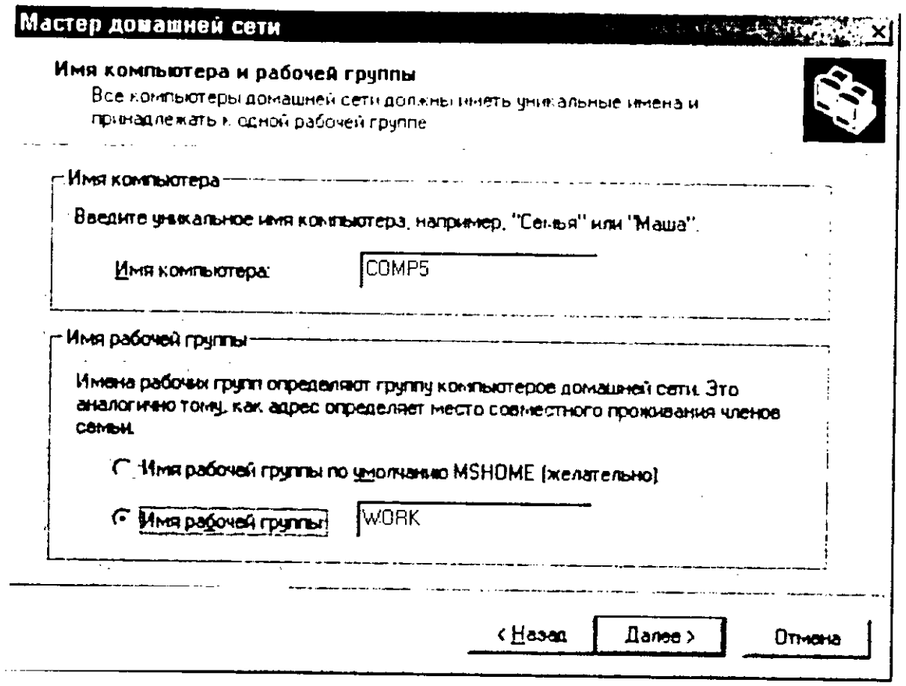


Рис. 15.6. *Имя компьютера и рабочей группы*

Следующий вопрос мастера связан с предоставлением общего доступа к файлам и принтерам. Тут ничего сложного нет: просто отметьте те объекты, которые вы хотите предоставить в общее использование.

Последний вопрос мастера связан с созданием дискеты для настройки остальных компьютеров сети. Создайте эту дискету прямо сейчас. Настройка каждого из клиентов займет не более 5 минут вашего времени. Для настройки компьютера-клиента вставьте диск настройки сети в дисковод A: и запустите программу NETSETUP, которая находится на этом диске.

15.1.2. На компьютере под управлением Windows 2000/XP

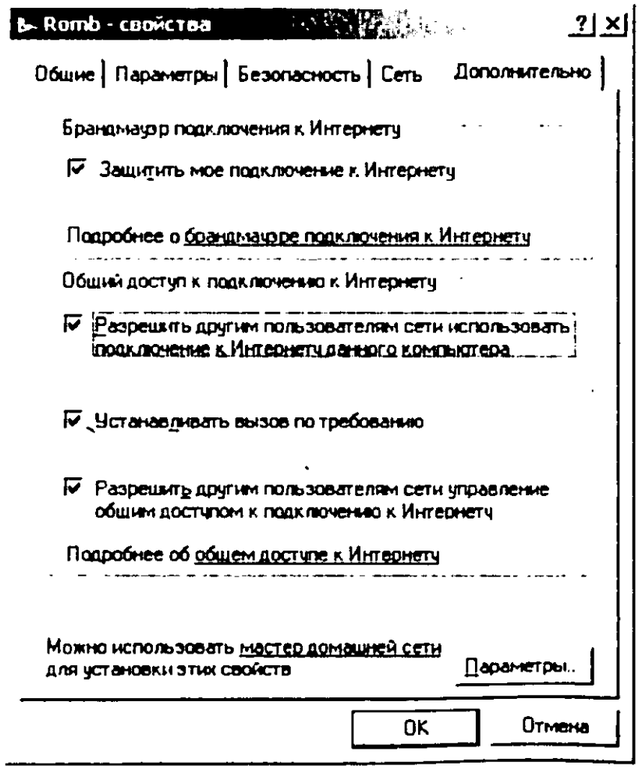
С помощью мастера

Если в вашей сети есть компьютер под управлением Windows XP, настройку общего соединения целесообразно производить на этом компьютере. Windows XP более эффективно работает не только с последовательным портом, но и с сетевыми соединениями в целом. Для настройки общего соединения вам нужно зарегистрироваться как Администратор или как пользователь, относящийся к группе Администраторы.

Для настройки общего доступа к соединению Интернета в Windows XP не нужно устанавливать специальный мастер — он уже установлен. Откройте папку **Сетевые подключения**, выберите имеющееся интернет-соединение и откройте его свойства. На вкладке **Дополнительно** включите общий доступ к соединению (рис. 15.7). Там же можно разрешить другим пользователям устанавливать соединение по их требованию и изменять параметры соединения (а вот это не рекомендуется).

Если вам удобнее использовать мастер, щелкните по ссылке Мастер домашней сети (его можно вызвать из главного меню **Пуск → Программы → Стандартные → Связь → Мастер настройки сети**). Первый вопрос мастера — это роль компьютера. На одном из компьютеров, который будет использоваться в роли шлюза для доступа в Интернет, нужно выбрать первый вариант — **Этот компьютер использует прямое подключение к Интернету. Другие компьютеры подключаются через этот компьютер** (рис. 15.8). Пример подключения показан на рис. 15.9.

Затем нам нужно выбрать соединения, которые мы хотим предоставить в совместное использование (рис. 15.10). После этого нам нужно ввести имя компьютера, его описание, а также название рабочей группы. Затем мастер выведет список всех параметров, и, если они правильны, попросит вас немного подождать.



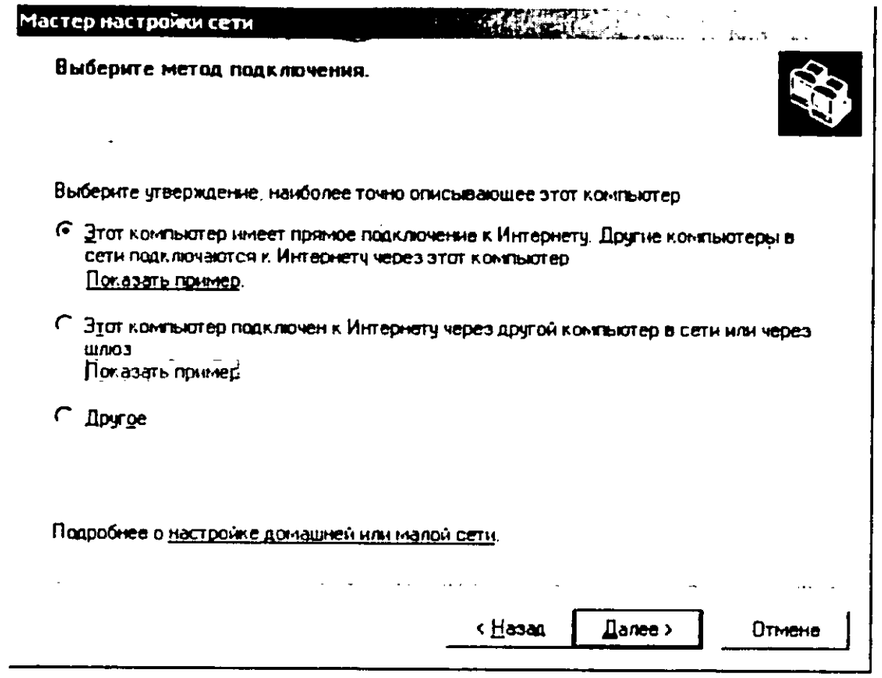


Рис. 15.8. *Мастер настройки сети*

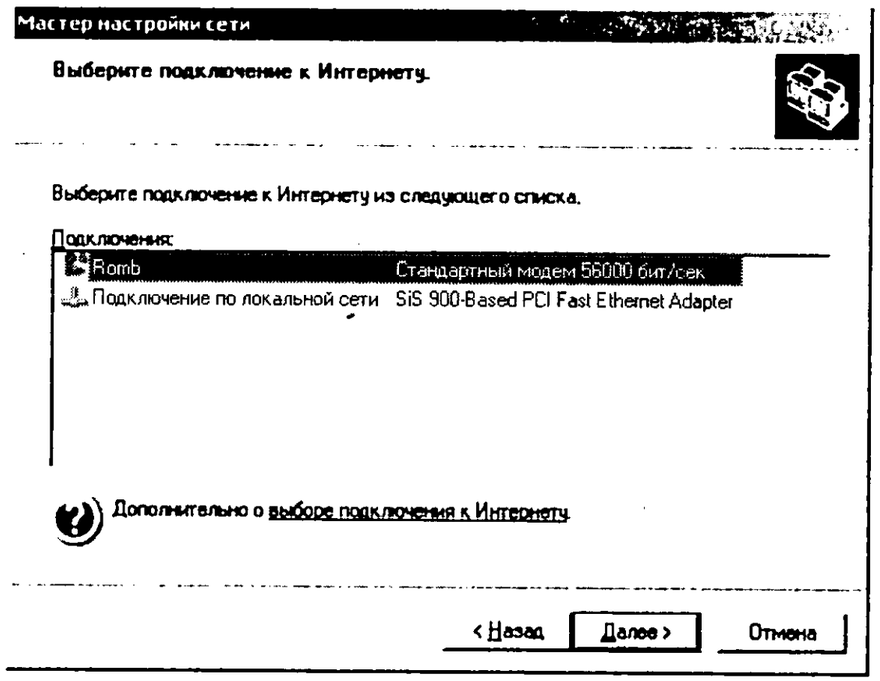


Рис. 15.10. *Выбор общего соединения*

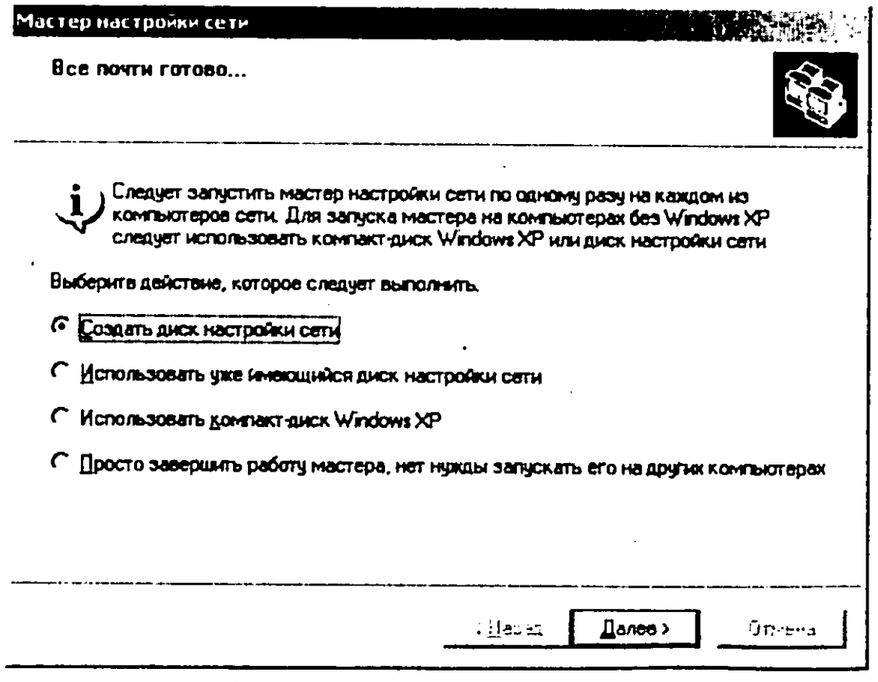


Рис. 15.11. *Почти все готово*

На предпоследнем этапе мастер предложит вам создать диск для настройки клиентов сети (рис. 15.11). Не отказывайтесь от этой возможности — тогда для настройки клиентов вам достаточно будет запустить программу NETSETUP (находится на созданном диске) на каждом компьютере и немного подождать. Если же дискеты нет, тогда вам нужно запустить мастер настройки сети вручную на каждом компьютере. Только на вопрос о методе подключения нужно выбрать второй вариант **Этот компьютер подключен к Интернет через другой компьютер** и следовать указаниям мастера.

Вручную

Теперь поговорим о настройке общего доступа вручную — без мастера. Ведь нам же нужно разобраться, что и как происходит? Когда вы в окне свойств соединения разрешаете общий доступ к соединению, происходит следующее:

- Данному компьютеру (который является шлюзом) назначается новый статический адрес — обычно 192.168.0.1.
- Обрываются все TCP/IP-соединения (если мы что-то в это время закачивали, закачка будет прервана)

На нашем компьютере будет развернут небольшой DHCP-сервер. На всех остальных компьютерах сети, если они используют статические адреса, нужно в свойствах протокола TCP/IP выбрать автоматическое получение IP-адреса. Учитывая то, что наш компьютер не только будет шлюзом, но еще и DHCP-сервером, возможность общего подключения к Интернету нельзя использовать:

- в сети, где уже есть настроенный сервер DHCP;
- в сети, где имеются контроллеры доменов, шлюзы или серверы DNS;
- в сети, рассчитанной только на использование статических IP-адресов (например, аутентификация пользователя проводится не только по имени, но и по IP-адресу).

После изменения свойств протокола TCP/IP все компьютеры вашей домашней сети нужно перезагрузить. После перезагрузки они получат свои IP-адреса, а также IP-адрес шлюза (192.168.0.1).

Стоит также отметить, чтобы клиенты могли нормально использовать службу общего доступа к Интернету (которая, кстати, называется ICS — Internet Connection Sharing), должен быть установлен браузер Internet Explorer версии 5.0 или выше. Вообще для настройки клиентов, особенно Windows 98/ME, рекомендуется использовать диск настройки сети, создаваемый мастером ICS.

Примечание.
Программа NETSEUP, создаваемая мастером настройки сети Windows XP, будет работать только на компьютерах под управлением:

- Windows 98;
- Windows 98 Second Edition;
- Windows Millennium Edition;
- Windows XP.

15.2. Управление общим подключением

В Windows 2000/XP за контроль над общим подключением к Интернету управляет служба ICS (Internet Connection Sharing). Она является достаточно развитой и позволяет решать все основные задачи. Однако большей популярностью для управления общим соединением пользуются программы WinGate и WinRoute. Они предоставляют удобный и понятный интерфейс для управления соединением, а кроме того — обладают достаточно широким спектром дополнительных полезных возможностей. Наиболее достойной из них является WinRoute. Основное внимание ей и уделим. Однако вначале кратко рассмотрим и WinGate.

15.2.1. С помощью программы WinGate

Программа WinGate условно-бесплатная (вы можете бесплатно использовать ее на протяжении 30 дней) и доступна по адресу `www.wingate.com`.

Во время установки программы вам нужно выбрать тип компьютера: клиент или сервер (рис. 15.12). Ясное дело, что сервер будет один в сети — это тот компьютер, через который все остальные будут подключаться к Интернету. Клиентами считаются все остальные компьютеры сети.

Вопросы программы установки несложные. В основном предложенные по умолчанию параметры являются вполне допустимыми, кроме одного. Когда программа установки спросит вас, какие компоненты нужно установить: все (Express setup) или только те, которые нужны вам (Custom setup). Ясное дело, выбираем второй вариант, а затем отмечаем только необходимые вам прокси-серверы. Вы будете слушать RealAudio? Нет? Так зачем вам этот прокси? Отключите его. То же касается двух последних прокси (рис. 15.13).

Затем нужно указать имя SMTP-сервера, на который будет переадресована почта. Обычно здесь указывается SMTP-сервер провайдера (рис. 15.14).

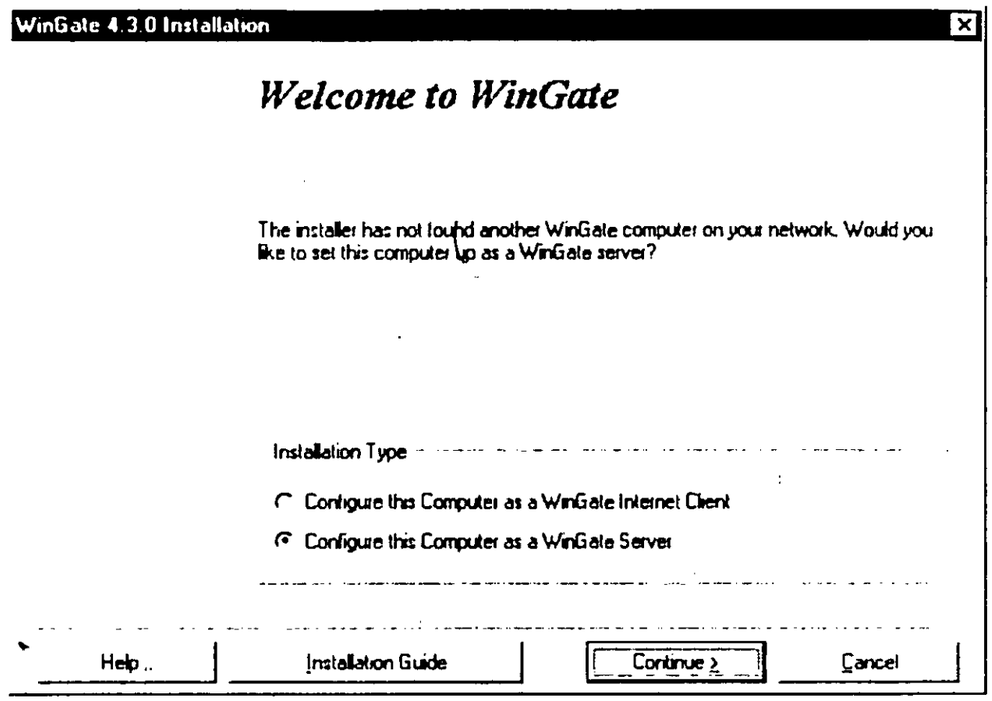
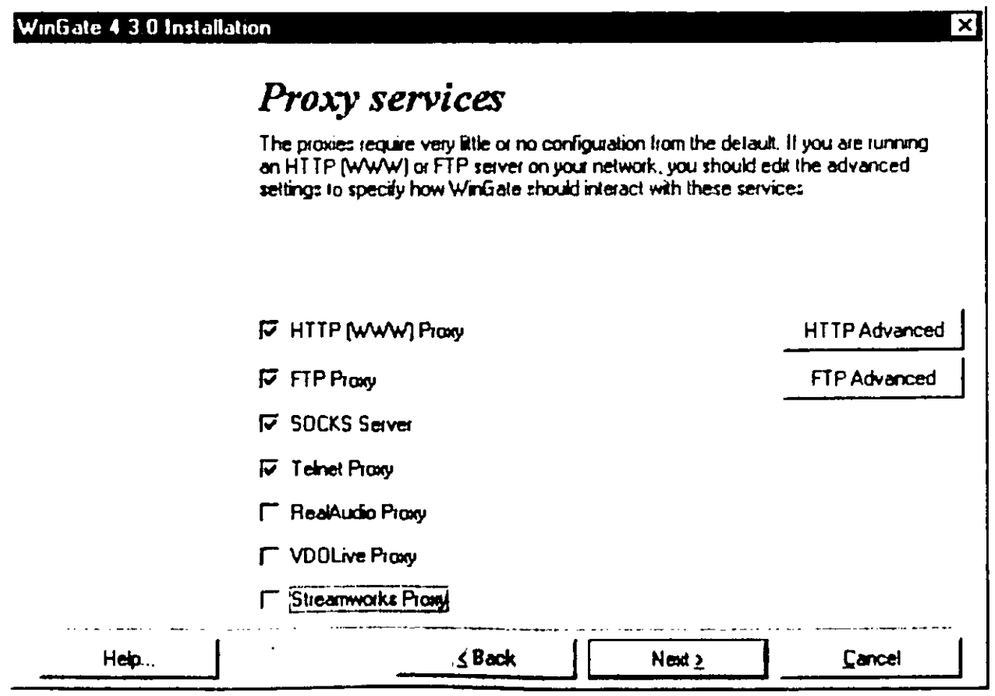


Рис. 15.12. Тип компьютера



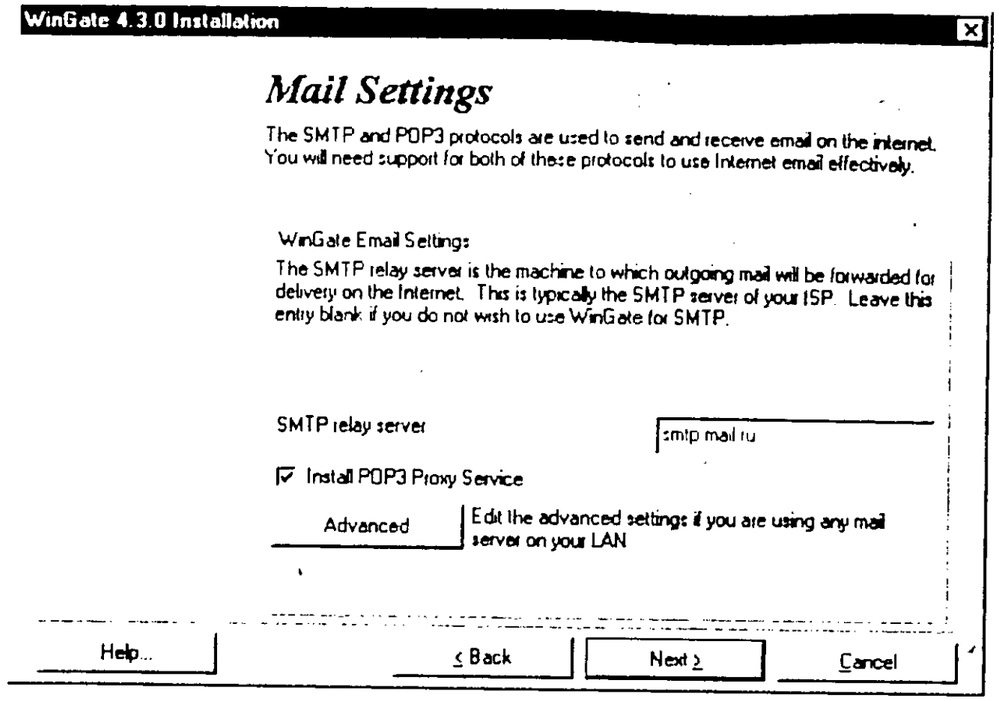


Рис. 15.14. *Параметры почты*

Параметры сервера новостей, IRC и IMAP-серверов можно оставить незаполненными. После этого можно оставить все параметры по умолчанию, кроме размера кэша прокси. По умолчанию размер равен 50 Мб. Честно говоря, это маловато, поэтому установите размер кэша из расчета Nx50, где N — это количество компьютеров в вашей домашней сети.

