Самоучитель

Александр Поляк-Брагинский

Сеть своими руками

3-е издание

- Принципы построения локальных сетей
- Удаленное администрирование
- Общее подключение к Интернету
- Антивирусные средства
- Защита сети
- Виртуальные технологии в сети
- Windows Vista и Linux в локальной сети

bhv

Александр Поляк-Брагинский

Сеть своими руками

3-е издание

Санкт-Петербург
«БХВ-Петербург»
2008

УДК 681.3.06
ББК 32.973.202
П54

Поляк-Брагинский А. В.

П54 Сеть своими руками. — 3-е изд. перераб. и доп. — СПб.: БХВ-Петербург, 2008. — 640 с.: ил. — (Самоучитель)

ISBN 978-5-9775-0163-7

Книга представляет собой практическое руководство по созданию локальной вычислительной сети для дома или небольшого офиса, от простейшей одноранговой до многоуровневой. Обсуждаются вопросы маршрутизации, удаленного администрирования и управления, настройки почтового сервера, совместного использования ресурсов. Представлено обстоятельное описание программ WinRoute, Radmin, Courier Mail Server и др., позволяющих создать полнофункциональную сеть. Даны многочисленные ссылки на соответствующие ресурсы в Интернете.

Третье издание дополнено примерами построения конкретных сетей, в которых работают компьютеры под управлением операционных систем Windows Vista и Linux. Рассмотрено применение виртуальных компьютеров в сети и введен ряд других новых тем. Обновлен раздел вопросов и ответов, составленный по реальным вопросам читателей первого и второго издания.

Для опытных пользователей

УДК 681.3.06
ББК 32.973.202

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Редактор	*Владимир Красовский*
Компьютерная верстка	*Натальи Смирновой*
Корректор	*Зинаида Дмитриева*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.11.07.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 51,6.
Тираж 3000 экз. Заказ №
"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.

Санитарно-эпидемиологическое заключение на продукцию № 77.99.02.953.Д.006421.11.04
от 11.11.2004 г. выдано Федеральной службой по надзору
в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0163-7

Оглавление

Введение

Ваша первая сеть

На дворе уже XXI век. Вся наша жизнь подчинилась компьютерным технологиям, хотим мы того или нет. Все чаще возникает необходимость в оперативной связи между компьютерами как в офисе, так и дома. Компьютеры теперь есть практически у каждого (во всяком случае, из тех, кто читает эту книгу). Однако объединение компьютеров в сеть считается до сих пор задачей весьма сложной и требующей специальной подготовки. Эта книга поможет вам создать свою сеть. Если вы решились на этот шаг, то вам необходимо согласовать вопросы строительства сети с друзьями или сотрудниками, возможно, с владельцем здания или помещения, где вы планируете организовать сеть. Определитесь с потребностями и только после этого приобретайте недостающие детали и оборудование.

Хотя назначение сети может быть самым разнообразным, общие принципы построения сети одинаковы. Мы обратим внимание на особенности сетей, предназначенных для выполнения конкретных задач, но большинство рекомендаций подойдут для всех случаев.

Шаг за шагом мы пройдем весь путь строительства нашей сети, рассматривая теоретический материал в минимально необходимом объеме. Дальнейшую поддержку сети вы сможете осуществлять самостоятельно.

Таким образом, эта книга поможет вам сэкономить определенную сумму, которую пришлось бы заплатить за организацию сети и ее поддержку. Конечно, когда размеры вашей сети существенно увеличатся, а требования повысятся, придется нанять специалиста. Но и в этом случае вы окажетесь в выигрыше. Уже имея минимальный опыт общения с сетью, вы никогда не позволите "запудрить себе мозги" заумными фразами.

В большинстве случаев мы будем говорить о работе в среде операционных систем Windows 98 и Windows XP, поскольку в настоящее время они самые распространенные. Существующие специализированные сетевые операционные системы требуют отдельного рассмотрения, и в книге представлены лишь описания некоторых из них. Применение таких систем оправданно при построении сетей с особыми характеристиками и задачами. Сложность специали-

зированных систем требует серьезной подготовки для поддержки и администрирования.

В предшествующих двух изданиях не рассматривалось применение операционных систем Linux. По просьбам читателей в третье издание включены описания некоторых сетевых возможностей этих операционных систем. Также рассмотрена и ОС Windows Vista, которая появилась совсем недавно. В наше время очень быстро развивается как аппаратная, так и программная база, позволяющая реализовать новые разработки в области сетевых коммуникаций. Описать все новое в этой небольшой книге невозможно, поэтому она не стала энциклопедией по современному сетестроению. Но создать сеть с применением новых операционных систем, пользуясь этой книгой, вы сможете. Особенно подробно мы рассмотрим проблемы согласования в одной сети старых и новых компьютеров. В официальной литературе этим вопросам уделяется мало внимания. Например, корпорация Microsoft постепенно перестает поддерживать свои старые продукты. С 30 июня 2005 года прекращена основная поддержка Windows 2000, с 11 июля 2006 года полностью прекращена поддержка Windows 98, а с 10 октября 2006 года прекращена поддержка Windows XP SP1 (**http://www.microsoft.com/windows/support/endofsupport.mspx**). MS-DOS уже давно не поддерживается разработчиками. Тем не менее в нашей стране эти системы еще очень распространены, поэтому часто возникает проблема совместимости старых и новых систем в одной сети.

В качестве базовой операционной системы мы рассмотрим Windows XP — самую распространенную в настоящее время. О некоторых возможностях новых операционных систем вы сможете прочитать в *приложении 1*. Операционная система — продукт дорогой, ее модернизация, а тем более замена требуют немалых вложений. Существующий парк оборудования и комплект программного обеспечения необходимо использовать с максимальной эффективностью, и только после этого делать новые приобретения.

Конечно, совсем ничего не приобретая, не удастся реализовать и недорогие проекты. Придется купить кое-что из оборудования и программного обеспечения, но затраты будут минимальными. Прогнозировать уровень затрат сложно, все зависит от задач вашей сети и от того, чтó у вас есть.

Требования к компьютерам в тех вариантах сети, которые мы рассмотрим, не выше, чем требования со стороны операционной системы.

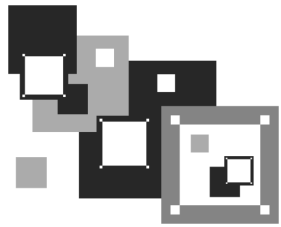
Таким образом, книга поможет вам войти в мир локальных сетей. Она станет для вас необходимой базой, если вы решите совершенствовать свои знания. А первая ваша сеть, созданная с ее помощью, будет работать на вас.

Благодарности

Когда основная работа отнимает все больше и больше времени, очень сложно найти в себе силы для работы над книгой. Если бы не содействие госпожи М.М.А., книга могла не выйти в свет. Огромная ей благодарность.

Особую признательность выражаю Евгению Рыбакову, с чьей легкой руки увидело свет первое издание этой книги, а теперь уже и третье.

Глава 1



Построение локальных вычислительных сетей

Большая часть из сотен миллионов компьютеров, существующих в мире, объединены в различные информационные сети. Зачем компьютеры объединяют в сеть? Что дает такое объединение? Почему тысячи рядовых пользователей хотят объединить свои компьютеры в единую систему, а те, кто уже объединил, так ревностно оберегают свою сеть от несанкционированного вторжения и стремятся развивать ее количественно и качественно? Что необходимо знать и какие технические средства достаточно иметь для того, чтобы самостоятельно и с разумными затратами организовать локальную вычислительную сеть (ЛВС) дома или в офисе? Ответы на эти и другие теоретические и практические вопросы построения ЛВС вы найдете в данной главе.

Для чего нужна сеть

Объединение компьютеров в сеть предоставляет пользователям дополнительные возможности:

- оперативного обмена информацией между пользователями;
- получения и передачи электронной почты, факсов, голосовой почты и других видов сообщений;
- мгновенного получения информации из любой точки земного шара;
- удаленного управления производственными процессами и удаленного администрирования;
- обмена информацией между компьютерами, работающими на разных платформах.

Рассмотрим основные преимущества, которые предоставляет пользователям объединение компьютеров в локальную сеть.

- Разделение ресурсов позволяет совместно использовать периферийные устройства (например, принтеры) и дисковое пространство удаленных компьютеров. Благодаря этому возможно применять имеющуюся дисковую память и периферийные устройства более рационально.
- Разделение данных предоставляет удаленным пользователям возможность доступа к базам данных и управления ими.
- Совместное применение программных средств.
- Использование вычислительной мощности удаленного процессора позволяет существенно снизить затраты на модернизацию оборудования и обновление парка компьютеров. Компьютер с небольшими возможностями подключается к более мощному компьютеру и используется как удаленный терминал — средство связи с удаленной рабочей станцией.
- Возможность многопользовательского режима работы с программами и документами.

Даже соединение между собой всего двух компьютеров может принести существенные выгоды и удобства.

Варианты использования сети

Пользователи могут применять предоставляемые сетью дополнительные возможности полностью или частично, постоянно или временно. Это зависит от конкретной задачи, ради которой создана данная сеть. Рассмотрим несколько видов сетей разного назначения.

Сеть для работы

Здесь имеется в виду работа, связанная с обработкой текстовых и графических материалов, обращением к базе данных, вычислениями. Такая работа чаще всего выполняется коллективно, но распределена в пространстве и времени таким образом, что только связь между компьютерами позволяет оперативно использовать результаты работы коллег или результаты своей работы при продолжении ее на другом компьютере. В этом случае компьютеры в сети имеют равноправное положение и каждый пользователь может при наличии права доступа обращаться к ресурсам другого компьютера.

Возможно, что один компьютер выделен особо. К его ресурсам могут обращаться все пользователи. Если надежность хранения информации в этой выделенной машине выше, чем в остальных, то в ее памяти сохраняются результаты труда всей группы. Такой компьютер называется *файл-сервер*. Повышенная надежность может быть обеспечена особым устройством дисковой подсистемы компьютера, надо заметить, весьма дорогостоящим. В небольших сетях затраты на оборудование не должны быть очень высокими, а надежность хранения информации можно обеспечить регулярным сохранением данных в архивах, дублированием сохраненных данных. Этим, собственно, и занимаются вышеупомянутые дорогостоящие дисковые подсистемы, но в автоматическом режиме.

Следует отметить, что при написании этой книги использовалась примерно такая сеть. Работа проходила на разных машинах, в разное время и требовались данные, которые не могли быть получены на локальном компьютере.

Сеть для учебы

Это может быть компьютеризированный класс, в котором один компьютер выделен для преподавателя, а остальные — для учащихся. В этом случае повышенные требования предъявляются к компьютеру преподавателя, а остальные компьютеры могут быть самыми обычными. Компьютер преподавателя должен иметь доступ к каждому компьютеру класса с возможностью вмешательства в его работу и работу учащегося. Обратный доступ — от учащегося к преподавателю — предусмотрен только в ограниченном виде — для получения заданий и пересылки ответов. Такой класс совсем не обязательно должен располагаться в одном помещении. Он вполне может быть распределен по территории организации для обучения сотрудников на рабочих местах. Само собой разумеется, что такая сеть применяется и совершенно в иных целях. Например, если необходим постоянный контакт с группой сотрудников для своевременного вмешательства в какой-либо коллективный процесс расчета. Это может быть и просто сеанс одновременной шахматной игры с несколькими противниками.

Сеть для бизнеса

Трудно рекомендовать какой-то вид сети для бизнеса — все зависит от задач конкретной компании. Два предыдущих варианта тоже могут применяться в бизнесе. Но все же некоторые особенности такой сети можно выделить. До-

пустим, на вашем предприятии существует деление сотрудников на кадровую службу, бухгалтерию, отдел продаж и другие отделы. В этом случае несколько компьютеров имеют специализированное назначение, а доступ к ним ограничен для большинства пользователей. Свободный доступ предусмотрен только к той части информации, которая предназначена для всех специалистов. Вы, как руководитель и сетевой администратор, получаете доступ ко всем ресурсам, чтобы иметь возможность контроля и получения различных отчетов и справок. Ограничение доступа к информации не всегда направлено на сохранение какой-либо тайны. Часто это связано со стремлением оградить важные файлы от разрушающего воздействия случайных факторов.

Сеть для игры

В этом случае требования к ресурсам компьютеров (память, быстродействие) максимальные. Кроме того, компьютеры должны быть оснащены самыми новыми версиями программ поддержки игр и устройствами, обеспечивающими работу этих программ. Эти требования не связаны непосредственно с характеристиками сети. Вызваны они лишь особенностями игрового программного обеспечения. Не только игры могут вызвать повышенные требования к компьютерам сети, но и работа с графикой, аудио- и видеомонтаж. Для коллективной игры должна быть предусмотрена возможность подключения одного компьютера к нескольким другим.

Домашняя сеть

Предполагается, что такая сеть не выходит за рамки одной квартиры или комнаты. Это особая организация сети, которая не предназначена для решения специфических сетевых задач. Она позволяет собрать в один комплекс два и более компьютера, каждый из которых не имеет необходимой вычислительной мощности для решения ряда задач. Сейчас постоянно появляются новые, достаточно мощные, но не обладающие безграничными возможностями компьютеры. В то же время у пользователей продолжают работать старые машины, которые в домашних условиях могут стать вспомогательными сетевыми компьютерами. При этом высвободятся ресурсы новой главной рабочей станции. Такая сеть имеет множество преимуществ: работа в Интернете одновременно с выполнением различных приложений, одновременное выполнение нескольких приложений, действенная защита рабочей станции от проникновения вирусов, отсутствие эффекта замедления работы

компьютера — это лишь небольшая часть возможностей, которые предоставит вам домашняя сеть. Домашняя сеть отличается от других сетей тем, что в нее с большой вероятностью могут входить компьютеры с различными операционными системами. Если на предприятии или в офисе стремятся к единообразию парка компьютеров с целью упрощения их обслуживания, то дома никто не запретит каждому использовать ту ОС, которая ему больше по душе. А возможно, кто-то из вашей семьи применяет не одну, а две или три операционные системы. Все большее распространение Linux, недавний выход Windows Vista позволяют предполагать, что в вашей сети будет несколько операционок. Во всяком случае, в моей домашней сети присутствуют компьютеры с четырьмя ОС, каждая из которых имеет свои особенности, которые следует учитывать при организации сети.

* * *

Рассмотренные варианты сетей имеют много отличий, но с точки зрения технологии их построения они весьма похожи. Сеть универсальна и ее качество во многом зависит от настроек сетевого программного обеспечения отдельных компьютеров и сетевого оборудования.

Предпосылки для организации сети

Для организации сети могут быть следующие предпосылки:

- наличие нескольких отдельных компьютеров, не имеющих возможности гибко обмениваться информацией между собой и с другими территориально удаленными компьютерами;
- необходимость создания общедоступной базы данных для накопления и хранения информации в требуемых объемах и с высокой оперативностью доступа;
- наличие программного и информационного обеспечения, которое не используется в полном объеме и не имеет общего стандарта хранения данных;
- необходимость повысить эффективность подключения к глобальной вычислительной сети (например, Интернет). Подключение отдельного компьютера к глобальной сети неэффективно, поскольку для других компьютеров приходится организовывать новые подключения (это, как вы понимаете, требует дополнительных расходов).

Самое рациональное решение любой из этих проблем — организация локальной сети, масштабы которой зависят от ваших конкретных задач. Сеть объединяет весь парк компьютеров (всех пользователей) в единое информационное пространство (ЕИП), обладающее следующими свойствами:

- доступность данных любому пользователю сети, которая позволяет решать многие задачи оперативно и с большей эффективностью, поскольку возможно контролировать ход работы, согласовывать и объединять ее результаты;
- достоверность и надежность хранения информации, достигаемая благодаря высокой помехо- и отказоустойчивости системы, которые, в свою очередь, обеспечиваются эффективным резервированием и организацией архивного хранения данных;
- упрощенный поиск необходимой информации с помощью объединенного архива;
- стандартизация документооборота в соответствии с общими требованиями;
- обеспечение доступа к информации авторизованному пользователю согласно его правам доступа и привилегиям.

Если вы думаете, что перечисленные предпосылки не имеют отношения к организации домашней сети, то вы очень ошибаетесь. Само собой разумеется, что имея дома более одного компьютера, вы захотите иметь возможность подключения к Интернету с каждого из них. Возможно, что вам еще не приходилось сталкиваться с необходимостью переустановки операционной системы на компьютере с огромным числом сохраненных вами файлов (документы, музыка, видео, дистрибутивы…). Наличие сети и возможность оперативно переместить файлы с компьютера на компьютер значительно облегчает такую задачу. Отказоустойчивость, защищенность данных также не помешают в домашних условиях. То есть даже самая простая сеть у вас дома должна строиться по тем же правилам, что и любая другая, но с учетом конкретных местных условий и требований.

С чего начать

Когда вы впервые подошли к персональному компьютеру и поняли, что уже не представляете без него дальнейшей жизни, вы, скорее всего, еще не задумывались о сетевых технологиях. Тем не менее вполне вероятно, что вы столкнулись с ними, осуществив подключение к Интернету. В большинстве

случаев Интернет не дает возможности доступа к отдельным компьютерам пользователей, и вот наступил момент, когда организация сети из ваших компьютеров стала насущной необходимостью. С чего начать? Где узнать? Вопросы появляются один за другим. А ответы? Несмотря на широкое распространение компьютерных технологий и упрощение доступа к разнообразной информации, не так просто найти конкретные рекомендации по созданию и настройке локальной сети да еще с минимальными затратами. Информация стала товаром, а товары редко раздают бесплатно. Теоретические сведения, помещенные в этой и последующих главах, не претендуют на полноту и абсолютную точность и приводятся здесь только для того, чтобы практические рекомендации и примеры были понятны и выполнимы. Организация больших сетей со сложной структурой не входит в круг рассматриваемых нами вопросов. Работа с *глобальными сетями*, которые объединяют удаленные на значительное расстояние (более 2 км) компьютеры, требует, конечно, специальной подготовки, большой практики работы с сетями более скромных масштабов и значительных материальных затрат. Наша задача — начать с малого, т. е. с организации *локальной вычислительной сети*, которая объединяла бы компьютеры, сосредоточенные на небольшой территории. Для этого необходимо, получив некоторый минимум теоретической и практической подготовки, организовать небольшую, но работоспособную сеть, которая будет приносить практическую пользу и моральное удовлетворение от сознания успешного преодоления очередного рубежа на пути освоения персонального компьютера. Затраты на материалы, оборудование и программное обеспечение постараемся минимизировать. За счет чего следует экономить? Будем ориентироваться на то, что имеем. Во-первых, в будущей сети можно полноценно использовать даже ваш, возможно, не очень новый и современный компьютер. Во-вторых, требуемое для организации сети программное обеспечение обойдется вам либо бесплатно, либо относительно недорого. Можно также использовать установленную на вашем компьютере операционную систему. В большинстве случаев мы будем ориентироваться на Windows, но и Linux вполне может работать в вашей сети. Итак, с чего начать построение сети?

При организации сети вы можете столкнуться не только с техническими трудностями. Например, если сеть должна расположиться на значительной площади, занимая несколько помещений или даже выходя за пределы одного здания. В этом случае придется согласовывать свои действия с владельцем помещения, если оно не ваше, или с местной администрацией, если кабель должен каким-то образом пересечь часть территории населенного пункта. Кроме неизбежных материальных проблем могут возникнуть проблемы пси-

хологического характера. Сеть — явление коллективное. Отдельно взятому, пусть и бесконечно увлеченному человеку, сеть не нужна. Друзья это или сотрудники, но они должны разделять ваше желание организовать сеть. Иначе вы не получите ни материальной, если в ней есть необходимость, ни моральной, ни какой бы то ни было другой поддержки. И даже, скорее, наоборот. Поэтому необходимо трезво оценить свои возможности, соотнести их со своими потребностями и четко представлять возможную выгоду (необязательно материальную). Если вы действительно заинтересованы в организации сети, то у вас все получится.

Дома, как это ни покажется вам странным, должны решаться те же проблемы. С членами семьи придется согласовать план организации сети, доказать им, что это не просто ваша прихоть, а полезное для всех мероприятие.

Компьютер 1 + компьютер 2

Два компьютера, соединенные между собой какой-либо линией связи, — это уже сеть. Такой линией связи может быть кабель, соединяющий параллельные или последовательные порты двух компьютеров, их сетевые карты (адаптеры) или модемы. Это может быть и телефонная линия, к которой компьютеры подключены посредством модемов.

На самом деле прямое кабельное соединение через параллельный или последовательный порты встречается довольно редко ввиду ограничений по скорости соединения и возможностей дальнейшего развития сети. Вариант связи по телефонной линии мы рассмотрим в *главе 4*. Пока предметом нашего разговора будет классическая сетевая технология типа Ethernet. Она позволяет быстро и эффективно объединять компьютеры различных типов в вычислительную сеть и дает возможность пользователям ощутить все преимущества ЛВС.

Основные сведения о ЛВС

Под локальной вычислительной сетью (ЛВС) понимают совместное подключение нескольких отдельных компьютеров (рабочих станций) к единому каналу передачи данных. Благодаря такому подключению различные пользователи, находясь на своих рабочих местах, могут одновременно применять программы, базы данных и оборудование. Ликвидируются ограничения, наложенные пространственным разделением рабочих мест.

В современной технической литературе для обозначения локальной сети часто используется английская аббревиатура LAN (Local Area Network — локальная сеть).

> ***ЗАМЕЧАНИЕ***
>
> Далее приводятся сведения, которые могут показаться не такими уж важными для практической организации сети. Но знания никогда не бывают лишними. Понимая теоретические основы устройства сетей в минимально необходимом объеме, вы сможете сориентироваться в сложных проблемах, возникающих в реальных практических ситуациях.

Многоуровневая модель сети

Для обеспечения единообразного представления данных при передаче информации по линиям связи была сформирована Международная организация по стандартизации (ISO — International Standards Organization). Эта организация разрабатывает модели международных коммуникационных протоколов, которые описывают международные стандарты систем передачи данных.

ISO предложила базовую модель взаимодействия открытых систем (OSI — Open Systems Interconnection). Эта модель стала международным стандартом проектирования систем передачи данных. Модель содержит семь уровней:

1. Физический — битовые протоколы передачи данных.
2. Канальный — формирование кадров, управление доступом к среде.
3. Сетевой — маршрутизация, управление потоками данных.
4. Транспортный — обеспечение взаимодействия удаленных процессов.
5. Сеансовый — поддержка диалога между удаленными процессами.
6. Представительный — интерпретация передаваемых данных.
7. Прикладной — пользовательское управление данными.

Основная идея этой модели заключается в том, что каждому уровню отводится конкретная роль. Благодаря этому общая задача передачи данных расчленяется на отдельные, легко обозримые задачи. Необходимые соглашения для связи одного из уровней с высшими и низшими уровнями называются *протоколами*.

Процесс взаимодействия пользователя с сетевой средой заключается в последовательном преобразовании передаваемых данных на передающей стороне от седьмого уровня до первого и в обратном преобразовании на приемной стороне.

- На первом, *физическом*, уровне определяются электрические, механические, функциональные и процедурные параметры для физической связи в системах. Физическая связь и неразрывная с ней эксплуатационная готовность являются основной функцией 1-го уровня. Стандарты физического уровня включают рекомендации V.24 МККТТ (CCITT), EIA RS232, X.21 и др. Все большее значение для передачи данных приобретает стандарт ISDN (Integrated Services Digital Network — цифровая сеть связи с комплексными услугами). В качестве среды передачи данных используют медный кабель (экранированная витая пара), коаксиальный кабель, оптоволоконный кабель и радиорелейную линию.
- *Канальный* уровень преобразует данные, полученные от 1-го уровня, в так называемые кадры и последовательности кадров. На этом уровне осуществляется: управление доступом к передающей среде, используемой несколькими ЭВМ, синхронизация, обнаружение и исправление ошибок.
- *Сетевой* уровень устанавливает в вычислительной сети связь между двумя абонентами. Соединение происходит благодаря функциям маршрутизации, которые требуют наличия сетевого адреса в пакете. К задачам сетевого уровня также относится обработка ошибок, мультиплексирование, управление потоками данных. Пример стандарта этого уровня — рекомендация X.25 МККТТ (для сетей общего пользования с коммутацией пакетов).
- *Транспортный* уровень поддерживает непрерывную передачу данных между двумя взаимодействующими друг с другом пользовательскими процессами. Надежность и непрерывность передачи данных возможна благодаря встроенной в протокол системе обнаружения и исправления ошибок, а также аппаратно-независимой реализации сервиса транспортировки.
- *Сеансовый* уровень обеспечивает управление диалогом, т. е. координирует прием, передачу и поддержку одного сеанса связи. Для координации необходим контроль рабочих параметров, управление потоками данных промежуточных накопителей и диалоговый контроль, гарантирующий передачу имеющихся в распоряжении данных. Кроме того, сеансовый уровень имеет дополнительные функции: управления паролями, подсчета оплаты за использование ресурсов сети, отмены и синхронизации связи в сеансе передачи после сбоя из-за ошибок в низших уровнях.

- *Представительный* уровень обеспечивает форму представления передаваемых по сети данных, а также их подготовку для пользовательского прикладного уровня. На этом уровне происходит преобразование данных из кадров, используемых для передачи данных, в экранный формат или формат для печатающих устройств оконечной системы.
- На *прикладном* уровне необходимо предоставить в распоряжение пользователей уже переработанную информацию. С этим может справиться системное и пользовательское прикладное программное обеспечение.

Проблемы преобразования данных при передаче

Для передачи по коммуникационным линиям информация преобразуется в цепочку следующих друг за другом битов (кодировка с помощью двоичной системы счисления, в которой используются только два знака "0" и "1").

Передаваемые алфавитно-цифровые знаки представляются в виде битовых комбинаций. Битовые комбинации располагаются в определенной кодовой таблице, содержащей 4-, 5-, 6-, 7- или 8-битовые коды.

Количество представленных знаков в коде зависит от количества используемых в нем битов. 4-битовый код позволяет передать максимум 16 значений, 5-битовый код — 32 значения, 6-битовый код — 64 значения, 7-битовый — 128 значений и 8-битовый код — 256 алфавитно-цифровых знаков.

Чем больше кодовая таблица, тем больше информации может быть передано за один такт передачи данных. В наше время достаточно широко применяются коды с разрядностью более 64 бит.

Среда передачи данных

В любой сети информация от одного компьютера до другого передается через некоторую среду передачи данных. Мы будем рассматривать, в основном, кабельные сети, но затронем и беспроводное соединение. В кабельных сетях информация в форме электрического сигнала передается по кабелю. На сегодняшний день для построения сетей применяются три вида кабеля:

- коаксиальный;
- витая пара;
- волоконно-оптический.

Последний вариант не освещен в данной книге вследствие его относительной дороговизны. Возможно, что, получив необходимый опыт работы с сетями, у вас появится желание усовершенствовать вашу сеть и перейти на волоконно-оптический кабель и соответствующее ему оборудование. Скорость передачи данных по такому кабелю многократно превышает скорости, с которыми нам придется иметь дело. Но пока (и, возможно, надолго) нас эти скорости устраивают, и мы будем говорить о применении первых двух видов кабелей. От качества и характеристик кабеля во многом зависит качество работы сети. Поэтому не лишним будет ознакомиться с применяемыми кабелями более подробно. Для передачи электрического сигнала требуется, как минимум, два проводника. По сути, и кабель представляет собой два проводника, но конструктивно они выполнены таким образом, что передаваемый по ним сигнал претерпевает меньше искажений, меньше затухает (теряет в мощности), может иметь более широкую полосу частот, чем сигнал, передаваемый по обычным проводам.

Коаксиальный кабель представляет собой гибкий, изолированный снаружи цилиндрический проводник, внутри которого строго по его оси расположен второй проводник, а пространство между проводниками заполнено диэлектриком (рис. 1.1).

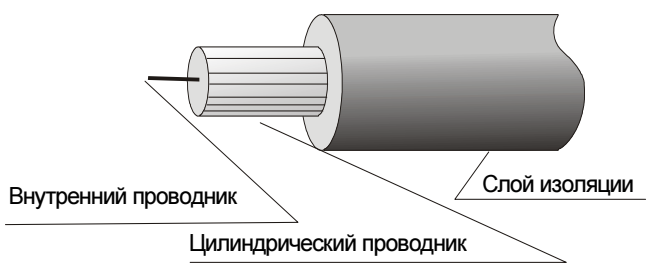


Рис. 1.1. Устройство коаксиального кабеля

Неэкранированная витая пара (рис. 1.2) или кабель UTP (Unshielded Twisted Pair — неэкранированная витая пара) представляет собой кабель, состоящий из двух или более пар скрученных между собой проводников, покрытых изоляцией и заключенных в общую защитную полимерную "рубашку". Каждый проводник в таком кабеле имеет свою уникальную расцветку и номер. Маркировка кабеля обычно содержит сведения о его категории "CATEGORY 5 UTP". Сведения о применении разных категорий кабеля приведены в табл. 1.1.

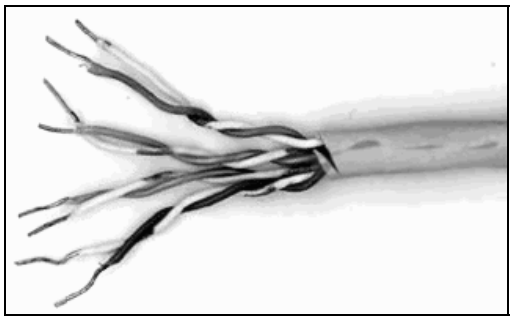


Рис. 1.2. Устройство кабеля типа "витая пара"

Таблица 1.1. *Применение различных категорий кабеля типа "витая пара"*

Категория	Область применения
1	Используется для телефонных коммуникаций и не подходит для передачи данных в компьютерных сетях
2	Используется для передачи данных со скоростью до 4 Мбит/с включительно
3	Используется для передачи данных со скоростью до 10 Мбит/с включительно. Применяется в старых сетях Ethernet
4	Используется для передачи данных со скоростью до 16 Мбит/с включительно. Применяется в сетях Token Ring
5	Используется для передачи данных со скоростью до 100 Мбит/с включительно. Применяется в современных сетях

Протоколы и стандарты

При передаче информации между одинаковыми вычислительными системами и разными типами компьютеров применяют различные коды. Для полной и безошибочной передачи данных необходимо придерживаться установленных правил. Все эти правила оговорены в *протоколе передачи данных*.

Протокол передачи данных описывает составляющие процесса передачи данных и его свойства.

- Синхронизация — механизм распознавания начала блока данных и его конца.

- Инициализация — установка соединения между взаимодействующими партнерами.
- Блокирование — разбиение передаваемой информации на блоки данных строго определенной максимальной длины (включая опознавательные знаки начала блока и его конца).
- Адресация — идентификация оборудования, которое во время взаимодействия обменивается информацией.
- Обнаружение ошибок — установка битов четности и вычисление контрольных битов.
- Нумерация блоков — присвоение каждому блоку идентификационного номера позволяет выявить ошибочно передаваемую или потерявшуюся информацию.
- Управление потоком данных — процесс распределения и синхронизации информационных потоков. Так, например, если в буфере устройства не хватает места или данные обрабатываются в периферийных устройствах (например, принтерах) недостаточно быстро, то это может привести к накапливанию сообщений и/или запросов.
- Методы восстановления процесса передачи данных после его прерывания, позволяющие вернуться к определенному положению для повторной передачи информации.
- Разрешение доступа — распределение, контроль и управление ограничениями доступа (например, "только передача" или "только прием").
- Сетевые устройства и средства коммуникаций. Под средством коммуникации понимается среда передачи.

Для обеспечения работы сети все ее оборудование должно работать по определенным стандартам и правилам. Они позволяют осуществить неискаженную передачу информации от одного компьютера к другому, а также добиться совместимости компьютеров, сетевых программ и оборудования разных производителей. Протоколов существует много, поскольку каждый описывает определенную сторону работы сети. Рассмотрим одну из важнейших групп протоколов, которую будем применять в нашей сети, — TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/Интернет-протокол). Задуманы эти протоколы для работы в сети Интернет, что отражено и в их названии, но они оказались полезны и для локальных сетей. Многие программы для работы в сетях используют IP-протокол.

TCP/IP-протоколы отвечают за передачу и прием проходящей по сети информации. Протокол TCP делит всю информацию, подлежащую передаче, на отдельные блоки — пакеты. Протокол IP эти пакеты нумерует и высылает по заранее определенному цифровому адресу в виде кадра информации — пакета, в который вложен пакет, созданный на основе TCP-протокола. На приемном конце процедура выполняется в обратном порядке. Пакеты принимаются, сортируются и собираются в исходном сочетании. Цифровой, а вернее IP-адрес, представляет собой четырехбайтовую последовательность чисел, записываемых обычно в десятичном виде, например, так: 192.168.55.3. Сети условно делятся на три класса. Каждому классу соответствует свой диапазон адресов (табл. 1.2).

Таблица 1.2. *Диапазоны адресов для классов сетей*

Класс сети	Маска подсети	Диапазон	Зарезервированные адреса
A	255.0.0.0	01.0.0.0—126.0.0.0	10.0.0.0127.0.0.0
B	255.255.0.0	128.0.0.0— 191.255.0.0	169.254.X.XC 172.16.0.0 по 172.31.0.0
C	255.255.255.0	192—222	C 192.168.0.0 по 192.168.255.0

Маска подсети указывает на биты, предназначенные для указания адреса сети, в остальных полях адреса должен располагаться адрес компьютера. Каждому классу сети соответствует свой диапазон применяемых и неприменяемых в Интернете (зарезервированных) адресов.

Структура адреса становится более понятной при представлении в двоичном коде. Например, маска 255.255.255.0 в двоичном коде выглядит так: 11111111.11111111.11111111.0. Все поля адреса сети заняты единицами. Ноль указывает на пустой адрес узла сети, поскольку в маске адреса узлов не отображаются. Адрес 198.168.55.1 в двоичном коде выглядит так: 11000110.10101000.110111.1. По таблице можно определить, что это адрес сети класса "C", а адрес компьютера (узла) выражен младшей единицей. Чем ниже класс сети, тем больше адресов сети может существовать и тем меньше компьютеров может находиться в такой сети. Каждый компьютер в сети имеет свой уникальный адрес, назначенный администратором сети или полученный автоматически. Именно с такими адресами и работает протокол IP.

Даже в самой сложной сети, допускающей передачу информации по наиболее короткому или наименее загруженному в настоящий момент пути, пакеты на приемном конце сортируются согласно последовательности их передачи, тогда как реальная последовательность приема может существенно отличаться от исходной. Тем не менее искажений информации не происходит (рис. 1.3).

Кроме TCP/IP-протоколов нам потребуется интерфейс NetBEUI (NetBIOS Enhanced User Interface — протокол расширенного пользовательского интерфейса сетевой базовой системы ввода/вывода). Такое название протокола мы увидим, настраивая компьютер для работы в сети. NetBEUI — это протокол, дополняющий спецификацию интерфейса NetBIOS (Network Basic Input/Output System — сетевая базовая система ввода/вывода), используемую сетевой операционной системой. NetBEUI формализует кадр транспортного уровня, не стандартизованный в NetBIOS. Данный интерфейс не соответствует какому-то конкретному уровню модели OSI. Он охватывает транспортный уровень, сетевой уровень и подуровень LLC (Logical Link Control — управление логическим соединением, верхний подуровень канального уровня). NetBEUI взаимодействует напрямую с NDIS (Network Driver Interface Specification — спецификация стандартного интерфейса сетевых адаптеров) подуровня MAC (Media Access Control — управление доступом к (передающей) среде, подуровень канального уровня, задающий методы доступа к среде, формат кадров, способ адресации). Таким образом, это немаршрутизируемый протокол. Этот протокол работает с обычными буквенно-цифровыми именами и отвечает за сеансы передачи данных между узлами сети, в нашем случае — между компьютерами. Он применяется только в локальных сетях, и упрощает работу с сетевыми адресами, позволяя использовать понятные имена компьютеров, которые могут быть связаны с именем пользователя или назначением компьютера в сети. Это существенно облегчает навигацию в сети, поиск необходимого адреса и связь с ним. В современных сетях протокол NetBEUI постепенно теряет свое значение. Все в большей мере протоколы TCP/IP справляются с передачей данных по сети, но в отдельных случаях, особенно применяя устаревшие операционные системы, без NetBEUI не обойтись.

Разные фирмы предлагали различные варианты структуры локальных сетей. Эти варианты отражены в различных стандартах, описывающих правила соединения компьютеров в сеть, типы сетевого оборудования, применяемые кабели, разъемы и прочие тонкости строения сети. Мы будем описывать преимущественно стандарт Ethernet, широко используемый в России и подходящий для работы с распространенными операционными системами и сетевым оборудованием.

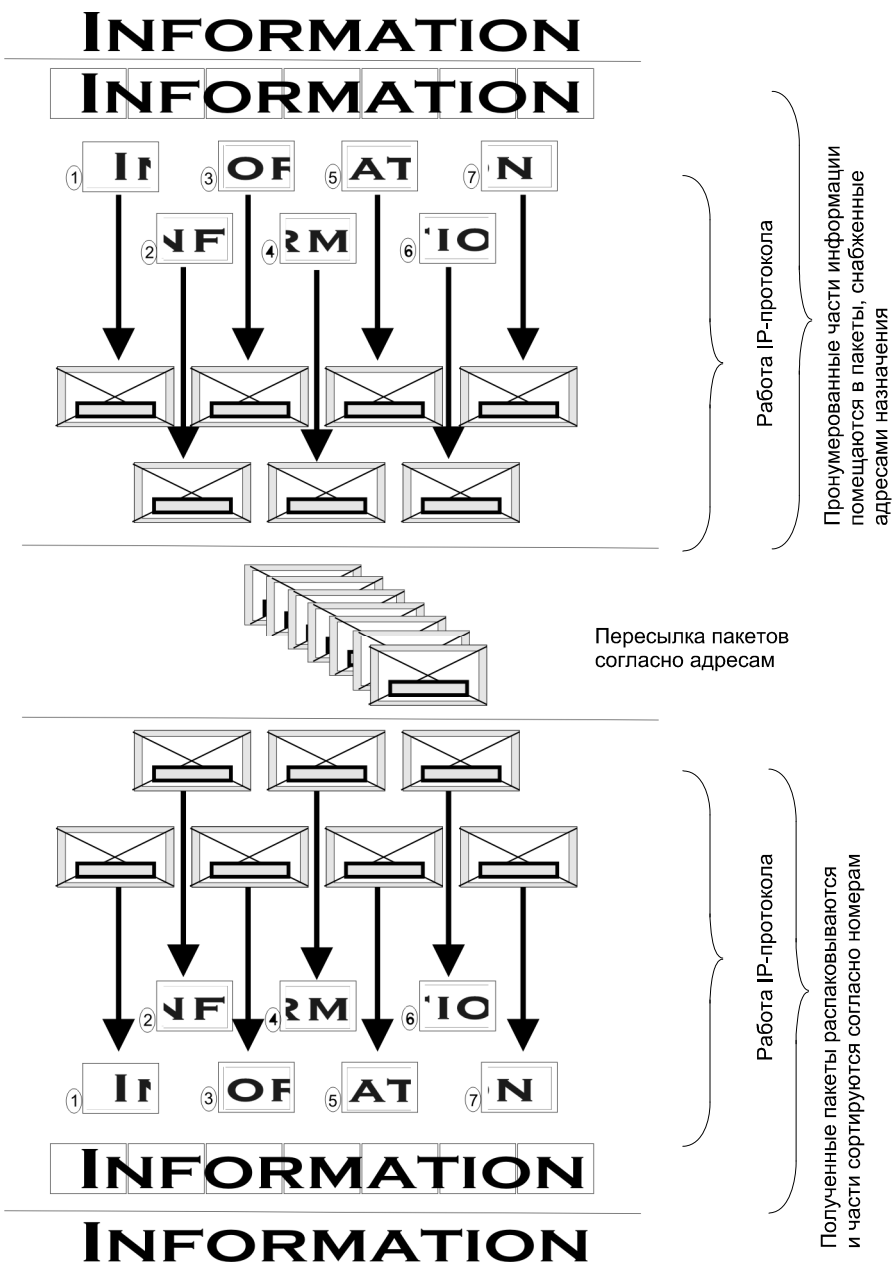


Рис. 1.3. Передача информации по IP-протоколу

После появления экспериментальной сети Ethernet Network фирмы Xerox в 1975 году этот стандарт неоднократно модернизировался, появилось несколько его модификаций. В настоящее время стандарт Ethernet применяется в миллионах сетей, в которых задействованы десятки миллионов компьютеров.

Применение стандарта Ethernet позволяет относительно простыми средствами добиться стабильной работы сети. Рассмотрим эти средства подробнее. Информация в компьютерных сетях обычно передается в двоичном коде — в том виде, в котором ее могут использовать компьютеры. Если несколько компьютеров одновременно передадут какие-то данные в сеть, то, несмотря на наличие адреса, ни один компьютер эту информацию принять не сможет. "Мешанина" из нулей и единиц не будет распознана как осмысленное сообщение с определенным адресом, и информация будет утеряна. Для того чтобы не терять информацию, включенные в сеть компьютеры должны "поделить" среду передачи данных между собой. Возможны различные способы раздела этой среды. По аналогии с радио, можно было бы передавать информацию в виде высокочастотного сигнала с частотной, фазовой или амплитудной модуляцией, разделив применяемый в сети частотный диапазон между компьютерами и используя в качестве адреса узла значение длины волны или частоты несущей этого сигнала. Недостаток такого метода разделения среды передачи данных очевиден. Чтобы в такой сети увидеть все подключенные компьютеры, требуется сканирование по всему частотному диапазону, а передача информации, предназначенной для нескольких или даже всех компьютеров сети, превращается в достаточно сложную задачу. Во всех сетях типа Ethernet применяется более простой метод разделения среды передачи данных — это метод CSMA/CD (Carrier Sense Multiply Access with Collision Detection — множественный доступ с контролем несущей и обнаружением конфликтов). Другими словами, этот метод можно назвать так: "Метод коллективного доступа с опознаванием несущей и обнаружением коллизий". Этот метод не требует деления частотного диапазона между компьютерами, что кроме упрощения всего процесса повышает быстродействие каналов связи.

Суть этого метода заключается в следующем: сформированный TCP/IP-пакет информации помещается в отдельный кадр данных, а компьютер ждет момента, когда в сети не будет несущей — физического носителя информации, представляющего собой электромагнитные колебания определенных частот. Компьютер ждет полной тишины. В наступившей тишине он передает свой кадр информации. Другие компьютеры обнаруживают факт передачи и анализируют наличие в передаваемом коде их адреса. Обнаружив свой адрес,

компьютер принимает информацию и посылает ответ об удачном завершении передачи кадра. Одновременная передача кадров двумя компьютерами приводит к ситуации, которая называется *коллизия*. Обнаружение коллизии — залог правильной передачи информации. Передающие компьютеры сравнили то, что отправляли, с тем, что оказалось в сети, и при следующем удобном случае опять пошлют этот кадр. И так до получения положительного ответа о приеме кадра. Таким образом, в каждый момент времени "говорить" позволено одному компьютеру. Остальные должны "слушать". Ясно, что к одному кабелю невозможно подключить бесконечно большое число компьютеров. Частоты, на которых передается информация в сетях Ethernet, довольно высоки. В нашем случае они достигают 16 МГц. Но существуют сети, в которых эти частоты доходят до сотен мегагерц. Несмотря на высокие частоты несущей, длительность самого кадра оказывается весьма заметной. Кроме того, после передачи или приема информации каждый компьютер должен выдержать паузу в 9,6 мкс, а после обнаружения коллизии длительность паузы определяется по случайному закону и может принимать значения, достигающие 52,4 мс. За единицу времени по сети может передаваться некоторое ограниченное количество информации. Кроме того, по технологии CSMA/CD сигнал о случившейся коллизии компьютер должен получить до окончания передачи своего кадра. Следовательно, длина кабеля в сети тоже ограничена. Как видим, на параметры сети по объективным причинам накладывается целый ряд ограничений. Определенные ограничения накладываются и на тип используемого кабеля и сетевого оборудования стандартом 10Base-T. Этот стандарт предполагает использование витой пары — кабеля, предназначавшегося ранее для передачи голоса. Применение качественного телефонного кабеля для передачи информации в компьютерных сетях оказалось чрезвычайно плодотворным. В стандарте определены также концентраторы, или хабы (hub). Эти устройства предназначены для подключения к одной точке кабеля нескольких компьютеров. Для надежной работы сети количество концентраторов между любыми двумя рабочими станциями не должно быть больше четырех (правило четырех хабов). В результате учета всех ограничений стандарт 10Base-T позволяет создать сеть со следующими параметрами:

- максимальное количество станций в сети — 1024;
- максимальное расстояние между двумя узлами сети (двумя точками подключения станций или концентраторов) — 500 м;
- максимальная длина сегмента — 100 м;
- максимальная пропускная способность сети — 10 Мбит/с.

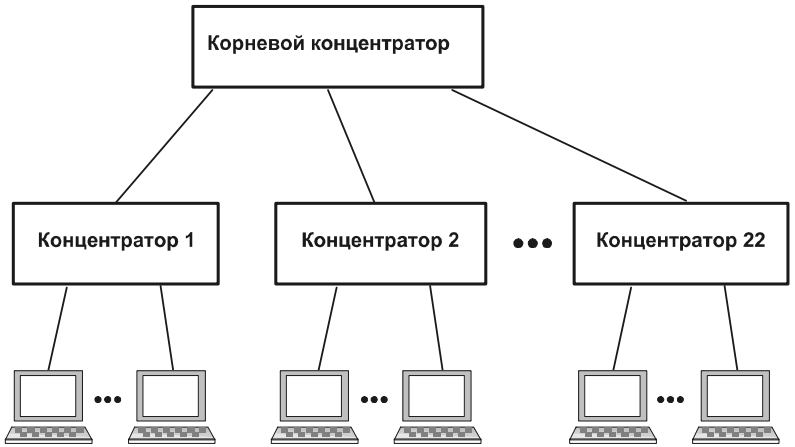


Рис. 1.4. Возможный вариант построения сети

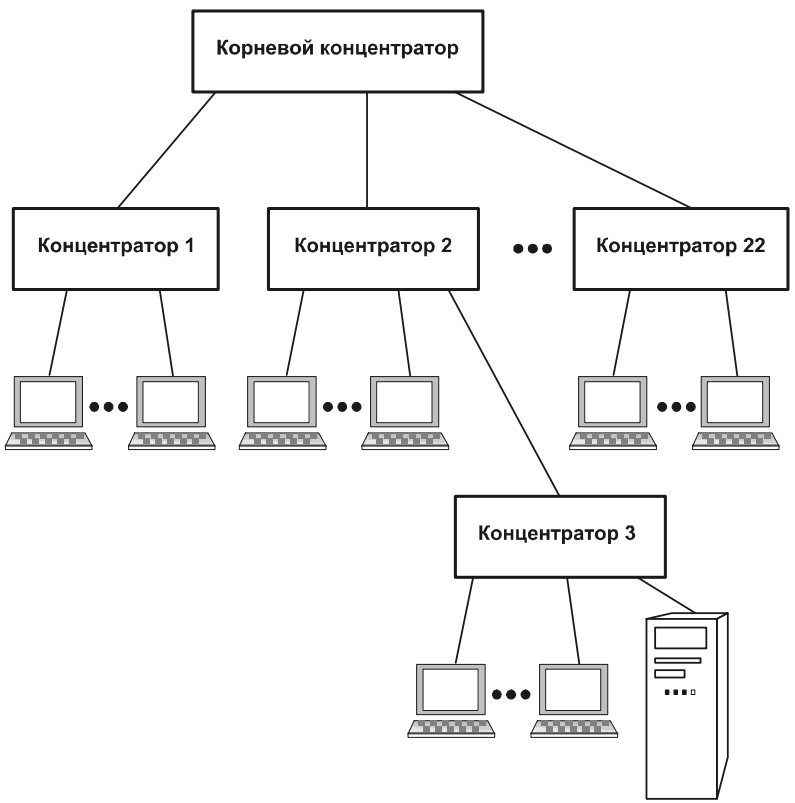


Рис. 1.5. Еще один вариант построения сети

Такими параметрами будет обладать сеть, схема которой приведена на рис. 1.4.

Конечно, реальная сеть может иметь схему, несколько отличающуюся от идеальной, но все известные ограничения должны быть соблюдены. От этого будет зависеть надежность работы сети. Не будет противоречить стандартам и вариант, схема которого изображена на рис. 1.5.

В то же время, вариант, показанный на рис. 1.6, уже не соответствует требованиям стандарта. В этом варианте между компьютерами, подключенными к концентраторам 3 и 4, оказалось более четырех концентраторов, что может привести к сбоям в работе сети ввиду нарушения правила четырех хабов.

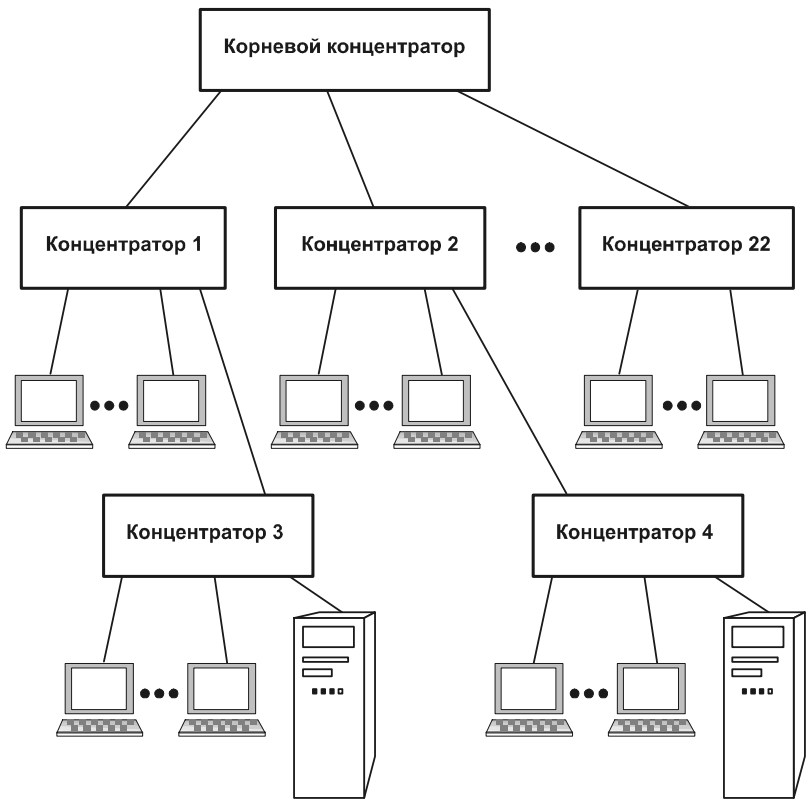


Рис. 1.6. Неправильный вариант построения сети

Параметры кабельных сетей семейства стандартов Ethernet приведены в табл. 1.3.

Таблица 1.3. *Параметры спецификаций физического уровня для стандарта Ethernet*

Характеристика	10Base-5	10Base-2	10Base-T	10Base-F
Кабель	Толстый коаксиальный кабель RG-8 или RG-11	Тонкий коаксиальный кабель RG-58	Неэкранированная витая пара категорий 3, 4, 5	Многомодовый волоконно-оптический кабель
Максимальная длина сегмента, м	500	185	100	2000
Максимальное расстояние между узлами сети (при использовании повторителей), м	2500	925	500	2500
Максимальное число станций в сегменте	100	30	1024	1024
Максимальное число повторителей между любыми станциями сети	4	4	4	4

Воспользовавшись приведенной таблицей, можно достаточно точно представить себе параметры проектируемой сети. Подробно разработанные протоколы и стандарты позволяют проектировать сети любой мыслимой конфигурации без серьезных проблем в расчетах.

Если, например, мы хотим организовать сеть, расположенную на нескольких этажах или даже в разных зданиях, то может быть оправданно применение коаксиального кабеля для соединения этажей или зданий. Коаксиальный кабель, обладая большей механической прочностью и устойчивостью к климатическому воздействию, будет служить дольше витой пары, а расстояние, которое коаксиальный кабель может перекрыть без дополнительных уст-

ройств, достигает пятисот метров (для толстого кабеля), что позволит соединить между собой удаленные друг от друга помещения.

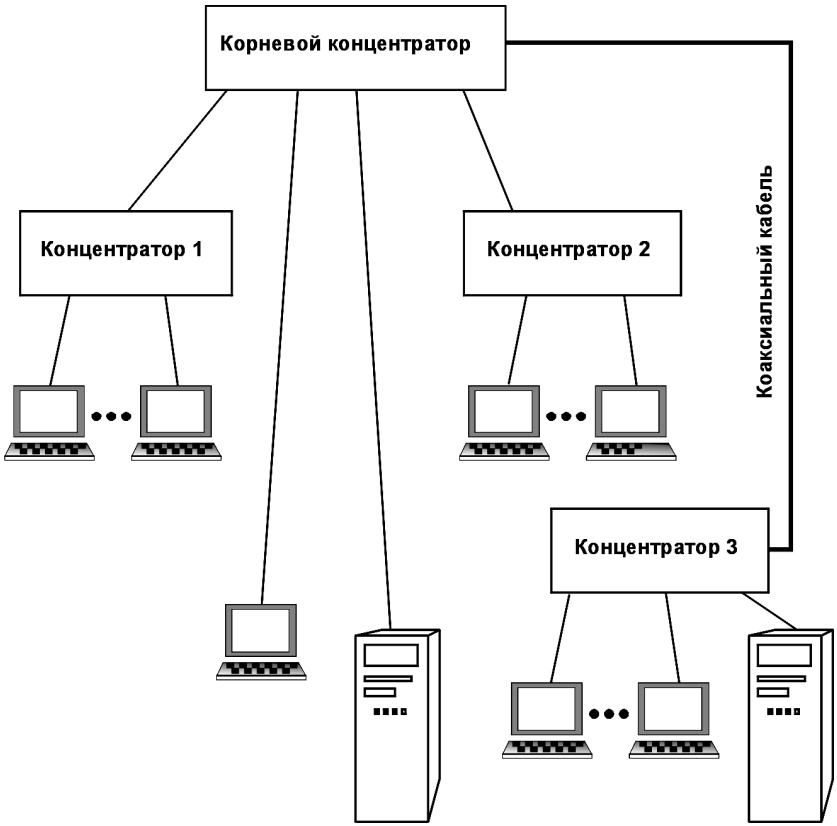


Рис. 1.7. Вариант построения сети с применением коаксиального кабеля (некоторые подробности опущены)

На рис. 1.7 показан вариант построения сети с применением коаксиального кабеля для соединения этажей или удаленных помещений. Другой вариант сети — простой, хотя и не самый надежный, — это сеть 10Base-2 (рис. 1.8). Она построена с применением тонкого коаксиального кабеля, подключаемого к сетевым адаптерам компьютеров.

Примечание

Следует отметить, что в настоящее время коаксиальный кабель в новых сетях практически не применяется. Если вам придется столкнуться с сетью

на коаксиальном кабеле, то это, вероятно, давно существующая сеть. Для объединения удаленных друг от друга участков сети применяют оптоволоконный кабель и соответствующее оборудование. Но самостоятельно проложить оптоволоконную сеть очень сложно. Требуется специальное оборудование и специальные знания.

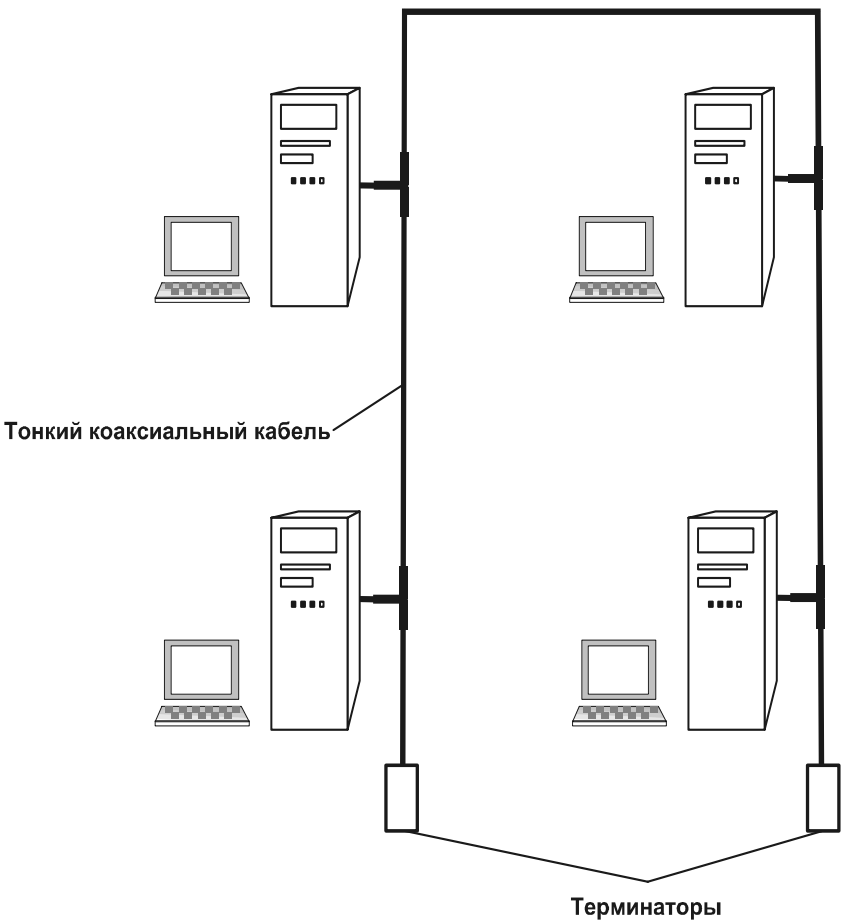


Рис. 1.8. Сеть 10Base-2

Существуют и другие протоколы и стандарты для построения сетей.

В 1980 году в IEEE (Institute of Electrical and Electronics Engineers — Институт инженеров по электротехнике и электронике) был организован комитет 802 по стандартизации локальных сетей. Результаты работы этого комитета легли в основу комплекса международных стандартов ISO 8802-1...5. Эти стан-

дарты были созданы на основе распространенных фирменных стандартов сетей Ethernet, ArcNet и Token Ring.

В соответствии с новыми стандартами могут быть спроектированы сети с пропускной способностью, достигающей 1 Гбайт/с. В последние годы в локальных сетях все чаще применяются так называемые активные коммутаторы. Они позволяют усложнить топологию сети, использовать резервные пути для информационного потока, чем достигается повышение надежности и быстродействия сети.

Несмотря на быстрое развитие новых технологий и появление новых стандартов, традиционные стандарты никто не отменяет, и они по-прежнему применяются настолько широко, что трудно ожидать их ухода со сцены, по крайней мере, в течение ближайших нескольких лет.

Работа в режиме "клиент-сервер"

Отдохнем немного от протоколов и стандартов. Объединенные в сеть компьютеры представляют собой организованную систему, где каждому компьютеру будет постоянно или временно отводиться определенная роль. Независимо от назначения сети и типов применяемых протоколов, два взаимодействующих в данный момент времени компьютера находятся в неравном положении. Один посылает некоторый запрос, другой должен определенным образом отреагировать на него. Проситель выступает в роли клиента, а просимый — в роли сервера. В ряде случаев компьютеры могут меняться ролями в процессе общения, но в каждый момент времени один клиент, другой сервер. В сети, как и в сфере услуг, клиент всегда прав. Сервер должен обеспечить клиента определенным сервисом — набором услуг. Файловый сервер должен обеспечить доступ к файлам в соответствии с правами клиента, сервер приложений должен обеспечить клиента необходимыми приложениями. В разных сетях сервер может выполнять самые разнообразные задачи. Это и почтовый сервер, и сервер базы данных, сервер доступа к глобальной сети Интернет, сервер печати, обеспечивающий доступ к принтерам сети. Словом, если требуется оказать услугу, то ее окажет клиенту сервер. В некоторых случаях сервер является как бы центром сети, а иногда, наоборот, один клиент собирает вокруг себя несколько серверов. Возможен вариант сети с выделенным сервером. Это значит, что один компьютер отводится исключительно для работы в качестве сервера. Это особенно действенно в больших сетях, где сервер работает с большой нагрузкой и требуется высокая стабильность его работы. Существуют операционные системы, спе-

циально предназначенные для сервера сети. Так, UNIX широко применяется для серверов в больших сетях, NetWare фирмы Novell — для сетей масштаба предприятия, Windows NT или Windows 2000 Server — для сетей различного назначения. В последние годы создано множество приложений, поддерживающих работу в режиме "клиент-сервер". Они позволяют нескольким пользователям обращаться к одним и тем же файлам без риска разрушить или испортить информацию. Распространенный во всем мире комплект MS Office как раз поддерживает работу в таком режиме, что может быть особенно полезно для программ Excel и Access, позволяющих работать с базами данных и создавать удобные специализированные приложения как для организаций, так и для личного пользования. Возможно применение нескольких операционных систем и нескольких серверов в одной сети. В этом случае возможно использовать особенности каждой операционной системы и более эффективно применять сеть, если круг решаемых задач широк и одна операционная система не предоставляет достаточно удобных средств для их решения. Необходимо отметить, что сами понятия сервера и клиента совсем не обязательно неразрывно связаны с сетью. Технология "клиент-сервер" может с успехом применяться и на локальном компьютере, который будет и клиентом, и сервером одновременно. В качестве клиента и сервера можно рассматривать части приложения, которое предназначено для работы в режиме "клиент-сервер". Подключение компьютера-сервера к сети ничем не отличается от подключения обычного компьютера. Применение виртуальных компьютеров позволяет на одной физической машине создавать *виртуальные* компьютеры-серверы и компьютеры-клиенты. О виртуальных технологиях пойдет речь в *главе 6*.

Сервер большой сети, используемой крупным предприятием или целой корпорацией (в такой сети сервер не один), работает круглосуточно, выполняя множество специфических серверных задач, без решения которых сеть такого масштаба не сможет нормально функционировать. У нас масштабы помельче, задачи попроще. Нет необходимости держать компьютеры включенными круглые сутки. Все наши потребности в плане сетевого сервиса вполне могут удовлетворить распространенные Windows 95/98 и Windows XP или Windows Vista. Windows 95/98 не предназначены для непрерывной работы в течение нескольких дней. Если такая необходимость появится, следует позаботиться о выделении нескольких минут в сутки для перезагрузки компьютера. Эта мера позволит существенно снизить риск зависания системы и потери данных. Windows 2000 и более новые ОС менее подвержены различного рода сбоям. Следовательно, на сервере она должна работать более устойчиво. Выделенный сервер обычно размещается в отдельном помещении.

Типовые топологии ЛВС

При построении сети сначала необходимо выбрать способ организации физических связей, т. е. *топологию*. Под топологией понимается конфигурация графа, вершинами (или узлами) которого являются компьютеры сети или другое сетевое оборудование (например, концентраторы), а ребрами — физические связи между ними.

Шинная топология

При шинной топологии среда передачи информации представляется в форме коммуникационного пути, доступного для всех рабочих станций. К нему должны быть подключены все рабочие станции. Любая рабочая станция может непосредственно вступать в контакт с любой другой рабочей станцией, имеющейся в сети.

Рабочая станция может быть подключена к сети или отключена от нее в любое время, причем работа всей вычислительной сети не будет прервана. Функционирование вычислительной сети не зависит от состояния отдельной рабочей станции.

В стандартной ситуации для шинной сети Ethernet часто используют тонкий кабель или Cheapernet-кабель с тройниковым соединителем. Отключение от такой сети и особенно подключение к ней требует разрыва шины, что вызывает нарушение циркулирующего потока информации и зависание системы. Этого можно избежать с помощью пассивных штепсельных коробок, через которые можно отключать и/или подключать рабочие станции во время работы вычислительной сети.

Благодаря тому, что рабочие станции можно включать без прерывания сетевых процессов и коммуникационной среды, очень легко прослушивать информацию, т. е. ответвлять ее из коммуникационной среды. В ЛВС с прямой (немодулируемой) передачей информации всегда существует только одна передающая станция. Для предотвращения коллизий (столкновений данных) в большинстве случаев применяется временной метод разделения, при котором для каждой подключенной рабочей станции в определенные моменты времени предоставляется исключительное право на использование канала передачи данных. Поэтому требования к пропускной способности вычислительной сети при повышенной нагрузке (например, при вводе новых рабочих станций) снижаются.

Рабочие станции присоединяются к шине посредством устройств TAP (Terminal Access Point — точка подключения терминала). TAP представляет собой специальный тип подсоединения к коаксиальному кабелю. Зонд игольчатой формы внедряется через наружную оболочку внешнего проводника и слой диэлектрика к внутреннему проводнику и присоединяется к нему. TAP имеет "народное" название — "зуб вампира". В ЛВС с модулированной широкополосной передачей информации различные рабочие станции получают, по мере надобности, частоту, на которой они могут отправлять и получать информацию. Для модуляции данных на соответствующих несущих частотах между средой передачи информации и рабочими станциями находятся модемы. Техника широкополосных сообщений позволяет одновременно транспортировать в коммуникационной среде довольно большой объем информации. Для дальнейшей дискретной транспортировки данных не имеет значения, какая информация была подана в модем (аналоговая или цифровая), так как в дальнейшем она все равно будет преобразована.

Топология типа "звезда"

Концепция топологии сети типа "звезда" пришла из области больших ЭВМ. В ней головной компьютер является активным узлом обработки данных. Он получает и обрабатывает всю информацию с периферийных устройств. Такой принцип применяется в системах передачи данных, например, в электронной почте RELCOM.

> ***Примечание***
>
> Эта сеть и компания упоминаются здесь как первопроходцы Интернета в России. Теперь, конечно, электронная почта и Интернет никого не удивляют, а поставщиков подобных услуг десятки, если не сотни.

Вся информация между двумя периферийными рабочими станциями проходит через центральный узел вычислительной сети. Пропускная способность сети зависит от вычислительной мощности узла и гарантируется для каждой рабочей станции. Коллизий не возникает. Кабельное соединение довольно простое, так как каждая рабочая станция связана с узлом. Затраты на прокладку кабелей высокие, особенно когда центральный узел территориально расположен не в центре топологии. При расширении вычислительных сетей нельзя использовать ранее проложенные кабельные связи, к новому рабочему месту приходится прокладывать отдельный кабель из центра сети.

Топология типа "звезда" является наиболее быстродействующей из всех топологий вычислительных сетей, поскольку передача данных между рабочими станциями проходит через центральный узел, причем для каждой станции выделена отдельная линия. Данная топология сети характеризуется сравнительно невысокой частотой запросов на передачу информации от одной станции к другой.

Производительность вычислительной сети с топологией типа "звезда" определяется мощностью ее центрального узла, который выполняет функции сервера. Он может быть узким местом вычислительной сети. В случае выхода из строя центрального узла нарушается работа всей сети.

Преимуществом такой топологии сети является возможность реализовать оптимальный механизм защиты информации, хранящейся на сервере, от несанкционированного доступа. Вся вычислительная сеть может управляться из ее центра.

Кольцевая топология

При кольцевой топологии сети рабочие станции связаны одна с другой по кругу, т. е. рабочая станция 1 с рабочей станцией 2, рабочая станция 2 с рабочей станцией 3 и т. д. Последняя рабочая станция связана с первой. Коммуникационная связь замыкается в кольцо.

Прокладка кабелей от одной рабочей станции до другой может быть довольно сложной и дорогостоящей, особенно если территориально рабочие станции не расположены по кольцу (например, в линию).

Сообщения регулярно циркулируют по кругу. Рабочая станция посылает по определенному конечному адресу информацию, предварительно получив из кольца запрос. Такая пересылка эффективна, так как большинство сообщений можно отправлять по кабельной системе одно за другим. Очень просто можно организовать кольцевой запрос на все станции. Продолжительность передачи информации увеличивается прямо пропорционально количеству рабочих станций, входящих в вычислительную сеть.

Основной недостаток кольцевой топологии заключается в том, что в случае выхода из строя хотя бы одной рабочей станции вся сеть парализуется, поскольку каждая станция активно участвует в передачи информации. Неисправности в кабельных соединениях локализуются легко.

Подключение новой рабочей станции требует краткосрочного выключения сети, так как во время установки кольцо должно быть разомкнуто. Ограниче-

ния на протяженность вычислительной сети не существует, поскольку определяющим является расстояние между двумя рабочими станциями.

Специальной формой кольцевой топологии является логическая кольцевая сеть. Физически она монтируется как соединение звездных топологий. Отдельные звезды включаются с помощью специальных коммутаторов, иногда называемых *хабами* или *концентраторами*.

Коммутатор, обладающий одновременно и функциями усилителя, называют *активным концентратором*. На практике активный концентратор обеспечивает подключение от 8 до 32 линий, в зависимости от его разновидности.

Коммутатор, к которому можно присоединить максимум три станции, называют *пассивным концентратором.* Пассивный концентратор обычно используется как разветвитель. Он не нуждается в дополнительном усилителе. Пассивный концентратор подключают в том случае, если расстояние от него до рабочей станции не превышает нескольких десятков метров.

Управление отдельной рабочей станцией в логической кольцевой сети происходит так же, как и в обычной кольцевой сети. Каждой рабочей станции присваивается адрес, на который передается управление (от старшего к младшему и от самого младшего к самому старшему). Разрыв соединения происходит только для ближайшего низшего узла вычислительной сети, так что работа всей сети может нарушаться лишь в редких случаях.

Смешанные топологии

Наряду с известными топологиями вычислительных сетей "кольцо", "звезда" и "шина", на практике применяется и комбинированная структура, например, древовидная. Она представляет собой комбинацию вышеназванных топологий. Основание дерева вычислительной сети (корень) располагается в точке, в которой собираются коммуникационные линии (ветви дерева).

Вычислительные сети с древовидной структурой используются там, где невозможно непосредственное применение базовых сетевых структур в чистом виде. Для подключения большого числа рабочих станций требуются сетевые усилители и/или коммутаторы.

Локальная сеть Ethernet

Спецификацию Ethernet в конце семидесятых годов прошлого века предложила компания Xerox Corporation. Позднее к этому проекту присоединились

компании Digital Equipment Corporation (DEC) и Intel Corporation. В 1982 году была опубликована спецификация на Ethernet версии 2.0. На базе Ethernet институтом IEEE был разработан стандарт IEEE 802.3. Различия между ними незначительные.

Основные принципы работы этой сети таковы:

- на логическом уровне в Ethernet применяется топология "шина";
- все устройства, подключенные к сети, равноправны, т. е. любая станция может начать передачу в любой момент времени (если передающая среда свободна);
- данные, передаваемые одной станцией, доступны всем станциям сети.

Локальная сеть Token Ring

Этот стандарт разработан фирмой IBM. В качестве передающей среды применяется неэкранированная или экранированная витая пара (UPT или SPT) или оптоволокно. Скорость передачи данных 4 или 16 Мбит/с. Для управления доступом станций к передающей среде используется метод *"маркерное кольцо"* (Token Ring).

Основные положения этого метода:

- устройства подключаются к сети по топологии "кольцо";
- все устройства, подключенные к сети, могут передавать данные, только получив разрешение на передачу *(маркер)*;
- в любой момент времени только одна станция в сети обладает таким правом.

Типы пакетов

В IBM Token Ring используются три основных типа пакетов:

- пакет *управление/данные* (Data/Command Frame — данные/командный кадр), с его помощью выполняется передача данных или команд управления работой сети;
- *маркер* (Token — маркер), станция может начать передачу данных только после его получения, причем в одном кольце может быть только один маркер и, соответственно, только одна станция с правом передачи;
- *пакет сброса* (Abort — прекращение), его посылка вызывает прекращение любых передач.

Локальная сеть ARCnet

ARCnet (Attached Resource Computer Network — вычислительная сеть с присоединенными ресурсами) — простая, недорогая, надежная и достаточно гибкая архитектура локальной сети. Она была разработана корпорацией Datapoint в 1977 году. Впоследствии лицензию на ARCnet приобрела корпорация SMC (Standard Microsistem Corporation), основной разработчик и производитель оборудования для сетей. В качестве передающей среды используется витая пара, коаксиальный кабель (RG-62) с волновым сопротивлением 93 Ом и оптоволоконный кабель. Скорость передачи данных — 2,5 Мбит/с. При подключении устройств в ARCnet применяют топологии "шина" и "звезда".

Передача каждого байта в ARCnet выполняется специальной посылкой ISU (Information Symbol Unit — единица передачи информации), состоящей из трех служебных старт/стоповых битов и восьми битов данных. В начале каждого пакета передается начальный разделитель AB (Alert Burst — предупреждение о пакете), который состоит из шести служебных битов. Начальный разделитель выполняет функции преамбулы пакета.

В ARCnet существует 5 типов пакетов:

- пакет ITT (Information To Transmit — информация для передачи) передает управление от одного узла сети к другому. Станция, принявшая этот пакет, получает право на передачу данных;
- пакет FBE (Free Buffer Enquiries — свободный буфер запросов) проверяет готовность узла к приему данных;
- пакет данных производит передачу данных;
- пакет ACK (Acknowledgment — уведомление) подтверждает готовность к приему данных или прием пакета данных без ошибок. Он высылается в ответ на FBE и пакет данных;
- пакет NAK (Negative Acknowledgments — отрицательное уведомление) определяет неготовность узла к приему данных (ответ на FBE) или прием данных с ошибкой.