После установки WinGate нужно перезагрузить компьютер. После перезагрузки в нижнем правом углу (в системном tray'е) появится пиктограмма WinGate, что свидетельствует о том, что сервис WinGate запущен.

Для настройки WinGate используется программа GateKeeper. Запустить ее можно, воспользовавшись командой главного меню **Пуск → Программы → WinGate → GateKeeper**. При запуске этой программы нужно ввести имя пользователя и пароль. Имя пользователя — `Administrator`, а вместо пароля ничего вводить не нужно. При первом запуске программа примет пустой пароль и попросит вас изменить его. Минимальная длина пароля — 8 символов.

После запуска программы GateKeeper не спешите ничего делать. Сначала настроим клиенты — остальные компьютеры сети, которые будут иметь доступ к нашему подключению. Для настройки клиента нужно:

1. Установить программу WinGate, выбрав роль компьютера — клиент.
2. Изменить параметры TCP/IP: IP-адрес шлюза 192.168.1.1 (это адрес компьютера, на котором установлена программа WinGate), IP-адрес сервера DNS — тоже 192.168.1.1.

3. Перезагрузить компьютер.
4. В свойствах браузера, например, Internet Explorer отключить использование удаленного доступа к сети (см. рис. 15.15) и установить параметры прокси-сервера: IP-адрес 192.168.1.1 и порт 80 (см. рис. 15.16). Дополнительно обращаю ваше внимание, что в состав WinGate входит DHCP-сервер, поэтому вы можете все ком-

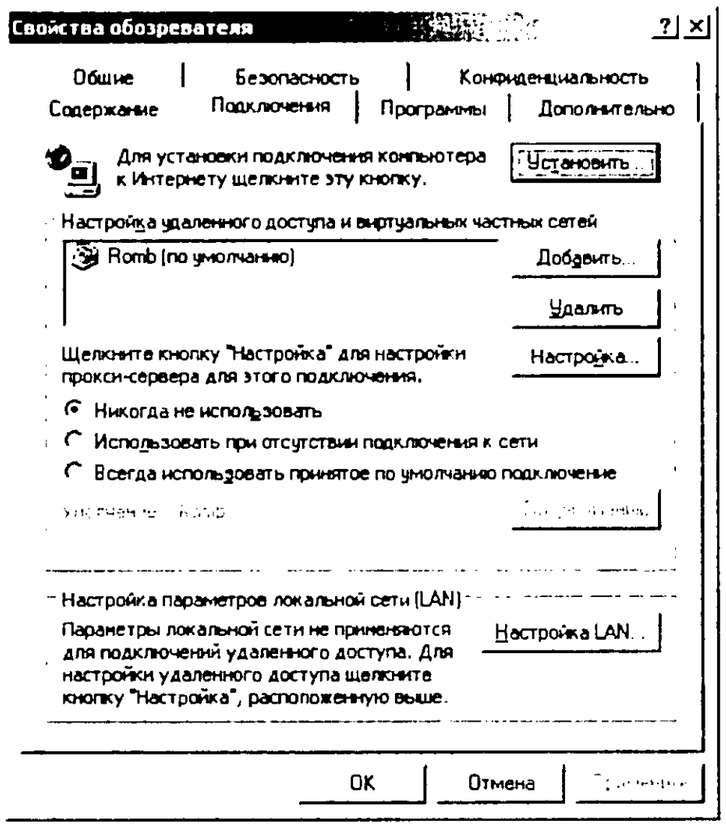


Рис. 15.15. *Параметры подключения*

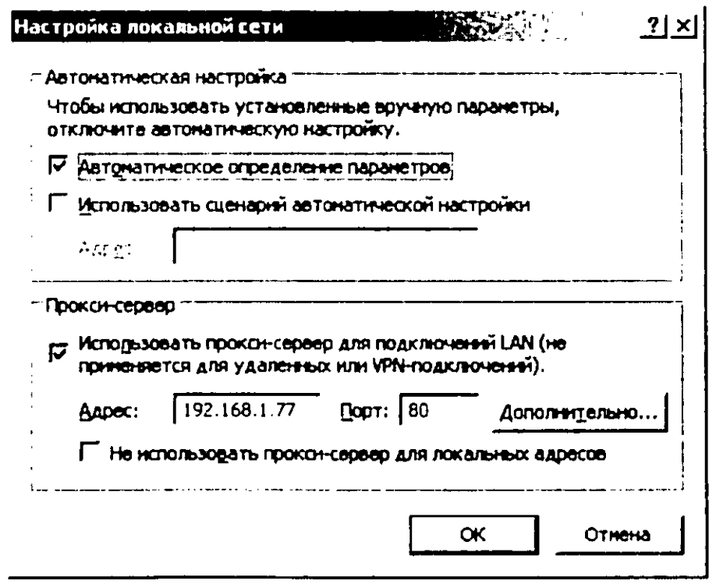


Рис. 15.16. *Параметры прокси*

пьютеры, кроме главного, настроить на автоматическое получение IP-адреса, а вместе с IP-адресом клиенты получат IP-адрес сервера DNS и IP-адрес шлюза. Поэтому, в случае автоматической настройки, вам нужно будет указать только IP-адрес прокси-сервера.

5. Запустите программу на компьютере клиента **Пуск → Программы → WinGate → WGIC Togle** и убедитесь, что WinGate-клиент включен (enabled) (см. рис. 15.17).

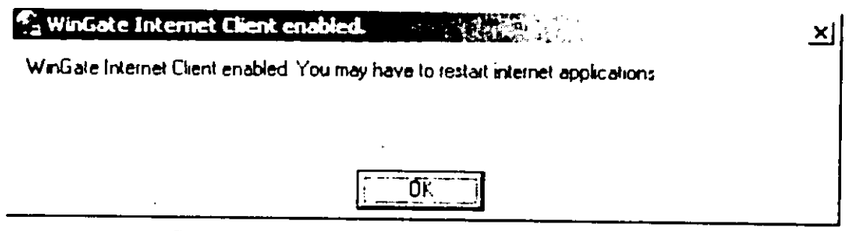


Рис. 15.17. *WinGate-клиент включен*

Вот теперь можно вернуться к компьютеру «серверу» и к программе GateKeeper. Чтобы установить соединение, перейдите на вкладку **System** (левый нижний угол) и дважды щелкните по пиктограмме **Dialer**.

В окне дайлера (рис. 15.18) вы можете выбрать соединение, которое хотите установить. Имя пользователя и пароль должны быть указаны в свойствах соединения. Выделите нужное вам соединение и нажмите кнопку **Dial**.

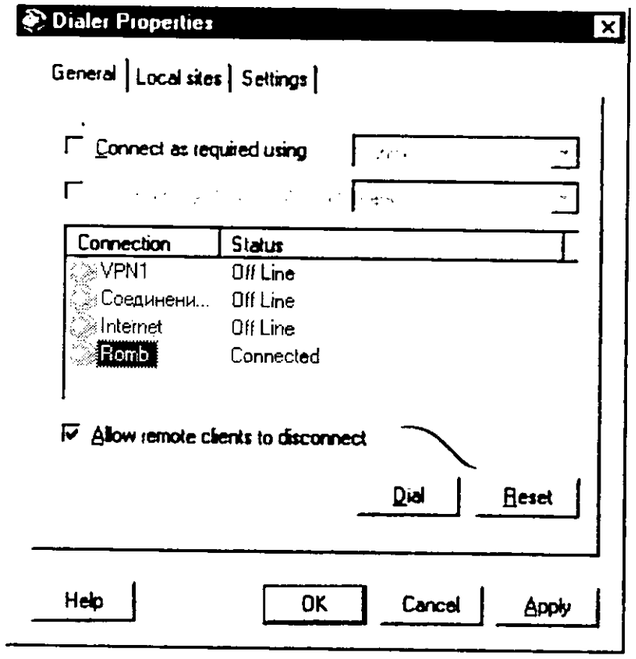


Рис. 15.18. *Дайлер*

Обратите внимание на три опции:

- **Connect as required using <имя_соединения>** — если один из компьютеров домашней сети попытается подключиться к Интернету, будет установлено подключение с выбранным соединением.
- **On failure, try to connect using <имя_соединения>** — в случае обрыва соединения будет выполнена попытка установления связи с использованием выбранного соединения.
- **Allow remote client to disconnect** — разрешить удаленным клиентам разрывать связь. Очень полезная опция: вы можете работать за другим компьютером и чтобы вам не подходить к «серверу», вы можете разорвать связь, работая за компьютером-клиентом.

Со всеми остальными опциями не составит особого труда разобраться самостоятельно. Хочу обратить ваше внимание на планировщик (Scheduler). С его помощью вы можете выполнять определенные действия, например, остановить сервис в 23-00, запустить в 7-00, или же соединиться в 7-00. Запустите планировщик (рис. 15.19).

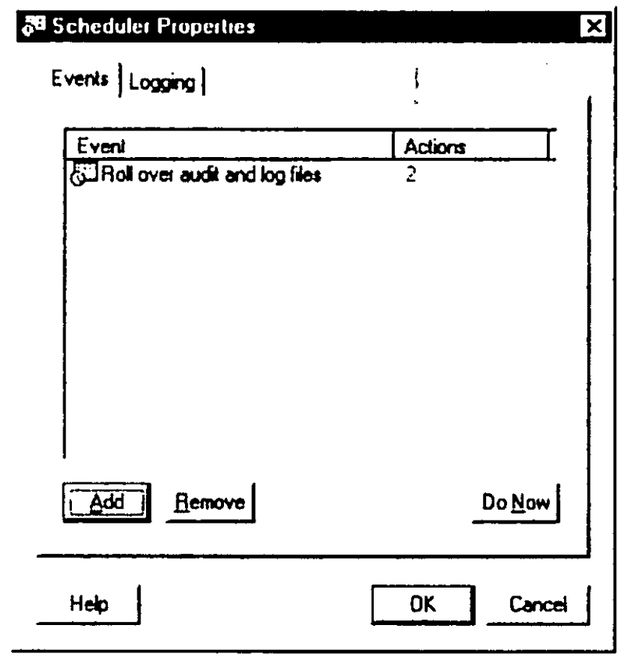


Рис. 15.19. *Планировщик*

Затем нажмите кнопку **Add**, введите описание события (например, **Stop service**), отметьте флажок **Event enabled** (Событие включено), установите, когда будет запускаться событие (рис. 15.20):

- **Daily** — каждый день;
- **Weekly** — каждую неделю;
- **Monthly** — каждый месяц;
- **Hourly** — каждый час.

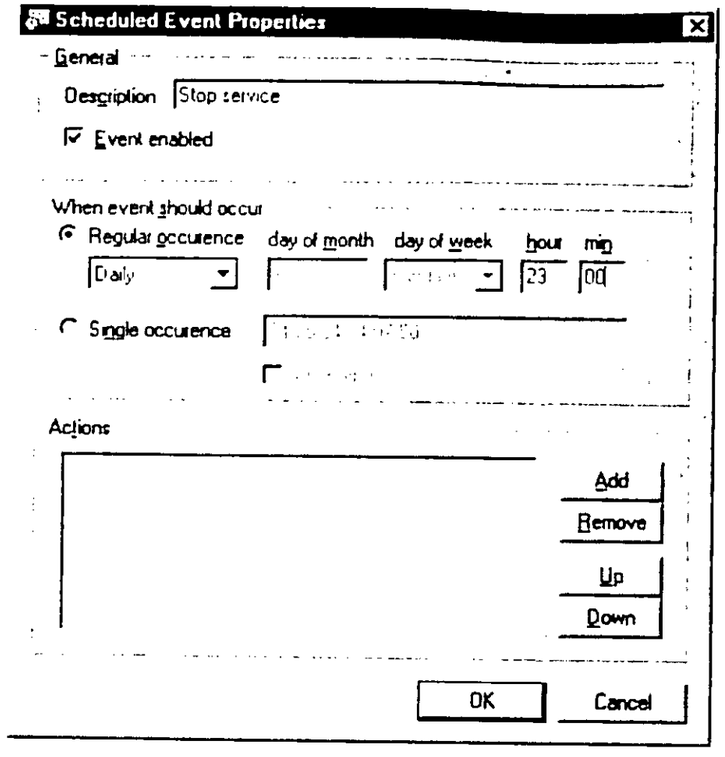


Рис. 15.20. *Редактирование события*

Затем нажмите кнопку **Add**, чтобы добавить действие (рис. 15.21). Действия, доступные для выбора, перечислены в табл. 15.1.

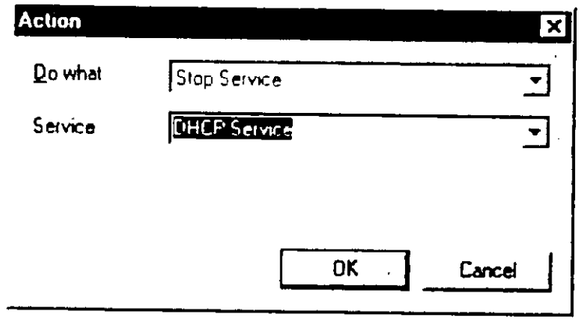


Рис. 15.21. *Выбор действия*

Действия планировщика WinGate *Таблица 15.1*

Действие	Описание
Do nothing	Ничего не делать
Stop/start service	Остановить/запустить службу. Вам понадобится уточнить, какую именно службу вы хотите остановить или запустить
Stop/start all services	Остановить/запустить все службы
Dial profile	Соединиться, используя профиль. Вам нужно будет утонить название профиля (соединения)

Таблица 15.1 (продолжение)

Действие	Описание
Hang up profile	Разорвать соединение с профилем, нужно уточнить с каким именно
Roll over logfiles	Выполнить ротацию журналов
Roll over Audit files	
Export user accounts	Экспортировать учетные записи пользователей в файл, вам нужно указать имя файла
Reset user account	Сбросить учетную запись
Reset all user accounts	Сбросить все учетные записи
Purge cache	Очистить кэш
Terminate all sessions	Прекратить все сеансы
Execute comandline	Выполнить команду (вам нужно будет указать командную строку)
Purge history database	Очистить базу данных истории
Send message to clients	Отправить широковещательное сообщение клиентам
Reminder	Используется для напоминания. Вы можете указать сообщение, дату и время и оно будет вам отправлено в указанный срок.
Enable/Disable	Включить/выключить пользователя. Можно выключать администратора на ночь – чтобы никто другой, пока вы спите, не изменил настройки WinGate. Только не забудьте включить запись утром (для этого вечером нужно создать соответствующее событие)
Backup WinGate registry	Сделать резервную копию реестра WinGate

15.2.2. С помощью программы WinRoute — правильный выбор

WinRoute, поскольку данная программа интегрирует в себе следующие функции:

- **Преобразование сетевых адресов** (Network Address Translation, NAT) — обеспечивает прозрачную интеграцию локальной сети с глобальной, например, Интернетом.
- **Кэширование информации** (прокси-сервер) — позволяет ускорить доступ к часто используемым ресурсам.
- **Динамическая конфигурация узлов** (DHCP-сервер) — позволяет указать сетевые параметры всех узлов сети автоматически.
- **Функции простого почтового сервера** — WinRoute с успехом можно использовать в роли *простого* SMTP/POP-сервера.
- **Функции DNS-сервера** — наличие собственного сервера DNS позволяет немного ускорить доступ к ресурсам Сети, поскольку не нужно ждать ответа от загруженного сервера провайдера.
- **Фильтрацию пакетов** (Firewall) — обеспечит надежную защиту вашей сети от вторжения извне.
- **Удаленное администрирование шлюза** — вы можете управлять вашим шлюзом из любой точки земного шара.

И это далеко не все функции, выполняемые программой. Вы получаете одно средство с единым интерфейсом для управления вашим Windows-шлюзом. Правда, за удобства нужно платить. Лицензия на использование программы WinRoute стоит, если я не ошибаюсь, около 150 долларов (кажется, 148). Лицензионная OEM-версия Windows XP — в пределах 75 долларов. Решайте сами... Ведь можно купить Windows XP и использовать ее стандартные средства по созданию общего модемного соединения.

Установка программы и первый запуск

Бесплатно загрузить программу можно со следующих сайтов:

- `http://www.kerio.com/` — официальный сайт WinRoute
- `http://www.listsoft.ru/` — каталог программ (файл `ftp://listsoft.ru/pub/1212/kerio-wrp-425-ru-win.exe` — русская версия WinRoute Pro 4.2.5)

Что же касается новой, шестой, версии WinRoute, я не рекомендую ее вам использовать. Во всяком случае, пока — уж слишком она навороченная и глючная. Четвертая версия намного надежнее, проще в использовании и ее функций вам хватит для организации полноценного шлюза.

Установка программы занимает несколько секунд, после чего вам нужно перезагрузить компьютер. После перезагрузки компьютера вы увидите сообщение о том, что весь входящий и исходящий трафик блокирован программой WinRoute до тех пор, пока вы не введете номер лицензии (рис. 15.22). А пока ваш шлюз будет «отрезан» от вашей сети. Где взять номер лицензии говорить не стану — вы и сами знаете.

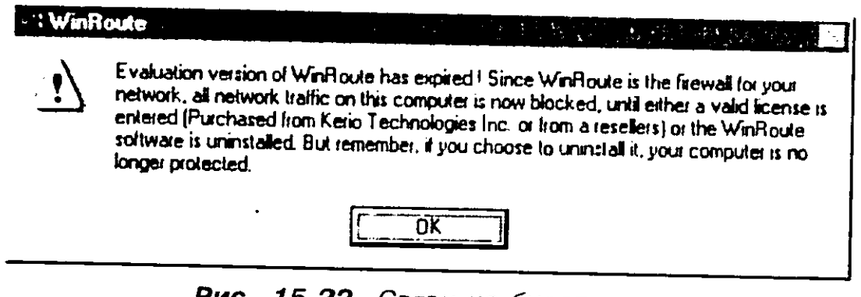


Рис. 15.22. *Связи не будет...*

Чтобы ваш компьютер смог снова работать в сети, щелкните на иконке WinRoute в системном трее и выберите команду **Stop WinRoute Engine**, а затем **Exit**. Зачем это надо? Ведь вам нужно как-то достать номер лицензии? Если WinRoute будет запущен без лицензии, вы не сможете даже работать в Интернет. Раздобыв номер лицензии, снова запустите WinRoute. В качестве имени пользователя введите `admin`, а вместо пароля ничего вводить не нужно. Для ввода номера лицензии выполните команду **Справка → О программе** и нажмите кнопку **Лицензирование**. Окно регистрации показано на рис. 15.23.

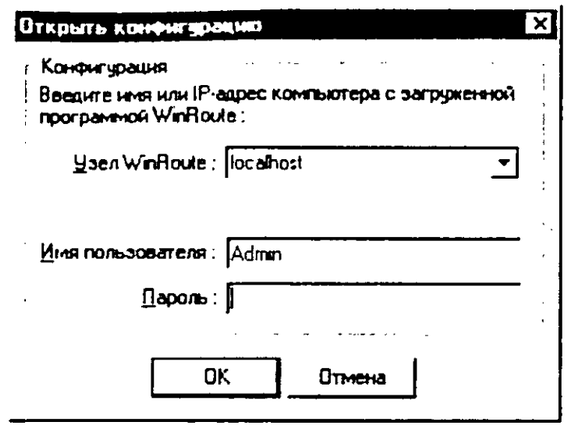


Рис. 15.23. *Регистрация в WinRoute*

Первым делом (после ввода лицензии) нужно изменить пароль администратора, дабы никто, кроме вас, не смог управлять шлюзом (рис. 15.24). Для этого выполните команду **Настройки → Учетные записи** или нажмите кнопку **Учетные записи** на панели инструментов.

Затем нажмите кнопку **Изменить**. В появившемся окне (рис. 15.25) введите новый пароль и нажмите кнопку Ok. Указывать особые параметры доступа для пользователя `Admin` не нужно — вы же не будете ограничивать сами себя.

В окне **Учетные записи** вы также можете определить группы пользователей, принадлежность пользователей к группам. Но пока этого делать не стоит — в этом нет особой необходимости.

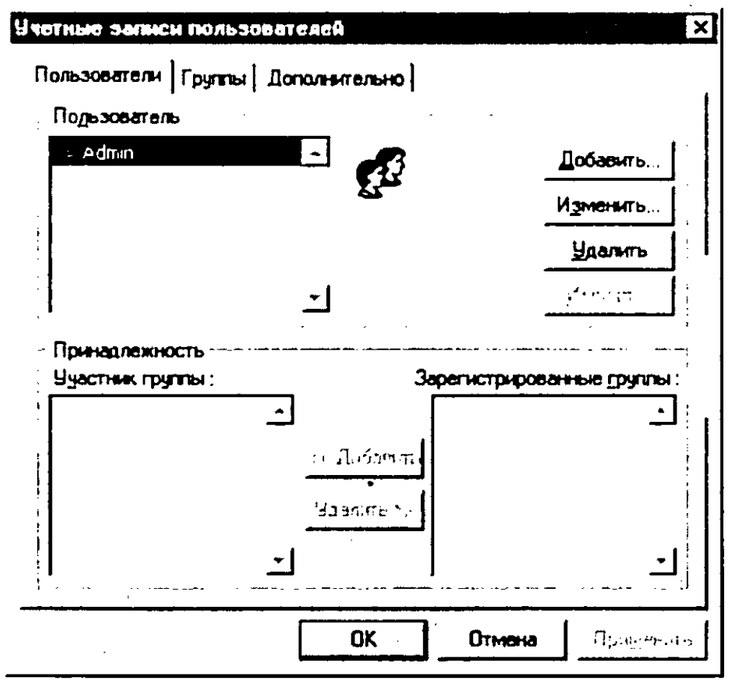


Рис. 15.24. *Учетные записи*

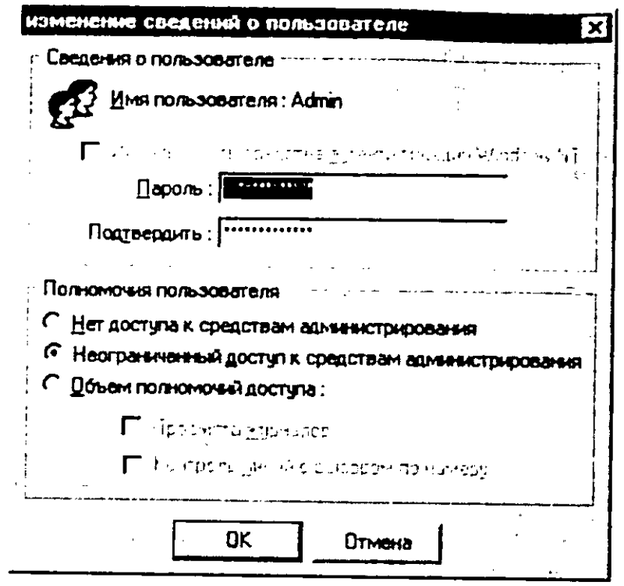


Рис. 15.25. *Редактирование учетной записи*

Преобразование сетевых адресов и WinRoute

Начнем с самой и первой и с самой главной функции WinRoute, ради которой многие пользователи, собственно, и устанавливают эту программу. Преобразование сетевых адресов позволяет скрыть настоящий IP-адрес компьютера, «замаскировав» его под адрес шлюза. Сейчас поясню. Предположим, что у нас есть пять компьютеров — это рабочие станции, и один компьютер — сервер, который будет использоваться для выхода в Интернет. Все шесть компьютеров объединены в локальную сеть и используют IP-адреса 192.168.1.1-192.168.1.6. Это так называемые локальные адреса, которые используются только в локальных сетях.