Доступ станций к передающей среде управляется с помощью метода *"маркерная шина*" (Token Bus). Основные принципы этого метода:

- все устройства, подключенные к сети, могут передавать данные, только получив разрешение на передачу (маркер);
- в любой момент времени только одна станция в сети обладает таким правом;
- данные, передаваемые одной станцией, доступны всем станциям сети.

Выбор оптимальной среды передачи данных

В качестве среды передачи наиболее часто используется витая пара, коаксиальный кабель или оптоволоконные линии. При выборе типа кабеля учитывают следующие показатели:

- стоимость монтажа и обслуживания;
- скорость передачи информации;
- ограничения на величину расстояния передачи информации (без дополнительных усилителей-повторителей);
- безопасность передачи данных.

Главная проблема заключается в одновременном обеспечении этих показателей. Например, чем больше расстояние передачи данных, тем меньше скорость и тем сложнее обеспечить должную защиту информации. Простота наращивания и расширения кабельной системы влияют на ее стоимость.

Витая пара является наиболее дешевым кабельным соединением. Она позволяет передавать информацию со скоростью до 100 Мбит/с, легко наращивается, однако имеет недостаточную помехозащищенность в условиях высокого уровня помех на линии связи. Преимуществом является низкая цена и отсутствие проблем при монтаже. Для повышения помехозащищенности информации часто используют экранированную витую пару, т. е. витую пару, помещенную в экранирующую оболочку, подобно экрану коаксиального кабеля. Это увеличивает стоимость витой пары и приближает ее по цене к коаксиальному кабелю.

Коаксиальный кабель обладает высокой помехозащищенностью и применяется для связи на большие расстояния (несколько километров). Скорость передачи информации — от 1 до 500 Мбит/с, в зависимости от типа кабеля и условий эксплуатации. Существует стандартная классификация коаксиального кабеля по его диаметру на "толстый" и "тонкий" коаксиальный кабель.

Оптоволоконные линии — наиболее дорогое соединение. Скорость распространения информации по ним достигает нескольких гигабайт в секунду. Допустимое удаление — более 50 км. Внешнее воздействие помех практически отсутствует. Применяются там, где возникают помехи в виде электромагнитных полей или требуется передача информации на очень большие расстояния без использования повторителей.

На базе различных стандартов могут быть организованы сети разной структуры с различными методами передачи информации.

На сегодняшний день физические спецификации технологии Ethernet включают следующие среды передачи данных:

- 10Base-5 — коаксиальный кабель диаметром 0,5 дюйма, называемый "толстым" коаксиалом. Имеет волновое сопротивление 50 Ом. Максимальная длина сегмента — 500 м (без повторителей);
- 10Base-2 — коаксиальный кабель диаметром 0,25 дюйма, называемый "тонким" коаксиалом. Имеет волновое сопротивление 50 Ом. Максимальная длина сегмента — 185 м (без повторителей);
- 10Base-T — кабель на основе неэкранированной витой пары (Unshielded Twisted Pair, UTP). Образует звездообразную топологию на основе хаба (концентратора). Расстояние между хабом и конечным узлом — не более 100 м;
- 10Base-F — волоконно-оптический кабель. Топология аналогична топологии стандарта 10Base-T. Имеется несколько вариантов этой спецификации — FOIRL (расстояние до 1000 м), 10Base-FL (расстояние до 2000 м), 10Base-FB (расстояние до 2000 м).

Выбор топологии локальной сети

Мы уже много говорили о топологии сетей вообще, пришло время подумать и о нашей сети. Топология — раздел математики, изучающий свойства фигур, не изменяющихся при любых перемещениях и деформациях. Этот термин также может означать "топологическое пространство" — множество элементов любой природы, в котором определены предельные соотношения. Таким образом, топология сети — это множество ее элементов, в котором определены предельные соотношения. И в самом деле, ЛВС строится на основе некоторых предельных соотношений, полученных расчетным путем, исходя из свойств электрических сигналов, используемых в сети, и параметров среды распространения этих сигналов (обычно это кабель). Несмотря на то, что в нашей сети может быть совсем не много компьютеров, определенные для ЛВС предельные соотношения не позволяют строить сеть так, как нам заблагорассудится. Для каждой из типовых топологий существует ряд ограничений.

- "Шина" (bus) — компьютеры подключены вдоль одного кабеля (сегмента) (рис. 1.9). Количество компьютеров, которое можно подключить к сег-

менту сети (на рисунке показан именно сегмент сети), ограничено. Оно не может превышать 30 единиц, а длина сегмента не должна превышать 185 м. Применяя репитеры (повторители), позволяющие соединять сегменты сети, можно увеличить протяженность сети до 925 м. Количество сегментов при этом не должно быть больше 5, количество репитеров между любыми двумя компьютерами не больше 4, а сами компьютеры могут находиться только в 3 из 5 сегментов. Коротко это правило записывается как 5-4-3. В качестве среды передачи данных в такой сети используется тонкий коаксиальный кабель.

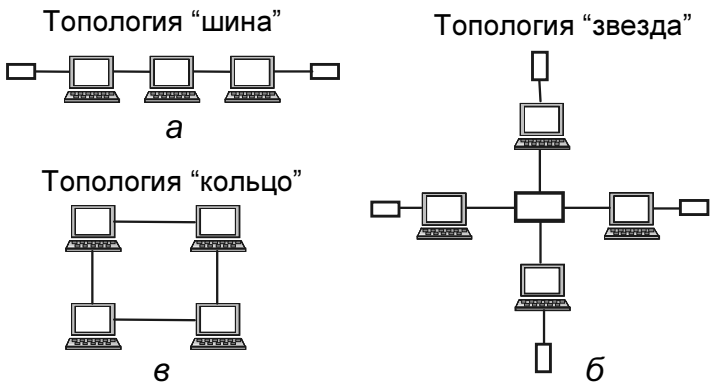


Рис. 1.9. Варианты топологии сети

- "Звезда" (star) — компьютеры подключены к сегментам кабеля, исходящим из одной точки, или хаба (концентратора) (рис. 1.9, *б*). Для этой топологии также действуют ограничения, которые будут рассмотрены несколько позже. На практике такая конфигурация редко применяется в чистом виде. Чаще сеть имеет комбинированную топологию.
- "Кольцо" (ring) — компьютеры подключены к кабелю, замкнутому в кольцо (рис. 1.9, *в*). Топология "кольцо" не применяется в сетях Ethernet.

Каждый вариант имеет свои преимущества и недостатки. Комбинируя, можно компенсировать недостатки одной схемы преимуществами другой. Хотя при этом возможно как усиление преимуществ, так и усугубление недостатков. Мы будем говорить только о первых двух вариантах топологии сети, но и этого нам вполне достаточно для реализации наших планов.

Характеристики локальных сетей различных топологий приведены в табл. 1.4.

Таблица 1.4. *Характеристики сетей*

Характеристики	Топология		
	"звезда"	**"кольцо"**	**"шина"**
Стоимость расширения	Незначительная	Средняя	Средняя
Присоединение абонентов	Пассивное	Активное	Пассивное
Защита от отказов	Незначительная	Незначительная	Высокая
Размеры системы	Любые	Любые	Ограничены
Защищенность от прослушивания	Хорошая	Хорошая	Незначительная
Стоимость подключения	Незначительная	Незначительная	Высокая
Поведение системы при высоких нагрузках	Хорошее	Удовлетворительное	Плохое
Возможность работы в реальном времени	Очень хорошая	Хорошая	Плохая
Разводка кабеля	Хорошая	Удовлетворительная	Хорошая
Обслуживание	Очень хорошее	Среднее	Среднее

Сеть без кабеля

В периодических изданиях, посвященных компьютерной технике, можно встретить рекламу и описание устройств для организации беспроводной сети. Развитие технологий беспроводных сетей идет тем же путем, что и развитие технологий проводных сетей.

Сначала беспроводные сети были дорогими и малоизвестными. Маленькие компании и домашние пользователи не могли о них даже мечтать. Теперь

появились образцы оборудования, которое позволяет организовать беспроводную связь между компьютерами дома или в небольшой организации.

Сегодня беспроводные сети (WLAN — Wireless Local Area Network, беспроводная локальная сеть) выстраиваются по протоколу 802.11b, также известному как Wi-Fi (Wireless Fidelity — беспроводная надежность). Этот стандарт является самым популярным, так как он имеет максимальную пропускную способность 11 Мбит/с, и цены на необходимое для такой сети оборудование приемлемые. Хотя существуют и другие стандарты беспроводных сетей. Компания Metricom, например, запустила Ricochet — сеть беспроводного доступа в Интернет — в различных городах США. Однако эта компания обанкротилась в 2001 году. В сети Ricochet использовались беспроводные модемы, работающие в диапазоне 900 МГц. С модемами было все в порядке, кроме того, что максимальное расстояние передачи данных было небольшим. Чтобы решить эту проблему, Metricom установила множество повторителей, которые создали достаточно большую зону покрытия. Компания приказала долго жить, маршрутизаторы остановились, но модемы могут работать автономно, без сети, для которой они предназначались.

Рис. 1.10. Модемы Ricochet "GS"

На рисунке показана пара модемов Ricochet "GS". Они работают на скорости 128 Кбит/с. Модемы предыдущих серий имеют меньшую скорость. Скорость, конечно, выше, чем при обычной модемной связи по телефонной линии, но существенно уступает скорости передачи данных в кабельной сети.

Два модема Ricochet могут соединяться друг с другом в режиме "точка-точка" и работать как любые другие модемы. Для такого соединения вам нужно ввести номер набора, указанный на наклейке, приклеенной к низу другого модема. Он будет примерно таким: 03-1234-5678, при этом черточки тоже имеют значение. Если другой модем настроен на автоматический ответ, вам остается только сказать компьютеру "ПОЗВОНИ", точно так же, как и при работе с обычным модемом. После этого установится обычное, только более быстрое, соединение. Сколько-нибудь заметной задержки при установке связи между модемами Ricochet нет. При использовании USB (USB, Universal Serial Bus — универсальная последовательная шина) или последовательного порта, что бы вы ни делали, скорость не будет выше 115 200 бит/с — а это нереально быстро для модемов, использующих телефонную линию, но ужасно медленно по сравнению со скоростью в любой сети Ethernet или 802.11b. Если мы вычтем из этого показателя служебные данные, то увидим, что пользователь может передать 10 Кбайт информации в секунду или чуть больше.

Гибкая 10-сантиметровая антенна обеспечивает соединение на расстояние до полутора километров при условии прямой видимости. Поскольку применяется диапазон 900 МГц, то это расстояние заметно уменьшается при прохождении сигнала через что-то более плотное, чем воздух. На практике радиус действия оказывается меньшим, он сильно зависит от местности и положения антенны. Разумеется, техника развивается, и теперь вы можете встретить большой выбор оборудования для организации беспроводного доступа к сети.

Сетевые USB-адаптеры Bluetooth

Стандарт Bluetooth не предназначен для беспроводных локальных сетей (WLAN), хотя такая возможность организации сети все же есть. Bluetooth был разработан для подключения к компьютеру периферийных устройств, а не для соединения компьютеров в режиме "точка-точка".

Стандарт Bluetooth использует тот же радиодиапазон (2,4 ГГц), что и в беспроводных сетях, построенных по стандарту IEEE 802.11b. В такой сети пропускная способность гораздо меньше, и не предусмотрена возможность работы на большом расстоянии. Соединение будет работать через стену или две, несмотря на слабые передатчики, которые обычно используются в оборудовании этого стандарта. Технология Bluetooth предназначена для объединения устройств, расположенных достаточно близко друг от друга, чтобы можно

было соединить их кабелем. Она предоставляет дополнительную возможность их беспроводного подключения.

Некоторые материнские платы, различные ноутбуки и компьютеры известных производителей уже имеют встроенные Bluetooth-адаптеры. Существует большое количество устройств и программного обеспечения с поддержкой этого стандарта (рис. 1.11).

Рис. 1.11. Bluetooth-адаптер Billionton USBBT02-X

Этот адаптер относится к третьему классу. Его максимальное расстояние работы всего десять метров (без препятствий). Этого достаточно для выполнения большинства задач, на которые рассчитан стандарт Bluetooth, но если вам необходимо покрыть большее расстояние, то потребуется адаптер первого класса. В этом случае радиус работы увеличится до 100 метров.

Если ваше Bluetooth-устройство не будет использовать специальную программу, то вам придется работать по FTP-протоколу. Одна папка на каждом из устройств, участвующих в Bluetooth-соединении, предоставляется для другого пользователя. Вы получаете к ней доступ так же, как и к любому другому FTP-серверу — для этого необходимо знать имя пользователя и пароль для другого устройства.

Полезная скорость передачи через FTP между адаптерами Billionton от 40 до 50 Кбайт/с при небольшом расстоянии и малом уровне помех в диапазоне 2,4 ГГц.

Стандарт 802.11b

Довольно распространен стандарт 802.11b. Различные 802.11b-устройства достаточно хорошо работают друг с другом. Оборудование этого стандарта выпускается в широком ассортименте малоизвестными фирмами и стоит от-

носительно недорого. Если применять стандарт 802.11b дома или в небольшом офисе, то могут возникнуть три проблемы.

Проблема первая — рабочий диапазон 2,4 ГГц, может быть занят излучением другого распространенного оборудования. Микроволновые печи, например, тоже используют 2,4 ГГц. Сигналы 2,4 ГГц плохо проходят через преграды, такие как дерево или тело человека. Многие материалы представляют существенные преграды для такого излучения.

Проблема вторая — сети 802.11b трудно обезопасить. Сетевой протокол (как и Ethernet) изначально не подразумевает безопасность. Если не использовать высокоуровневые решения, то сеть оказывается незащищенной.

Безопасность большинства сетей Ethernet и почти всех домашних сетей и сетей малых офисов практически нулевая. Любой подключившийся к сети может получить доступ ко всем ее ресурсам, доступ в Интернет через общее подключение и многое другое. Хотя для того чтобы подключиться, необходимо с компьютером находиться где-то поблизости.

Беспроводные сети позволяют подключаться злоумышленнику, находящемуся на возвышении даже на расстоянии мили, с тем же успехом, что и в здании при условии использования небольшой направленной антенны. Поместите точку доступа в сеть, защищенную брандмауэром, и для злоумышленника ваша сеть окажется практически открытой.

Проблема третья — невысокая скорость передачи данных в сетях 802.11b. Теоретическая пиковая пропускная способность 802.11b составляет 11 Мбит/с. Ее вы получите только при сильном сигнале, а минимальная скорость — всего 1 Мбит/с. Такая пропускная способность возможна только в том случае, если в каждый момент времени только одно устройство в сегменте передает данные. Чем больше пользователей одновременно работают в сети, тем хуже. Стандартом 802.11 не предусмотрен отдельный канал для определения коллизий, поэтому используется метод множественного доступа к среде передачи. Если на среду передач претендует более чем один пользователь, то полоса пропускания делится на всех. Каждый пользователь получает меньшую долю, чем вы можете ожидать.

Существует более новый, но менее популярный стандарт 802.11a.

Стандарт 802.11a

Стандарт 802.11a работает, с точки зрения конечного пользователя, так же, как и 802.11b, за исключением того, что используется диапазон чуть больше

5 ГГц вместо 2,4 и пиковая пропускная способность составляет 54 Мбит/с вместо 11. Минимальная скорость — 6 Мбит/с. Если вы хотите создать беспроводную сеть там, где большое количество помех в диапазоне 2,4 ГГц, то вас спасет стандарт 802.11a.

Рис. 1.12. Точка доступа 802.11a компании Actiontec

На рис. 1.12 представлена точка доступа 802.11a компании Actiontec. На задней панели расположен последовательный порт для настройки (хотя большинство пользователей никогда его не применяют), традиционный сетевой разъем 10/100Base-T, разъем для подключения питания и утопленная кнопка сброса — для тех, кто забыл пароль.

На нижней части устройства расположены четыре отверстия, обеспечивающие надежное крепление устройства на стену или потолок.

Стандарт предусматривает возможность создания списка доступа ACL (Access Control List — список контроля доступа). В нем указываются MAC-адреса, с которыми разрешено подключение к точке доступа. Это простой способ разрешить доступ к WLAN только тем, кому вы доверяете.

Установка точки доступа не представляет ничего сложного. Как и большинство других пластмассовых коробочек современного сетевого оборудования, она имеет HTML-интерфейс. С ним можно работать, если указать в любом браузере IP-адрес точки доступа.

Компания Actiontec выпускает адаптеры PCMCIA для сетей 802.11a (рис. 1.13). С помощью адаптера (как и в случае со стандартом 802.11b) вы можете подключить компьютер к WLAN без точки доступа — в режиме ad-

hoc (ad-hocity — прицеп). Традиционное (с использованием точек доступа) подключение к WLAN происходит в режиме infrastructure (инфраструктура). Компания Actiontec выпускает адаптеры 802.11a — так же, как и 802.11b — со встроенными антеннами и без разъемов для подключения внешних антенн. У точки доступа традиционно есть две антенны, но их нельзя снять или заменить. Поскольку оборудование 802.11a работает на более высокой частоте, то оно несовместимо с имеющимися на рынке антеннами для 802.11b. Этот частотный диапазон используется редко, поэтому антенну для него вам придется либо сделать самостоятельно, либо попытаться найти ее в продаже.

Рис. 1.13. Адаптеры PCMCIA для сетей 802.11a

Стандарт 802.11g

Новый стандарт WLAN — 802.11g. Он применяет диапазон 2,4 ГГц. Пропускная способность в такой сети доходит до 54 Мбит/с при работе совместно с другим оборудованием 802.11g. Кроме того, оборудование этого стандарта совместимо с устройствами 802.11b. Новизна стандарта предполагает, что помимо первой версии будет разработано еще множество дополнений. Не надейтесь, что оборудование одного производителя будет работать с оборудованием другого и что сегодняшнее оборудование одного производителя будет работать с его завтрашними образцами без обновления прошивки или чего-нибудь еще. Технология 802.11g выглядит идеальным решением для многих целей: обратная совместимость, работа с антеннами на 2,4 ГГц, высокая скорость.

Существуют и устройства других производителей, которые подходят для организации беспроводной связи между компьютерами. Приобретая такое оборудование, важно убедиться, что оно поддерживает стандарт 802.11b. На

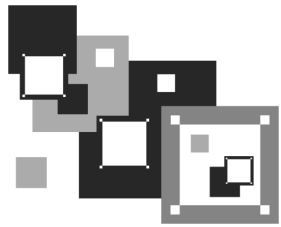
корпусе таких устройств должна быть метка "WECA" (Wireless Ethernet Compatibility Alliance — блок совместимости с радио-Ethernet), подтверждающая, что оборудование соответствует стандарту беспроводной связи, и логотип "Wireles Fidelity" (Wi-Fi), который указывает, что оборудование предназначено именно для организации беспроводной сети.

Но несмотря на радужные перспективы и хорошо работающие, но пока еще дорогие образцы оборудования, кабельные сети нельзя заменить сетью на радио-Ethernet. Во всяком случае, если сеть вам нужна теперь и вы планируете ее развивать, то не стоит ориентироваться на пока еще экстравагантные технологии. Они могут применяться как дополнение к традиционной сети. На практике с помощью радиодоступа может подключаться ограниченное число пользователей, находящихся на некотором удалении от точки доступа. Переход на радиодоступ ко всей сети приведет к чрезвычайному замедлению ее работы. Ни о каких 100 Мбит/с не придется и мечтать. Лишь в отдельных случаях, если есть необходимость обеспечить доступ к сети пользователю, перемещающемуся по некоторой территории с блокнотным компьютером, есть смысл использовать радиодоступ. Если же вы решили соединить с помощью радиоканала два участка сети, расположенные в разных зданиях, то следует зарегистрировать свое оборудование, получить разрешение на его использование в данном месте. Эта мера обезопасит вас и других пользователей радиоканалов от взаимных помех. Вполне возможно, что свободных частот не окажется, в этом случае придется ждать появления нового оборудования, работающего на более высоких частотах.

Несмотря на имеющиеся проблемы при организации беспроводных сетей, эта технология довольно активно развивается. Наибольшее применение она получает для организации доступа в Интернет. В крупных городах, в местах, посещаемых большим числом жителей и гостей организуются точки доступа к глобальной сети. Имея ноутбук или КПК можно получить доступ к Интернету во многих аэропортах, ресторанах, кафе, кинотеатрах. Некоторые организации для удобства сотрудников и гостей создают точки доступа на своих территориях. Но в этом случае стараются соблюдать меры предосторожности, исключающие возможность несанкционированного подключения к сети. Как пример можно привести новый офис корпорации Microsoft, где подключение к внутренней сети и Интернету через Wi-Fi возможно только внутри здания и защищено серьезными средствами авторизации.

Собственно локальные сети на основе беспроводных технологий не создаются. Учитывая, что беспроводные варианты соединения компьютеров могут применяться как дополнительные, продолжим рассматривать наиболее распространенные сети — кабельные.

Глава 2



Создание одноранговой сети

В предыдущей главе мы уже говорили о том, что выбор структуры и режима работы будущей сети зависит от ее назначения и требований к ее возможностям. Если безопасность и режим доступа к данным, их хранения и обмена ими через сеть не требуют выделения сервера, то достаточно организовать *одноранговую* сеть. Все компьютеры такой сети равноправны и могут выступать как в роли пользователей (клиентов) ресурсов, так и в роли их поставщиков (серверов), предоставляя другим узлам сети право доступа ко всем или некоторым из имеющихся в их распоряжении ресурсам (файлам, принтерам, программам). Предметом данной главы станет одноранговая сеть, теоретические и практические вопросы ее построения, а именно: обзор необходимого сетевого оборудования и программных средств (операционных систем, ОС), процедуры монтажа, настройки и эксплуатации такой сети.

Выбор оборудования

Для обеспечения возможности подключения к сети каждый компьютер должен иметь сетевой адаптер, который также называют *сетевой картой*. Сетевая карта устанавливается в свободный разъем на материнской плате компьютера, имеет собственный процессор, память и разъемы для подключения кабелей определенного сетевого стандарта.

Учитывая, что стандарт Ethernet — один из самых распространенных, проблем с выбором сетевой карты быть не должно. Внешний вид типичной сетевой карты показан на рис. 2.1. Установлена ли в компьютере сетевая карта, можно определить, взглянув на заднюю панель, на которой находятся разъемы и индикаторы контроля состояния.

Далее приводится краткое описание возможностей и особенностей одного из распространенных типов контроллеров, устанавливаемых на сетевых картах.

Контроллер RTL8029AS — это совместимый с NE2000 Ethernet-контроллер для интерфейса PCI. Используя высокую скорость шины PCI, контроллер RTL8029AS работает в 32-битовом режиме, благодаря чему скорость передачи данных становится гораздо выше по сравнению с ISA-картами. Функция Plug and Play ("включи и работай") шины PCI позволит разрешить конфликты системных ресурсов. Это значит, что вам не придется, как на многих старых картах, вручную устанавливать диапазон ввода/вывода и прерывание и менять эти значения при возникновении аппаратных конфликтов. Контроллер RTL8029AS поддерживает также полнодуплексный режим и возможность автоматического отключения. Благодаря функции отключения питания вы немного снизите потребление электроэнергии, а функция полного дуплекса позволит вам (при наличии полнодуплексного хаба) увеличить скорость передачи с 10 до 20 Мбит/с.

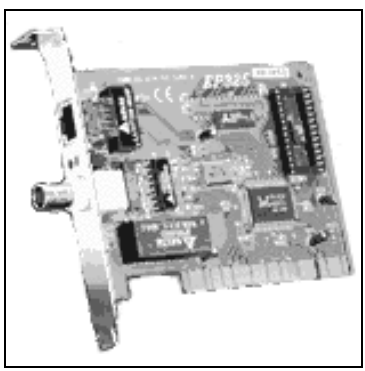


Рис. 2.1. Типичная сетевая карта
(Realtec RTL8029 Ethernet Adapter)

В микросхему (чип) RTL8029AS интегрирован кодер/декодер манчестерского кода и трансивер для 10Base-T, который автоматически корректирует неправильную полярность. Возможность подключения двух диагностических диодов позволяет упростить процедуру настройки. Наличие разъема для установки загрузочного ПЗУ (Boot ROM) емкостью 8, 16 и 32 Кбайт позволяет осуществлять загрузку компьютера из сети без использования диска. Благодаря функции предпосылки данных также возможно увеличение скорости передачи данных.

Ниже приводятся характеристики еще нескольких сетевых адаптеров, хорошо зарекомендовавших себя в домашних сетях (табл. 2.1). Данные взяты на сайте **http://homenetworks.ru**.

К приведенным характеристикам сетевых адаптеров можно добавить следующие комментарии:

- 3COM 509 — сетевой адаптер с наибольшей дальностью действия при условии использования кабеля с низким коэффициентом затухания;
- OvisLink LE-8009 — отличный сетевой адаптер с режимами jumperless и PnP. Используется при длине сегментов кабеля до 305 м, но на практике работает и на бóльшие расстояния;
- D-Link DE-220C — надежен и прост в настройке, имеет режим jumpless;
- SURECOM EP-329 — выполнен на чипе RTL8029, отлично себя зарекомендовал (установлен у 30% отечественных пользователей), работает при длинных сегментах кабеля;
- LongShine LCS-8734 — обычный адаптер.

Таблица 2.1. *Характеристики сетевых адаптеров*

Характеристики	Сетевые адаптеры					
	3COM 509	**OvisLink LE-8009**	**D-Link DE-220C**	**SURECOM EP-329**	**Long-Shine LCS-8734**	**NoName UM9008F**
Интерфейс	ISA	ISA	ISA	PCI	PCI	ISA
Проверенный рабочий сегмент, м	600	400	400	400	300	200
Примерная цена нового/бывшего в употреблении, $	45/25	20/10	20/10	13/8	15/8	11/5

Производители сетевых адаптеров регулярно предлагают все более совершенные и зачастую менее дорогие устройства. В современных компьютерах сетевой адаптер может быть интегрирован в материнскую плату. Тем не менее, используя в сети старые компьютеры, вам, вероятнее всего, придется иметь дело и со старыми сетевыми адаптерами.

В книге не рассматриваются, но существуют сетевые адаптеры для оптоволоконных кабелей. В Интернете можно встретить не только устройства для кабельных сетей, но и средства для передачи цифровой информации по радио- или оптическому каналу без применения кабеля. Для подключения к компьютеру не имеет значения, для какой физической среды передачи данных предназначен сетевой адаптер.

Управление работой любого устройства (в частности, сетевой карты) осуществляется операционной системой при помощи драйвера. После установки сетевой карты в компьютер необходимо также установить на жесткий диск ее драйвер или подключить его из списка драйверов, предлагаемых операционной системой. Обычно драйвер содержится на прилагаемых к адаптеру дискете или компакт-диске. Возможно, драйвер вашей сетевой карты уже имеется в составе Windows. Тогда достаточно проверить содержимое компакт-диска для установки Windows.

Для установки сетевой карты (платы) нужно снять крышку системного блока и найти свободный разъем (слот), соответствующий нашей плате, соблюдая необходимые меры предосторожности. Чтобы не получить поражение электрическим током и не повредить компьютер, его следует выключить и отключить от питающей сети. Вставив плату в свободный разъем и закрепив ее винтом, закройте крышку системного блока, подключите питание и включите компьютер. После загрузки, если операционная система самостоятельно не обнаружила новое устройство, выберите в меню **Пуск** команду **Настройка | Панель управления**. Найдите значок **Сеть** и дважды щелкните по нему мышью. Нажмите на вкладке **Конфигурация** кнопку **Добавить**. В появившемся окне **Выбор типа компонента** выделите пункт **Сетевая плата**. Снова нажмите кнопку **Добавить**. Далее выберите из предлагаемого операционной системой списка или установите с диска драйвер вашей сетевой платы. Если операционная система обнаружила устройство, следуйте появляющимся на экране инструкциям. Если протоколы TCP/IP и NetBEUI не были установлены ранее, то их следует установить. Процедура установки такая же, как и для сетевой карты, только для ее выполнения компьютер запросит диск, с которого проводилась установка Windows, впрочем он может потребоваться и при установке сетевой карты.

Примечание

Протокол NetBEUI может и не понадобиться, если применяются ОС Windows XP или Windows Vista.

Если у вас старый компьютер или сама сетевая карта, то установке сетевого адаптера придется уделить особое внимание. Необходимо выяснить, возможна ли установка данной конкретной платы в ваш компьютер. Компьютеры, выпущенные в разное время, могут иметь различные типы шин данных. Наиболее распространенные шины — ISA и PCI. Первые использовались в более старых компьютерах и уже не применяются, вторые — в более новых. В некоторых случаях можно использовать оба варианта шин, для этого на материнской плате должны быть предусмотрены разъемы двух видов. Необходимо убедиться, что имеющийся у вас сетевой адаптер может быть установлен в компьютер.

Кроме того, сетевые платы старого образца могут не поддерживать технологию Plug and Play ("включи и работай"). Эта технология существенно упрощает процедуру установки устройств в компьютер и активно используется в системах Windows. Плата, не поддерживающая эту технологию, потребует ручной установки всех ее параметров, включая прерывания (IRQ — Interrupt Request, запрос прерывания) и адрес ввода/вывода (I/O — Input/Output Address). Смысл этих параметров состоит в том, что операционная система не может в один и тот же момент обслуживать несколько устройств и процессов, и для незаметного пользователю переключения между задачами используются прерывания. Процессы выполняются поочередно, пошагово, при этом создается иллюзия параллельной и непрерывной работы устройств. Адрес ввода/вывода определяет начало области памяти, используемой операционной системой при обращении к устройству. Если плата не поддерживает технологию Plug and Play, к ней должна прилагаться дискета с программой конфигурации, которая обычно работает в среде DOS. Можно применять сеанс DOS из Windows. При отсутствии дискеты с программой настройки платы можно использовать программу от однотипной платы, найдя ее в Интернете на сайтах производителей плат или на сайтах архивов программного обеспечения и драйверов.

Если ваш компьютер работает под управлением Linux, то в большинстве случаев, применяя сетевые адаптеры известных производителей, вы не столкнетесь с проблемами при установке драйверов. Современные редакции Linux содержат в своем составе огромное число драйверов устройств. В крайнем случае такой драйвер можно будет найти на сайте производителя сетевого адаптера.

Дальнейшую настройку компьютера придется отложить до того момента, когда в нашей сети смогут работать хотя бы два компьютера.

После установки сетевой платы можно подключить компьютер к существующей сети. Если сети нет, займемся ее организацией. Назначение сети выбирать вам. Мы рассмотрим универсальный вариант, корректируя и модернизируя который вы сможете получить сеть с необходимыми вам качествами. Возможно, некоторые детали нашей сети покажутся вам лишними. В таком случае вы их просто можете не устанавливать, а выбрать только то, что необходимо. В самом простом случае можно соединить кабелем два компьютера, снабженных сетевыми платами, и настроить их для работы в этой миниатюрной сети. Мы примем за основу немного более сложный вариант, схема которого изображена на рис. 2.2.

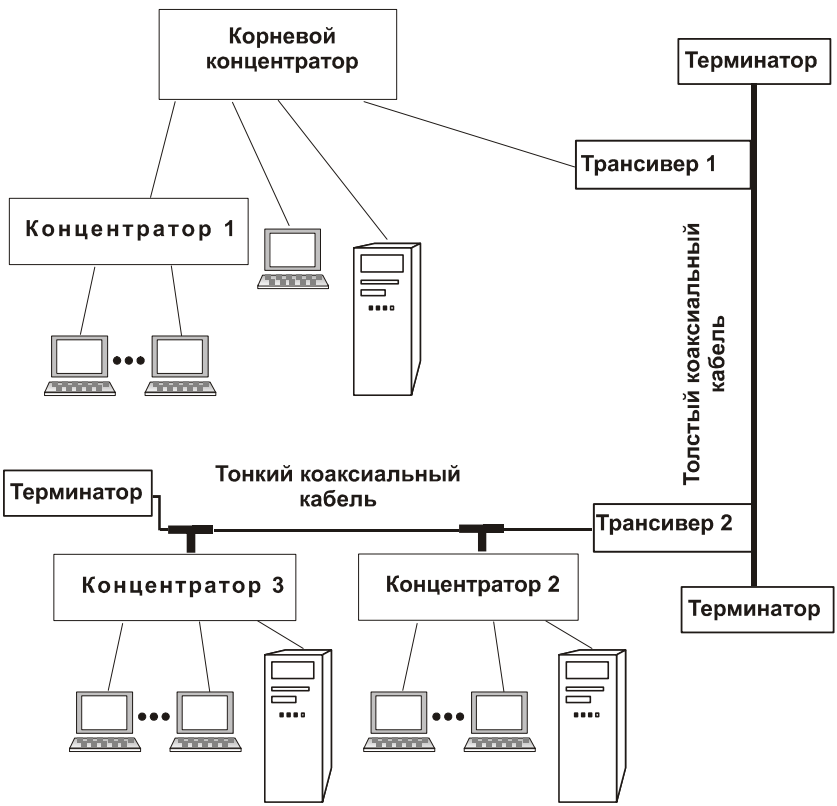


Рис. 2.2. Возможный вариант нашей сети

Настройки, которые мы будем описывать для этого варианта, подойдут и для более простых, и для более сложных сетей. В приведенном варианте приме-

нены три вида коммуникаций между коммутаторами и компьютерами. Использованы два вида коаксиального кабеля и кабель типа "витая пара", при помощи которого все рабочие станции подключены к концентраторам. Концентраторы, в свою очередь, подключены к тонкому коаксиальному кабелю и, через трансиверы, — к толстому коаксиальному кабелю.

Трансивер — это специальное устройство, используемое для подключения компьютера или концентратора к локальной компьютерной сети Ethernet, создаваемой с применением толстого коаксиального кабеля (далее — сеть на толстом кабеле). Такая сеть обладает гораздо лучшей защитой от электромагнитного излучения, чем сеть, в которой используется тонкий коаксиальный кабель (далее — сеть на тонком кабеле), и может иметь длину до 2,5 км (при использовании дополнительных устройств).

Такой вариант комбинированного использования кабелей предпочтителен при организации сети, отдельные участки которой расположены на разных этажах одного здания или даже в различных зданиях. Трансивер 1 может быть соединен с корневым концентратором посредством кабеля AUI или витой пары. Трансивер 2 должен иметь разъем BNC. Разумеется, что такой вариант рабочей сети предложен лишь в качестве примера. В вашей власти изменять, дополнять или сокращать составляющие сеть элементы.

Рассмотрим все составляющие нашей сети.

Хаб (концентратор) является центральным устройством сети на витой паре, от него зависит ее работоспособность. Его необходимо подключать к сети электропитания и располагать в легкодоступном месте, чтобы можно было без проблем подключать кабели и следить за индикацией. Концентраторы выпускаются на разное количество портов, чаще всего на 8, 12, 16, 24.

Концентраторы можно объединять, образуя каскадную структуру сети. При этом надо придерживаться следующих правил:

- ❒ избегать закольцовывания путей;
- ❒ следить за тем, чтобы количество концентраторов между любыми двумя станциями не превышало 4.

В нашем случае предполагается применить три концентратора. При отсутствии четкого представления о структуре будущей сети можно использовать одинаковые концентраторы. В противном случае можно выбрать по потребности. В зависимости от типа концентраторы могут иметь разный внешний вид. На рис. 2.3 приведен один из возможных вариантов.

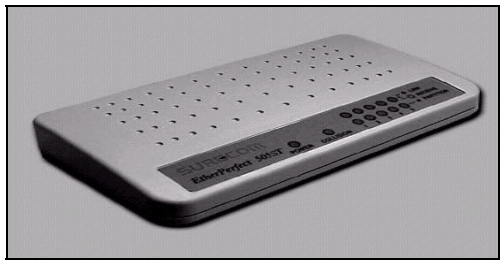


Рис. 2.3. Внешний вид концентратора EP-505ST

Подключение концентратора к другим концентраторам и компьютерам осуществляется кабелем типа "витая пара" через разъемы RJ-45. Схематично внешний вид этих разъемов представлен на рис. 2.4.

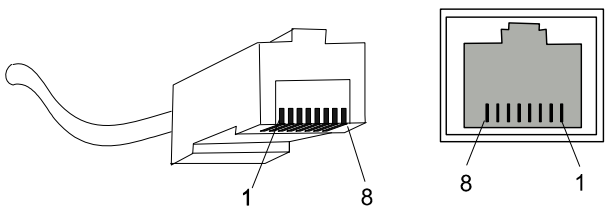


Рис. 2.4. Разъем RJ-45

Вам придется самостоятельно подключать разъемы, поэтому ниже приводится расположение (табл. 2.2) контактов для двух случаев:

- *нормальный режим* — это подключение к сетевому адаптеру;
- *каскадирование* — это подключение к другому концентратору для образования каскадной структуры, позволяющей увеличить количество рабочих станций в сети без применения многопортовых хабов.

Таблица 2.2. *Разводка контактов RJ-45*

Контакт	Каскадирование	Нормальный режим
1	RD + (прием)	TD + (передача)
2	RD – (прием)	TD – (передача)
3	TD + (передача)	RD + (прием)

Таблица 2.2 *(окончание)*

Контакт	Каскадирование	Нормальный режим
4	Не используется	Не используется
5	Не используется	Не используется
6	TD – (передача)	RD – (прием)
7	Не используется	Не используется
8	Не используется	Не используется

Способ соединения хаба с трансивером зависит от их типов, поэтому эти устройства лучше приобретать одновременно. Это уменьшит вероятность ошибки и несовместимости устройств.

Трансивер подключают непосредственно к толстому сетевому кабелю, "прокусывая" его. От трансивера к компьютеру или концентратору идет специальный кабель, максимальная длина которого — 50 м. На рис. 2.5 показан внешний вид типичного трансивера.

Рис. 2.5. Типичный трансивер

При построении сети может быть очень полезен репитер (рис. 2.6).

Репитеры (повторители) — это устройства, используемые для "удлинения" локальных компьютерных сетей.

Например, максимальная длина сети Ethernet на тонком кабеле составляет 185 м, тогда как соединение сегментов сети по 185 м с помощью репитеров позволяет получить сеть общей длиной до 925 м (в сети не может быть больше 4 репитеров). Сегмент сети подключается к репитеру через Т-коннектор

(разветвитель). К одному концу коннектора подключается сегмент, а на другом ставится терминатор.

Использование репитеров в сети Ethernet на толстом кабеле позволяет удлинить ее до 2,5 км. В этом случае репитеры подключаются к сетевому кабелю через трансивер.

Традиционный репитер имеет два порта, к которым с помощью BNC-разъема (для сети на тонком кабеле) или с помощью 15-контактного DIX/AUI-разъема (для сети на толстом кабеле) подключаются соединяемые сегменты сети. Репитер, имеющий большее число портов, может объединять, соответственно, большее число сегментов сети.

Существуют совмещенные репитеры, каждый порт которых имеет две пары разъемов: BNC и DIX, но они не могут быть задействованы одновременно.

Еще раз обратимся к базе данных сайта **http://homenetworks.ru**.

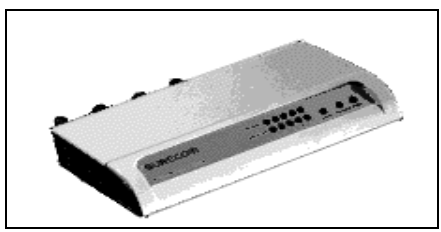


Рис. 2.6. Репитер

Репитер — это устройство, позволяющее увеличить длину коаксиального сегмента, разбив его на несколько независимых сегментов. В случае обрыва или короткого замыкания репитер также позволяет заблокировать порт с проблемным сегментом, т. е. кроме увеличения длины коаксиального сегмента, который по стандарту не должен превышать 925 м, репитер повышает надежность сети. Повреждение одного из сегментов не скажется на работе остальной части сети.

При построении домашних сетей, особенно на начальном этапе, ведущим фактором при покупке репитера является цена и только потом — длина рабочего сегмента, надежность и универсальность. В сети StarLink используется четыре вида репитеров: 2- и 7-портовые репитеры Repotec и 2- и 4-портовые репитеры SURECOM, которые удовлетворяют всем нашим требованиям.

Рассмотрим основные характеристики этих репитеров (табл. 2.3).

Таблица 2.3. *Характеристики репитеров*

Характеристики	Репитеры			
	Repotec 7-port Ethernet Repeater	**Repotec 4-port Ethernet Repeater**	**SURECOM EP-505C**	**SURECOM EP-502C**
Порты	4 BNC, 2 UTP, 1 AUI	2 BNC, 2 AUI	4 BNC, 1 AUI	2 BNC, 2 AUI
Проверенный рабочий сегмент, м	500	500	400	400
Примерная цена (новый/ бывший в употреблении), $	100/70	80/50	110/70	75/40

Каждый из указанных репитеров имеет свои преимущества и недостатки.

- Repotec 7-port Ethernet Repeater — при низкой цене дает простор для проектирования топологии. Очень удобно вести коаксиальный сегмент по чердаку или крыше, от него опускать витой парой сегмент до хаба в подъезд, а от хаба уже вести витую пару по квартирам. У этих репитеров есть один минус — очень слабые блоки питания, они быстро перегреваются и сгорают, но при замене блока питания на самодельный или взятый от какого-либо устройства отечественного производства этот репитер будет работать великолепно.
- Repotec 4-port Ethernet Repeater — дешевый и надежный репитер (при условии замены блока питания), оптимальное решение на первом этапе соединения.
- SURECOM EP-505C — простой дешевый репитер, имеет очень качественные блоки питания (однажды я нечаянно подключил к нему две фазы, так он в таком состоянии "умудрился" целый месяц проработать!).
- SURECOM EP-502C — дешево и сердито.

Все соединения между элементами сети осуществляются разъемами (коннекторами).

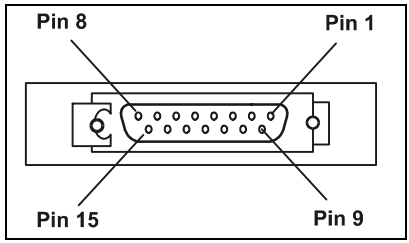


Рис. 2.7. Разъем AUI

Разъем RJ-45 мы уже рассмотрели. Но существуют и другие виды разъемов, без которых нам не обойтись.

Разъемы AUI (рис. 2.7) используются для подключения внешних трансиверов, имеющих скорость передачи данных 10 Мбит/с, и специальных кабелей, позволяющих соединить устройство с магистралью на основе толстого коаксиального кабеля. Разводка контактов такого разъема приведена в табл. 2.4.

Таблица 2.4. *Разводка контактов AUI*

Контакт	Сигнал	Контакт	Сигнал
1	Управление — вход (экран)	8	Управление — выход (экран)
2	Управление — вход (Control In)	10	Передача данных (возврат)
3	Передача данных (Transmit Data)	11	Передача данных (экран)
4	Прием данных — экран	12	Прием данных (возврат)
5	Прием данных (Recieve Data)	14	Питание (экран)
6	Ощий провод питания +12V	15	Управление — выход (Control Out)
7	Управление — выход (Control Out)		

Для подключения тонкого коаксиального кабеля применяются разъемы BNC, а для заглушки свободного конца кабеля или тройника — BNC-терминаторы (рис. 2.8).

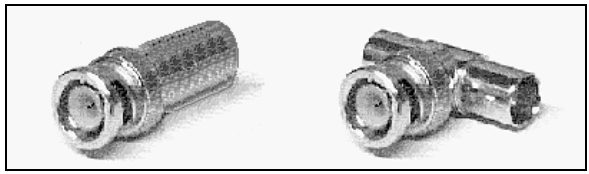


Рис. 2.8. Терминатор и тройник BNC

Сетевые операционные системы

Структура сетевой операционной системы

Сетевая операционная система (сетевая ОС) составляет основу любой вычислительной сети. Каждый компьютер в сети в значительной степени автономен, поэтому в широком смысле под сетевой операционной системой понимается совокупность операционных систем отдельных компьютеров, взаимодействующих с целью обмена сообщениями и разделения ресурсов по единым правилам (протоколам). В узком смысле сетевая ОС — это операционная система отдельного компьютера, обеспечивающая ему возможность работать в сети.

В сетевой операционной системе отдельной рабочей станции можно выделить несколько частей, каждая из которых имеет определенное функциональное назначение:

- средства управления локальными ресурсами компьютера:
  - распределение оперативной памяти между процессами;
  - планирование и диспетчеризация процессов;
  - управление процессорами в мультипроцессорных компьютерах;
  - управление периферийными устройствами и управление ресурсами локальных ОС;
- средства предоставления собственных ресурсов и услуг в общее пользование — серверная часть ОС (сервер):
  - блокировка файлов и записей, необходимая для их совместного использования;
  - ведение справочников имен сетевых ресурсов;

- обработка запросов удаленных пользователей к собственной файловой системе и базе данных;
- управление очередями запросов удаленных пользователей к собственным периферийным устройствам;

❒ средства запроса доступа к удаленным ресурсам и услугам и средства использования этих ресурсов и услуг — клиентская часть ОС (редиректор):

- распознавание и перенаправление в сеть запросов доступа к удаленным ресурсам от приложений и пользователей (при этом запрос от приложения поступает в локальной форме, а передается в сеть в форме, соответствующей требованиям сервера);
- прием ответов от серверов и преобразование их в локальную форму. В результате такого преобразования выполнение локальных и удаленных запросов для приложения неразличимо;

❒ коммуникационные средства ОС, с помощью которых происходит обмен сообщениями в сети — средства транспортировки сообщений:

- адресация и буферизация сообщений;
- выбор маршрута передачи сообщения по сети;
- обеспечение надежности передачи и т. п.

В зависимости от функций, возлагаемых на конкретный компьютер, в его операционной системе может отсутствовать либо клиентская, либо серверная часть.

Редиректор перехватывает все запросы, поступающие от приложений, и анализирует их. Если выдан запрос к ресурсу данного компьютера, то он переадресуется соответствующей подсистеме локальной ОС, если же это запрос к удаленному ресурсу, то он перенаправляется в сеть. При этом клиентская часть преобразует запрос из локальной формы в сетевую и передает его транспортной подсистеме, которая отвечает за доставку сообщений указанному серверу. На принимающем компьютере серверная часть операционной системы преобразует запрос и передает его для выполнения своей локальной ОС. После того как результат получен, сервер обращается к транспортной подсистеме и направляет ответ клиенту, выдавшему запрос. Клиентская часть преобразует результат в соответствующий формат и адресует его тому приложению, которое выдало запрос.

Первые сетевые ОС представляли собой совокупность существующей локальной ОС и надстроенной над ней сетевой оболочки. При этом в локаль-

ную ОС встраивался минимум сетевых функций, необходимый для работы оболочки. Основные сетевые функции выполнялись сетевой оболочкой. Примером такой технологии является использование на каждой рабочей станции сети операционной системы MS-DOS (начиная с третьей версии у DOS появились необходимые для совместного доступа к файлам встроенные функции, такие как блокировка файлов и записей). Принцип построения сетевых ОС в виде сетевой оболочки над локальной ОС использовался и в таких ОС, как LANtastic или Personal Ware.

Однако более эффективным представляется путь разработки операционных систем, изначально предназначенных для работы в сети. Сетевые функции у ОС такого типа глубоко встроены в основные модули системы, что обеспечивает их логическую стройность, простоту эксплуатации и модификации, а также высокую производительность. Примером такой ОС является Windows NT/2000, а также все последующие системы корпорации Microsoft, которые благодаря встроенным сетевым средствам обеспечивают более высокую производительность и защищенность информации, чем, например, сетевая ОС LAN Manager (совместная разработка Microsoft и IBM), являющаяся надстройкой над локальной операционной системой OS/2 (до настоящего времени есть приверженцы этой ОС среди опытных пользователей ПК).

В современных сетевых операционных системах (NOS — Network Operation System) вычислительные операции производятся преимущественно на рабочих станциях. На основе сетевых систем создаются и успешно применяются системы с распределенной обработкой данных. Это, в первую очередь, связано с ростом вычислительных возможностей персональных компьютеров и все более активным внедрением мощных многозадачных операционных систем: OS/2, Windows NT/2000/XP/Vista, Windows 95/98. Кроме того, внедрение объектно-ориентированных технологий (OLE, DCE, IDAPI) позволяет упростить организацию распределенной обработки данных. В такой ситуации основной задачей сетевой ОС становится объединение неравноценных операционных систем рабочих станций и обеспечение транспортного уровня для широкого круга задач, таких как обработка баз данных, передача сообщений, управление распределенными ресурсами сети (directory/name service — сервис имен/каталогов).

Применяют три основных подхода к организации управления ресурсами сети:

1. *Таблица объектов* (Bindery) — используется в сетевых операционных системах NetWare 286 — NetWare 4.1*x*. Такая таблица находится на каждом файловом сервере сети. Она содержит информацию о пользовате-

лях, группах, их правах доступа к ресурсам сети (данным, сервисным услугам и т. п.). Такая организация работы удобна, если в сети только один сервер. В этом случае требуется определить только одну информационную базу и контролировать ее. При расширении сети, добавлении новых серверов объем задач по управлению ресурсами сети резко возрастает. Администратор системы вынужден определять и контролировать работу пользователей на каждом сервере сети. Абоненты сети, в свою очередь, должны точно знать, где расположены те или иные сетевые ресурсы, а для получения доступа к этим ресурсам — регистрироваться на выбранном сервере. Конечно, для информационных систем, состоящих из большого количества серверов, такая организация работы не подходит. В современных сетях такой подход практически не применяется.

2. *Структура доменов* (Domain) — используется в таких сетевых ОС, как LAN Server и LAN Manager. Все ресурсы и пользователи сети объединены в группы. Домен можно рассматривать как аналог таблиц объектов (bindery), только здесь такая таблица является общей для нескольких серверов, а ресурсы серверов — общими для всего домена. Чтобы получить доступ к сети, пользователю достаточно подключиться к домену (зарегистрироваться), после этого ему становятся доступны все ресурсы домена, ресурсы всех серверов и устройств, входящих в состав домена. Однако и при таком подходе возникают проблемы при построении информационной системы с большим количеством пользователей, серверов и, соответственно, доменов. Например, в сети для предприятия или большой разветвленной организации проблемы уже связаны с обеспечением взаимодействия и управления несколькими доменами. (По содержанию эти проблемы такие же, как и в первом случае.)

3. *Система доменных имен* (DNS — Domain Name System) — лишена этих недостатков. Все ресурсы сети: сетевая печать, хранение данных, пользователи, серверы и т. п. — рассматриваются как отдельные ветви или каталоги информационной системы. Таблицы, определяющие DNS, находятся на каждом сервере. Во-первых, это повышает надежность и работоспособность системы, а во-вторых, — упрощает обращение пользователя к ресурсам сети. Зарегистрировавшись на одном сервере, пользователь получает доступ ко всем ресурсам сети. При таком подходе управлять системой проще, чем при использовании доменов, поскольку в первом случае все ресурсы сети определяются при помощи одной таблицы, а при доменной организации необходимо определять ресурсы, список пользователей и права доступа для каждого домена отдельно.

Рассмотрим возможности некоторых сетевых операционных систем и требования, которые они предъявляют к программному и аппаратному обеспечению устройств сети. Некоторые из рассматриваемых систем приведены в большей степени для информации, чем для практического их применения. Несмотря на то что все эти системы еще применяются в отдельных сетях, постепенно идет переход на новые ОС.

Сетевые ОС компании Novell

Рассмотрим семейство сетевых ОС компании Novell в порядке появления версий.

NetWare 3.11

Отличается самой эффективной файловой системой среди современных сетевых ОС, имеет самый широкий выбор аппаратного обеспечения.

Ниже приводятся основные характеристики и требования к аппаратному обеспечению.

- Центральный процессор: класса 386 и выше.
- Минимальный объем жесткого диска: 9 Мбайт.
- Объем оперативной памяти (ОП) на сервере: 4 Мбайт — 4 Гбайт.
- Минимальный объем ОП рабочей станции клиента: 640 Кбайт.
- Операционная система: собственная разработка Novell.
- Протоколы: IPX/SPX (Internetwork Packet Exchange — межсетевой пакетный обмен/Sequenced Packet Exchange — упорядоченный пакетный обмен).
- Мультипроцессорность: нет.
- Количество пользователей: 250.
- Максимальный размер файла: 4 Гбайт.
- Шифрование данных: нет.
- Монитор UPS (Uninterruptible Power Supply — система бесперебойного электропитания, УПС): есть.
- TTS (Teletype Setter — телетайпсеттерный код): есть.
- Управление распределенными ресурсами сети: таблицы объектов на сервере.

- Система отказоустойчивости: дублирование дисков, зеркальное отражение дисков, SFT II, SFT III (System Fault Tolerance — системная отказоустойчивость), поддержка накопителя на магнитной ленте, резервное копирование таблиц bindery и данных.
- Компрессирование данных: нет.
- Фрагментация блоков (Block suballocations): нет.
- Файловая система клиентов: DOS, Windows, Windows NT, Mac (доп.), OS/2 (доп.), UNIX (доп.).

NetWare 4

Отличительная черта этой операционной системы — применение специализированной системы управления ресурсами сети (NDS, Novell Directory Services — служба каталогов Novell). Это позволяет строить эффективные информационные системы с количеством пользователей до 1000. В NDS определены все ресурсы, услуги и пользователи сети. Эта информация распределена по всем серверам сети.

Для управления памятью используется только одна область или пул (pool), поэтому оперативная память, освободившаяся после выполнения каких-либо процессов, сразу становится доступной операционной системе (в отличие от предыдущих версий).

Новая система управления хранением данных (Data Storage Managment System) состоит из трех подсистем (компонентов), позволяющих повысить эффективность файловой системы:

- *подсистема фрагментации или разбиения блоков данных на подблоки* (Block Suballocation Subsystem). Если размер блока данных на томе — 64 Кбайт, а требуется записать файл размером 65 Кбайт, то ранее потребовалось бы выделить два блока по 64 Кбайт. При этом 63 Кбайт во втором блоке не могут использоваться для хранения других данных. В NetWare 4 система выделит в такой ситуации один блок размером 64 Кбайт и два блока по 512 байт. Каждый частично используемый блок делится на подблоки по 512 байт, свободные подблоки доступны системе при записи других файлов;
- *подсистема упаковки файлов* (File Compression Subsystem). Если какие-то данные длительное время не используются, то система автоматически выполняет сжатие (компрессию) и упаковку таких данных для экономии

места на жестких дисках. При обращении к этим данным автоматически выполняется декомпрессия данных;

- *подсистема перемещения данных* (Data Migration Subsystem). Не используемые в течение длительного времени данные система автоматически копирует на магнитную ленту либо другие носители, экономя таким образом место на жестких дисках.

В NetWare 4 встроена поддержка протокола передачи серии пакетов (Packet-Burst Migration). Этот протокол позволяет передавать несколько пакетов без ожидания подтверждения о получении каждого из них. Подтверждение передается после получения последнего пакета из серии.

При передаче данных через шлюзы и маршрутизаторы обычно выполняется разбиение передаваемых данных на сегменты по 512 байт. Это уменьшает скорость передачи данных примерно на 20%. Применение в NetWare 4 протокола LIP (Large Internet Packet — большой интернет-пакет) позволяет повысить эффективность обмена данными между сетями, так как в этом случае разбиение на сегменты по 512 байт не требуется.

Графический интерфейс пользователя организован таким образом, что все системные сообщения используют специальный модуль. Для перехода на другой язык достаточно поменять этот модуль или добавить новый. Возможно одновременная работа с несколькими языками, например один пользователь при выполнении утилит применяет английский язык, а другой в это же время — немецкий. Утилиты управления поддерживают интерфейс DOS, Windows и OS/2.

По основным характеристикам и требованиям к аппаратному обеспечению эта версия сетевой ОС компании Novell несколько превосходит NetWare 3.11.

- Центральный процессор: класса 386 и выше.
- Минимальный объем жесткого диска: от 12 до 60 Мбайт.
- Объем ОП на сервере: 8 Мбайт — 4 Гбайт.
- Минимальный объем ОП рабочей станции клиента: 640 Кбайт.
- Операционная система: собственная разработка Novell.
- Протоколы: IPX/SPX.
- Мультипроцессорность: нет.
- Количество пользователей: 1000.
- Максимальный размер файла: 4 Гбайт.

- Шифрование данных: C-2.
- Монитор UPS: есть.
- TTS: есть.
- Управление распределенными ресурсами сети: NDS.
- Система отказоустойчивости: дублирование дисков, зеркальное отражение дисков, SFT II, SFT III, поддержка накопителя на магнитной ленте, резервное копирование таблиц NDS.
- Компрессирование данных: есть.
- Фрагментация блоков (Block Suballocation): есть.
- Файловая система клиентов: DOS, Windows, Windows NT, Mac (5), OS/2, UNIX (доп.).

NetWare 5.1

Рассмотрим еще одну сетевую ОС компании Novell, появившуюся совсем недавно.

Это полноценная сетевая операционная система для вычислительных сетей. Она отлично подходит для установки как на сервер, так и на рабочую станцию. Благодаря NetWare 5.1 вы можете также создавать серверы в Интернете, такие как Web-сервер, FTP (File Transfer Protocol — протокол передачи файлов), поисковые, мультимедийные, ASP-сервер (Active Server Pages — активные серверные страницы) и др. Novell NetWare 5.1 поддерживает Windows различных версий в качестве ОС-клиентов. Это позволяет использовать компьютеры на базе этих операционных систем в ЛВС Novell.

В NetWare 5.1 очень четко определены права доступа и ограничения, причем на уровне загрузки. Все версии ОС NetWare поддерживают множество драйверов, дополнительных устройств, что позволяет устанавливать большое количество компонентов. В NetWare 5.1 предусмотрено много новых приложений: Novell Directory Services, NDS8, Web Sphere IBM 3.0 (Web-глобус компании IBM версии 3.0), Web Sphere Studio 3.0 Entry Edition (Первое издание Web-глобуса для студий версии 3.0), NetWare Enterprise Web Server 3.6 (NetWare Web-сервер для предприятий, версия 3.6), Oracle8i, FTP, Web Search (Поиск в Web), серверы Multimedia (мультимедиа) и Halcyon InstantASP. Все вместе это составляет довольно сильный набор приложений-серверов.

Самое интересное добавление — Novell's NetWare Server Management Portal (портал сервера администрации сети NetWare компании Novell), который позволяет вызывать администрацию сервера и NDS через окно просмотра Web.

Администраторы больше не должны иметь рабочую станцию управления с приложением Client32 — сетевым программным обеспечением Novell, загружаемым на сервере вместо приложения Microsoft's NetWare Client (NetWare-клиент корпорации Microsoft), которое работает на клиентской рабочей станции. Вместо этого любое окно просмотра, которое поддерживает безопасный HTTP-протокол (HyperText Transfer Protocol — протокол передачи гипертекста), может действовать как соединение для управления работой приложений в сети NetWare и службы каталогов NDS.

Приложение NetWare 5.1 Server Management Portal также позволяет выполнять некоторые дополнительные функции по администрированию сети.

Требования к аппаратному обеспечению у этой сетевой ОС следующие:

- ❒ серверное оборудование с процессором Pentium II или выше;
- ❒ видеокарта с поддержкой режима VGA (рекомендуется поддержка SVGA-режима);
- ❒ раздел DOS — минимум 50 Мбайт с 35 Мбайт свободного пространства;
- ❒ доступное дисковое пространство за пределами раздела DOS (для хранения компонентов NetWare и WebSphere Application Server for NetWare) — минимум 1,3 Гбайт (том SYS);
- ❒ оперативная память (RAM):
  - стандартные продукты NetWare — 128 Мбайт;
  - Web Sphere Application Server for NetWare — 256 Мбайт (рекомендуется 512 Мбайт) в дополнение к объему, рассчитанному для стандартных продуктов NetWare;
- ❒ одна сетевая карта или более;
- ❒ накопитель CD-ROM, поддерживающий диски в формате ISO 9660;
- ❒ мышь, подключенная к последовательному порту или PS/2-порту.

LAN Server, IBM Corporation

Отличительные черты:

- ❒ доменная организация сети, упрощающая управление и доступ к ресурсам сети;

- поддержка полного взаимодействия с иерархическими системами, например с архитектурой SNA (Systems Network Architecture — сетевая архитектура систем) и поддержка межсетевого взаимодействия;
- целостность операционной системы и широкий набор услуг. Работает на базе OS/2, поэтому сервер может быть невыделенным (nondedicated).

Существуют две версии LAN Server: Entry (Первоначальная) и Advanced (Усовершенствованная). Advanced, в отличие от Entry, поддерживает высокопроизводительную файловую систему (HPFS — High Perfomance File System). Она включает системы отказоустойчивости (Fail Tolerances) и секретности (Local Security).

Серверы и пользователи объединяются в домены. Серверы в домене работают как единая логическая система. Все ресурсы домена становятся доступны пользователю после регистрации в этом домене. В одной кабельной системе могут работать несколько доменов. Если на рабочей станции установлена OS/2, ресурсы этой станции становятся доступны пользователям других рабочих станций, но не всем сразу, а только одному из них в отдельный момент времени. Администратор может управлять работой сети только с рабочей станции, на которой установлена операционная система OS/2. LAN Server поддерживает удаленную загрузку рабочих станций (RIPL — Remote Interface Procedure Load) для DOS, OS/2 и Windows.

К недостаткам LAN Server можно отнести сложность ее установки и ограниченное количество поддерживаемых драйверов сетевых адаптеров.

Ниже приводятся основные характеристики и требования к аппаратному обеспечению.

- Центральный процессор: класса 386 и выше.
- Минимальный объем жесткого диска: 4,6 Мбайт для клиентской части ОС, 7,2 Мбайт — для серверной.
- Минимальный объем ОП на сервере: 1,3—16 Мбайт.
- Минимальный объем ОП рабочей станции клиента: 4,2 Мбайт — для OS/2, 640 Кбайт — для DOS.
- Операционная система: OS/2 2.*x*.
- Протоколы: NetBIOS, TCP/IP.
- Мультипроцессорность: поддерживается.
- Количество пользователей: 1016.

- Максимальный размер файла: 2 Гбайт.
- Шифрование данных: нет.
- Монитор UPS: есть.
- Управление распределенными ресурсами сети: структура доменов.
- Система отказоустойчивости: дублирование дисков, зеркальное отражение дисков, поддержка накопителя на магнитной ленте, резервное копирование таблиц домена.
- Компрессирование данных: нет.
- Фрагментация блоков (Block Suballocation): нет.
- Файловая система клиентов: DOS, Windows, Windows NT, Mac, OS/2, UNIX.

VINES 5.52, Banyan System Inc.

Отличительные черты:

- возможность взаимодействия с любой другой сетевой операционной системой;
- использование службы имен StreetTalk, позволяющей создавать разветвленные системы.

До появления NetWare 4 VINES преобладала на рынке сетевых операционных систем для распределенных сетей и для сетей масштаба предприятия (enterprise networks — промышленная сеть). Тесно интегрирована с UNIX.

Для организации взаимодействия используется глобальная служба имен StreetTalk — база данных, распределенная по всем серверам сети, во многом схожая с NetWare Directory Services. Она позволяет подключиться пользователю, находящемуся в любом месте сети.

Поддержка протокола X.29 позволяет удаленной рабочей станции DOS подключиться к локальной сети через сеть, поддерживающую протокол X.25, или через сеть ISDN.

VINES критична к типу компьютера и жестких дисков. Поэтому при выборе оборудования необходимо убедиться в совместимости аппаратного обеспечения и сетевой операционной системы VINES.

Ниже приводятся основные характеристики и требования к аппаратному обеспечению.

- Центральный процессор: класса 386 и выше.
- Минимальный объем жесткого диска: 80 Мбайт.
- Объем ОП на сервере: 8—256 Мбайт.
- Минимальный объем ОП рабочей станции клиента: 640 Кбайт.
- Операционная система: UNIX.
- Протоколы: VINES IP, AFP, NetBIOS, TCP/IP, IPX/SPX.
- Мультипроцессорность: есть — SMP (Symmetrical MultiProcessing — симметричная многопроцессорная обработка).
- Количество пользователей: не ограничено.
- Максимальный размер файла: 2 Гбайт.
- Шифрование данных: нет.
- Монитор UPS: есть.
- TTS: нет.
- Управление распределенными ресурсами сети: глобальная служба имен StreetTalk.
- Система отказоустойчивости: резервное копирование таблиц StreetTalk и данных.
- Компрессирование данных: есть.
- Фрагментация блоков (Block Suballocation): нет.
- Файловая система клиентов: DOS, Windows, Windows NT (доп.), Mac (доп.), OS/2, UNIX (доп.).

Сетевые ОС корпорации Microsoft

В данном обзоре сетевых ОС корпорации Microsoft мы рассмотрим Windows NT, Windows 98, Windows 2000, Windows XP, Windows Server 2003, Windows Vista. Постепенно более новые операционные системы заменяют своих предшественниц. Но у многих пользователей старые ОС продолжают работать. Если они могут в полной мере удовлетворять требованиям сети, то заменять их нет смысла.

Windows NT Advanced Server 3.1

Простота интерфейса пользователя, доступность средств разработки прикладных программ и поддержка прогрессивных объектно-ориентированных технологий — все это привело к тому, что Windows NT стала одной из самых популярных сетевых операционных систем.

Ее интерфейс напоминает оконный интерфейс Windows 3.1, инсталляция занимает около 20 мин. Модульное построение системы упрощает внесение изменений и перенос на другие платформы. Подсистемы защищены от несанкционированного доступа и от их взаимного влияния (если "зависает" один процесс, это не влияет на работу остальных). Предусмотрена поддержка удаленных станций (RAS — Remote Access Service, сервис удаленного доступа), но не поддерживается удаленная обработка заданий.

По сравнению с NetWare, Windows NT предъявляет более высокие требования к производительности компьютера.

Основные характеристики Windows NT и ее требования к аппаратному обеспечению приведены ниже.

- Центральный процессор: класса 386 и выше, MIPS, R4000, DEC Alpha AXP.
- Минимальный объем жесткого диска: 90 Мбайт.
- Минимальный объем ОП на сервере: 16 Мбайт.
- Минимальный объем ОП рабочей станции клиента: 12 Мбайт для Windows NT; 512 Кбайт — для DOS.
- Операционная система: Windows NT.
- Протоколы: NetBEUI, TCP/IP, IPX/SPX, AppleTalk, AsyncBEUI.
- Мультипроцессорность: поддерживается.
- Количество пользователей: не ограничено.
- Максимальный размер файла: не ограничен.
- Шифрование данных: уровень C-2.
- Монитор UPS: есть.
- TTS: есть.
- Управление распределенными ресурсами сети: структура доменов.

- Система отказоустойчивости: дублирование дисков, зеркальное отражение дисков, RAID 5, поддержка накопителя на магнитной ленте, резервное копирование таблиц домена и данных.
- Компрессирование данных: нет.
- Фрагментация блоков (Block Suballocation): нет.
- Файловая система клиентов: DOS, Windows, Windows NT, Mac, OS/2, UNIX.

Windows 2000

Второе название системы — Windows NT 5.

Операционная система применима как для рабочей станции, так и для сервера. Имеет собственную файловую систему (NTFS — New Technology File System, файловая система новой технологии), являющуюся модернизацией файловой системы из Windows NT. По сравнению со своей предшественницей, имеет множество усовершенствований, в частности эффективные средства доступа в Интернет через локальную сеть, а также систему автовосстановления утраченных и поврежденных программных модулей с установочного компакт-диска.

Как и Novell NetWare 5.1, Windows 2000 имеет повышенные требования к ресурсам компьютера. Для реализации всех ее серверных возможностей требуется 256 Мбайт оперативной памяти и более 3 Гбайт дискового пространства (для обеспечения работы самой операционной системы, а также под сетевые каталоги, программы).

Одной из интересных и полезных особенностей этой операционной системы является возможность удаленного администрирования с помощью встроенного сервиса Telnet (Протокол виртуального терминала). Но по умолчанию запуск Telnet-сервиса отключен.

Еще одна возможность — терминальный доступ.

Если приложение затребует большие вычислительные мощности, то терминальный сервер позволяет при необходимости предоставить для выполнения сложной задачи от 5 до 20 MIPS (миллионов операций в секунду), и это никак не отразится на других клиентах с терминальным доступом.

Терминалами могут служить практически любые компьютеры, вы сможете использовать компьютеры класса 386/486/Pentium 60 и др. Применение терминального доступа снижает нагрузку на сеть, поскольку все вычислитель-

ные операции производятся на сервере. К сожалению, старые DOS-приложения, требующие прямого доступа к аппаратной части компьютера, не могут работать на терминальном сервере. Впрочем, они не могут работать и с современными операционными системами класса Windows NT.

Windows 2000 Server

Эта операционная система специально разработана для установки на сервере. На рабочей станции работать она, конечно, будет, но в этом нет никакого смысла, поскольку основная ее задача — управление компьютерной сетью. Для Windows 2000 Server необходим компьютер с рабочей частотой не ниже 500 МГц, объемом оперативной памяти не ниже 256 Мбайт, размером винчестера не менее 20 Гбайт. Требования для установки системы намного скромнее, но практика показывает, что при указанных параметрах большинство задач сети сервер решает прекрасно.

Windows XP

Операционная система разрабатывалась специально для рабочей станции. Как и Windows 2000, имеет файловую систему (NTFS — New Technology File System, файловая система новой технологии). Имеет все положительные качества Windows 2000 и новый интерфейс, ориентированный на пользователя средней подготовки. Для тех, кто привык к классическому интерфейсу Windows, есть возможность перейти к нему. Требования к ресурсам компьютера такие же, как и у Windows 2000.

Есть возможность адаптации к старым приложениям, которые под управлением Windows 2000 не работают или работают плохо.

По сравнению со всеми предыдущими операционными системами семейства Windows обладает повышенной стабильностью. Настройка компьютера под управлением Windows XP для работы как в локальном режиме, так и для работы в сети подобна настройкам в системе Windows 2000.

Большое внимание разработчики уделили защите компьютера с установленной Windows XP от проникновения злоумышленников из сети. Все сетевые подключения, как и соединение с Интернетом, могут быть защищены встроенным межсетевым экраном.

Возможности применения Windows XP в качестве серверной операционной системы ограниченны.

Windows Server 2003

Корпорация Microsoft постоянно совершенствует свои программные продукты. Новая операционная система для сервера Windows Server 2003, о выпуске которой было объявлено в апреле 2003 года, предназначена для применения как в небольших, так и в очень крупных организациях. Предполагается выпустить локализованные версии системы для всех вариантов. Для нашей небольшой сети применение новой операционной системы, возможно, и не принесет существенных выгод и удобств. Но поскольку она уже существует, рассмотрим некоторые особенности этой системы.

Установка может производиться как из среды предыдущей версии Windows, так и при загрузке с компакт-диска. Процедура установки новой версии системы практически не отличается от установки Windows 2000 Server. Но когда дело доходит до настройки сервера, мы обнаруживаем, что, в отличие от предыдущей версии, сервисы не устанавливаются по умолчанию. Все, что вы хотите установить, необходимо выбирать самостоятельно. Кроме того, установив Active Directory, вы увидите, что политика безопасности не определена. Необходимо самостоятельно определить правила доступа к домену для всех создаваемых групп и пользователей. С одной стороны, для начинающего администратора это представляет неудобство и сложность, с другой — позволяет эффективно решить проблему безопасности. Ни одно из правил доступа к ресурсам домена не будет использоваться без вашего ведома. Работа с новой операционной системой мало отличается от работы с Windows 2000 Server. Новые возможности, которыми обладает Windows 2003, делают удобным управление большими сетями (эта операционная система разрабатывалась именно с этой целью). Добавлены новые функции для разработчиков программного обеспечения. Некоторые возможности Windows Server 2003 могут привлечь особое внимание, например встроенный почтовый сервер. Следует отметить и защиту сетевых соединений, существующую и в Windows XP. Если ваш сервер будет постоянно подключен к Интернету, то злоумышленнику трудно будет проникнуть в вашу сеть извне, — система безопасности находится под вашим контролем! Очень хорошо построена справочная система. Из каждого окна ссылки вы имеете возможность пройти по дополнительным ссылкам. Даже после нескольких лет после выхода этой ОС многие администраторы предпочитают использовать Windows 2000 Server в качестве системы для сервера. Настройка Windows Server 2003 требует более серьезной подготовки, чем настройка Windows 2000 Server. Во многих случаях для простой локальной сети не требуются возможности Windows

Server 386/486, но организуя выход в Интернет для вашей сети, следует подумать о применении Windows Server 2003. Безопасность вашей сети в этом случае может быть выше.

Windows Vista

Это операционная система для рабочей станции. Соответствующая этой новой ОС серверная система Viridian, или Windows Server 2008 еще в разработке. Но вобрав в себя все достижения предыдущих версий, новые идеи и достижения разработчиков, Windows Vista стала на сегодняшний день самой совершенной операционной системой для IBM-совместимых компьютеров нового поколения. Почему нового? Просто потому, что на совсем старые компьютеры новая ОС, скорее всего, не установится.

> ***Примечание***
>
> Интересно, что старые версии Windows, например 2.0, вы не сможете установить на современный компьютер.

Тем не менее опыт показывает, что в базовом варианте система может быть установлена практически на любой компьютер, на котором могла работать Windows XP. Самым критичным параметром является размер оперативной памяти, который не должен быть менее 512 Мбайт, но для комфортной работы в системе лучше иметь не менее 1 Гбайт оперативной памяти.

Основные минимальные требования к компьютеру для Windows Vista приведены ниже.

- Процессор: с частотой 1 ГГц, 32-разрядный или 64-разрядный.
- Оперативная память: 512 Мбайт.
- Видеопамять: 128 Мбайт.
- Жесткий диск: 40 Гбайт.
- Свободное пространство на жестком диске: 15 Гбайт.
- Оптический привод: DVD-ROM.
- Наличие звуковой карты.
- Наличие подключения к Интернету.

Жесткий диск размером 40 Гбайт очень быстро заполнится, если вы будете сохранять видео- и аудиоинформацию, устанавливать игры. Для комфортной работы на компьютере с операционной системой Vista лучше иметь жесткий диск размером не менее 160 Гбайт.

Безопасность системы существенно выше, чем у всех предыдущих версий Windows. Теперь нет необходимости работать в системе в сеансе администратора системы. Для решения административных задач необходимо лишь ввести пароль администратора, когда этого потребует система. Подобный метод защиты системы от несанкционированных действий вирусов и хакеров используется в Linux.

Linux

Название Linux, как и Windows, относится не к одной ОС, а к целому классу систем. Различные разработчики вносят в свои продукты свои идеи и представления о том, какой должна быть операционная система. Практически все версии Linux имеют поддержку русского языка, но русификация может быть более или менее корректной. Для русскоязычных пользователей в наибольшей степени могут подойти ASP Linux (**http://www.asplinux.ru/**), Linux XP (**http://www.linux-online.ru/desktop/**), Alt Linux (**http://altlinux.ru/**), специализированные серверные ОС BSL OS (**http://www.bslos.com/download.html**) и MOPS Linux (**http://www.rpunet.ru/content/view/23/1/**).

Постепенно все разработчики Linux начинают распространять не только настольные системы, но и серверные. Часто Linux распространяется бесплатно или за небольшую цену. При необходимости получить техническую поддержку ее можно купить дополнительно.

Системные требования для установки любой версии Linux не превышают требований для Windows. Надежность системы обычно очень высока ввиду особенностей файловой системы. Существует очень мало вирусов, написанных для атак на Linux, что делает систему еще более стабильной.

Интерфейс системы несколько отличается от интерфейса Windows, но опытный пользователь Windows за короткое время может освоиться в новом для себя окружении. Несколько большее время требуется для освоения командной строки Linux. При желании вы можете ознакомиться с командной строкой Linux по материалам сайта по адресу **http://zero.kanet.ru/site/index.php?page=15**.

Выбор операционной системы для нашей сети

До недавнего времени Windows 9*x* была самой универсальной и распространенной операционной системой. Очень существенный недостаток этой системы — нестабильность, частично вызванная универсальностью и совместимостью с устаревшими приложениями, заставила большинство пользователей перейти на Windows XP (разработанной на базе Windows 2000), ставшую теперь самой распространенной системой.

При подготовке Windows 2000 и Windows XP разработчики не только постарались учесть опыт создания NT-систем предыдущего поколения, сохранив все их традиционные достоинства, но и включили в нее много полезных наработок из привычной Windows 9*x*, как бы сблизив эти две разные системы. Вероятно, это вписывается в стратегический план корпорации Microsoft по переводу всех пользователей Windows именно на платформу NT. Смена названия с NT 5 на Windows 2000 говорит о том, что в Microsoft хотели сделать эту систему ближе к народу, привыкшему к Windows 9*x* и пугающемуся аббревиатуры NT.

Система эта имеет много преимуществ не только по сравнению с системой Windows 9*x* или другими не столь распространенными ОС, но и по сравнению со своей предшественницей — Windows NT 4. Главное же и важнейшее ее достоинство — это совместимость с большинством программ Windows 9*x* (но не со всеми!). При этом надежность Windows 2000 — существенно выше, чем у Windows 9*x*. В Windows XP в значительной мере решена проблема совместимости со старыми программными продуктами, под ее управлением работают практически все старые приложения.

Устойчивость работы Windows 2000/XP объясняется тем, что в них, в отличие от Windows 9*x*, применена так называемая *вытесняющая многозадачность*, как в UNIX-подобных системах (Linux, например). При таком способе реализации многозадачности ни один самый "глючный" процесс не сможет полностью завладеть центральным процессором, а получит в свое распоряжение лишь небольшой кусочек времени его работы, после чего процессор благополучно перейдет к обслуживанию следующего процесса — и так по кругу. Таким образом, каждый процесс обрабатывается по очереди под управлением специального диспетчера, а "зависшая" программа принудительно освобождает процессор по истечении отведенного ей на работу времени. При появлении сбоя достаточно снять повисшую задачу. Такой сбой

никак не отражается на деятельности всей системы и других программ, так как они никак не влияют друг на друга. В Windows 2000 отсутствует еще один источник проблем — VxD-драйверы, свободно хозяйничающие во всех областях оперативной памяти (VxD-драйвер — виртуальный драйвер устройства, управляющий единственным ресурсом от имени всех выполняемых процессов).

Перейдя на Windows 2000/XP, кроме избавления от большинства "глюков" вы получите массу других полезных функций, например повышенную надежность хранения информации на диске благодаря модифицированной файловой системе NTFS 5.0. Или встроенную возможность шифрования данных "на лету" средствами файловой системы EFS, позволяющую скрыть частную информацию от посторонних глаз. Благодаря NTFS сама ОС "умеет" сжимать файлы и папки без посредников-архиваторов. В общем, всех функций "продвинутой" NTFS и не перечислишь...

По сравнению с Windows NT 4, новые операционные системы не только значительно облагорожены приятным внешним видом пользовательского интерфейса, который не вызовет никаких проблем у тех, кто знаком с Windows 9*x*, но и заметно улучшена поддержка широкого спектра нового оборудования. Система хорошо воспринимает Plug and Play, USB (Universal Serial Bus — универсальная последовательная шина), IEEE, ACPI (Advanced System Configuration and Power Interface — усовершенствованный интерфейс конфигурирования системы и управления энергопитанием), AGP (Accelerated Graphics Port — порт ускоренной графики), MMX (MultiMedia eXtension — мультимедийное расширение), даже FAT32 (File Allocation Table — таблица размещения файлов) и еще множество интересных и нужных функций типа мультимониторинга (поддержки нескольких мониторов) и сканеров с фотокамерами. Кроме того, в Windows 2000 встроен компонент DirectX 7.0 для программирования компонентных объектных приложений на основе модели COM (Component Object Model — модель компонентных объектов).

Таким образом, появились операционные системы, которые могут заменить Windows 9*x*, позволяя при этом не расставаться с любимыми программами. В большинстве случаев программы под Windows 2000/XP работают быстрее, чем под Windows 9*x*!

Если вы до сих пор используете Windows 98, не спешите переустанавливать систему. Следует убедиться, что компьютер отвечает требованиям для установки более новых ОС. Прежде чем вы решите установить эту ОС на домашнем компьютере, необходимо определить, насколько она вам подходит и чего вы можете лишиться при переходе на нее. А это зависит как от состояния

ваших аппаратных ресурсов, так и от тех задач, которые вы ставите перед компьютером.

Надо сказать, что имеется несколько вариантов Windows 2000/XP, из которых мы будем рассматривать только версию Professional.

Главный недостаток Windows 2000/XP Professional — высокая требовательность к аппаратной конфигурации персонального компьютера, значительно превышающая запросы Windows 9*x*. И хотя Microsoft заявляет, что минимум для Windows 2000 Professional — процессор класса Pentium 133, ОП емкостью 32 Мбайт, жесткий диск емкостью 2 Гбайт, на такой компьютер установить Windows 2000 Professional можно, но работать на нем будет некомфортно. Даже с рекомендуемыми 64 Мбайт оперативной памяти, система будет "безбожно тормозить". Ей требуется минимум 96 Мбайт, при которых уже можно более или менее комфортно работать. Если же вы хотите, чтобы свопинг (периодическая запись на диск и чтение с него не умещающейся в оперативной памяти информации) не раздражал, а только слегка беспокоил вас, то будьте готовы разориться на ОП емкостью 128 Мбайт и более. Процессор же необходим не хуже, чем Pentium 233 МГц. Свободного пространства на жестком диске в 650 Мбайт, как написано в руководстве Microsoft, едва-едва хватит под саму операционную систему, а все программы придется устанавливать в другие разделы. Но и в этом случае диск будет быстро заполняться файлами системы. Разбейте жесткий диск таким образом, чтобы под раздел с ОС было отведено минимум 2—4 Гбайт в зависимости от того, куда вы будете инсталлировать прикладные программы. Для Windows XP требования не ниже, а если учесть встроенные мультимедийные возможности, то даже выше. По опыту пользователей, системный раздел для Windows XP должен быть не менее 20 Гбайт, если предполагается работа только с офисными приложениями.

Если вы еще не передумали устанавливать Windows 2000/XP, то составьте полный список имеющегося оборудования. Хотя под эти ОС и написано уже достаточно много драйверов, может оказаться, что производитель какого-нибудь компонента именно вашего компьютера поленился это сделать, и вы не получите, например, другого разрешения экрана от вашей видеокарты в Windows 2000, кроме как 640×480. Драйверы, особенно для 3D-ускорителей, пока являются одним из самых узких мест этой системы. Поиску драйвера следует уделить особое внимание и владельцам внешних контроллеров SCSI (Small Computer Systems Interface — интерфейс малых компьютерных систем) или IDE (Integrated Drive Electronics — встроенный интерфейс накопителей). Поэтому перепишите драйвер на дискету или временно отключите само устройство — программа инсталляции часто не способна правильно оп-

ределить такой контроллер и просит дискету с драйвером. Постоянно обновляемый список совместимых с Windows 2000/XP аппаратных средств находится на сайте **www.microsoft.com/hcl**. С несколько устаревшей его версией можно ознакомиться и на самом компакт-диске с дистрибутивом. Бывает, что совместимость BIOS со стандартом ACPI (Advanced System Configuration and Power Interface — усовершенствованный интерфейс конфигурирования системы и управления энергопитанием) является непременным условием успешной установки Windows 2000/XP на компьютер, тогда придется сначала позаботиться о перепрограммировании (перепрошивке) BIOS.

Начиная с первого издания мы ориентировались в основном на применение Windows 98. Во втором издании Windows 98 предлагался целый ряд новых возможностей для работы с Интернетом и обеспечивалась дополнительная поддержка аппаратных средств.

- Internet Explorer 5. Широко распространенные технологии обзора, созданные корпорацией Microsoft, позволяют значительно повысить быстродействие, качество и гибкость при работе в Интернете.
- Windows NetMeeting 3. Последняя версия NetMeeting® расширяет возможности проведения сетевых конференций, повышает быстродействие и обеспечивает безопасность и поддержку стандартов Интернета.

Подключение к Интернету с общим доступом (ICS — Internet Connection Sharing). ICS — это комплекс передовых технологий, дающих возможность пользователям нескольких компьютеров одновременно получать доступ в Интернет через одно общее подключение.

Преимущества Microsoft Windows 98 SE перечислены ниже.

- Простота использования и доступа в Интернет:
  - динамическая справочная система на основе Web-технологии и 15 программ-мастеров упрощают работу на компьютере;
  - Web-совместимый интерфейс пользователя Windows 98 облегчает поиск, унифицируя представление информации в компьютере, локальной сети и в Web (World Wide Web — Всемирная паутина);
  - возможность одновременного доступа в Интернет с нескольких сетевых компьютеров через одно общее подключение.
- Высокая производительность и надежность:
  - сокращение времени запуска приложений;
  - новые средства очистки диска и повышения эффективности его работы;

- использование преимуществ новейших стандартов и технологий, таких как шина USB, DVD (Digital Video Disk — цифровой видеодиск) и IEEE 1394, расширение возможностей за счет подключения к одному компьютеру нескольких мониторов, поддержка технологий Digital Imaging (цифровой обработки изображений) и Microsoft WebTV (браузер) для Windows.

В третьем издании книги значительное внимание будет уделено Windows XP, а также другим современным ОС, но и описания работы с Windows 98 сохранены. Во многих случаях они актуальны и для работы с новыми операционными системами. В других случаях полезны при использовании устаревших машин.

Во многих случаях нас вполне бы устроила старая и достаточно надежная DOS. Но, к сожалению, сетевые возможности этой системы очень ограничены. В сетях, которые применяют операционную систему Novell NetWare, можно использовать компьютеры, не имеющие ничего, кроме DOS. Но настройка и дальнейшее обслуживание такой сети связаны со значительными проблемами, и вам в любом случае не обойтись без выделенного сервера. Ряд сайтов постоянно публикуют вопросы и ответы об эксплуатации таких сетей. Возникают проблемы по самым разным причинам. То новый принтер отказывается печатать в сети, то новая программа конфликтует с NetWare-клиентом. Приходится выдумывать пути обхода возникающих проблем, которых со временем не уменьшается. Конечно, компания Novell работает над своей системой и совершенствует ее. Но обновление сетевой операционной системы — это целая эпопея. Во-первых, сеть должна быть остановлена на какое-то время, некоторые используемые в сети программы должны быть обновлены или заменены, обеспечена совместимость всего оборудования с новой системой. А дальше — новые проблемы. Кроме того, новые версии программ стоят некоторых денег. Конечно, у нас еще повсеместно применяются пиратские копии программ и операционных систем. Но если вы хотите заниматься бизнесом, применяя нашу локальную (пока) сеть, то желательно иметь лицензионные программные продукты на всех рабочих станциях сети. Закон есть закон. Когда-нибудь он доберется и до вашей фирмы. Есть варианты бесплатные. UNIX, Linux — системы бесплатные, но и программного обеспечения для этих систем еще немного. Вам же надо работать, а не смотреть на бесплатную сеть. Но для выделенного сервера такая операционная система вполне подходит, а учитывая ее бесплатность, можно подумать и о ее применении. Появляются новые версии Linux для рабочих станций с широкими возможностями и совместимостью с сетью под Windows. Но мы в

основном рассматриваем возможности Windows. Причем пытаемся использовать то, что установлено на наших компьютерах.

И еще одно замечание: перейти с Windows 95/98 на Windows 2000/XP никогда не поздно. Если вы уверены, что применяемые вами оборудование и программное обеспечение совместимы с новой системой и других проблем нет, то установка пройдет без проблем. Надо учесть, что применение сервера с установленным на нем приложением Windows 2000 Server в полной мере оправданно, если на рабочих станциях вашей сети установлен компонент Windows 2000/XP Professional.

Если компьютеры вашей сети приобретены недавно, то вполне возможно, что на них уже установлена Windows 2000 или Windows XP. Во всяком случае, вы сами можете установить новые операционные системы на новые компьютеры, не задумываясь о совместимости с ними вашего "железа".

Приобретая совсем новые компьютеры, вы можете столкнуться с тем, что на них уже установлена Windows Vista. Прежде чем купить такой компьютер, убедитесь, что оперативной памяти у него не менее 1 Гбайт. Иначе вы не сможете работать с системой достаточно комфортно.

Нередко пользователям приходится производить установку операционной системы самостоятельно. Поэтому рассмотрим далее процедуры установки некоторых ОС.

Процедура установки Windows 2000

Выбор способа установки

Итак, если ваша система в принципе готова принять новую ОС, вы нашли драйверы ко всему оборудованию и готовы ради душевного спокойствия пожертвовать парой-тройкой привычных программ и чуть бóльшим количеством игрушек, начав с понедельника новую жизнь, то вам идеально подойдет один из следующих вариантов:

1. "Чистая" установка одной ОС — Windows 2000.

   Пользователь, применяющий компьютер по его прямому назначению — для работы дома или в офисе, — почти не заметит никакой разницы при переходе на Windows 2000. Могут не запуститься старые игрушки, прикладные же программы, с которыми вы и будете в основном общаться, в подавляющем своем большинстве не вызовут никаких проблем. "Чис-

тая" система чаще всего свободна от "глюков", позволяет сэкономить много места на диске, обычно не возникает никаких конфликтов. Однако этот вариант неудобен тем, что придется заново переустанавливать все имеющиеся программы. Если вас это не устраивает, то вполне допускается выбрать второй вариант.

2. Обновление версии (upgrade) текущей Windows (9*x* либо NT) до Windows 2000.

   Самый, пожалуй, удобный и простой способ установки ОС, но имеющий большой недостаток — в новую систему могут попасть "глюки" из старой. Будьте также готовы, что в процессе инсталляции программа установки Windows выдаст вам список несовместимых с новой ОС приложений, тогда придется искать им достойную замену. Обновлению поддаются Windows NT Workstation 4.0, Windows NT Workstation 3.51, Windows ME, Windows 98 (98 SE), Windows 95. Тем же, кто не хочет расставаться с любимыми программами и у кого есть большой современный винчестер, нужен третий вариант.

3. Установка нескольких ОС для построения мультизагрузочной системы.

   Если у вас накопился не один десяток игр, не работающих в Windows 2000, то ничто не мешает (кроме размеров винчестера), поставить на ваш персональный компьютер две операционные системы — и Win2K, и Windows 9*x*. Такой вариант оптимален для большинства домашних компьютеров. Вы получаете одновременно и высокую надежность, и полную совместимость со всеми приложениями для Windows. При такой конфигурации следует загружать Windows 9*x* только для тех программ и игр, которые "ни в какую" не хотят запускаться в Windows 2000. Саму же Windows 2000 используйте как обычную, основную рабочую среду для "офисов", "автокадов", "фотошопов" и прогулок по Интернету — при этом вы не только обезопасите результаты своего труда, но и будете значительно лучше защищены от вторжения из Сети.

При загрузке ПК (в случае установки нескольких ОС на один винчестер) вы получите удобное загрузочное меню, в котором и будете выбирать нужную в данный момент систему. В принципе, ничто не мешает иметь на одном "винте" (винчестере) три или четыре разных ОС — от Linux до BeOS, только каждой из них необходимо отвести свой раздел. Официально же двойная загрузка поддерживается с Windows NT 3.51, Windows NT 4.0, Windows 95, Windows 98, Windows 3.1, Windows for Workgroups 3.11, MS-DOS, OS/2. Надежнее всего установить каждую ОС на собственный винчестер и управлять

загрузкой с помощью меню начальной установки CMOS SETUP. Хотя это несколько расточительно и не так удобно, как выбор из загрузочного меню.

Подготовка файловой системы

Исходя из выбранного способа установки ОС, следует определить наиболее подходящую файловую систему и заранее разбить диск на нужное количество разделов. При установке только одной ОС (Windows 2000) на мощный компьютер, думаю, оптимальным вариантом будет ее "родная" NTFS (New Technology file system — файловая система новой технологии) — она чрезвычайно надежна, работает в ряде случаев быстрее, чем FAT, и гораздо более функциональна. При этом не нужно заботиться о какой-либо предварительной подготовке диска, кроме удаления с него оставшегося от предыдущей ОС "мусора", — программа установки Windows 2000 сама предложит вам конвертировать FAT в NTFS без потери информации.

Единственная проблема, которая возникнет при переходе на NTFS, заключается в том, что тома NTFS не видны из некоторых других ОС, а значит, в случае серьезного сбоя вам будет сложно восстановить реестр из его резервной копии. Придется, например, использовать Emergency Recovery Disk (диск аварийного восстановления), системный загрузочный компакт-диск или набор дискет для восстановления системы — все это нудно и неудобно. В случае же с FAT32 все файлы реестра элементарно копируются вручную из Windows 9*x* или MS-DOS. Преобразовать же FAT в NTFS очень легко и после установки системы — достаточно набрать в командной строке следующую команду: `convert <буква_диска>: /fs:ntfs`. Если объем оперативной памяти мал, а процессор — не из самых последних, то FAT32 будет работать быстрее из-за своей простоты, поскольку специфические службы NTFS загружаются в память. Так что допускается отложить это до лучших времен: сначала установите операционную систему, программы, все настройте, и только потом переходите к NTFS. Тогда быстрое восстановление работоспособного реестра уже не будет столь важным фактором. Не забудьте, однако, при столь глубоких изменениях файловой системы зарезервировать все важные данные!

Вы можете получить подробную информацию о работе с утилитой convert, если введете команду `convert /?`. Если же вы все-таки решите остановиться на более гибкой и универсальной, но менее надежной файловой системе FAT32, то учтите, что разделы FAT32 размером более 32 Гбайт следует создавать и форматировать заранее, до установки Windows 2000. Загрузку ком-

пьютера необходимо выполнить с дискеты Windows 9*x*, поскольку Windows 2000 "не умеет" делать такие большие разделы, но с уже готовыми работает вполне нормально. В любом случае желательно предварительно подготовить диск, а не доверять это программе установки Windows 2000. В общем, выбирайте — надежность NTFS или совместимость и простота FAT32.

При серьезных сбоях обратиться к файловой системе NTFS и отредактировать, скопировать или заменить необходимые файлы можно используя программу BartPE (**http://www.nu2.nu/pebuilder**). Полезно совместно с BartPE использовать программу Acronis True Image (**www.acronis.ru**), которая позволяет делать резервные копии любого диска и восстанавливать его при необходимости.

Сложнее ситуация при построении мультизагрузочной системы. Если вы хотите использовать несколько ОС на одном винчестере, то обязательно отведите каждой из них свой логический диск. Это поможет предотвратить проблемы, возникающие при совместном использовании папки Program Files. Каждая ОС должна поддерживать формат (уметь "писать-читать-загружаться") файловой системы системного раздела винчестера. Если вы установите две системы (Windows 9*x* и Windows 2000), пусть даже в разные разделы одного диска, то загружаться они все равно будут с одного и того же раздела (вы будете выбирать ОС в загрузочном меню). Поэтому при таком варианте необходимо делать диск C: стандарта FAT32, размещать на нем Windows 9*x*, которая не поддерживает NTFS. Раздел с Windows 2000 (уже по вашему усмотрению) — стандарта NTFS либо FAT32 в зависимости от того, нужен ли вам доступ к нему из Windows 9*x* или нет. Только будьте внимательны, не преобразуйте случайно системный раздел в NTFS при установке Windows 2000. Проводите конвертирование только после установки ОС. При использовании же большего числа систем придется вообще делать загрузочный раздел самого универсального формата FAT16, его "понимает" и MS-DOS, и Linux.

Кроме того, существуют специальные программы — менеджеры загрузки типа BootMagic и System Commander. Изучите хорошенько их инструкции, программы могут показаться вам более удобными и функциональными, чем загрузочное меню Windows 2000.

Последние приготовления. Итак, все важные решения приняты, и вы точно знаете, что делаете и что хотите получить. Перед запуском программы установки Windows 2000 или перед подготовкой диска обязательно сделайте резервную копию самой важной информации, особенно если собираетесь раз-

решить системе преобразовать файловую систему на этапе установки. Учтите также, что при обновлении версии Windows NT файловая система тоже будет обновлена до NTFS 5.0, причем программа установки вас об этом даже не спросит. Возможность сбоя при этом мала, но исключать ее нельзя. Запишите отдельно всю информацию о компьютере — сетевое имя, имя рабочей группы или домена, параметры TCP/IP, всевозможные logins (логины, регистрационные имена пользователя) и пароли. Временно удалите программное обеспечение, которое может вызвать проблемы согласно результатам анализа вашего диска утилитой Windows 2000 Readiness Analizer, удалите антивирусы, а также сетевые сервисы и клиентское программное обеспечение сторонних разработчиков. При установке возможность "сжатия" дисков с помощью утилит Drivespace и Doublespace не поддерживается, поэтому проведите декомпрессию сжатых томов.

Если в компьютере есть экзотическое оборудование, то лучше вынуть его на время инсталляции — чем меньше в компьютере деталей, тем выше вероятность успешной установки. Отключите диски Iomega Jaz или аналогичные. Microsoft настоятельно рекомендует временно отключить даже блоки бесперебойного питания (вероятно, речь идет об "особо умных" UPS, подключенных к COM-портам). При "чистой" установке убедитесь, что выбранный вами способ загрузки ПК с дискеты или с компакт-диска работает.

При наличии нескольких винчестеров существует небольшая тонкость — Windows 2000 может перемешать их буквенные обозначения и даже присвоить своему разделу какую угодно букву вместо C. Чтобы такого не произошло, и система "встала" на привычный раздел C:, следует не просто отключить второй винчестер на время установки, но и снять с него питание — только тогда ОС его не найдет. Впрочем, возможно, вам будет удобнее, если Windows 9*x* всегда, при загрузке с любого диска, будет находиться на диске C:, а Windows 2000 — на диске D:.

Установка

Чтобы начать установку ОС, необходимо запустить файл WINNT.EXE (при установке из MS-DOS) или WINNT32.EXE (при установке из Windows). Находятся эти файлы в папке установочного компакт-диска. Файлов в этой папке так много, что при попытке открыть ее из DOS-оболочки типа Norton Commander вы получите сообщение о нехватке памяти и не увидите исполняемый файл — его надо будет запускать из командной строки. Если вы запускаете инсталляцию не из графической оболочки предыдущей версии

Windows, то первым делом загрузите драйвер кэширования дисков SMARTDRIVE, иначе время инсталляции будет слишком велико.

Инсталляция Windows 2000 предельно упрощена. Самая важная процедура, которую придется делать вручную, — это отвечать на некоторые наводящие вопросы, например о том, в какой раздел установить ОС и какую файловую систему для него следует выбрать. После копирования файлов и перезагрузки ПК вам придется задать также региональные установки — тут нужно выбрать все "кириллическое" и русское. Кроме того, надо будет ввести пароль администратора. Можно, конечно, оставить поле ввода пароля и пустым, но это создаст большую брешь в системе безопасности ОС — зачем тогда вообще ее устанавливать? Нежелательно также выполнять повседневную работу на компьютере, если на вкладке **Пользователи и пароли** для вас установлены права администратора — лучше зарегистрировать при первой загрузке ПК еще одного пользователя, запретив ему всё и вся, и для обычной работы входить в систему от его имени. Мастер сетевой идентификации (Network Identification Wizard), который и просит вас в обязательном порядке зарегистрировать первую учетную запись, предложит установить еще и опцию автоматического ввода пароля при загрузке ПК (**Всегда использовать следующее имя пользователя**). Не стоит ее выбирать, если не хотите пробить в системе еще одну дыру. Хотя, конечно, вводить каждый раз логин и пароль не очень хочется, особенно если за компьютером сидите только вы один. Но выбрать автоматическую регистрацию пользователя можно и позднее в настройках Windows — решайте сами, что лучше.

К сожалению, во время установки Windows 2000 Professional нет возможности выбрать компоненты ОС, которые вы не хотите устанавливать. Даже после установки системы они не появятся в списке **Add/Remove Programs** (Установка и удаление программ). Чтобы включить их отображение, уберите слово HIDE в файле C:\WINNT\INF\sysoc.inf везде, где оно встретится.

При обновлении предыдущей ОС процедура инсталляции и вовсе становится автоматической, вопросов почти не задается, хотя процесс может продлиться час и даже больше в зависимости от мощности ПК и быстродействия дисков. Программа установки перенесет в Windows 2000 почти все настройки и программы из предыдущей версии Windows. Не пугайтесь, если компьютер по 5—10 минут не будет подавать никаких признаков жизни. При обновлении версии существующей ОС до Windows 2000 необходимо запустить WINNT32.EXE под управлением предыдущей Windows и выбрать режим обновления, а не новую инсталляцию. Создать систему с двойной загрузкой тоже не очень сложно, особенно если уже имеется Windows 9*x* — просто на

этот раз, запустив WINNT32.EXE в Windows 9*x*, выберите не модернизацию системы, а новую инсталляцию в меню программы установки ОС. Не забудьте, что в этом случае нельзя разрешать преобразовывать файловую систему в NTFS, чтобы не потерять возможность загрузить Windows 9*x*. После установки вы конвертируете раздел с Windows 2000 в NTFS, оставив для загрузочного раздела FAT32 или FAT16. Для многовариантной загрузки Microsoft рекомендует такой порядок установки ОС: MS-DOS (с Windows 3.1), Windows 9*x*, Windows NT, Windows 2000. Следуя ему, вы избежите затирания загрузочного сектора предыдущей системы и получите меню выбора ОС. Можно, конечно, установить и Windows 9*x* в качестве второй ОС "поверх" Windows 2000, но заранее будьте готовы к необходимости восстановления загрузчика Windows 2000, так как он будет уничтожен.

Процедура установки Windows XP практически не отличается от описанной выше.

Установка Windows Vista

Если вы только что приобрели компьютер, то обычно достаточно вставить диск, чтобы началась установка операционной системы. Следует, правда, уточнить, какой диск и куда следует вставлять. Дистрибутив Windows Vista распространяется на DVD-дисках. Диски — загрузочные. Следовательно, компьютер должен иметь дисковод, который может читать DVD-диски. Для большинства современных компьютеров это обычная составляющая. Если вы решили использовать старый компьютер, несколько модернизировав его, то обратите внимание на эту деталь. Кроме того, в отдельных случаях, если компьютер не имеет наклейки о совместимости с Vista, может потребоваться обновление BIOS (базовая система ввода-вывода) для повышения стабильности работы системы. Вот здесь следует быть максимально осторожным. Версию BIOS для обновления всегда можно найти на сайтах производителей материнских плат. Обязательно сохраните резервную копию BIOS вашей старой версии. Если что-нибудь не заладится при установке Vista на ваш не очень новый компьютер, его можно продолжать использовать под управлением Windows XP. Но вероятна такая ситуация, когда Windows XP не будет устанавливаться после обновления BIOS. Причем, уже установленная система будет продолжать работать. Если вы не устанавливали Windows Vista в качестве второй системы, и Windows XP необходимо установить заново, то придется вернуть BIOS той версии, что была ранее установлена. При этом

необходимо иметь программу для перезаписи BIOS, которая будет работать с загрузочной дискеты.

Если вы сами не уверены, что сможете произвести процедуры обновления BIOS без ошибок, то лучше доверьте эти процедуры опытным пользователям ПК, объяснив им, для чего это необходимо выполнить. Начинать обновление BIOS есть повод только в том случае, если вы обнаружили, что Windows Vista работает нестабильно, без всякой видимой причины появляется синий экран с указанием на неизвестную ошибку системы, а после перезагрузки в журналах системы не обнаруживается никакой информации о сбое, которая помогла бы выявить его причину. Но будем надеяться, что у вас не возникнет необходимости в таких сложных для начинающих пользователей действиях.

Применив дистрибутив, специально локализованный для России, вы увидите процесс установки на русском языке, и практически никаких решений во время установки вам принимать не придется. Если же предполагается использование дистрибутива английской версии, а затем самостоятельная локализация с помощью языкового пакета, то вы встретитесь с процессом установки, описанным далее.

После вставки диска и начала загрузки с него появится надпись "Windows is loading files…" ("Идет загрузка файлов") и индикатор выполнения в виде белой полосы.

> ***Примечание***
>
> Требуется нажать любую клавишу для начала загрузки с DVD-диска, если есть другие варианты загрузки, когда на вашем компьютере установлена другая версия операционной системы. Конечно, в BIOS Setup должна быть установлена загрузка с CD или DVD.

Следует просто подождать, пока завершится загрузка файлов, о чем и сообщает надпись на экране.

Если установка не началась, следует просто поправить установки в BIOS Setup (настройки BIOS). Для этого в начале загрузки компьютера необходимо нажать клавишу <Del> или <F2>. Это наиболее часто встречающиеся способы входа в BIOS Setup. После входа в программу настройки BIOS найдите вкладку или раздел **Boot**. В нем в зависимости от версии BIOS тем или иным способом должен быть указан порядок загрузки. Это может быть список дисков, в котором можно изменить порядок следования записей, а может быть одно поле, в котором перечислены варианты загрузки одной строкой.

В большинстве случаев порядок записей в списке или выбор строки в поле выполняется клавишами <+> или <–> на цифровой части клавиатуры. Обычно, чтобы выбор был возможен, требуется выделить элемент списка или поле, "встав" на него, перемещаясь по экрану с помощью клавиш со стрелками или клавишей <Tab>. Первым в списке или в строке должен быть дисковод компакт-дисков. Он может обозначаться как **CD**, **CD-ROM**, **CD-ROM Drive**. Вероятно, возможны и другие варианты, но всегда понятно, о каком диске идет речь. После установки правильного порядка загрузки нажмите последовательно клавиши <Esc>, <F10> и <Enter>. Компьютер перезагрузится и, если в дисководе вставлен установочный диск Windows Vista, попытается с него загрузиться. При исправном дисководе и диске начнется загрузка и установка системы.

Программа установки системы продумана очень хорошо. Возможны два варианта установки системы: установка "с нуля" и обновление системы, если у вас уже была установлена более ранняя или менее функциональная ее версия. Причем, обновление возможно, если запустить программу установки из-под уже загруженной Windows Vista.

Если, загрузившись с DVD-диска, выполнить установку поверх ранее установленной версии Windows Vista, то программа установки сохранит все документы и файлы ранее установленной системы. Это предотвратит потерю важной для вас информации, если вы забыли сохранить ее на другом носителе.

Установка "с чистого листа" всегда более надежна. В систему не смогут проникнуть ошибки из ранее установленной системы, но программы, которые были установлены, придется установить снова. Мы предполагаем, что на вашем компьютере Windows Vista еще не устанавливалась, соответственно, установка проводится "с нуля" на новый винчестер.

После загрузки файлов начнет работу программа установки.

На этом этапе следует выбрать языковые параметры системы. Если вы живете в России, то выбирайте формат времени и чисел (**Time and currency format**) — **Russian** и параметры клавиатуры или метод ввода (**Keyboard or input method**) — **Russian**. После нажатия кнопки **Install now** (Установить сейчас) начнется собственно установка системы.

Для того чтобы была возможна активация системы после установки, необходимо ввести ключ продукта (Product key) (дефисы при вводе ключа подставляются автоматически). Если вы не уверены в необходимости автоматической активации системы после установки, снимите флажок **Automatically**

activate Windows when I'm online (Автоматически активировать Windows, когда я подключен к Интернету). Дело в том, что число активаций ограничено, и если вам не понравится работа системы на данном компьютере, вы сможете ее переустановить на другую машину. Для оценки необходимости переустановки или активации у вас будет 30 дней.

Для удобства ввода ключа продукта предусмотрена экранная клавиатура.

Если вы не введете ключ продукта, то программа установки попросит вас подтвердить, что вы согласны переустановить систему после приобретения. Но взамен вы получите возможность ознакомиться с любой версией системы. Дистрибутив обычно содержит все версии, и вы сможете выбрать интересующую вас для ознакомления. Период ознакомления, конечно, 30 дней. Возможность ознакомиться с любой версией Windows Vista может быть полезной для принятия решения о необходимости приобретения более полнофункциональной версии, чем та, которую вы уже имеете.

После ввода ключа продукта программа установки предложит прочитать и принять лицензионное соглашение. Вы будете предупреждены, что при желании обновить систему вы должны начать установку из-под Windows. Если выбрать продолжение установки, потребуется указать диск, на который будет установлена система.

Если диск был отформатирован заранее, то начнется копирование файлов, в противном случае диск будет подготовлен и отформатирован перед началом копирования файлов, но процесс будет идти скрытно от вас.

Все дальнейшие действия программа выполнит самостоятельно, информируя вас о состоянии процесса установки выделением строк с описанием текущего процесса установки и отображая в нижней части экрана индикатор выполнения установки.

Установка может продлиться довольно долго. Если есть подключение к Интернету, которое система сможет использовать в процессе установки, то автоматически будут установлены и самые необходимые обновления. После завершения установки компьютер будет автоматически перезагружен. Теперь останется выбрать имя пользователя, ввести придуманный для него пароль и выбрать пиктограмму. Для ввода имени и пароля латиницей достаточно нажать сочетание клавиш <Alt>+<Shift>. Нажав кнопку **Next**, мы попадем в окно настройки защиты Windows. Для начинающих лучше выбрать вариант, предложенный системой, — **Use recommended settings** (Использовать рекомендуемые установки).

До полного завершения установки остается совсем немного. Остается установить правильные значения даты, времени и часовой пояс.

В окне **Set Up Windows: Select your computer current location** (Установка Windows: выбор расположения вашего компьютера) следует указать, в какой сети находится компьютер. Это окно появится только в том случае, если компьютер действительно подключен к сети. Скорее всего, ваш компьютер находится в домашней сети, что и выберем. И наконец, долгожданное **Thank you** (Спасибо!) после полного завершения установки.

Осталось нажать кнопку **Start** (Пуск) для начала работы с установленной системой.

Весь процесс установки у вас может занять от часа до трех часов (зависит от параметров компьютера). Но после загрузки системы при наличии подключения к Интернету тут же будет предложено загрузить и установить последние обновления. Для Windows обновления никогда не были лишними. Если подключение к Интернету позволяет загрузить предложенный объем информации, то согласитесь и обновите систему.

Если подключение к Интернету не настроено, вы можете выполнить обновления позднее, отказавшись пока от их загрузки. На экране появится окно центра настройки компьютера. Но это уже не установка системы, а начало работы в ней.

Единственное, о чем еще следует сказать, — это локализация. Для локализации английской версии системы для России требуется языковый пакет. После установки системы следует в **Control Panel** (Панель управления) найти апплет **Regional and Language Options** (Язык и региональные стандарты). В нем на вкладке **Keyboard and Languages** (Языки и клавиатуры) найти кнопку **Install/Uninstall Languages** (Установить или удалить язык). Далее потребуется только указать расположение пакета русификации и подождать завершения его установки.

После перезагрузки в поле **Choose Display Language** на вкладке **Keyboard and Languages** (Языки и клавиатуры) следует выбрать язык **русский**. Теперь достаточно выйти и снова войти в систему, и язык системы будет изменен.

Если вы использовали русскую версию дистрибутива, то изменить язык системы на английский, вероятнее всего, не получится. Языковый пакет для английского языка, по информации, предоставленной сотрудниками Microsoft, не существует. Он просто сразу встроен в английскую версию.

Об установке Linux

Пожалуй, подробно описывать установку современных версий Linux не имеет большого смысла. Программы установки очень хорошо отработаны, всегда есть возможность выбрать язык программы установки. Перед установкой системы программа может предложить модифицировать разделы винчестера и подготовить разделы для установки системы. В большинстве случаев все, что предлагается по умолчанию подходит для тех, кто впервые столкнулся с установкой Linux.

В процессе установки, как и при установке Windows, потребуется ответить на несколько вопросов.

Дистрибутивы Linux распространяются не только на дисках, но и в виде файлов-образов. Скачав такой файл из Интернета, вы можете создать установочный диск с помощью, например, программы Nero или использовать сам образ для установки системы на виртуальный компьютер, который может быть создан с помощью, например, программы VMware Workstation (**http://www.vmware.com/products/ws/**).

Последний вариант установки позволяет изучить возможности незнакомой системы перед ее использованием на отдельном компьютере. Виртуальный компьютер может работать в локальной сети так же, как и реальный.

Установив систему на два или более компьютера или имея не менее двух компьютеров с установленной сетевой ОС, можно начинать создание сети.

Монтаж сети

Познакомившись в общих чертах с составляющими деталями нашей сети, попробуем собрать ее простейший вариант. Рассмотрим две среды передачи данных — коаксиальный кабель и витая пара. Каждая из них имеет право на жизнь, и только вы сами сможете решить, с чего начать, но вполне возможно, что вам потребуются оба вида кабеля. Готовясь к прокладке кабеля, необходимо позаботиться о приобретении или изготовлении вспомогательных принадлежностей, без которых прокладка и сборка сети окажутся затруднительными.

Прежде всего инструменты. В приведенных далее разделах помещено описание инструментов, применяемых при монтаже сетей. Не все инструменты понадобятся вам для работы с сетью. Но в будущем, если вам придется вести

более сложный и трудоемкий монтаж, то для быстрого и качественного проведения работ потребуется профессиональный инструмент.

Прокладка кабеля

При создании "домашней" сети вам придется тянуть кабель с дома на дом или из подъезда в подъезд через чердак/крышу/подвал (по улице это делать нецелесообразно — инициативные любители ножниц могут постараться). Чердак/крыша/подвал обычно закрыты на ключ, который, как правило, лежит в хорошо защищенном ящике у злобной тетушки — охранницы общественного спокойствия. Вам необходимо корректно этот самый ключ у нее попросить. Очень часто вас могут отослать в РЭУ, а оттуда — к более высоким властям (например, к главному управляющему района) для визирования бумаги о том, что вы собираетесь только протянуть свой кабель и ничего больше (а то обрезанную кем-нибудь ТВ-антенну обязательно "повесят" на вас). Рекомендуется сделать следующее: пойти в РЭУ, узнать адрес вышестоящей инстанции жилищного хозяйства, и уже у них просить разрешение, ссылаясь на то, что вот ребятам оттуда-то (район/улица) уже дали такую бумагу (при этом желательно иметь на руках аналогичную, но уже подписанную бумагу, позаимствованную на время у тех, у кого она реально есть). Также рекомендуется в разговоре с властями изображать из себя активную молодежь, которая не курит, не пьет, а "тянет сети", поскольку тогда, при удачном стечении обстоятельств, вам могут помочь не только ключами, а еще чем-нибудь полезным. Правда, такие исключения бывают редко. Перед тем как делать большую сеть, рекомендуется пообщаться с теми, кто ее уже сделал и у кого она есть. Они вам точно скажут, как, что и где взять и что делать.

Пользуйтесь опытом уже набивших шишки, а главное, по-человечески общайтесь с властями. Не факт, что вам уже на следующий день дадут разрешение или ключи. Все это может затянуться и на месяц, и на больший срок. Главное — терпение, и все будет. Проверено. (Рекомендации ведущих собаководов.)

В принципе, можно обойтись и без всех этих процедур, действуя нелегально. В этом случае не факт, что ваш кабель случайно не обрежут "мастера" или "инициативные любители колюще-режущих предметов", либо какая-нибудь внезапно приехавшая комиссия не "настучит вам по голове".

Получив ключи, можно приступить к осмотру открывшихся просторов.

Техника безопасности

При монтаже сети следует соблюдать следующие меры безопасности:

- ❒ не "тянуть сеть" в дождь либо после дождя;
- ❒ не "тянуть сеть" вечером и ночью;
- ❒ не использовать неизолированный провод;
- ❒ обязательно использовать устройства типа APC (Automatic Power Control — автоматическая регулировка мощности) ProtectNet, защищающие сеть от перенапряжения и спасающие во время грозы (известен случай, когда во время грозы от перенапряжения полностью выгорел один компьютер, а у второго сгорела сетевая карта). Такое устройство — штука хоть и дорогая, но очень нужная (выгоревшее оборудование будет стоить гораздо больше).

Прокладка кабеля по воздуху

Первый вариант прокладки кабеля, который мы рассмотрим, — воздушный, т. е. с крыши на крышу. Принимая за основу описанный выше метод построения сети, нам необходимо перекинуть магистраль с крыши одного дома на крышу другого. Это можно сделать:

- ❒ при помощи лесы/нити с грузом;
- ❒ при помощи стреляющих устройств;
- ❒ при помощи сильно "продвинутых" игрушек.

В первом случае берется нить/леска с привязанным к ней грузом (не очень большой, но и не очень маленькой массы) и спускается с крыши одного дома на землю. С крыши второго дома спускается кабель, к которому привязывается спущенная нить. Затем, получив разрешение на подъем, человек на крыше первого дома начинает вытягивать нить на себя, поднимая, таким образом, вместе с нитью и кабель. Здесь существует проблема: кабель может запутаться в кроне деревьев (или зацепиться за строения, фонарные столбы и т. п.), что доставит немало хлопот. Поэтому перед тем, как протягивать кабель, необходимо максимально очистить его будущий путь. С проводами на столбах проблема решается заранее — как только вы спустили нить с грузом вниз и направились в сторону другого дома, вам необходимо перекинуть груз и нить через всевозможные висящие препятствия. С деревьями несколько сложнее, поскольку, по себе знаю, исполнять роль новоиспеченной "тарзан-

ки" не очень легко, хотя и возможно. Другие препятствия можно обойти сбоку, соответственно, с ними особых проблем возникнуть не должно.

Во втором случае на помощь "сететянульщикам" приходят всевозможные стреляющие приспособления типа арбалета и ему подобных. К стреле арбалета привязывается нить, разложенная на крыше (для легкости разматывания), после чего производится выстрел в сторону нужного здания. Правда, в случае использования арбалета есть риск, что:

- попадешь в ловяще-тянущего напарника, стоящего на другом доме;
- попадешь кому-нибудь в окно;
- вообще никуда не попадешь.

Поймав нить на другом конце, привязываем к ней кабель и тянем. Цель достигнута.

В третьем случае нить и груз переносятся на крышу другого дома при помощи летучих игрушек наподобие вертолета. Вертолет с радиоуправлением прекрасно выполняет свою роль, правда, возможно, что:

- ловяще-тянущий напарник случайно попадет под винт, в результате чего ему будет не очень хорошо;
- внезапно налетевший поток ветра затруднит полет, и несчастная игрушка спикирует в "ракушку" с шестисотым "мерсом";
- из-за запутавшейся нити вертолет может просто упасть вниз со всеми вытекающими последствиями.

Поймав нить, поступаем так же, как и в случае с арбалетом.

Возможно и такое: если один дом выше другого, и между ними есть соединение, например радиолиния (но никак не "высоковольтка", т. е. не ЛЭП (линия электропередач) и даже не линия с напряжением 380 В) или линия с напряжением 127 В, то, используя хитроумное приспособление "крючок", можно спустить нить с грузом по этому проводу.

Кстати, желательно предупредить жильцов квартир, которые могут наблюдать за вашими действиями из окон, чтобы они, не дай бог, не вызвали милицию (особо инициативные ведь и не такое могут сделать). Еще одной проблемой могут стать вездесущие бабуси (обитающие у подъездов), которым всегда... ну, в общем, сами знаете.

Итак, способы — перед глазами, выбор — за вами. Меня, например, больше устраивает первый.

Перекинутый с дома на дом кабель не должен висеть сам по себе, его нужно закрепить на растянутом тросе, который, в свою очередь, надежно закреплен на обеих крышах. Крепить следует при помощи полиэтиленовых стяжек (продаются в хозяйственном магазине). Многие в качестве закрепителя используют скотч либо металлические скобы, но:

- ❒ после зимы скотч приходит в не совсем годное состояние;
- ❒ металл ржавеет, а кабелю от этого не лучше.

Полиэтиленовые стяжки позволяют кабелю быть не "намертво" притянутым к тросу, что соответствует основному правилу крепления кабеля — он не должен быть натянут и сжат.

В качестве троса можно использовать:

- ❒ "полевку" (полевой сдвоенный военный кабель);
- ❒ тросик 0,5 мм для протяжки;
- ❒ все, что только пожелаете, лишь бы было прочно.

"Полевка" хорошо зарекомендовала себя еще с военных времен, она недорого стоит и прекрасно выдерживает погоду и достаточно большой вес (до тонны на 100 м) — ну чем не "наш выбор"?

Стандартный стальной тросик может быть неудобен из-за следующих особенностей:

- ❒ не изолирован, необходима обязательная изоляция;
- ❒ подвержен ржавчине.

В принципе, никаких стандартов и ограничений на вид и модель троса для подвешивания нет, поэтому главное правило, которым стоит руководствоваться, — выбирать изолированный непромокающий (не веревку — сгниет) провод.

Прокладка кабеля под землей

Следующий способ прокладки кабеля — через подвалы и городские подземные коммуникации. Особых рекомендаций и пожеланий здесь вы не найдете, поскольку главное требование — правильное крепление кабелей, чтобы они не болтались и не провисали. Крепить лучше к стенам и их подобиям, желательно подальше от высоковольтных проводов и помехонезащищенных каналов. При прокладке через коммуникационные люки у вас могут возникнуть проблемы с правоохранительными органами, поэтому такие вещи лучше

проделывать в сопровождении сертифицированного специалиста (да, есть и такие). Вообще-то, без карты подземных коммуникаций в люки лучше не лазить, а то ничем хорошим это не закончится.

Не следует также забывать, что с властями необходимо договориться и по этому поводу — попросить карту, подыскать людей в помощь. Главное, чтобы вы к ним хорошо, и они к вам... так же.

По поводу копания: если между домами не асфальт, можно, конечно, прокопать канаву и уложить кабель в нее, но тут никто не застрахован, что лопнувшая в этом месте труба не соберет вокруг себя кучу угрюмых дяденек с лопатами, которые во время раскопок повредят (если повезет), а то и вообще выкопают и обрежут ваш кабель, как мешающий работе.

Предостережения и рекомендации по защите — такие же, как и в случае с перекидыванием кабеля с крыши на крышу.

Прокладка кабеля в подъездах

И вот кабель, наконец-то, перекинут, магистраль создана. Остается одна из мелких трудностей — разводка по подъездам. При условии, что на каждый подъезд была заготовлена магистральная петля, теперь необходимо разместить на чердаке хаб, который следует ставить в разрез петли. Сами хабы нужно ставить в защищенных помещениях на последних этажах (чтобы не ходили посторонние), доступ в которые был бы только у вас и вашей команды. Эти помещения также должны быть защищены от внешних раздражителей (солнце, протекание крыши и т. п.) и хорошо вентилируемы. Такие комнаты в дальнейшем могут использоваться в качестве компьютерных комнат, где будут стоять отдельные серверы.

Установив хаб в удобном месте, можно начинать спуск кабелей вниз по этажам. Многие считают, что кабели нужно спускать через вентиляционные шахты, мусоропровод и другие доступные ходы. Могу сказать только одно: это заблуждение. В каждом доме, там, где "обитают" низковольтные провода (ТВ, радио, телефон), всегда есть несколько свободных труб, которые можно использовать для достижения наших целей. Стоит отметить, что если вы взяли не стандартный кабель, а его замену, то ваша сеть может работать со сбоями либо создавать наводки в соседних кабелях. Это, в свою очередь, вызовет недовольство жителей (вы представляете, какая-то там сеть помешала мне нормально досмотреть 584-ю серию "Санты-Барбары"!), которые вызовут электрика дядю Васю, который просто вырежет "ненужные", по его мнению, кабели. Но это я так, к слову.

Выловив кабель из трубы на необходимом этаже, дотянуть его до квартиры, я думаю, проблем не составит. Подключив все нужные соединительные шнуры, разъемы и кабели, можете считать работу выполненной.

Резка и разделка кабеля

Для быстрой и ровной обрезки телефонных и коаксиальных кабелей, а также кабелей питания без заломов и повреждений изоляции жил используются кабельные ножницы, которые называются "кабелерезы". Лезвия ножей специального профиля предотвращают выдавливание кабеля при резке, а длинные ручки позволяют осуществить операцию без значительных усилий. Следует отметить, что резка оптического кабеля, особенно усиленного стальным тросом, требует применения специального "кабелереза".

Снятие внешней изоляции в кабелях категории 3 или 5 осуществляется с помощью комбинированного инструмента. Разделка обычных и бронированных магистральных кабелей выполняется специальными ножами-пилами или ножницами из закаленной стали, а обрезка волокон кевлара — ножницами с керамическими лезвиями.

Обрезку жил и снятие изоляции удобнее всего выполнять комбинированным инструментом, имеющим несколько калиброванных пазов. Если работа ведется с одним видом провода, то специальный инструмент можно настроить под требуемый диаметр провода регулировочным винтом или кулачком. При обработке большого количества жил небольшого сечения лучше применять специализированный высокопроизводительный инструмент, который приводится в действие простым нажатием рукоятки. Такой инструмент обеспечивает настройку на необходимый диаметр и длину снимаемой изоляции, а кроме того, он имеет встроенный нож для обрезки проводов.

Надежность соединений коаксиального кабеля с разъемами непосредственно зависит от качества его разделки. Экономичное решение — применение простейших приспособлений, обеспечивающих заданную глубину разрезания оболочки для определенного типа кабеля. Разделка кабеля с помощью таких приспособлений осуществляется за несколько итераций. Профессиональный инструмент позволяет зачистить кабель за одну операцию. Кабель достаточно поместить в кассету, сделать один полный оборот и снять подрезанную часть изоляции и экрана. Для получения нужного профиля зачищаемого кабеля в кассету устанавливается необходимое число сменных лезвий, каждое из которых настраивается на требуемую глубину разреза.

Расшивка на кросс

Для расшивки проводов (жил) кабеля на кросс применяется специальный инструмент, который вдавливает провод в разрез контакта плинта и, если это необходимо, осуществляет обрезку остатка провода. Его экономичный вариант обеспечивает работу только с одним типом плинтов кросса. Универсальный инструмент позволяет обрабатывать плинты различного типа (66, 110, KRONE, BIX и др.) с помощью сменных головок.

Профессиональный вариант имеет пружинный механизм, обеспечивающий равномерность усилия при вдавливании провода в контакт плинта и удар в конце для обрезки. Ручка инструмента оснащена пеналом для хранения одного запасного лезвия, а также приспособлениями для извлечения проводов из контактов плинтов и плинтов из держателей. В набор головок расширенного инструмента включены отвертка, шило, кернер, адаптер для 1/4-дюймовых шестигранных отверток и торцевых ключей.

Для обеспечения высокой производительности работ при расшивке кабельных окончаний структурированных кабельных систем на контакты типа 110 может использоваться ручной или электрический инструмент групповой обработки, обеспечивающий одновременную обработку всех восьми проводников.

Расшивка кабелей на специализированные соединители типа RJ-45 для установки в "подрозетники" (гнезда под розетки) кабельных каналов выполняется, как правило, инструментом, поставляемым их фирмой-производителем.

Поиск нужного провода среди выполненных кросс-соединений удобнее всего вести специальным щупом. С его помощью можно аккуратно раздвигать провода, вытаскивать нужные из них, проверять качество расшивки.

Монтаж разъемов опрессовкой

Для монтажа модульных разъемов RJ-22 (4P4C), RJ-11 (6P2C), RJ-14 (6P4C), RJ-25 (6P6C) опрессовкой применяется специальный инструмент. Он позволяет выполнить все операции: от разделки модульных двух/четырех/шестипроводных телефонных шнуров до опрессовки на них разъемов. Обрезка шнура, снятие внешней изоляции и опрессовка выполняются отдельно, различными рабочими органами. Инструменты отличаются типом обрабатываемых разъемов и сроком службы. В качестве экономичного варианта для мелких ремонтных работ можно использовать пластмассовый инструмент.

Профессиональные инструменты выполнены из металла, а качество опрессовки достигается за счет движения пуансонов строго перпендикулярно к поверхности разъема за счет специальной конструкции рабочего органа. Опрессовка разъемов на коаксиальных кабелях выполняется аналогичным инструментом за несколько операций. Как правило, этот инструмент не имеет встроенных средств зачистки кабеля.

Аналогичный комбинированный инструмент для монтажа электропроводки служит для выполнения всех операций. Он имеет рабочие органы для обрезки, зачистки жил кабеля, обжимки неизолированных клемм и наконечников, а также для укорачивания болтов, шпилек и винтов без нарушения их резьбы. Все рабочие поверхности маркированы сообразно их назначению. Большая длина ручек обеспечивает удобство работы и небольшое рабочее усилие при опрессовке.

Кроме этого, множество инструментов предназначено специально для опрессовки контактов различных разъемов, например разъемов для плоских кабелей и разъемов типа D и D-SUB, широко применяемых в компьютерах. При необходимости, совместно с этим инструментом используются приспособления для установки контактов в корпуса разъемов и их съемки.

Пайка

Выполнить пайку в местах, где работа с обычным электрическим паяльником неудобна или невозможна, можно газовым паяльником. Топливом служит обычный газ для зажигалок. Время работы при полной заправке достигает 120 минут. Заправленный паяльник всегда готов к работе, легко поджигается и нагревается за 30 секунд. Поджиг паяльника осуществляется кремниевой или пьезоэлектрической зажигалкой. Подстройка мощности в диапазоне 10—60 Вт производится с помощью регулятора подачи газа.

Совместно с паяльником могут использоваться насадки: высокотемпературная горелка с пламенем температурой до 1300 °С для легкой сварки и пайки высокотемпературными припоями, нагнетатель горячего воздуха с фокусированным потоком воздуха температурой до 620 °С без пламени для обработки термоусадочных муфт небольшого размера и размягчения пластмассовых деталей перед сгибанием, горячий нож для обрезки или подрезания синтетических тросов и листовых материалов. Для удобства переноски паяльники снабжены защитным колпачком или футляром с аксессуарами. Профессиональные паяльники отличаются исполнением корпуса (из пластмассы

или нержавеющей стали), наличием автоподжига, а также набором жал и насадок. В нерабочем положении колпачок полностью закрывает жало паяльника и блокирует включение подачи газа. Благодаря небольшим габаритам и клипсе на колпачке паяльник удобно носить в кармане. В футляре помимо набора насадок имеется подставка и чистящее приспособление для жала.

Общие замечания

В любом случае отвертка плоская и крестовая, пассатижи, острый нож у вас должны быть обязательно. Хорошо, если есть возможность приобрести специализированный универсальный инструмент для обжима разъемов RJ-45 и разделки кабеля типа "витая пара" (рис. 2.9), но можно обойтись и без него. Для разделки кабеля типа "витая пара" необходимо, сняв наружную изоляцию на концевом участке кабеля длиной 12,5 мм и расплетя кабель, ввести обработанный конец кабеля в разъем RJ-45, соблюдая расположение жил в соответствии с таблицей разводки. Монтаж разъемов RJ-45 можно осуществить, применяя тонкую отвертку, утапливая контакты и фиксатор провода. Необходимо только принять меры предосторожности для предохранения от излома фиксатора разъема. Изоляцию с жил кабеля снимать не нужно. Контакты разъема при обжиме проткнут ее, и надежное соединение будет обеспечено.

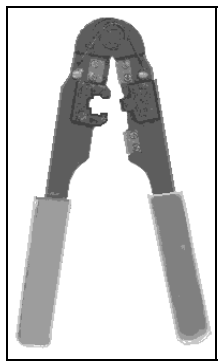


Рис. 2.9. Специализированный инструмент для обработки UTP-кабеля типа "витая пара" и обжима разъемов RJ-45

Следует также быть готовым к проведению работ по прокладке кабеля как внутри помещения, так и, возможно, через перегородки, потолочные перекрытия или между строениями. Для этих целей понадобятся инструменты,

применяемые в строительстве, такие как дрель, перфоратор и пр. Для крепления кабеля на стенах или плинтусах нужны пластиковые хомутики, а для протяжки кабеля по воздуху между строениями потребуется проволока или трос, за который можно закрепить кабель, чтобы исключить его повреждение при натягивании. Применение дополнительного оборудования, такого как хабы, повторители и пр., потребует крепления приборов на стенах или установку их на подготовленные заранее полки, стойки или кронштейны. Перечень необходимых инструментов далеко не полный, но разнообразие ситуаций и потребностей настолько велико, что лучше, ориентируясь на эту краткую информацию, решить самостоятельно, что конкретно понадобится вам для проведения работ.

На сайте **http://homenetworks.ru** помещен рассказ неизвестного автора под названием "Нитворк нейбахуд, или Домашняя сеть по-русски", в котором он делится опытом по протяжке и прокладке кабеля в разнообразных условиях.

Монтаж сети с использованием тонкого коаксиального кабеля

Это вариант сети по технологии Ethernet, стандарту 10Base-2 (шинная топология). Отличается простотой и отсутствием в конструкции хабов.

Для монтажа понадобятся:

- ❒ две сетевые карты с разъемами BNC, например Realtec RTL8029 Ethernet Adapter (если они еще не установлены в компьютеры);
- ❒ два тройника BNC (Т-коннекторы). Обычно продаются в комплекте с адаптерами, но могут приобретаться и отдельно;
- ❒ коаксиальный кабель с волновым сопротивлением 50 Ом. (Не используйте телевизионный антенный кабель, он абсолютно не подходит для нашего случая!) Длина кабеля не должна превышать 185 м, но вам, вероятнее всего, понадобится меньше. Необходимо измерить путь, по которому будет проложен кабель, и добавить к полученной величине еще три-пять метров на случай перемещения компьютеров;
- ❒ два разъема BNC на концы кабеля. Разъемы отечественного производства могут требовать пайки при соединении с кабелем. Импортные коннекторы пайки не требуют, надежность контакта в месте соединения обеспечивается обжимом кабеля;
- ❒ два терминатора.

Если все есть, приступаем к монтажу.

1. Аккуратно, не допуская повреждений, резких изломов и перекручивания, прокладываем кабель по выбранному пути. Запас длины равномерно распределяем на оба конца кабеля.

2. На концах кабеля закрепляем разъемы. Для этого кабель необходимо подготовить следующим образом:

   - аккуратно отрежьте так, чтобы его торец был ровным. Наденьте на кабель металлическую муфту (отрезок трубки), который поставляется в комплекте с BNC-разъемом;

   - снимите с кабеля внешнюю пластиковую оболочку на длину примерно 20 мм. Будьте аккуратны, чтобы не повредить по возможности ни один проводник оплетки;

   - оплетку аккуратно расплетите и разведите в стороны. Снимите изоляцию с центрального проводника на длину примерно 5 мм;

   - установите центральный проводник в штырек, который также поставляется в комплекте с разъемом BNC. Используя специальный инструмент, надежно обожмите штырек, фиксируя в нем проводник, либо впаяйте проводник в штырек. При пайке будьте особенно аккуратны и внимательны — плохая пайка через некоторое время станет причиной отказов в работе сети, причем локализовать это место будет довольно трудно;

   - вставьте центральный проводник с установленным на него штырьком в тело разъема до щелчка. Щелчок означает, что штырек "сел" на свое место в разъеме и зафиксировался там;

   - равномерно распределите проводники оплетки по поверхности разъема, обрежьте их до нужной длины, если необходимо. Надвиньте на разъем металлическую муфту;

   - аккуратно обожмите муфту специальным инструментом (или плоскогубцами) до тех пор, пока не будет обеспечен надежный контакт оплетки с разъемом. Не обжимайте слишком сильно — есть опасность повредить разъем или пережать изоляцию центрального проводника, что может привести к неустойчивой работе всей сети. Но и слишком слабо обжимать тоже нельзя — плохой контакт оплетки кабеля с разъемом также приведет к отказам в работе.

3. Вставляем в компьютер сетевую карту (если еще не вставили). Включаем компьютер и устанавливаем, если это необходимо, драйвер адаптера (необходимости может не быть, если Windows сама обнаружит драйвер у себя). Вставляем по требованию компьютера диск с дистрибутивом Windows, перезагружаем компьютер и до некоторых пор выключаем. Повторяем эти действия со вторым компьютером.
4. Надеваем на разъем сетевой платы тройник. Разъем, закрепленный на кабеле, подключаем к одному концу тройника, а к другому присоединяем терминатор. То же повторяем для второго компьютера.

Все готово для пробного запуска и настройки. Но об этом несколько позже, а сейчас рассмотрим вариант сети на витой паре.

Монтаж сети с использованием витой пары

Для двух компьютеров хаб пока не нужен. Потребуются:

- ❒ две сетевые карты с разъемами RJ-45, например Realtec RTL8029 Ethernet Adapter (если они еще не установлены в компьютеры);
- ❒ два разъема RJ-45 (вилки). Если в дальнейшем предполагается строить сеть на витой паре, то желательно приобрести обжимной инструмент для закрепления разъемов на концах кабеля. В противном случае можно обойтись и отверткой с плоским жалом;
- ❒ кабель "витая пара" категории 5. Длина кабеля не должна превышать 100 м, но вам, вероятнее всего, понадобится меньше. Необходимо измерить путь, по которому будет проложен кабель, и добавить к полученной величине еще три-пять метров на случай перемещения компьютеров.

Последовательность действий следующая:

1. Аккуратно, не допуская повреждений, резких изломов и перекручиваний, прокладываем кабель по выбранному пути. Запас длины равномерно распределяем на оба конца пути. На концах кабеля закрепляем разъемы, соблюдая соответствие нумерации контактов разъемов цвету жил кабеля (табл. 2.5). Необходимо учесть, что в таком варианте разделки кабеля мы получим cross-over-кабель (cross-over — перекрестный), который впоследствии можно использовать либо для прямого соединения компьютеров, либо для подключения компьютера к IN-порту хаба при недостатке мест подключения. Поэтому, если компьютеры будут располагаться далеко друг от друга, есть смысл первичные настройки провести с коротким ка-

белем по приведенной схеме разделки. Когда настройка будет завершена, определите место расположения хаба, к которому будут подключены первые два компьютера, и от него проложите два кабеля к каждому из них. Но разделка кабеля в этом случае должна проводиться по схеме "один-к-одному", т. е. номер контакта, от которого жила кабеля отходит с одного конца, должен совпадать с номером контакта разъема на другом конце кабеля (см. табл. 2.5).

2. Вставляем в компьютер сетевую карту (если еще не вставили). Включаем компьютер и устанавливаем, если это необходимо, драйвер адаптера (необходимости может не быть, если Windows сама обнаружит драйвер у себя). Вставляем по требованию компьютера диск с дистрибутивом Windows, перезагружаем компьютер и на некоторое время выключаем. Повторяем эти действия со вторым компьютером.

3. Втыкаем разъемы кабеля в розетки сетевых карт до щелчка. Все готово для пробного запуска и настройки. Но об этом несколько позже.

Таблица 2.5. *Разводка кабеля*

Разъем 1	Цвет провода	Разъем 2
Кабель на две пары		
1	Бело-оранжевый	3
2	Оранжевый	6
3	Бело-синий	1
6	Синий	2
Кабель на четыре пары		
1	Бело-зеленый	3
2	Зеленый	6
3	Бело-оранжевый	1
4	Синий	4
5	Бело-синий	5
6	Оранжевый	2
7	Бело-коричневый	7
8	Коричневый	8

Проверка правильности подключения

Если после монтажа сеть не работает, проверьте:

- стоят ли на обоих концах магистрали терминаторы (на коаксиальном кабеле);
- не разорвана/придавлена/расплющена ли в каком-нибудь месте магистраль;
- включено ли питание у хабов;
- воткнуты ли все провода в хаб;
- соединен ли хаб с магистралью;
- воткнут ли сетевой кабель в компьютер (не 220 В, а сетевой кабель, хотя и наличие 220 В тоже не мешало бы проверить);
- правильны ли установки port и IRQ у сетевой карты.

В случае если все нормально, но сеть все равно не работает, следует обратиться к более компетентным людям либо к системным администраторам.

Конечно, сеть будет функционировать при условии, что хотя бы два компьютера включены. Вы имеете возможность определить наличие в сети включенного компьютера, используя команду `ping`, набрав ее в командной строке. Эта команда имеет несколько параметров, с которыми можно ознакомиться, набрав команду без параметров. Если за именем команды указать реальный IP-адрес в вашей сети, будет проверена связь с указанным адресом. Можно вместо адреса указать имя компьютера, под которым вы подключили его к сети. В зависимости от настроек, сделанных на каждом компьютере, доступ к его ресурсам может быть ограничен паролем. Если на вашем компьютере установлена Windows 2000, то доступ к ресурсам может быть настроен и на уровне пользователей. Правда, для небольшой сети в этом может и не быть смысла. В небольшом коллективе, совместно использующем несколько рабочих станций, люди, основываясь на взаимном доверии, могут установить единый пароль для доступа к ресурсам, защищающий сеть от постороннего проникновения. При этом следует иметь в виду, что если есть вероятность несанкционированного использования компьютеров такой сети, то нельзя включать опцию кэширования пароля. При каждом подключении к сетевым ресурсам необходимо вводить пароль, а не устанавливать флажок **Запомнить пароль**. Совершенно уверенно можно сказать, что вас не устроит ситуация, когда возможность доступа в Интернет есть только у одной рабочей станции. Правда, при нежелании или невозможности проводить дальнейшие

настройки и модернизации, вы тем не менее сможете воспользоваться накопленной такой рабочей станцией информацией.

Настройка односегментной сети

Настройку проводим в среде Windows 98. Для начала выбираем для настройки два компьютера.

Все готово для настройки. Включаем компьютеры и устанавливаем протоколы и службы, необходимые для работы в нашей сети. Выберите в окне **Панель управления** значок **Сеть**. Двойным щелчком на этом значке откройте окно **Сеть** (рис. 2.10).

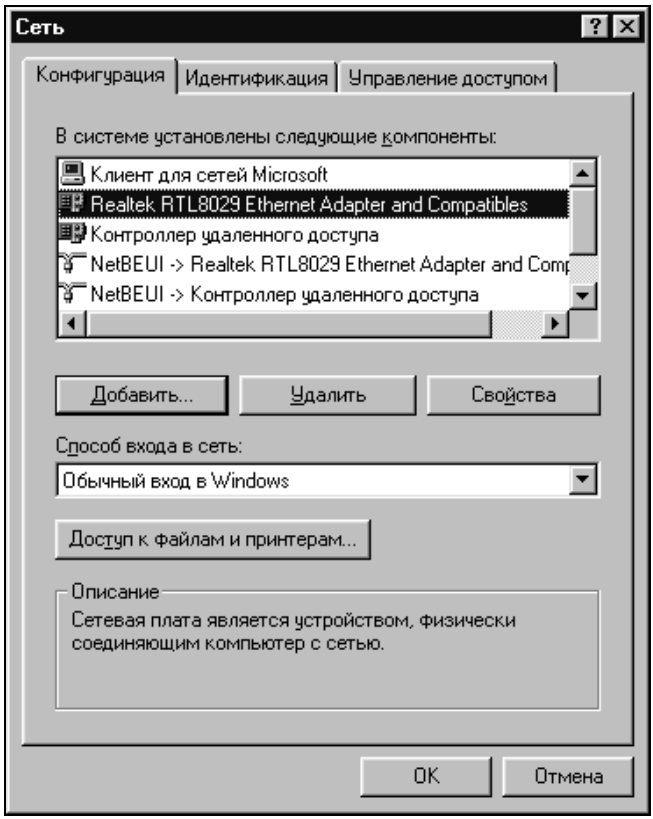


Рис. 2.10. Диалоговое окно **Сеть**

Для проведения настройки проверьте наличие на вашем компьютере нижеперечисленных средств для работы в сети.

- ❒ Клиент для сетей Microsoft.
- ❒ Сетевая карта.
- ❒ NetBEUI.
- ❒ TCP/IP.
- ❒ Служба доступа к файлам и принтерам сетей Microsoft.

Если установлен модем, то добавьте к этому списку также контроллер удаленного доступа. При этом протоколы для контроллера добавятся автоматически. Лишние протоколы и службы, если они установлены, следует удалить.

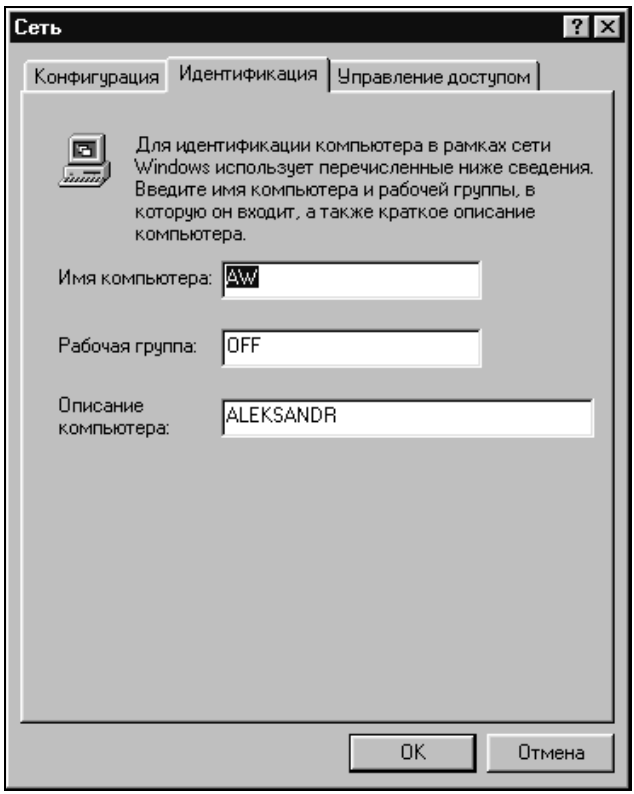


Рис. 2.11. Диалоговое окно **Сеть**, вкладка **Идентификация**

Далее переходим на вкладку **Идентификация** (рис. 2.11) и заполняем или меняем содержимое полей, если значения не соответствуют тому, что вы хотели бы иметь в вашей сети.

Имя рабочей группы назначайте в соответствии с назначением вашей рабочей станции. Все компьютеры бухгалтерии, например, могут быть объединены рабочей группой BUH. Все имена лучше писать латиницей, поскольку иногда компьютер не воспринимает русские буквы. Далее переходим на вкладку **Управление доступом** (рис. 2.12).