Для работы в Интернет нужны реальные IP-адреса, то есть адреса, не принадлежащие к диапазонам:

- 192.168.0.0...192.168.255.0 — сеть класса C;
- 172.16.0.0...172.16.31.0 — сеть класса B;
- 10.0.0.0 — сеть класса A.

Чтобы узел мог обратиться к Интернет-ресурсу, у него должен быть реальный IP-адрес. Покупать целую «пачку» реальных IP-адресов не рационально и дорого — ведь так ресурсы IP-адресов быстро будут исчерпаны, да и целая подсеть стоит дороже, чем один настоящий IP-адрес. Поэтому небольшие (и не только) организации ограничиваются, как правило, одним реальным IP-адресом, который присваивается компьютеру-шлюзу.

Целые подсети, состоящие из реальных IP-адресов, которые являются частью Интернет, покупают, как правило, если не считать правительственные учреждения, только Интернет- или хостинг-провайдеры.

Что же делать, если у нас всего один реальный IP-адрес, а «общаться» с Интернетом нужно всем компьютерам локальной сети. На помощь приходит преобразование сетевых адресов. Когда компьютер локальной сети, не имеющий реального IP-адреса, запрашивает Интернет-ресурс, вместо локального IP-адреса подставляется реальный IP-адрес шлюза. Удаленный ресурс «думает», что к нему обращается шлюз. Получив ответ, шлюз пересылает его локальному компьютеру. На рис. 15.26 изображена типичная локальная сеть, разбитая на два сегмента, со шлюзом для подключения к Интернету на базе WinRoute

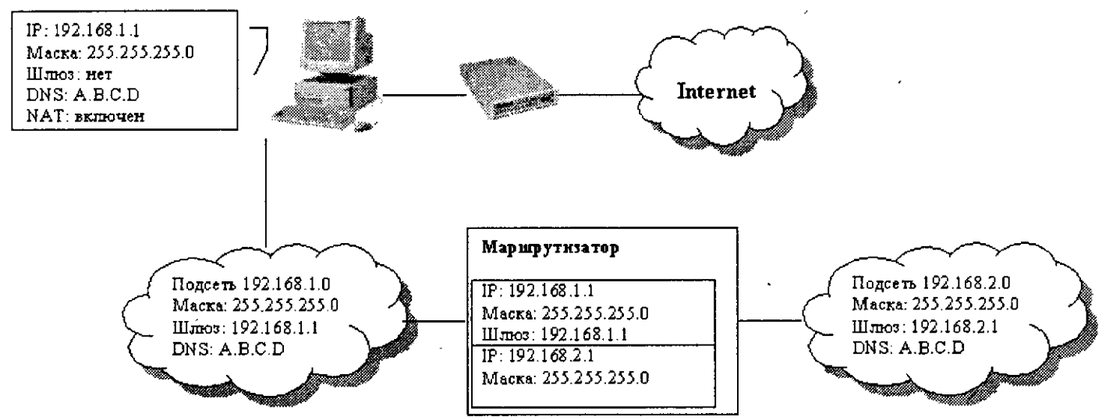


Рис. 15.26. *Схема локальной сети*

На рис. 15.26 показана сеть, разбитая на два сегмента. На компьютере-маршрутизаторе установлена программа WinRoute. Для своей работы WinRoute использует таблицу маршрутизации операционной системы Windows. Поэтому для того, чтобы WinRoute «видел» второй сегмент, нужно добавить постоянный маршрут:

```
route -p add 192.168.2.0 mask 255.255.255.0 192.168.1.77
```

На компьютере 192.168.1.77 нужно создать маршрут по умолчанию, который бы указывал на компьютер 192.168.1.1 (это компьютер, на котором установлена программа WinRoute).

Рассмотрим, как выполняется преобразование исходящих и входящих пакетов. Пусть компьютер, который посылает исходящий пакет, например, запрос удаленного ресурса, имеет адрес 192.168.1.7. Адрес удаленного ресурса — 111.111.1.56. Адрес шлюза 194.67.88.99. Преобразование проиллюстрировано рис. 15.27.

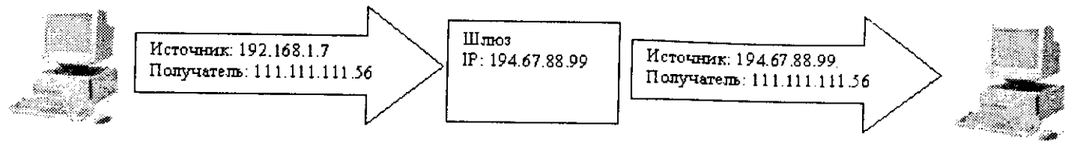


Рис. 15.27. *Преобразование исходящих пакетов*

Узел 192.168.1.7 отправляет пакет узлу 111.111.1.56. Так как адрес 192.168.1.7 не является реальным IP-адресом, шлюз выполняет преобразование адресов — замещает адрес 192.168.1.7 своим собственным адресом — 194.67.88.99. Узел 111.111.1.56 воспринимает запрос не как от узла 192.168.1.7, а как от узла 194.67.88.99.

Преобразование входящих пакетов (ответа от узла 111.111.1.56) выполняется в обратном порядке (рис. 15.28):

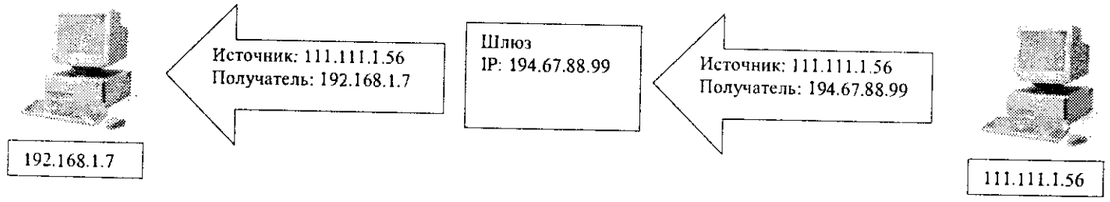


Рис. 15.28. *Преобразование входящих пакетов*

Шлюз принимает пакет от узла 111.111.1.56 и переписывает поле назначения, заменяет свой адрес адресом компьютера 192.168.1.7. Таким образом, компьютер 192.168.1.7 «думает», что получил пакет непосредственно от узла 111.111.1.56, то есть преобразование адреса выполняется совершенно прозрачно.

Преобразование адресов задается отдельно для каждого интерфейса. Включить преобразование адресов можно в окне **Интерфейсы/Преобразование сетевых адресов** (рис. 15.29).

В нашем случае NAT (преобразование адресов) включен только для интерфейса `line1` — модемного соединения. Если вы хотите включить преобразование для другого интерфейса, нажмите кнопку **Свойства** и установите флажок **Преобразовывать IP-адреса этого интерфейса со всех случаях установки связи** (рис. 15.30).

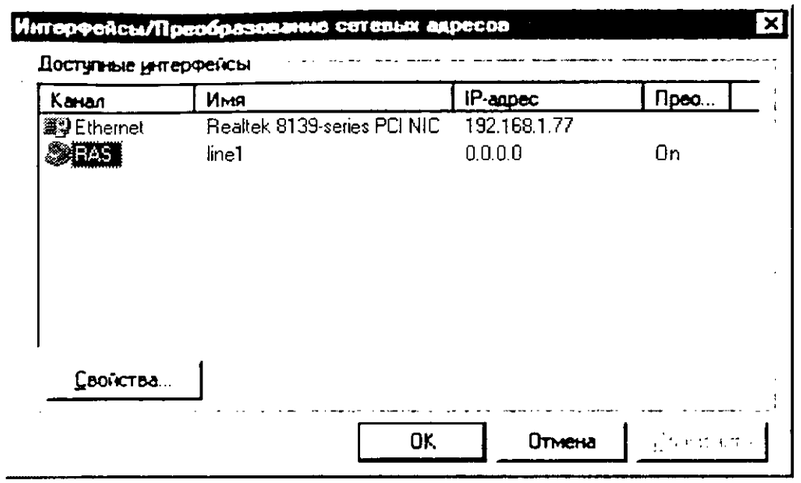


Рис. 15.29. *Интерфейсы/Преобразование сетевых адресов*

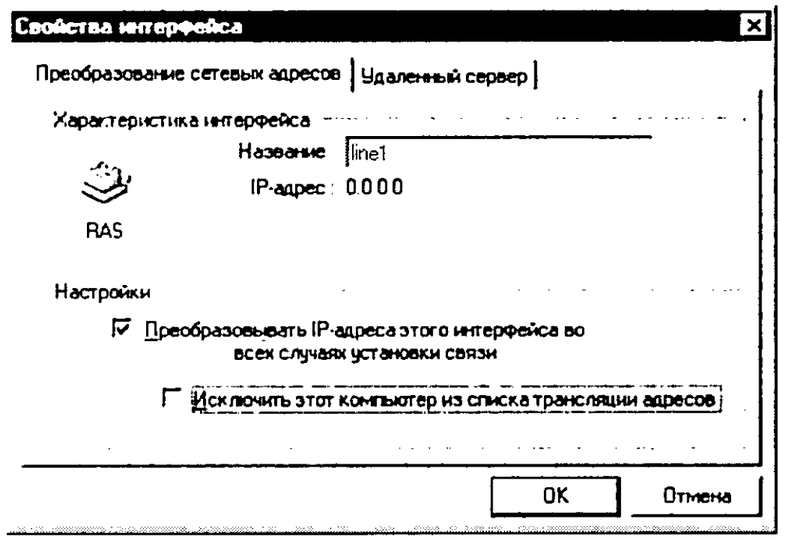


Рис. 15.30. *Свойства интерфейса*

Указать дополнительные параметры NAT можно в окне **Дополнительно по преобразованию сетевых адресов**, показанном на рис. 15.31. Для вызова этого окна выполните команду **Настройки → Дополнительно → Преобразование адресов**.

Привязки портов

Очень тесно с NAT связаны привязки портов. Предположим, что в нашей локальной сети есть Web-сервер (порт 80) с IP-адресом 192.168.1.5, и мы хотим предоставить пользователям Интернета доступ к нему. Для этого нужно создать привязку портов, показанную в табл. 15.2.

Обратите внимание, что, мы открываем доступ не ко всем компьютерам нашей сети, а только к одному — к 192.168.1.5.

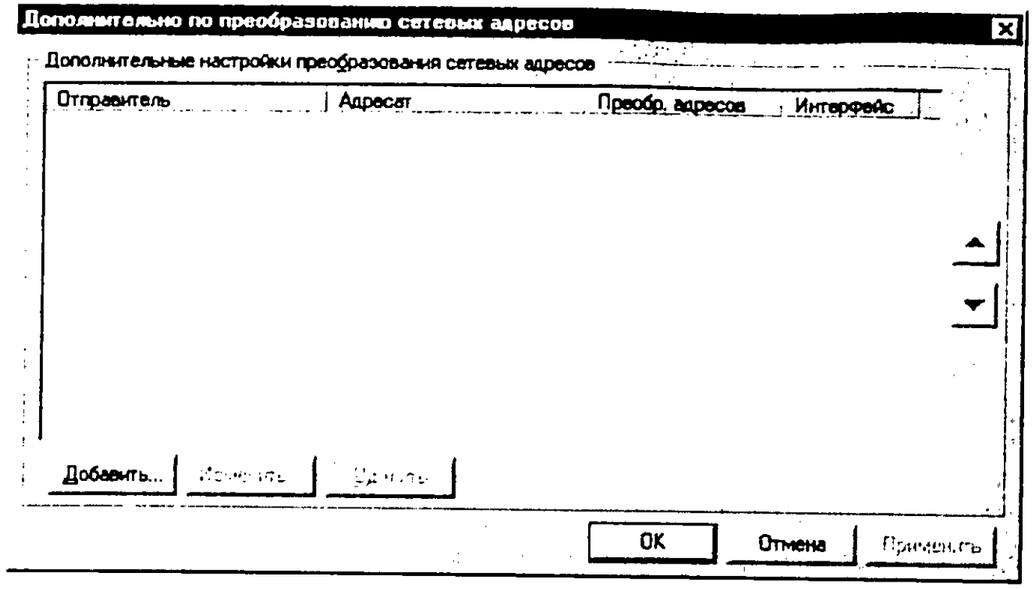


Рис. 15.31. *Дополнительные параметры NAT*

Привязка портов для Web-сервера *Таблица 15.2*

Протокол	TCP
Прослушивать IP-адрес (ожидание сигнала)	не указан
Прослушивать порт	80
IP адресата	192.168.1.5 (адрес Web-сервера)
Порт адресата	80

Для создания привязки портов выполните команду **Настройки → Дополнительно → Распределение адресов**. В появившемся окне нажмите кнопку **Добавить** и введите параметры привязки (рис. 15.32), согласно табл. 15.2.

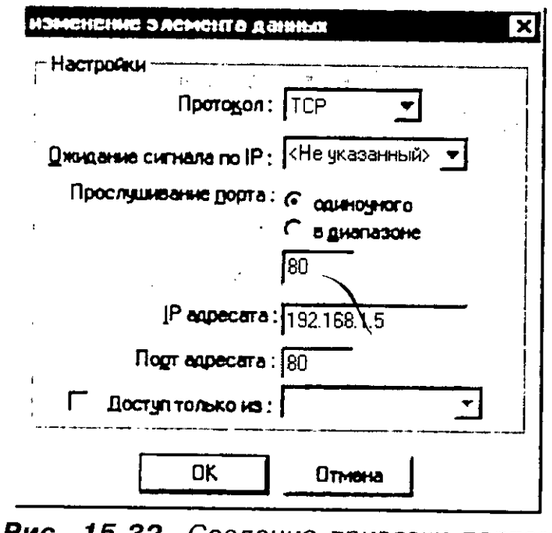


Рис. 15.32. *Создание привязки портов*

Для создания привязки для других серверов параметры привязки остаются теми же, изменяется только IP-адрес сервера и номера портов:

- 25 — для SMTP;
- 110 — для POP3;
- 5000...50011 (диапазон портов) — для ICQ.

О ICQ нужно сказать отдельно. В меню **ICQ Main** выберите пункт **Preferences** и перейдите на вкладке **Connections**. На вкладке **General** выберите **Using Firewall,** а затем **Not using proxy**.

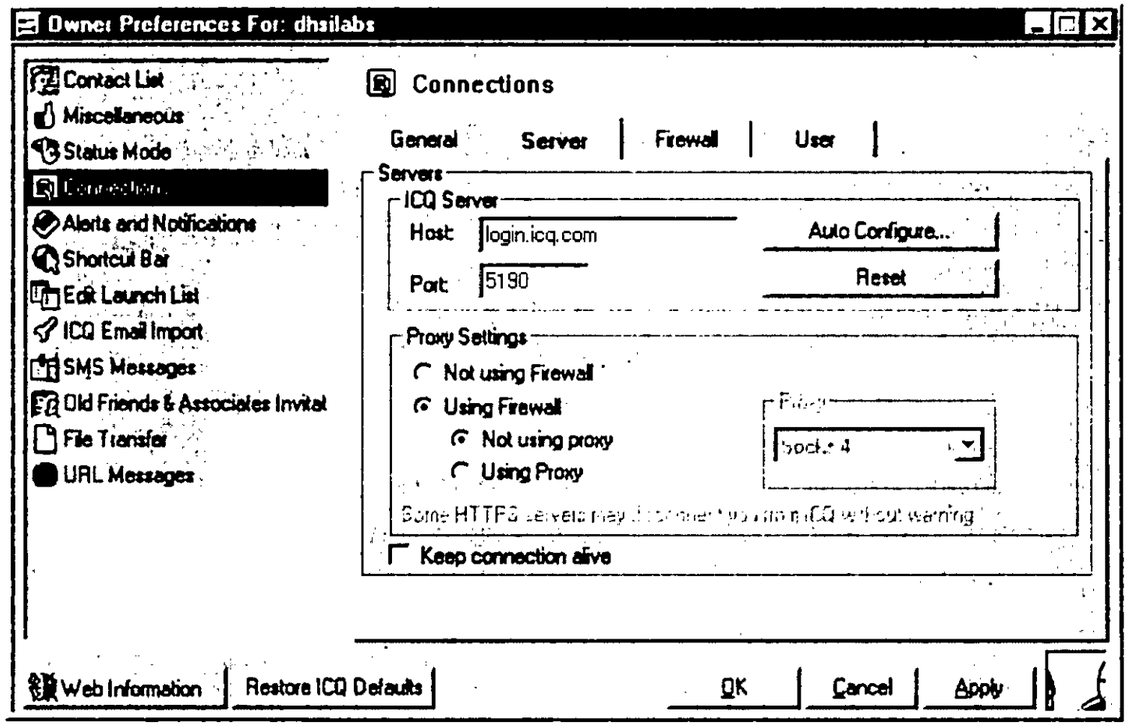


Рис. 15.33. *Общие параметры соединения*

На вкладке **User** (рис. 15.34) выберите **Not using proxy,** а затем **Use the following TCP listen port for incoming event** и введите диапазон портов 5000...5011.

Привязку портов нужно создавать отдельно для каждого компьютера, на котором может быть запущен клиент ICQ. Для каждого клиента нужно настраивать другой диапазон портов, например, 5012...5023, 5024...5033 и т.д. Также нужно отдельно настраивать каждый клиент, указывая его собственный диапазон портов.

WinRoute — прокси-сервер

Настройка прокси-сервера обычно не вызывает какого-либо затруднения. Все, что вам нужно — это включить прокси-сервер в окне **Настройки прокси-сервера** (рис. 15.35). Вызвать это окно можно из меню **Настройки**.

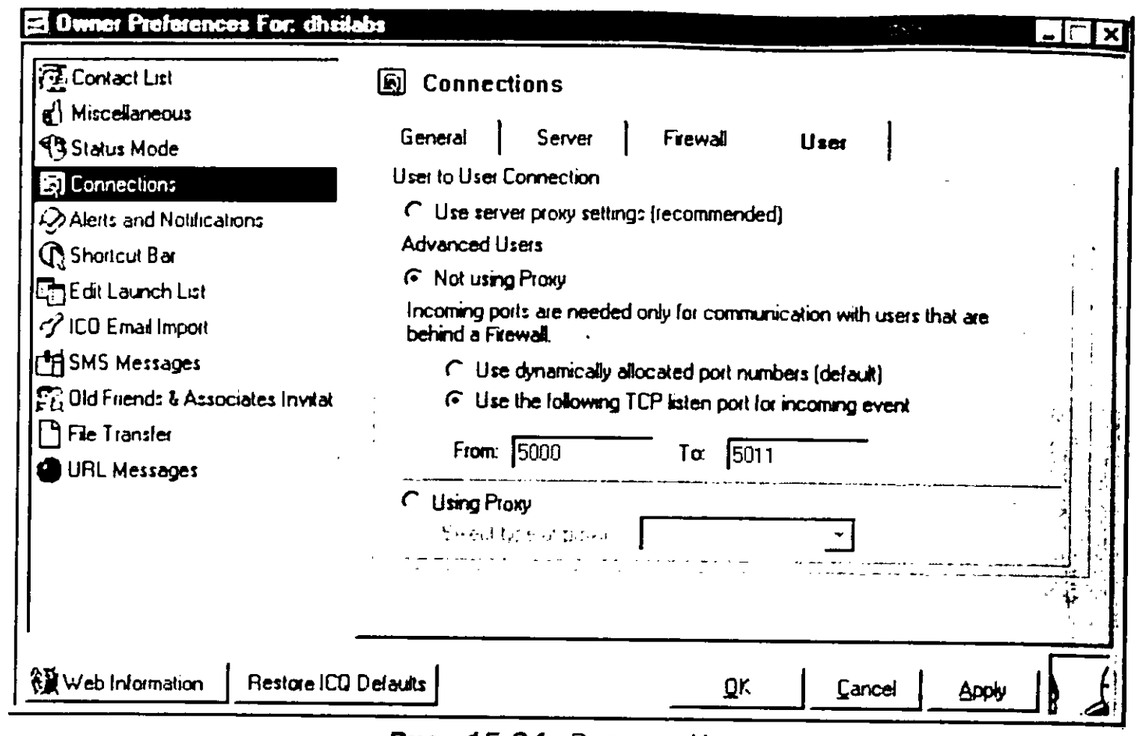


Рис. 15.34. *Вкладка User*

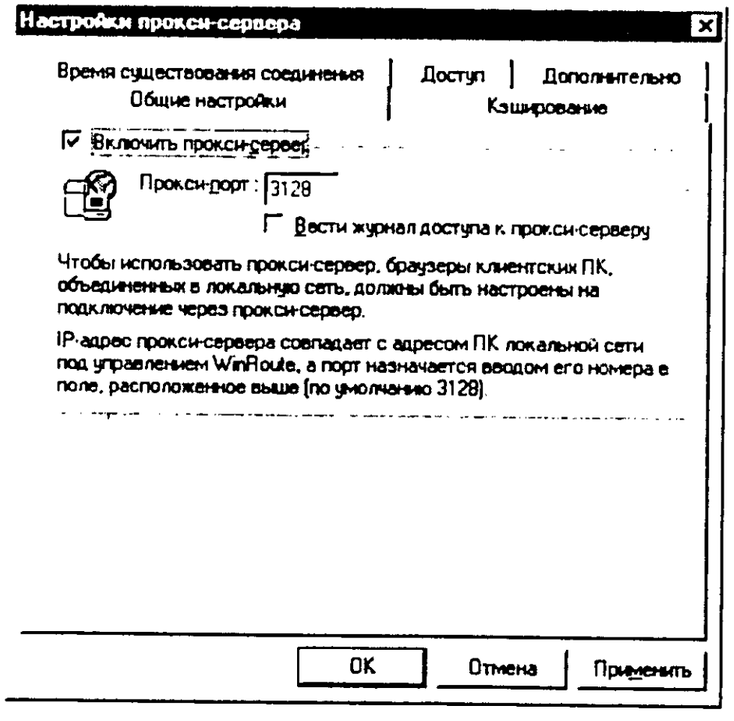


Рис. 15.35. *Включить прокси-сервер*

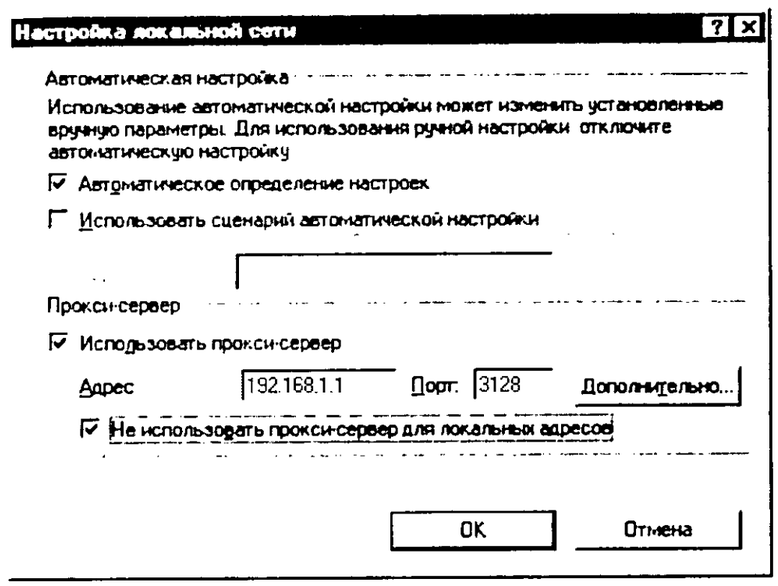


Рис. 15.36. *Параметры браузера*

Затем нужно настроить все браузеры (на всех компьютера вашей локальной сети) на использование прокси-сервера. На рис. 15 вы видите параметры прокси-сервера браузера Internet Explorer 5.0. Порт по умолчанию — 3128.