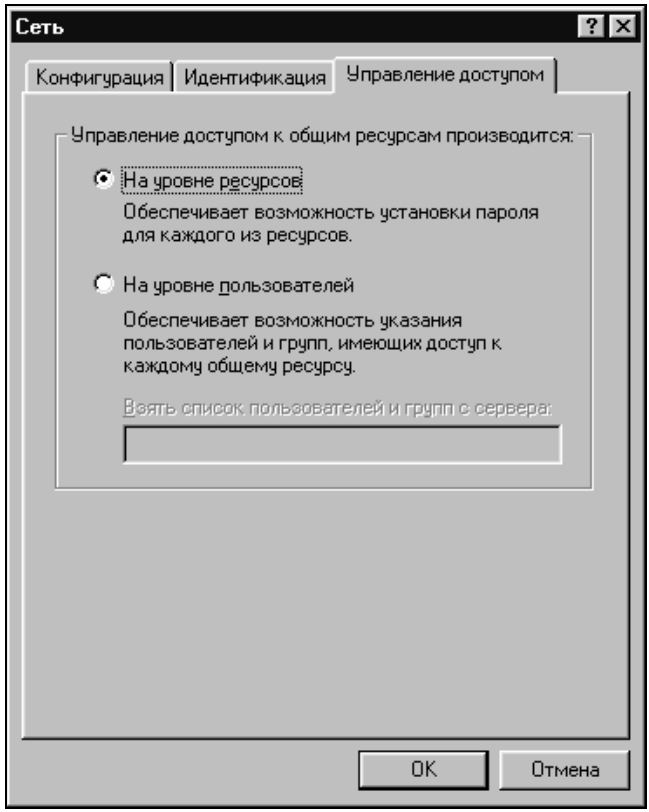


Рис. 2.12. Диалоговое окно **Сеть**, вкладка **Управление доступом**

На этой вкладке можно выбрать вариант управления доступом к ресурсам компьютера. Предлагаются два варианта, один — управление на уровне ресурсов, другой — управление на уровне пользователей. Рассмотрим подроб-

нее оба варианта. Уровень пользователей предполагает, что для каждого пользователя установлены права доступа к определенным ресурсам. Это имеет смысл, если требуется строго индивидуальный подход к информации или существует некоторая иерархия прав. Условно — начальник, заместитель, главный специалист, специалист, исполнитель.

Уровень ресурсов предполагает, что все, зная пароль, могут получить доступ к любому ресурсу. Кому дается пароль и как часто он меняется — это уже ваше дело. Мы возьмем за основу уровень ресурсов, вполне достаточный для защиты и удобный в применении для небольшой сети.

На вкладке **Конфигурация** есть еще одно поле, на которое мы пока не обращали внимания, — **Способ входа в сеть**. Если выбрать опцию **Обычный вход в Windows**, то сетевые диски и принтеры, о которых мы будем говорить дальше, будут подключаться автоматически при обращении к ним. Пароль, если мы решим его установить, необходимо будет вводить при загрузке Windows. Если вы не хотите устанавливать пароль, то когда система попросит первый раз ввести его, не вводите, а нажмите кнопку **ОК**, а при необходимости подтвердить пароль опять ничего не вводите и нажмите кнопку **ОК**. Теперь при входе в систему больше не будет запрашиваться пароль, пока вы сами не решите его установить. На той же вкладке, нажав кнопку **Доступ к файлам и принтерам**, поставьте галочки в полях напротив надписей, говорящих о том, что файлы и принтеры этого компьютера можно сделать общими. Поскольку компьютер становится сетевым, придется делиться его ресурсами с другими пользователями сети. После всех настроек и нажатия кнопок **Применить** и **ОК** ОС может "потребовать" диск с Windows и перезагрузку. Согласитесь с ней. Если вы установили пароль, то при входе в Windows введите его по требованию системы. Раньше, работая с компьютером, вы могли заметить, что пароль можно не вводить, а просто отменить его ввод. Но в этом случае сетевые подключения автоматически осуществляться не будут, а при попытках обратиться к сетевым ресурсам пароль будет запрашиваться снова и снова. Но это еще впереди. А пока двойным щелчком на значке **Мой компьютер** откройте структуру каталогов, найдите значок диска C: и щелкните на нем правой кнопкой мыши. В появившемся меню выберите команду **Свойства**, а затем — вкладку **Доступ** (рис. 2.13).

На этой вкладке установите переключатель **Общий ресурс**. Затем установите параметры доступа к диску и пароли (на стадии экспериментов пароли вводить не обязательно, достаточно ввести простые пароли, чтобы не забыть и не потерять их, — установить или поменять пароли вы сможете позже). Установить параметры доступа можно не только для диска, но и для любой

папки. Можно ввести также сетевое имя диска или папки. С этим именем они будут отображаться на других компьютерах сети.

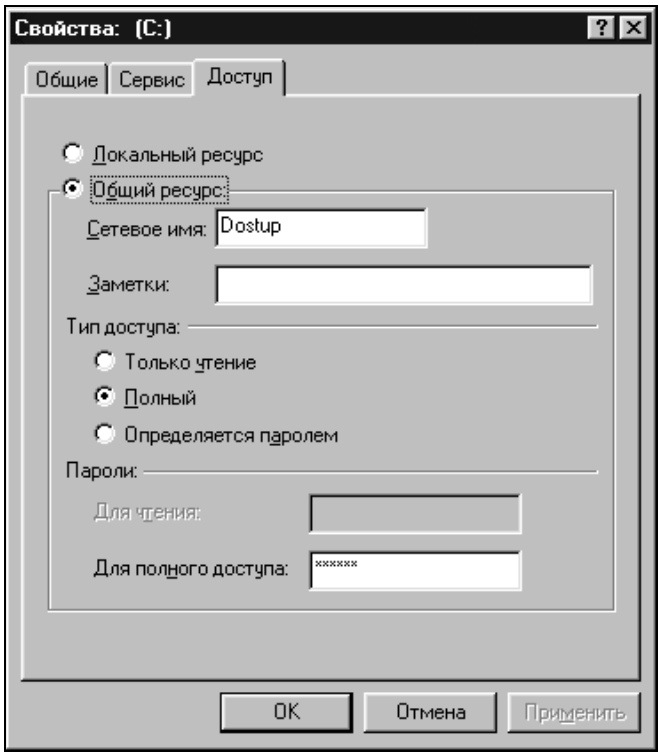


Рис. 2.13. Диалоговое окно свойств диска, вкладка **Доступ**

На этой рабочей станции значки всех дисков и папок, для которых установлен общий доступ, будут отмечены изображением поддерживающей руки (рис. 2.14).

Если такого изображения нет, то либо настройка проведена с ошибкой, либо вы отменили перезагрузку после настройки, и ее следует произвести теперь. После удачного завершения настроек на этой рабочей станции переходим ко второй и повторяем все настройки на ней. Само собой разумеется, что имя компьютера должно отличаться, а имя рабочей группы может и совпадать — по вашему желанию.

Теперь наступает ответственный момент. Оба компьютера включены, настроены и подсоединены к сети. Это значит, что мы уже можем воспользо-

ваться первыми плодами своего труда и провести пробный сеанс связи между компьютерами.

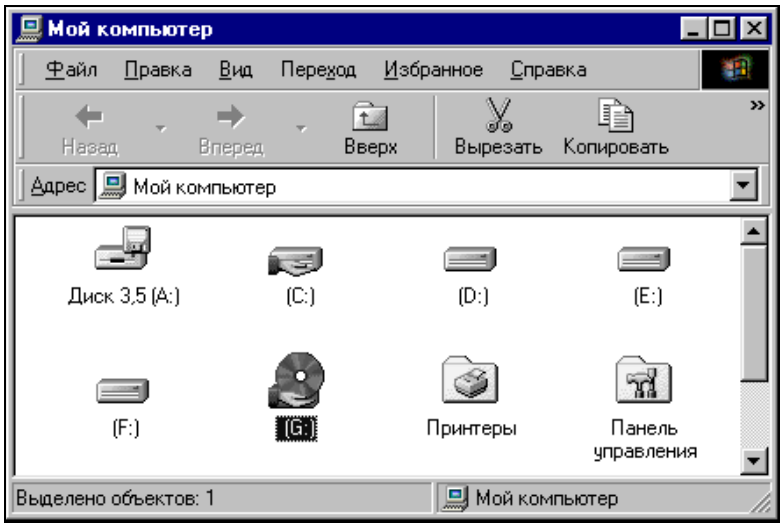


Рис. 2.14. Изображения дисков с установленным общим доступом отмечены поддерживающей рукой

На рабочем столе того компьютера, который мы только что настроили, находим значок **Сетевое окружение**, щелкаем на нем правой кнопкой мыши и в появившемся меню выбираем команду **Найти компьютер**. В поле раскрывающегося списка **Имя** вводим имя второго компьютера. В нашем случае это `AW`. Через несколько мгновений в области вывода результатов поиска появится значок компьютера с именем AW (рис. 2.15). В столбце **Размещение** будет указано имя рабочей группы, и, если при заполнении вкладки **Доступ** мы вставили пару слов в столбце **Заметки**, они тоже появятся в поле вывода результатов поиска. Если это произошло, *наша сеть начала работать*. Теперь двойным щелчком на значке компьютера **AW** вы можете вызвать окно, в котором увидите диски и/или папки, доступ к которым разрешен (рис. 2.16). При попытке открыть диск (его изображение не отличается от изображения папки) или папку система потребует ввести пароль для доступа к ресурсу, если он был установлен при настройке компьютера.

После ввода пароля мы можем открыть нужный ресурс и работать с ним так, будто он находится на нашем компьютере. Если постоянный доступ к этому ресурсу требуется при каждом включении компьютера, достаточно в меню,

которое появляется при щелчке правой кнопкой мыши на значке **Сетевое окружение** или **Мой компьютер**, выбрать команду **Подключить сетевой диск**, набрать путь к диску или папке и отметить флажок **Автоматически подключать при входе в систему**.

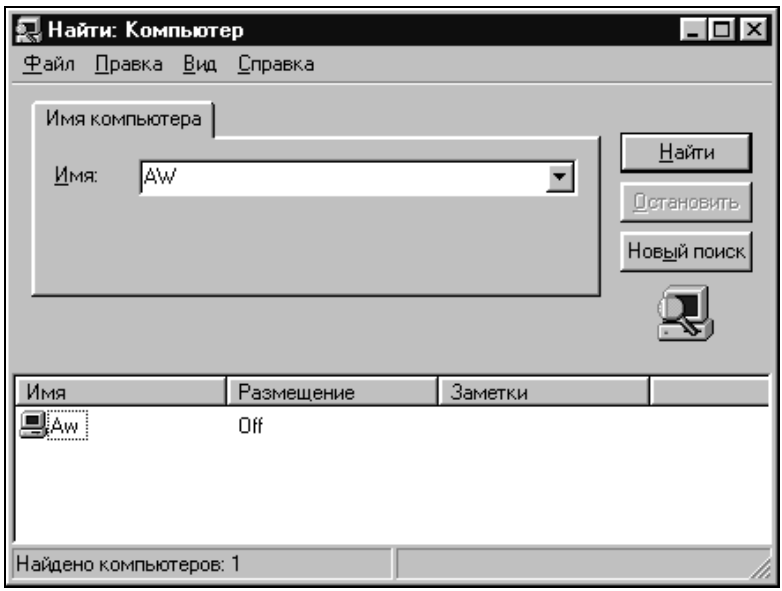


Рис. 2.15. Окно поиска компьютера в сети

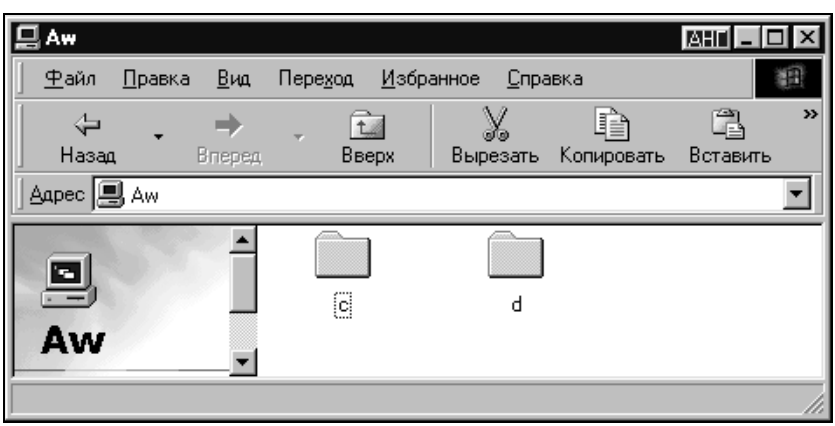


Рис. 2.16. Папки с разрешенным доступом

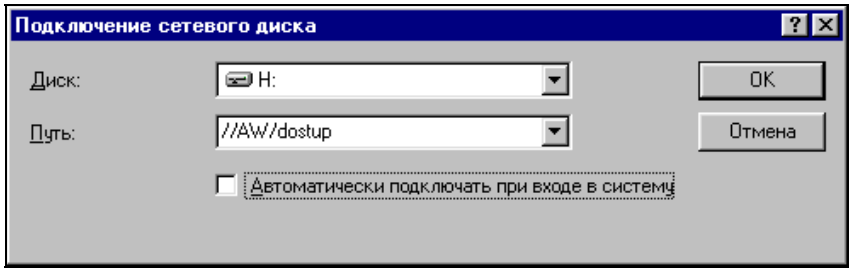


Рис. 2.17. Окно подключения сетевого диска

Сетевой путь вводится несколько иначе, чем обычный путь к файлу на локальном компьютере. В начале пути ставятся две, а между уровнями пути — одна прямая черта, в отличие от обратной черты при указании обычного пути. Поскольку Windows позволяет запомнить пароли для автоматического их ввода, диск будет подключаться каждый раз без нашего вмешательства (рис. 2.17). Но надо иметь в виду, что это несколько снижает защищенность данных от несанкционированного доступа, так как ввод пароля для подключения сетевого диска на этом компьютере больше не требуется.

По этой причине не всегда есть смысл применять автоматическое подключение сетевых дисков.

Теперь оба компьютера могут использовать ресурсы друг друга.

Подключение дополнительных рабочих станций

После настройки простейшего варианта подключим еще один, третий, компьютер. При использовании коаксиального кабеля никаких проблем не возникает. Достаточно настроить еще одну рабочую станцию аналогично тем, что уже настроены, проложить кабель от конца существующей сети до места установки дополнительной рабочей станции, снять терминатор, присоединить кабель к соединяемым компьютерам, а на открытую часть тройника, присоединенного к сетевой карте устанавливаемой рабочей станции, надеть снятый терминатор. Все! Получилась сеть, содержащая три узла. Дальнейшее наращивание количества компьютеров в сети проводится по этой же схеме. Но простота этого пути — лишь надводная часть айсберга. При эксплуатации такой сети обнаруживаются проблемы. Если в вашей сети, предположим, десять рабочих станций, и на пятой, находящейся где-то посередине всей це-

почки, нарушился контакт в соединении тройника с кабелем, то сеть рвется на две не связанные друг с другом части. Несколько более сложный вариант с применением витой пары лишен этого недостатка. В этом случае для количественного наращивания сети потребуется концентратор. Кабель, проложенный от концентратора до компьютера, теперь должен одинаково соединяться с разъемом с обоих концов (табл. 2.6). К каждому компьютеру должен быть проложен индивидуальный кабель от хаба (рис. 2.18).

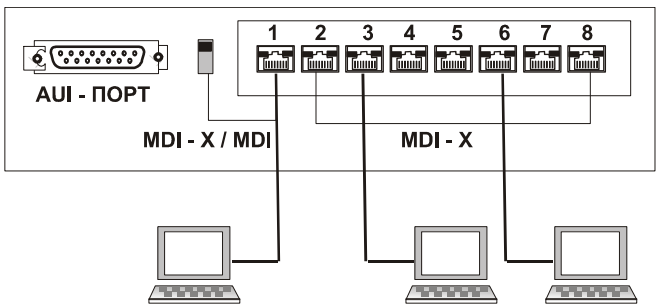


Рис. 2.18. Концентратор 10Base-T — соединение с компьютерами

Таблица 2.6. *Разводка кабеля от хаба к компьютеру*

Одна сторона	Цвет провода	Другая сторона
Кабель на две пары		
1	Бело-оранжевый	1
2	Оранжево-белый	2
3	Бело-синий	3
6	Сине-белый	6
Кабель на четыре пары		
1	Бело-зеленый	1
2	Зеленый	2
3	Оранжевый	3
4	Синий	4
5	Бело-синий	5

Таблица 2.6 *(окончание)*

Одна сторона	Цвет провода	Другая сторона
Кабель на четыре пары		
6	Оранжево-белый	6
7	Бело-коричневый	7
8	Коричневый	8

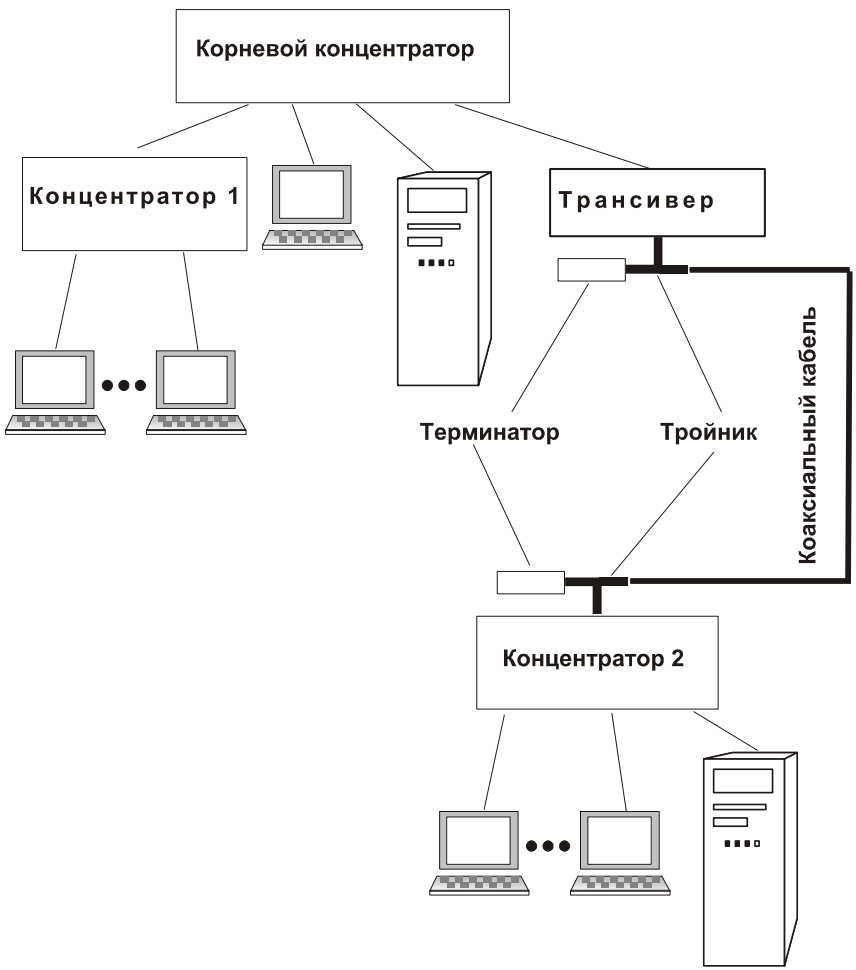


Рис. 2.19. Вариант комбинированного построения сети

Один из входов хаба может иметь переключатель MDI-X/MDI, предназначенный для изменения режима работы этого входа. Возможно подключение рабочей станции как к обычному входу, так и подключение вышестоящего хаба, когда используется их каскадирование, или подключение выхода трансивера, подсоединенного к толстому коаксиальному кабелю.

Нами уже настроены для подключения к сети при прямом соединении их сетевых адаптеров две рабочие станции. Связь между этими станциями будет установлена после включения питания хаба и присоединения кабелей в соответствии с рис. 2.19. Третья рабочая станция настраивается аналогично первым двум.

Теперь мы имеем практически неограниченную возможность увеличивать количество рабочих станций в нашей сети. Можно соединить компьютеры (см. рис. 2.2) как с помощью толстого, так и с помощью тонкого коаксиального кабеля (см. рис. 2.19), или применить только каскадное подключение хабов, не используя коаксиальный кабель — словом, простор для творчества широчайший.

Приобретая оборудование, необходимо предусмотреть возможность подключения рабочих станций. Например, терминаторы и трансиверы существенно отличаются в зависимости от того, для соединения с каким коаксиальным кабелем они предназначены: тонким или толстым. В некоторых случаях при использовании тонкого кабеля трансивер может не понадобиться вовсе, а подключение кабеля будет произведено прямо к концентратору, имеющему BNC-разъем (на рис. 2.19 это Концентратор 2). Таким образом, перед полным монтажом сети необходимо продумать ее структуру, по возможности учитывая и перспективы развития.

Дополнительные настройки

По умолчанию при настройках свойств протоколов устанавливается вариант **Получить IP-адрес автоматически**. Для работы в локальной сети есть смысл использовать статические, т. е. заданные при настройке адреса (рис. 2.20).

Выбрав на вкладке **Конфигурация** окна **Сеть** протокол TCP/IP для сетевого адаптера, нажмем кнопку **Свойства**. В открывшемся окне **Свойства: TCP/IP** выберем вкладку **IP-адрес** и установим значения IP-адресов для каждого компьютера. Маску подсети установим равной 255.255.255.0. Адреса могут начинаться со значения 10.0.0.1 и продолжаться последовательно до

10.0.0.*NN*, где *NN* — это количество компьютеров в вашей сети. Необходимость этой настройки объясняется тем, что ряд программ, предназначенных для работы в сети, идентифицируют компьютеры по IP-адресу. Если адрес меняется от включения к включению, то его невозможно запомнить и использовать при очередном соединении.

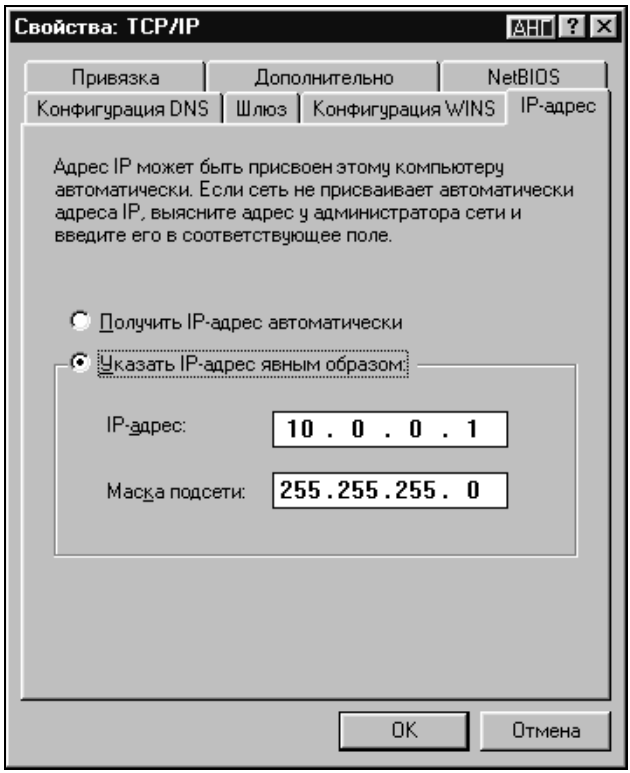


Рис. 2.20. Окно свойств TCP/IP — установка адреса

Обратите внимание на то, что эти изменения следует производить только для сетевого адаптера. Протокол TCP/IP, применяемый контроллером удаленного доступа, который используется для соединения с Интернетом, обычно требует установки IP-адреса автоматически, поскольку этот адрес назначается сервером на стороне провайдера.

Операционные системы Windows 95/98 имеют в своем составе некоторые вспомогательные программы для работы в сети. Одна из них — программа WinPopup (рис. 2.21), находящаяся в каталоге Windows.

Если ярлык программы поместить в папку **Автозагрузка**, то при включении компьютеров она будет готова к приему и передаче сообщений внутри сети. Она может быть настроена таким образом, что при появлении сообщения окно программы будет разворачиваться, а при удалении последнего прочитанного сообщения окно автоматически свернется в значок на панели задач. Эта программа — минимальный вариант сетевой почты, которая не позволяет пересылать сколько-нибудь объемные послания и документы, но позволяет оперативно передать срочные короткие сообщения. Программа может не устанавливаться по умолчанию при инсталляции операционной системы, в этом случае ее следует добавить, воспользовавшись опцией **Установка и удаление программ** в меню **Панель управления**.

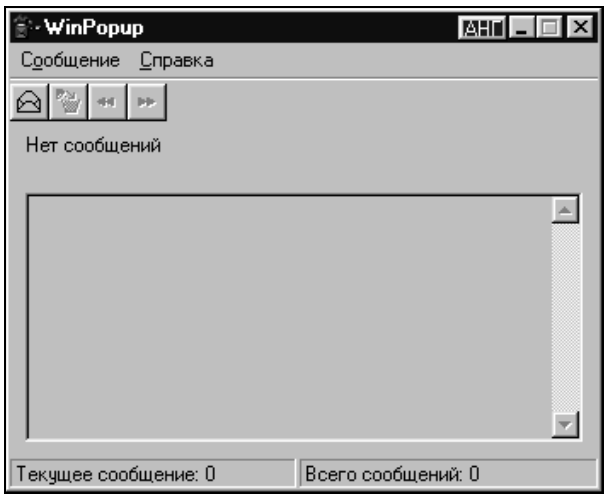


Рис. 2.21. "Выскочка" — программа для передачи сообщений по локальной сети

Определив имена пользователей и включив всех пользователей в одну рабочую группу, мы получили возможность доступа от одной рабочей станции к другой и возможность видеть пиктограммы пользователей в Проводнике. Для удобства работы в сети при значительном количестве пользователей можно условно распределить их по рабочим группам. При этом мы получим возможность обращаться сразу к группе пользователей. По какому принципу производить деление на группы, вам виднее. Но после того как на каждой рабочей станции установлена принадлежность ее к рабочей группе, в проводнике **Сетевое окружение** будут видны компьютеры, входящие в эту

группу (рис. 2.22). Остальные компьютеры можно будет найти, дважды щелкнув по значку **Вся сеть** (рис. 2.23) и открыв нужную рабочую группу.

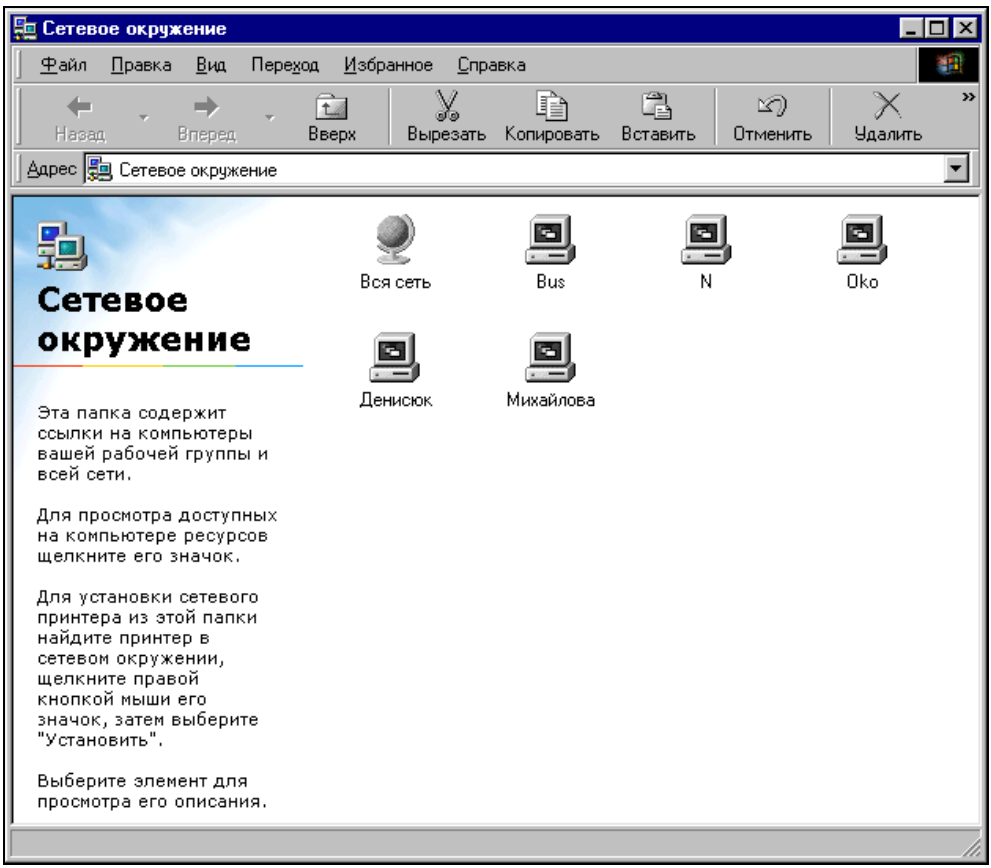


Рис. 2.22. В окне **Сетевое окружение** видны компьютеры вашей рабочей группы

Доступ к файлам и папкам мы получим только после того, как с помощью окна **Свойства** установим доступ к папкам на каждом компьютере.

К сожалению, под управлением Windows 95/98 невозможно запускать программы, установленные на другом компьютере. Но при некоторых ограничениях на свободу перемещения и изменения файлов на рабочих станциях можно существенно сэкономить место на жестких дисках слабых компьютеров, помещая файлы редко используемых программ на диск одной рабочей

станции. Для этого при установке программы необходимо указать сетевой путь для ее каталога. В этом случае одни и те же файлы могут использовать разные компьютеры. Но процедура установки программ должна проходить на каждом компьютере индивидуально, и папки, в которых должны сохраняться результаты работы этих программ, должны определяться также индивидуально. Некоторые программы, пришедшие из эпохи DOS, и некоторые простые программы для Windows могут запускаться и с чужого диска без предварительной индивидуальной установки. Например, утилита Norton Commander (NC) может быть установлена на одном компьютере, а запускаться в сеансе DOS с другого. Достаточно настроить ярлык NC с указанием сетевого адреса каталога, где находится программа.

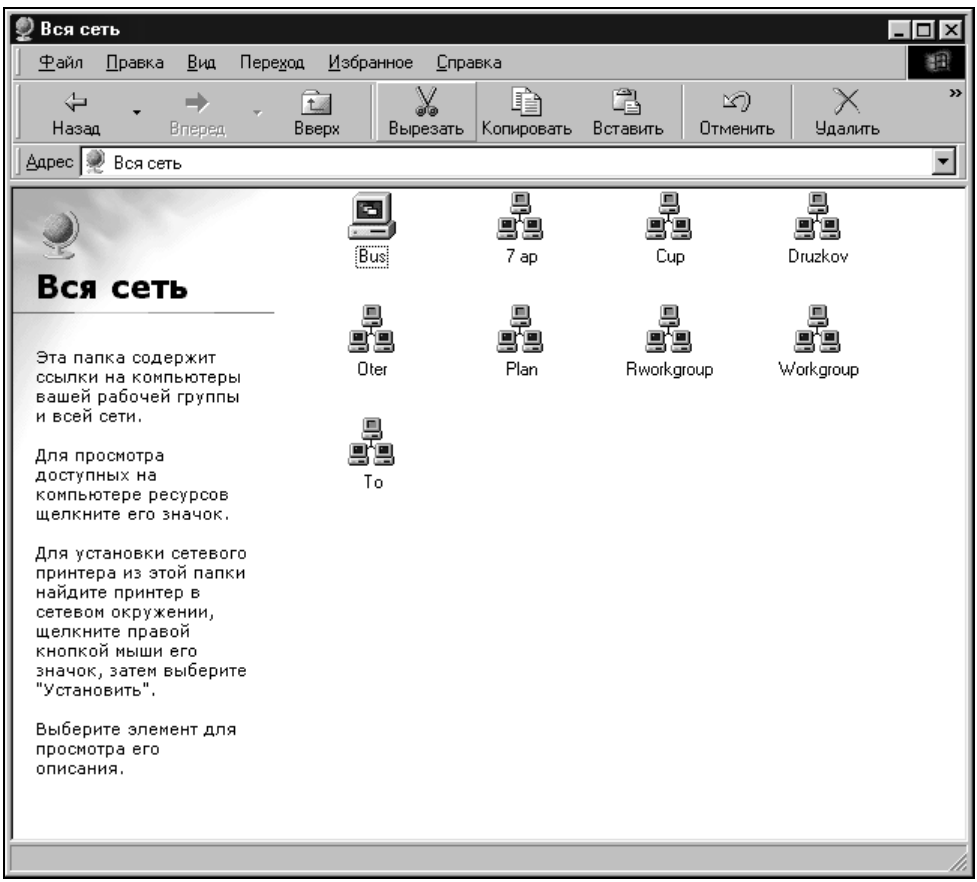


Рис. 2.23. Окно **Вся сеть** показывает все рабочие группы сети

Некоторые особенности работы в сети

Ярлыки и работа в сетевом окружении

Работа в сети иногда требует особенного подхода. Несмотря на то что все настройки проведены верно, проходящие в сети процессы иногда требуют значительного времени. Например, после включения компьютеров и выбора значка **Сетевое окружение** мы обнаружим, что не все, что вокруг нас в сети, и не сразу видно в сетевом окружении. Несколько больше можно увидеть, обратившись к значку **Вся сеть**, но и там не все появляется моментально.

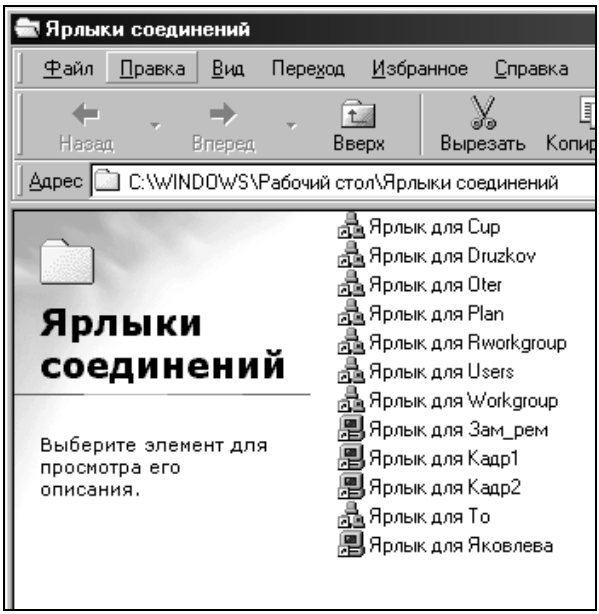


Рис. 2.24. Ярлыки соединений
могут ускорить доступ к компьютерам сети

Иногда требуется довольно значительное время, чтобы увидеть и получить доступ к компьютеру, который, возможно, находится рядом с вами. Из этой ситуации существует довольно простой выход. Когда все соединения или, по крайней мере, их часть видны, можно создать к ним ярлыки и поместить в отдельную папку. При следующем включении, несмотря на то что еще не все компьютеры видны в окне **Сетевое окружение**, их всегда можно вызвать,

воспользовавшись ярлыком. Ярлыки можно создавать как для отдельных рабочих станций, так и для групп пользователей (рис. 2.24).

Принтер обычно доступен сразу после обращения к нему при печати.

В ряде случаев для комфортной работы в сети желательно применять дополнительные средства, которые не видны явно при сетевых настройках и являются частью операционной системы или офисного комплекта.

В Windows дополнительными функциями обладают ярлыки командных файлов — PIF-файлы, которые сами являются программами конфигурации системы на время запуска какой-либо программы. Не слишком опытный пользователь боится командной строки, сомневаясь в правильности введенных команд и опасаясь испортить чего-нибудь в своем компьютере. Неверно введенные в командной строке команды редактировать не очень удобно. Приходится заново набирать всю команду (если, конечно, у вас не установлена утилита DOSKEY.EXE). Сохранить набранную команду можно в BAT-файле, записав ее туда, проверив и отредактировав, чтобы все сомнения в ее правильности отпали. Имя файла выбирайте попроще, чтобы можно было набрать его без ошибки. Теперь ваша команда будет выполнена, а вы сможете воспользоваться ей еще раз, когда появится необходимость. Простые команды можно быстро научиться вводить напрямую. Если требуется выполнить сложную серию команд, которые, например, архивируют, переименовывают, перемещают или копируют группы файлов, особенно если такая потребность возникает часто, то и опытный пользователь обратится к помощи BAT-файла. Windows позволяет сделать операции с файлами более наглядными, а безликие BAT-файлы могут приобрести выразительные ярлыки.

Может возникнуть необходимость поменять что-либо на всех компьютерах сети, объединяющей множество машин. Например, требуется изменить свойства ярлыка общедоступной программы, установленной в сетевом варианте, и добавить две вложенные друг в друга папки на каждом компьютере. Для этого можно в общедоступной папке поместить ярлык **ЯРЛЫК.LNC** с необходимыми свойствами, файл **<КОМАНДА>.BAT** и ярлык **<КОМАНДА>.PIF** для этого командного файла с картинкой, например, из Windows\SYSTEM\PIFMGR.DLL. BAT-файл должен содержать следующие строки:

```
DEL C:\Windows\РАБОЧИ~1\ЯРЛЫК.LNC
COPY F:\<ПУТЬ>\ЯРЛЫК.LNC C:\Windows\РАБОЧИ~1\ЯРЛЫК.LNC
MD C:\DIR1
CD DIR1
MD DIR2
```

В окне **Свойства** ярлыка для этого файла необходимо установить флажок **Закрывать окно по завершении сеанса**.

Теперь процедура замены ярлыка и создания двух вложенных папок на каждом компьютере заключается в щелчке на этом ярлыке в окне общедоступной сетевой папки.

Ярлыки можно использовать и внутри офисных приложений. MS Excel, например, позволяет работать с общедоступными файлами на сетевых дисках, а также применять пользовательские функции, т. е. функции, разработанные пользователями. Но, работая в сети, каждый пользователь должен иметь доступ к функции, которая обычно помещается в каталог Program Files\Microsoft Office\Office\XLStart. В этот каталог можно поместить не саму функцию, а ее ярлык, который будет ссылаться на файл на сетевом диске или в удаленном каталоге. При этом с помощью окна **Свойства** файла функции необходимо установить общий доступ без возможности изменения. Теперь каждый раз при старте MS Excel будет подключаться эта функция, доступная для каждого пользователя.

Организация системы имен в сетях

Протокол NetBIOS позволяет обращаться к любому компьютеру по имени, но этот протокол работает только в локальных сетях. IP-адрес состоит из цифр, удобных для компьютера, но неудобных для пользователей сети. Это значит, что при выходе за пределы локальной сети трудно будет, не применяя каких-либо иных средств кроме рассмотренных, использовать понятные и удобные имена компьютеров и адреса Интернета. По сложившейся практике в больших сетях используют систему доменных имен DNS (Domain Name System). Домен — организационная единица безопасности в сети. Рабочая станция является доменом. Домен может охватывать несколько физических точек. В каждом домене своя политика безопасности, и у каждого домена свои отношения с другими доменами.

Адреса записываются в соответствии с подчиненностью сетей и компьютеров. Если компьютер сети имеет постоянный IP-адрес, а сеть, в которую он входит, зарегистрирована в вышестоящем домене, то его адрес может выглядеть следующим образом:

наш_компьютер.наша_сеть.домен_3-го_уровня.домен_2-го_уровня.ru.

На самом нижнем уровне находится имя нашего компьютера, далее следует название нашей сети, которое зарегистрировано в домене 3-го уровня, и т. д. На вершине адреса — зона **ru** — имя домена верхнего уровня, в котором

обычно регистрируются домены второго уровня. Протокол TCP/IP определяет систему IP-адресов, которые в специальных конфигурационных файлах переводятся в имена доменные. Эти файлы находятся на серверах доменных имен (DNS — Domain Name Server) и позволяют компьютеру определить IP-адрес по его символьной записи. Например, при связи с компьютером (сервером) провайдера его IP-адрес записан в конфигурации соединения. Адреса, вводимые нами в адресную строку браузера, переводятся в IP-адреса, исходя из имеющейся на сервере информации. Если символьному адресу не соответствует IP-адрес на сервере, то никакого соединения не произойдет. Для компьютера во время сеанса связи с провайдером временно выделяется цифровой адрес. Компьютер также имеет имя. При этом с другого компьютера, который через того же провайдера в данный момент подключен к Интернету, нельзя соединиться с первым компьютером, набрав его символьный адрес. Но, зная цифровой адрес первого компьютера, такое соединение осуществить можно. Для того чтобы обеспечить соединение нашей сети с другими сетями, наша сеть должна иметь выделенный сервер — особый компьютер, который не используется для обычной работы. Установленные на нем сервисы должны выполнять самые разнообразные запросы пользователей, в том числе и регистрацию имен для обеспечения удобной связи между компьютерами.

Необходимо отметить очень важный момент в использовании IP-адресов: адреса в вашей сети не должны повторяться. Повторение адресов приведет к остановке компьютеров, адреса которых совпали. А если один из этих компьютеров — сервер? Или компьютеров всего три? Для работы NetBIOS тоже важно отсутствие одинаковых имен, но совпадения не приводят к полной остановке работы. Более серьезные последствия будет иметь совпадение MAC-адресов (Media Access Control — управление доступом к среде), адресов сетевого оборудования, которые заданы производителем и "вшиты" в это оборудование. Впрочем, такое совпадение практически невозможно, так как в состав MAC-адреса входит много сведений, которые не могут совпасть. При совпадении IP-адресов необходимо перезапустить компьютеры с совпавшими адресами, изменив адрес на одном из них, выяснить причины совпадения адресов и принять меры к исключению подобных случаев в будущем. Реальный адрес в локальной сети может не соответствовать принятому стандартному диапазону адресов для данной категории сети. На работоспособности сети обычно это не сказывается до тех пор, пока сеть не становится частью другой сети или не получает выход в Интернет. В этом случае возможны неустранимые конфликты адресов. Поэтому, продумывая организацию сети, следует заранее запланировать соответствующие стандартам диапазоны адресов компьютеров и подсетей.

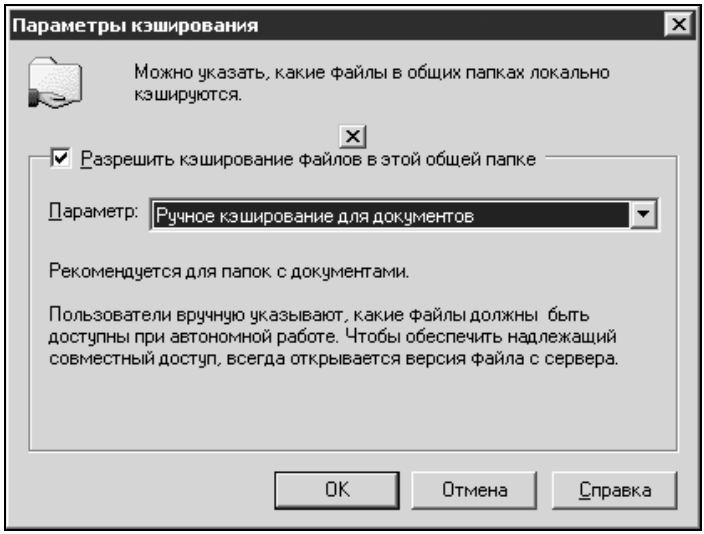


Рис. 2.25. Настройка кэширования папок с документами

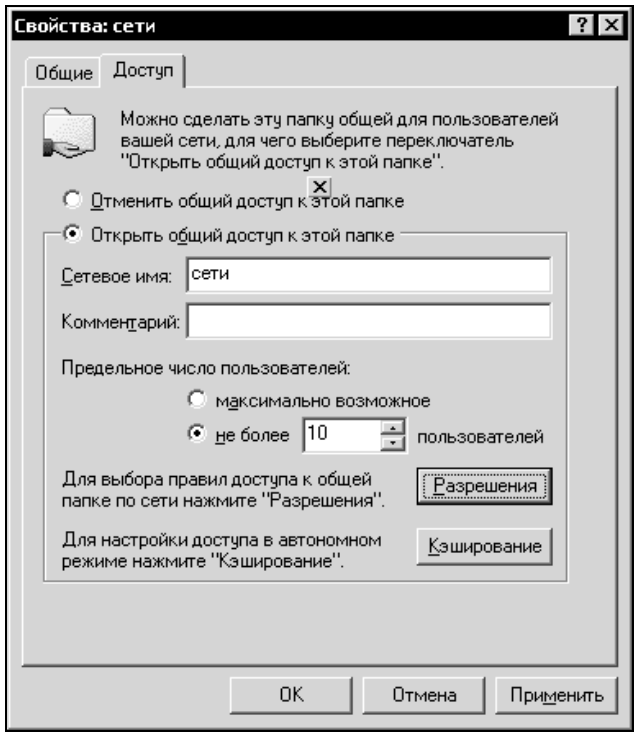


Рис. 2.26. Окно настройки сетевого доступа к папкам

Доступ к ресурсам в Windows 2000

По сравнению с Windows 98, в Windows 2000 настройка доступа делается иначе. Можно включить кэширование папок с документами (рис. 2.25), что позволит работать с ними после отключения от сетевого ресурса, поскольку документы будут сохранены на локальном компьютере.

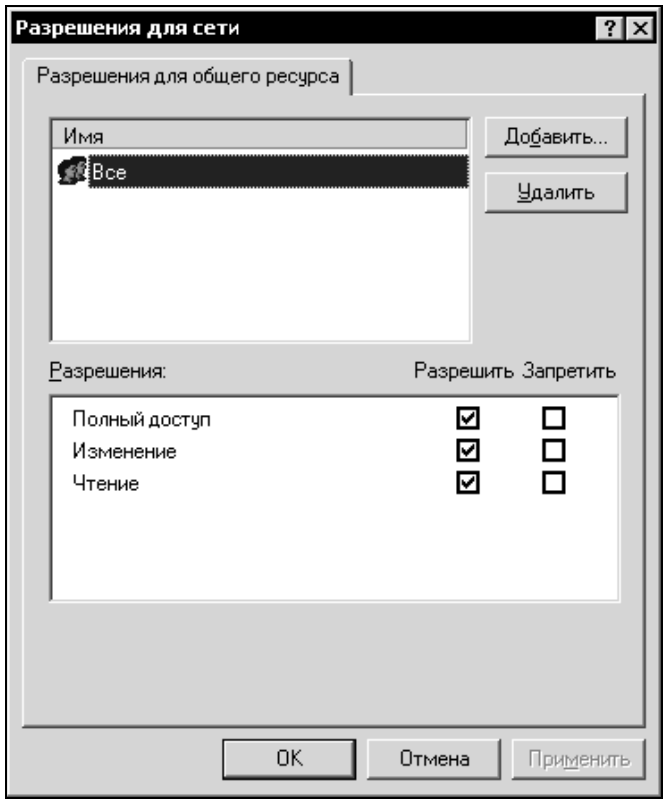


Рис. 2.27. Установка разрешений

Если не отменен общий доступ (см. рис. 2.26) к папке, то можно задать предельное число пользователей, которые могут обращаться к этой папке одновременно. Также можно установить разрешения, определяющие параметры доступа для каждого пользователя (которого можно добавлять в список и удалять из него) (рис. 2.27). Пользователю, не включенному в список имеющих доступ, ресурс будет недоступен.

Общение в одноранговой сети

Для передачи простых сообщений в одноранговой односегментной сети существуют стандартные средства, например программа WinPopup. Более широкие возможности для общения предоставляют программы, обеспечивающие режим чата. Это режим текстовых переговоров, широко распространенный в Интернете, но часто применяемый и в локальных сетях. Среди бесплатно распространяемых программ широкой известностью пользуется программа Intranet Chat (рис. 2.28), которую можно найти по адресу **http://vnalex.tripod.com**. Программа обладает большим количеством настроек и возможностей, делающих работу с ней приятной и надежной. Предусмотрены как общий, так и приватный режимы общения, имеется доска объявлений, возможна установка фильтров на принимаемые сообщения.

Интерфейс программы простой, а в случае затруднений помощь, которая может быть оперативно вызвана во время работы, дает лаконичные советы. Программа работает под управлением Windows 95/98/NT/XP/2000. Проблемы, которые могут возникнуть при установке и настройке, подробно описаны в документации. Даже начинающий пользователь сети сможет воспользоваться этой программой уже через несколько минут после установки. Потребуется лишь небольшая настройка. Одно из условий стабильной работы программы в локальной сети — это необходимость ввода имени рабочей группы на всех компьютерах сети. Часть настроек осуществляется по умолчанию и обычно не требует изменений.

> ***ПРИМЕЧАНИЕ***
>
> Описание настроек приведено в соответствии с экземпляром программы, имевшимся у автора на момент написания этих строк.

С помощью меню и кнопок главного окна программы пользователю доступны следующие настройки:

- **Использовать однострочный редактор**

  Переключение типа используемого редактора для сообщений (однострочный/многострочный). Переключение также возможно при помощи клавиши <F4>;

- **Показывать личные сообщения во всплывающем окне**

  Если опция выбрана и текущий режим чата не запрещает выносить его на передний план при получении личного сообщения, то каждое личное со-

общение будет дополнительно отображаться в отдельном всплывающем окне;

- **Фильтровать приходящие сообщения**

  Это глобальный переключатель для разрешения/запрета фильтрации сообщений с использованием разрешенных фильтров.

  Дополнительно в отдельном плавающем окне (аналог того, как это сделано в ICQ) будет отображено состояние чата. Его можно переместить в самое удобное для вас место на экране. Этот режим отображения очень полезен тем, у кого включено автоматическое скрытие панели задач Windows. Двойным щелчком в этом окне можно выбрать главное окно чата. При щелчке правой кнопкой появляется меню;

- **Показать**

  - **Список пользователей**

    Показать/спрятать список пользователей;

  - **Тулбар**

    Показать/спрятать панель инструментов;

  - **Доску объявлений**

    Показать/спрятать доску объявлений;

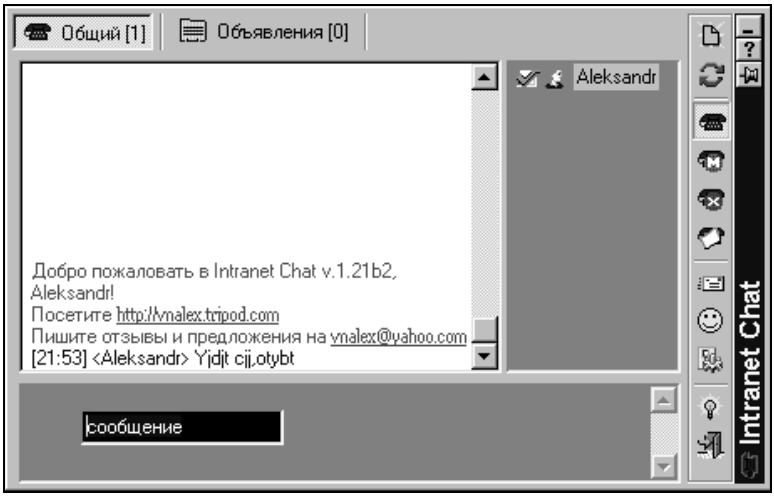


Рис. 2.28. Окно программы Intranet Chat

- **Информация о пользователях**

  Данный пункт позволяет посмотреть расширенную информацию о всех пользователях, находящихся в данный момент в чате. Подпункты определяют, как будет отсортирована выводимая информация: по имени в чате, по имени компьютера, по имени пользователя в Windows, по версии чата;

- **О программе**

  Показать информацию о разработчике, его e-mail, ссылку на домашнюю страницу чата;

- **Помощь**

  Показать файл помощи;

- **Выход**

  Выход из программы.

Программа позволяет автоматически преобразовывать "смайлики" в картинки. Комбинации символов-смайликов будут автоматически преобразованы в соответствующие картинки. Преобразование работает и в русской, и в латинской раскладке клавиатуры.

Далее приведены основные возможности программы.

- Не требует выделенного сервера. Для передачи сообщений чат использует Windows MailSlots (Слоты электронной почты в Windows). Для их работы достаточно одного из установленных протоколов в системе протоколов, "привязанного" к Microsoft Network. Но из-за некоторых ограничений при использовании MailSlots чат очень плохо работает в многосегментных сетях.

- Возможность работы с сервером по протоколу TCP/IP. При таком соединении чат нормально работает в многосегментных сетях и даже в Интернете. Сервер чата существует как в виде обычного приложения, так и в виде сервиса Windows NT.

- Общий чат. Это чат, доступный всем пользователям. Создается при запуске. Любой пользователь может отправить сообщение в этот чат, и все остальные пользователи его получат.

- Обмен личными сообщениями. Возможность отправить выбранному пользователю или нескольким пользователям личное сообщение. Только выбранные пользователи получат его. Личные сообщения могут отображаться в отдельном всплывающем окне.

- Личный чат. Это чат между двумя пользователями. Недоступен никому, кроме них.
- Линия и канал. Аналогично общему чату. Могут быть созданы любым из пользователей. При этом могут быть заданы название и пароль на вход. Так что войти в нее сможет только тот, кто знает пароль.
- Доска объявлений. Каждый пользователь чата может оставить свое объявление, и, когда он находится в чате, его объявление будет отображаться у всех остальных пользователей.
- Фильтр для принимаемых личных сообщений. Можно задать различные фильтры на принимаемые личные сообщения, включать одни и выключать другие. При этом сообщения принимаются, но пользователю об этом не сообщается.
- Быстрый ввод. Возможность задания сообщений и назначения на них "горячих" клавиш для быстрой их вставки при вводе в строку редактирования.
- Предупредительные сообщения в режиме активного соединения. Возможность задания предупредительного сообщения на вход в чат пользователя с определенным именем или пользователя с определенного компьютера. Можно выбрать действие, которое при этом будет произведено:
  - появится чат и сообщит о том, что пользователь "находится" в чате;
  - набранное при задании предупредительное сообщение будет отправлено появившемуся пользователю;
  - набранное предупредительное сообщение будет отправлено вам.
- Возможность ведения регистрационного журнала общего чата и личных сообщений.
- Наличие нескольких состояний чата:
  - "Обычное". Принимаются все сообщения;
  - "Не беспокоить" на личные сообщения, отправленные всем пользователям. Так называемые массовые сообщения;
  - "Не беспокоить" на все сообщения;
  - "Меня нет" или "Я далеко".
- На все эти состояния можно задать сообщения, которые будут пересылаться отправителю полученного личного сообщения. В соответствии с режимом чата изменяется и значок чата в окне задач.

- Возможность задания имени пользователя и его изменения в процессе работы.
- Отдельное окно для отображения состояния чата (как в ICQ).
- Автоматический переход в режим "Меня нет" по истечении указанного времени, если не была нажата клавиша на клавиатуре и не изменялось положение курсора мыши.
- Два режима игнорирования пользователя. Один — игнорировать только личные сообщения. Второй — все.
- Возможность перекодировки сообщения из одной раскладки клавиатуры в другую по "горячим" клавишам. Полезна в случае, если вы забыли переключить раскладку перед набором сообщения и заметили это только после набора сообщения.
- Поддержка двадцати языков интерфейса.

Печать в сети

Ясно, что полноценная работа на компьютере невозможна без принтера. В то же время, используя несколько компьютеров, слишком накладно приобретать отдельный принтер для каждого из них. Есть смысл использовать возможности сети для печати на одном принтере с разных компьютеров. Для этого следует выбрать принтер, удовлетворяющий большей части ваших требований к его свойствам. При необходимости можно использовать два принтера с разными характеристиками, которые нельзя совместить в одном устройстве. Предположим, что один из принтеров — лазерный, для массовой распечатки каких-либо документов с высоким качеством, а другой — струйный, для печати цветных изображений и другой графики. Если есть возможность выбора принтера, то следует поинтересоваться, поддерживает ли он печать русского шрифта в режиме DOS. Несмотря на то что DOS все более и более вытесняется из практики пользователей персональных компьютеров, это качество принтера может потребоваться при отладке компьютеров сети и в других специальных случаях, а также при печати из программ, работающих под DOS. Если принтер не поддерживает печать в DOS, незаметная задача, возникшая, может быть, неожиданно и не представляющая собой ничего сложного, может превратиться в неприятную проблему. Вообще, при выборе любого применяемого в сети оборудования лучше обращать внимание на более универсальные экземпляры. Это даст свободу выбора дальнейших действий и упростит решение возникших проблем.

Как же заставить принтер работать в сети? В нашем случае это делается следующим образом:

1. Подключаем принтер к любой машине, там, где его будет удобно расположить.
2. Проводим инсталляцию необходимых драйверов и настройку принтера для локальной печати.
3. Открыв в меню **Панель управления** папку **Принтеры** и перейдя на вкладку **Доступ**, устанавливаем флажок общего доступа и необходимые настройки.
4. Переходим к компьютеру, с которого предполагается печать на сетевом принтере.

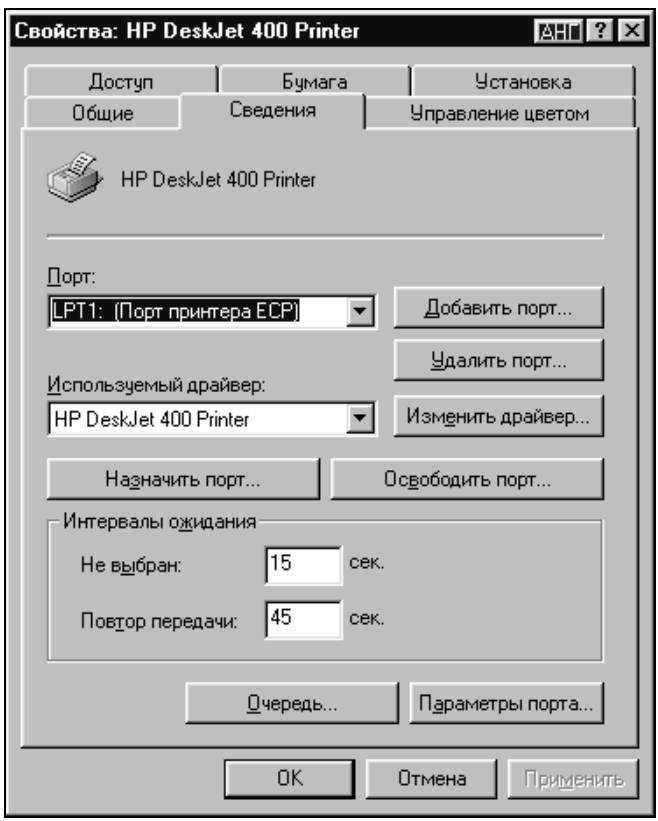


Рис. 2.29. Настройка сетевого принтера

5. Устанавливаем драйвер принтера так, как при локальной установке, но на предложение напечатать пробную страницу отвечаем отказом.
6. Выбрав в меню **Панель управления** папку **Принтеры**, открываем окно свойств принтера, переходим на вкладку **Сведения**, где видим настройки, подобные изображенным на рис. 2.29.
7. Нажав кнопку **Добавить порт**, вводим сетевой путь к принтеру. Для исключения ошибки при вводе пути и имени можно воспользоваться кнопкой **Обзор** и выбрать сетевой принтер из существующих в сети — конечно, только в том случае, если сеть работает, компьютеры с принтерами включены и настраиваемый компьютер прошел процедуру входа в сеть. Если для доступа к принтеру определен пароль, его следует ввести при первом запросе и сохранить (по предложению операционной системы), чтобы при печати не вводить пароль каждый раз заново.

После добавления порта в поле **Порт** появится возможность выбора порта принтера (рис. 2.30).

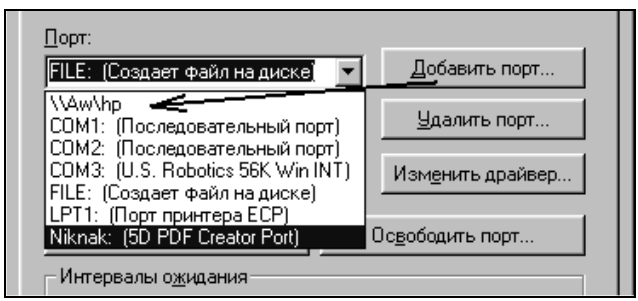


Рис. 2.30. Выбор порта принтера

Если есть несколько сетевых принтеров и для каждого установлен и настроен драйвер, можно, при необходимости, выбирать сетевой принтер. В свойствах каждого сетевого принтера должен быть выбран порт и соответствующий драйвер. В некоторых случаях принтеры позволяют использовать один и тот же драйвер для разных принтеров, а иногда возникшие проблемы с печатью в сети решаются подбором другого драйвера. Чаще всего взятый на сайте производителя обновленный драйвер принтера позволяет решить возникшие проблемы.

По окончании установки сетевого принтера следует напечатать пробную страницу. Различные принтеры имеют свои особенности сетевой настройки,

но внимательно ознакомившись со свойствами принтера, можно выбрать оптимальный вариант. При необходимости можно поэкспериментировать для выбора наиболее подходящих настроек.

Настраивая принтер для сетевой печати, необходимо обратить внимание на настройку очереди печати. Смысл опций очереди вполне понятен, а при затруднениях с их выбором следует провести пробную печать с различными установками и выбрать лучший вариант. При необходимости проводить печать из программ для DOS надо настроить параметры порта, поставив галочку напротив флажка очереди заданий печати из DOS.

Среди большого числа существующих принтеров могут представлять особый интерес принтеры со встроенным *принт-сервером* — устройством, которое позволяет использовать принтер в сети автономно, не подключая его физически к конкретному компьютеру. В качестве примера рассмотрим установку лазерного принтера KYOCERA FS-6900, который может поставляться со встроенным принт-сервером. Далее будет рассмотрен именно такой вариант этого принтера, и слова "принтер" и "принт-сервер" будут в ряде случаев синонимами.

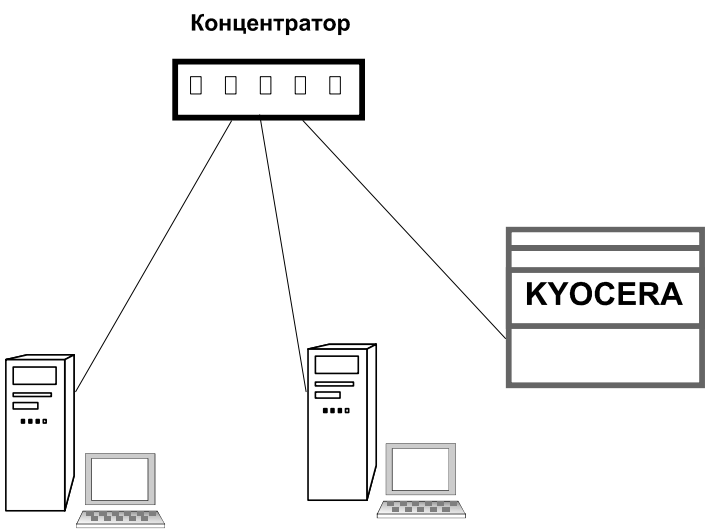


Рис. 2.31. Подключение сетевого принтера с принт-сервером к сети

В отличие от обычных принтеров такой принтер должен быть подключен непосредственно к сети. Для этого необходимо предусмотреть отдельную точку подключения принтера к сети. Как и компьютер, принт-сервер можно

подключить к хабу (концентратору) обычным кабелем — витой парой. На рис. 2.31 показано соединение двух компьютеров и принтера с принт-сервером в одну сеть.

К принтерам со встроенным принт-сервером должны прилагаться дистрибутивы как для локальной установки, так и для подключения принтера в сеть. В первую очередь, принтер устанавливается как локальный.

Установка принтера для ОС Windows 9*x*

Для установки необходимо вставить в дисковод компакт-дисков диск с драйверами принтера и, если не поддерживается автоматическая установка принтера, открыть папку **Принтеры**. В Windows 9*x* ярлык этой папки находится на Панели управления. Дважды щелкаем кнопкой мыши по значку **Установка принтера** (рис. 2.32).

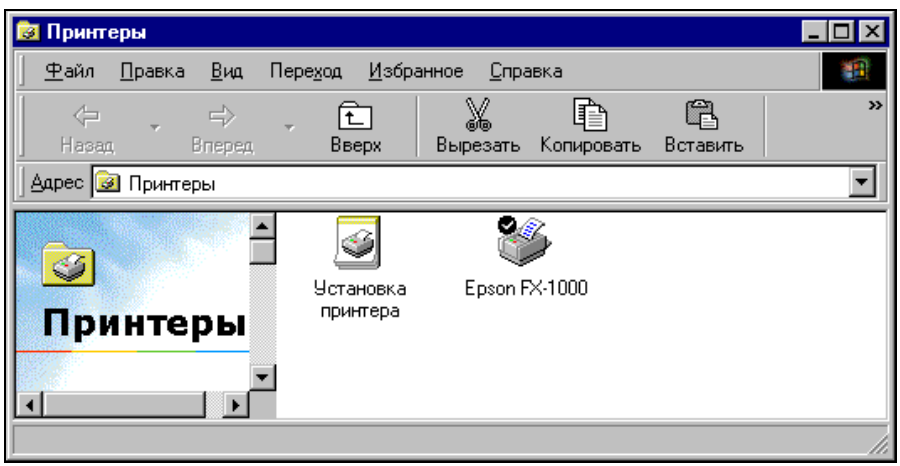


Рис. 2.32. Окно **Принтеры**

В открывшемся окне **Мастер установки принтера** (рис. 2.33) выбираем переключатель **Локальный принтер**. Откроется список драйверов, доступных в Windows (рис. 2.34).

В этом окне нажимаем кнопку **Установить с диска**.

Следующее окно позволит с помощью кнопки **Обзор** выбрать место размещения драйвера принтера (рис. 2.35 и 2.36).

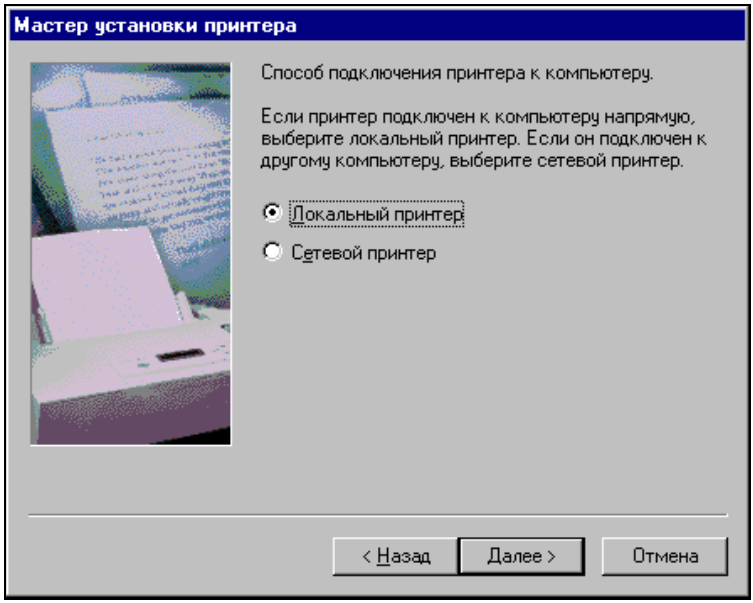


Рис. 2.33. Окно **Мастер установки принтера** для выбора варианта установки

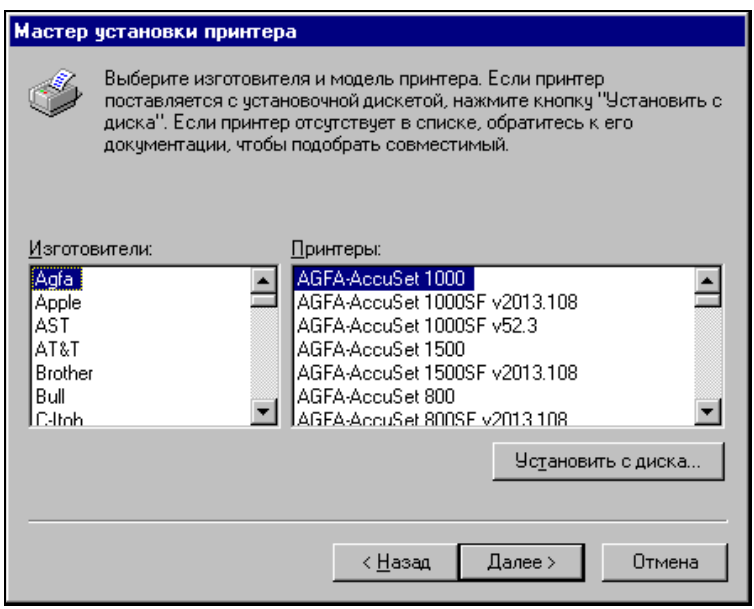


Рис. 2.34. Окно **Мастер установки принтера** со списком доступных драйверов

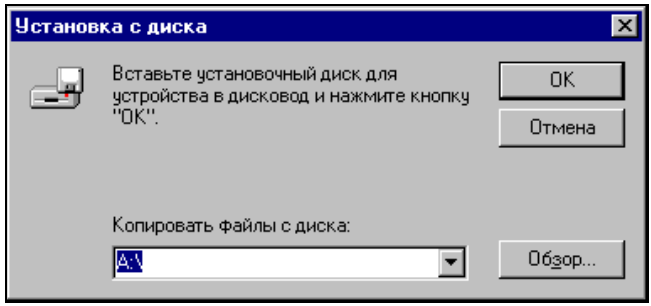


Рис. 2.35. Окно **Установка с диска**

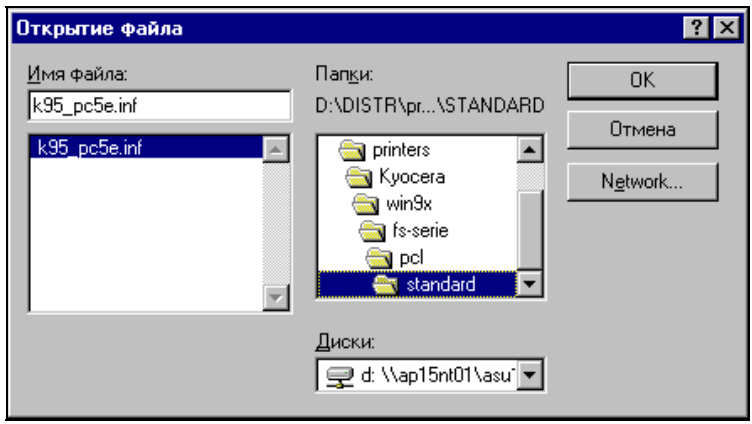


Рис. 2.36. Окно **Открытие файла**

Нажмите кнопку **ОК**. В новом окне (рис. 2.37) найдите драйвер вашей модели принтера и нажмите кнопку **Далее**.

В окне выбора порта (рис. 2.38) укажите порт LPT1.

В следующем окне (рис. 2.39) вы можете изменить название принтера и назначить его для использования по умолчанию.

В последнем, появившемся после нажатия кнопки **Далее**, окне (рис. 2.40) остается отказаться от печати пробной страницы и нажать кнопку **Готово**.

Теперь принтер появился среди установленных в окне **Принтеры** (рис. 2.41).

Но установка принтера не завершена. Наш принтер сетевой, да еще с принт-сервером. Необходимо настроить принт-сервер для работы в нашей сети. Для этих целей в дистрибутиве принтера есть специальная утилита KyoNetCon.

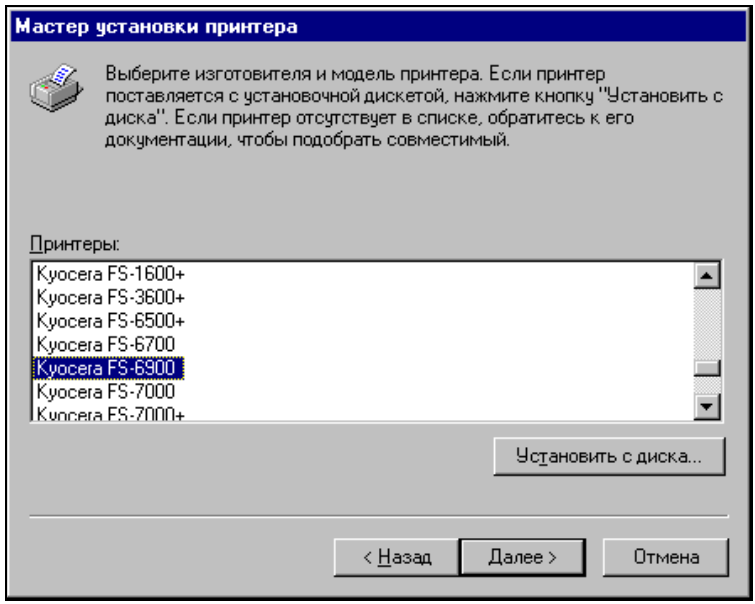


Рис. 2.37. Окно **Мастер установки принтера** для выбора драйвера принтера семейства Kyocera

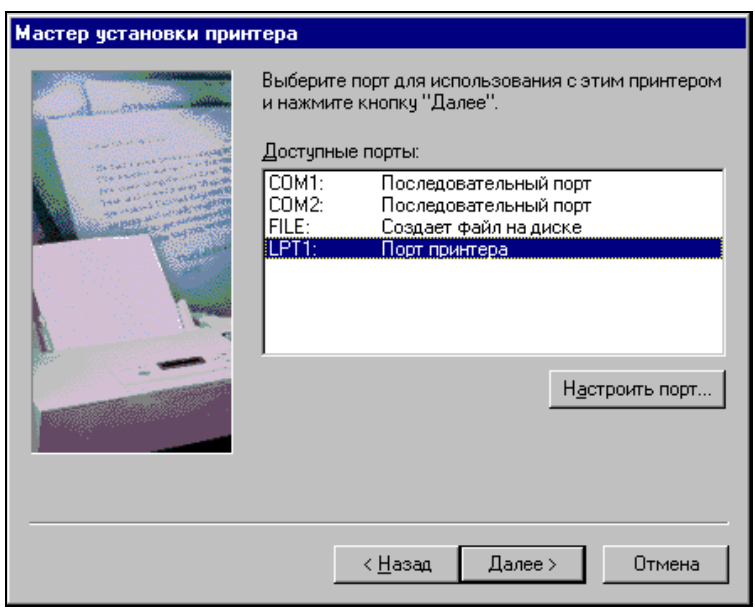


Рис. 2.38. Окно **Мастер установки принтера** для выбора порта

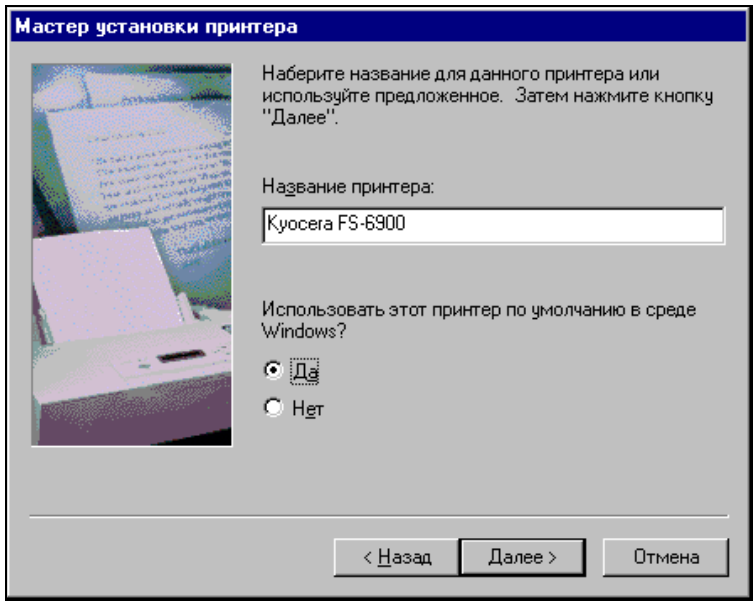


Рис. 2.39. Окно **Мастер установки принтера** для изменения имени принтера и назначения его использования по умолчанию

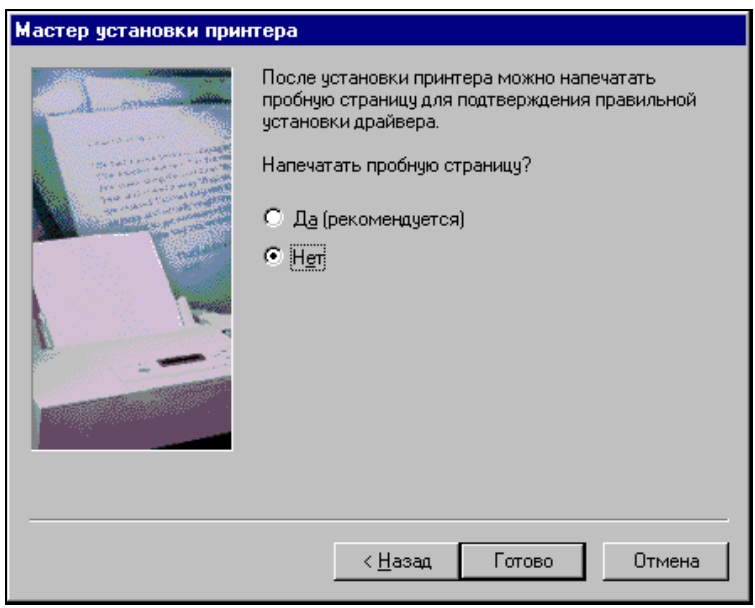


Рис. 2.40. Окно **Мастер установки принтера**, завершающее установку

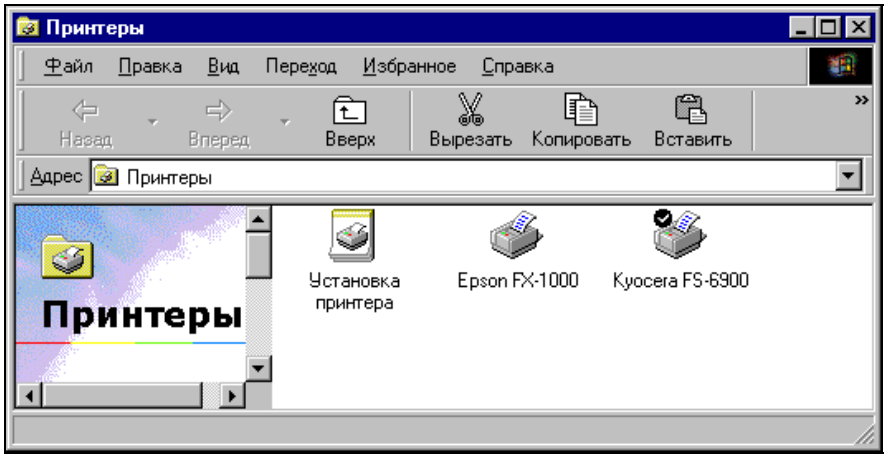


Рис. 2.41. Окно **Принтеры** с установленным принтером KYOCERA

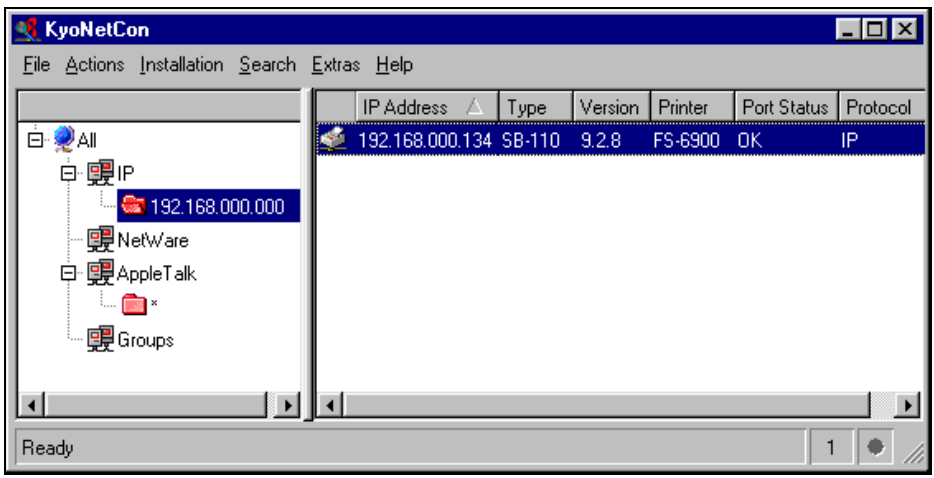


Рис. 2.42. Окно **KyoNetCon**

Для других принтеров и принт-серверов она будет иметь, конечно, иное имя. Эту утилиту необходимо установить на один из компьютеров сети. Лучше, если этот компьютер принадлежит сетевому администратору, поскольку по мере развития сети, возможно, придется менять некоторые настройки. На рис. 2.42 показано главное окно этой утилиты.

Утилита автоматически обнаруживает подключенный к сети и включенный принтер. В узле **IP**, который соответствует нашему типу сети, находим адрес

необходимого принтера и правой кнопкой мыши открываем меню, в котором выбираем пункт **Properties...** (Свойства). Следующее окно утилиты, показанное на рис. 2.43, позволяет настроить сетевые параметры принт-сервера.

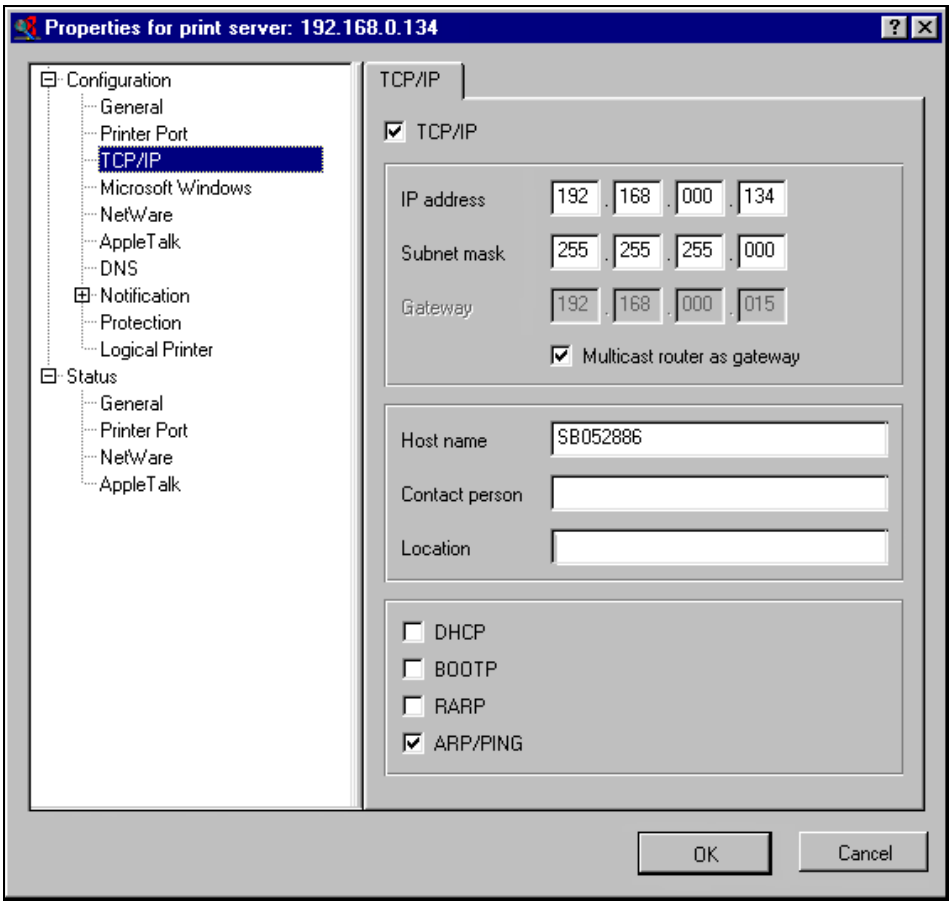


Рис. 2.43. Окно свойств для принт-сервера 192.168.0.134

IP-адрес, который указан в окне, принт-сервер выбрал себе сам, но мы можем изменить его в соответствии с нашими требованиями или оставить прежним. В любом случае, запишите этот адрес или запомните. Итак, мы установили принтер как локальный.

Остается воспользоваться еще одной утилитой, прилагаемой к принт-серверу. В случае установки принтера в среде Windows 9*x* — это Kyomon. Эту утили-

ту необходимо инсталлировать именно на том компьютере, на котором устанавливается принтер. После ее установки ничего внешне не изменится. Никаких окон эта утилита не имеет, но позволяет определить параметры принтера, находящегося в сети. После установки Kyomon можно изменить порт принтера, сделав его сетевым.

Щелкните правой кнопкой мыши на значке принтера в окне **Принтеры**, в появившемся меню выберите строку **Свойства** и откройте панель свойств принтера (рис. 2.44).

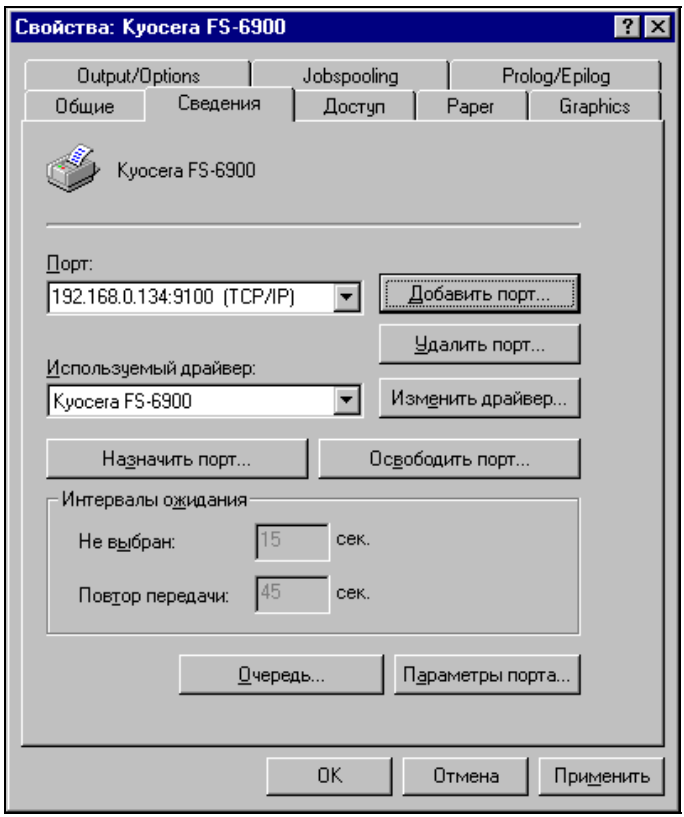


Рис. 2.44. Окно свойств принт-сервера KYOCERA

Откройте вкладку **Сведения**, нажмите кнопку **Добавить порт**. В открывшемся окне (рис. 2.45) выберите переключатель **Другой** и укажите в списке **KYOCERA Monitor**. Далее нажмите кнопку **ОК**.

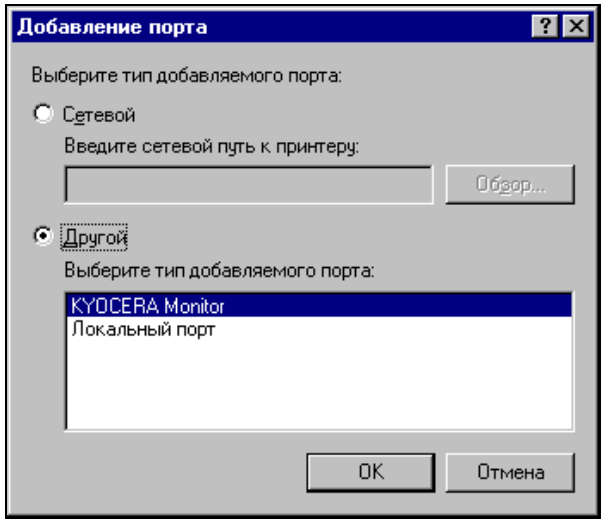


Рис. 2.45. Окно **Добавление порта**

Откроется окно **KYOCERA TCP/IP Port Configuration** (Конфигурация TCP/IP порта KYOCERA). В верхнем поле этого окна (рис. 2.46) необходимо указать IP-адрес принт-сервера, который вы запомнили или записали. Номер порта во втором поле лучше оставить без изменений. Теперь можно нажать кнопку **ОК**.

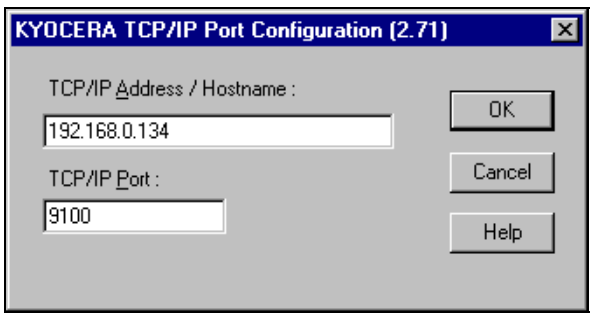


Рис. 2.46. Окно **KYOCERA TCP/IP Port Configuration**

Если к вашему компьютеру разрешен сетевой доступ, то на вкладке **Доступ** вы можете дать возможность участникам сети использовать и вновь установленный принтер (рис. 2.47).

Очередь печати будет обрабатываться вашим компьютером, если у другого пользователя при установке принтера будет выбран порт, соответствующий вашему компьютеру в сети.

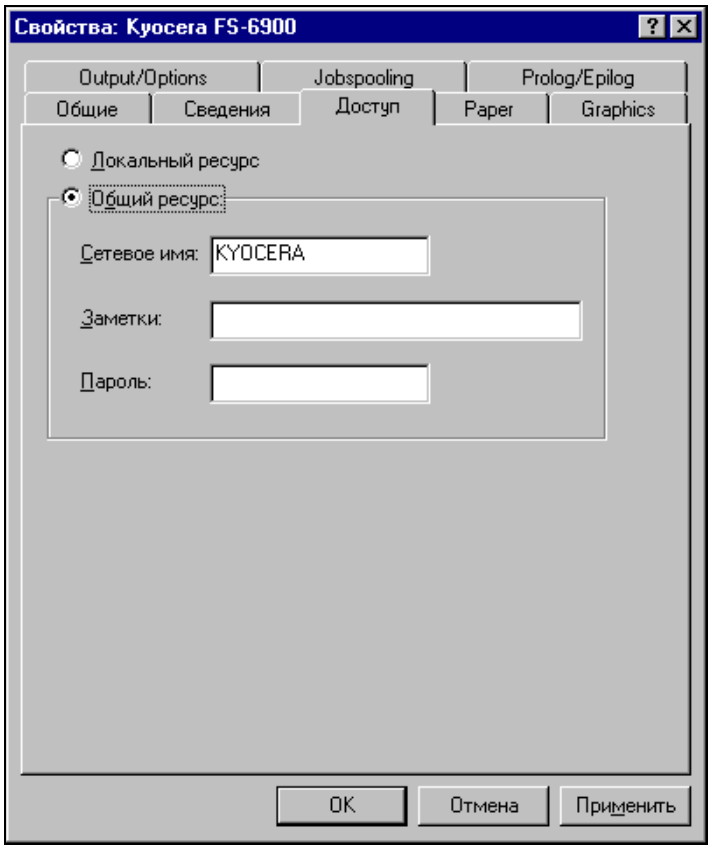


Рис. 2.47. Окно свойств принтера, вкладка **Доступ**

Установка принтера для Windows 2000/XP

Установка принтера для операционных систем Windows 2000/XP отличается от только что описанной. Прежде всего, необходимо выбирать драйверы, соответствующие операционной системе. Несколько отличается интерфейс окон и применяемые утилиты. Интерфейс — это дело привычки, и, имея некоторый опыт общения с компьютером, можно найти все необходимые окна.

В Windows XP, например, окну **Принтеры** из Windows 9*x* соответствует окно **Принтеры и факсы**, находящееся на Панели управления (рис. 2.48).

Для установки принтера необходимо в меню **Файл** выбрать пункт **Установить принтер**. Как и в других случаях установки нового оборудования, мастер установки проведет вас по всем этапам этого процесса. Рассмотрим лишь некоторые особенности установки сетевого принтера с принт-сервером в операционной системе Windows XP. Мастер установки принтера Windows 2000/XP может автоматически обнаружить и установить принтер, подключенный к LPT-порту компьютера. Но в нашем случае мы должны отказаться от автоматической установки и выбрать принтер самостоятельно. После установки на порт LPT1 необходимо добавить новый порт, нажав кнопку **Добавить порт** на вкладке **Порты** окна свойств принтера. Среди предложенных портов выбрать **Standard TCP/IP Port**. В свойствах порта установить сетевой адрес принтера. Нажать кнопку **OK**. Можно дать команду для пробной печати, чтобы убедиться, что принтер работает. Можно изменить порт и в процессе установки, выбрав **Standard TCP/IP Port**, а в свойствах порта установить сетевой адрес принтера. Так же, как и в случае с Windows 9*x*, можно разрешить доступ к принтеру другим пользователям. В целом, установка доступа к принт-серверу KYOCERA для операционных систем Windows 2000/XP даже проще, чем для Windows 9*x*, поскольку не требует применения дополнительных утилит, если не считать KyoNetCon для первичной настройки принт-сервера.

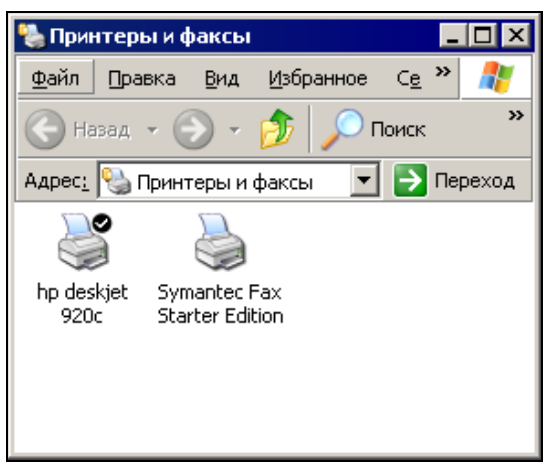


Рис. 2.48. Окно **Принтеры и факсы**

Сеть с Windows Vista

Операционная система Windows Vista по сравнению с предыдущими версиями Windows существенно упростила работу администратора локальной сети и компьютера по настройке сетевых подключений. Независимо от выбранного варианта настройки, мастера помогают не пропустить важные моменты, а сама система научилась определять параметры сети и даже показывать ее схематическое устройство.

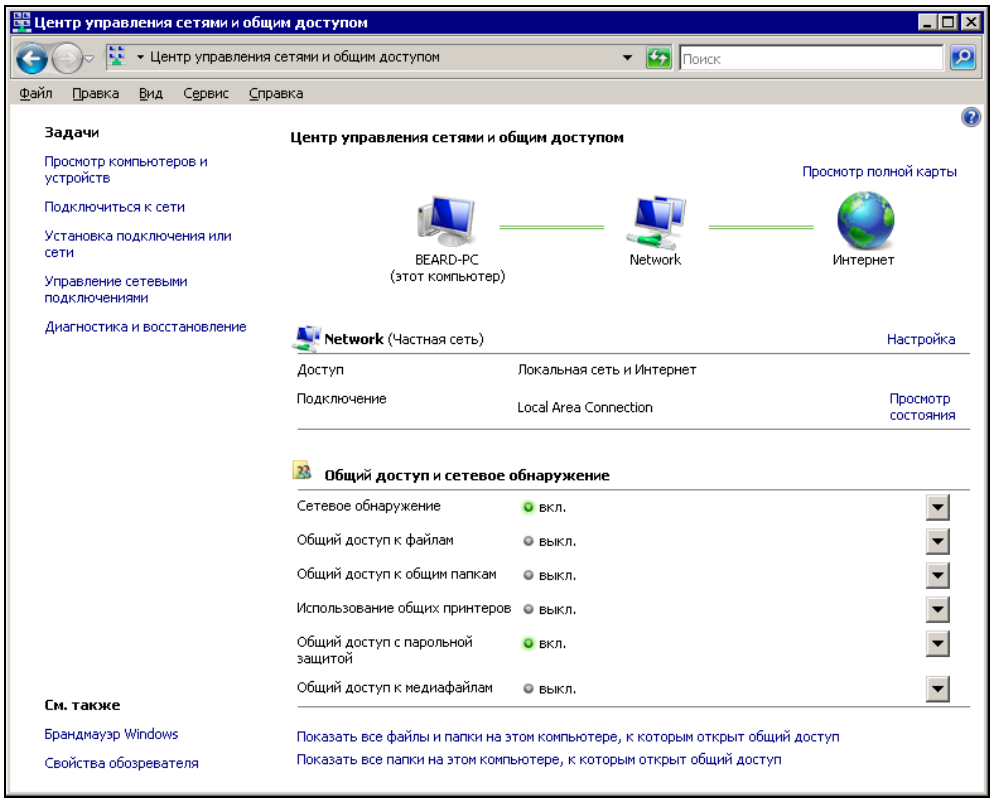


Рис. 2.49. Окно **Центр управления сетями и общим доступом**

Еще во время установки система с помощью нескольких наводящих вопросов настраивает сетевое подключение компьютера, если оно существует физически. Если во время установки системы компьютер находится в правильно настроенной локальной сети, через которую осуществляется выход в Интернет,

вам не придется настраивать подключение к Интернету и к сети. После установки системы все будет настроено.

Для доступа к различным настройкам сети удобно использовать окно **Центр управления сетями и общим доступом** (рис. 2.49), которое можно открыть из Панели управления. В этом окне показана карта сети, которую удалось определить системе. Пройдя по ссылке **Просмотр полной карты**, можно увидеть все компьютеры сети (рис. 2.50).

Устройства, которые системе не удалось отобразить на карте сети, можно обнаружить, пройдя по предложенной ссылке. Интересно, что среди этих устройств может быть отображен Проигрыватель Windows как отдельное устройство с именем компьютера, на котором он запущен.

Вариант сети, который показан на рис. 2.49 и 2.50, соответствует случаю с применением постоянно включенного ADSL-модема с Ethernet-подключением к сети. Если какое-либо сетевое оборудование будет отключено или, наоборот, добавлено, карта сети изменится, поэтому ее можно применять для визуального контроля состояния сети.

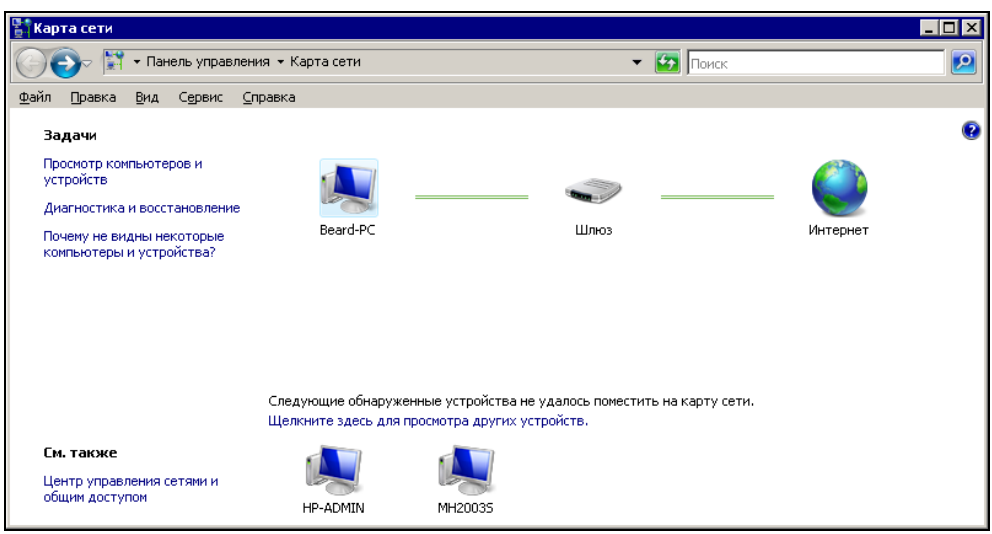


Рис. 2.50. Окно **Карта сети**

В данном случае все сетевые адаптеры компьютеров настроены одинаково. Все они получают свои настройки автоматически от DHCP-сервера, который содержится в ADSL-модеме и обнаруживается операционной системой каж-

дого компьютера сети. Такие настройки не требуют ручного назначения IP-адресов, и любой новый компьютер, включенный в сеть, сразу становится ее равноправным участником. Если в вашей сети нет DHCP-сервера, вы можете и самостоятельно выполнить настройки сетевых подключений.

Несмотря на краткость описания настройки сети с Windows Vista, уже можно представить себе, насколько просто выполняются сетевые настройки в этой ОС. Тем не менее сеть это не только настройки рабочих станций. Сетестроителю нередко приходится решать множество проблем, о решении которых мы и ведем разговор в этой книге.

Linux в вашей сети

Linux — это большое семейство операционных систем. Приверженцы Linux спорят между собой о преимуществах той или другой версии системы, но пользователи Windows, которые решили "пересесть" за компьютер с Linux, надеются увидеть привычный рабочий стол и офис. Среди всего разнообразия Linux можно выделить не бесплатную, но и не дорогую систему Linux XP. Система быстро развивается, разработчики осуществляют поддержку пользователей на своих форумах. Учитывая, что требования к оборудованию у этой системы не слишком высоки, и то, что под управлением этой системы может работать OpenOffice — бесплатный офисный пакет с возможностями, близкими к MS Office 2003, — а интерфейс близок к Windows XP, вполне вероятно, что скоро будут появляться машины с этой ОС и в вашей сети.

Одной из причин распространения Linux может стать и недостаток средств у организаций на приобретение достаточного числа лицензий на Windows и MS Office. Почему бы не перейти на Linux XP, или другую версию Linux, распространяемую в России, и на OpenOffice, если они полностью удовлетворяют все потребности ваших пользователей? Только приложения, которые пока в Linux работать не могут, останутся на Windows XP или Windows Vista.

Вот и получится, что в вашей сети окажутся не совсем привычные операционные системы.

Программное обеспечение для рабочей станции Linux

Среди программ, которые работают в среде Linux, есть почти все, что может потребоваться обычному пользователю. Но все же не все программы могут

быть запущены в Linux, несмотря на наличие средств, позволяющих запускать программы, написанные для Windows. Например, до настоящего времени нет программ машинного перевода под Linux. В таких случаях можно выходить из сложившейся ситуации двумя путями. Во-первых, учитывая, что рабочая станция находится в сети, можно воспользоваться другой рабочей станцией или сервером для запуска необходимого приложения через удаленный рабочий стол.

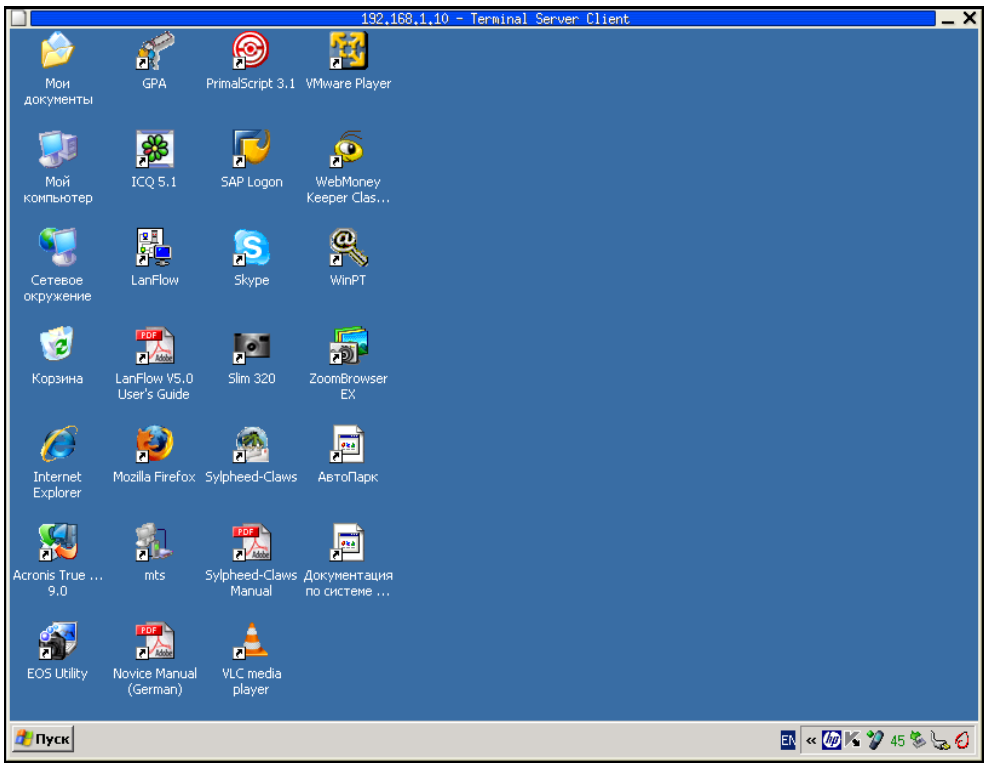


Рис. 2.51. Окно **<IP-адрес> — Terminal Server Client**

На рис. 2.51 показано окно Terminal Server Client, открытое на рабочей станции Linux XP.

Второй способ использования специфических Windows-приложений — это *виртуальный компьютер*. Правда, до недавнего времени установка виртуального компьютера под Linux не всегда удавалась начинающим пользователям Linux. Теперь VMware Workstation 6.0 прекрасно устанавливается на Li-

nux XP SR2 и другие современные версии Linux, перечень которых можно найти на сайте **vmware.com**.

Конечно, установка приложений под Linux отличается от аналогичной процедуры в Windows, но, немного почитав руководства, которых достаточно можно найти в Интернете, вы освоите необходимые для этого средства Linux. Для того чтобы вам не было очень страшно начинать установку виртуальной машины самостоятельно, приведем несколько строк, которые вы увидите в окне терминала во время установки программы. Работая в Linux, придется значительно чаще обращаться к окну терминала, чем к окну командной строки в Windows, которые во многом имеют сходство.

Открыть окно терминала можно прямо из контекстного меню рабочего стола **Создать терминал**. Так же, как и в Windows, вы можете настроить вид этого окна по своему вкусу, но сейчас мы рассмотрим только содержание окна во время установки VMware Workstation 6.0.

Само собой разумеется, что дистрибутив в виде файла VMware-workstation-e.x.p-42757.i386.rpm (это версия файла на момент написания этих строк, у вас будет более новая) заранее подготовлен и помещен в папку /tmp в файловой системе Linux XP.

> ***Примечание***
>
> Обратите внимание, что мы говорим о файловой системе, и не упоминаем о дисках, как в Windows. В Linux все диски объединены в файловую систему, состоящую из каталогов.

Для успешной установки программы требуются права администратора компьютера. Команда `su` вызывает сеанс суперпользователя root, остается ввести его пароль.

braginsky@lin.myhome[~]$ su

Password:

Для установки приложения из rpm-пакета выполняем команду, приведенную в следующем фрагменте. Ключ `force` позволяет программе установки не обращать внимания на возможные мелкие проблемы с версиями файлов. Кроме того, программа устанавливается поверх предыдущей версии и желательно не видеть запросов на замену файлов.

root@lin.myhome[/home/braginsky]# rpm -ivh --force VMware-workstation-e.x.p-42757.i386.rpm

Подготовка... ## [100%]

1:VMwareWorkstation ## [100%]

Установка завершается быстро. Далее при попытке запуска виртуальной машины программа установки сообщает, что необходимо конфигурировать программу:

root@lin.myhome[/home/braginsky]# vmware

vmware is installed, but it has not been (correctly) configured for this system.

To (re-)configure it, invoke the following command: /usr/bin/vmware-config.pl.

Запускаем процесс конфигурации так, как подсказала программа.

root@lin.myhome[/home/braginsky]# /usr/bin/vmware-config.pl

Далее на все вопросы программы отвечаем нажатием клавиши <Enter>, соглашаясь с выбором программы. Автоматически настраиваются все необходимые параметры.

Making sure services for VMware Workstation are stopped.Stopping VMware services: Virtual machine monitor [OK]
Blocking file system: [OK]

Bridged networking on /dev/vmnet0 [OK]

Host network detection [OK]

DHCP server on /dev/vmnet1 [OK]

Host-only networking on /dev/vmnet1 [OK]

DHCP server on /dev/vmnet8 [OK]

NAT service on /dev/vmnet8 [OK]

Host-only networking on /dev/vmnet8 [OK]

Virtual ethernet [OK]

Configuring fallback GTK+ 2.4 libraries. In which directory do you want to install the theme icons? [/usr/share/icons]

What directory contains your desktop menu entry files? These files have a.desktop file extension. [/usr/share/applications]

In which directory do you want to install the application's icon? [/usr/share/pixmaps]

Trying to find a suitable vmmon module for your running kernel. None of the pre-built vmmon modules for VMware Workstation is suitable for your running kernel. Do you want this program to try to build the vmmon module for your system (you need to have a C compiler installed on your system)? [yes]

Только один раз программа установки засомневалась, обнаружив несоответствие версии одного из компонентов системы с требованиями программы. Но в данном случае это различие не существенно. Можно не согласиться с предложенным отказом от дальнейших действий и вместо подтверждения `[no]` вписать самостоятельно `yes` и нажать клавишу <Enter>.

Using compiler "/usr/bin/gcc". Use environment variable CC to override. Your kernel was built with "gcc" version "3.4.4", while you are trying to use "/usr/bin/gcc" version "3.4.3". This configuration is not recommended and VMware Workstation may crash if you'll continue. Please try to use exactly same compiler as one used for building your kernel. Do you want to go with compiler "/usr/bin/gcc" version "3.4.3" anyway? [no] ***yes***

Далее удалены строки работы программы конфигурации. На все дальнейшие вопросы следует отвечать положительно.

В конце концов программа сообщает, что конфигурация завершена и программа может быть запущена. При этом указан путь к исполняемому файлу.

configuration of VMware Workstation e.x.p build-42757 for Linux for this running kernel completed successfully.

You can now run VMware Workstation by invoking the following command: "/usr/bin/vmware".

Enjoy, --the VMware team

root@lin.myhome[/home/braginsky]#

Можно так и поступить. Но можно воспользоваться окном **Start | Запустить приложение**. Введя в этом окне строку `VMware`, можно запустить установленную программу.

На рис. 2.52 показано окно VMware Worksation с уже работающим виртуальным компьютером на фоне рабочего стола Linux XP.

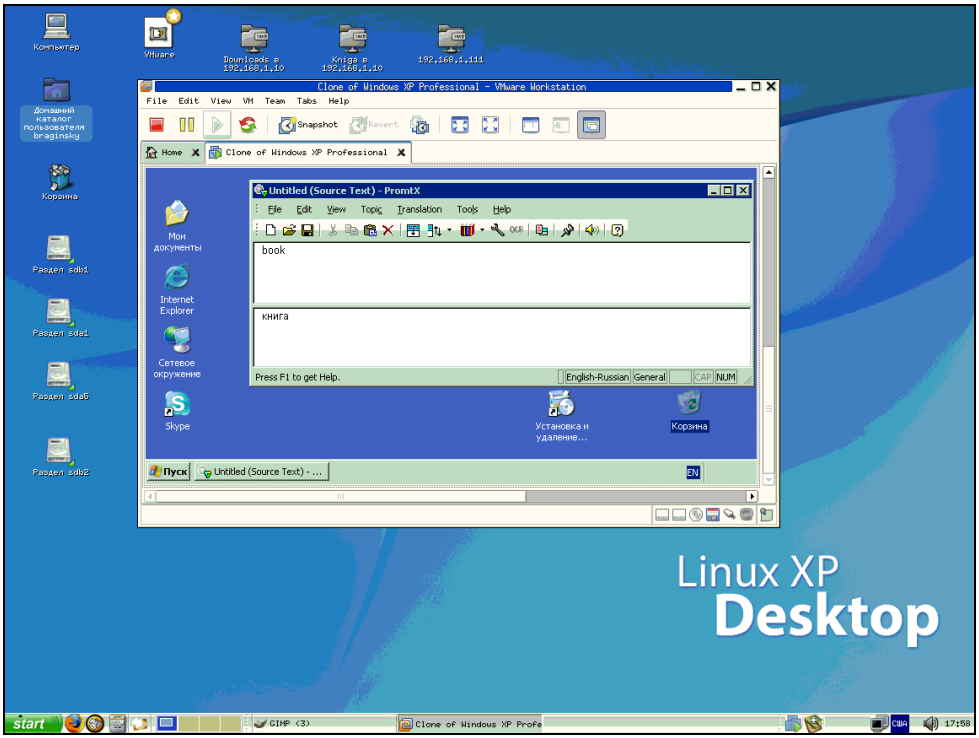


Рис. 2.52. Окно VMware Worksation
(с установленной и запущенной системой Windows XP)

Представляет интерес, что виртуальный компьютер, как и реальный, имеет свой IP-адрес и к нему можно подключаться любыми известными вам средствами. При этом окно виртуального компьютера может быть свернуто или помещено на другое рабочее место (в нижней части рабочего стола видно еще три доступных рабочих места). Сетевые пользователи смогут работать в среде Windows на не существующем реально компьютере.

Обычная работа в сети

Чаще всего сетевым пользователям требуется доступ к каким-либо файлам, находящимся в сети.

Выбрав **Start | Стандартные | Сетевое окружение**, можно получить доступ к сети.

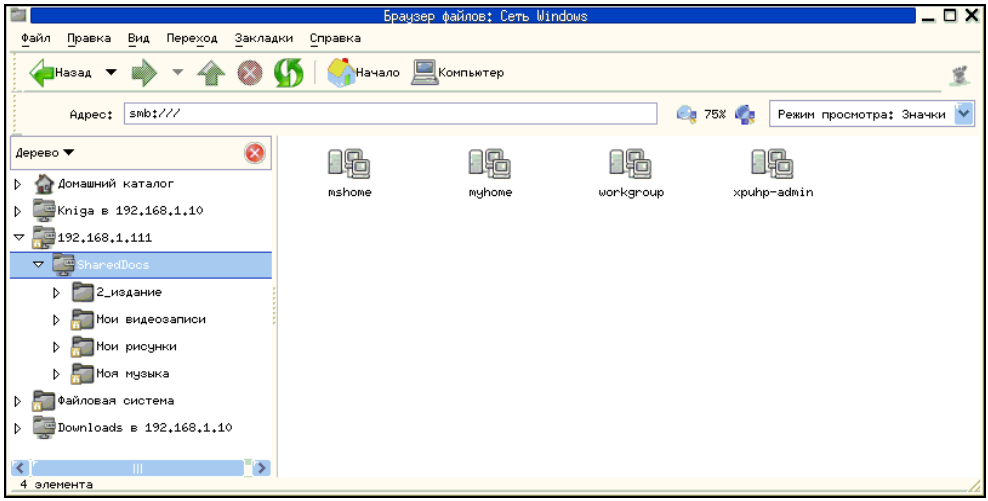


Рис. 2.53. Окно **Браузер файлов: Сеть Windows**

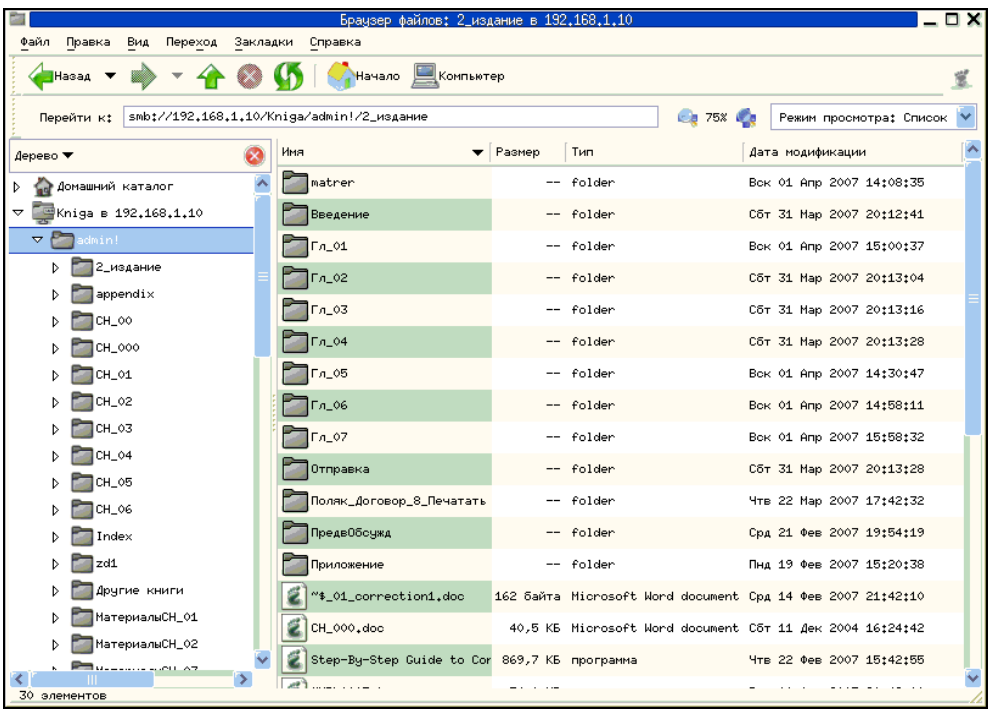


Рис. 2.54. Окно **Браузер файлов: <Каталог_в_IP-адрес>**

Правда, если ничего не вводить в строку **Адрес**, придется довольно долго ждать, пока Linux отобразит имеющиеся сети, рабочие группы или домены (рис. 2.53). Теперь можно, как на рабочей станции Windows, открывать рабочие группы, подключаться к серверам и рабочим станциям.

Если адрес компьютера с общедоступными ресурсами известен, то воспользовавшись оконным меню **Файл | Соединиться с сервером**, можно указать адрес компьютера, ввести учетные данные, а при необходимости указать конкретный каталог, к которому необходим доступ. На рабочем столе при удачном подключении будет автоматически создан ярлык соединения, который можно будет использовать в дальнейшем.

На рис. 2.54 приведено окно с открытым сетевым каталогом. Как видите, работа с файлами в сети для Linux XP не так уж сильно отличается от аналогичных процедур в Windows.

Окно терминала в Linux

Как открыть это окно (рис. 2.55), мы уже знаем. С помощью окна терминала мы установили виртуальный компьютер в реальной системе Linux XP.

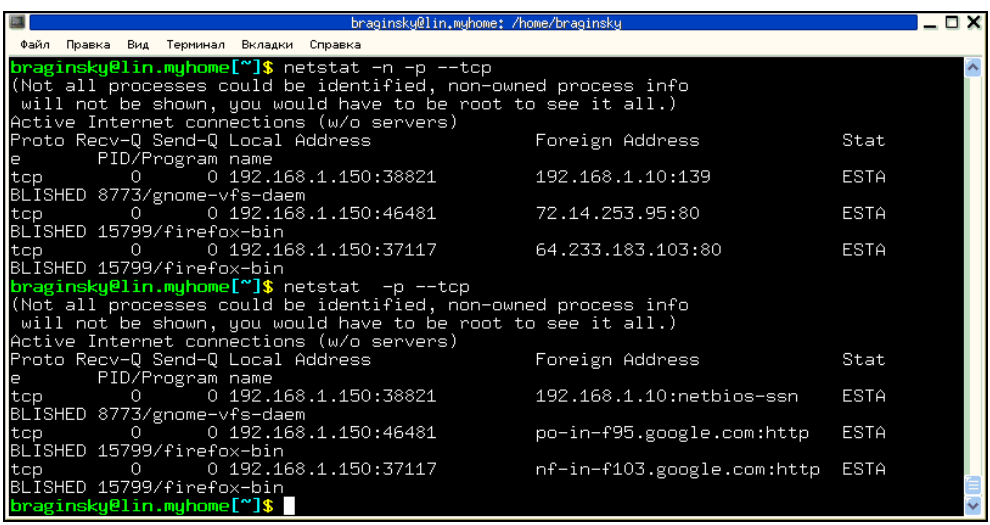


Рис. 2.55. Окно терминала

Но, как уже было сказано, этим окном можно пользоваться просто как командной строкой Windows. Совершенно аналогично командной строке можно вводить и выполнять известные или найденные по команде Help команды.

На рисунке показан результат выполнения известной вам команды `netstat`, которая позволяет узнать подробности о работе вашей сети, о подключениях компьютера к известным и неизвестным вам узлам.

Подробно о параметрах этой команды можно узнать в Интернете по адресу **http://www.opennet.ru/man.shtml?topic=netstat&category=1&russian=0**.

Пример создания сети в домашних условиях

На сайте **http://homenetworks.ru**, посвященном домашним сетям, есть публикация, как там указано, неизвестного автора, в которой с хорошим юмором и знанием дела рассказывается о проблемах, возникающих при строительстве сети и путях их решения.

> **"FRIENDNET"**
>
> Надеюсь, что кем бы ты ни был, тебя заинтересует или развлечет эта статья, однако по правде сказать, обращаюсь я к таким же маньякам, как и я сам.
>
> Речь пойдет об опыте создания и эксплуатации домашней компьютерной сети. "Зачем?" — спросят некоторые. Но другие, те, кто понимает, уже догадались, и на них-то сейчас и будет излит мой графоманский зуд.
>
> Страна буквально замусорена компьютерами, многие из которых оседают в жилищах граждан и обретают статус "домашних". В отличие от своих "деловых" и "ученых" собратьев, они долго томились без общения с себе подобными. И, наконец, настает великий час их объединения! Так вот, владельцы этого чуда, этого источника головной боли и виновника ссор с домашними, к вам я взываю. Если вы делали что-либо подобное, думаете о чем-то похожем или имеете конкретные планы, надеюсь, что шишки, набитые нашей компанией при запуске сети, помогут вам уберечь свои лбы.
>
> Не знаю, есть ли термин для подобного явления, но мне нравится словечко "FRIENDNET", и впредь я постараюсь его придерживаться.
>
> Наша дружеская компания живет в небольшом подмосковном поселке, и так получилось, что со временем у каждого из нас дома появились компьютеры. Как водится, рано или поздно возникла мысль, что неплохо было бы как-то обмениваться данными, да и поиграть во что-нибудь, в конце концов!

Первым опытом было использование позаимствованных на работе модемов. К сожалению, мы сразу столкнулись с недостатками этого средства связи при использовании его в домашних условиях.

Первое — мой телефон подключен через блокиратор, и к исходу второго часа обмена данными соседи начали роптать.

Второе — скорость передачи да и надежность соединения оставляли желать лучшего.

Третье — в условиях Подмосковья модем позволяет связаться лишь двоим абонентам. В общем, этот способ общения оказался для нас неудобным.

Не помню точно, кто из нас в шутку предложил проложить компьютерную сеть. Я в то время работал в фирме, занимающейся монтажом кабеля для сетей, и мучительно вчитывался во всю литературу, где встречалось слово сеть, желая заполнить пробел в знаниях. К концу апреля 1995 года пробел перестал быть таким заметным, а идея из области юмора перешла в область разговоров.

Несколько раз на конспиративных квартирах собирались пятеро пайщиков и обсуждали всевозможные варианты устройства предприятия, а главное — его экономическую целесообразность. По причине отсутствия оной один из пайщиков покинул предприятие, пытаясь при этом доказать, что оно невозможно в принципе.

В ходе дальнейших дискуссий образовались две партии:

- консерваторов (сторонников коаксиального кабеля);
- прогрессистов (сторонников витой пары).

Надо отметить, что единственным рассматриваемым вариантом был "ETHERNET".

Консерваторы, имеющие опыт эксплуатации сетей на коаксиальном кабеле, утверждали, что "витая пара" — миф, а также высказывали существенное соображение, что для "коаксиала" не нужен HUB[1].

Прогрессисты, к коим принадлежал ваш автор, настаивали на историческом будущем витой пары. Консерваторы не верили.

Партии прогрессистов пришлось пойти на отчаянный шаг. С немалым риском пришлось позаимствовать около восьмидесяти метров витой пары и два сетевых адаптера, подключаемых к параллельному порту.

[1] Хаб — *Ред.*

Как известно, при помощи TP (Twisted Pair, витая пара) два компьютера можно соединить сетью и без концентратора. В одно прекрасное майское утро такое соединение было осуществлено. Вы спросите как? Так получилось, что четыре участника нашей авантюры живут в трех стоящих по соседству пятиэтажных домах, представляющих собой звезду, в центре которой расположена моя квартира. Один из лучей звезды, лежащий в пределах одного здания, и был использован в качестве демонстрационного.

Мы рассмотрели несколько вариантов прокладки кабеля и остановились на последнем.

Первый вариант — через подвал, с использованием коммуникационных стояков в подъездах для подъема кабеля. К сожалению, строители наглухо замуровали коммуникационные отверстия, и этот вариант не прошел.

Второй вариант предусматривал подъем на крышу через окна, что могло вызвать недоумение жителей верхних этажей. От этого варианта мы также отказались.

Нами был избран третий вариант. Из моего окна на третьем этаже мы опустили кабель до уровня между окнами первого этажа и балконами второго этажа. Далее при помощи садовой лестницы прикрепили его специальными клипсами к стене и затем ввели в окно второго этажа. По дороге нам пришлось отвечать на вопросы удивленных обитателей первого этажа, что кабель де телевизионный, потому как антенна общественная барахлит и в телевизоре ничего не видно.

Наконец соединение (точка-точка) было запущено. С помощью "Personal Netware" мы увидели диски друг друга и запустили парочку простеньких игр. Это произвело определенное впечатление, и участники концессии начали делать взносы. Постепенно было приобретено необходимое оборудование, и кабель был проложен к остальным пайщикам. При прокладке кабеля между зданиями нам встретилось несколько других проблем.

Первая — долговечность свободно висящей проводки, эксплуатируемой в условиях русской зимы.

Вторая — необходимость соблюдения мер безопасности при пересечении силовых линий.

Третья — обилие любопытных, порой стремящихся помешать движению прогресса. Мы постарались обойти эти проблемы следующим образом.

Кабель был усилен с помощью авиационного троса, тонкого и прочного, прикрепленного к кабелю по всей длине. В одном случае расстояние между зданиями по прямой превышало 50 метров. На пути была улица с фонарями и линией электропередач. Для пересечения этого участка в качестве столбов мы использовали деревья, и в течение одного дня, при помощи альпинистского снаряжения одного из нас и высоченной армейской лестни-

цы другого, кабель был надежно закреплен на уровне третьего этажа, а участок, пересекающий линию электропередачи, был еще раз изолирован по всей длине. Надо отметить, что скучающая старушка пообещала пожаловаться на нас, если у нее перестанет работать телевизор. Так как телевизор поводов для беспокойства не давал, впоследствии она вызвала телефонного мастера, дабы покарать дерзких, но, увы, из этого тоже ничего не вышло.

К последнему из пайщиков кабель был проложен через крышу. И здесь были проблемы, но другого рода. Жители последнего этажа были недовольны визитами на крышу, после которых у них протекал потолок. Пришлось соблюдать конспирацию, дабы не повлечь впоследствии "вендетты" в отношении кабельного хозяйства. Таким образом, с этой частью проблем более или менее ясно.

Теперь коснемся "железа", необходимого для работы сети. Первое и самое больное место — это HUB, или концентратор, который должен быть установлен в центре звезды и быть подключенным к источнику питания. В условиях квартиры постоянно работающее устройство порой вызывает раздражение домочадцев, поэтому здесь надо выбирать компромиссный вариант. Лучше всего подключить это устройство через тройник с кнопкой и объяснить домочадцам, на что надо нажать в ваше отсутствие, если другие пользователи жаждут общаться друг с другом. Другим недостатком концентратора является его цена. Простенький восьмипортовый хаб сложно купить дешевле $150. Нам удалось приобрести такой — Palm-Hub ETHER-H9+ за $135. Что составило на каждого — $34.

Следующее по значимости и головной боли железо — это сетевые карты. Здесь возможны варианты. Сетевые карты можно найти от $20. Но не надо забывать о проблемах совместимости. Самое лучшее — взять для начала пару приглянувшихся карт и "обкатать" их на всех машинах в сети. Нужно также учитывать, что бывают системные платы, которые не понимают даже самых фирменных сетевых карт. В этом случае лучше всего сделать модернизацию машины, которая скорее всего уже давно назрела.

Перейдем теперь к носителю. Стандартный кабель UTP 3 Category стоит около $0.30 за метр. На сеть из четырех пользователей у нас ушло около 270 метров.

Для каждой рабочей станции необходимо также 2 разъема RJ-45 — $0.20 за штуку. Помимо этого, необходимы различные крепежные материалы. 100 штук крепежных клипс — $10, подойдут также ржавые гвозди и жесть от банок с тушенкой. 200 крепежных поясков — $20, в качестве замены могу посоветовать проволоку.

Авиационный трос — 150 метров (цена неизвестна), замену подбирайте сами.

В итоге полный комплект для одного пользователя в сети из 4-х рабочих станций стоит не дороже $100.

Весь кабель и крепежный материал был приобретен нестандартным путем. Вообще говоря, я считаю, что подобные вещи надо стараться делать за счет организаций, в которых вы работаете.

Теперь коснемся программного обеспечения. Для обмена данными и совместного использования принтеров и CD-ROM идеально подойдет и "WINDOWS 95", и "WINDOWS 3.11". К сожалению, в стране еще полно стареньких машин, и может получиться так, что у вас в сети окажутся ортодоксальные "DOS" пользователи. Для них подойдут "NW-Lite", "Personal NetWare" или "Lantastic". Эти основанные на "DOS" одноранговые сетевые операционные системы вполне позволяют решать простейшие задачи.

Поговорим теперь о преимуществах "витой пары" перед "коаксиалом". Надо отметить, что выигрыш в стоимости при использовании коаксиального кабеля оказывается мифическим. В нашем случае при топологии и расстояниях для коаксиального кабеля вместо хаба понадобился бы репитер. Если кто-то не согласен, то что же, сколько людей, столько мнений. Лично я стараюсь придерживаться рекомендаций разработчиков стандартов.

Еще одно преимущество "витой пары" в безопасной работе сети. Обрыв на линии легко локализуется и не влияет на работу других рабочих станций (в домашних условиях это существенно).

И еще одно преимущество состоит в том, что стандарт Ethernet 10Base-T использует для передачи данных 4 провода, а стандартный кабель UTP содержит 8 проводов. Оставшиеся провода идеально подходят для организации селекторной связи. Для нашей сети FRIENDNET мы приобрели такое устройство для четырех абонентов за $36. Это оказалось настолько удобно, что теперь для связи между собой мы практически не пользуемся телефоном.

Работы по монтажу и наладке сети мы завершили к концу августа 1995 года. Теперь при расставании один из нас частенько говорит: "Встретимся, дескать, в другом месте", или что-то в этом роде. За почти что два года работы у нас не было обрывов и вообще проблем с физическим соединением. Зимой 97-го подключился еще один пользователь. Мы перепробовали массу сетевых игр. Излюбленными оказались Action и Strategy (Doom, Heretic, Hexen, Quake, Duke, Rise Of Triad, Warcraft I/II, C&C, Red Alert, KKnD, MOO2...). Согласитесь, порой приятно погоняться за своим закадычным приятелем с бензопилой или запустить в своего заклятого друга ракетой, а то и раздавить Мамонтами или налететь Мигами.

По вечерам квартира оглашается воплями невинно убиенных, воем бензопилы, треском пулеметов, грохотом взрывов и прочими звуками, которыми программисты оснащают свои творения.

> Порой меня посещают сомнения, а не наркотик ли это все?
>
> Впрочем, если и наркотик, то чертовски приятный.
>
> Как и полагается, надо добавить пару слов о перспективах нашей FRIENDNET. Пара новых пользователей изъявила желание подключиться к нам. Один из нас прорабатывает вариант подключения нашей сети к "RELCOM" через местного провайдера. Вот пока и все.
>
> *Неизвестный автор*

Мы еще обратимся к произведениям этого автора в следующих главах, которые помогут литературно иллюстрировать процесс строительства сети.

Сеть заработала — что дальше?

В следующих главах мы рассмотрим возможности, предоставляемые некоторыми программами сторонних разработчиков, а также стандартные и нестандартные средства операционной системы, повышающие удобство работы и возможности сети.

Строительство сети — процесс творческий. Создав одноранговую сеть, вы не остановитесь на этом. Одноранговая сеть реально позволяет работать небольшому числу компьютеров. При напряженной работе сети, когда работает бухгалтерия, активно пересылаются файлы, используется принтер, берутся справки из какого-либо архива общего пользования, одноранговая сеть позволит активно работать только пяти-восьми компьютерам. Конечно, если такая загрузка сети не предполагается, то можно иметь и двадцать компьютеров в одноранговой сети, а учитывая, что не все из них одновременно входят в сеть (в домашней сети), то и больше. Перегрузка сети приводит к продолжительному ожиданию выполнения ваших запросов, иногда длящемуся несколько минут. Компьютеры "пытаются вставить свое слово", но запросов так много, что они сталкиваются, возникает коллизия, и компьютеры снова ждут возможности передачи своей порции информации. Существенно улучшить ситуацию может применение выделенного сервера. Даже в одноранговой сети четкое распределение обязанностей между рабочими станциями приводит к уменьшению количества проблем. Если, например, какая-либо рабочая станция используется только для печати, к ней подключен принтер, который используется всеми пользователями, но на ней никто не работает, то проблем с печатью и ошибками в работе приложений на этом компьютере

станет меньше. Возможно и введение некоторых ограничений. Если необходимо использовать вычислительную мощность компьютера в роли сервера приложений (это возможно в Windows 2000 и Windows 95/98 с привлечением программ сторонних производителей), то разумно ограничить число одновременных подключений. При использовании существующего парка персональных компьютеров, которые изначально предназначены для работы одного пользователя, не стоит заставлять компьютер "тянуть" нескольких пользователей. Даже серверная ОС Windows 2000 Server, установленная на специальном сервере, имеющем более 512 Мбайт оперативной памяти и процессор частотой 800 МГц, не может нормально обслужить в режиме сервера приложений более 20 пользователей. Разумные ограничения позволят, не делая больших вложений и применяя уже имеющиеся в вашем распоряжении средства, получить сеть с широкими возможностями.

Если ваша сеть работает на ваш бизнес, она со временем принесет прибыль, которую можно направить на ее реорганизацию и модернизацию. Домашние сети, которых появляется все больше, иногда переходят на коммерческую основу, что позволяет развивать их, расширяя и совершенствуя. На сайте **mosnet.ru** содержится информация о более чем двух сотнях домашних сетей Москвы. Многие из них не ограничиваются своими внутренними коммуникациями. Используя сервер какого-либо провайдера, они организуют скоростной канал в Интернет, который в состоянии обслужить практически всех пользователей сети. Администраторы и пользователи создают свои страницы, размещая их как на серверах самой сети, так и используя общедоступные возможности, которые предоставляет сервер **www.narod.ru**, где каждый желающий может разместить свою страницу бесплатно, поместив ссылку на ресурсы сети. Таким образом, домашняя сеть получает в свое распоряжение ресурсы всего Интернета.

Некоторые сети организуют доступ к своим ресурсам по телефонной линии. Правда, те сети, сайты которых мне довелось посетить, не используют такой доступ для широкой публики, как гостевой. Но и применение такого доступа "для служебного пользования" может существенно расширить коммуникационные возможности сети. Для доступа по телефонной линии приходится выделять телефон одного из пользователей сети в определенные часы. Несмотря на разумные ограничения (время доступа), пользователи получают возможность удаленного доступа к ресурсам своей сети с не имеющего доступ к Интернету компьютера. Есть домашние сети, которые пытаются развить свой сетевой бизнес, что может принести доход, позволяющий осуществить обновление оборудования и модернизацию сети в направлении

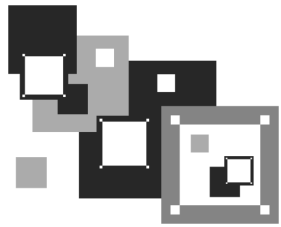
увеличения быстродействия, обновить парк оборудования, предназначенного для коллективного использования.

В следующих главах будут рассмотрены средства, чаще всего не входящие в состав операционной системы Windows 9*x*, но позволяющие существенно расширить возможности вашей сети. Эти средства не всегда бесплатны, но стоимость их вполне разумна, и их приобретение по силам практически каждому желающему. Вполне возможно, что со временем вы решите отказаться от этих средств, перейдя на технологии, использующие UNIX или другие операционные системы, не родственные системам Microsoft. Все чаще известные фирмы предлагают приобрести универсальный сервер для рабочих групп с предустановленной операционной системой Linux. Такой сервер выведет вашу сеть в Интернет, станет почтовым отделением внутри локальной сети, свяжет каждого пользователя сети с его собственным почтовым ящиком у провайдера, будет прекрасным файловым сервером. Но наша текущая задача — получить сеть с минимальными затратами, используя в основном то, что уже имеем. Да и творческий подход предполагает, что все нужно потрогать своими руками. Радиолюбитель, самостоятельно собирающий радиоприемник из бывших в употреблении деталей, получает удовлетворение не оттого, что его приемник обладает какими-то исключительными свойствами. А столяр-любитель, смотря на табурет, изготовленный самостоятельно, не претендует на соревнование с известной мебельной фирмой. Да и вы сами разве не заглядывали уже в свой компьютер с целью поменять какое-то устройство или установить новое, добавить памяти? Сколько времени вы уделили настройке своего любимого компьютера? А сколько радости было, когда заработала ваша первая простенькая программка? Творческий процесс не заменить самым современным и даже бесплатным готовым решением. Иногда, правда, мы упоминаем оборудование и программное обеспечение, которое позволяет получить результаты достаточно высокого уровня. Так, нами уже рассматривалась операционная система Windows 2000, которая не является близкой родственницей Windows 9*x* и потому обладает своими особыми свойствами и возможностями. Установив Windows 2000 или Windows 2000 Server и пользуясь руководством и справочной системой, можно настроить ее для работы в сети, получив некоторые возможности без особых усилий. Но эти сведения даются для ориентировки в мире программного обеспечения и аппаратных средств, которые в дальнейшем позволят самостоятельно продвигаться к более сложным решениям. Вполне возможно, что, попробовав применить более сложные и дорогие средства, вы обнаружите, что вам это не

нужно, что никакой выгоды вы не получили, и сеть ваша не стала работать лучше. Все зависит от конкретных обстоятельств и требований. Мне известна сеть, принадлежащая довольно крупной организации, имеющей конструкторское бюро, которое разрабатывает сложную технику, работая если не на всю, то на половину страны. Но сеть этой организации не вышла за рамки одноранговой уровня с операционной системой Windows 9*x*. Потребности организации были удовлетворены, а поддержка такой сети в рабочем состоянии не требовала больших затрат. В других учреждениях уже были приобретены современные программные сетевые средства (по требованию вышестоящей организации). Но переход на них так и не был осуществлен, так как привел бы к необходимости замены оборудования, которое не соответствовало требованиям нового программного обеспечения. Само программное обеспечение потребовало серьезных затрат на его приобретение с соблюдением авторских прав, а реального эффекта от его внедрения не предвиделось. Программы, которые используются на этом предприятии, были разработаны своими силами и прекрасно работают в среде, для которой разрабатывались. Мода, а особенно неукоснительное следование ей, стоит дорого. Соизмеряя свои потребности со своими возможностями, имея опыт достижения необходимых результатов простыми средствами, вы сможете принять верное решение, когда встанет проблема выбора пути развития вашей сети. Во всяком случае, затраты на преобразование и модернизацию сети должны быть соизмеримы с достигаемым эффектом. Для чего, например, приобретать дополнительное оборудование и программное обеспечение, если задача состоит в эпизодической передаче одного-двух файлов между двумя компьютерами? В этом случае даже кабель не очень нужен, поскольку такую передачу можно осуществить через телефонную линию с помощью модема, используя HiperTerminal — программу, входящую в состав Windows, или применяя другие терминалы, например из состава Norton Commander. Для работы с таким терминалом модем должен поддерживать работу в DOS. Распространенные по причине невысокой цены модемы под Windows (Winmodem) не могут работать без загрузки этой операционной системы. Их работа поддерживается программой, работающей под управлением Windows. Некоторые из этих модемов не могут работать и с Windows 2000, которая не поддерживает работу драйверов VxD, широко применяющихся в других Windows. Для постоянной и оперативной связи двух пользователей уже нужна линия связи (кабель), а для повышения комфортности связи можно использовать программу типа Intranet Chat. В случае необходимости регулярного и оперативного доступа нескольких пользователей к ресурсам одной рабочей станции есть яв-

ный смысл выделить ее отдельно (конечно, если позволяет материальная база). Эта рабочая станция станет выделенным сервером сети, который может использоваться как файловый сервер или как сервер приложений. Возможны другие варианты применения выделенных серверов. Они могут выполнять функции маршрутизаторов, т. е. управлять направлением передачи информации при соединении двух или более подсетей, хранить таблицы имен и обеспечивать связь одной или нескольких небольших локальных сетей с глобальными сетями наподобие Интернета. Эти возможности мы рассмотрим в следующих главах.

Глава 3



Иерархическая сеть

Настроив одноранговую сеть, вы в скором времени можете почувствовать необходимость ее развития. Во-первых, сеть работает только при условии включения по крайней мере двух машин. Если хранение файлов распределено по разным машинам, то для получения необходимой информации придется ждать включения компьютера, на котором она хранится. Если ваша сеть находится в офисе, это не будет существенной проблемой, при условии что соблюдается трудовая дисциплина и все машины включаются в начале рабочего дня. Но в домашней сети, когда ваш сосед слева (условно) работает в ночь, а сосед справа часто уезжает в командировки, вам, возможно, придется долго ждать удачного стечения обстоятельств, чтобы переписать важную для вас информацию или передать сообщение. А если вы решите организовать выход в Интернет через одного из участников сети для более рационального использования самого быстрого подключения, то кому из соседей вы отдадите предпочтение? Есть сети даже не домашние, а весьма известные и серьезные, в которых приходится мириться с режимом жизни пользователей. Это, например, FIDO. Сеть использует коммутируемые соединения, причем телефон системного оператора может быть занят его женой. Конечно, "сисоп" (системный оператор) договорился со своей половиной, что после 19:00 до 00:03 телефон находится в полном распоряжении пользователей, ожидающих очереди, чтобы получить или передать свою порцию информации. Но все же, не очень это удобно. Даже в FIDO удается организовать круглосуточный доступ к некоторым телефонам. Выходом из сложившейся ситуации может быть создание файлового сервера. Для этого необходимо выбрать наиболее подходящий компьютер из существующих в вашей сети или приобрести дополнительную машину. Поскольку требования к серверу зависят от конкретной сети, следует провести хотя бы приблизительный расчет ее параметров. Большим подспорьем в расчетах может стать автоматическое проектирование сети, которое предлагается некоторыми сайтами в режиме on-line.

Автоматическое проектирование сети

Бурное развитие средств автоматического проектирования привело к тому, что теперь каждый пользователь ПК, имеющий доступ в Интернет, может получить проект будущей сети буквально за считанные минуты. Такую возможность предоставляет компания "Тауэр-Сети и Технологии" с помощью *своей разработки — системы интерактивного проектирования информационных систем* **www.netwizard.ru**. Она ***бесплатно*** осуществляет разработку эскизных проектов информационных систем любой сложности. Все консультации по вопросам выбора, монтажа и использования сетевого оборудования, кабельных систем и вычислительной техники проводятся ***бесплатно***. Если все же заплатить некоторую сумму, то вы получите более широкие возможности выбора оборудования, применяемого в сети. Попробуем получить проект несложной сети с помощью этого прогрессивного метода.

Войдя на страницу компании, нам придется зарегистрироваться, внеся сведения о себе в предлагаемые формы. После ответов на несколько вопросов программы о наших требованиях к будущей сети начинается расчет и формирование документации. Проект содержит схему сети, структурную схему, спецификацию и смету на активное оборудование. Конечно, проект поддерживается определенными фирмами и рекомендует использовать оборудование этих фирм. Но, даже если у вас уже есть бóльшая часть оборудования, вы вполне можете дополнить его, руководствуясь спецификацией. Некоторые элементы система навязывает, не спрашивая вас, но вы можете подойти к проекту рассудительно и использовать только необходимое оборудование. В спецификации приведены как цены на оборудование, так и расценки на работы по прокладке кабеля и монтажу сети. Даже приблизительно составленный этой системой проект поможет вам сориентироваться в ценах и определить ваши возможности. Предположим, что будущая сеть состоит из двух рабочих мест, расположена компактно на одном этаже, расстояние между машинами и хабом около десяти метров. До сих пор мы не рассматривали вариант сети с выделенным сервером, но автоматический проектировщик самостоятельно предлагает включить в состав сети сервер. Конкретные типы рабочих станций и серверов, операционные системы для них система не указывает. Конкретный выбор зависит от множества факторов, включая и личные пристрастия администратора.

Посмотрим на подготовленные автоматическим проектировщиком документы.

Схема локальной вычислительной сети

Схема локальной вычислительной сети (рис. 3.1) выглядит совсем просто. Показан сервер, коммутатор и компьютеры. Никаких особых характеристик элементов сети не указано. Число компьютеров указано на один больше, чем задумано в нашем проекте. Это сделано потому, что выбирая условия проекта, было сделано предположение о развитии сети, добавлении в нее позднее еще одной машины.

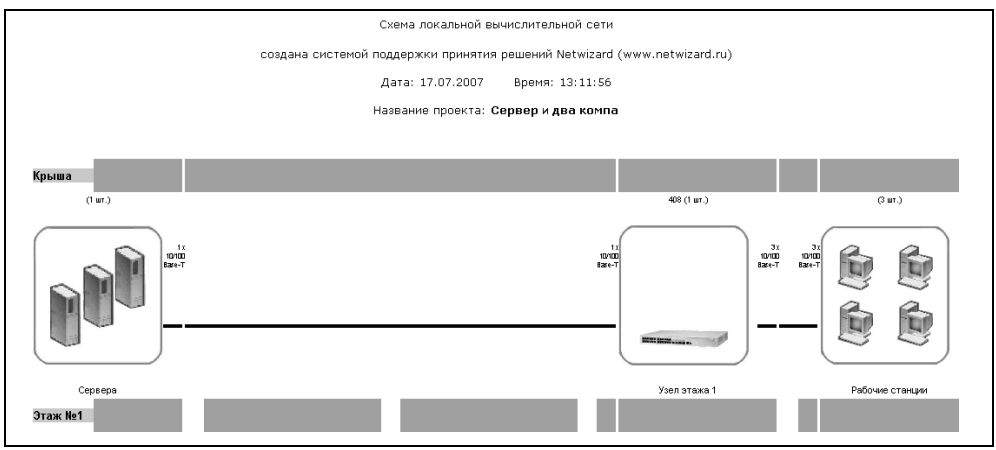


Рис. 3.1. Схема локальной вычислительной сети

Структурная схема компьютерной сети

Структурная схема компьютерной сети (рис. 3.2) содержит описание элементов сети. Количество коммуникационных центров в нашем варианте сети соответствует количеству хабов (коммутаторов). Все компьютеры подключены к одному устройству, позволяющему им связываться друг с другом и с сервером. Каждый ПК подключен к сети через свой порт. Поэтому в проекте указано, что количество активных портов — 2.

Главный коммутационный центр. В нашем случае — это вся компактно расположенная сеть. В больших сетях с несколькими серверами могут применяться несколько коммутационных центров. Среди них есть главный и подчиненные коммутационные центры, осуществляющие связь как с компьютерами главной сети, так и с машинами других сетей, которые могут быть

связаны с главной. Для упрощения проекта при "заказе" мы отказались от управления активным оборудованием (например, можно управлять коммутаторами), а также от его резервирования.