Практически все остальные параметры, кроме параметров кэширования, должны удовлетворить запросы практически любого администратора. Перейдите на вкладку **Кэширование**. На этой вкладке вам нужно изменить следующие параметры:

- Размер кэша = 20×N, где N — это количество компьютеров в вашей локальной сети.
- Объем кэш-памяти можно увеличить до 1024 Кб или даже до 2048. Все зависит от объема оперативной памяти компьютера-шлюза и от того, используется ли он для других целей, например, в качестве рабочей станции для набора текста. Если шлюз «по совместительству» является еще и печатающей машинкой, то размер кэш-памяти не нужно устанавливать большим — 1024 Кб вполне хватит, если же компьютер выделен только под шлюз, размер памяти можно увеличить до 8096 Кб.
- Если на диске, на котором расположен кэш, нет больше места, перенесите каталог кэширования на другой диск.
- Можно также увеличить размер кэшируемого объекта до 1024 Кб, особенно это актуально для FTP.

На вкладке **Доступ** можно определить доступ к определенным ресурсам только определенным группа пользователей. Разобраться с этой страничкой несложно, поэтому перейдем сразу к настройке почтового сервера.

Примечание.

Стоит только отметить, что при указании имени ресурса вы можете использовать символьные маски * и ? как при указании маски файла. Например, маска *bmw* выделит все ресурсы, в имени которых содержится слово «bmw».

WinRoute — почтовый сервер

Сразу нужно отметить, что в состав программы WinRoute входит *простой* почтовый (SMTP/POP3) сервер, который, впрочем, позволит вам получать почту от других пользователей (включая пользователей сети Интернет) и отправлять почту по протоколу SMTP. Если вас интересует профессиональный почтовый сервер, посетите страничку www.kerio.com. На ней вы найдете Kerio MailServer 5, который обладает антивирусной защитой, фильтром вложений, функцией ограничения доступа, Web-интерфейсом и многими другими полезными функциями.

Намного рациональнее установить Kerio MailServer 5 или же просто использовать почтовый сервер провайдера, не ломая себе голову настройкой WinRoute — в любом случае сервер провайдера будет работать надежнее и будет более функциональным, чем почтовый сервер WinRoute.

WinRoute — DHCP-сервер

А вот с сервером DHCP все намного проще. Его функций вполне хватает, чтобы в вашей сети появился полноценный DHCP-сервер. Для включения DHCP-сервера выберите команду меню **Настройки → Сервер DHCP**, а затем отметьте флажок **Включить сервер DHCP**. Для создания нового диапазона IP-адресов нажмите кнопку **Новый диапазон**.

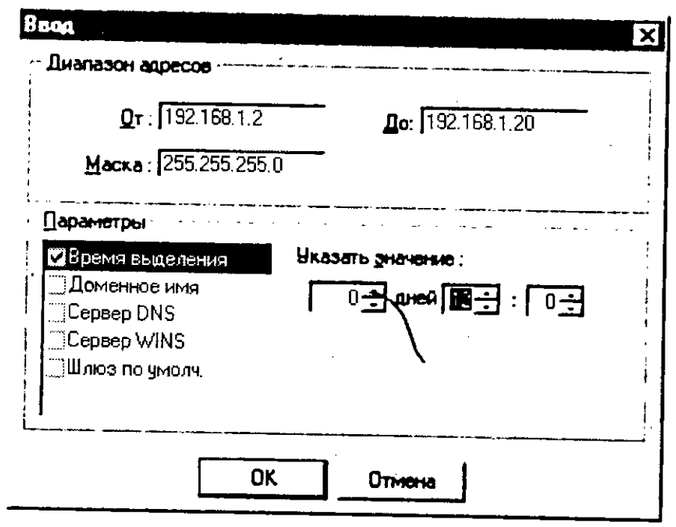


Рис. 15.37. *Параметры диапазона IP-адресов*

В появившемся окне (рис. 15.37) введите новый диапазон, например, 192.168.1.2...192.168.1.20, маску сети — 255.255.255.0. Также можно указать дополнительные параметры, такие как:

- Время выделения;
- Доменное имя;
- Сервер DNS;
- Сервер WINS;
- Шлюз по умолчанию.

Нажав на Ок, вы получите свой DHCP-сервер с указанными параметрами (рис. 15.38).

Настройка клиентов производится как обычно — нужно настроить все клиенты сети на автоматическое получение IP-адреса.

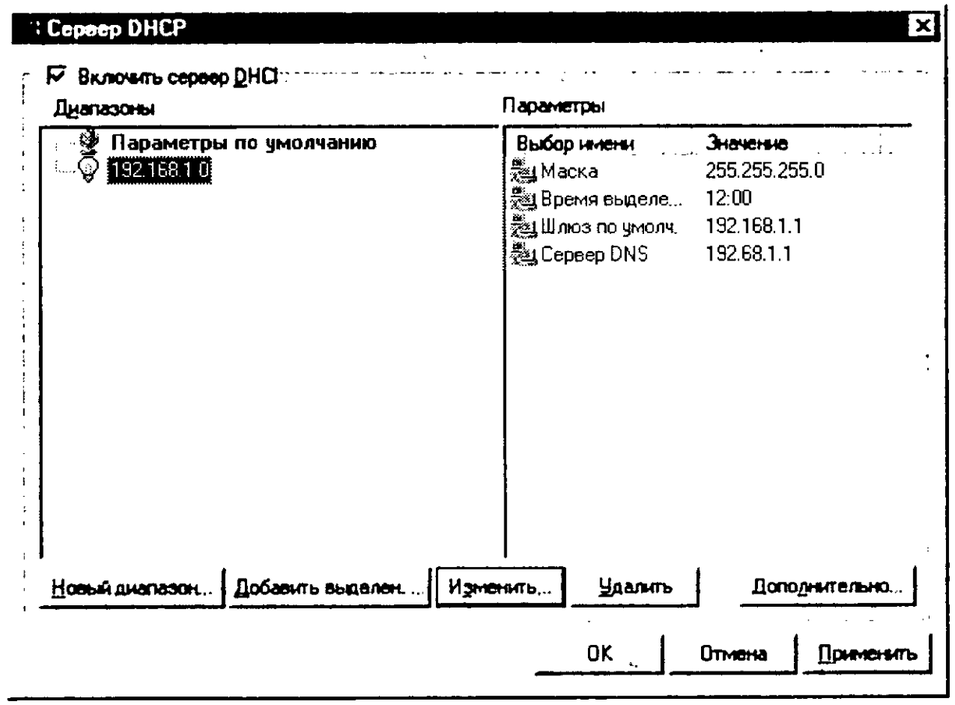


Рис. 15.38. *DHCP-сервер*

WinRoute — ретранслятор DNS

Программа WinRoute выполняет функции ретранслятора сервера DNS, то есть самим сервером она не является, но перенаправляет DNS-запросы клиентов на один из DNS-серверов, известных операционной системе. Вы можете также указать отдельный DNS-сервер, например, сервер провайдера.

WinRoute также может выполнять функции кэширующего DNS-сервера, что позволяет немного ускорить время обращения к Интернет-ресурсам, поскольку ответ приходит от кэширующего сервера DNS (в роли которого выступает WinRoute), а не от сервера провайдера. Все, что вам нужно для ретрансляции DNS — это ее включить. Справедливости ради нужно отметить, что она включена по умолчанию.

Изменить параметры ретрансляции можно в окне **Ретранслятор DNS** (вызвать его можно выбрав **Настройки → Ретранслятор DNS**), показанном на рис. 15.39.

Параметры по умолчанию должны устроить большинство администраторов, поэтому я не думаю, что вам придется их изменять.

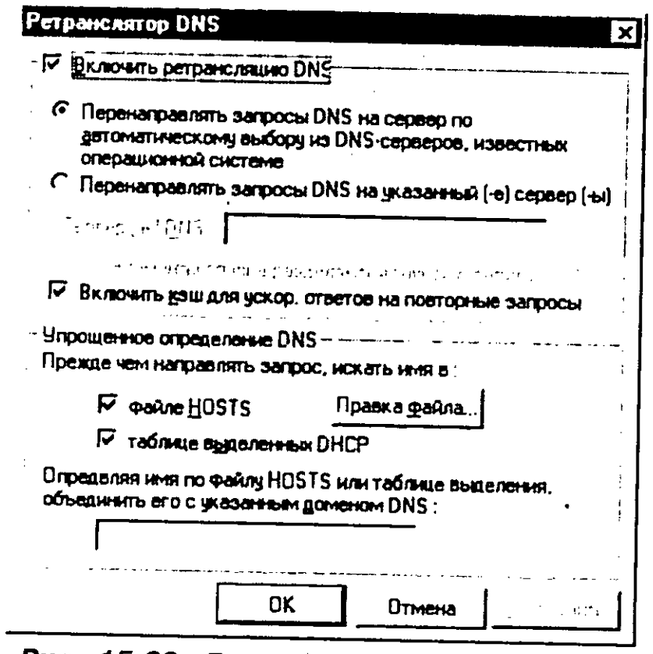


Рис. 15.39. *Параметры ретрансляции DNS*

Фильтрация пакетов

Программа WinRoute также может выполнять функции бастиона (межсетевого экрана). Рассмотрим как действуют политики WinRoute. Откройте окно пакетного фильтра (**Настройки → Дополнительно → Фильтр пакетов**). В этом окне (см. рис. 15.40) вы увидите две вкладки — одна для входящих пакетов, другая — для исходящих.

На каждой страничке вы можете определить интерфейс, для которого хотите определить правила фильтрации. Также можно определить правила для любого интерфейса. Предположим, что у нас есть последовательность правил для интерфейса `line1` (модемное соединение):

- A
- B
- C
- D

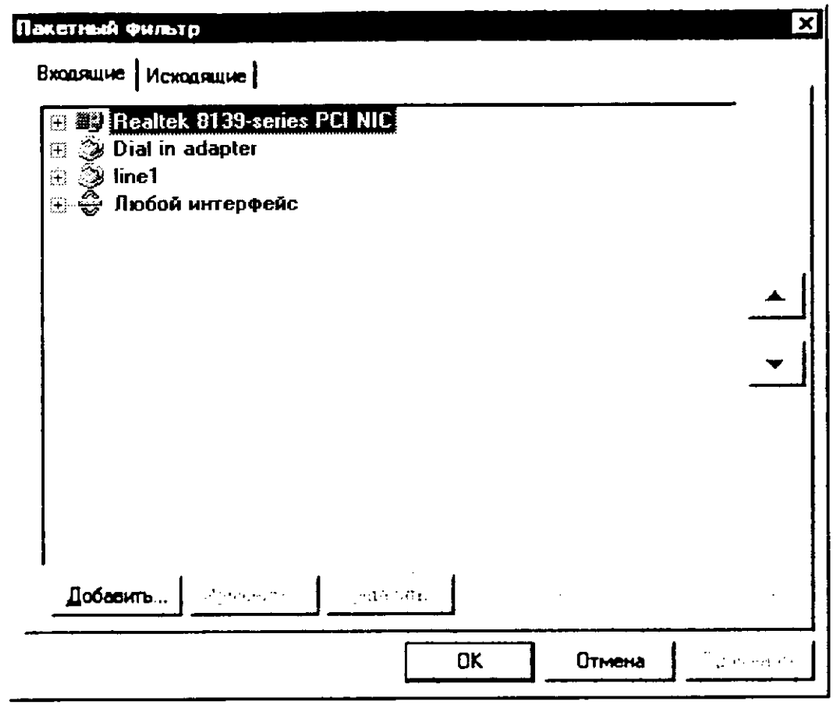


Рис. 15.40. *Пакетный фильтр*

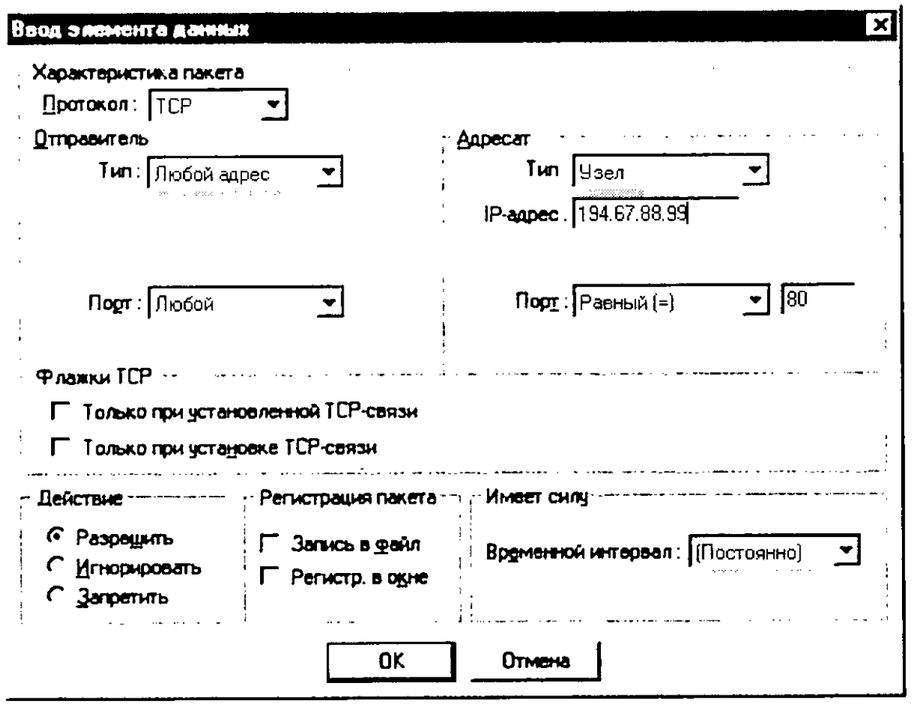


Рис. 15.41. *Создание правила, разрешающего всем доступ к нашему Web-серверу 194.67.88.99:80*

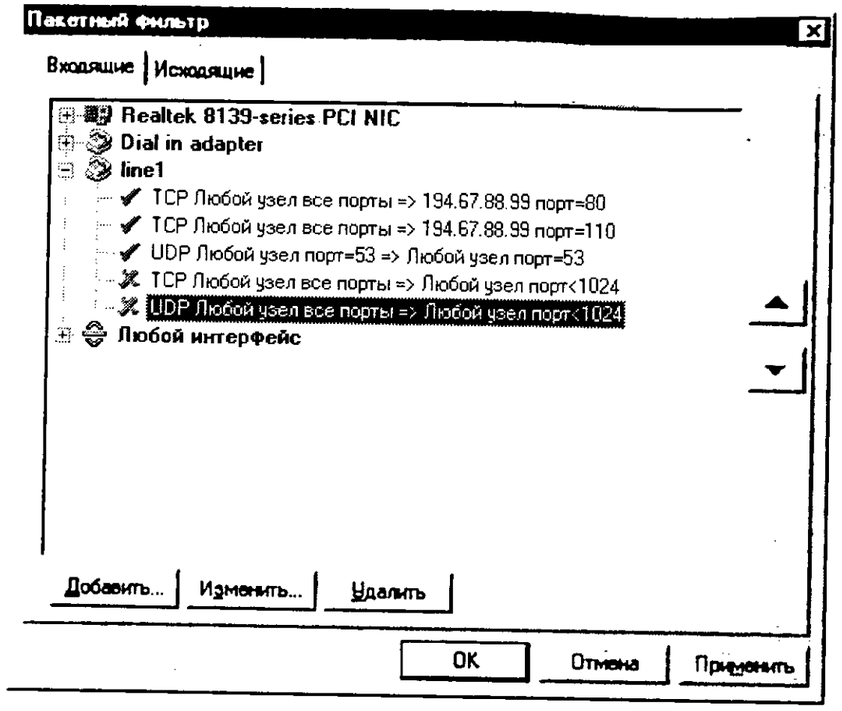


Рис. 15.42. *Политика безопасности*

Поиск правила осуществляется в порядке его добавления. Например, если было найдено совпадение с правилом B, то правила C и D не обрабатываются.

Как же составлять последовательность правил? Сначала в индивидуальном порядке разрешаем передачу входящих/исходящих пакетов для компьютеров, для которых допускается использование извне, например, для Web-сервера, POP3-сервера. Номера портов, как правило, в этом случае будут меньше 1024. Затем разрешаем входящие UDP-пакеты, номера портов которых равняются 53 — это необходимо для службы DNS. Затем запрещаем входящие TCP/UDP-пакеты, номера портов которых меньше 1024.

Глава 16

Подключаем локальную сеть к Интернету через Linux-сервер

16.1. Постановка задачи. Выбор конфигурации

Сначала определим функции, которые должен выполнять шлюз:

1. Поддержка связи с провайдером.
2. Маршрутизация IP-пакетов между локальной сетью и сетью Интернет для выхода пользователей локальной сети в Интернет.
3. Обеспечение IP-сервиса.
4. Защита локальной сети от несанкционированного доступа из Интернет.

Конфигурирование шлюза в операционной системе Linux состоит из следующих этапов:

1. Настройка ядра.
2. Настройка сети.
3. Конфигурирование IpChains.
4. Настройка DNS.
5. Настройка Squid.

Для определенности будет использоваться два сетевых интерфейса — `eth0`, идущий к провайдеру, и `eth1` — во внутренней сети. Пусть интерфейсу `eth0` назначен IP-адрес 111.111.111.111, а `eth1` — 192.168.1.1.

16.2. Пошаговое описание настройки шлюза

16.2.1. Настройка ядра

Скорее всего, вам придется перекомпилировать ядро. При этом должны быть активизированы следующие опции:

```
Networking support (CONFIG_NET) [y]
TCP/IP networking (CONFIG_INET) [y]
IP forwarding/gatewaying (CONFIG_IP_FORWARD) [y]
IP multicasting (CONFIG_IP_MULTICAST) [y]
IP firewalling (CONFIG_IP_FIREWALL) [y]
IP accounting (CONFIG_IP_ACCT) [y]
```

Можно также поэкспериментировать с набором опций **Advanced Router**, если данные функции есть в вашем ядре. Более подробно о процессе компилирования ядра вы можете прочитать в следующей главе.

16.2.2. Настройка сети

После перекомпилирования ядра нужно включить **IP-forwarding**. Сделайте это при помощи следующей команды:

```
# echo "1" > /proc/net/ip_forward
```

Настройку сетевых карт произведите с помощью программы **netconf**. О том, как это сделать, было рассказано в начале книги, в соответсвующей главе.

16.2.3. Конфигурирование IPTables (или IpChains)

Теперь приступим к настройке **IPChains/IPTables**. В зависимости от вашего дистрибутива, вы будете использовать один из этих бастионов. Параллельно я буду писать команды IPChains и IPTables Создайте цепочку, через которую пойдет весь трафик от провайдера:

```
ipchains -N prov
ipchains -A input -i eth0 -j prov  iptables -N prov
iptables -A INPUT -i eth0 -j prov
```


Запретите **ip-spoofing**:

```
ipchains -A prov -s 192.168.1.1/16 -l -j DENY
ipchains -A prov -s 127.0.0.1/8 -l -j DENY iptables -A
prov -s 192.168.1.1/16  -j DROP
iptables -A prov -s 127.0.0.1/8  -1  -j DROP
```

Запретите Telnet снаружи:

```
ipchains -A prov -p tcp --destination-port 23 -j REJECT
```

Эта же команда «в переводе на IPtables» будет выглядеть так:

```
iptables -A prov -p tcp --destination-port 23 -j REJECT
```

Если вы не хотите, чтобы **samba** «светилась» наружу, запретите порты 137...139:

```
ipchains -A prov -p tcp --destination-port 137 -j REJECT
ipchains -A prov -p udp --destination-port 137 -j REJECT
```

То же самое проделайте для портов 138 и 129. На IPTables данные команды будут выглядеть так:

```
iptables -A prov -p tcp --destination-port 137 -j REJECT
iptables -A prov -p udp --destination-port 137 -j REJECT
```

О настройке **samba** вы можете прочитать в Samba-HOWTO.