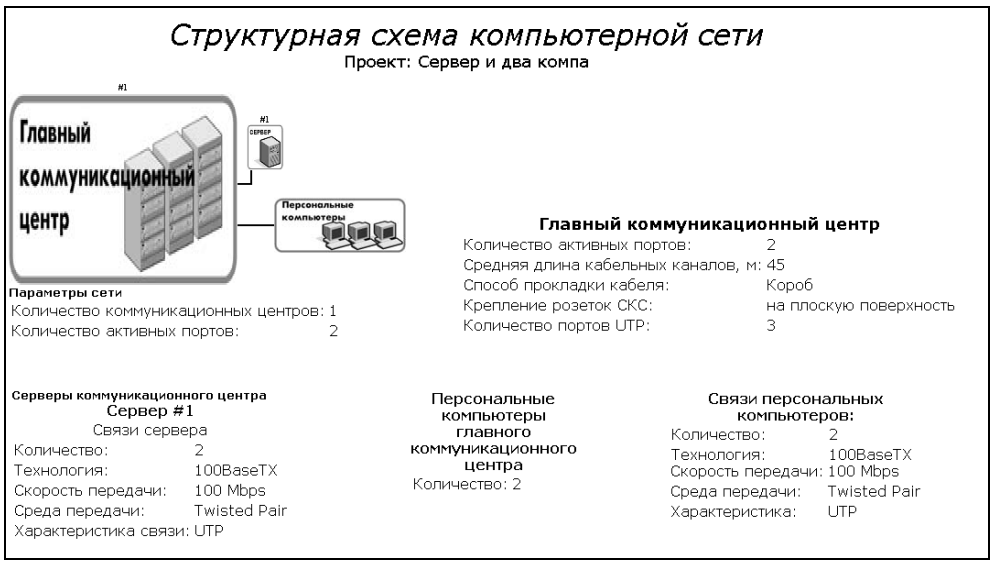


Рис. 3.2. Структурная схема компьютерной сети

Сметный расчет оборудования

Сметный расчет оборудования (рис. 3.3) содержит наименования и цены на активное оборудование сети. В нашем случае к такому оборудованию относится единственный коммутатор. Предложенная проектировщиком модель имеет 32 порта. С точки зрения возможностей дальнейшего развития сети это весьма разумно. Нельзя заранее предполагать сколько сетевых принтеров, IP-телефонов, другого сетевого оборудования появится в будущем.

Спецификация

В спецификации (рис. 3.4) перечислены почти все "мелочи", о которых недосуг задуматься, когда мечтаешь об организации сети и представляешь ее работу.

Сметный расчёт оборудования

произведён системой поддержки принятия решений Netwizard (www.netwizard.ru)

Дата: 17.07.2007 Время: 13:12:10

Название проекта: **Сервер и два компа**

В этом здании узел здания отсутствует.

Номер коммуникационного узла этажа: **1**
Восходящие порты: количество: **1** тип: **10/100 Base-T**
Нисходящие порты: количество: **3** тип: **10/100 Base-T**
Вид узла: **Узел Этажа**
Вид оборудования: **Активное оборудование**

Вид оборудования	SKU	Название	Цена	Количество	Стоимость
Коммутатор	J4097B	HP ProCurve Switch 408	86	1	86
				Итого:	86

Номер коммуникационного узла этажа: **1**
Нисходящие порты: количество: **1** тип: **10/100 Base-T**
Вид узла: **Узел Этажа**
Часть узла: **Серверная ферма**
Непосредственно к восходящим портам этого коммуникацинного узла этажа подключаются сервера.

Общая стоимость: **86** US$

При расчёте использованы GPL цены производителя.
(Global Price List - общемировой список цен)
Они не учитывают региональных особенностей, проектных скидок и промоакций.

Рис. 3.3. Сметный расчет оборудования

Кабели должны быть аккуратно уложены и защищены от случайного смещения половой тряпкой, от повреждения передвигаемой мебелью и от других неблагоприятных воздействий. В спецификации приведены детали кабельных каналов с указанием цен, размеров и необходимого количества. Вполне возможно, что у вас уже есть какие-либо иные средства для прокладки кабеля или вы упростите систему прокладки из-за архитектурных особенностей строения, где будет находиться сеть. Но в любом случае, изучив спецификацию, вы не упустите незаметные с первого взгляда, но важные моменты в процессе организации сети. В разделе "Пассивное сетевое оборудование" перечислены кабели, разъемы, розетки, панели для монтажа разъемов и подключения кабелей. Для удешевления проекта при малых размерах сети от этих элементов можно отказаться, проводя подключения компьютеров к хабу напрямую, без использования промежуточных панелей, а также управляя пи-

танием от сети переменного тока с помощью выключателей на сетевых фильтрах. Их применение при отсутствии источников бесперебойного питания очень желательно. И, наконец, в спецификации приведен перечень работ по монтажу сети. Для небольшой сети, монтируемой своими руками, вся стоимость работ может быть равна нулю. Налицо существенная экономия по сравнению с затратами при вызове специалистов.

Спецификация

Проект:Сервер и два компа

Артикул	Наименование товара	Ед. изм	Кол-во	Цена, $	Сумма, $
Кабельные каналы					**356,47**
NCT1050	Короб 100х50	м	30	8,74	262,20
NCI1050	Соединитель 100х50	шт	13	1,46	18,98
NJC1050	Заглушка на шов 100х50	шт	13	1,46	18,98
NAF1050	Плоский угол 100х50	шт	2	4,72	9,44
NWP1050	Заглушка внутренняя 100х50	шт	3	2,18	6,54
YT4	Короб 40х25	м	15	2,28	34,20
YC4	Соединитель 40х25	шт	7	0,56	3,92
YEP4	Заглушка 40х25	шт	1	0,39	0,39
YAF4	Плоский угол 40х25	шт	2	0,91	1,82
Пассивное сетевое оборудование					**447,97**
PID-00058	19" Patch Panel, 24xRJ45 KATT with cover, 568B, UTP, Power Cat, 1U, Graphite	шт	1	96,49	96,49
25.B016G	19" Ring Run (Jumper) Panel, 1U, Graphite	шт	1	18,47	18,47
45.0B.011.D022E	Patch Cord RJ45, 568B-N, UTP stranded, PowerCat, 1m, Grey	шт	2	3,75	7,50
45.0B.011.D024E	Patch Cord RJ45, 568B-N, UTP stranded, PowerCat, 3m, Grey	шт	1	4,92	4,92
39-504-PS	UTP PVC Cable PowerCat 4-pair	м	135	0,34	45,90
17.1B.011.A042P	Euromod 1xRJ45, M1 Straight, 568B, UTP, PoweCat, White	шт	3	3,50	10,50
17-0413-02	Euromod Blank, M1, White	шт	3	0,65	1,95
42-501-32	Розеточная коробка для установки на плоскую поверхность Surface Box UK 1G 32mm	шт	3	2,52	7,56
17-0111-02	Лицевая панель розетки Labelled Single Gang Wallplate, United Kindom, 86x86x10mm, White	шт	3	1,56	4,68
SWJ-003-2	Шкаф настенный 19", 15U, 737x600x300, со стеклянной дверью в стальной раме	шт	1	250,00	250,00
Работы по монтажу сети					**524,00**
MUTP5	Прокладка кабеля UTP	м	135	0,30	40,50
MKOROB	Монтаж короба	м	77	2,00	154,00
MKOROBB	Монтаж короба на бетонной стене	м	9	2,50	22,50
MROZ1	Установка розетки RJ-45	шт	3	10,00	30,00
MRACK	Установка шкафа	шт	1	150,00	150,00
MPATCH	Монтаж патч-панели, 1 порт	шт	3	4,00	12,00
TUTP	Тестирование UTP/STP порта	шт	3	5,00	15,00
MDOC	Подготовка документации на СКС	шт	1	100,00	100,00
ИТОГО					**1 328,44**

Рис. 3.4. Спецификация

Техническое задание на разработку проекта компьютерной сети

К сожалению, в настоящее время автоматический проектировщик не готовит техническое задание (ТЗ) на разработку компьютерной сети. Тем не менее в ряде случаев ТЗ может потребоваться. Возможно, что в будущем эта функция пректировщика заработает снова, а пока рассмотрим основные разделы ТЗ, чтобы можно было составить его самостоятельно.

Название проекта: "Проект сети на два пользователя".

Дата и время создания: 18.07.2007 19:56:42.

Общие положения

Данное техническое задание составлено на основе анализа требований заказчика к создаваемой компьютерной сети.

Описание задачи

1. Основные параметры.

   Компьютерная сеть проектируется для 1-го этажа здания, в котором необходимо обеспечить взаимодействие двух персональных компьютеров. Кабельная инфраструктура строится на базе одного главного коммуникационного центра. Проектируемая сеть должна обеспечить решение следующих задач:

   - сетевое хранение файлов и сетевая печать;
   - электронная почта.

2. Распределение персональных компьютеров по коммуникационным центрам.

   Главный коммуникационный центр — 2 штуки.

3. Активное сетевое оборудование.

   Коммутатор на 32 порта (указать тип).

4. Параметры производительности:

   - полоса пропускания канала связи с рабочими станциями должна составлять не менее 100 Мбит/с.

5. Управление трафиком.

   Средства эффективного управления трафиком в сети не требуются.

6. Структурированная кабельная система:

   - для связи с серверами нужно применять кабель типа "неэкранированная витая пара";
   - для связи с рабочими местами необходимо использовать кабель типа "неэкранированная витая пара";
   - на каждом рабочем месте необходимо установить 2 порта кабельной системы.

7. Параметры кабельной системы главного коммуникационного центра:
   - среднее расстояние от коммуникационного центра до рабочего места составляет 10 м;
   - монтаж кабельной системы в комнатах должен быть выполнен в узком коробе;
   - бетонные стены составляют 10%.
8. Программное обеспечение:
   - программное обеспечение должно быть представлено продукцией корпорации Microsoft;
   - в качестве операционной системы персональных компьютеров необходимо применять Windows XP, при этом предпочитаемый язык интерфейса — русский;
   - в качестве офисных приложений для персональных компьютеров должен использоваться программный продукт MS Office 2003 Standard, при этом предпочитаемый язык интерфейса приложения — русский.
9. Центральные серверы и персональные компьютеры.

   Для центральных серверов проекта должно быть выбрано оборудование группы (указать изготовителя и тип):
   - количество центральных серверов должно равняться 1;
   - распределение приложений и пользователей по серверам приведено в табл. 3.1.

Таблица 3.1. *Распределение по серверам*

Серверы уровня 1	**Распределение пользователей по серверам**	
	Сервер электронной почты (кол-во клиентов)	**Файловый и принт-сервер (кол-во клиентов)**
Сервер 1	2	2

10. Необходимая конфигурация сервера № 1:
    - тип процессора: обычный;
    - количество процессоров в сервере: 1;

- объем оперативной памяти (ОЗУ) сервера: 512 Мбайт;
- необходимый объем дискового пространства: 80 Гбайт;
- желаемый тип корпуса: монтируемый в стойку (RackMount);
- количество линий связи сервера: 2;
- скорость передачи линии связи должна составлять 100 Мбит/с.

11. Источники бесперебойного питания.

    Требуется обеспечить бесперебойным питанием следующие компоненты компьютерной сети:

    - активное сетевое оборудование;
    - серверы;
    - рабочие станции.

    Для организации бесперебойного питания активного сетевого оборудования и серверов необходимо использовать распределенную систему бесперебойного питания.

    Время работы от батарей должно составлять не менее 7 мин.

Однажды зарегистрировавшись на сайте **www.netwizard.ru**, вы можете пересчитывать свою сеть столько раз, сколько будет необходимо. За это с вас платы не возьмут, кроме платы за время, проведенное в Интернете. Расчет, подобный приведенному выше, длится около 5 мин. Более сложные задания, возможно, потребуют большего времени. Обращение к такому помощнику избавит вас от большого количества ошибок при разработке сети. А незначительные отличия вашего замысла от предложенного проекта не должны вас пугать — такие вопросы вы можете разрешить самостоятельно.

Выбираем сервер

Какими особыми свойствами должна обладать машина, претендующая на роль сервера в нашей сети? Многое зависит от размеров и задач сети. Если выделенный сервер предполагается использовать как сервер приложений, это должна быть очень серьезная машина. Компьютер, рассчитанный на работу одного пользователя с современными приложениями, требует уже более 512 Мбайт оперативной памяти, винчестер 80 Гбайт и графический ускоритель для игрушек. Запустив два-три прожорливых офисных приложения, мы

уже заставим эту машину изыскивать резервы ресурсов, увеличивать своп-файл и "тормозить" при обработке более или менее объемных файлов. Что же говорить о сервере приложений, доступ к которому получат несколько пользователей? Определенно, без многопроцессорной машины эта затея не удастся. Поэтому реальные характеристики сервера приложений вы сможете узнать у продавца, когда наберете достаточно средств для приобретения чудо-компьютера. Пока этого не случится, придется довольствоваться файл-сервером. Надо сказать, что большинство современных офисных и домашних сетей пользуются именно файл-сервером, но позже мы все же рассмотрим вариант работы с удаленным компьютером, как с сервером приложений. Этот же компьютер может выполнять попутно еще несколько функций, работая по совместительству маршрутизатором, например почтовым сервером, или выполняя еще какую-нибудь экзотическую работу. Для файлового сервера требования существенно ниже, чем для сервера приложений. Ему не приходится много "думать", от него требуется лишь надежное хранение информации и отправка ее по первому запросу клиента, имеющего право доступа к ней. Другие задачи, возложенные на такой сервер, могут занимать небольшую часть его ресурсов и не вызовут проблем.

Очень часто в качестве файлового сервера применяют обычный персональный компьютер. Если альтернативное решение невозможно, то можно пойти и на такой вариант. Ориентируясь на него, мы и рассмотрим настройки сервера. Но надо учесть, что обычный ПК не может в полной мере выполнять функции файлового сервера, поскольку не имеет некоторых, присущих именно серверу свойств. А свойства эти определяются особенностями рабочего цикла файлового сервера — чтение, изменение и запись файла. Изменение, правда, в большинстве случаев проходит на другой машине, и серверу остается начало и завершение цикла. Но именно эти моменты требуют от сервера очень ответственного отношения к своим обязанностям. Представьте, что вы создали новый текстовый или графический шедевр, потратив несколько часов или даже дней, а когда в очередной раз решили взять с сервера этот файл для предоставления заказчику или для вынесения на суд зрителей и читателей, его там не оказалось... А может быть, и оказался, но чрезвычайно похудевший и абсолютно нечитаемый. В чем дело? Кто виноват? Как компенсировать потерю? Легче болезнь предупредить. Возможно, что в момент последнего сохранения файла моргнул свет и незащищенный файловый сервер не смог правильно записать ваш шедевр, хотя и очень старался. Если бы около него стоял в тот момент ИБП — источник бесперебойного питания, который на тот краткий миг отдал бы часть своей, запасенной в аккумуляторах, энергии, то трагедии не случилось. Возможна и другая причина порчи

файлов — ошибка файловой системы или дефект поверхности на винчестере сервера. Для защиты от такого рода проблем файловый сервер снабжают жестким диском повышенной надежности, обычно с SCSI-интерфейсом (Small Computer Systems Interface — интерфейс малых компьютерных систем), да еще с зеркально отраженными дисками, на которых повторяется информация. Для пользователей виден лишь один диск. В случае потери данных на одном из дисков информация будет тут же восстановлена с отраженного диска. Выполняется такое отражение программными средствами (как в Novell NetWare) или аппаратными. Возможно также резервирование самих серверов, путем соединения двух машин для синхронной записи всей информации, приходящей на любую из них. SCSI-контроллеры в дисковой системе обладают еще одним важным свойством. Они существенно уменьшают нагрузку на центральный процессор, решая самостоятельно задачи ввода/вывода. Так, если на одном шлейфе в вашем сервере будут два IDE/ATA-винчестера, а один из них выйдет из строя (пусть даже временно), задержавшись в фазе чтения сбойного участка диска, то и второй диск не сможет выполнять свою работу до завершения операции первым диском. У SCSI-дисков такой проблемы не возникает, но и цена их несколько выше обычных винчестеров. Можно учесть эту особенность дисковой системы и подключать IDE-винчестеры к разным слотам на материнской плате. Можно также заставить сервер с обычными дисками проводить регулярное резервное копирование данных на второй винчестер, используя для этого моменты с наименее интенсивной нагрузкой.

Возможно, что подходящим решением будет использование RAID (Redundant Array of Inexpensive Disks — массив недорогих дисков с избыточностью). RAID может быть выполнен как аппаратно в виде отдельного устройства, так и программно — средствами операционной системы (NetWare, Windows NT/2000/2003), с использованием установленных в машине дисков. Но в любом случае не помешает копирование важных данных на носитель, не связанный с компьютером постоянно. Ассортимент таких носителей и цены на них позволяют выбрать подходящий вариант для любой конфигурации сервера вашей сети.

Следует уделить внимание также механизмам, которые не связаны напрямую с вычислительными процессами, но при неисправности этих механизмов вычислительные процессы могут прекратиться вовсе. Система охлаждения блоков питания процессоров требует особого внимания. Регулярная профилактика кулеров и замена их при подозрении на скорый выход из строя существенно повысит надежность вашей сети. Не слишком быстрые процессоры двух-четырехлетней давности могут проработать достаточно долго да-

же при остановившемся вентиляторе. Процессоры последних серий, рабочая частота которых достигает 3 ГГц и выше, не протянут без принудительного охлаждения и часа. Для некоторых из них предлагаются системы с водяным охлаждением. Не следует отказываться от программного средства поддержания оптимального температурного режима процессора.

В последнее время фирмы-производители уделяют достаточно много внимания выпуску сравнительно высоконадежных серверов начального уровня с заложенными в них необходимыми дополнительными функциями. Так что выбор остается за вами. А поэкспериментировать в любом случае можно на обычной рабочей станции, временно исполняющей роль сервера.

При больших размерах сети следует выбрать операционную систему, специально предназначенную для работы на сервере. Огромным потенциалом обладает и Windows 2000/2003. Но и привычные Windows 98/XP имеют массу возможностей, которые могут с успехом применяться на сервере маленькой сети. При этом отсутствуют материальные затраты на приобретение новой операционной системы и затраты времени на ее освоение. Надежность системы на обычных машинах обеспечивается с помощью зеркальных дисков и файловой системы NFS (Network File System — сетевая файловая система), которая не позволит использовать сервер иначе, чем по непосредственному назначению. Для обычной работы файлового сервера рекомендуется иметь 16 Мбайт оперативной памяти на каждый гигабайт используемого дискового пространства. Соблюдая это условие, можно обеспечить одновременную работу с сервером пятидесяти пользователей сети. Физические ограничения на доступ к дискам сервера могут быть вызваны недостаточной пропускной способностью канала связи (сетевая карта — кабель — хаб — кабель — сетевая карта), интенсивной работой сети, частым возникновением коллизий. Для повышения пропускной способности сети можно рекомендовать не использовать устаревшие хабы, а применить коммутаторы, которые направляют приходящие через них запросы на ту машину, к которой они адресованы, и не загружают трафиком сегменты, не находящиеся непосредственно на пути следования сигнала.

Установка на сервер операционной системы Windows 2000 Server

Если, прочитав книгу, вы решите, что вам необходима серьезная серверная операционная система семейства Windows, то лучшим выбором на сегодняшний день будет Windows 2000 Server. Она несколько отличается от

обычных ОС. Обычный компьютер — рабочая станция — может работать под управлением любой версии Windows, но Windows 2000 Server на рабочей станции не нужна. Эта операционная система специально разрабатывалась для сервера, для управления вычислительными сетями. Возможности, которыми она обладает, позволяют без лишних хлопот эффективно администрировать достаточно крупные сети. Тем более эта система будет надежно управлять небольшой сетью, соблюдая необходимый уровень защиты информации и надежности ее хранения. Существует и более новая Windows Server 2003, возможности которой несколько шире.

Процедура установки Windows 2000 Server на сервер почти ничем не отличается от установки системы на любой другой компьютер, однако некоторые отличия все же есть. Прежде всего необходимо отметить, что после запуска сервера в рабочем режиме сложно, а иногда и невозможно, изменить или добавить компоненты операционной системы. Несколько лучше дело обстоит с программным обеспечением. Во многих случаях Windows 2000 Server не требует перезагрузки после установки новых программ. Это позволяет расширять возможности сервера "в горячем режиме". Но операционная система должна устанавливаться сразу в необходимой конфигурации. Важно сразу решить, какую роль будет выполнять этот сервер, будет единственным или вторым сервером в сети, если вторым, то будет ли он главным. Мы будем ориентироваться на ситуацию, когда наш сервер единственный в сети. В отличие от Windows NT, а тем более от Windows 98, Windows 2000 Server включает очень важный компонент — Active Directory, содержащий всю информацию о пользователях, компьютерах, других объектах сети, а также информацию о правах этих объектов и правах доступа к ним. Подробное описание Active Directory не входит в нашу задачу, его можно найти в справочниках по операционной системе Windows 2000 Server. Но очень важно, устанавливая операционную систему, сразу иметь четкое представление о том, будет ли этот сервер контроллером домена или он будет играть роль подчиненного сервера. В случае если у вас единственный сервер, ему необходимо дать роль контроллера домена. Имя компьютера при этом должно состоять не более чем из 15 символов (это обеспечит совместимость со старыми операционными системами других компьютеров сети), не должно содержать пробелов, должно являться комбинацией латинских букв, цифр и символов подчеркивания.

В процессе установки Windows 2000 Server необходимо указать некоторую информацию:

- имя компьютера (сервера), например `myserver`. Полное имя сервера будет состоять из имени компьютера и имени домена, например **myserver.firma.dom**;

- имя домена. Если ваш сервер не входит в другие домены и является единственным, то имя домена может быть любым, например **firma.dom**. Где **firma** — это либо название фирмы, либо название рабочей группы, **dom** — это имя глобальной зоны сети, по аналогии с **ru**, **com**, **org** в Интернете. Если у вас есть зарегистрированное имя домена в Интернете, то лучше использовать именно это имя. Это позволит вам держать на вашем сервере свой сайт и обеспечивать доступ к нему из Интернета. Все компьютеры, входящие в ваш домен, должны иметь одинаковое имя рабочей группы, соответствующее имени домена (**firma**). Это упростит работу компьютеров в сети. Если необходимо подразделять пользователей на отделы, функциональные группы или еще каким-либо образом, то Windows 2000 Server позволяет осуществить это средствами Active Directory. Обслуживая сеть, вы сможете управлять группами более эффективно, чем "старыми" рабочими группами;
- пароль учетной записи администратора. Пароль может содержать не более 14 символов;
- количество пользовательских лицензий на подключение к серверу. Если вы не успели приобрести достаточное количество лицензий, то можно просто указать необходимое их количество, и сервер разрешит подключаться всем вашим пользователям, позже можно приобрести недостающие лицензии. При наличии одного сервера в сети удобно использовать лицензии, определяющие количество одновременно подключенных пользователей. Если число подключений достигло количества лицензий, то сервер будет отклонять все последующие подключения. Лицензирование можно применять и для ограничения нагрузки на сервер;
- список компонентов операционной системы, которые вы хотите установить. Большую их часть можно добавлять после установки;
- режим работы сервера: сервер приложений или файл-сервер. Для работы сервера приложений необходимо обеспечить терминальный доступ пользователей. Причем если на компьютерах-клиентах установлены операционные системы ниже Windows 2000, то потребуются дополнительные лицензии на терминальный доступ. Кроме того, установка программ на сервер терминалов имеет много особенностей. Иногда требуются дополнительные компоненты значительного объема, которые можно найти в Интернете. Например, установка Office 2000 со стандартного инсталляционного диска невозможна без этих дополнительных компонентов. Если вам необходимо иметь терминальный доступ к серверу лишь в целях администрирования, то эта возможность предоставляется при любом вари-

анте установки. Всегда есть два доступных и не требующих лицензий сеанса для администраторов.

Установка может быть проведена с локального привода CD-ROM или по сети. Для реализации второго варианта требуется, чтобы на компьютер была уже установлена другая операционная система. Это может быть как Windows любой версии, так и DOS (в книге будет рассмотрен вопрос настройки рабочих станций под управлением MS-DOS для работы в сети). Особый интерес представляет предварительная подготовка винчестера на другом компьютере. Команда `Winnt32`, с помощью которой можно начать установку на компьютерах с предустановленной операционной системой Windows NT или Windows 2000, имеет среди прочих ключи: `/tempdrive:буква_диска` и `/syspart:буква_диска`. Запустив программу установки с такими ключами, мы заставим ее скопировать загрузочные файлы на диск и пометить его как активный. Данный диск можно установить в другой компьютер. После загрузки этого компьютера установка будет продолжена.

В случае сетевой установки может быть полезен ключ `/makelokalsource`. При наличии этого ключа все установочные файлы будут скопированы на локальный жесткий диск, и процесс установки продолжится даже при прекращении сетевого доступа. Такая ситуация возможна, когда предыдущая операционная система полностью заменяется на новую. Если предыдущая операционная система должна быть сохранена, то после установки Windows 2000 Server возможна загрузка по выбору. Более полную информацию о ключах можно найти в справочной системе Windows 2000 Server. Для первой установки нам достаточно рассмотренного материала. Отметим только, что Windows 2000 Server использует файловую систему NTFS 5.0, несовместимую с другими файловыми системами, но обеспечивающую наивысший уровень надежности хранения данных. Может быть использована и FAT32, которую поддерживает Windows 98, но эта файловая система не позволит в полной мере реализовать возможности сервера. Поэтому, когда потребуется выбрать раздел для установки операционной системы, преобразуйте его в NTFS 5.0. На эту операцию уйдет некоторое время, но никаких дополнительных знаний и умений не потребуется.

Установка Windows 2000 Server при установленной Windows 9*x*

В этом случае на винчестере должен быть свободный раздел достаточного размера или второй винчестер. Если винчестер один и свободного раздела

нет, раздел можно создать с помощью распространенной утилиты PartitionMagic. Эта утилита позволяет без потери данных уменьшить основной раздел винчестера и на освободившемся месте создать расширенный раздел и логический диск. Форматировать этот логический диск под NTFS не следует, это будет сделано в процессе установки.

Подключение к файловому серверу

Работа с файловым сервером по сути не отличается от работы с ресурсами других рабочих станций при сетевом подключении к ним. Отличие заключается в основном в том, что сервер работает практически всегда, когда включены рабочие станции. Соответственно, подключение к удаленным дискам может восстанавливаться каждый раз при включении рабочей станции. При этом пользователь может и не обращать внимания на то, что диск или папка находятся не на его машине.

Подключение из среды DOS

Для пользователей домашних сетей, да и для тех, кто работает в сетях малых предприятий, может представлять интерес работа сети в режиме командной строки. Множество приложений, распространенных в нашей стране, до сих пор используют среду DOS. На этот факт обращает свое внимание и корпорация Microsoft, выражая надежду, что в скором времени эти приложения уступят дорогу Windows-приложениям. Новые операционные системы этой корпорации все дальше отходят от DOS, требуя от компьютеров многократного увеличения ресурсов, но в результате не предлагающих ничего, кроме красивого интерфейса программ под Windows. Если применяются проверенные временем, безотказно работающие и полностью удовлетворяющие пользователей программы под DOS, какой смысл переходить на новые, отличающиеся красивой оберткой, но более дорогие во всех отношениях программы? Ради возможности работать в сетях Microsoft? Но эта корпорация позаботилась и о пользователях DOS, выпустив клиент DOS с поддержкой нескольких протоколов, включая и TCP/IP. Для работы клиента необходимо, чтобы на сервере была установлена ОС Windows NT/2000. Сетевая карта должна работать под DOS, т. е. иметь загруженные драйверы для той операционной системы, в которой проходит ее работа. Возможна работа этого клиента и под Windows в сеансе DOS. Но в этом режиме будет работать и обычное Windows-сетевое соединение, которое смогут использовать DOS-программы.

Окно соединения имеет понятный интерфейс (рис. 3.5), и в случае ошибок в действиях пользователей выдаются сообщения с информацией о них (рис. 3.6).

Рис. 3.5. Вид окна сетевого соединения DOS-клиента

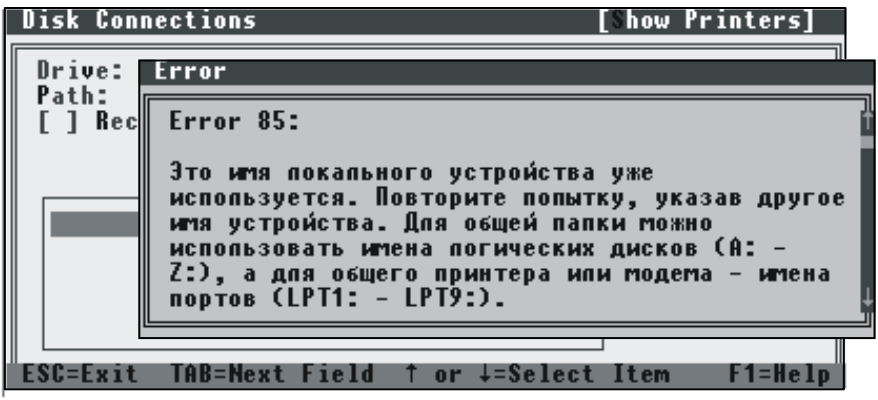


Рис. 3.6. Сообщение об ошибке DOS-клиента

Подробное описание настроек приводится в файле Readme.txt, который находится в папке с установленным клиентом. Сетевой диск, подключаемый с помощью данного клиента, будет обозначен первой не занятой системными ресурсами буквой. Параметры доступа к сетевому диску или папке указаны не будут. Если доступ к какой-либо папке запрещен на удаленной системе, то узнать об этом можно, попытавшись соединиться с этим ресурсом.

Скачать клиента DOS можно бесплатно с сервера **www.microsoft.com**.

PTS-DOS

Справедливости ради следует отметить тот факт, что работа в MS-DOS возможна и с применением операционной системы российского производства PTS-DOS 2000 — мощной и быстрой дисковой операционной системы, полностью совместимой с MS-DOS и всеми ее приложениями (**www.phystechsoft.com**). В отличие от предыдущего клиента работа в этой операционной системе не требует Windows NT/2000 на сервере. В пакет PTS-DOS входят:

- поддержка одноранговой локальной сети LotLAN, имеющая все стандартные сетевые функции;
- файловый менеджер;
- архиватор;
- boot manager — менеджер загрузки операционных систем;
- средства защиты от boot-вирусов;
- графический Web-браузер;
- e-mail-клиент;
- FTP-клиент;
- Telnet — сетевой теледоступ;
- dial-up — вызов с помощью кодонабирателя.

Инсталляция сети LotLAN

Программы LotLAN, входящие в состав PTS-DOS, будут перенесены на жесткий диск с дистрибутивных дискет с помощью программы SETUP. При этом будут установлены все необходимые файлы для сетевой операционной системы LotLAN. Затем эту сеть необходимо инсталлировать. В частности, нужно создать ресурсы сети, определить параметры запуска драйверов NetBIOS, параметры программ сервера и рабочей станции.

Последовательность инсталляции приведена далее.

1. Вначале вы должны запустить программу Command Processor (Командный процессор), входящую в пакет PTS-DOS Extended, и далее для инициализации LotLAN: нажмите комбинацию клавиш <Ctrl>+<S> и выберите

пункт **Поддержка сети LotLan**. На экране появится главное меню менеджера сети LotLAN, содержащее пункты:

- **Управление ресурсами**;
- **Имена пользователей**;
- **Трассировка запросов к серверу**;
- **Установка**;
- **Выход**.

2. Выберите пункт **Инсталляция**. После этого появится меню **Установки сети**:
   - **Полная процедура инсталляции**;
   - **Установки Netbios**;
   - **Установки редиректора**;
   - **Установка ресурсов**;
   - **Создать STARTNET.BAT**;
   - **Главное меню**.
3. Выберите пункт **Полная процедура инсталляции**. После этого нужно выбрать тип драйвера NetBIOS для вашей сети:
   - **NE1000**;
   - **NE2000**;
   - **RS232**;
   - **Другие совместимые Netbios**.

   После выбора типа драйвера NetBIOS необходимо ввести номера портов и прерываний, а для драйвера RS232 — и скорость обмена. Для RS232 параметры NetBIOS такие: скорость обмена 115 200, порт COM 1, линия IRQ 4.

   Все необходимые для двух вышеприведенных меню параметры вы можете узнать с помощью утилиты NET_ADDR.exe, входящей в состав пакета.
4. Определите установки редиректора:
   - **Имя машины** — LOT;
   - **Тип машины** — сервер или рабочая станция.

Для того чтобы открыть доступ к серверу с рабочей станции или с другого сервера, выберите меню **Установка ресурсов**. Программа автоматически создаст ресурсы, соответствующие логическим дискам сервера, например ADRIVE, BDRIVE и т. д., а также ресурс, соответствующий каталогу сервера, в котором содержатся файлы для печати на сетевом принтере (Network Printer Queue — очередь заданий на сетевую печать). Этот ресурс называется SPOOLDIR.

После этого вы можете создать BAT-файл, который будет запускать вашу сеть автоматически. Для этого выберите пункт меню **Создать STARTNET.BAT**. Используя текущую конфигурацию сети, менеджер сети создаст примерно следующий BAT-файл (листинг 3.1).

Листинг 3.1. STARTNET.BAT

```
rem NetBios Loading
rem Here insert YOUR NetBIOS running string
ne2000 port=300h irq=5
rem Redirector Loading
redir.com LOT
IF ERRORLEVEL 1 goto exit
:exit
```

Запуская этот файл, вы загружаете сеть в оперативную память. В данном примере загружается программа рабочей станции. Но соединение с каким-либо сервером автоматически не устанавливается. Для этого нужно запускать программу NET.EXE. Для удобства работы можно дополнить программу STARTNET.BAT командами запуска NET.EXE, например:

```
rem NetBIOS Loading
rem Here insert YOUR NetBIOS running string
ne2000 port=300h irq=5    ;;запуск NetBIOS-драйвера
rem Redirector Loading
redir.com LOT        ;;запуск REDIRECTOR с именем рабочей станции
LOT
IF ERRORLEVEL 1 goto exit
Net login    \\      ;;установить логическое соединение с сервером
                     ;;STEVE
Net use f:   \\steve ;;переназначить логический диск F: на ресурсы
                     ;;сервера STEVE
```

```
Net use lpt1 \\steve ;;переназначить принтерный вывод на
                     ;;сервер STEVE
:exit
```

В конфигурации "СЕРВЕР" STARTNET.BAT будет иметь следующий вид:

```
rem NetBIOS Loading
rem Here insert YOUR NetBIOS running string
ne2000 port=300h irq=5   ;;запуск NetBIOS-драйвера
rem Redirector Loading
server.com LOT       ;;запуск REDIRECTOR с именем рабочей
                     ;;станции LOT
IF ERRORLEVEL 1 goto exit
Net share lpt1       ;;использовать локальный принтер в
                     ;;качестве сетевого
:exit
rem Net
```

Команды PTS-DOS во многом похожи на стандартные команды MS-DOS, а в случае затруднений команда `help` выводит необходимую справочную информацию.

Эта операционная система доступна в демонстрационной версии, которая отличается от зарегистрированной только наличием предупреждений о виде версии и задержкой запуска в одну минуту. Для приобретения лицензии необходимо заплатить около 150 руб.

При установке этой системы в качестве дополнительной необходимо учесть одну особенность. Система может быть установлена в любом разделе на любом логическом диске. Но если она устанавливается в расширенный раздел, то "видит" только логические диски этого раздела. Так, на машине, где установлено два винчестера, причем диск D: разбит на три логических диска: D:, I:, H:, установка PTS-DOS на диск I: привела к тому, что при запуске в режиме PTS-DOS были видны только I: и H:, которые получили буквы C и D. Выбирать систему при запуске можно с помощью программы BootMagic, но и здесь есть тонкость. Сама программа не может увидеть, что на диске I: есть какая-либо система. Надо просто указать как вариант запуск с диска I:. В меню появится новый пункт, и при его выборе запустится PTS-DOS.

Еще одна версия этой системы — PTS-DOS 32 совместима не только с DOS 6.22, но и с DOS 7.0 (поддерживает диски больших размеров), и может быть установлена на тот же диск, где стоит Windows. Кроме того, она отлич-

но работает с клиентом MS-DOS, позволяя организовать одноранговую сеть. Все программы для PTS-DOS 2000 работают с PTS-DOS 32.

В качестве менеджера загрузки разработчики рекомендуют Acronis OS Selector (можно получить на сайте **www.Acronis.com**).

Маршрутизация

В некоторых случаях требуется соединить две или более небольших сети, организованные как самостоятельные локальные сети. В этом случае хотя бы один компьютер (или более) должен иметь две сетевые платы или другие устройства связи, каждое из которых должно быть включено в свою подсеть. Через этот (эти) компьютер(ы) будет осуществляться связь между подсетями, причем сами подсети могут работать совершенно самостоятельно.

Если на компьютере-маршрутизаторе установлена Windows NT/2000, то можно воспользоваться рекомендациями Microsoft по его настройке.

Далее приведена выдержка из справочного руководства по Windows 2000.

Конфигурирование маршрутизируемых сетей

Здесь наиболее интересны типовые ситуации и сценарии использования RRAS (Routing and removed access service — служба маршрутизации и удаленного доступа) для маршрутизации в различных условиях. Мы рассмотрим подробно следующие вопросы:

- маршрутизируемая сеть в небольшом офисе;
- маршрутизируемая домашняя сеть.

Маршрутизируемая сеть в небольшом офисе

Сеть небольшого офиса обладает следующими характеристиками:

- несколько сегментов ЛВС (например, отдельные сегменты на каждом этаже или в каждом крыле здания);
- только один сетевой протокол (IP или IPX) в каждом сегменте;
- закрытость, т. е. отсутствие соединения с другими сетями.

Рассмотрим типовую конфигурацию сети малого офиса, содержащую три подсети. В каждом маршрутизаторе имеется по две сетевые платы, каждая плата подключена к своему сегменту сети. Так как сеть небольшая, то выбираем сеть класса "С", что позволит использовать до 254 компьютеров в каждом сегменте. Для примера можно назначить адреса, приведенные в табл. 3.2.

Таблица 3.2. *Адреса сегментов*

Сегмент	Сеть	IP	Маска
Сеть А Сеть Б Сеть В	200.1 200.1 200.1	.1.0 .2.0 .3.0	255.255.255.0

Как показано в таблице адресов, сетевым картам маршрутизатора 1 можно присвоить адреса 200.1.1.1 (подключенной к сети А) и 200.1.2.1 (подключенной к сети Б). Соответственно, сетевые карты маршрутизатора 2 будут иметь адреса: 200.1.2.2 (подключенная к сети Б) и 200.1.3.1 (подключенная к сети В). Всем остальным компьютерам в каждой из подсетей также назначаются адреса либо вручную, либо с помощью DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации хоста). В том случае, если для автоматического назначения адресов используется DHCP-сервер, оба маршрутизатора должны иметь сконфигурированного агента передачи DHCP/BOOTP. Это позволит клиентам сетей А и В получать адреса, назначаемые расположенным в сети Б DHCP-сервером, т. е. компьютер каждой из подсетей сможет соединяться с компьютерами двух других подсетей.

Для настройки RRAS с помощью утилиты Routing and RAS Admin добавляют статические маршруты для каждого из маршрутизаторов. Так, для маршрутизатора 1 для сетевого интерфейса, подключенного к сети Б, добавляют маршрут, показанный в табл. 3.3.

Таблица 3.3. *Маршрут для маршрутизатора 1*

Назначение	Маска	Шлюз	Метрика	Интерфейс
200.1.3.0	255.255.255.0	200.1.2.2	1	Название сетевой платы

Для маршрутизатора 2 для сетевого интерфейса, подключенного к сети, добавляют маршрут, показанный в табл. 3.4.

Таблица 3.4. *Маршрут для маршрутизатора 2*

Назначение	Маска	Шлюз	Метрика	Интерфейс
200.1.1.0	255.255.255.0	200.1.2.1	1	Название сетевой платы

Устанавливают агент передачи DHCP (DHCP Relay Agent) на обоих маршрутизаторах и конфигурируют их для его использования. Убедитесь в работоспособности DHCP-сервера, а также сервера WINS (Windows Internet Naming Service — служба имен Интернета для Windows) или DNS (в зависимости от того, что вы используете).

Маршрутизируемая домашняя сеть

Рассмотрим теперь небольшую домашнюю сеть, подключенную к Интернету. Характерные черты такой сети:

- один сегмент;
- протокол IP;
- подключение к поставщику услуг Интернета по коммутируемому или выделенному каналу с дозвоном по необходимости.

На маршрутизаторе необходимо сконфигурировать сетевой адаптер и установить модем или иное устройство для подключения к поставщику услуг Интернета (провайдеру). Провайдер (в данном случае это компьютер, предоставляющий доступ к Интернету), как правило, назначает для домашних сетей подсети класса "C". В рассматриваемом примере диапазон адресов — 14, номер сети — 198.1.1.16, а маска — 255.255.255.240. Протоколы маршрутизации в столь малой сети не нужны, достаточно указать статические маршруты на маршрутизаторе. Домашние компьютеры следует сконфигурировать для использования DNS-провайдера, почтовых серверов, серверов новостей и т. д. Кроме того, надо установить фильтры для внешнего интерфейса, чтобы исключить просмотр содержимого вашего компьютера из Интернета.

Обходимся без Windows 2000

Как уже говорилось ранее, мы будем использовать все возможности привычной операционной системы Windows 95/98. Для большинства пользователей

одним из важнейших вопросов является подключение компьютера к Интернету через локальную сеть. Для этого следует организовать переход из вашей маленькой сети в глобальную сеть Интернет. Используя операционные системы Windows 95/98, это можно осуществить описанным ниже способом. Для Windows 95 на компьютере с модемом придется дополнительно установить сервер удаленного доступа из комплекта Microsoft Plus! и провести обновление до Winsock 2.0, если оно еще не проведено.

Существуют и другие варианты организации удаленного доступа. Преимущество предлагаемого решения — минимальные изменения в одноранговой сети с ОС Windows 95, которая является одной из наиболее распространенных в малом офисе и домашнем секторе в наше время.

Сеть строим на основе протокола TCP/IP. Создаем две подсети. Одна — локальная с IP-адресами из диапазона, принятого для внутренних сетей, другая — соединение "модем — модем". Для компьютеров локальной сети можно указать следующие параметры:

- ❒ адрес IP: любой из диапазона 192.168.0.2—192.168.0.255;
- ❒ маска подсети: 255.255.255.0;
- ❒ шлюз: 192.168.0.1.

Для удаленных пользователей:

- ❒ адрес IP: любой из диапазона 192.168.1.2—192.168.1.255;
- ❒ маска подсети: 255.255.255.0;
- ❒ шлюз по умолчанию: 192.168.1.1.

Для DUN-сервера (Dial-Up Networking — система удаленного доступа):

- ❒ **TCP/IP ->сетевой контроллер**:
  - адрес IP: 192.168.0.1;
  - маска подсети: 255.255.255.0;
- ❒ **TCP/IP->контроллер удаленного доступа**:
  - адрес IP: 192.168.1.1;
  - маска подсети: 255.255.255.0.

Чтобы компьютеры из разных подсетей видели друг друга, как обычные клиенты и серверы сетей Microsoft, у каждого прописывается соответствующий файл LMHOSTS в каталоге Windows. Подробно формат описан в файле LMHOSTS.sam. На практике это будет выглядеть следующим образом.

Удаленный пользователь:

- `192.168.0.2 Имя_компьютера1_в_LAN`;
- `192.168.0.3 Имя_компьютера2_в_LAN`

и т. д.

Пользователь LAN:

- `192.168.1.2 Имя_ удаленного_компьютера1`;
- `192.168.1.3 Имя_ удаленного_компьютера2`

и т. д., если удаленные пользователи разные.

В настройках сервера удаленного доступа (**Удаленный доступ к сети | Соединения | Сервер удаленного доступа**) выбрать тип сервера — PPP, прописать пароль и включить собственно доступ. После этого стоит проверить, что компьютеры в каждой из подсетей видят друг друга, причем компьютеры, связанные через модемы, должны друг друга видеть через команду **Поиск | Компьютер | Имя**. Если в сети установлены (для чего-то еще) другие протоколы, убедиться в наличии связи через TCP/IP можно с помощью команды `PING IP_адрес` (должен приходить ответ).

Теперь о маршрутизации. В системном реестре (команда `REGEDIT`) в разделе HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/VxD/MSTCP прописать (если нет — создать) строковую переменную `EnableRouting = "1"`. Перезагрузив ПК, запускаем программу WINIPCFG.exe. Пункт **IP Routing Enabled** должен быть отмечен флажком. Маршрутизация работает. Теперь если все было сделано правильно, то все компьютеры должны видеть друг друга. Для контроля можно использовать команды `PING IP_адрес` и `TRACERT IP_адрес`. Команда `TRACERT` должна показывать путь между подсетями, где первым адресом должен быть адрес шлюза, вторым — запрашиваемый компьютер. Если вместо IP-адресов выдается `Timeout`, значит, настройки IP проведены ошибочно.

Если с какого-либо из компьютеров устанавливается соединение с Интернетом, то для правильной маршрутизации удаленных компьютеров (а не через Интернет, как "захочет" Windows 95/98), нужно вручную на этом компьютере прописать маршрутизацию через шлюз на сервере удаленного доступа командой `ROUTE` из окна DOS. Подробности формата можно узнать, запустив `ROUTE` без параметров, для одного удаленного пользователя с IP, равным 192.168.1.2, в нашем случае команда выглядит так:

```
ROUTE ADD 192.168.1.2 192.168.0.1
```

Для нескольких пользователей удобнее использовать параметр `MASK`.

Теперь, поставив на компьютер с выходом в Интернет прокси-сервер, а на остальные — по модему, можно поиграть в интернет-провайдера.

При наличии достаточных материальных, аппаратных, программных, интеллектуальных и/или прочих ресурсов существуют более надежные и производительные решения (например, на основе Windows NT, аппаратных маршрутизаторов и т. д. и т. п.), но и возможности Windows 95/98 могут с успехом применяться в небольших сетях на основе TCP/IP.

Способ корпорации Microsoft

Один из простых вариантов предложен самой корпорацией Microsoft. Возможность управлять домашней сетью, имеющей выход в Интернет, заложена в один из вариантов Windows 98 — Windows 98 SE.

Компонент **Общий доступ к подключению Интернета** предоставляет удобный способ организации и настройки домашней сети. Непосредственное подключение к Интернету должен иметь только сервер, он же назначает IP-адреса для остальных компьютеров. Таким образом, остальные компьютеры сети получают возможность доступа к Интернету через сервер, используя преобразование личных IP-адресов.

Когда компьютер сети отправляет запрос в Интернет, его личный IP-адрес передается серверу. Сервер преобразует этот адрес в свой IP-адрес, а затем отправляет запрос в Интернет. Получив результаты запроса, сервер выполняет обратное преобразование IP-адреса и направляет полученные результаты соответствующему компьютеру сети. Единственным компьютером сети, видимым другим пользователям Интернета, является сервер, и применение специальных средств для скрытия компьютеров пользователей сети от постороннего доступа со стороны Интернета не требуется.

Для подключения к Интернету необходимо выбрать подходящий для общего доступа компьютер и подключить его к глобальной сети удобным для вас способом. После проверки работоспособности подключения выполните установку компонента операционной системы **Общий доступ к подключению Интернета**. Настройкой общего доступа к Интернету (рис. 3.7) через компьютер, на котором установлена ОС Windows 98 SE, руководит встроенный мастер установки подключения. Необходимо лишь установить **Общий доступ к подключению Интернета** и запустить мастер. Будет предложено создать дискету с дистрибутивом клиентской части программы настройки общего доступа. На этой дискете будет и описание некоторых настроек компьютеров. Но без ручной настройки все же не обойтись.

Если автоматическое назначение адресов включено, то сервер использует протокол DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации хоста) для динамического назначения личных IP-адресов всем компьютерам домашней сети. Кроме того, возможно отключить службу автоматического назначения адресов и назначить статический IP-адрес каждому компьютеру сети.

Можно также настроить компьютеры сети на использование общего доступа к файлам и принтерам, что позволит им осуществлять доступ к ресурсам друг друга. Сервер закрывает доступ к общим ресурсам из Интернета.

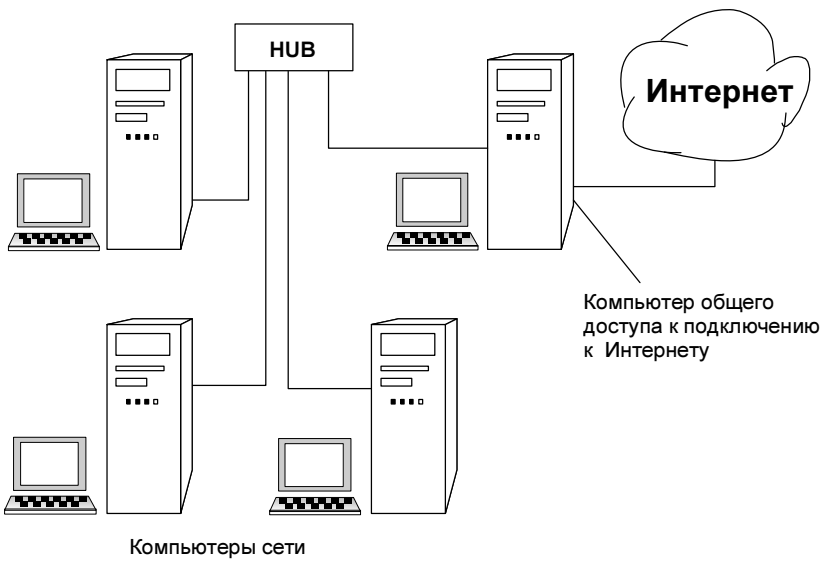


Рис. 3.7. Общий доступ к подключению Интернета

Настройка домашней сети с общим доступом в Интернет

Если у вас еще не установлен общий доступ к подключению Интернета, то:

1. Нажмите кнопку **Пуск**, выберите последовательно команды **Настройка** и **Панель управления**, дважды щелкните по значку **Установка и удаление программ** и выберите вкладку **Установка Windows**.

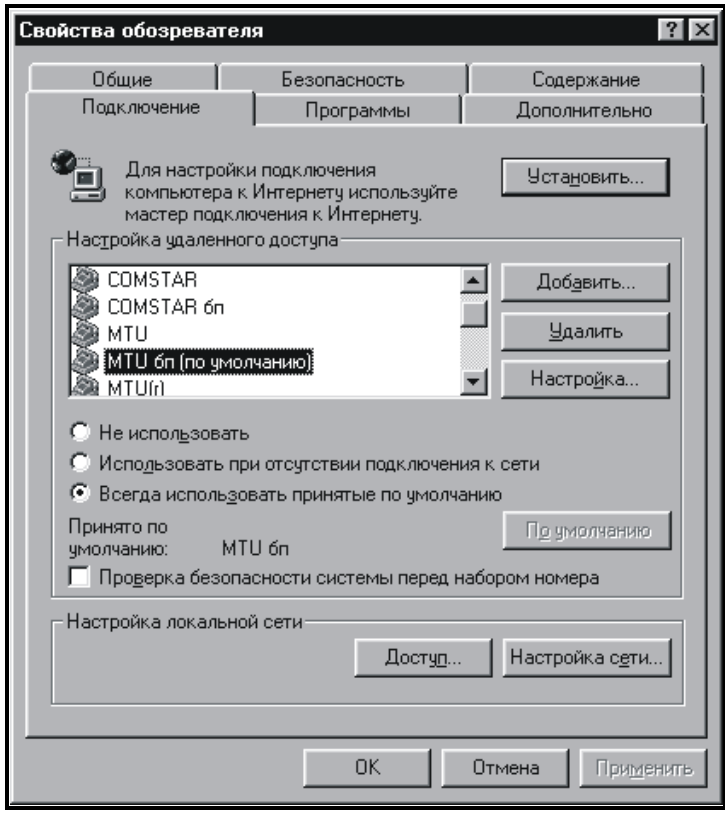


Рис. 3.8. Окно **Свойства обозревателя**

2. Выберите команду **Средства Интернета** и нажмите кнопку **Состав**.

   Активизируйте флажок **Общий доступ к подключению Интернета** и нажмите кнопку **OK**. Если установка Windows выполнялась с компакт-диска, будет выведено приглашение вставить компакт-диск.

3. Следуйте указаниям мастера общего доступа к подключению Интернета.

   Откройте вкладку **Подключение** в диалоговом окне **Свойства обозревателя**.

   Для этого нажмите кнопку **Пуск**, выберите команды **Настройка** и **Панель управления**, дважды щелкните по значку **Свойства обозревателя**, выберите вкладку **Подключение** и нажмите кнопку **Доступ** в группе **Настройка локальной сети** (см. рис. 3.8).

   Если кнопка **Доступ** отсутствует в группе **Настройка локальной сети**, необходимо запустить мастер общего доступа к подключению Интернета.

Мастер общего доступа назначит IP-адрес 192.168.0.1. Остальным компьютерам домашней сети могут быть назначены любые статические IP-адреса из диапазона 192.168.0.2—192.168.0.253.

4. В открывшемся окне **Internet Connection Sharing** (Общее подключение к Интернету) (рис. 3.9) введите параметры, указанные в табл. 3.5.

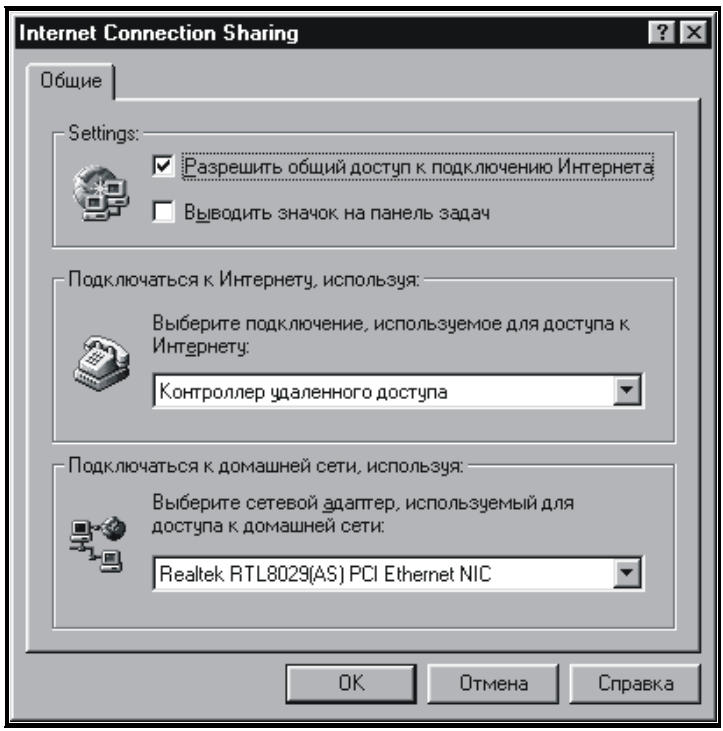


Рис. 3.9. Окно **Internet Connection Sharing**

Таблица 3.5. *Параметры настройки общего доступа к подключению Интернета*

Параметр	Описание
Выводить значок на панель задач	Добавление значка общего доступа к подключению Интернета на панель задач. Значок показывает число подключенных в данное время компьютеров и включает контекстное меню, содержащее параметры общего доступа к подключению Интернета

Таблица 3.5 *(окончание)*

Параметр	Описание
Выберите подключение, используемое для доступа к Интернету	Выберите нужный параметр
Разрешить общий доступ к подключению Интернета	Включение или отключение общего доступа к подключению Интернета
Выберите сетевой адаптер, используемый для доступа к домашней сети	Выберите нужный параметр

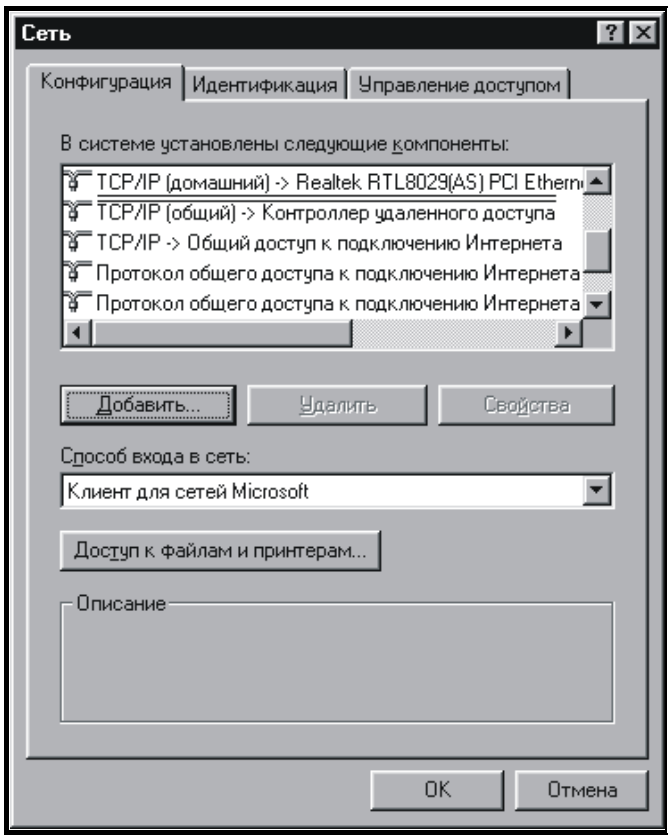


Рис. 3.10. Окно **Сеть**

Следующие шаги выполняются на компьютерах сети:

1. Откройте диалоговое окно **Сеть**.

   Для этого нажмите кнопку **Пуск**, выберите команды **Настройка** и **Панель управления**, а затем дважды щелкните по значку **Сеть**.

2. Выберите в списке **В системе установлены следующие компоненты** адаптер **TCP/IP Ethernet** (рис. 3.10).

3. Нажмите кнопку **Свойства**. Появится окно, изображенное на рис. 3.11:

   - чтобы автоматически назначить IP-адрес, установите переключатель **Получить IP-адрес автоматически**. Если при этом в сети нет сервера DHCP, то компьютер сам автоматически назначит себе IP-адрес. То же произойдет и в случае сбоя в сети с включенной службой DHCP. После восстановления работы службы DHCP личный адрес будет отброшен и восстановлено получение адреса от сервера;

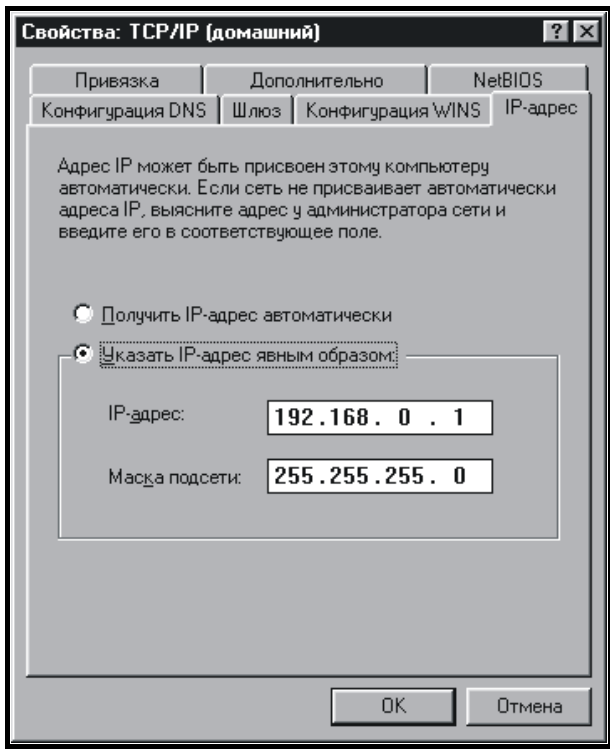


Рис. 3.11. Указание IP-адреса

- чтобы назначить статический IP-адрес, установите переключатель **Указать IP-адрес явным образом**. Назначение статического IP-адреса отменяет динамическое получение адресов с серверов DHCP.

Как правило, личные автоматические IP-адреса используют пространство сетевых IP-адресов LINKLOCAL и формат 169.254.*x.x*. Сети с общим доступом к подключению Интернета используют адреса в диапазоне 192.168.0.*xxx*.

Правильно выбранные адреса компьютеров не вызовут затруднений в работе сети, но Microsoft рекомендует доверять назначение IP-адресов серверу.

В Windows 98 протокол Microsoft TCP/IP обеспечивает механизм IP-адресации, который называют автоматическим назначением личных IP-адресов. Если имеется небольшая сеть, в которой отсутствует служба DHCP, то можно назначить сетевому адаптеру уникальный IP-адрес с использованием пространства сетевых IP-адресов LINKLOCAL. Сетевые адреса LINKLOCAL всегда начинаются с цифр 169.254 и имеют следующий формат:

```
169.254.X.X
```

Сетевые адреса LINKLOCAL применяются только для личной внутренней адресации и недействительны для видимых в Интернете узлов. Они неприменимы для компьютеров, объединенных в сеть с общим доступом к подключению Интернета. После того как сетевой IP-адрес LINKLOCAL назначен сетевому адаптеру, компьютер получает возможность связываться посредством протокола TCP/IP с любым другим компьютером сети, если в ней используется та же адресация.

Компьютер с операционной системой Windows 98, настроенный на автоматическую личную IP-адресацию, может назначать себе личный IP-адрес, если выполняется любое из следующих условий:

- ❒ если компьютер не сконфигурирован как переносной, он может автоматически назначить себе IP-адрес при запуске, в случае если он не имеет допустимой привязки в службе DHCP и в сети не найден сервер DHCP;
- ❒ если компьютер имеет конфигурацию переносного компьютера, он может автоматически назначить себе IP-адрес, если в сети не найден сервер DHCP, вне зависимости от допустимой привязки в службе DHCP.

При автоматической IP-адресации становится возможной автоматическая настройка IP-адресов. Этот способ снижает временные затраты на администрирование и позволяет повторно использовать IP-адреса. Рекомендуется его использовать в сетях любых размеров, не имеющих прямого подключения к Интернету или действующей службы DHCP. Статическая IP-адресация по-

зволяет ввести постоянный IP-адрес вручную. Этот способ Microsoft рекомендует применять только в крайних случаях. Если в дальнейшем будет найдена служба DHCP, компьютер прекратит использование автоматически назначенных IP-адресов и будет использовать IP-адреса, присвоенные службой DHCP. IP-адрес службы DHCP не заменяет статический IP-адрес. Последний должен быть изменен вручную. Если компьютер переводится из локальной сети со службой DHCP в локальную сеть без этой службы, то для освобождения адресов DHCP можно использовать служебную программу настройки IP (WINIPCFG). После этого можно позволить компьютеру назначить себе личный IP-адрес.

Настройка доступа в операционной системе Windows 2000/XP

Этот вариант настройки, как и в предыдущем случае, не следует применять в сети с контроллерами домена, работающими под управлением системы Windows 2000 Server, с серверами DNS, шлюзами, серверами DHCP или системами, настроенными на использование статических IP-адресов.

На узловом компьютере общего доступа к подключению Интернета необходимы два сетевых подключения. Подключение локальной сети, автоматически создаваемое при установке сетевой платы, связывает его с остальными компьютерами домашней сети или сети малого предприятия. Другое подключение связывает домашнюю сеть или сеть малого предприятия с Интернетом; оно осуществляется:

- через модем со скоростью передачи данных 56 Кбит/с;
- по линии ISDN (Integrated Service Digital Network — международный стандарт передачи голоса, видео- и SOCKS-данных по цифровым телефонным линиям);
- по линии DSL (Digital Subscriber Line — цифровая абонентская линия; "свободная" местная линия между центральной АТС и оборудованием клиента, используемая для речевой связи и высокоскоростной передачи данных. Данные модулируются по частоте, находящейся выше слышимого диапазона);
- через кабельный модем.

При установке общего доступа к подключению Интернета изменяется статический адрес и настройка подключения локальной сети к домашней или малой сети. Следовательно, подключения по протоколу TCP/IP между компью-

терами локальной сети и узловым компьютером общего доступа к подключению Интернета при этом теряются и должны быть восстановлены. Например, если Web-обозреватель Internet Explorer соединяется с Web-узлом при установленном общем доступе к подключению Интернета, необходимо обновить настройки обозревателя, чтобы восстановить его подключение к Web-узлу. Клиентские компьютеры домашней сети или сети малого предприятия необходимо настроить так, чтобы протокол TCP/IP в локальных подключениях автоматически получал IP-адрес. Кроме того, для работы с общим доступом к подключению Интернета пользователи домашней сети или сети малого предприятия должны настроить параметры доступа в Интернет. Для того чтобы включить службу обнаружения общего доступа к подключению и управления этим подключением (ICS, Discovery and Control) на компьютере, работающем под операционной системой Windows 98, Windows 98 Second Edition или Windows Millennium Edition, следует запустить с компакт-диска или дискеты мастер установки сети. Для работы службы обнаружения общего доступа к подключению Интернета и управления этим подключением на компьютерах с системой Windows 9*x*/ME должен быть установлен обозреватель Internet Explorer версии 5.0 или более поздней.

Установка подключения

Для того чтобы выполнить описанные далее действия, необходимо войти в систему с учетной записью владельца (администратора) компьютера.

1. Нажмите кнопку **Пуск**, выберите пункт **Панель управления** и дважды щелкните мышью значок **Сетевые подключения**. Откроется папка **Сетевые подключения**.
2. Выберите подключение, для которого необходимо установить общий доступ, и в области **Типичные сетевые задачи** нажмите кнопку **Изменить настройку подключения**.
3. На вкладке **Дополнительно** (рис. 3.12) установите флажок **Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера**.
4. Если для выбранного подключения требуется обеспечить автоматический набор номера при обращении компьютеров домашней сети или сети малого предприятия к внешним ресурсам, установите флажок **Устанавливать вызов по требованию**.

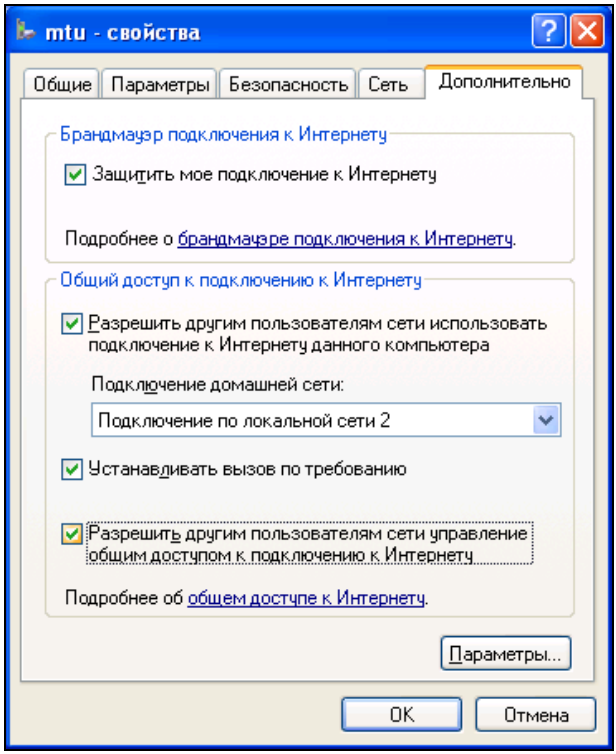


Рис. 3.12. Вкладка **Дополнительно** окна свойств подключения

5. Если требуется, чтобы остальные пользователи сети могли включать и выключать общий доступ к подключению Интернета, установите флажок **Разрешить другим пользователям сети управление общим доступом к подключению к Интернету**.
6. В области **Общий доступ к подключению к Интернету** в группе **Подключение домашней сети** выберите любую сетевую плату, через которую компьютер, подключенный к Интернету, будет соединен с остальными компьютерами сети. Группа **Подключение домашней сети** появляется только тогда, когда на компьютере установлены по меньшей мере две сетевые платы.

Настройка остальных компьютеров сети

1. Запустите обозреватель Internet Explorer. Для этого нажмите кнопку **Пуск** и последовательно выберите пункты **Программы | Internet Explorer**.

2. В меню **Сервис** выберите пункт **Свойства обозревателя**.
3. На вкладке **Подключение** установите переключатель **Не использовать** и нажмите кнопку **Настройка сети**.
4. В группе **Автоматическая настройка** снимите флажки: **Автоматическое определение настроек** и **Использовать сценарий автоматической настройки**.
5. В группе **Прокси-сервер** сбросьте флажок **Использовать прокси-сервер**.

С этого момента каждый пользователь простой сети сможет подключаться к ресурсам Интернета, не мешая другим пользователям. Настройки для Windows 2000 отличаются незначительно. Если одна и та же телефонная линия используется для телефонных разговоров и для подключения к Интернету, то соединение лучше устанавливать вручную, не разрешая пользователям устанавливать его автоматически (по требованию). Можно определить разрешенные для подключения интервалы времени.

Средства подключения для сети с сервером Windows 2000 Server

Рассмотренные варианты общего доступа в Интернет обладают определенными недостатками. Самый неприятный из них — это необходимость назначения определенного IP-адреса узловому компьютеру общего доступа и назначение этим компьютером динамически выделяемых адресов другим компьютерам сети. Это приводит к тому, что вы не можете использовать описанные методы в сети с сервером Windows 2000 Server. Но и в этом случае есть выход. Существует довольно большое число платных и бесплатных, сложных и простых программ, которые могут помочь решить поставленную задачу. Для небольшой сети с выделенным сервером под управлением Windows 2000 Server можно применить хорошо зарекомендовавшую себя программу AnalogX Proxy.

AnalogX Proxy v4.14

Бесплатно распространяемый прокси-сервер AnalogX Proxy 4.10 (адрес программы: **www.analogx.com**) очень компактен, но имеет весьма широкие возможности. Он поддерживает практически все, необходимые для работы в сети Интернет, протоколы. Поддержка протоколов серии SOCKS позволяет использовать в локальной сети FTP-клиенты, например распространенный клиент

CuteFTP. (SOCKS от socket (розетка, разъем) — это один из протоколов передачи информации, который автоматически перенаправляет (подключает) сетевые запросы на соответствующий SOCKS-сервер. Протокол имеет несколько модификаций.) Почтовые клиенты на машинах пользователей (например, Microsoft Outlook Express) при работе через AnalogX Proxy нужно специально настраивать — т. е. указывать в качестве POP3- и SMTP-серверов IP-адрес машины, на которой установлен AnalogX Proxy. На самом же прокси-сервере в специальном меню (кнопка **Configure Email Alias's** — Настройка почтовых псевдонимов) нужно указать реальные адреса POP3- и SMTP-серверов. AnalogX Proxy способен работать с внешним прокси-сервером более высокого уровня, запрашивая файлы из его кэш-буфера. Адрес внешнего прокси вводится в поле **Proxy Binding** (Связь с прокси). При настройке AnalogX Proxy применяет различные порты для разных служб (например, для HTTP и HTTPS используется порт 6588). В сети, применяющей AnalogX Proxy, нет необходимости изменять уже назначенные адреса компьютеров.

Рассмотрим настройку AnalogX Proxy для использования общего доступа к подключению Интернета. Для совместного использования электронной почты Интернета в *главе 4* будет описана более удобная бесплатная программа.

Скопировав дистрибутив программы AnalogX Proxy (269 Кбайт), запустите программу ее установки — proxyi.exe. Процесс установки не имеет каких-либо особенностей. Ее можно проводить на компьютере с любой операционной системой семейства Windows, начиная с Windows 98. После установки в меню **Программы** появится группа **Analogx**, в которой будет ярлык **Proxy**.

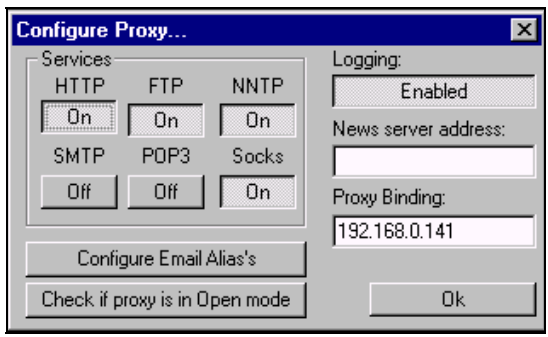


Рис. 3.13. Окно **Configure Proxy**

Программа не устанавливается как сервис, ее необходимо запускать вручную. После запуска программы ее значок появится в системном лотке около

часов. Щелкните по значку правой кнопкой мыши и выберите в раскрывшемся меню пункт **Configure** (Настройка). При этом откроется окно **Configure Proxy** (Настройка прокси) (рис. 3.13).

Установите в положение **On** (Включено) кнопки **HTTP**, **FTP**, **NNTP**, **Socks**. Кнопки **SMTP** и **POP3** оставьте в положении **Off** (Выключено). Кнопку **Logging** (Авторизация) установите в положение **Enabled** (Включено), в поле **Proxy Binding** (Связь с прокси) введите IP-адрес компьютера. Эта мера позволит защитить соединение от подключения извне.

В процессе настройки программы обратите внимание на цвет ее значка в системном лотке — он красный. После нажатия кнопки **Ok** его цвет изменится на зеленый, а окно настроек закроется.

На этом настройка программы завершена!

Теперь необходимо настроить клиентские рабочие станции.

1. Запустите обозреватель Internet Explorer.
2. В меню **Сервис** выберите пункт **Свойства обозревателя**.
3. На вкладке **Подключение** установите переключатель **Не использовать** и нажмите кнопку **Настройка сети** или **Настройка LAN** на компьютерах с Windows 9*x*.
4. В группе **Автоматическая настройка** снимите флажки **Автоматическое определение настроек** и **Использовать сценарий автоматической настройки**.
5. В группе **Прокси-сервер** установите флажок **Использовать прокси-сервер**.
6. Введите адрес компьютера с установленной программой Analogx Proxy и порт 6588.
7. Другие настройки обычно не требуются.

Теперь достаточно установить подключение к Интернету на компьютере с AnalogX Proxy и с любой настроенной рабочей станции можно свободно подключаться к Всемирной паутине.