Создайте цепочку для подсчета трафика:

```
ipchains -N trafin
ipchains -I input -i eth0 -s ! 123.123.123.0/24 -p all -j trafin
ipchains -A trafin -d 123.123.123.123
```

Соответственно, на iptables команды будут выглядеть следующим образом:

```
iptables -N trafin
iptables -I input -i eth0 -s ! 123.123.123.0/24 -p all -j trafin
iptables -A trafin -d 123.123.123.123
```

Для того чтобы ваши правила были постоянными (при перезагрузке машины правила IpChains теряются), используйте скрипты **ipchains-save** и **ipchains-restore**. Настройте свои правила, а затем выполните команду:

```
# ipchains-save > /etc/ipchains.rules
# iptables-save > /etc/iptables.rules
```

Далее создайте скрипт, подобный тому, что приведен в листинге 16.1.

Листинг 16.1. Скрипт управления пакетной фильтрацией на ipchains

```
#! /bin/sh
# Скрипт управления пакетной фильтрацией.
# Если правил нет, то ничего не делать.

#! /bin/sh
# Скрипт управления пакетной фильтрацией.

# Если правил нет, то ничего не делать.
[ -f /etc/ipchains.rules ] || exit 0
case "$1" in

start)
     echo -n "Включение пакетной фильтрации:"
     /sbin/ipchains-restore < /etc/ipchains.rules || exit
1
     echo 1 > /proc/sys/net/ipv4/ip_forward
     echo "." ;;

stop)
     echo -n "Отключение пакетной фильтрации:"
     echo 0 > /proc/sys/net/ipv4/ip_forward
     /sbin/ipchains -X
     /sbin/ipchains -F
     /sbin/ipchains -P input ACCEPT
     /sbin/ipchains -P output ACCEPT
     /sbin/ipchains -P forward ACCEPT

     echo "." ;;

*)
     echo "Использование: /etc/init.d/packetfilter {start|stop}"
     exit 1 ;;

esac

exit 0
```


Этот скрипт добавьте в сценарии загрузки системы. Если вы используете IPTables данный скрипт будет выглядеть так, как показано в листинге 16.2.

Листинг 16.2. Скрипт управления пакетной фильтрацией на IPTables

```
#! /bin/sh
# Скрипт управления пакетной фильтрацией.

# Если правил нет, то ничего не делать.

#! /bin/sh
# Скрипт управления пакетной фильтрацией.

# Если правил нет, то ничего не делать.
[ -f /etc/iptables.rules ] || exit 0
case "$1" in

start)
     echo -n "Включение пакетной фильтрации:"
     /sbin/iptables-restore < /etc/iptables.rules || exit
1
     echo 1 > /proc/sys/net/ipv4/ip_forward
     echo "." ;;
stop)
     echo -n "Отключение пакетной фильтрации:"
     echo 0 > /proc/sys/net/ipv4/ip_forward
     /sbin/iptables -X
     /sbin/iptables -F
     /sbin/iptables -P INPUT ACCEPT
     /sbin/iptables -P OUTPUT ACCEPT
     /sbin/iptables -P FORWARD ACCEPT

     echo "." ;;

*)
     echo "Использование: /etc/init.d/packetfilter {start|stop}"
     exit 1 ;;
esac

exit 0
```

16.2.4. Настройка DNS

Напомню, что основной задачей сервера доменных имен (Domain Name System) является преобразование мнемонических имен машин в IP-адреса и обратно. Обычно сервер DNS устанавливается на шлюзе, который используется для выхода в Интернет.

Прежде чем приступить к настройке сервера, нужно определить, запущен ли он:

```
# ps -ax | grep named
```

Если он запущен, его нужно остановить (с помощью **ndc**), а если он вообще не установлен, то придется установить пакет **bind**. Для работы сервера должен быть активизирован сервис **network**.

Теперь приступим к непосредственной настройке сервера. Основная информация о параметрах сервера содержится в файле `/etc/named.conf` (см. листинг 16.3).

Листинг 16.3. Файл named.conf

```
logging {
    category cname {null; };
    };

options {
    directory "/var/named";
    };

zone "." {
    type hint;
    file "named.ca";
    };

zone "dhsilabs.com" {
    type master;
    file "dhsilabs.com";
    notify no;
    };

zone "0.0.127.in-addr.arpa" {
    type master;
    file "named.local";
    };

zone "1.168.192.in-addr.arpa" {
    type master;
    file "192.168.1";
    notify yes;
    };
```

Основной каталог сервера — `/var/named`. В нем сервер будет искать файлы `dhsilabs.com`, `named.local`, `192.168.1`, `named.ca` (см. листинги 16.4, 16.5, 16.6). Обслуживаемая нашим сервером зона (домен) — `dhsilabs.com` (см. листинг 16.4). Файл `named.ca` — корневой кэш — содержит информацию о корневых серверах DNS. Позже займемся его обновлением.

Листинг 16.4. Файл dhsilabs.com (для преобразования имен в IP-адреса)

```
@     IN  SOA den.dhsilabs.com. hostmaster.dhsilabs.com. (
          93011120    ; серийный номер
          10800       ; обновление каждые 3 часа
          3600        ; повтор каждый час
          3600000 ; хранить информацию 1000 часов
          86400  )       ; TTL записи — 24 часа
      IN  NS  den.dhsilabs.com.
      IN  A   192.168.1.1
      IN  MX 150 den.dhsilabs.com.

den   IN  A   192.168.1.1
      IN  HINFO   INTEL CELERON (LINUX)
      IN  MX 100 den
      IN  MX 150 evg.dhsilabs.com.
ns    IN  CNAME  den.dhsilabs.com.
www   IN  CNAME  den.dhsilabs.com.
ftp   IN  CNAME  den.dhsilabs.com.
mail  IN  CNAME  den.dhsilabs.com.

evg   IN  A   192.168.1.2
      IN  MX 100 den.dhsilabs.com.

localhost IN A   127.0.0.1
```

Здесь :

- NS — обозначает name server;
- A — IP-адрес;
- MX — почтовик <приоритет>. Чем ниже значение, тем выше приоритет;
- HINFO — сведения об аппаратном обеспечении (заполнять не рекомендую);
- TXT — прочие сведения;
- CNAME — каноническое имя, т.е. если вы в окне браузера введете http://www.dhsilabs.com, то обращение будет произведено к den.dhsilabs.com.

Обратите внимание на точку в конце:

```
@     IN  SOA den.dhsilabs.com. hostmaster.dhsilabs.com.
```

(Если точка не указана, то к имени будет добавлено имя домена (т.е. dhsilabs.com).

Листинг 16.5. Файл named.local

```
@     IN  SOA dhsilabs.com. root.dhsilabs.com. (
          199609203   ; серийный номер
          28800       ; обновление каждые 8 часов
          7200        ; повтор каждые 2 часа
          604800      ; хранить информацию 168 часов (7 дней)
          86400)      ; TTL записи — 24 часа
          NS  dhsilabs.com.
1         PTR localhost.
```

Листинг 16.6. Файл 192.168.1 или файл обратного соответствия

```
@     IN  SOA den.dhsilabs.com. hostmaster.dhsilabs.com. (
          93011120    ; серийный номер
          10800       ; обновление каждые 3 часа
          3600        ; повтор каждый час
          3600000     ; хранить информацию 1000 часов
          86400 )     ; TTL записи — 24 часа
@     IN  NS  den.dhsilabs.com
1     IN  PTR den.dhsilabs.com
2.1.168.192 IN  PTR evg.dhsilabs.com
```


Запись **PTR** используется для преобразования IP-адреса в имя. Если указан не весь IP:

```
1     IN  PTR den.dhsilabs.com
```

то к нему будет добавлен адрес подсети 1.168.192. Обратите внимание: IP-адреса указываются в обратном порядке!

16.2.5. Настройка прокси Squid

Установите пакет **squid**. Осталось настроить и запустить его. Для этого нужно отредактировать файл конфигурации `/etc/squid/squid.conf`. Сначала укажите адрес прокси провайдера:

```
cach_peer proxy.your_isp.com
```

Задайте объем ОЗУ, который будет использовать прокси-сервером:

```
cache_mem
```

В том случае, если вы планируете использовать этот компьютер еще и для других целей, кроме как в качестве прокси-сервера, то не рекомендуется устанавливать здесь более трети физического объема ОЗУ.

Далее укажите, где будет располагаться кэш (первое число — это количество Мб для кэша):

```
cache_dir /usr/local/squid 2048 16 256
```

Затем укажите хосты, из которых разрешен доступ к прокси-серверу:

```
acl allowed_hosts src 192.168.1.0/255.255.255.0
acl localhost src 127.0.0.1/255.255.255.255
```

После этого пропишите пользователей, которым разрешено пользоваться **squid** (в приведенном примере это `den`, `admin`, `developer`):

```
ident_lookup on
acl allowed_users user den admin developer
http_access allow allowed_users
http_access deny all
```

Тэги **maxium_object_size** и **maxium_object** устанавливают ограничения на размер передаваемых объектов.

В заключение хочу дать один хороший совет: из соображений безопасности отредактируйте свои `/etc/services` и `/etc/inetd.conf` и отключите неиспользуемые сервисы — это уменьшит вероятность взлома вашей системы. Вот, в общем-то, и все.

Часть VI

НАСТРОЙКА ДОСТУПА К ЛОКАЛЬНОЙ СЕТИ ИЗВНЕ

Глава 17

Настраиваем сервер удаленного доступа из Windows 98

Сначала у нас была небольшая одноранговая сеть, потом, по мере расширения сети, в ней появляются сервера: DNS, DHCP, контроллеры домена. По мере развития сети возникает необходимость разделения одной большой сети на подсети, связь между которыми устанавливается благодаря механизму и протоколам маршрутизации. Следующий этап развития нашей сети — это подключение ее к глобальной сети Internet.

Рано или поздно у вас возникнет необходимость удаленного подключения к вашей сети. Например, вы хотите поработать дома над каким-нибудь документом, но, придя домой, вы обнаруживаете, что забыли его скопировать. Не ехать же опять на работу? Намного проще установить удаленное соединение с сетью предприятия и скопировать на свой компьютер необходимый документ.

17.1. Простой сервер удаленного доступа на базе Windows 98

17.1.1. Настройка сервера

Сервер удаленного доступа на базе Windows 98 больше подходит для персонального использования, чем для реального подключения к сети предприятия. Такой сервер можно настроить дома: например, если вам понадобился какой-нибудь файл, который вы забыли дома, вы можете подключиться к домашнему серверу удаленного доступа и скопировать его.

Телефон есть практически везде, как и компьютер с модемом, а еще лучше, если у вас будет с собой ноутбук. Если же использовать Интернет для подключения к домашней сети, это будет стоить в два раза дороже, поскольку вам нужно будет платить и за телефон и за Интернет, причем за Интернет вам придется платить вдвойне: за домашний компьютер и за ноутбук. Поэтому удаленный доступ к домашней сети на базе Windows 98 — это идеальное решение.

Вряд ли к вашей домашней сети будут подключаться сразу несколько пользователей, поэтому конфликтов из-за занятости линии не должно быть. Можно, конечно, провести многоканальную телефонную линию, но не многим пользователям это доступно. К тому же нужно учитывать стоимость мультипортовой платы и модемов. Это уже уровень предприятия. А предприятие должно использовать что-то надежнее, чем Windows 98. Например, Windows 2000 Server или Linux.

Наверное, я слишком много теоретизирую, лучше перейдем к практике. Итак, у нас есть один домашний компьютер под управлением Windows 98 и модем. На компьютере наличие сетевой платы необязательно.

Сначала мы будем настраивать сервер (компьютер, к которому подключаемся), а потом — клиент (компьютер, который подключается). Перейдите на Панель управления и откройте апплет **Установка и удаление программ**. Затем перейдите на вкладку **Установка Windows**, выделите группу **Связь** и нажмите кнопку **Свойства**. Выделите четыре компонента группы **Связь**:

- **Удаленный доступ к сети** — данный компонент нужен для сервера удаленного доступа, обязательно установите его, если он еще не установлен.
- **Сервер удаленного доступа** — собственно, сам сервер удаленного доступа.
- **Телефон** — программка для набора номера, устанавливать необязательно.
- **Hyper Terminal** — установите эту программу, если она еще не установлена — она понадобится для отладки модема.

Перед установкой не забудьте в CD-ROM вставить компакт-диск с дистрибутивом.

После установки сервера удаленного доступа необходимо перезагрузить систему. После перезагрузки откройте апплет **Сеть** с Панели управления. У вас должны быть установлены следующие компоненты:

- Контроллер удаленного доступа;
- Протокол TCP/IP;
- Протокол NetBEUI;
- Клиент для сетей Microsoft;
- Служба доступа к файлам и принтерам.

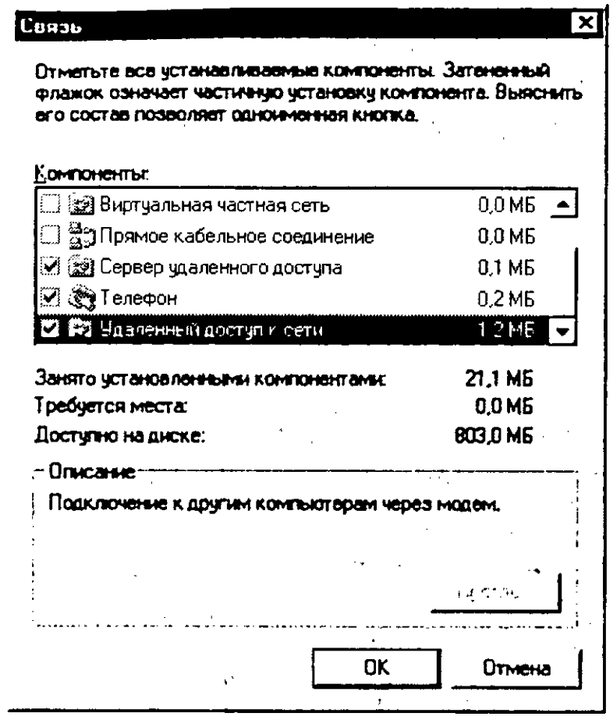


Рис. 27.1. *Установка необходимого программного обеспечения*

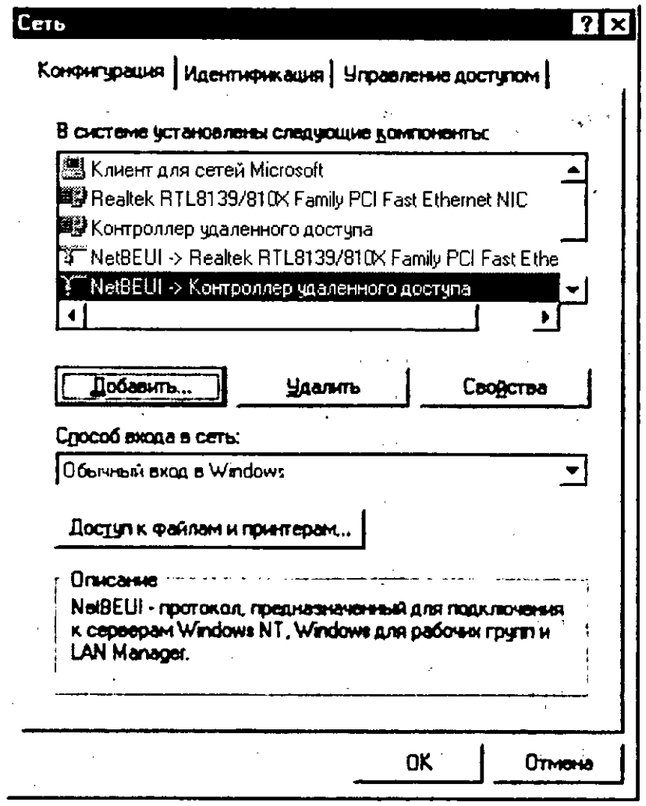


Рис. 27.2. *Необходимые сетевые компоненты*

Возможны два варианта настройки:

- если сервер подключен к локальной сети и его сетевой плате назначен статический IP-адрес;
- если сервер не подключен к локальной сети и у него вообще нет сетевой платы.

Предположим, что в первом случае компьютер подключен к сети 192.168.1.0. Тогда для контроллера удаленного доступа следует установить адрес 192.168.2.1 (в свойствах протокола TCP/IP) и маску подсети 255.255.255.0.

Если же сервер не подключен к локальной сети и не имеет сетевой платы, то можно воспользоваться автоматическим присвоением IP-адресов или же назначить IP-адрес самостоятельно, например, 192.168.1.1 (маска 255.255.255.0). Если воспользоваться автоматическим присвоением IP-адресов (выбрать **Получить IP-адрес автоматически**), то при установлении соединения серверу будет назначен IP-адрес 192.168.55.1, а клиенту — 192.168.55.2. Это стандартные IP-адреса, используемые сервером удаленного доступа Microsoft.

Возможен и третий вариант — сервер оснащен сетевой платой, но не подключен к сети — просто в нем установлена сетевая плата. В этом случае нужно или отключить ее и настраивать как было выше сказано, или же присвоить ей какой-нибудь IP-адрес и настраивать так, как будто мы подключены к сети.

Разобравшись с IP-адресами, выделите **Клиент для сети Microsoft** и нажмите кнопку **Свойства**. В свойствах клиента для сети Microsoft установите **Быстрый вход**. В этом случае при входе в сеть не будут восстанавливаться сетевые подключения. Для удаленного доступа — это оптимальный вариант, поскольку, учитывая качество наших линий, связь может оборваться быстрее, чем восстановиться сетевое подключение.

Затем нужно разрешить общий доступ к файлам и принтерам, если это еще не сделано. Вот теперь можно нажимать кнопку Ок. Если у вас были установлены не все компоненты, то после нажатия кнопки Ок потребуется еще одна перезагрузка.

После перезагрузки откройте папку **Удаленный доступ к сети** (она находится в папке **Мой компьютер**). Затем выполните команду меню **Соединения → Сервер удаленного доступа**.

В окне сервера удаленного доступа (рис. 17.3) вы можете разрешить или запретить удаленные соединения, задать пароль, а также установить другие параметры сервера, например, его тип, параметры безопасности.

Если у вас внутренний модем, то есть нет возможности включить и выключить само устройство, то разрешать принимать входящие соединения нужно, когда вы уходите из дому, иначе модем начнет принимать каждый

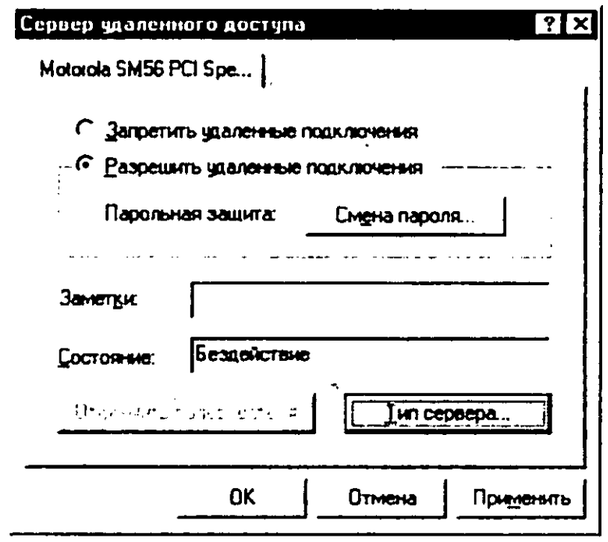


Рис. 27.3. *Сервер удаленного доступа*

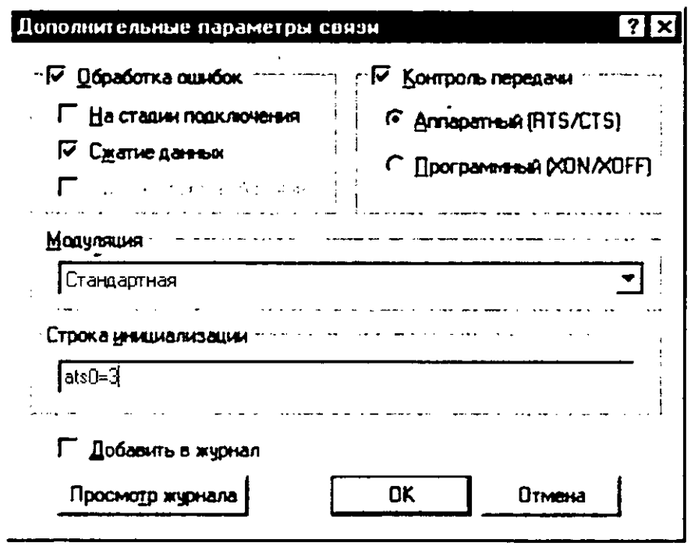


Рис. 27.4. *Строка инициализации модема*

звонок. Кстати, не забудьте указать команду ATS0=3 в строке инициализации вашего модема (**Панель управления → Модемы**, далее **Модем → Свойства → Подключение → Дополнительно**). Данная АТ-команда означает, что модем будет поднимать трубку после третьего вызова (рис. 17.4).

Вот практически и все. Вам осталось настроить только общий доступ к файлам и принтерам, чтобы, подключившись к компьютеру, вы смогли скопировать нужный вам файл.

17.1.2. Настройка клиента

На компьютере-клиенте должны быть установлены следующие сетевые компоненты:

- Контроллер удаленного доступа (служба удаленного доступа);
- Протокол TCP/IP;
- Протокол NetBEUI;
- Клиент для сетей Microsoft;
- Служба доступа к файлам и принтерам.

Убедившись, что с конфигурацией сети все нормально (все компоненты установлены), можно создавать новое соединение. Задайте номер телефона, пароль (если нужно). Откройте свойства соединения и на вкладке **Тип сервера** включите флажки **Войти в сеть**, **NetBEUI** и **TCP/IP**, а все остальное можно отключить.

Если вы подключаетесь к серверу, который, в свою очередь, подключен к сети, нужно установить определенные значения IP-адреса и маски сети, например, 192.168.1.2 (маска 255.255.255.0). Если же подключаетесь к серверу, который не подключен к сети, выберите **Получить IP-адрес автоматически**. Все, теперь можно набирать номер!

Глава 18

Настройка удаленного доступа в Windows 2003 Server

18.1. Установка службы удаленного доступа

Входящие и исходящие соединения в Windows 2000 (2003, NT) устанавливаются с помощью службы удаленного доступа — Remote Access Service (RAS). Для установки службы удаленного доступа выполните команду главного меню **Start → Settings → Control Panel → Administrative Tools → Configure Your Server**. В окне **Configure Your Server (Настройка вашего сервера)**, показанном на рис. 18.1, выберите **Remote Access/VPN Server** и нажмите кнопку **Next**. Если в столбце **Configured** напротив строки **Remote Access/VPN Server** стоит **Yes**, значит, RAS уже установлена. Дальнейшая настройка осуществляется с помощью утилиты **Routing and Remote Access**.

Обращаю ваше внимание! Есть один важный момент: ПЕРЕД НАСТРОЙКОЙ СЕРВЕРА УДАЛЕННОГО ДОСТУПА НУЖНО НАСТРОИТЬ ACTIVE DIRECTORY.

В появившемся окне нажмите дважды кнопку **Next** и подождите, пока откроется окно мастера установки сервера удаленного доступа и маршрутизации (рис. 18.2).

Нажмите кнопку **Next**, а затем выберите **Remote access (dial-up or VPN)** для настройки удаленного доступа (см. рис. 18.3). В следующем окне выбираем Dial-up, настраивать VPN нам не нужно (рис. 18.4).

Далее нажимаем кнопку **Next** и указываем параметры DHCP (рис. 18.5). Первая опция (**Automatically**) означает автоматическую настройку DHCP, а вторая позволяет настроить DHCP вручную (**From a specified range of address**).

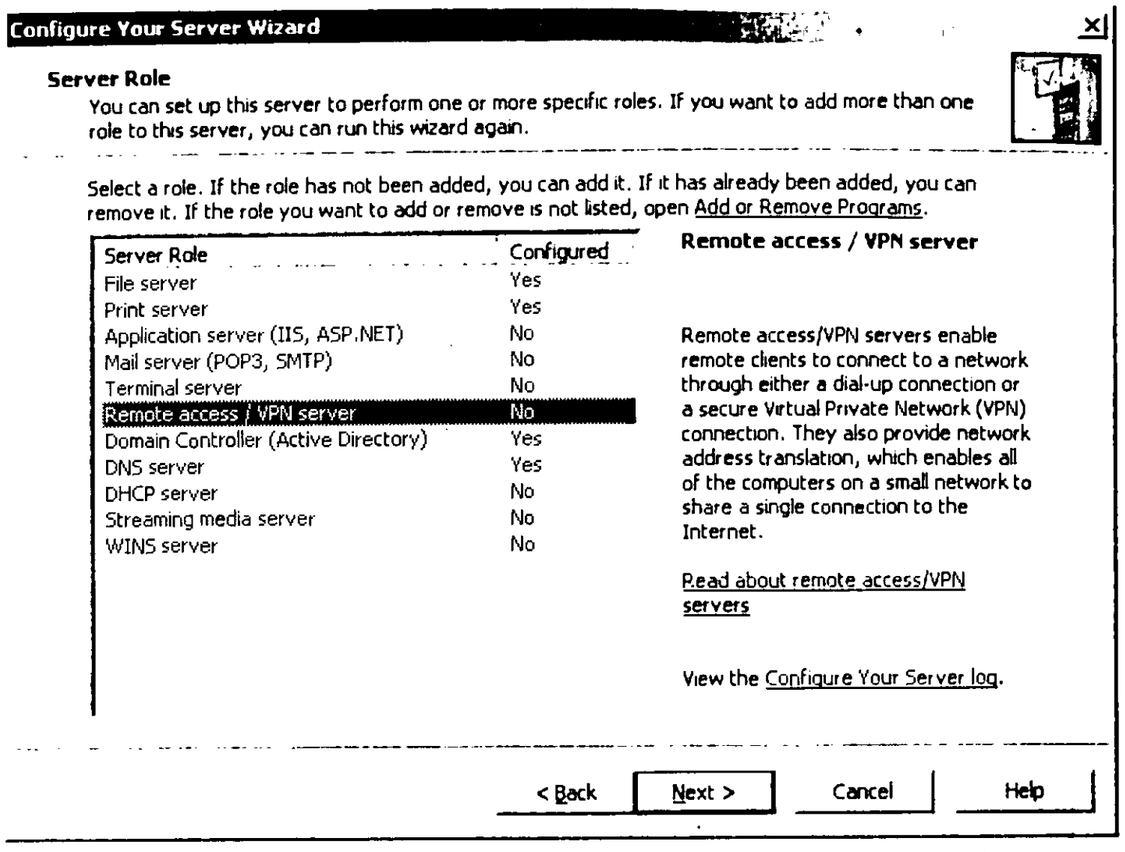


Рис. 18.1. *Configure Your Server (Настройка вашего сервера)*

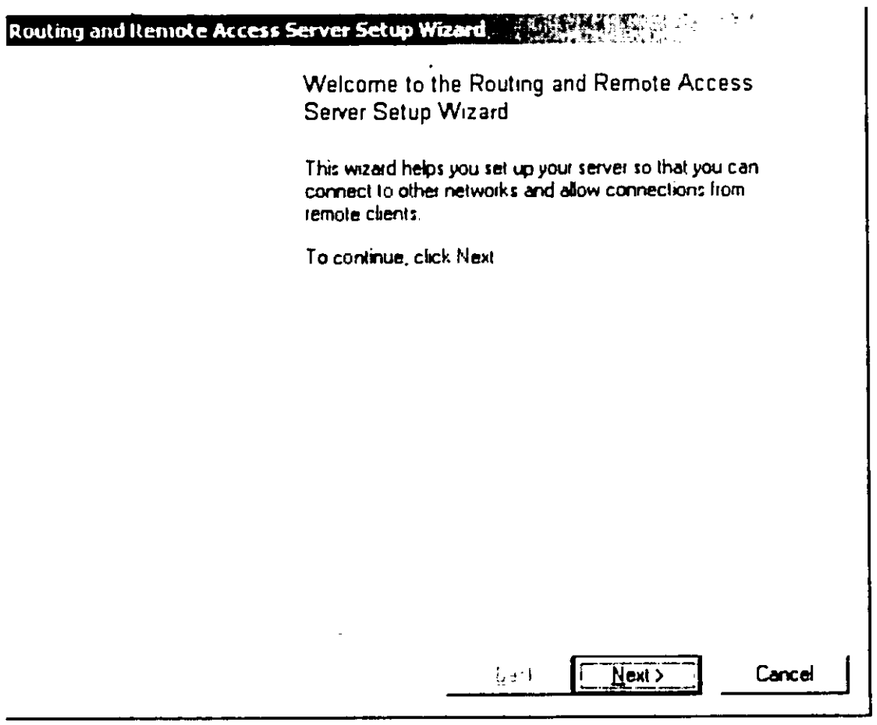


Рис. 18.2. *Мастера установки сервера удаленного доступа и маршрутизации*

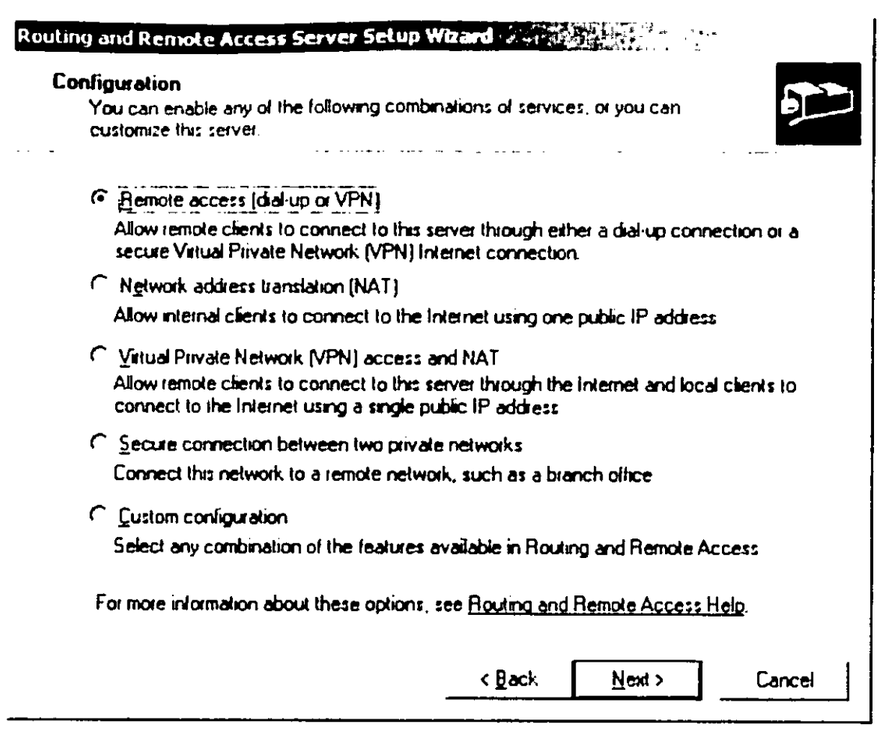


Рис. 18.3. *Выбираем Remote access*

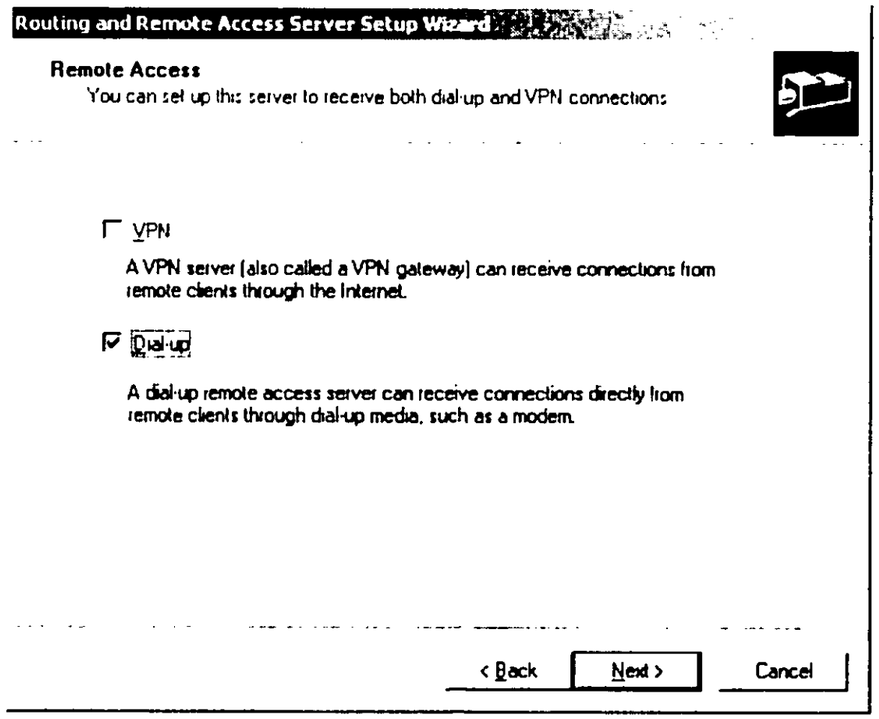


Рис. 18.4. *Какой удаленный доступ будем настраивать: VPN или dial-up?*

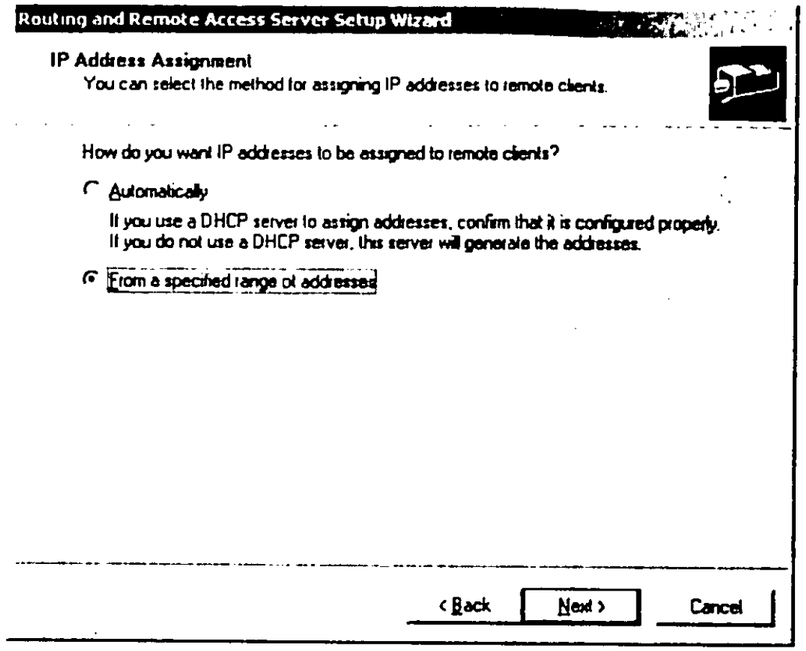


Рис. 18.5. *Параметры DHCP*

Для нас более предпочтительный второй вариант, поскольку позволяет указать нужный нам диапазон IP-адресов. Ясное дело, нужно указывать IP-адреса из нашей сети. Например, если у нас сеть 192.168.1.0, то нужно указать IP-адреса из диапазона 192.168.1.2...192.168.1.254 (мы считаем, что IP-адрес 192.168.1.1 зарезервирован для сервера). На рис. 18.6 указан диапазон из 11 адресов 192.168.1.11...192.168.1.21. Для ввода диапазона адресов нажмите кнопку **New**. После этого введенный диапазон появится в окне (рис. 18.7).

В следующем окне (см. рис. 18.8) нужно выбрать параметры аутентификации — как будет она производиться — средствами RAS (службой Routing and Remote Access) или средствами сервера RADIUS. Настройка RADIUS в этой книге рассматриваться не будет, поэтому выбираем первый вариант.

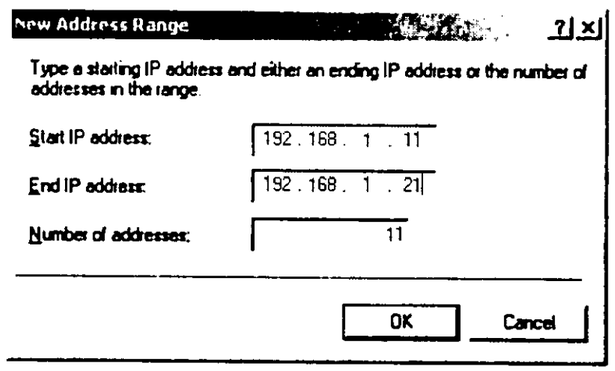


Рис. 18.6. *Диапазон IP-адресов для dial-up клиентов*

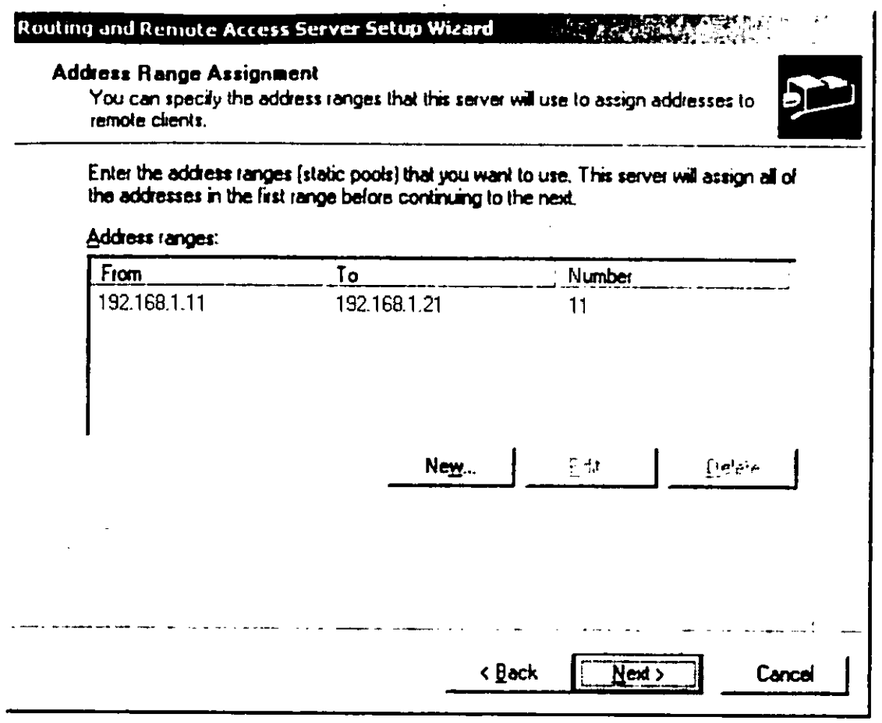


Рис. 18.7. *Указанный диапазон адресов*

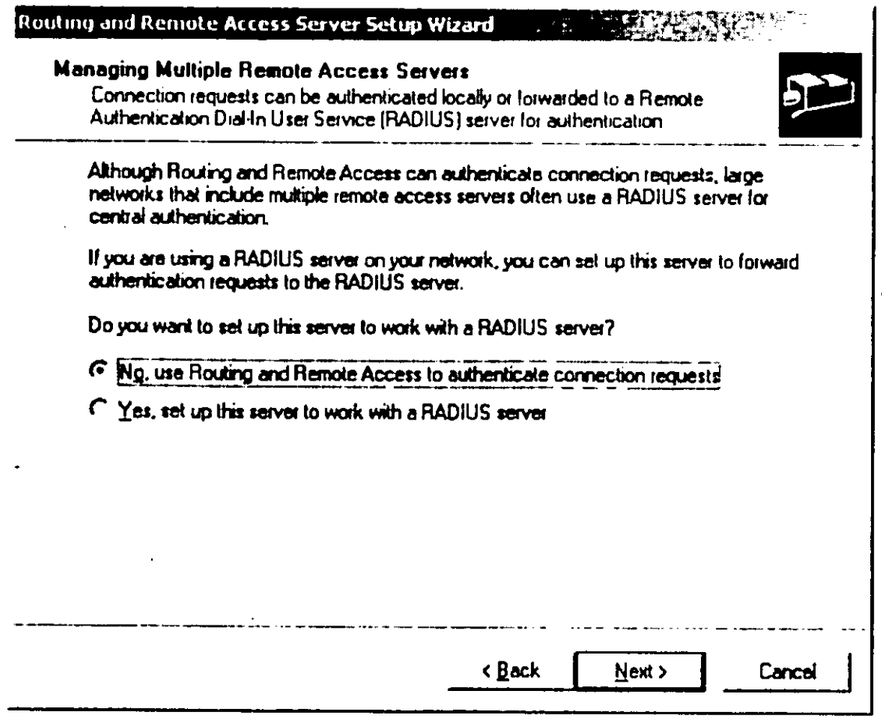


Рис. 18.8. *Настройка RADIUS*

В следующем окне нужно нажать только кнопку **Finish**. Но не спешите этого делать: сначала прочитайте описание выбранных вами настроек, если, конечно, вы знаете английский. Если же нет, не отчаивайтесь и нажимайте **Finish** (рис. 18.9).

Затем нужно сконфигурировать DCHP (рис. 18.10). Конфигурация выполняется автоматически, вам нужно только подождать.

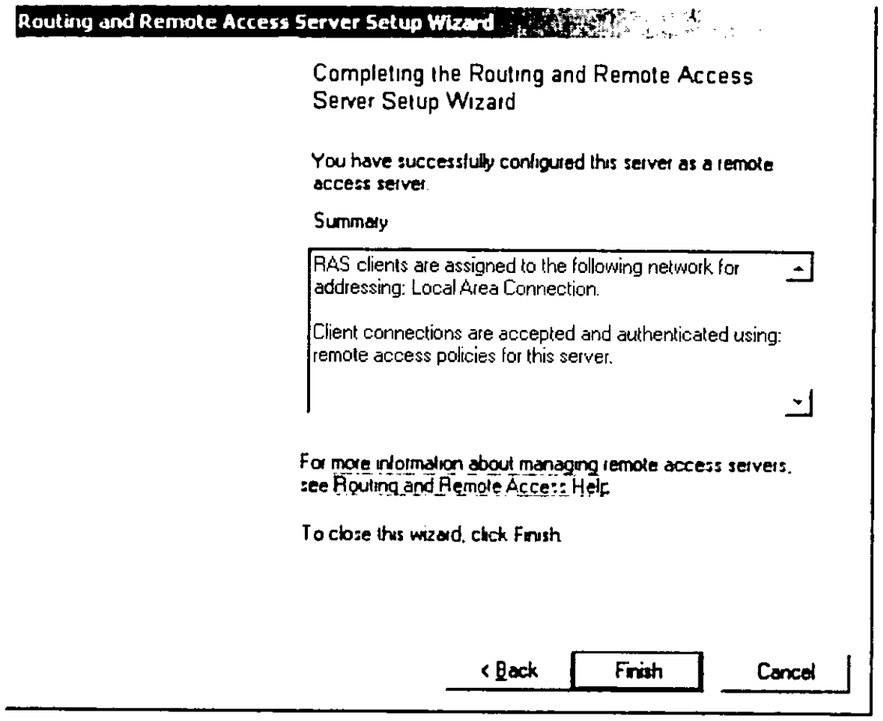


Рис. 18.9. *Финишная прямая*

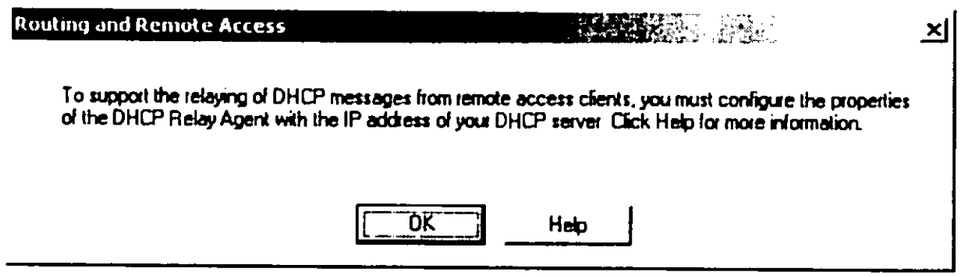


Рис. 18.10. *Конфигурация DHCP*

18.2. Установка устройств удаленного доступа

Скорее всего, удаленный доступ к вашей сети будет устанавливаться по модему, а не по какому-то WAN-порту. Поэтому перед настройкой устройств удаленного доступа нужно установить модем с помощью утилиты **Phone and Modem Options** панели управления.

Затем запускаем утилиту **Routing and Remote access** (для этого выбираем **Start →Settings → Control Panel → Adminitrative Tools → Routing and Remote Access**) и переходим в раздел Ports (см. рис. 18.11).