Настройка доступа в Интернет через сервер с Windows 2000 Server

Корпорация Microsoft включила в состав серверной операционной системы возможность общего подключения к Интернету.

Предупреждение

Настройки главного сервера сети не следует изменять без крайней необходимости. Для подключения к Интернету лучше использовать второй сервер, выполняющий второстепенные функции. Если вы абсолютно уверены, что все делаете верно, или сервер еще не включен в сеть в качестве основного, то можете поэкспериментировать.

Настройка общего доступа к подключению Интернета

1. Прежде всего, на сервере должен быть установлен модем или другой адаптер для подключения к глобальной сети Интернет.

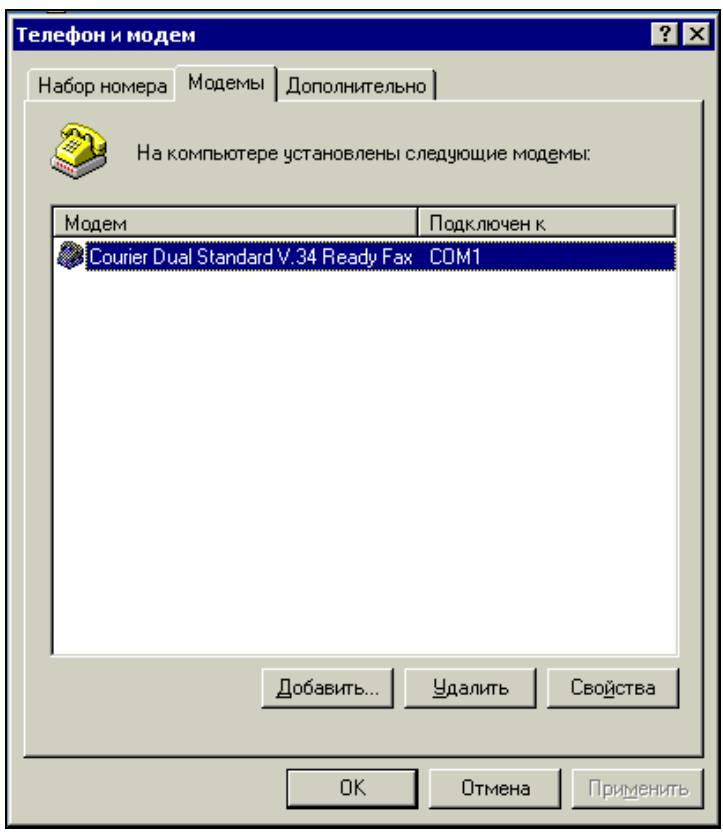


Рис. 3.14. Окно **Телефон и модем**

Установка модема осуществляется через окно **Телефон и модем** (рис. 3.14), которое можно открыть двойным щелчком мыши по одноименному значку в окне **Панель управления**. После нажатия кнопки **Добавить** будет запущен мастер, который поможет установить новый модем.

2. Нужно включить службу **Маршрутизация и удаленный доступ**. Она находится в окне **Службы компонентов** (рис. 3.15), которое можно открыть из меню **Пуск | Программы | Администрирование | Службы компонентов**. Для того чтобы запустить службу, щелкните по ее значку правой кнопкой мыши и выберите из открывшегося меню пункт **Пуск**.

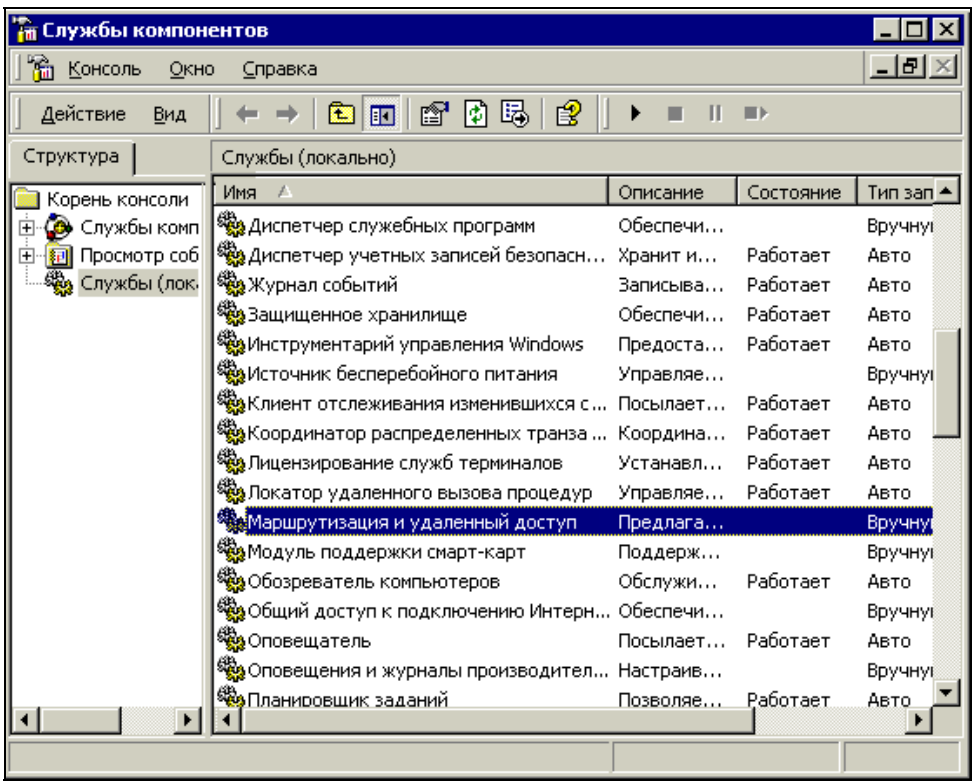


Рис. 3.15. Окно **Службы компонентов**

3. Из меню **Пуск | Программы | Администрирование | Маршрутизация и удаленный доступ** откройте окно **Маршрутизация и удаленный доступ** (рис. 3.16).

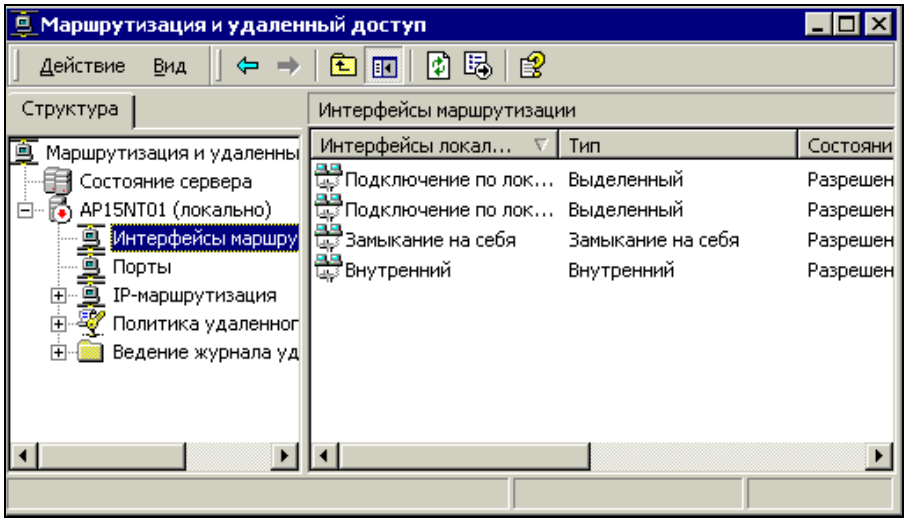


Рис. 3.16. Окно **Маршрутизация и удаленный доступ**

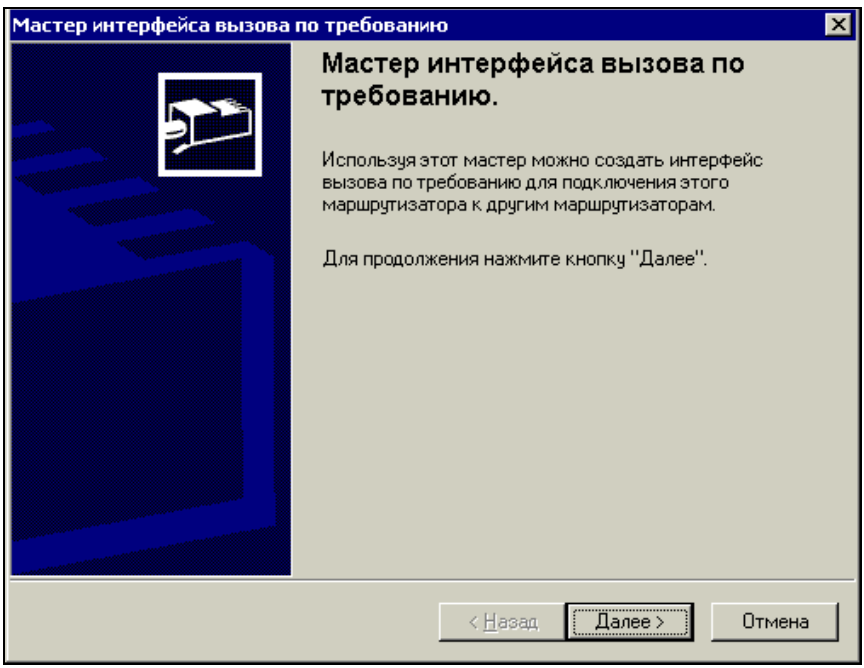


Рис. 3.17. Окно **Мастер интерфейса вызова по требованию**

4. Найдите в открытом окне значок **Интерфейсы маршрутизации** и выделите его. Щелкнув по нему правой кнопкой мыши, выберите **Создать новый интерфейс вызова по требованию**. При этом запустится мастер интерфейса вызова по требованию (рис. 3.17).
5. После нажатия кнопки **Далее** потребуется ввести имя нового интерфейса (рис. 3.18).
6. На следующем этапе выбираем переключатель **Подключаться, используя модем, адаптер ISDN или другое устройство**.
7. После нажатия кнопки **Далее** необходимо выбрать **Протоколы и безопасность** (рис. 3.19). Устанавливаем флажок **Перенаправлять пакеты IP на этот интерфейс**.
8. В следующем окне мастера необходимо ввести учетные данные исходящего подключения (рис. 3.20). Это обычные данные для подключения к Интернету, которые вы получили у провайдера.

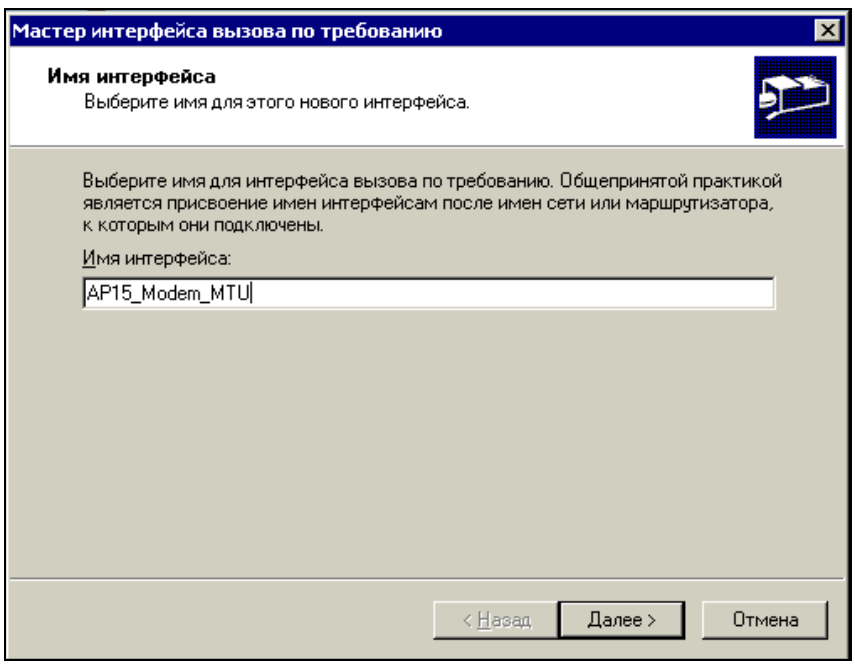


Рис. 3.18. Окно **Мастер интерфейса вызова по требованию** для назначения имени интерфейсу

9. На следующем этапе работа мастера завершается, а в окне **Маршрутизация и удаленный доступ** (рис. 3.21) появляется новый интерфейс.
10. Переходим к значку **Порты** в окне **Маршрутизация и удаленный доступ**. Щелкните по нему правой кнопкой мыши и выберите из открывшегося меню пункт **Свойства**. На экран выводится окно **Свойства: Порты** (рис. 3.22).
11. В открывшемся окне выберите устройство, которое требуется настроить. В данном случае это модем.
12. Выделите модем и нажмите кнопку **Настроить**. В открывшемся окне введите номер телефона и установите флажок **Подключения по требованию (входящие и исходящие)** (рис. 3.23).
13. Разверните раздел **IP-маршрутизация** в окне **Маршрутизация и удаленный доступ** (см. рис. 3.21) и щелкните правой кнопкой мыши по значку **NAT-преобразование сетевых адресов**.

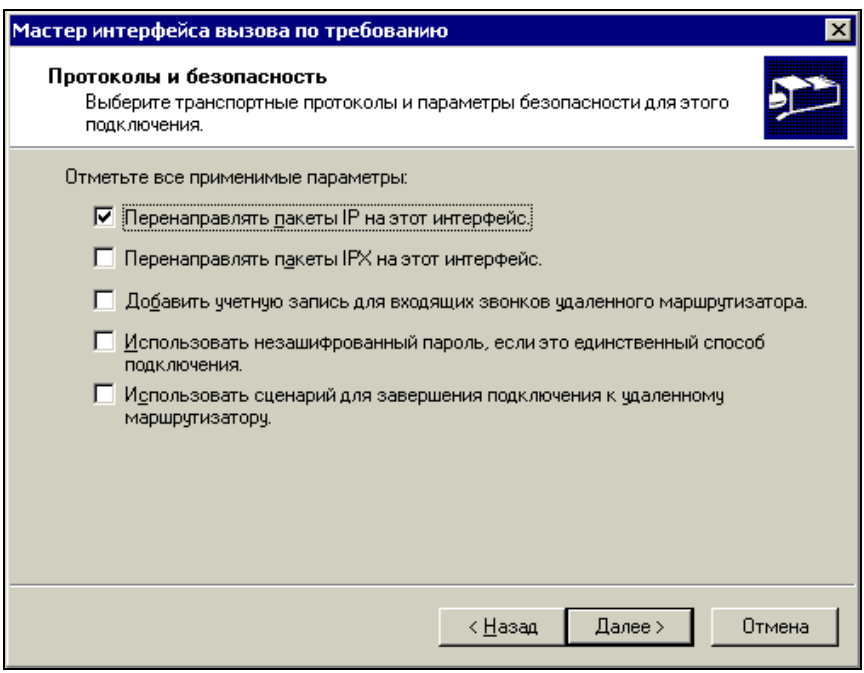


Рис. 3.19. Окно **Мастер интерфейса вызова по требованию** для выбора протоколов и безопасности

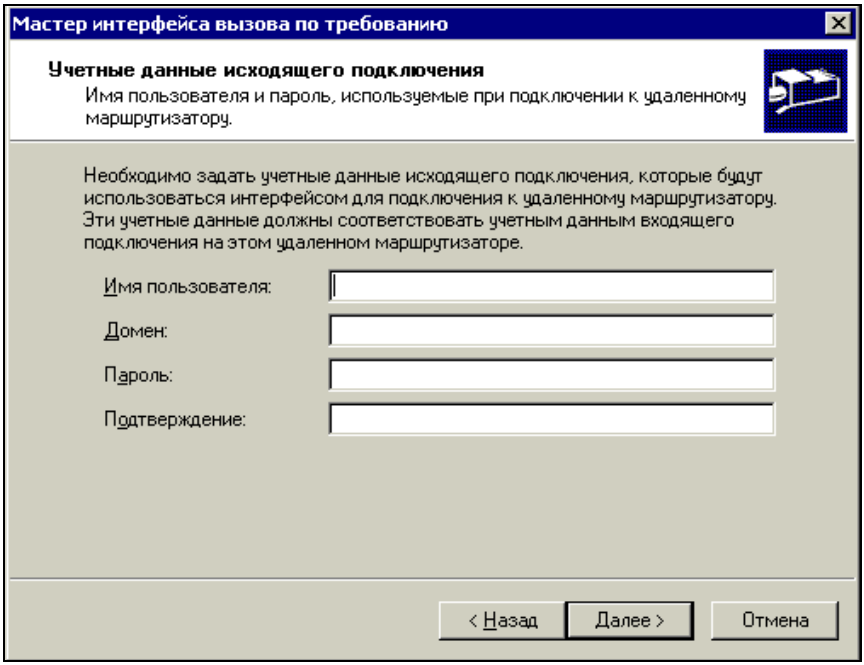


Рис. 3.20. Окно **Мастер интерфейса вызова по требованию** для ввода данных исходящего подключения

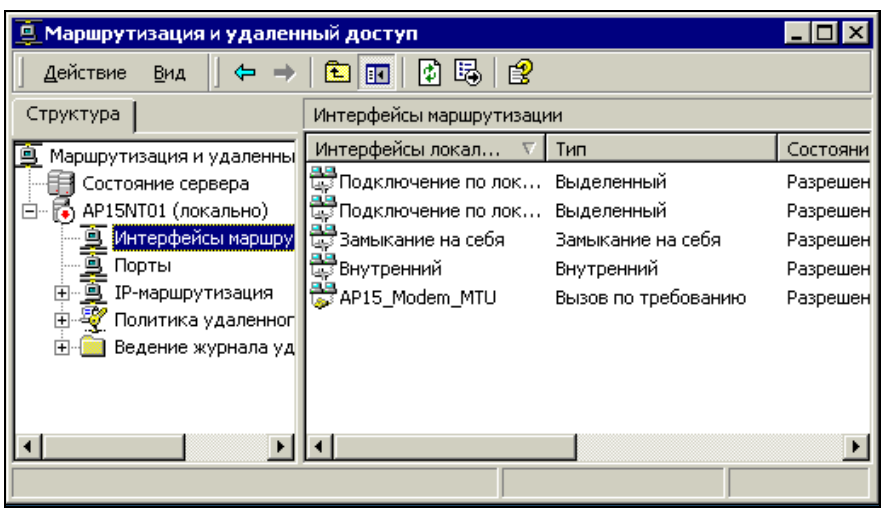


Рис. 3.21. Окно **Маршрутизация и удаленный доступ** с новым интерфейсом вызова по требованию

14. Выберите пункт меню **Новый интерфейс**. Откроется окно со списком доступных интерфейсов (рис. 3.24). Скорее всего, в списке будет только наш модем.

15. Нажмите кнопку **OK**. Откроется окно **Свойства: Свойства NAT — AP15_Modem_MTU** (имя интерфейса подключения) (рис. 3.25).

16. Перейдите на вкладку **Пул адресов** открытого окна. Нажмите кнопку **Добавить** и введите начальное и конечное значения пула адресов, которые можно узнать у провайдера (рис. 3.26).

17. Создайте новый статический маршрут (рис. 3.27), вызвав окно нового маршрута щелчком правой кнопки мыши по значку **Статические маршруты** и выбрав пункт меню **Новый маршрут**.

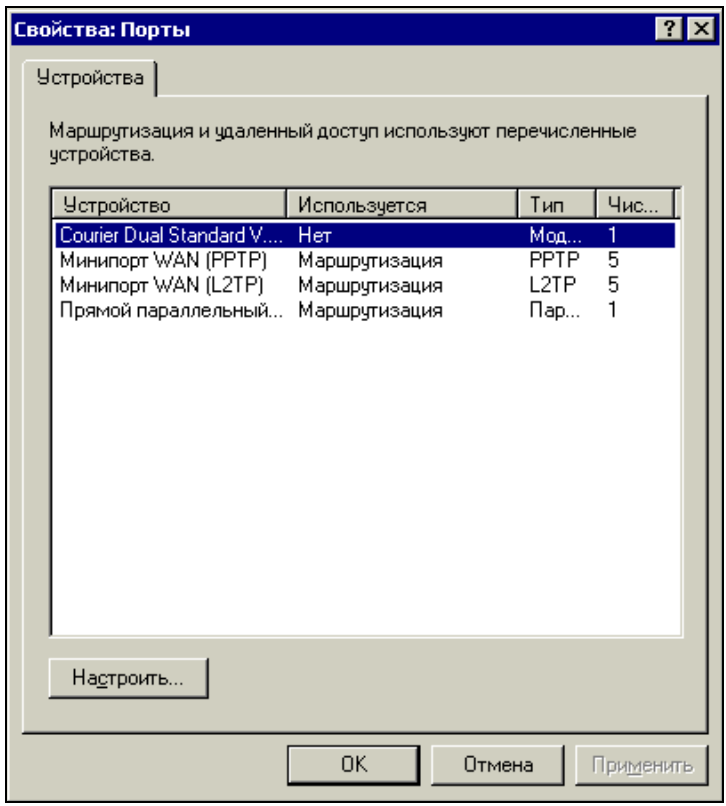


Рис. 3.22. Окно **Свойства: Порты**

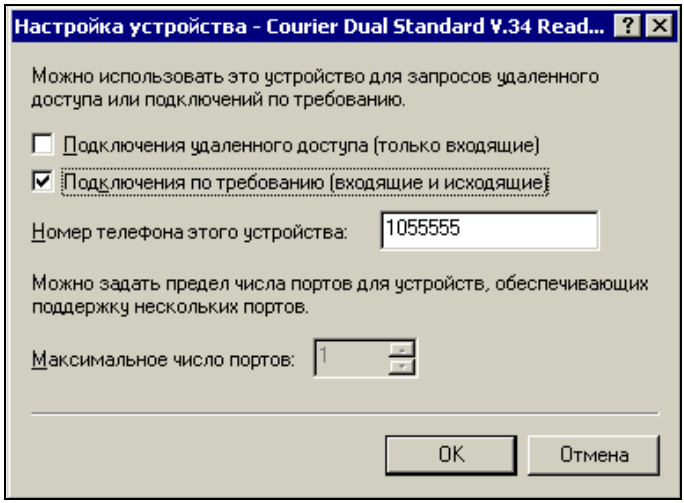


Рис. 3.23. Окно **Настройка устройства** (модем)

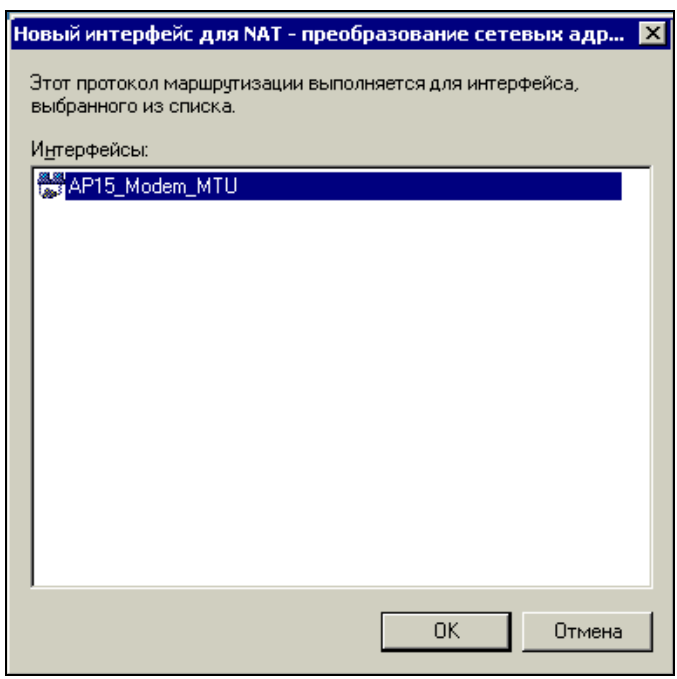


Рис. 3.24. Окно **Новый интерфейс для NAT — преобразование сетевых адресов**

18. В окне **Свойства: NAT — преобразование сетевых адресов** на вкладке **Разрешение имен в адреса** установите все флажки и выберите из списка имя интерфейса вызова по требованию (рис. 3.28).

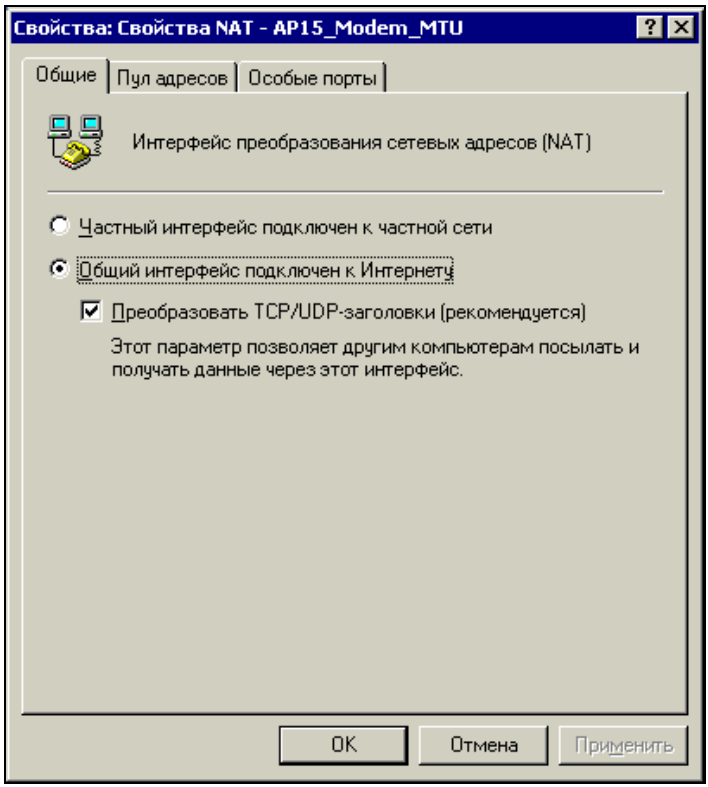


Рис. 3.25. Окно
Свойства: Свойства NAT <имя модема>

19. Нажмите кнопки **ОК** на каждом из открытых окон. Можно включить модем и попытаться установить соединение с каким-либо внешним адресом.

Более тонкая настройка преобразования сетевых адресов потребует немалого времени, но если вы решили использовать этот вариант общего доступа к подключению Интернета, то придется пройти весь путь от начала до конца. На каждом этапе настройки доступна справочная система, которую можно вызвать из любого окна настроек.

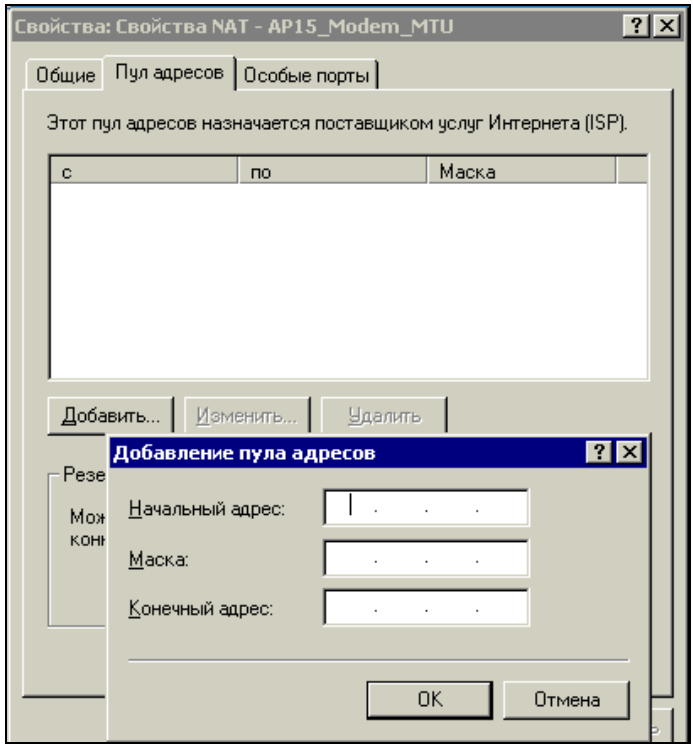


Рис. 3.26. Окно **Добавление пула адресов**

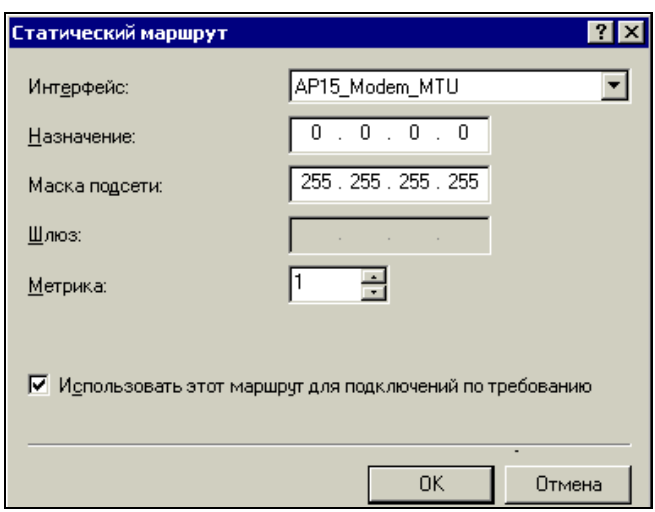


Рис. 3.27. Окно **Статический маршрут**

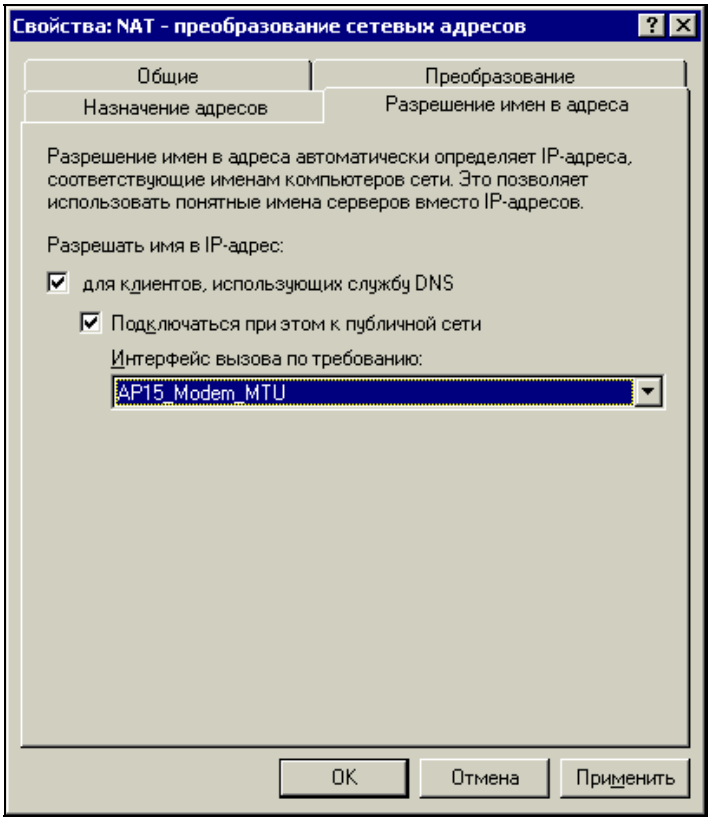


Рис. 3.28. Окно **Свойства: NAT — преобразование сетевых адресов**, вкладка **Разрешение имен в адреса**

Общий доступ в Интернет через Windows Server 2003 и ADSL-модем

Некоторые отличия Windows Server 2003 от Windows 2000 Server

Windows Server 2003 Standard Edition — это наиболее подходящая для малых сетей версия Windows Server 2003. Если вам приходилось иметь дело с Windows 2000 Server, то в большинстве случаев общения с сервером вы будете встречаться с уже знакомыми операциями и функциями. Тем не менее будут заметны и отличия.

Прежде всего, сервер на базе Windows Server 2003 более стабилен и более защищен по сравнению с Windows 2000 Server. Многие положительные качества Windows XP перенесены в новую серверную систему, что увеличило ее устойчивость и защищенность. Пользователям малых сетей не придется приобретать дополнительное программное обеспечение для организации надежной защиты сети со стороны Интернета и удобного почтового сервера. В Windows 2000 Server эти возможности отсутствовали. Возможное объединение вашей сети с другими, более крупными сетями может потребовать изменения некоторых параметров уже работающей сети или настройки взаимодействия объединяемых сетей, чтобы обеспечить совместную работу пользователей. Такие преобразования в Windows Server 2003 требуют меньше усилий и времени, чем в Windows 2000 Server. В отдельных случаях можно увидеть более удобные средства управления учетными записями пользователей в сети. Другие преимущества новой ОС могут быть заметны разработчикам новых интернет-приложений с использованием языка XML.

Тем не менее вполне возможно сосуществование в одной сети обеих операционных систем. Так, если у вас уже работает сервер с настроенным контроллером домена под управлением Windows 2000 Server, то вы вполне можете применить Windows Server 2003 в качестве второго сервера, обеспечивающего разнообразные Web- и почтовые сервисы, может быть, и сервер печати, и сервер архивов, а также другие необходимые в вашей сети функции. Возможности ОС позволяют отказаться от приобретения дополнительного оборудования для настройки маршрутизации и NAT, обеспечивая доступ вашей сети к другим сетям и Интернету, а также работу сетевых приложений.

Установка

Мы будем исходить из предположения, что ваша сеть еще не имеет сервера и работает одноранговая сеть. Вам решать — использовать описанные далее настройки сервера или применять другие средства, обеспечивающие описанные возможности программными или аппаратными средствами, если они у вас уже работают. Но при отсутствии других средств вы можете настроить работу сети, основываясь только на возможностях операционной системы.

Начиная модернизацию одноранговой сети до сети с выделенным сервером, можно выбрать различные планы перехода. Можно начать с установки Active Directory, чтобы обеспечить простоту управления учетными записями, но можно сначала настроить и дополнительные функции сервера, обеспечи-

вающие связь с внешним миром. Мы начнем именно с этих дополнительных функций. Это позволит тем, у кого уже работает Active Directory, приступить к установке второго сервера. Мы будем считать этот сервер своим первым сервером. Само собой разумеется, что начать придется с установки ОС. Но описывать процесс первоначальной установки мы здесь не будем. Он мало отличается от подобных процедур для других операционных систем. Главные отличия появляются уже после установки ОС, когда сервер предлагает настроить свои роли в сети.

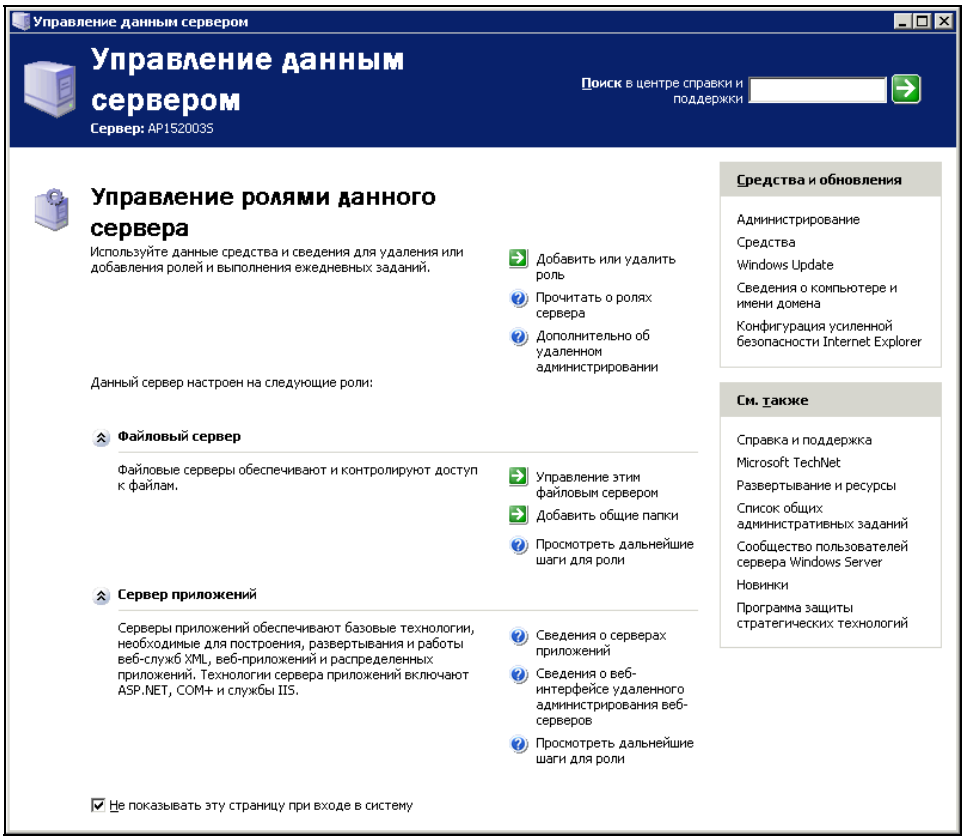


Рис. 3.29. Окно **Управление данным сервером**

После установки ОС окно **Управление данным сервером** (рис. 3.29) появляется автоматически. Если вы отказались от показа этой страницы при входе в систему, то позднее ее можно открыть, выбрав пункт меню **Администри-**

рование | Управление данным сервером. В этом окне нас на начальном этапе будет интересовать пункт меню **Добавить или удалить роль**. Перед выбором роли сервера вы можете в том же окне воспользоваться ссылками на справочные материалы. Это позволит более подробно познакомиться с возможностями вашего сервера.

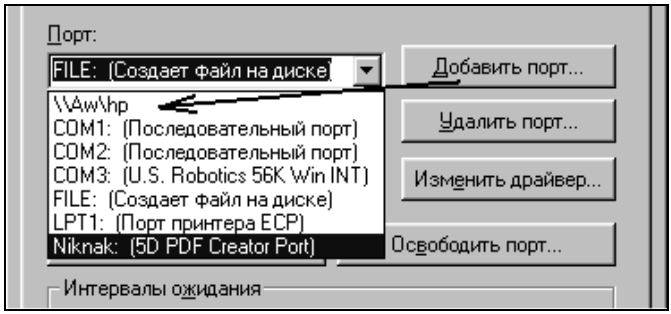


Рис. 3.30. Окно **Мастер настройки сервера**

При выборе пункта меню **Добавить или удалить роль** мастер настройки сервера (рис. 3.30) сразу предложит проверить все условия, которые должны быть выполнены перед продолжением настройки.

Подключение сети к Интернету

В данном примере мы будем рассматривать не совсем обычный вариант подключения, который продемонстрирует достаточно широкие возможности сервера в сети и возможности конфигурирования локальной сети. Сеть, в которой работает этот сервер, уже имеет выход в Интернет через аппаратные средства. А доступ через сервер предоставляется еще одной сети, подключаемой к серверу через отдельный интерфейс (второй сетевой адаптер). При подключении к Интернету единственной сети через ADSL-модем, подключенный к серверу, изменятся только IP-адреса. Процедура настройки подключения останется совершенно такой же.

В данном примере (рис. 3.31) компьютер-сервер имел до проведения настроек роль обычной рабочей станции в сети 192.168.1.0. Роль этого компьютера повышается до сервера, но для второй сети, которая только что устанавливается. Во второй сети для доступа в Интернет будет использоваться уже работающий сервер.

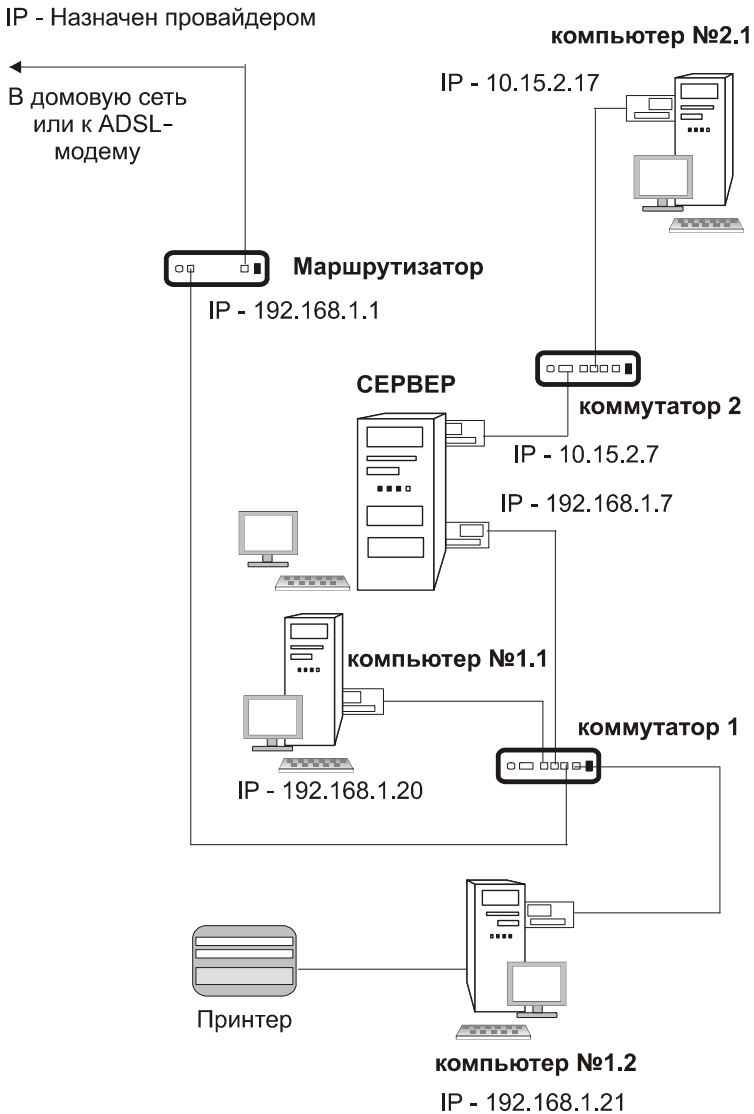


Рис. 3.31. Подключение сети 10.15.2.0 к Интернету через сервер

Маршрутизатор, применяемый для доступа в Интернет одноранговой сети 192.168.1.0, имеет внешний IP-адрес, назначенный провайдером. Для сети 10.15.2.0 провайдером будет сеть 192.168.1.0. Адрес, назначенный для выхода в Интернет второй сети, — 192.168.1.7. Это адрес сетевого адаптера сервера, обращенный в первую сеть. Сервер для второй сети в данном случае

играет роль маршрутизатора. Причем рассматриваемый пример предполагает настройку NAT, что приведет к тому, что все компьютеры второй сети (10.15.2.0) будут подключаться к Интернету и даже в первую сеть с одним общим IP-адресом. На этом, собственно говоря, и основана работа NAT.

> ***Примечание***
>
> Если вы не имели опыта работы с сетями подобного рода, рекомендуем внимательно разобраться в описываемом примере. Это позволит в дальнейшем понять работу своей реальной сети и принять верные решения при ее настройке и модернизации.

На рис. 3.31 показана только одна рабочая станция из сети 10.15.2.0, но реально их число может быть любым допустимым в сети (ограничивается маской подсети).

Мастер предлагает уже сейчас, перед продолжением настроек, подключить сервер к Интернету. Этот момент нашей работы следует предварить важным замечанием.

> ***Замечание***
>
> Подключение к Интернету без соблюдения мер предосторожности может привести к неприятным последствиям. Активность различных вирусов, существующих в сетях, меняется и иногда достигает угрожающих значений. Первое подключение сервера к Интернету следует делать при отключенной локальной сети. Обязательно следует включить брандмауэр.

Конечно, если вы повторяете описываемый пример полностью, то угрозы неожиданного заражения уже практически не существует, ведь реальное подключение к Интернету уже настроено. Но подключение единственной сети с единственным сервером требует осторожности.

Продолжим настройки.

Сетевой адаптер, смотрящий во внешнюю сеть, должен быть настроен до продолжения работы мастера.

На рис. 3.32 показаны настройки внешнего сетевого адаптера сервера. Еще раз отметим, что при использовании подключения через ADSL-модем необходимо указать значения IP-адреса, маски подсети, основного шлюза и DNS-серверов, предоставленные провайдером. Но в нашем случае эти параметры выбраны в соответствии с параметрами внешней (для настраиваемой) сети.

Кроме настройки подключения сервера к Интернету мастер настройки сервера требует подключения всех кабелей и установки всех сетевых адаптеров. Проверим настройку второго сетевого адаптера, который будет соединять сервер со второй сетью (рис. 3.33).

Для этого адаптера нет необходимости указывать основной шлюз. Если в вашей сети уже настроен DNS-сервер, то можно указать его адрес в качестве альтернативного. Основной DNS-сервер в нашем случае имеет адрес, предоставленный провайдером.

Примечание

Для доступа в Интернет можно использовать адреса любых DNS-серверов. Но серверы, не имеющие отношения к провайдеру, могут быть не доступны в процессе установления соединения.

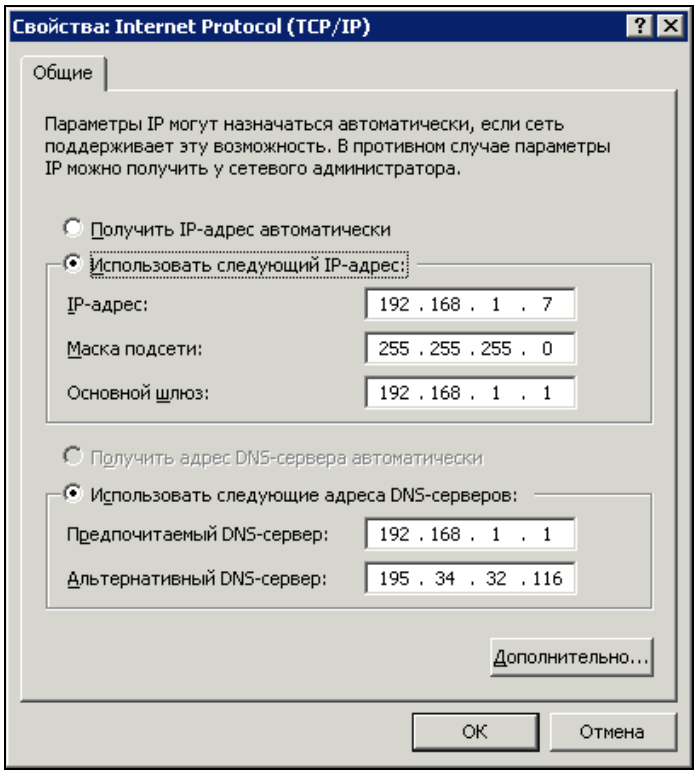


Рис. 3.32. Окно **Свойства: Internet Protocol (TCP/IP)** для внешнего сетевого адаптера сервера

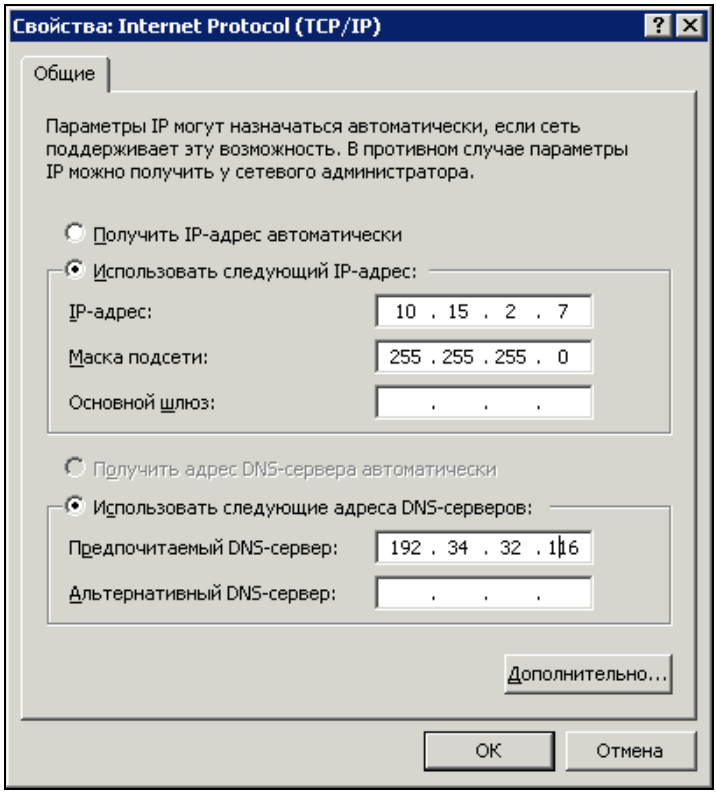


Рис. 3.33. Окно **Свойства: Internet Protocol (TCP/IP)** для внутреннего сетевого адаптера сервера

Возможно, что вы обратили внимание на то, что маска подсети, используемая в этом примере, не соответствует обычному значению для сетей класса "A", которые обычно имеют адреса вида 10.*X.X.X*. У каждого правила есть исключения. Ведь нам не требуется такого количества компьютеров в сети, которое позволяет иметь сеть класса "A". Маска подсети, примененная нами, дает возможность включать в нашу сеть всего 254 компьютера, но нам этого более чем достаточно.

Остается проверить работу сети 10.15.2.0, подключив к внутреннему сетевому адаптеру сервера через коммутатор хотя бы одну рабочую станцию.

Если вы можете подключиться к общедоступным ресурсам сервера или можете "пинговать" сервер с рабочей станции и `ping` дает положительные результаты, то можно приступать к дальнейшей настройке сервера.

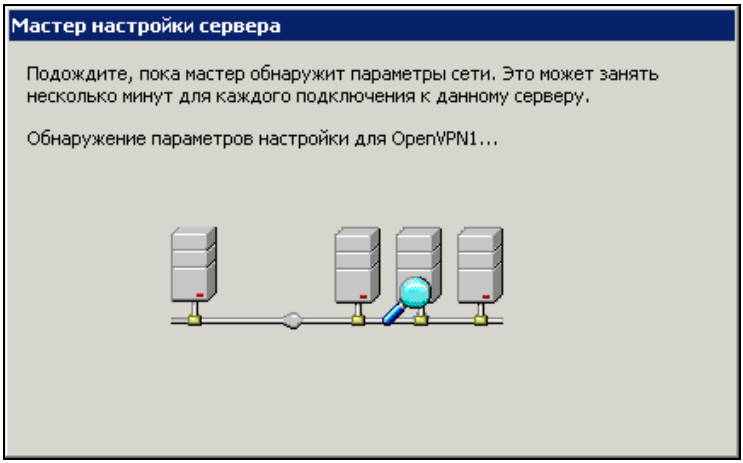


Рис. 3.34. Мастер настройки сервера определяет параметры подключений

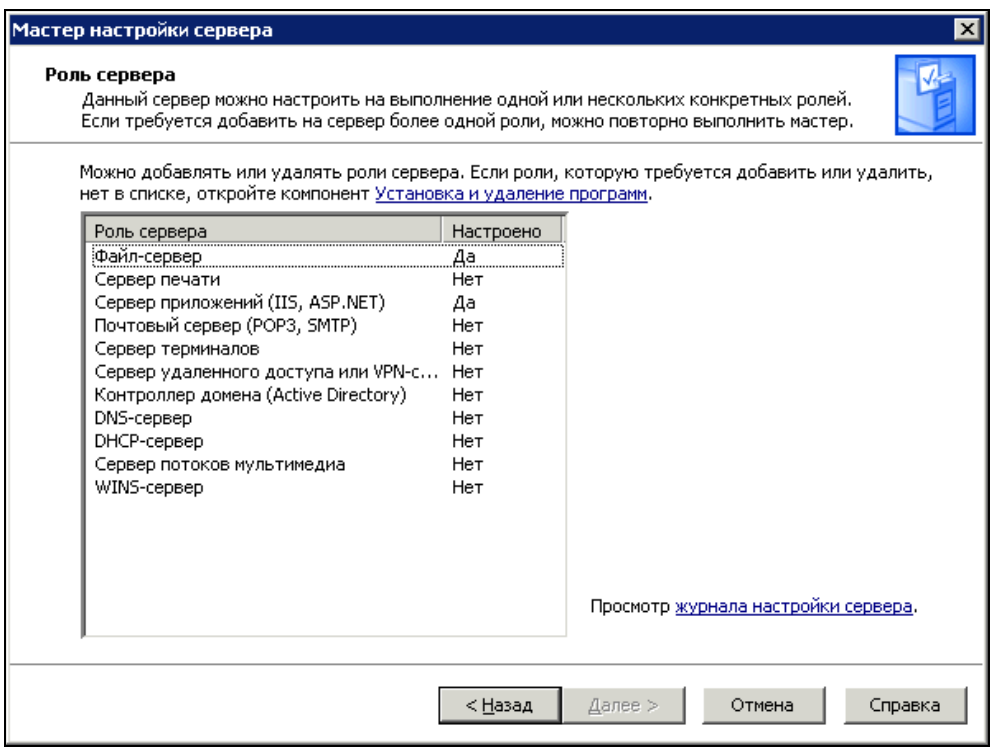


Рис. 3.35. Мастер настройки сервера, раздел **Роль сервера**

После нажатия кнопки **Далее** в окне мастера настройки сервера начнется сбор информации о параметрах сети (рис. 3.34). Проанализировав сеть, мастер настройки сети покажет следующее окно (рис. 3.35), в котором перечислены уже применяемые или не применяемые роли сервера.

На данном сервере уже работает общий доступ к файлам и создан Web-сервер. Поэтому роли **Файл-сервер** и **Сервер приложений** отмечены как настроенные. Нас в приведенном списке интересует строка **Сервер удаленного доступа или VPN-с…**. Выбрав этот пункт, нажимаем кнопку **Далее**. Появится окно с информацией о том, что после нажатия кнопки **Далее** будет запущен мастер настройки маршрутизации и удаленного доступа. Нажимаем кнопку **Далее**.

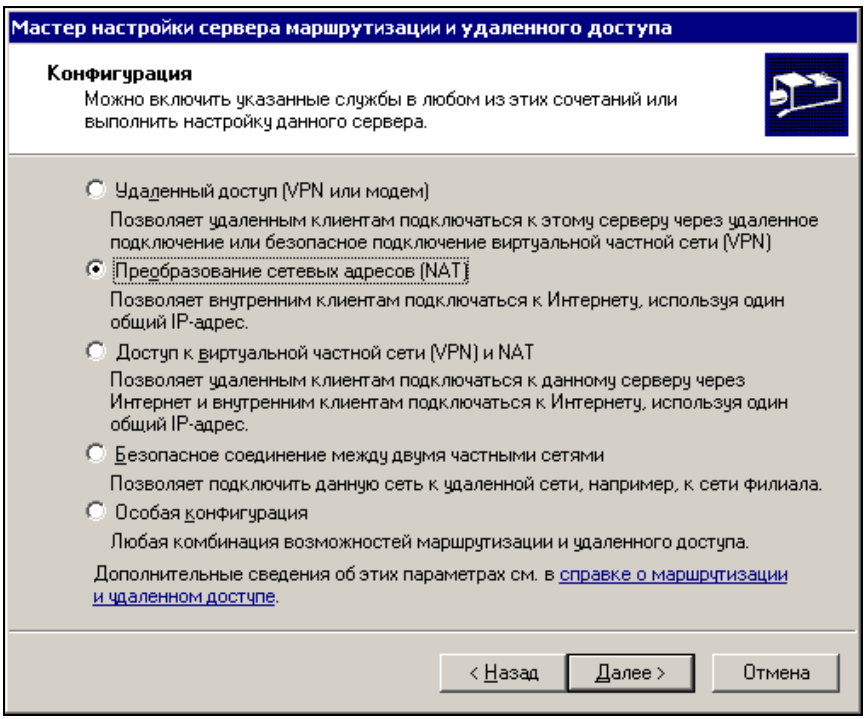


Рис. 3.36. Окно **Мастер настройки сервера маршрутизации и удаленного доступа**, раздел **Конфигурация**

Мастер настройки маршрутизации и удаленного доступа предлагает выбрать вариант продолжения настроек (рис. 3.36). В соответствии с нашей задачей

выбираем **Преобразование сетевых адресов (NAT)**. Конечно, опять нажимаем кнопку **Далее**. Мастер снова предлагает выбор (рис. 3.37). На этот раз нужно выбрать общедоступный сетевой адаптер или создать интерфейс для нового подключения по требованию. Второй вариант можно выбрать, если вы решили настроить подключение через коммутируемый доступ к Интернету или другое подключение, которое должно включаться по требованию. Но в данном примере мы настраиваем доступ через постоянное подключение к Интернету. Поэтому выбираем сетевой адаптер, который смотрит в подключаемую сеть. В нашем примере IP-адрес этого адаптера 10.15.2.7.

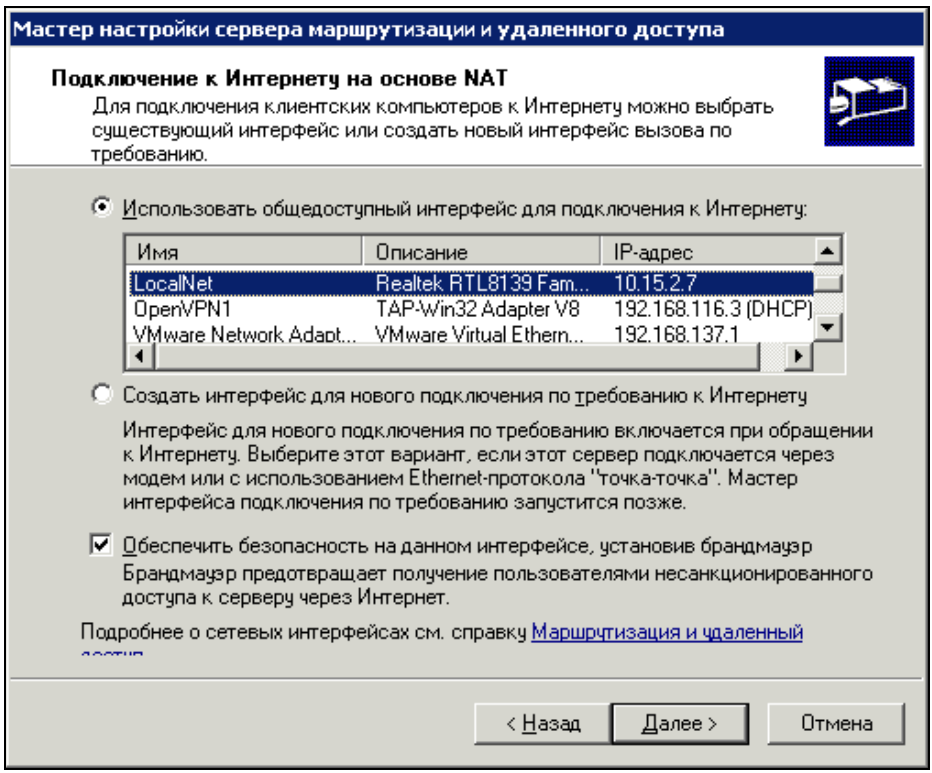


Рис. 3.37. Окно **Мастер настройки сервера маршрутизации и удаленного доступа**, раздел **Подключение к Интернету на основе NAT**

При настройке подключения напрямую в Интернет обязательно отмечаем флажок **Обеспечить безопасность на данном интерфейсе, установив брандмауэр**.

В следующем окне выбираем соединение, через которое сервер подключен к Интернету (рис. 3.38). В нашем случае это адаптер с адресом 192.168.1.7.

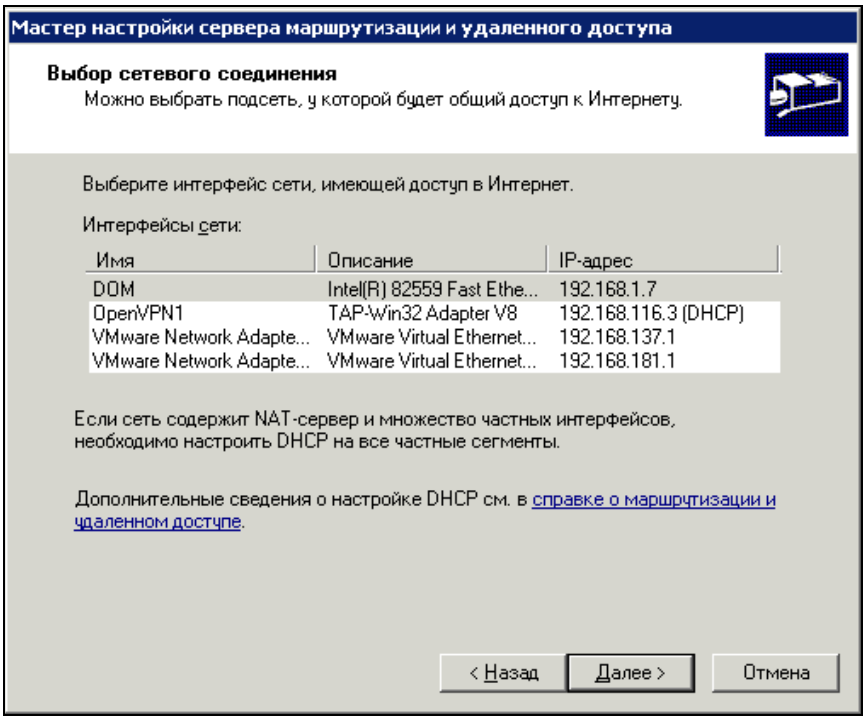


Рис. 3.38. Окно **Мастер настройки сервера маршрутизации и удаленного доступа**, раздел **Выбор сетевого соединения**

Далее наступает завершающий этап работы мастера. Он предупреждает, что должны быть правильно настроены службы DNS и DHCP. Пока не обращаем внимания на эти предупреждения. Ведь при отсутствии какой-либо службы сервер не взорвется. Но имеем пока в виду, что все адреса компьютеров наших сетей мы назначили сами. С серверами DNS и DHCP разбираться будем несколько позднее.

Последним шагом мастера настройки будет запуск службы маршрутизации и удаленного доступа и сообщение о том, что сервер настроен в качестве сервера маршрутизации и удаленного доступа.

Пробуем подключение к Интернету с компьютера 10.15.2.17… Ничего не получилось! Проверяем весь путь наших настроек. Если вы делали реаль-

ные настройки, то, вероятно, документировали их. Просмотрим наши записи или текст в книге… Во время работы мастера были перепутаны интерфейсы сервера!

Подключение к Интернету выбранной подсети происходит на самом деле через адаптер с адресом 10.15.2.7, а общедоступный интерфейс 192.168.1.7. Что ж, ошибки всегда возможны. Обнаруживаются они обычно потому, что не работает то, что мы настраивали. Исправим ошибку. Откроем **Администрирование | Маршрутизация и удаленный доступ**. Появится окно **Routing and Remote Access** (рис. 3.39).

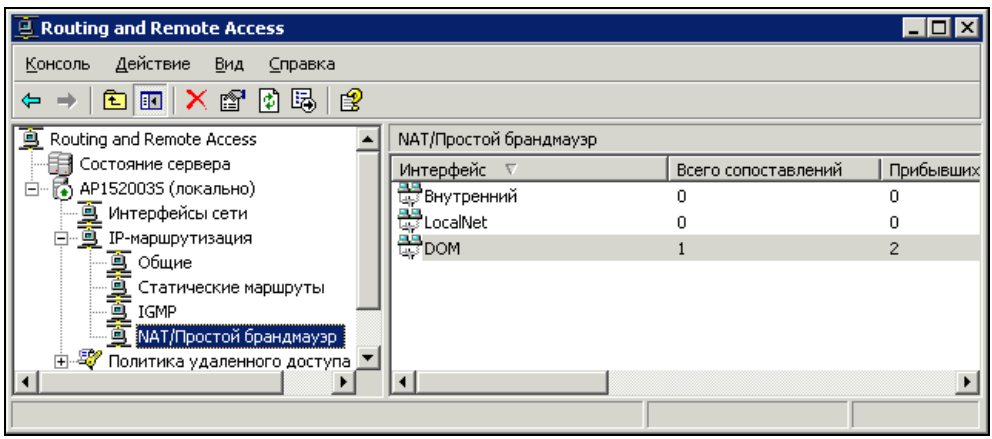


Рис. 3.39. Окно **Routing and Remote Access**

Выберите в дереве объектов в левой части окна **NAT/Простой брандмауэр**. В правой части окна проверьте свойства интерфейсов, которые подключены на сервере. В данном случае это **LocalNet**, смотрящий в новую сеть 10.15.2.0, и **DOM**, имеющий адрес 192.168.1.7.

Для **LocalNet** окно свойств должно выглядеть, как на рис. 3.40, а для **DOM** — как на рис. 3.41. Имена сетевых подключений на вашем сервере могут быть иными. Лучше, если вы их переименуете, для того чтобы легче ориентироваться в их назначении, когда идет настройка сети.

Простое изменение состояния переключателей и флажков в этих окнах приведет сразу к возможности выхода в Интернет с компьютеров второй сети (10.15.2.0). В частности с компьютера с адресом 10.15.2.17, который участвует в примере.

Окно **Routing and Remote Access** (см. рис. 3.39) еще не раз нам понадобится для проведения довольно интересных настроек сети. Можно было вообще все настройки выполнить из этого окна, но для этого надо было бы точно знать, как и что изменить. Мастер настройки сделал это за нас. С помощью данного окна и некоторых дополнительных средств можно будет настроить доступ к вашей сети из Интернета, например из другой сети, имеющей постоянное подключение к Интернету. Но об этом позднее.

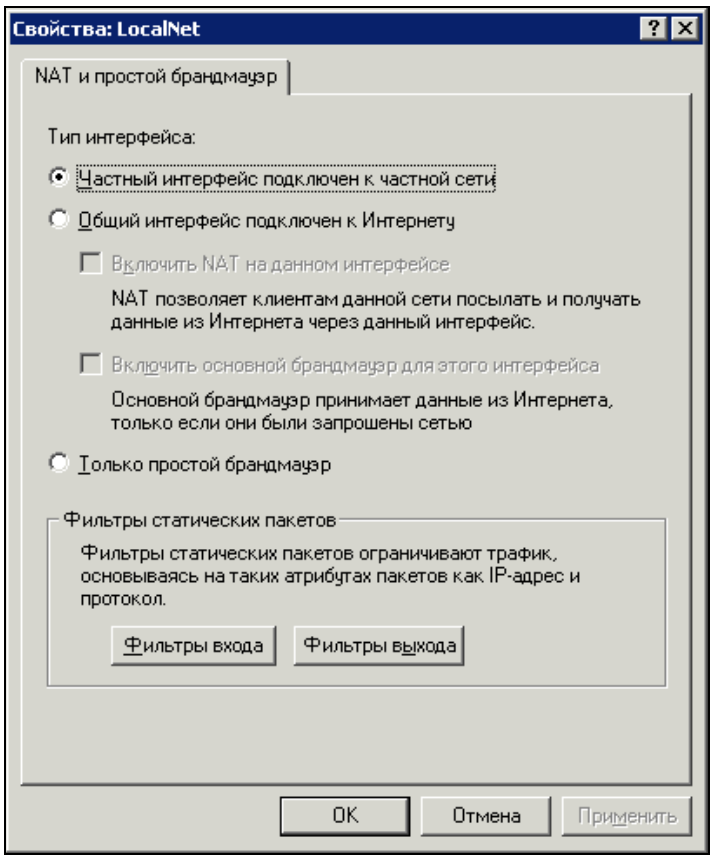


Рис. 3.40. Окно **Свойства: LocalNet**

Все в мире относительно. Наш сервер стал выполнять одну из своих ролей для второй сети (10.15.2.0). Для сети с адресом 192.168.1.0 этот компьютер остался рядовым.

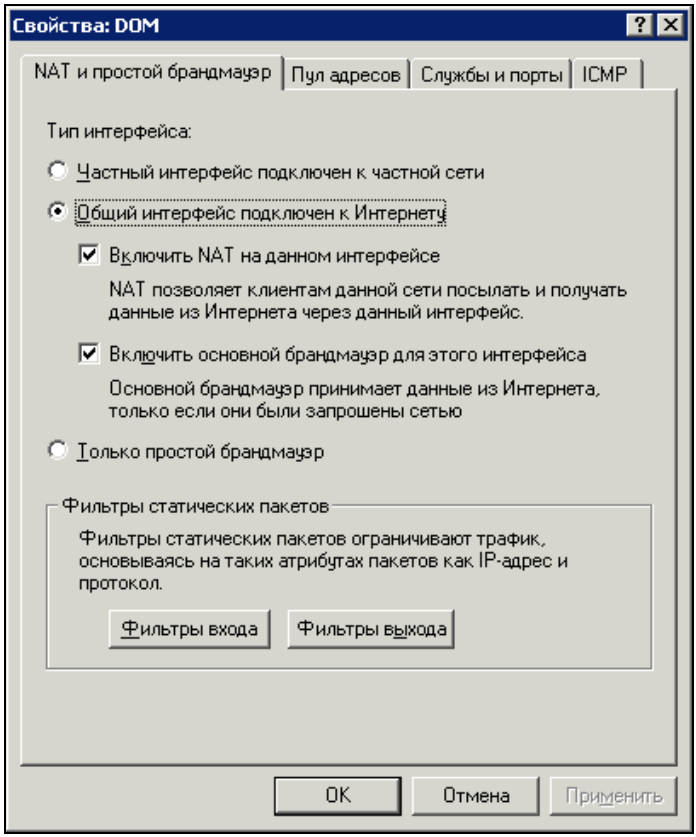


Рис. 3.41. Окно **Свойства: DOM**

Практика применения общего доступа к подключению Интернета

Практическая реализация общего доступа к подключению Интернета может вызвать множество вопросов и затруднений. Поэтому приведем реально работающий простой вариант такого доступа с использованием обычного dial-up-подключения в сети с выделенным сервером Windows 2000 Server, с работающими DNS-, DHCP-, WINS-серверами и управлением сетью на основе Active Directory. Основной сервер сети является контроллером домена.

IP-адрес основного сервера сети — 192.168.0.15, другие компьютеры получают адреса через DHCP-сервер. Для отдельных компьютеров адреса заре-

зервированы, чтобы их значения не могли измениться случайным образом. Задача по обеспечению доступа к Интернету возложена на компьютер с операционной системой Windows 2000 Pro, выполняющий функции вспомогательного сервера (внутренняя почта, внутренний Web-сайт, резервное копирование данных по расписанию, автоматическое выполнение некоторых сервисных задач по обслуживанию программного обеспечения и подключение к Интернету). Доступ к серверу предоставляется с помощью Radmin. Для обеспечения информационной безопасности локально (и через Radmin) к вспомогательному серверу могут подключаться пользователи сети с правами администратора и с ограниченными правами, дающими доступ к подключению Интернета. На рабочий стол вспомогательного сервера для пользователей с ограниченными правами выведен ярлык модемного соединения.

> ***Примечание***
>
> Если в качестве вспомогательного сервера применяется компьютер с операционной системой Windows 2000 Server, доступ к нему может осуществляться через сервер терминалов.

IP-адрес вспомогательного сервера зарезервирован и никогда не изменяется. Это необходимо для обеспечения стабильности настроек интернет-браузера и Radmin-клиента у пользователей.

На вспомогательном сервере установлена программа AnalogX Proxy. Сеанс пользователя с ограниченными правами включен практически всегда. Применение средств безопасности NT для Radmin-сервера дополнительно повышает информационную защиту.

На клиентских рабочих станциях используется браузер Internet Explorer 6 с настроенной системой безопасности. Самостоятельное изменение этих настроек пользователям запрещено. Соединение устанавливается по локальной сети, в качестве адреса прокси-сервера указывается адрес вспомогательного сервера (рис. 3.42).

Для подключения к Интернету пользователь включает со своего рабочего места сеанс связи со вспомогательным сервером через Radmin и щелкает кнопкой мыши по ярлыку соединения на рабочем столе вспомогательного сервера. Если в это время сеансы связи не запрещены администратором сети (можно просто выключать модем), то связь устанавливается. При установленном соединении пользователь видит информацию о соединении. Теперь можно запускать браузер и выходить в Интернет. Программа Radmin обеспечивает работу нескольких пользователей в одном сеансе. В данном случае

это позволяет любому пользователю видеть состояние подключения, установленного другим пользователем. Нет необходимости разрывать соединение, поскольку это произойдет автоматически при бездействии в течение пяти минут (настройки соединения). Во время эксплуатации подключения по такой схеме не было обнаружено каких-либо конфликтов или неполадок. Работа с электронной почтой напрямую через Интернет пользователям запрещена (централизованно принимаемая почта может быть оперативно проверена на наличие вирусов), поэтому для обеспечения почтовой связи применяются другие средства, которые будут рассмотрены в *главе 4*. Скорость связи при такой схеме не ниже, а часто даже выше, чем скорость связи через тот же модем с локальной машины. Вспомогательный сервер работает круглосуточно, свои основные обязанности по автоматическому архивированию и обслуживанию базы данных он выполняет преимущественно в ночное время. Днем его возможности могут использоваться почти без ограничения времени.

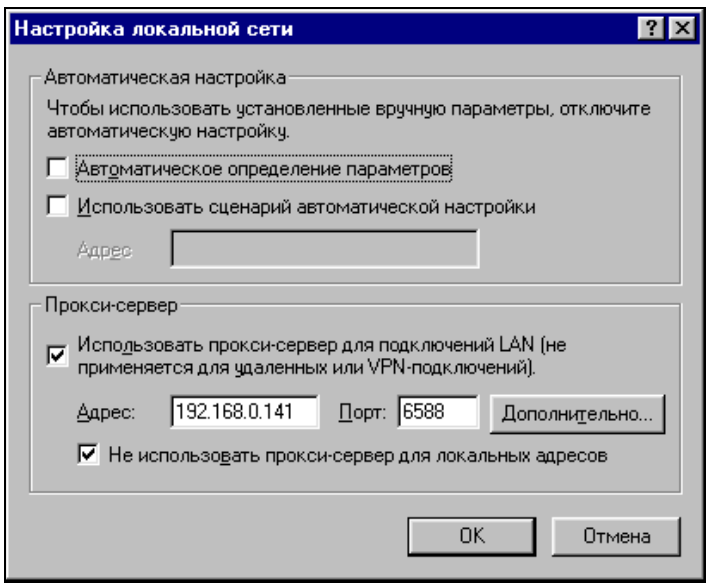


Рис. 3.42. Окно **Настройка локальной сети**

Можно организовать подключение к Интернету по расписанию. В этом случае, необходимо выделить определенные часы для общего доступа к подключению Интернета и поместить ярлык соединения в планировщик заданий, настроив расписание для выполнения подключения.