Убедитесь, что раздел **Ports** активен (выделен), затем выберите команду меню **Action → Properties** и вы увидите свойства портов (рис. 18.12).

Выбираем наш модем и нажимаем кнопку **Configure** (или дважды щелкаем по модему — как кому нравится). В появившемся окне нужно выбрать **Remote access connections (inbound only)**, что на русском звучит так: «Удаленные соединения (только входящие)», то есть по этому модему будут приниматься только входящие соединения. Вторая опция **Demand-dial routing connections (inbound and outbound)** — это соединения по требованиям, то есть ваш модем может быть использован как для входящих, так и для исходящих соединений. Мы ограничимся только первой опцией (рис. 18.13).

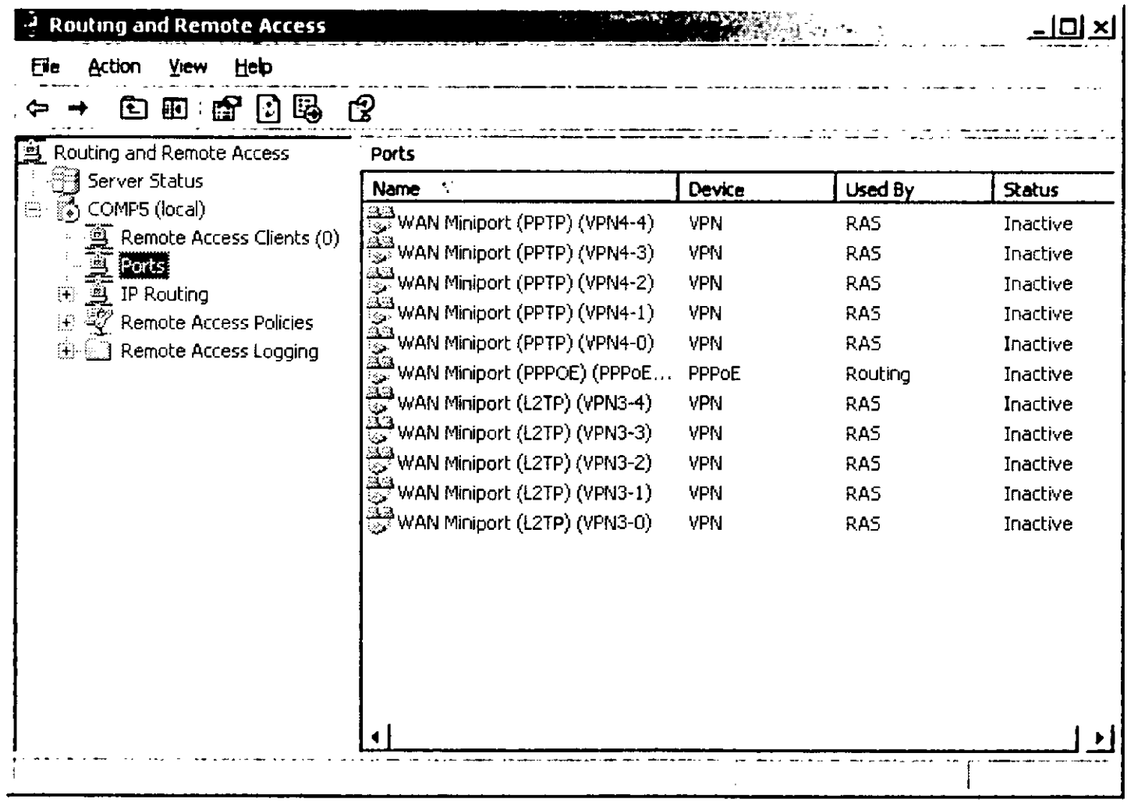


Рис. 18.11. *Утилита Routing and Remote Access*

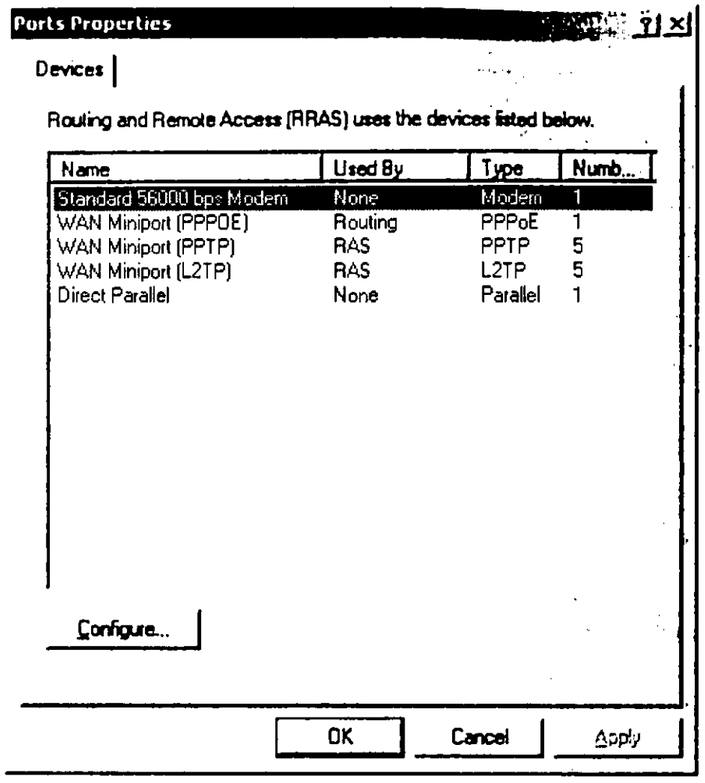


Рис. 18.12. *Свойства портов*

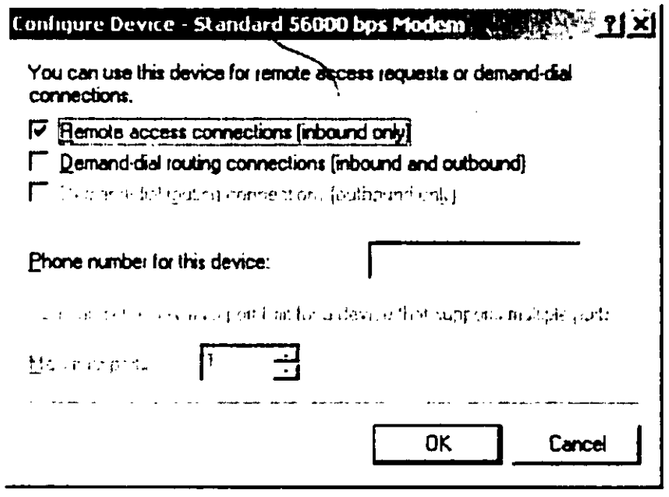


Рис. 18.13. *Свойства модема*

Теперь в окне свойств портов отображается наш модем с пометкой, что он используется службой удаленного доступа — **Used by RAS** (рис. 18.14). Модем также будет отображен в списке портов утилиты Routing and Remote Access (рис. 18.15).

В свойствах модема не забудьте указать строку инициализации **ATS0=1** — без нее модем не будет поднимать трубку.

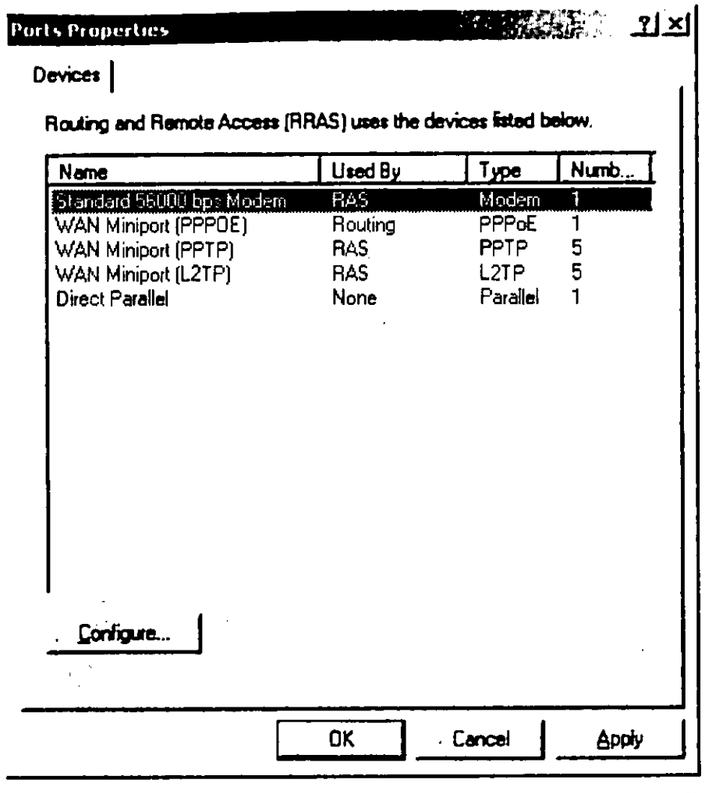


Рис. 18.14. *Теперь наш модем используется службой RAS*

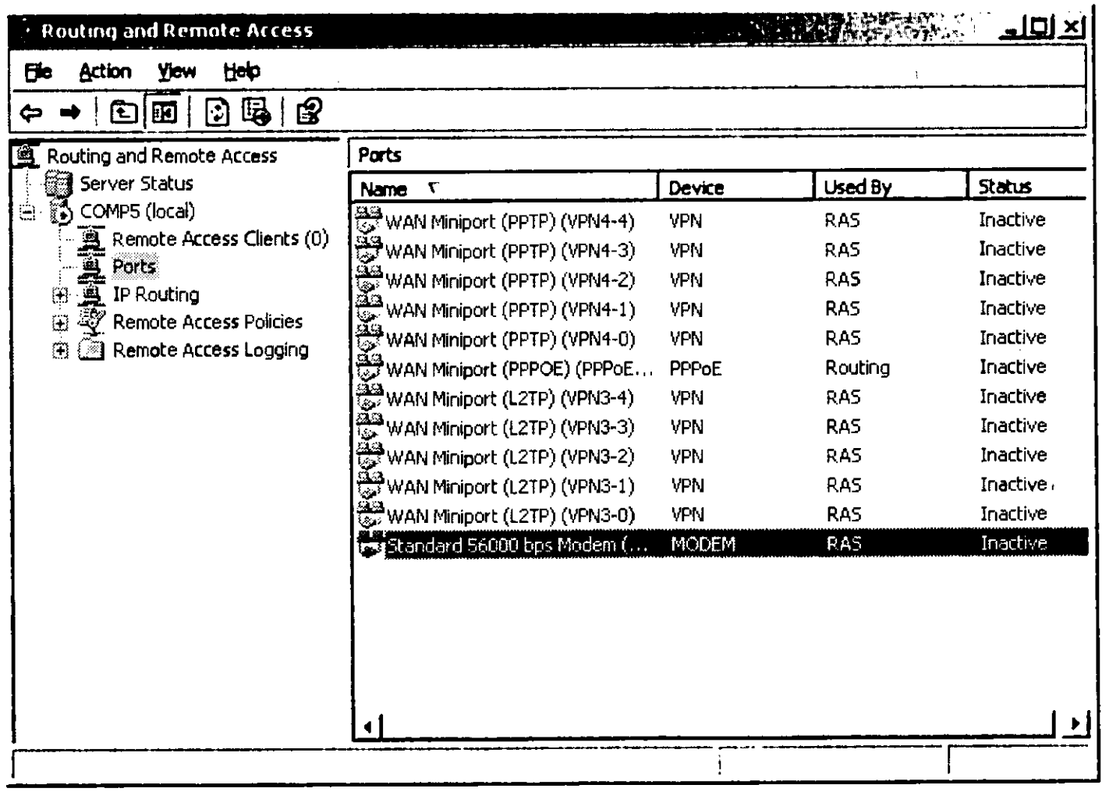


Рис. 18.15. *Модем в списке портов*

18.3. Пользователи

На этом настройка сервера входящих звонков практически завершена. Осталось только добавить пользователей, которым разрешен удаленный доступ. Возможно, пользователи уже добавлены, тогда остается только в свойствах пользователя разрешить удаленный доступ. Для этого откройте утилиту **Active Directory Users and Computers** (она, как и все предыдущие, находится в меню **Administrative Tools**). Окно утилиты показано на рис. 18.16.

Затем нужно создать нового пользователя. Для этого нажмите кнопку с изображением пользователя на панели инструментов (рис. 18.17).

Будьте внимательны при вводе пароля пользователя: в зависимости от ваших политик безопасности система может не принять короткий или простой пароль. Параметры учтенной записи также устанавливаются в окне ввода пароля:

- **User must change password at next logon** — пользователь должен изменить пароль при следующем входе в систему.
- **User cannot change password** — пользователь не может изменить пароль.
- **Password never expires** — срок действия пароля никогда не истекает
- **Account is disabled** — учетная запись отключена.

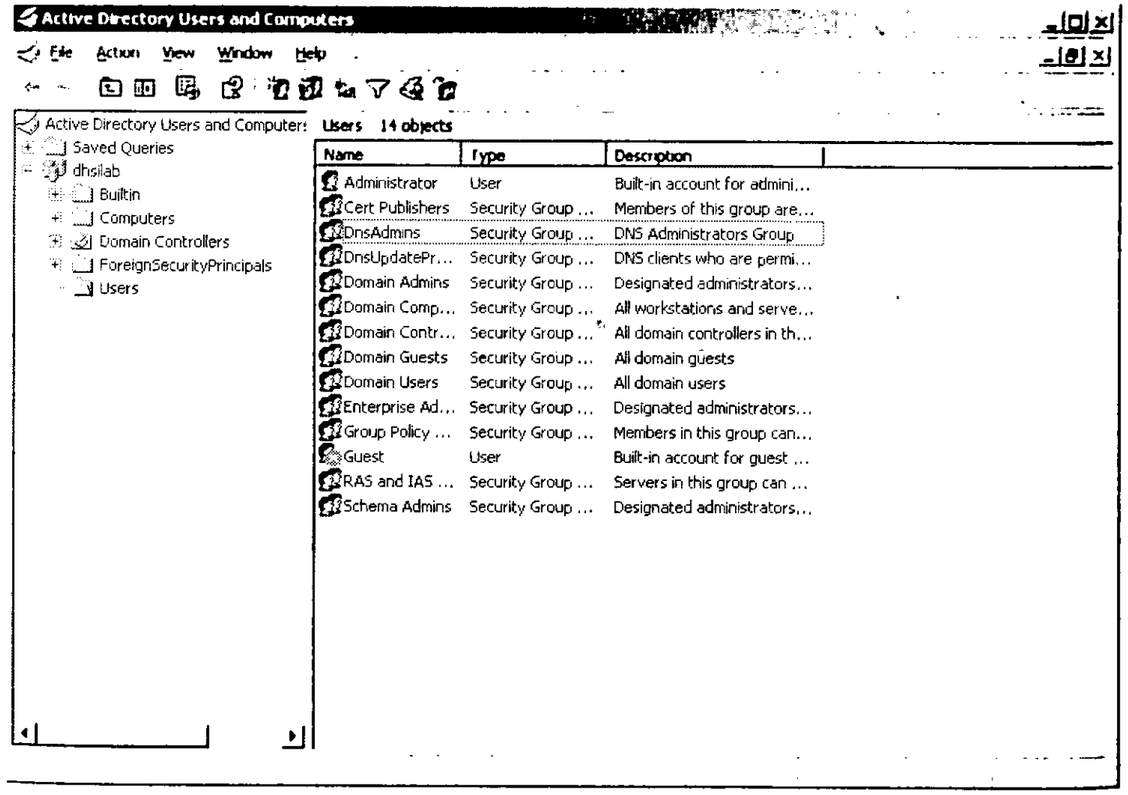


Рис. 18.16. *Утилита Active Directory Users and Computers*

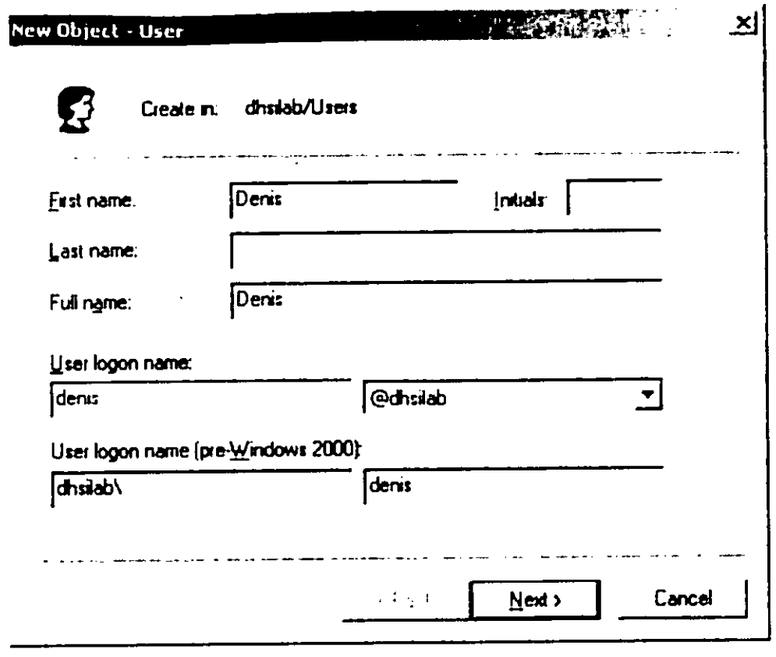


Рис. 18.17. *Создание нового пользователя*

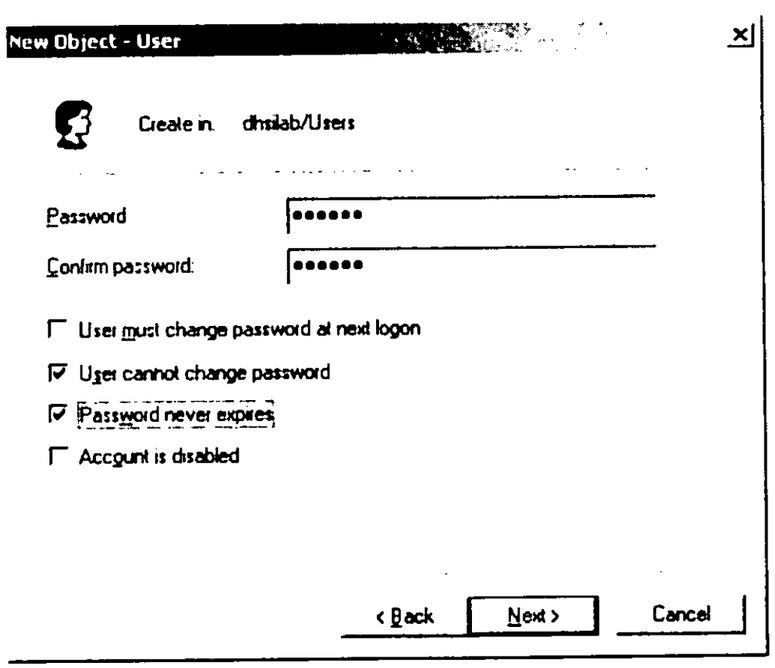


Рис. 18.18. *Окно ввода пароля*

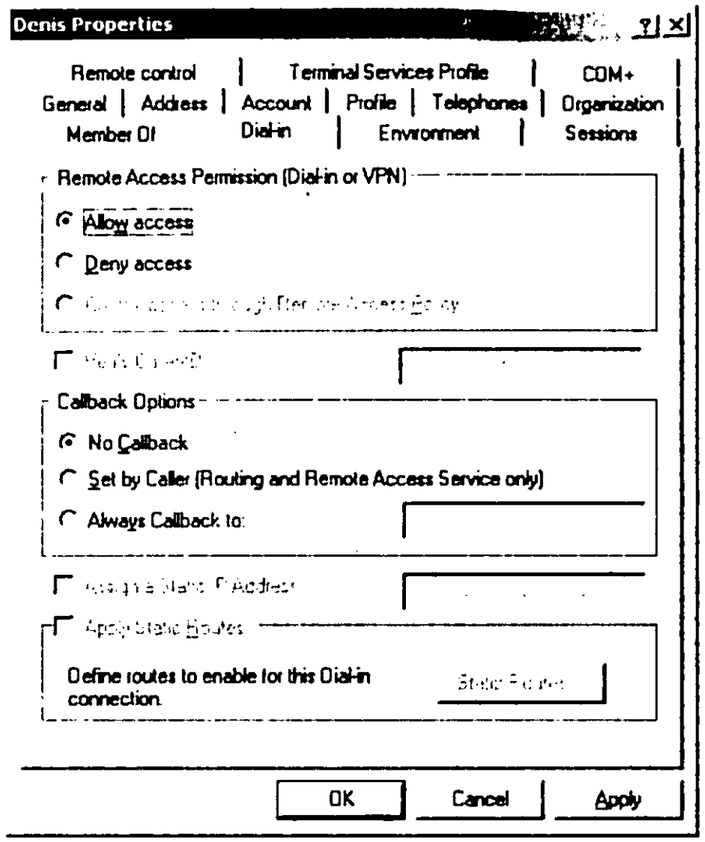


Рис. 18.19. *Разрешение удаленного доступа.*

Затем щелкните правой кнопкой мыши по созданному пользователю и выберите команду **Properties**. В окне свойств пользователя перейдите на вкладку **Dial-up** и выберите режим **Allow access** (Разрешить удаленный доступ) (рис. 18.19).

На этом настройка сервера удаленного доступа завершена. Можете приступать к тестированию настроек.

Что делать, если нужно настроить сервер удаленного доступа под Linux

В данной главе я лишь хочу порекомендовать, если вам нужно настроить сервер удаленного доступа на основе Linux — обратитесь к моей книге «Linux-сервер своими руками». Вопрос построения сервера удаленного доступа является достаточно серьезным и отдельными инструкциями здесь не обойтись. А рассматривать в данной книге сетевые механизмы Linux в полном объеме нет никакого резона, так как это отдельная книга.

Часть VII

ВЫЯВЛЕНИЕ НЕИСПРАВНОСТЕЙ И РЕШЕНИЕ ПРОБЛЕМ

Глава 20

Тестирование сети

В этой главе мы поговорим о поиске неисправности в сети, то есть постараемся ответить не только на вопрос «Почему «упала» сеть?», но и сказать, где именно она «упала».

Неисправности сети могут быть связаны или с нашим локальным компьютером, или же с удаленным. Прежде чем обвинять кого-то, продиагностируем свой компьютер. Узнать, где именно возникла проблема, на локальном или удаленном компьютере, иногда довольно сложно. Но если везде сеть есть, а у вас нет, то ясное дело, что проблемы с вашим компьютером.

20.1. Тестирование локального компьютера и локальной сети

Перед тем как приступить к тестированию программного обеспечения, проверим аппаратное обеспечение. Для начала хватит простой визуальной проверки: подключен ли сетевой кабель к сетевой плате, подключен ли второй его конец к концентратору, включен ли модем и подключен ли он к компьютеру и т.д. Если визуально все нормально, можно приступать к программному обеспечению.

Иногда бывает так, что выглядит все нормально, а провод перебит или витая пара плохо обжата. Тогда провода нужно «прозвонить», но все это только после того, как вы убедитесь, что с настройками сети у вас все нормально, иначе вы рискуете потратить впустую много времени, пытаясь найти неисправность, которой нет.

Проверим, есть ли вообще поддержка сети на нашем локальном компьютере. Для этого мы будем использовать программу **ping**:

```
# ping localhost
PING localhost (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=255 time=0.4 ms
^C
-- localhost ping statistics --
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.4/0.4 ms
```

Программа **ping** работает в беспрерывном режиме. Для ее завершения нажмите Ctrl + C.

В Linux, если вы увидите сообщение об ошибке, значит, вы неправильно настроили сеть. Возможно, просто отключен сервис **network**, попробуйте его активизировать:

```
service network start
```

После этого попробуйте опять пропинговать `localhost`. Если же опять возникла ошибка, значит, вам самое время прочитать главу «Настройка сети» заново, чтобы правильно настроить сеть — периодически я буду направлять вас к этой главе, поскольку не вижу смысла переписывать ее еще раз.

В Windows проблемы с адресом 127.0.0.1 могут быть связаны с отсутствием протокола TCP/IP или повреждением некоторых системных файлов. Убедитесь, что протокол TCP/IP установлен. Если он установлен, а проблема все равно есть, удалите его и установите заново. После перезагрузки компьютера проблема должна исчезнуть.

Примечание.

Возможными причинами отказа интерфейса lo могут быть:

- Вы забыли внести localhost (или это не сделал сервис network в Linux) в таблицу маршрутизации: route add 127.0.0.1. В Windows данная запись вносится автоматически.
- Вы не внесли запись «localhost 127.0.0.1 localhost.localdomain» в файл /etc/hosts.

Если же с адресом `localhost` все нормально, убедимся, что наши сетевые интерфейсы работают правильно. Для этого введите команду:

```
ifconfig
```



```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          Collisions:0
eth0      Link encap 10Mps Ethernet HWaddr  00:11:D1:90:B7:55
          inet addr 192.168.1.1 Bcast 192.168.1.255 Mask 255.255.255.0
          UP BROADCAST RUNNING  MTU 1500  Metric 1
          RX packets 0 errors 0 dropped 0 overrun 0
          TX packets 0 errors 0 dropped 0 overrun 0
```

В списке интерфейсов вы должны увидеть интерфейс localhost и несколько других сетевых интерфейсов — ethX, pppX.

В Windows вместо программы **ifconfig** используется программа **ipconfig**, однако данная программа не отображает информацию об адресе 127.0.0.1.

```
Настройка IP для Windows 98
0 Ethernet: плата :
     IP-адрес. . . . . . . . . . . . . . : 192.168.1.77
     Маска подсети . . . . . . . . . . . : 255.255.255.0
     Стандартный шлюз. . . . . . . . . . :
1 Ethernet: плата :
     IP-адрес. . . . . . . . . . . . . . : 0.0.0.0
     Маска подсети . . . . . . . . . . . : 0.0.0.0
     Стандартный шлюз. . . . . . . . . . :
```

Предположим, что вы подключаетесь к локальной сети с помощью сетевой платы (`eth0`). Если интерфейса `eth0` нет в списке, его нужно поднять (при условии, что вы до этого вообще настраивали сеть):

```
ifconfig eth0 192.168.1.1 up // 192.168.1.1 — это наш IP-адрес
```

Примечание.

За интерфейсы pppX отвечает демон pppd, поэтому не нужно пытаться поднять их с помощью **ifconfig**.

Если же интерфейс есть в списке и нормально работает, в чем можно убедиться, пропинговав его:

```
ping 192.168.1.1
```

В Windows активизация сетевых интерфейсов не нужна — они активизируются при запуске системы автоматически. Проблемы с сетевой платой могут быть связаны с некорректной установкой или повреждением файлов драйвера.

Если вы не можете пропинговать плату по ее IP-адресу, а настройки сетевого адаптера верны (то есть вы видите назначенный IP-адрес, но не можете его пропинговать), попробуйте переустановить драйвер сетевого адаптера или же переустановить протокол TCP/IP. Возможно, вы указали IP-адрес, который уже используется другим узлом в этой подсети, тогда программа отобразит указанный вами IP-адрес, но маска сети будет 0.0.0.0.

Если сетевой интерфейс работает нормально, то тут может быть несколько вариантов:

1. **Если вы не можете подключиться к соседнему узлу вашей локальной сети, а можете подключиться к любому другому узлу локальной сети**, значит, ваш компьютер работает исправно, а проблемы возникли «на том конце провода».
2. **Если же вы не можете подключиться ни к одному компьютеру локальной сети,** проверьте сетевой кабель: подключен ли он к компьютеру и к хабу. Если же визуальная проверка ничего не показала, попробуйте прозвонить его и, если нужно, заново обжать (при условии, что вы используете коаксиал или витую пару). В самом крайнем случае проблемы могут быть с самим концентратором, но это только теоретически — на практике мне не встречались хабы, которые работают частично (то есть один порт работает, а другой — нет) — он или работает, или нет.
3. **Если вы не можете подключиться к узлу другой сети или Internet,** проверьте параметры маршрутизации: шлюз по умолчанию, маршруты. Подробнее обо всем этом мы поговорим в следующем пункте.

Перед тем как перейти к следующему пункту, рассмотрим параметры программы **ping**, которую мы недавно использовали. В табл. 20.1 указаны не все параметры, а только самые нужные, имеющиеся в Linux. Формат вызова команды:

```
ping [параметры] <IP-адрес|доменное имя>
```

Параметры Windows-версии программы ping несколько отличаются и приведены в табл. 21.2.

Все остальные параметры программы **ping** для Windows несущественны.

Параметры программы ping для Linux *Таблица 20.1*

Параметр	Описание
-b	Разрешить пинг широковещательного адреса, например, 192.168.1.255
-c число	Отправить указанное число пакетов
-i интервал	Отправлять пакеты с заданным интервалом
-q	«Тихий» режим
-t TTL	Использовать указанный TTL для отправки пакетов указанному узлу
-r	Отправка пикетов непосредственно, в обход таблиц маршрутизации. Данная опция полезна, если у вас проблемы с маршрутизацией

Параметры программы ping для Windows *Таблица 20.2*

Параметр	Описание
-t	Отправлять пакеты непрерывно, до команды прерывания (нажатия Ctrl + C)
-a	Определение адресов по имени узлов (разрешение имен)
-n количество	Отправить указанное количество пакетов
-l буфер	Задание размера буфера отправки
-f	Запретить фрагментацию пакета
-i TTL	Задание TTL (Time To Live) – времени жизни пакета
-v TOS	Задание TOS (Type of Service)
-w секунды	Интервал ожидания каждого ответа в секундах

20.2. Проблемы с подключением к другой подсети

Методики и инструменты выявления неполадок

Как правило, доступ к другой сети производится посредством маршрутизатора. Поэтому, если вы не можете получить доступ к узлам соседней сети, возможны три причины:

- У вас неправильные настройки маршрутизации.
- Администратор маршрутизатора запретил вам доступ к соседней сети. Очень часто такая ситуация случается на Internet-шлюзах.
- Неисправен маршрутизатор.

На вторые две причины вы вряд ли сможете повлиять, поэтому рассмотрим только первую. Для диагностики параметров маршрутизации используйте программу **route**. Для установки шлюза 192.168.100.254 по умолчанию используйте команду:

```
/sbin/route add default gw 192.168.100.254 netmask 0.0.0.0 metric 1
```

В Windows для установки шлюза по умолчанию намного удобнее воспользоваться панелью управления. В свойствах соединения просто установите IP-адрес шлюза по умолчанию. Можно также использовать команду route:

```
route add 0.0.0.0 mask 255.255.255.0 192.168.1.1 metric 1
```

Если вы хотите создать постоянный маршрут (который не теряется при перезагрузке системы), используйте параметр **–p**.

Просмотрим таблицу маршрутизации Linux

```
[root@server]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Metric  Ref    Use   Iface
192.168.100.0   0.0.0.0         255.255.255.0   U       0       0      0     eth0
127.0.0.0       0.0.0.0         255.0.0.0       U       0       0      0     lo
0.0.0.0         192.168.100.254 0.0.0.0         UG      0       0      0     eth0
```

Примечание.

Параметр –n команды **route** означает, что нам нужно выводить не символьные имена, а IP-адреса.

В Windows для вывода таблицы маршрутизации используется команда **route print**:

```
Активные маршруты:
Сетевой адрес   Маска           Адрес шлюза     Интерфейс       Метрика
0.0.0.0         255.255.255.0   192.168.1.1     192.168.1.77    1
127.0.0.0       255.0.0.0       127.0.0.1       127.0.0.1       1
192.168.1.0     255.255.255.0   192.168.1.77    192.168.1.77    1
192.168.1.77    255.255.255.255 127.0.0.1       127.0.0.1       1
192.168.1.255   255.255.255.255 192.168.1.77    192.168.1.77    1
224.0.0.0       224.0.0.0       192.168.1.77    192.168.1.77    1
255.255.255.255 255.255.255.255 192.168.1.77    192.168.1.77    1
```

Если же параметры маршрутизации у вас правильны (полчаса назад все работало, а сейчас — нет), тогда посмотрим, где именно происходит обрыв в маршруте. Для этого нам понадобятся следующие программы:

- **traceroute** — печать маршрута прохождения пакетов;
- **traceroute6** — аналог traceroute, но предназначен для работы с IPv6;
- **tracepath** — это несколько упрощенный аналог traceroute;
- **tracepath6** — то же, что и tracepath, но для работы с IPv6.

Утилита **traceroute** (в Windows — tracert) предназначена для печати маршрута, который проходят по сети пакеты, от узла-источника до узла-назначения. Например, мы хотим узнать, через какие узлы (маршрутизаторы) проходят наши пакеты до узла `smtp.mail.ru`. Введите команду:

```
traceroute smtp.mail.ru

traceroute to smtp.mail.ru (194.67.23.10), 30 hops max, 38 byte packet
1   max.romb.net (193.254.218.12) 193 ms   183 ms   269 ms
2   sat-router.romb.net (193.254.218.2) 197 ms   245 ms   184 ms
3   vcad1.kw.ukrtel.net (195.5.59.14) 210 ms   268 ms   245 ms
4   crouter.kw.ukrtel.net (195.5.59.1)  223 ms   243 ms   281 ms
5   195.5.54.249 (195.5.54.249)  259 ms   270 ms   379 ms
6   STM1-Kiev-Dnepr.ukrtel.net (195.5.5.197)  619 ms   330 ms   331 ms
7   195.5.53.54 (195.5.53.54)  747 ms   698 ms   600 ms
8   bpt-b1-pos0-2.telia.net (213.248.69.65)  800 ms   1368 ms   599 ms
9   ffm-b1-pos13-1.telia.net (213.248.103.1)  699 ms   893 ms   599 ms
10  POS3-1.BR2.FFT1.ALTER.NET (146.188.67.85)  620 ms   623 ms   599 ms
11  so-0-2-0.TR1.FFT1.ALTER.NET (146.188.6.109)  548 ms   746 ms   721 ms
12  so-2-0-0.TR1.STK2.ALTER.NET (146.188.3.145)  575 ms   623 ms   578 ms
13  ge-7-3-0.XR1.STK3.ALTER.NET (146.188.11.229)  667 ms   601 ms   570 ms
14  POS1-0.GW9.STK3.ALTER.NET (146.188.11.229)  667 ms   601 ms   570 ms
15  Sovintel-gw.customer.ALTER.NET (146.188.65.38) 657 ms   660 ms   599 ms
16  cat01.Moscow.gldn.net (194.186.157.70)  538 ms   632 ms   649 ms
17  smtp.mail.ru (194.67.23.10)  646 ms   600 ms   649 ms
```

Вы видите, что по дороге до `smtp.mail.ru` наши пакеты проходят 17 маршрутизаторов. Может случиться такое, что ваш компьютер отлично работает, `smtp.mail.ru` тоже чувствует себя отлично. Но пакеты, отправленные нами, до `smtp.mail.ru` не доходят. Значит, где-то оборвалась цепочка произошел сбой на одном из маршрутизаторов. Команда **traceroute** поможет вам определить, на каком именно маршрутизаторе произошел сбой.

Программа **traceroute** делает три попытки обращения к узлу, поэтому вы видите три колонки с временем:

```
17  smtp.mail.ru (194.67.23.10)  646 ms   600 ms   649 ms
```

Формат вызова команды **traceroute** следующий:

```
traceroute [параметры] узел
```

В табл. 20.3 приведено описание параметров команды **traceroute** в Linux, а в табл. 20.4 — ее Windows-аналога tracert.

Параметры программы traceroute (в Linux) *Таблица 20.3*

Параметр	Описание
-f	Установить начальное значение TTL по первому пакету
-F	Не разбивать пакеты (устанавливает флаг don't fragment)
-d	Включает отладку на уровне сокетов
-i интерфейс	Использовать указанный интерфейс для отправки пакетов
-I	Использовать ICMP ECHO вместо UDP-дейтаграмм
-m переходы	Установить максимальное число переходов (hops), по умолчанию – 30
-p порт	Использовать указанный порт (по умолчанию 33434)
-r	Действовать в обход таблиц маршрутизации
-v	Вывод дополнительной информации

Параметры программы tracert (в Windows) *Таблица 20.4*

Параметр	Описание
-d	Не определять IP-адреса по именам узлов
-h число	Задает максимальное число переходов
-j список	Свободный выбор маршрута по списку узлов
-w интервал	Интервал ожидания каждого ответа в секундах

Программа **tracepath** очень похожа на **traceroute**, но кроме времени ответа она возвращает значения MTU, что бывает очень полезно, особенно при отладке ADSL-соединений. Программа **tracepath** устанавливается по умолчанию в современных дистрибутивах (иногда даже **traceroute** не устанавливается, зато **tracepath** доступна).

Формат вызова этой программы такой:

```
tracepath узел [порт]
```

Программа **tracepath6** предназначена для работы по протоколу IPv6. Вот ее вывод:

```
[root@server ~] # tracepath6 3ffe:2400:0:109::2
1?: [LOCALHOST]                                      pmtu 1500
1:  dust.inr.ac.ru                                    0.411ms
2:  dust.inr.ac.ru          asymm  1    0.390ms pmtu 1480
2:  3ffe:2400:0:109::2                  463.514ms reached
 Resume: pmtu 1480 hops 2 back 2
```


Ошибки DNS

Если мы можем обратиться к узлу по IP-адресу, но не можем по имени, то причина кроется в следующем. Скорее всего, мы неправильно настроили систему разрешения имен. Настройки системы DNS хранятся в файлах `/etc/hosts.conf` и `/etc/resolv.conf`.

В Windows проверьте свойства соединения: может, вы забыли указать IP-адреса серверов DNS или указали неправильные IP-адреса.

Если же IP-адреса серверов DNS указаны правильно, значит, ошибка происходит на уровне самого сервера DNS, а это уже не ваша проблема, а проблема администратора сервера DNS.

Проблемы с PPP-соединением

Чаще всего возникает проблема маршрута по умолчанию. Вы настраиваете ppp, потом устанавливаете соединение. Соединение установлено, но вы не можете передать ни одного пакета в сеть, к которой подключились. Обычно причина заключается в том, что вы забыли указать опцию defaultroute в файле `/etc/ppp/options`. Если же и после этого пакеты отправить невозможно, попробуйте ввести следующую команду:

```
route add -net default ppp0
```

В Windows, как правило, таких проблем не возникает.

Итак, для тестирования сети используются подручные средства, которые можно найти в любой операционной системе:

- **ping** — посылает пакеты до узла-назначения;
- **traceroute** (**tracert** в Windows) — печатает маршрут, который проходят пакеты от узла-источника до узла-назначения;
- **route** — управляет таблицей маршрутизации ядра.

Глава 21

Неприятные ситуации и как от них избавиться

Иногда бывает так, что будто бы все настраиваешь правильно, а ничего не работает. Это как раз о вас? Тогда данная глава предназначена именно для вас.

21.1. Проблемы, связанные с сетевыми адаптерами, и их решение

Проблема 1

Очень часто производители материнских плат стараются удешевить свою продукцию. Пользователи стараются удешевить стоимость всей системы. Вот и выходит, что на рынке очень часто можно увидеть материнские платы со встроенными видео, звуковыми, сетевыми платами и модемами. Как правило, интегрированные компоненты работают намного хуже, чем их обыкновенные сородичи, которые устанавливаются в шину компьютера.

Один раз пришлось оснащать отдельными сетевыми адаптерами целый компьютерный класс, поскольку встроенные сетевые платы отказывались работать со скоростью, большей 10 Мбит/с.

Проблема 2

Еще одна неприятная ситуация получилась со старенькой платой Realtek. Она то работала, то не работала. Пробовал пинговать — через раз — один раз пинг до соседнего узла «доходит», другой — нет. Оба узла подключены к одному концентратору и находятся в одной комнате.

Пробовал подключать к другому порту хаба — не помогло, затем обжал витую пару заново — тоже не помогло. После этого переустановил драйвер, причем драйвер был родной — шел именно с этой платой. Последний шаг — переустановил сначала TCP/IP и все остальные сетевые компоненты, а затем Windows. И это не помогло. В общем, все закончилось заменой сетевой платы.

Отсюда можно сделать вывод, как проверять сетевую плату:

1. Сначала пробуем подключить к другому порту хаба. Если проблема исчезла, значит, причина в хабе (или коммутаторе). Если же нет, то следует перейти к следующему пункту.
2. Потом проверяем обжимку. Легче проверить порт хаба, чем обжимку, поэтому данный пункт второй.
3. Иногда помогает установка сетевой платы в другой слот (если она не интегрирована в материнскую).
4. Проверив аппаратную часть, переходим к программной. По очереди переустанавливаем и проверяем результат: драйвер, сетевые компоненты, Windows.

Проблема 3

Вернемся к вопросу о встроенных сетевых адаптерах. Многие производители материнских плат используют встроенные сетевые платы на базе чипа Realtek. Это хороший, проверенный, а главное — дешевый чип. Вот только не используйте первый попавшийся драйвер для этого чипа. Нужно использовать только драйвер производителя. Хорошо, если стандартный драйвер операционной системы подошел. Тогда проблем не будет.

Проверить это просто. Попробуйте подключиться к другому компьютеру. Подключение прошло успешно? Если да, то попробуйте скачать с этого компьютера какой-то файл, желательно большой. Если файл оказался поврежден, то причина может скрываться в драйвере. Установите драйвер производителя, и все будет нормально.

21.2. Проблемы в локальной сети и их решение

Проблема 1

Представим такую ситуацию. У нас есть сеть Microsoft с контроллером домена на базе Windows NT или Windows 2000/2003 Server. Вход в сеть выполняется очень долго. Причина, скорее всего, заключается в том, что вы используете один и тот же каталог для хранения профиля пользова-

теля и «домашних» файлов пользователя. При входе в сеть каталог, содержащий профиль, копируется на локальный компьютер. Профиль, как правило, не занимает много места, а вот домашний каталог пользователя может содержать сотни мегабайт информации. И пока эти сотни мегабайт не скопируются на локальный компьютер, пользователь в сеть не войдет. Понимаете, о чем я?

Проблема 2

Помню, у меня был компьютер, на котором был установлен модем — для доступа к Internet. Модем работал нормально, выполняя возложенную на него задачу — доступ к всемирной Сети. Спустя некоторое время появилась необходимость подключить компьютер к локальной сети.

Драйвер сетевого адаптера был установлен корректно, сетевой адаптер отображался в списке устройств, конфигурация сети в аплете **Сеть** с Панели управления также была правильной. Но я не то что не мог получить доступ к этому компьютер из локальной сети, я даже не мог пропинговать его локально — команда **ping**, выполнявшаяся на этом компьютере, сообщала что «узел недоступен».

Я ввел команду **ipconfig**. Оказалось, что в системе присутствует только контроллер удаленного доступа — это тоже своеобразная сетевая плата для доступа к удаленной сети. Как оказалось, такое случается довольно часто с операционными системами Windows 95/98 — на языке Microsoft — это «feature», то есть неотъемлемая особенность работы.

Лечится это горе довольно просто. Вы должны очистить всю конфигурацию сети: удалить все протоколы, все клиенты, все сетевые адаптеры, включая контроллер удаленного доступа. Перед перезагрузкой компьютера убедитесь, что сетевой адаптер удален из списка устройств (модем удалять не нужно). После перезагрузки компьютера сконфигурируйте сеть, как обычно. А *потом* добавьте контроллер удаленного доступа. После перезагрузки можно проверить конфигурацию сети программой **ipconfig**. Она будет примерно такой:

```
Настройка IP для Windows 98
0 Ethernet: плата :
     IP-адрес. . . . . . . . . . . . . . : 192.168.1.5
     Маска подсети . . . . . . . . . . : 255.255.255.0
     Стандартный шлюз. . . . . :
1 Ethernet: плата :
     IP-адрес. . . . . . . . . . . . . . : 0.0.0.0
     Маска подсети . . . . . . . . . . : 0.0.0.0
     Стандартный шлюз. . . . . :
```


Проблема 3

Довольно часто, особенно в больших сетях, вы можете забыть, какой IP-адрес уже занят, и назначить уже занятый адрес другом компьютеру. В результате у нас будут два компьютера и один IP-адрес. Избежать конфликта адресов и автоматизировать их «раздачу» позволяет DHCP сервер.

Если у вас нет желания его настраивать, выявить конфликт IP-адресов поможет сама система — при загрузке она сообщит, что уже есть такой IP-адрес в сети. Если же вы после изменения IP не перезагружали систему, выявить конфликт поможет программа ipconfig. Если вы назначили уже занятый IP-адрес, программа выведет его, но маска сети будет 0.0.0.0.

Проблемы с удаленным доступом

Проблема 1

Если модем не снимает трубку, значит, вы забыли указать специальную строку инициализации. Она выглядит так:

```
ATS0=n
```

n — это количество гудков, после которых модем должен поднять трубку.