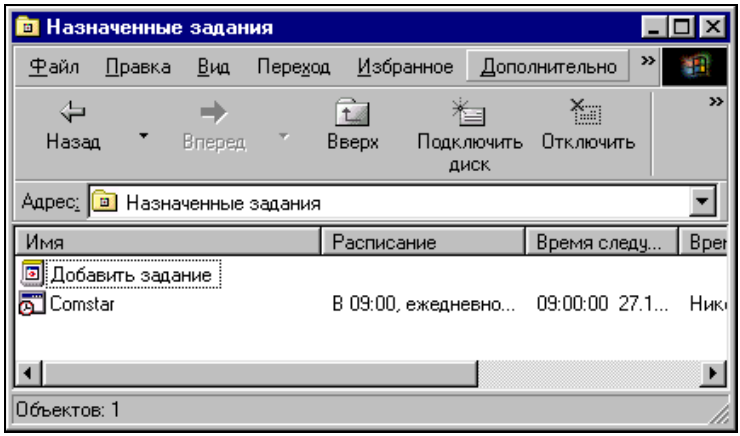


Рис. 3.43. Окно **Назначенные задания** планировщика заданий

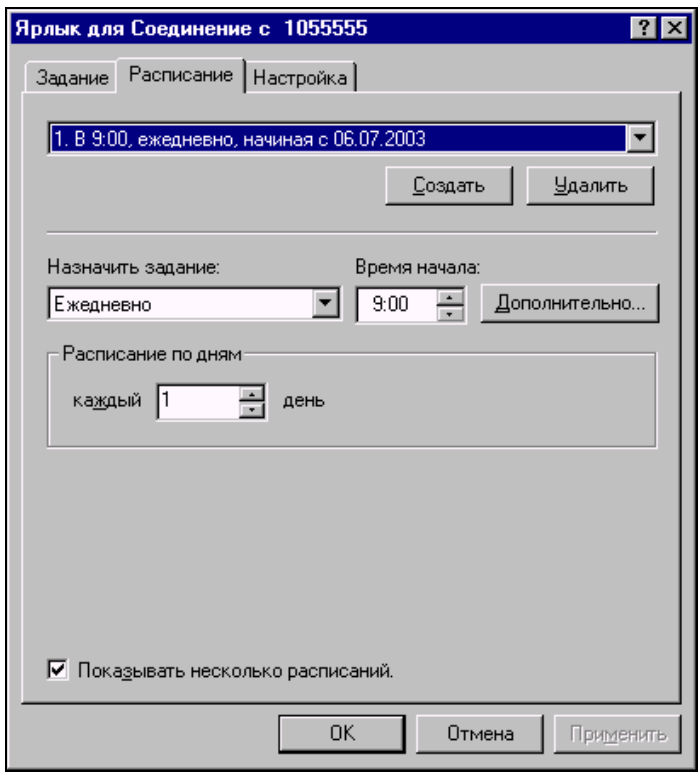


Рис. 3.44. Вкладка **Расписание** в свойствах задания

При этом отпадет необходимость предоставлять пользователям доступ к вспомогательному серверу и не понадобится Radmin на их компьютерах. Чтобы поместить ярлык соединения в планировщик заданий, достаточно этот ярлык перетащить мышью в открытое окно планировщика (рис. 3.43).

Для настройки расписания необходимо щелкнуть правой кнопкой мыши по значку задания и выбрать пункт **Свойства**, а затем открыть вкладку **Расписание** (рис. 3.44).

Можно установить несколько расписаний, учитывая выходные дни и различие в режимах работы в течение недели, месяца и даже года. Возможна и комбинация методов подключения для различных пользователей в соответствии с потребностями вашей сети.

Программа настройки IP (WINIPCFG)

Windows 95/98 имеет в своем составе полезную служебную программу WINIPCFG.EXE. Она позволяет проверить настройки IP, которые устанавливаются в различных окнах системы и трудно контролируются, а также обновить настройки, получаемые автоматически.

Для запуска программы выполните следующие шаги:

1. Нажмите кнопку **Пуск** и выберите команду **Выполнить**.
2. В поле **Открыть** введите `winipcfg`.
3. Нажмите кнопку **Сведения**.
4. Для просмотра адресов серверов DNS, указанных в настройке компьютера, нажмите кнопку с многоточием (**...**) справа от поля **Серверы DNS**. Если эта кнопка отсутствует, то для данного компьютера поддержка DNS отключена.
5. Для просмотра сведений об адресах сетевых адаптеров выберите адаптер в поле со списком в группе **Ethernet: сведения**.

Служебная программа настройки IP позволяет пользователям и администраторам просматривать сведения о текущих IP-адресах и другие данные о сетевой конфигурации. Пользователь имеет возможность выполнить сброс одного или нескольких IP-адресов. Для одного IP-адреса следует использовать кнопку **Освободить** или **Обновить**. Если требуется обновить или освободить все IP-адреса, нажмите кнопку **Освободить все** или **Обновить все**. После этого компьютер либо получает новый IP-адрес от службы DHCP, либо автоматически назначает себе личный IP-адрес.

С помощью Windows 95/98 можно обеспечить маршрутизацию, но придется привлечь некоторые дополнительные программки. Windows 95 нужно обновить, установив DUN 1.3 с сайта **www.microsoft.com**. Далее в системном реестре необходимо сделать маленькое исправление: добавить строковый параметр (String Value) в ключ `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP`, назвать его `EnableRouting` и присвоить значение `1`.

После чего можно запустить программу WINIPCFG (рис. 3.45). Если стоит флажок рядом с надписью **Маршрутизация IP** (IP Routing enabled), то все прописанные таблицы маршрутизации начали работать. По умолчанию в Windows 95/98 этот флажок не выставлен.

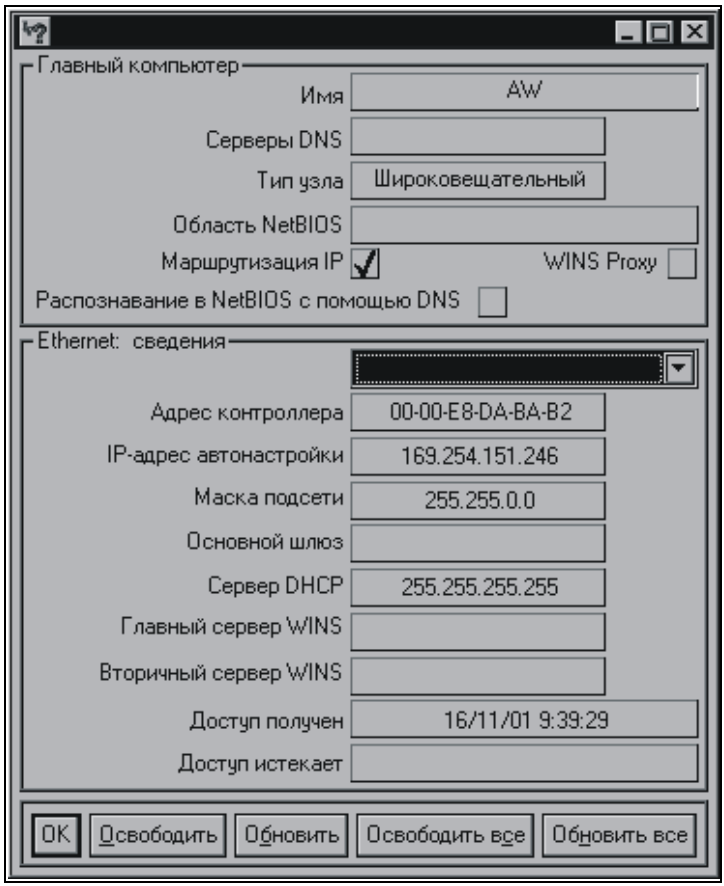


Рис. 3.45. Окно программы WINIPCFG.EXE

Для осуществления маршрутизации необходимо наличие на компьютере-маршрутизаторе двух интерфейсов связи с сетями, например двух сетевых адаптеров, каждый из которых имеет собственный IP-адрес, соответствующий подсети, с которой он связан. Командой `route` из командной строки можно установить необходимые маршруты.

Далее приведена справка команды `route`, полученная с экрана монитора.

```
C:\WINDOWS>route/?
Обработка таблиц сетевых маршрутов.
ROUTE [-f] [команда [узел] [MASK маска] [шлюз] [METRIC метрика]]
  -f            Очистка таблиц маршрутов от записей для всех шлюзов.
                При указании одной из команд таблицы очищаются
                до выполнения команды.
  команда       Одна из четырех команд
                  PRINT     Печать маршрута
                  ADD       Добавление маршрута
                  DELETE    Удаление маршрута
                  CHANGE    Изменение существующего маршрута
  узел          Адресуемый узел.
  MASK          Если вводится ключевое слово MASK, то следующий параметр
                интерпретируется как параметр "маска".
  маска         Значение маски подсети, связываемое с записью для данного
                маршрута. Если этот параметр не задан, по умолчанию
                подразумевается 255.255.255.255.
  шлюз          Шлюз.
  METRIC        Определение параметра метрика/цена для адресуемого узла.
                Поиск всех символических имен узлов проводится в файле
                сетевой базы данных.
NETWORKS        Поиск символических имен шлюза проводится в файле базы
                данных имен узлов HOSTS.
Для команд PRINT и DELETE можно указать узел и шлюз с помощью подстано-
вочных знаков или опустить параметр "шлюз".
Сведения диагностики:
    неправильное значение MASK приводит к ошибке, (DEST & MASK) != DEST.
    Например> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1
              Сбой добавления маршрута: 87
Примеры:
    > route PRINT
```

```
    > route   ADD 157.0.0.0     MASK 255.0.0.0   157.55.80.1 METRIC 3
              назначение        маска            шлюз        метрика
    > route PRINT
    > route DELETE 157.0.0.0
    > route PRINT
C:\WINDOWS>
```

Существуют также программы, с помощью которых можно превратить компьютер в шлюз между сетями.

Программа, описание которой приведено далее, позволяет установить маршрутизацию как между локальными подсетями, так и между локальной сетью и Интернетом. Эта программа называется WinRoute, разработана компанией Tiny Software Inc. Между версиями программы есть некоторые отличия (например, защита сети различных уровней), но основные функции программы доступны во всех версиях. В Интернете можно найти версии от WinRoute Lite до WinRoute Pro 4.1.

Маршрутизация и WinRoute

Маршрутизация — процесс, задающий путь прохождения пакета от источника к приемнику.

С точки зрения маршрутизации компьютеры подразделяются на две группы.

- Клиентские станции.

  На клиентских станциях обычно стоит один сетевой адаптер и они не осуществляют пересылку пакетов с одного интерфейса на другой. У них есть таблица маршрутизации, однако они используют ее только для отсылки собственных пакетов. Таблица маршрутизации обычно содержит запись маршрутизатора (шлюза) по умолчанию. Имеет место прямой путь (route) от клиентской станции до маршрутизатора по умолчанию.

- Маршрутизаторы (шлюзы).

  На шлюзах установлено более одного сетевого адаптера (интерфейса). На уровне интерфейсов шлюз имеет подключение к двум и более сетям. Когда по интерфейсу прибывает пакет, шлюз должен принять решение, по какому из оставшихся интерфейсов должен быть отослан этот пакет. Подходящий интерфейс выбирается в соответствии с IP-адресом назначения пакета и таблицей маршрутизации шлюза.

WinRoute — программа, которая позволяет организовать шлюз.

В обычной сети (т. е. односегментной ЛВС, подключенной к Интернету через модем) нет надобности модифицировать таблицу маршрутизации на компьютере, где работает WinRoute. С другой стороны, более чем необходимо модифицировать таблицу маршрутизации в многосегментной сети.

Маршрутизация в сети с несколькими сегментами

В сети с несколькими сегментами, расположенными за другими шлюзами, может возникнуть необходимость вручную ввести маршруты для каждого сегмента (если в вашей сети не используется какой-либо протокол маршрутизации).

На рис. 3.46 показана сеть с двумя сегментами, один из которых подключен через маршрутизатор.

В этом случае настройка маршрутизации следующая:

1. На компьютере с WinRoute должен быть введен путь до сегмента 192.168.2.0. Это может быть сделано из командной строки:

   ```
   c:\>route -p add 192.168.2.0 mask 255.255.255.0 192.168.1.100.
   ```

2. На маршрутизаторе 192.168.1.100 путь по умолчанию должен вести к компьютеру WinRoute, т. е. 192.168.1.1.

Маршрутизация в среде Windows

WinRoute использует таблицу маршрутизации, предоставляемую операционной системой Windows.

Для работы с таблицей маршрутизации используется системная команда `route`, введенная из командной строки.

Вы можете использовать команду `route` следующим образом:

- `route print` (для распечатки содержимого таблицы маршрутизации);
- `route add` (для добавления маршрута);
- `route delete` (для удаления маршрута).

Как упоминалось ранее, шлюз использует таблицу маршрутизации для определения интерфейса, по которому будет пересылаться пакет.

Основные пункты таблицы маршрутизации:

- ❒ network/network mask (сеть/сетевая маска);
- ❒ metric (метрика);
- ❒ interface (интерфейс);
- ❒ gateway (шлюз).

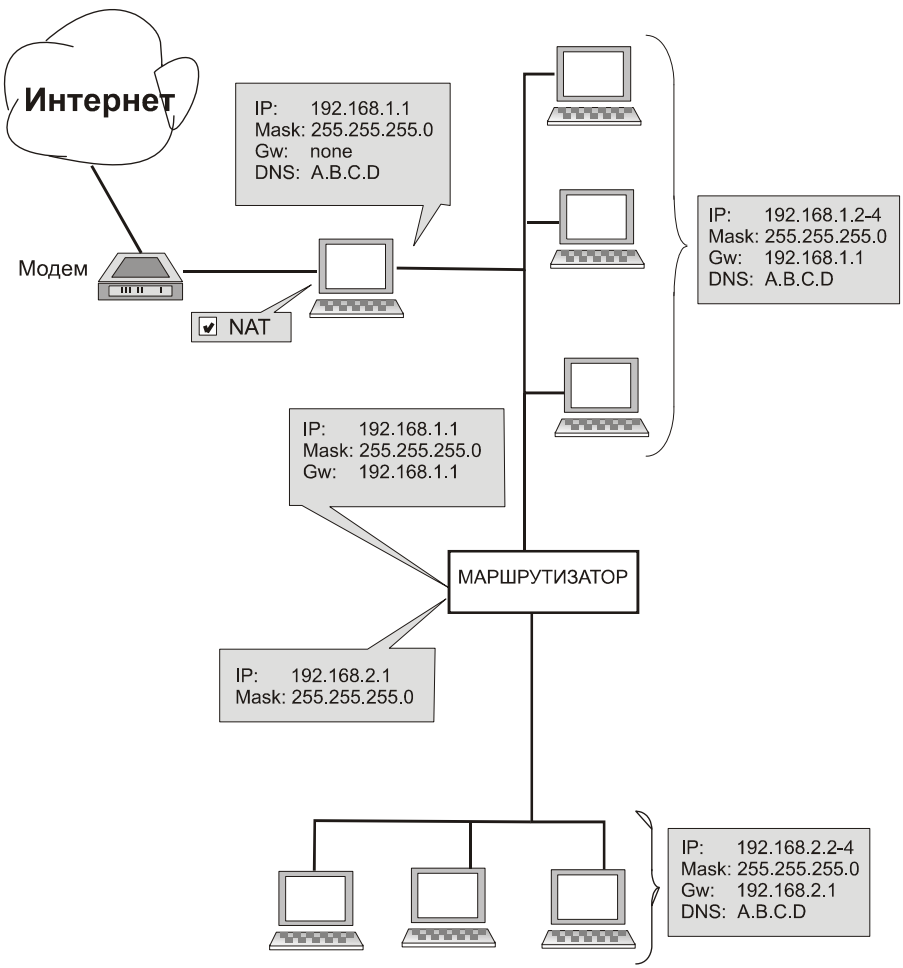


Рис. 3.46. Сеть с двумя сегментами, один из которых подключен через маршрутизатор

После принятия решения, каким интерфейсом будет отослан пакет, применяется следующий алгоритм:

1. Просматривается таблица маршрутизации для обнаружения записи, в которой параметр **network** совпадает с IP-адресом назначения, указанным в заголовке пакета (а также с сетевой маской). Если найдено несколько таких записей, выбирается запись с наиболее подходящей маской. Если есть две или более записи, выбирается запись с наименьшей метрикой.
2. Пакет отсылается по интерфейсу, указанному в записи. Если компьютер назначения не входит в сеть, подключенную к интерфейсу, пакет пересылается на шлюз, указанный в записи.

Запись с нулевым сетевым адресом и нулевой маской имеет особый смысл. Она обозначает маршрут по умолчанию, указывает, куда отсылать пакет, если для него не была найдена соответствующая запись.

Мы можем разбить записи в таблице маршрутизации на категории в соответствии с их источниками.

- Direct (Прямые).

  Прямые маршруты добавлены в таблицу с использованием IP-адреса и маски, которые назначены для индивидуальных интерфейсов маршрутизатора. Они идентифицируют сети, доступные напрямую.

- Persistent (Постоянные).

  Устойчивые маршруты идентифицируют сети, которые не подключены напрямую к интерфейсам маршрутизатора. Эти маршруты конфигурируются лицом, обслуживающим маршрутизатор, и устанавливаются при загрузке ОС.

- Temporary (Временные).

  Временные маршруты вводятся пользователем или получаются посредством протокола маршрутизации. Они теряются при выключении системы.

Таблица маршрутизации создается во время загрузки Windows следующим образом: создаются прямые маршруты и постоянные маршруты считываются из реестра Windows (постоянные маршруты могут конфигурироваться только в Windows NT/2000). Также добавляется маршрут по умолчанию (в настройках TCP/IP для каждого интерфейса маршрут по умолчанию устанавливается шлюзом по умолчанию). Вы можете установить маршруты по умолчанию на некоторых интерфейсах, однако имеет смысл сделать это только для одного интерфейса — соединяющего компьютер с внешней сетью (Интернет).

Таблица может быть модифицирована пользователем или протоколом маршрутизации (например, RIP — Routing Information Protocol, протокол маршрутной информации), если таковой используется. Если вы создаете модемное соединение, Windows добавляет маршрут по умолчанию (в соответствии с настройками применяемого модемного соединения). Если таблица маршрутизации уже содержит маршрут по умолчанию, его метрика увеличивается, а модемное соединение получает приоритет. При закрытии модемного соединения маршрут удаляется.

Примеры работы с портами

Приведенные далее примеры представляют типичное использование привязки портов. Однако вы можете создавать множество других привязок портов. При этом всегда нужно помнить о безопасности вашей сети. Создавая порт, вы разрешаете доступ из Интернета к некоторым службам вашей сети. Используйте фильтрацию пакетов, если хотите разрешить доступ к порту только с нужных адресов в Интернете.

Web-сервер. Предположим, у вас в ЛВС работает Web-сервер (адрес — 192.168.1.10) и вы хотите открыть к нему доступ из Интернета. Вам необходимо создать порт:

- Protocol: `TCP`;
- Listen IP: <не определен>;
- Listen Port: `80`;
- Destination IP: введите IP-адрес Web-сервера (в нашем случае `192.168.1.10`);
- Destination Port: `80`.

SMTP. Если у вас в ЛВС работает почтовый сервер и вы хотите получать почту из Интернета по протоколу SMTP, добавьте следующие записи в таблицу портов:

- Protocol: `TCP`;
- Listen IP: <не определен>;
- Listen Port: `25`;
- Destination IP: введите IP-адрес вашего почтового сервера;
- Destination Port: `25`.

PPTP. Если у вас в ЛВС работает сервер PPTP (Point to Point Tunneling Protocol) и вы хотите открыть доступ к вашему серверу по PPTP, нужно создать два порта.

- Для управляющего соединения:
  - Protocol: `TCP`;
  - Listen IP: <не определен>;
  - Listen Port: `1723`;
  - Destination IP: IP-адрес вашего сервера PPTP;
  - Destination Port: `1723`.
- Для пакетов GRE (PPTP):
  - Protocol: `PPTP`;
  - Listen IP: <не определен>;
  - Destination IP: еще раз адрес вашего сервера PPTP.

CU-SeeMe. Если вы просто вызываете других пользователей посредством CU-SeeMe, у вас не должно быть проблем. Если же вы хотите также получать вызовы CU-SeeMe, то должны создать следующие порты:

- Protocol: `UDP`;
- Listen IP: <не определен>;
- Listen Port: `7648`;
- Destination IP: IP-адрес компьютера, на котором запущен клиент CU-SeeMe;
- Destination Port: `7648`;
- Protocol: `UDP`;
- Listen IP: <не определен>;
- Listen Port: `7649`;
- Destination IP: IP-адрес компьютера, на котором запущен клиент CU-SeeMe;
- Destination Port: `7649`.

ICQ. Вы можете соединяться с серверами ICQ и общаться с другими пользователями ICQ без создания портов.

Если требуется получать вызовы от пользователей ICQ, необходимо создать следующие записи в таблице портов:

- Protocol: `TCP`;
- Listen IP: <не определен>;
- Listen Port: `5000–5011`;
- Destination IP: IP-адрес машины, на которой запущен клиент ICQ;
- Destination Port: `5000–5011`.

Затем необходимо сделать следующее: в ICQ в меню **Preferences** (Настройки) выбрать пункт **Connection** (Соединение) и подпункты **I'm using a permanent internet connection (LAN)** (Я использую соединение локальной сети с Интернетом), **I'm behind a firewall or proxy** (Я защищен экраном или прокси-сервером). В меню **Firewall Settings** (Настройки экрана) выбрать **I don't use a SOCKS Proxy server** (Я не использую подключение через прокси-сервер), нажать кнопку **Next** (Далее), выбрать **Use the following TCP listen ports for incoming event** (Использовать следующие TCP-порты для входящих подключений) и ввести порты от 5000 до 5011.

Если вы хотите, чтобы в сети работало несколько клиентов ICQ (и эти клиенты должны получать вызовы из Интернета), необходимо создать запись в таблице портов для каждого дополнительного клиента и назначить ему промежуток портов (например, `5012–023`). Также необходимо настроить каждого клиента соответствующим образом.

Все большее число пользователей используют для связи с Интернетом быстрые соединения, такие как в системе DirecPC, осуществляющей связь через спутник.

Уверенный прием сигнала со спутника Eutelsat II F3 возможен на северо-западе России — в Ленинградской, Псковской, Новгородской, Мурманской области, Карелии и, конечно, в Калининградской области. Также уверенный прием возможен на западе Украины и Белоруссии. Спутник HotBird 3 обеспечивает уверенный прием во всей европейской части России на антенну диаметром 0,6—1,5 м. Первая в России система DirecPC была запущена в феврале 1997 года фирмой SoftJoys в Санкт-Петербурге. В октябре 1997 года первую систему запустили в Diamond Communication в Москве.

Для обеспечения работы системы можно установить обычную телевизионную приемную спутниковую антенну с конвертером соответствующего диапазона и купить ISA- или PCI-карту DirecPC. Для работы через спутник HotBird 3 подходит только PCI-карта.

Комплект оборудования DirecPC поставляется с программным обеспечением для работы под управлением ОС Windows 95 или Windows NT. Можно приобрести сетевую версию программного обеспечения DirecPC или, в качестве более дешевого решения, при наличии у вас dial-up-соединения с Интернетом, для раздачи по локальной сети на компьютер с DirecPC и модемом, можно установить WinGate для Win95. Возможно более продвинутое использование DirecPC — например, если у вас уже есть постоянное соединение с Интернетом, можете непосредственно включить ваш компьютер в последовательный порт вашего маршрутизатора.

Использование WinRoute с DirecPC

Это описание предполагает, что вы хорошо знакомы с DirecPC и у вас на машине установлено и нормально работает соответствующее программное обеспечение.

WinRoute может работать с DirecPC в зависимости от того, как отсылаются в Интернет пакеты.

1. Отсылаются программным обеспечением DirecPC (DirecPC Navigator).
2. Отсылаются WinRoute через выбранный интерфейс.

В обоих случаях DirecPC Navigator должен работать.

Если вы решили использовать второй способ, то необходимо выбрать интерфейс для пересылки пакетов. Это можно сделать через последовательность команд **Settings | Interfaces | Interface Settings | DirecPC | Send outgoing packets through**.

Отметьте опцию **Through interface** (Через интерфейс) и выберите интерфейс в поле **GW**, если выбран интерфейс типа **ethernet-type** (Локальная сеть Ethernet), необходимо ввести IP-адрес маршрутизатора/шлюза сети, подключенной к этому интерфейсу.

В поле **DirecPC Gateway** (Шлюз DirecPC) введите IP-адрес шлюза DirecPC. Адрес используется тот же, что и в настройках DirecPC. Если вы не знаете адрес, узнайте его у провайдера DirecPC.

Если выбран интерфейс RAS, то в настройках TCP/IP записи RAS должен быть помечен флажок **Use default gateway of remote network** (Использовать стандартный шлюз для удаленной сети).

На рис. 3.47 и 3.48 показана конфигурация сети с использованием первого метода (пакеты отсылаются в Интернет с помощью DirecPC Navigator).

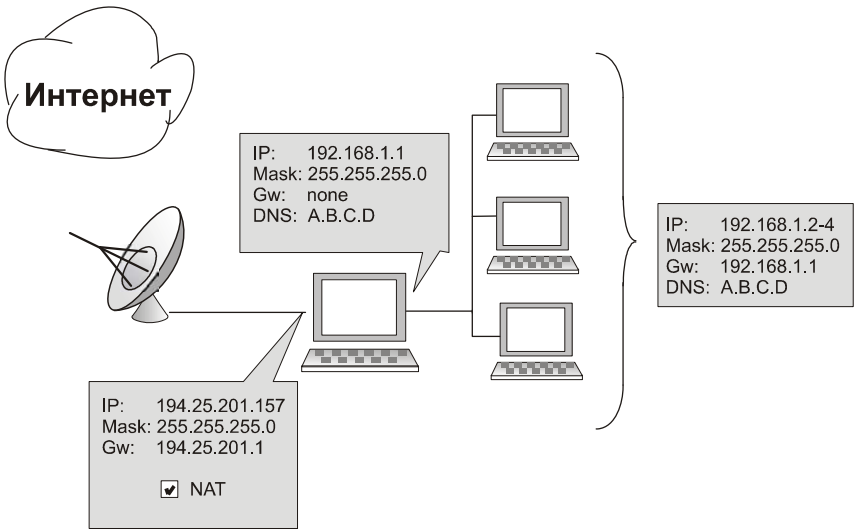


Рис. 3.47. Настройка с использованием DirecPC Navigator

На рис. 3.49 и 3.50 показана конфигурация с использованием второго метода. Пакеты отсылаются через интерфейс RAS (модем или адаптер ISDN). В настройках TCP/IP для RAS опция **Use default gateway of remote network** (Использовать стандартный шлюз для удаленной сети) не должна быть выбрана, иначе весь трафик пойдет через RAS, и DirecPC не будет использоваться.

На рис. 3.51 и 3.52 показана конфигурация сети с использованием второго метода; исходящие пакеты отсылаются через интерфейс Ethernet.

Чтобы получить наилучшую пропускную способность при подключении к Интернету через DirecPC, установите размер окна TCP на всех компьютерах, использующих DirecPC, следующим образом:

- в Windows NT.

  Добавьте (если уже существует, отредактируйте) в системном реестре запись "`TcpWindowSize`" (тип `DWORD`) в ключ

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`.

  Установите значение `0xBB80`;

- в Windows 95/98.

  Добавьте (если уже существует, отредактируйте) в системном реестре запись "`DefaultRcvWindow`" (тип `string`) в ключ

  `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP`.

  Установите значение "`0xBB80`".

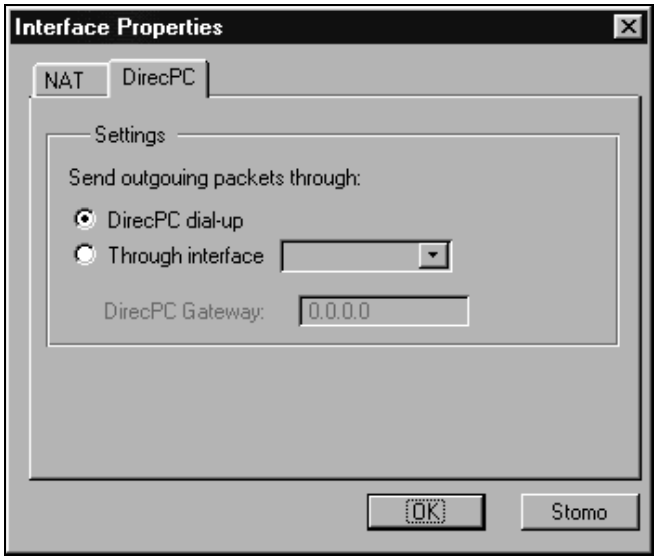


Рис. 3.48. Окно **Interface Properties**

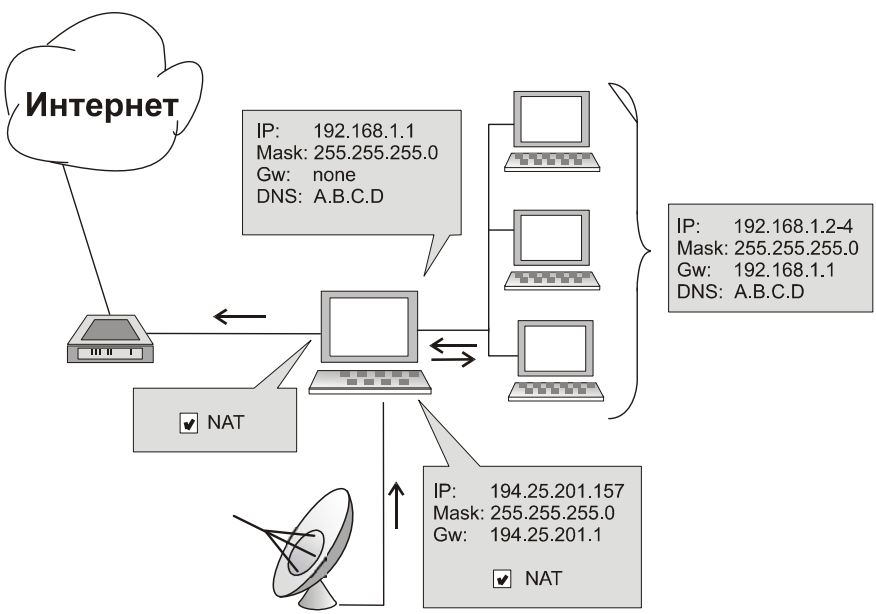


Рис. 3.49. Настройка сети с использованием RAS

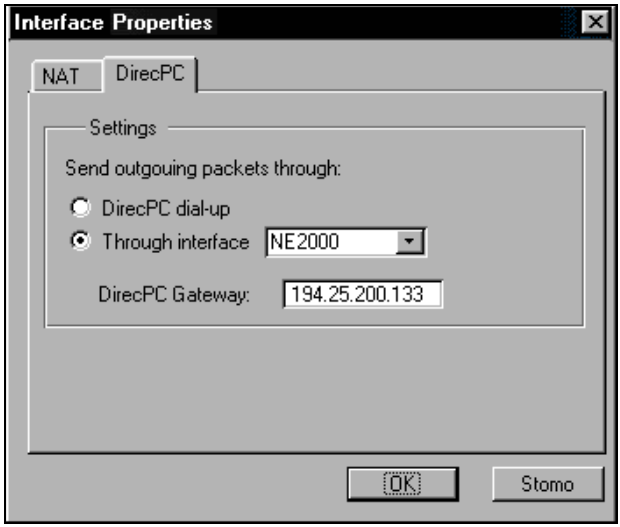


Рис. 3.50. Окно **Interface Properties**
(пакеты отсылаются через интерфейс RAS)

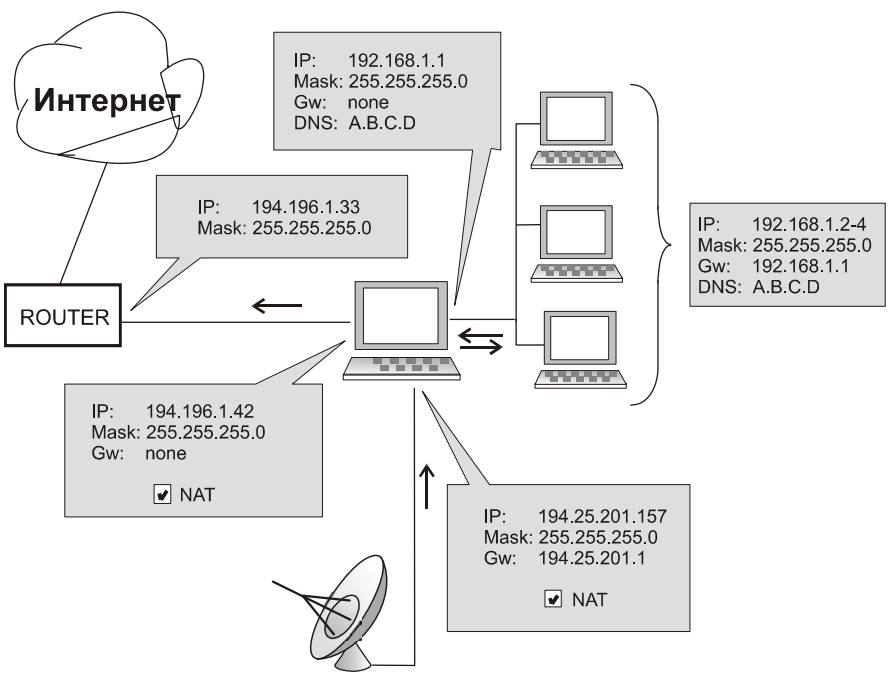


Рис. 3.51. Использование интерфейса Ethernet

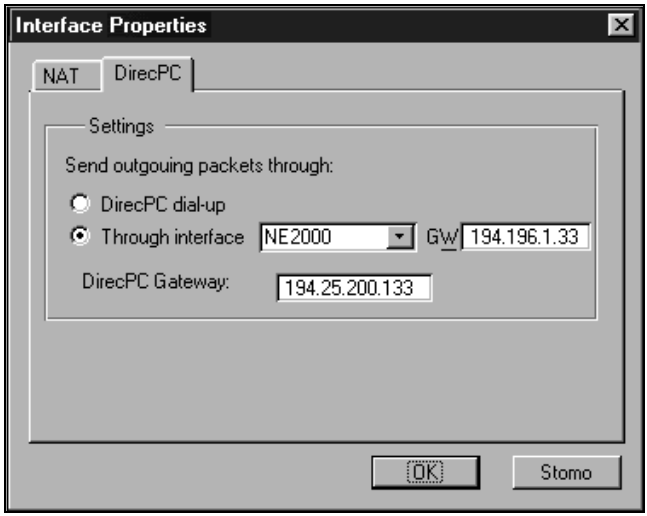


Рис. 3.52. Окно **Interface Properties**
(пакеты отсылаются через интерфейс Ethernet)

Разбиение сети на несколько сегментов

При использовании брандмауэра для защиты ЛВС в некоторых случаях необходимо изменять конфигурацию сети. Первый пример показывает, какие возможности возникают при подключении ЛВС к Интернету через маршрутизатор с использованием зарегистрированного IP-адреса (рис. 3.53).

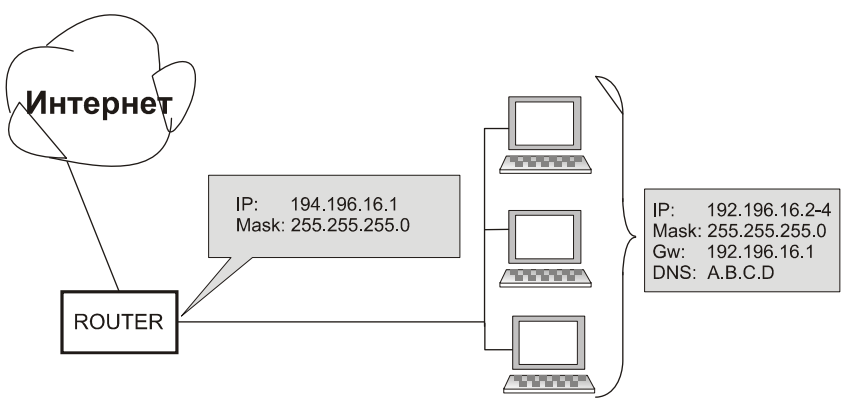


Рис. 3.53. Подключение через маршрутизатор (Router)

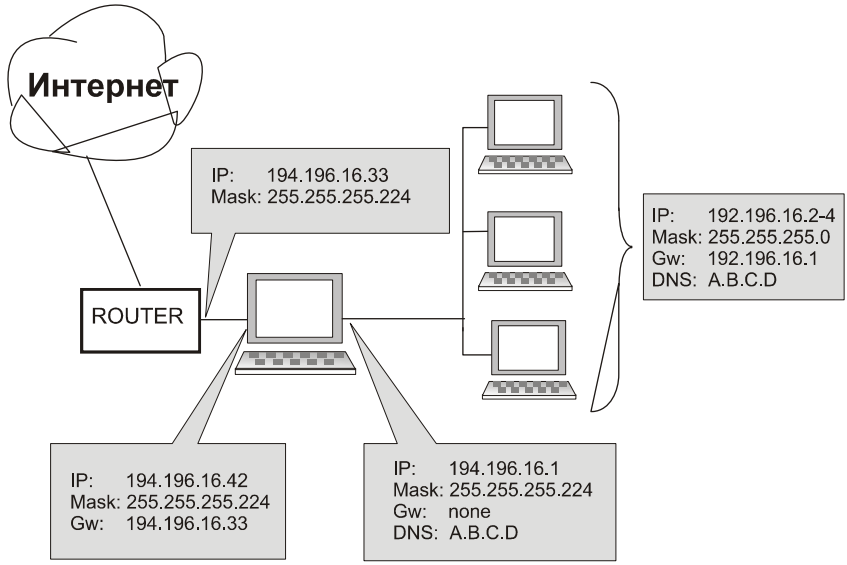


Рис. 3.54. К маршрутизатору подключены два сегмента сети

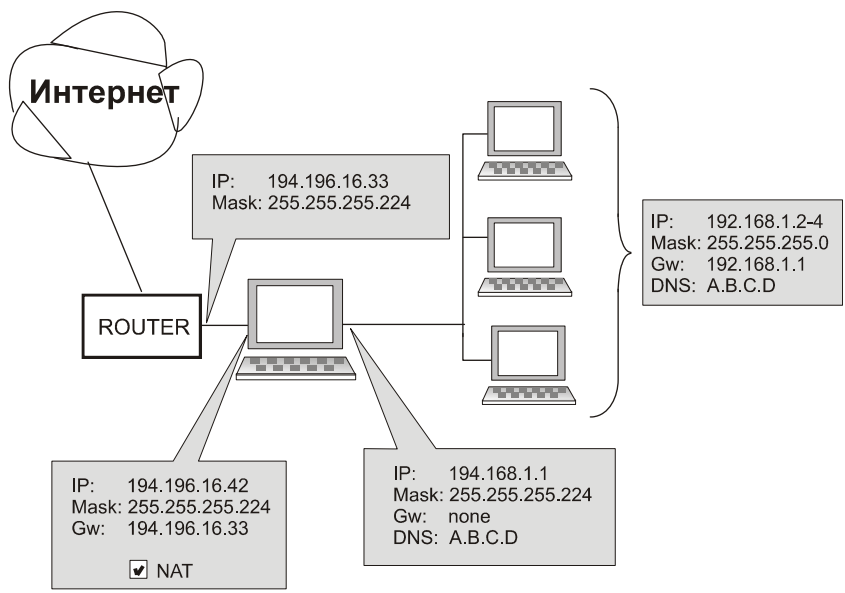


Рис. 3.55. Использование NAT для доступа к Интернету из приватного сегмента

Возможна следующая конфигурация:

- без NAT — сеть продолжает использование зарегистрированного IP-адреса, но поделена на сегменты с маской 255.255.255.224. Маршрутизатор подключен к сегменту 194.196.16.32, тогда как сегмент ЛВС — 194.196.16.0. Компьютер, на котором работает WinRoute, использует две сетевые карты и подключен к обоим сегментам (рис. 3.54);
- с NAT — сеть разделена на два сегмента. Один из них открыт (public), использует зарегистрированные IP-адреса, другой применяет адрес вне приватного блока. Для доступа в Интернет из приватного сегмента используется NAT. Компьютер, на котором работает WinRoute, применяет две сетевые карты и подключен к обоим сегментам (рис. 3.55).

"Горячие" клавиши в WinRoute

При работе в программе WinRoute используются "горячие" клавиши:

- <Ctrl>+<I> — интерфейсы/NAT;
- <Ctrl>+<D> — простой DNS-сервер;
- <Ctrl>+<H> — DHCP-сервер;
- <Ctrl>+<A> — интерфейсы/верификация;
- <Ctrl>+<M> — назначение портов;
- <Ctrl>+<S> — запись настройки на диск.

На сайте **www.winroute.com** в разделе Download можно найти даже русскую версию программы.

С помощью NAT (Network Address Translation) WinRoute преобразовывает вышеупомянутые адреса в "удобоваримые" для Интернета.

Кроме того, WinRoute выполняет следующие полезные функции:

- NAT, Firewall;
- DNS-сервер;
- DHCP-сервер;
- прокси-сервер;
- Mail-сервер.

Для настройки удаленных машин достаточно установить шлюз на адрес компьютера с WinRoute и в DNS прописать ISP (DNS провайдера).

Вот и все, работайте, как будто вы напрямую соединились с Интернетом. WinRoute работает быстрее многих других прокси-серверов, так как весь обмен пакетами реализован на низком уровне.

Пример подключения локальной сети к Интернету показан на рис. 3.56.

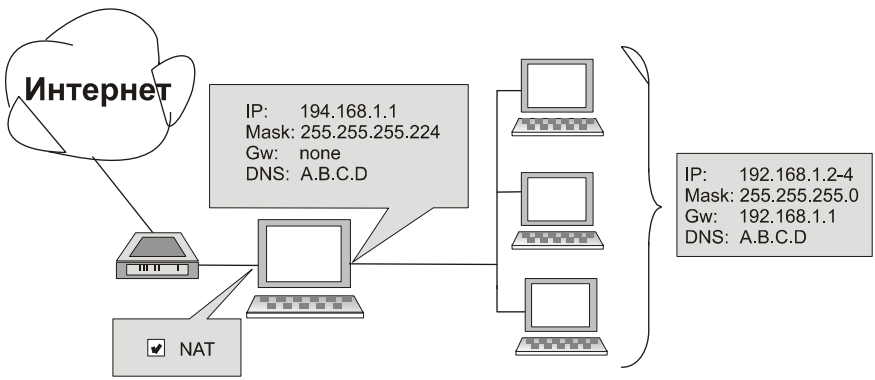


Рис. 3.56. Пример подключения локальной сети к Интернету

Краткий обзор возможностей программы WinRoute Pro 4.1 RU

WinRoute Pro представляет собой уникальный по своим возможностям программный интернет-маршрутизатор и межсетевой экран, позволяющий практически без каких-либо усилий подключить к Интернету все ваши компьютеры, объединенные в локальную сеть, по одному-единственному каналу, будь то обычная телефонная линия, DSL, кабельная связь, ISDN, ЛВС, T1, радиомодем или система DirecPC.

Удаленное администрирование

Настройку конфигурации системы под управлением программы WinRoute обеспечивает управляющая утилита WinRoute Administrator — отдельное приложение (файл wradmin.exe), запускаемое с любого компьютера, подключенного к главной машине, на которой установлено ядро системы WinRoute. Защита доступа к ядру системы обеспечивается мощными средствами криптографии и паролем.

Протоколирование

Программа WinRoute Pro предоставляет сетевым администраторам уникальные возможности контроля сетевого трафика, проходящего через главную машину, на которой установлено ядро программы. Администраторы могут анализировать пакеты TCP, UDP, ICMP и ARP, запросы DNS, сведения о драйверах и многие другие данные. Все операции снабжаются меткой даты/времени.

IP-маршрутизатор NAT

В системе WinRoute применена лучшая в своем классе технология преобразования сетевых адресов (Network Address Translation, NAT), предоставляющая уникальные возможности маршрутизации и сетевой защиты. Драйвер NAT, написанный специально для программы WinRoute, обеспечивает безопасность на уровне, сравнимом с показателями гораздо более дорогостоящей продукции.

Расширенная NAT-маршрутизация

Расширенные возможности преобразования сетевых адресов включают в себя модификацию IP-адреса отправителя исходящих пакетов на основании ряда критериев, что обеспечивает простоту интеграции ЛВС, работающей под управлением WinRoute, с корпоративной территориально распределенной сетью (WAN), ее различными сегментами, демилитаризованными зонами, виртуальными частными сетями и т. п.

Хостинг-серверы под управлением WinRoute

По умолчанию система WinRoute держит все порты закрытыми, обеспечивая тем самым максимальный уровень защиты. Это означает, что если не создана схема распределения портов, то в ответ на все инициируемые запросы направляется отказ. Технология распределения портов предоставляет пользователям право решать самим, куда именно направлять IP-пакеты, проходящие через любой интерфейс, управляемый программой WinRoute. Иными словами, с помощью WinRoute пользователи могут направлять пакеты на тот или иной порт для дальнейшей передачи на конкретный компьютер внутри сети. Таким образом, гарантируется полная безопасность функционирования Web-

сервера, почтового сервера, FTP-сервера, сервера, обслуживающего виртуальную частную сеть, и в целом любого сервера, защищенного межсетевым экраном.

Система межсетевой защиты

Сочетание NAT-архитектуры и способности системы WinRoute функционировать на низком уровне обеспечивает уровень межсетевой защиты, сравнимый с возможностями гораздо более дорогостоящих решений. Способность межсетевого экрана WinRoute перехватывать как входящие, так и исходящие пакеты делает его практически неуязвимым в случае попыток взлома. Наряду с фильтрацией пакетов, средства антиспуфинга предоставляют дополнительный уровень защиты ЛВС от нападения извне с применением фальсифицированного IP-адреса отправителя.

Простота настройки сетевой конфигурации

Система WinRoute Pro включает в себя сервер- DHCP и ретранслятор DNS, обеспечивающие простоту настройки сетевой конфигурации и управления ею. Оба эти компонента представляют собой весьма развитые технологии. Сервер DHCP программного комплекса WinRoute с успехом заменяет аналогичный компонент операционной системы Windows NT.

Почтовый сервер

Исключительно многофункциональный почтовый сервер системы WinRoute, полностью совместимый с протоколами SMTP/POP3, обеспечивает практически неограниченные возможности использования псевдонимов и автоматической сортировки почты. Пользователи могут создать один или несколько почтовых адресов, эффективно работать в составе группы (например, по сбыту, технической поддержке и т. п.), при этом каждая такая группа может включать в себя расширенное число участников. Все эти возможности предоставляются независимо от типа подключения к Интернету.

Кэширование HTTP

В архитектуре WinRoute применен не имеющий аналогов механизм кэширования. В отличие от прокси-серверов, обладающих возможностью кэширова-

ния, этот механизм записывает проходящие через него данные не в отдельный файл для каждого объекта, а в единый файл предустановленного объема, тем самым обеспечивая значительную экономию выделенного под кэш дискового пространства, особенно при использовании 16-разрядной таблицы размещения файлов (FAT16), характерной для большинства версий ОС Windows 95.

Поддержка интернет-протоколов

Программа WinRoute поддерживает все стандартные интернет-протоколы, в том числе: IPsec, H.323, NetMeeting, Net2Phone, WebPhone, UNIX talk, RealAudio, RealVideo, ICA WinFrame, IRC, FTP, HTTP, HTTPS, Telnet, PPTP, Traceroute, Ping, Year 2000 AOL, CHARGEN, CUSeeMe, Daytime, DISCARD, DNS, Echo, Finger, Gopher, IMAP3, IMAP4, IPR, IPX over IP, Netstat, NNTP, NTP, Ping, POP3, RADIUS, WAIS, RCP, Rlogin, RSH, SMTP, SNMP, SSL, SSH, Systat, TACACS, UUCP over IP, WHOIS, XTACACS.

Преобразование сетевых адресов

Одним из самых мощных средств обеспечения безопасности в системе WinRoute служит технология преобразования сетевых адресов (Network Address Translation, сокращенно — NAT). NAT представляет собой предварительный стандарт интернет-протокола, применяемый, чтобы "спрятать" истинные адреса частной сети за одним или несколькими выделенными адресами. Версия технологии NAT, известная как IP Masquerading (Имитация IP-адресов), уже давно завоевала популярность в среде Linux. Система WinRoute стала одним из немногочисленных средств на платформе Windows, обеспечивающих функциональные возможности NAT на базовом уровне.

Сферы применения технологии NAT весьма разнообразны, однако в нашем случае ее главная задача заключается в создании почти неограниченного адресного пространства внутри локальных сетей, которое "преобразуется" программой WinRoute таким образом, что при установке двусторонней связи с общедоступными сетями обеспечивается полная защита информации о чувствительных узлах локальных систем. Поскольку сведения о закрытом адресном пространстве внутреннего интерфейса недоступны, практически невозможно атаковать напрямую тот или иной узел внутренней сети, защищенной технологией NAT.

Как действует технология NAT

Преобразование сетевых адресов (NAT) предполагает видоизменение пакетов, пересылаемых из локальной сети в Интернет или другие сети на базе IP-протокола, а также в обратном направлении.

- Исходящие пакеты.

  Претерпевая преобразование адресов по пути из ЛВС, пакеты видоизменяются таким образом, что выглядят как отправленные компьютером, оснащенным технологией NAT (имеется в виду компьютер, напрямую подключенный к Интернету). Конкретно речь идет о замене IP-адреса отправителя в головной метке пакета (общедоступным) IP-адресом "NAT-компьютера" (рис. 3.57). Одновременно механизм преобразования адресов создает таблицу протоколирования каждого пакета, направляемого в Интернет.

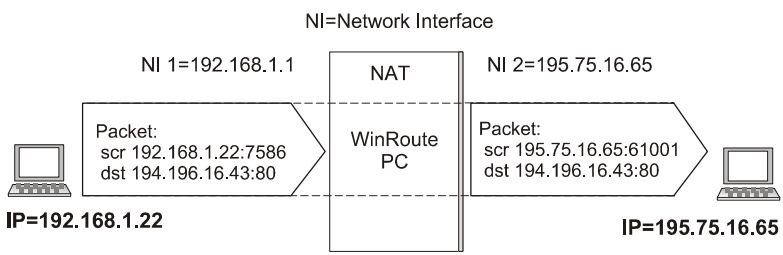


Рис. 3.57. Преобразование исходящих пакетов

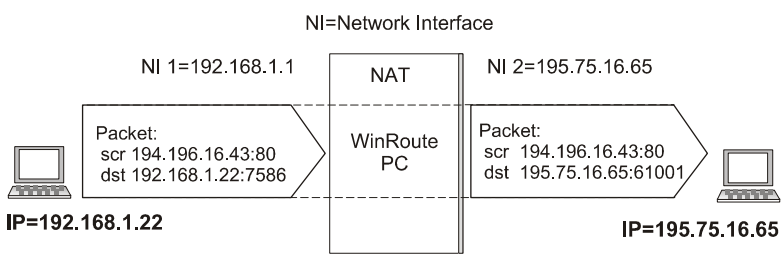


Рис. 3.58. Преобразование входящих пакетов

- Входящие пакеты.

  Попадая в ЛВС, пакеты подвергаются "досмотру" согласно записям, хранимым механизмом NAT. При этом IP-адрес "адресата" снова заменяется (на основании упомянутых записей) на закрытый IP-адрес конкретного компьютера, подключенного к ЛВС. Следует помнить, что входящий па-

кет поступает с указанием открытого IP-адреса NAT-компьютера в качестве "адресата". Следовательно, чтобы доставить пакет верному адресату внутри локальной сети, механизм преобразования адресов должен заменить указанный в оригинале адрес (рис. 3.58).

Архитектура WinRoute

Для освоения расширенных возможностей работы с Интернетом полезно иметь представление о принципах функционирования программного комплекса WinRoute. Из приведенных ниже разъяснений и примеров станет очевидным, что WinRoute представляет собой великолепное решение практически для любых сетевых конфигураций.

Абсолютная защита

WinRoute функционирует ниже TCP-стека, на уровне IPsec. Это означает, что программный комплекс перехватывает как исходящие, так и входящие пакеты *прежде*, чем они попадут в компьютер.

Благодаря столь совершенной архитектуре система безопасности WinRoute становится практически *неуязвимой*.

Полная поддержка протоколов

Будучи программным маршрутизатором, WinRoute работает практически с любыми интернет-протоколами, в отличие от таких прокси-серверов, как WinGate или WinProxy. В то же время программный комплекс WinRoute проверяет все без исключения пакеты с использованием самых совершенных средств обеспечения безопасности и межсетевой защиты. В системах, работающих под управлением Windows 95/98, WinRoute берет на себя функции маршрутизации пакетов. В оборудовании под управлением Windows NT маршрутизацию выполняет сама операционная система, тогда как WinRoute обеспечивает преобразование сетевых адресов (NAT) и обработку других данных.

Предельная гибкость

Преобразование сетевых адресов (NAT) выполняется в избранных вами интерфейсах программы WinRoute. Точно так же она выполнит в указанных

вами интерфейсах предустановленные правила обеспечения защиты. Иными словами, пользователь обладает самыми широкими возможностями по установке и настройке параметров безопасности.

Установка NAT в обоих интерфейсах

Программный комплекс WinRoute можно использовать только как *нейтральный маршрутизатор* потока (пакетов) данных, поступающих из Интернета в *локальную сеть*. Если имеющееся у вас решение по организации коллективного доступа в Интернет не позволяет эксплуатировать внутри частной сети серверы и приложения, к которым необходимо обеспечить доступ из Интернета, тогда установка системы WinRoute в этой конкретной конфигурации может стать единственно верным решением.

Вот некоторые сетевые сервисы, к которым вам может понадобиться доступ из Интернета:

- Telnet-сервер (например, AS400);
- Web-сервер;
- почтовый сервер;
- PcAnywhere;
- FTP-сервер;
- другие серверы (сервисы), доступ к которым обеспечивается через определенный порт.

Система WinRoute предоставит вашим пользователям и клиентам надежный, защищенный доступ к таким сетевым службам. Описание соответствующих настроек конфигурации WinRoute приводится в последующих главах. Различия в настройках показаны в табл. 3.6.

Таблица 3.6. *Отличия в настройках WinRoute для случая нейтрального маршрутизатора*

Набор функций	Рекомендуемая настройка	В данном сценарии
NAT в интерфейсе Интернета	ВКЛ.	ВКЛ.
NAT во внутреннем (ЛВС) интерфейсе	ВЫКЛ.	ВКЛ.

Таблица 3.6 *(окончание)*

Набор функций	Рекомендуемая настройка	В данном сценарии
IP-адрес внутреннего интерфейса WinRoute как шлюз по умолчанию для других компьютеров внутри сети	ДА (ОБЯЗАТЕЛЬНО)	НЕТ (не нужно)

Иными словами, WinRoute позволяет открыть к определенным службам доступ из Интернета без изменения сетевой конфигурации.

> ***ПРИМЕЧАНИЕ***
>
> Установка NAT в обоих интерфейсах не позволяет использовать WinRoute как средство коллективного доступа в Интернет!

Приведенные в этом примере настройки шлюза по умолчанию предоставляют вам колоссальную свободу действий без необходимости внесения каких-либо изменений в настройки вашей сетевой инфраструктуры. Чтобы предоставить внешним пользователям доступ к серверам внутри вашей локальной сети, сохранив в неприкосновенности уже имеющиеся маршрутизаторы и маршруты, достаточно подключить новые компьютеры с установленной на них программой WinRoute.

Эта возможность представляется весьма полезной, если (к примеру) у вас уже есть территориально распределенная сеть (WAN), и вы хотите предоставить внешним пользователям доступ к вашему Telnet-серверу AS400, либо получить доступ к закрытой внутренней сети по протоколу PPTP.

Для этого необходимо выполнить следующие действия:

1. Подключите к вашей сети компьютер с двумя интерфейсами, один из которых (внешний) обеспечивает доступ в Интернет, а второй (внутренний) — к имеющейся у вас сети.
2. Назначьте внешнему интерфейсу IP-адрес, который будет использоваться для подключения к службам/серверам, доступным из Интернета.
3. Назначьте внутренний IP-адрес либо вручную, либо с помощью сервера DHCP.

4. Настройте WinRoute на преобразование сетевых адресов (NAT) в обоих интерфейсах.
5. Настройте распределение портов для сервисов, работающих внутри вашей сети.

После того как эти настройки будут выполнены, внешние пользователи получат из Интернета доступ к вашим внутренним сетевым сервисам по выделенным портам. Безопасность такого доступа гарантирует межсетевой экран WinRoute.

Распределение портов и переадресация пакетов

Механизм преобразования сетевых адресов (NAT) блокирует доступ извне к сети, защищенной системой WinRoute. В свою очередь, механизм распределения портов (или PAT — Port Address Translation, преобразование адресов портов) может блокировать доступ из Интернета к таким общедоступным сервисам внутри вашей частной сети, как, например, Web-сервер, FTP-сервер и т. д.

Как действует механизм распределения портов

На рис. 3.59 наглядно показан механизм распределения портов. Все пакеты, поступающие извне (в том числе из Интернета), проверяются на предмет соответствия их атрибутов (т. е. протокола, порта и IP-адреса адресата) настройкам таблицы распределения портов (протокол, прослушивание порта, ожидание сигнала по IP). Если входящий пакет отвечает необходимым критериям, то он, подвергшись модификации, направляется на IP-адрес защищенной сети, указанный в настройках таблицы как "IP адресата", и на порт, указанный как "порт адресата".

Например, вы хотите предоставить пользователям из Интернета доступ к Web-серверу, работающему по внутреннему IP-адресу 192.168.1.3. На компьютер, работающий под управлением программы WinRoute, поступают запросы пользователей из Интернета на подключение к внешнему IP-адресу, соответствующему DNS-адресу вашего Web-сервера **www.yourdomain.com**. Поскольку все такие запросы поступают на порт 80, механизм распределения портов необходимо настроить таким образом, чтобы любое подключение по TCP к порту 80 перенаправлялось на внутренний IP-адрес 192.168.1.3.

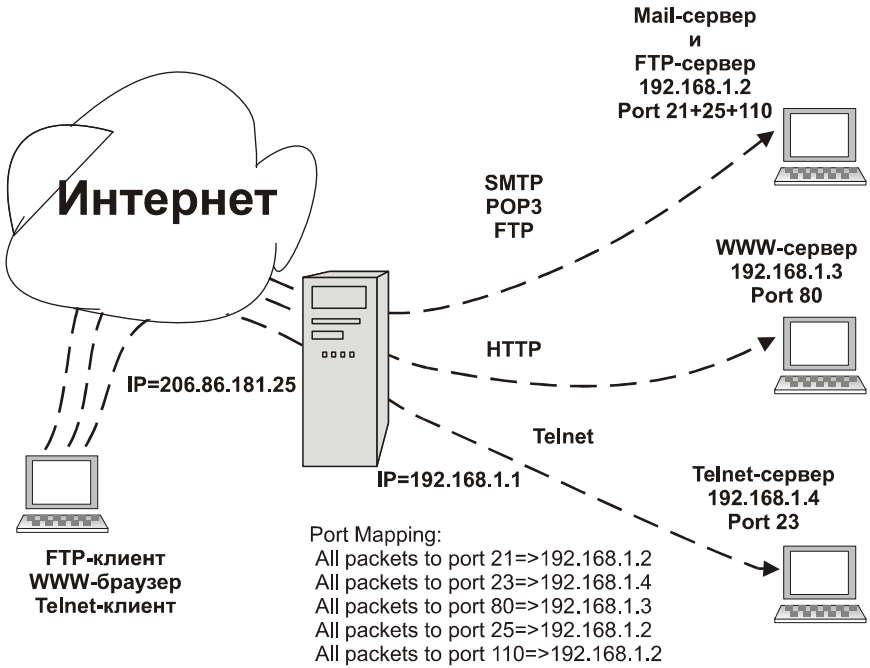


Рис. 3.59. Распределение портов

Настройка механизма распределения портов

Чтобы настроить механизм распределения портов, войдите в меню **Setting | Advansed | Port Mapping** (Настройки | Дополнительно | Распределение портов) (рис. 3.60) и введите новую настройку распределения порта.

- **Protocol** (Протокол).

  Введите протокол, используемый приложением или сетевым сервисом. Некоторые приложения и сервисы, например модуль управления программой WinRoute, используют одновременно протоколы TCP и UDP.

- **Listen IP** (Ожидание сигнала по IP).

  Речь идет об IP-адресе, на который поступают входящие пакеты. Как правило, это IP-адрес, соответствующий вашему интернет-интерфейсу.

> ***Примечание***
>
> Этому интерфейсу могут соответствовать несколько IP-адресов (например, если у вас несколько Web-серверов).

- **Listen Port** (Прослушивание порта).

  Имеется в виду порт, на который поступают пакеты.

- **Destination IP** (IP-адресат).

  IP-адрес внутри вашей локальной сети, по которому работает сервер (или сервис), отвечающий на входящие пакеты (Web-сервер, FTP-сервер и т. п.).

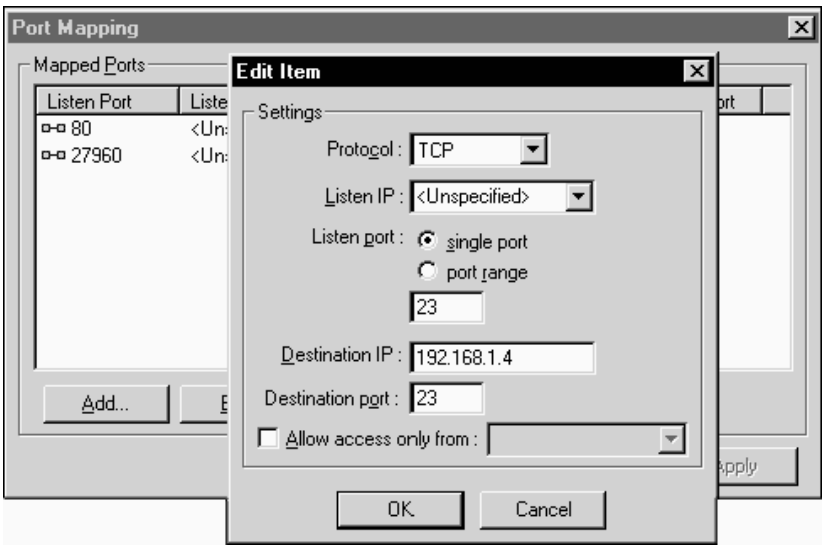


Рис. 3.60. Настройка распределения портов

- **Destination port** (Порт адресата).

  Порт, прослушиваемый приложением, для которого предназначается входящий пакет. Его номер, как правило, совпадает с номером порта, который вводится в графу **Прослушивание порта**.

- **Allow access only from** (Доступ только из).

  Здесь указывается конкретный IP-адрес, с которого разрешен доступ, что крайне важно для обеспечения повышенного уровня безопасности в том случае, если вы хотите предоставить доступ к механизму распределения портов таким приложениям удаленного администрирования, как утилита WinRoute Administrator, pcAnywhere и т. п. Можно указать и группу IP-адресов. Для этого ее нужно создать с помощью диалогового окна **Address Groups** (Группы адресов).

❒ **NAT...** (Мульти-NAT).

Наряду с простым преобразованием сетевых адресов (NAT), программа WinRoute обладает и более изощренными возможностями. Так, например, механизм NAT можно настроить таким образом, чтобы он в зависимости от IP-адреса отправителя или адресата пакета присваивал ему дополнительные IP-адреса (т. е. пакет будет выглядеть как исходящий из другого IP-адреса), либо отказаться от NAT вообще (рис. 3.61).

Такие расширенные возможности крайне важны для сложной сетевой среды, в которой:

- IP-адреса определенных компьютеров должны выглядеть как отличные от основного адреса, используемого остальными узлами сети;
- имеются подключенные к глобальной сети подразделения корпоративной структуры, обладающие закрытым адресным пространством, при этом требуется обеспечить им единый доступ в Интернет;
- под управлением WinRoute работает несколько сегментов сети, из которых один (или более) служит "демилитаризованной зоной" с общедоступными IP-адресами;
- внутри частной сети необходимо иметь общедоступные IP-адреса.

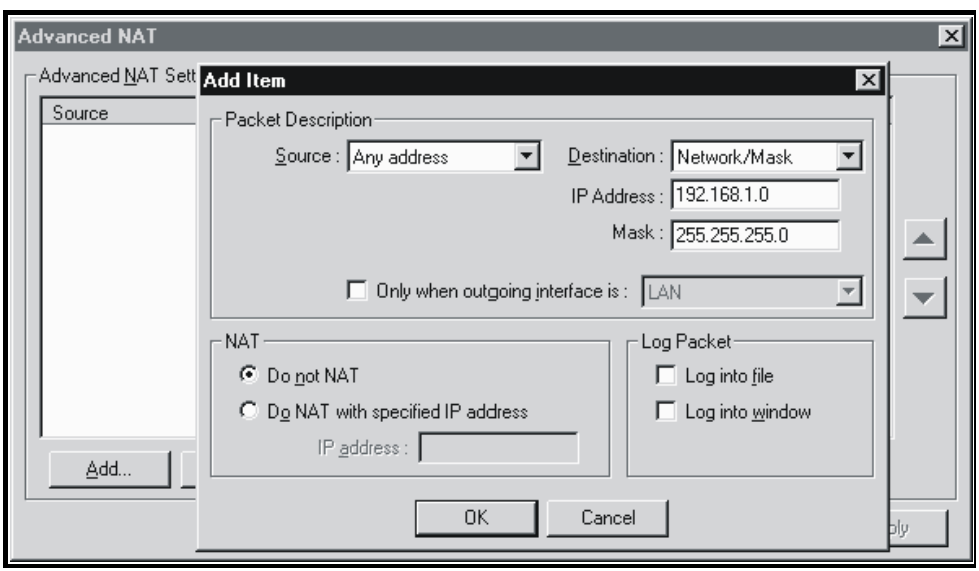


Рис. 3.61. Дополнительные настройки NAT

ВНИМАНИЕ!

Необходимо согласовать с вашим интернет-провайдером маршрутизацию таких IP-адресов через ваш основной адрес.

- **IP Address** (IP-адрес).

  Дополнительные настройки NAT выполняются на основе IP-адреса источника (отправитель) или получателя (адресат) пакетов данных. В качестве отправителя можно ввести IP-адрес главного узла, всей сети (эта возможность ограничена сетевой маской), либо группу IP-адресов, предварительно созданную в меню **Setting | Advansed | Address Groups Setting** (Настройки | Дополнительно | Группы адресов).

- **Do not NAT** (Не преобразовывать).

  Если эта опция отмечена, то в пакеты, проходящие через интернет-интерфейс, изменения не вносятся.

- **Do NAT with specified IP address** (Преобразовывать по указанному адресу).

  Если эта опция отмечена, то модификации подвергаются только пакеты, исходящие из указанных IP-адресов.

- **Interface Table** (Таблица интерфейсов).

  Таблицей интерфейсов называется диалоговое окно, в котором отображены все интерфейсы компьютера, распознаваемые программой WinRoute. Если в этом диалоговом окне отображены не все установленные интерфейсы, скорее всего, драйвер отсутствующего интерфейса (или интерфейсов) не загружен операционной системой надлежащим образом, вследствие чего WinRoute его не может распознать.

- **Interface** (Название интерфейса).

  Его можно изменить, войдя в меню **Свойства**.

- **IP address** (IP-адрес).

  Значение этого параметра задается в меню TCP/IP-свойств интерфейса. Если интерфейс настроен на получение IP-адреса от сервера DHCP, в окне выводится истинный IP-адрес, назначенный интерфейсу.

- **NAT "on"** или **"off"** (NAT "вкл." или "выкл.").

  Если на экран выведено значение "вкл.", значит, механизм преобразования сетевых адресов по данному интерфейсу активизирован.

Поддержка виртуальных частных сетей (VPN)

Как уже отмечалось, программный комплекс WinRoute полностью совместим с двумя наиболее популярными сегодня VPN-протоколами: IP Security protocol (IPSec), предложенным Комитетом по инженерным проблемам Интернета (IETF), и Point-to-Point Tunneling protocol (PPTP), завоевавшим в последние годы популярность в результате включения его в клиентскую операционную систему Microsoft Windows.

Как фильтруются пакеты

Краеугольным камнем всякого механизма контроля доступа через межсетевой экран является, конечно же, технология, разрешающая либо запрещающая входящим пакетам данных доступ к защищенным сетям. В программном комплексе WinRoute применена одна из наиболее распространенных технологий контроля доступа к сетям — фильтрация пакетов. Хотя система WinRoute оснащена и другими механизмами контроля доступа, в частности встроенным кэширующим прокси-сервером для протоколов HTTP, FTP и Gopher, основное назначение таких средств — повышение быстродействия исходящего трафика, а не обеспечение безопасности.

Технология фильтрации пакетов, издавна применяемая специалистами по обеспечению защиты сетей, широко используется и по сей день в таких сетевых продуктах, как, например, разработанная компанией Cisco интегрированная операционная система IOS для сетевых устройств. При надлежащей настройке конфигурации механизм фильтрации пакетов обеспечивает весьма высокий уровень безопасности, пригодный для высокопроизводительных интернет-узлов, которые помимо всего прочего выигрывают и в быстродействии.

Защита от вторжений из Интернета

Как правило, межсетевые экраны устанавливаются на платформах, оснащенных усиленными средствами защиты, программное обеспечение которых уже само по себе малоуязвимо. Однако самым слабым местом многих устройств защиты сетей является тот короткий промежуток времени, когда аппаратные средства уже полностью инициализированы и способны обеспечивать эффективную маршрутизацию сетевого трафика, а программная часть еще не успела взять под свой полный контроль сетевые интерфейсы. Вот в этом кри-

тическом промежуточном состоянии и таится опасность взлома сетевой защиты.

Драйвер WinRoute (называемый Engine, или механизм) активизируется в тот момент, когда файлы ядра (kernel) операционной системы Windows загружаются в память. Другими словами, механизм загружается раньше модулей NDIS (Network Device Interface Specification — спецификация интерфейса сетевых устройств), благодаря чему сетевое подключение просто не поддерживается до момента полной активизации WinRoute. Таким образом, все интерфейсы оказываются полностью защищенными, прежде чем в систему могут попасть какие-либо зловредные данные либо она иным образом подвергнется атаке. Такая схема обладает очевидными преимуществами перед автономными средствами обнаружения признаков вторжения, которые являются, по сути дела, сетевым сервисом, а следовательно, не могут быть активизированы до того момента, как система полностью загрузится.

Особая технология, примененная в программном комплексе WinRoute, "обволакивает" модули NDIS таким образом, что весь TCP/IP-трафик перенаправляется от сетевого адаптера (network interface card, сокращенно NIC) к механизму WinRoute, прежде чем он достигнет сетевого коммуникационного стека и далее — операционной системы.

Благодаря такому "вмешательству" в работу операционной системы на низком уровне механизм WinRoute контролирует весь сетевой трафик (как входящий, так и исходящий), прежде чем он достигнет любого интерфейса. Как и многие межсетевые экраны уровня предприятия (например, Firewall-1 компании Check Point), WinRoute обладает полномочиями приоритетного решения относительно того, принять или отвергнуть тот или иной пакет. Отметим еще раз, что такая схема обеспечивает предотвращение атак на операционную систему или любое другое программное обеспечение, даже если нарушителю удается обойти межсетевой экран. Безусловно, это крайне важно для интернет-шлюзов, обеспечивающих доступ извне, однако и автономные узлы, нуждающиеся в высокой степени безопасности или анонимности, получают неоспоримые преимущества, в частности в отношении применения систем обнаружения вторжения. На узле, защищенном WinRoute, такие программные средства обнаружения вторжения, как, например, система Real Secure компании Internet Security Systems (ISS), становятся практически невидимыми.

Отметим, что механизм WinRoute берет на себя все функции операционной системы Windows (будь то Windows 9*x*, NT или 2000) по маршрутизации лю-

бых коммуникационных средств. Благодаря этому в случае сбоя, произошедшего по той или иной причине в механизме WinRoute, весь межсетевой трафик гарантированно блокируется. Такой способ "блокировки по сбою", который традиционно применяется по умолчанию в самых разнообразных конфигурациях межсетевых экранов на протяжении многих лет, обеспечивает защиту закрытых сетей от наиболее распространенных системных сбоев.

Антиспуфинг

Наряду с вышеперечисленным, программный комплекс WinRoute обладает возможностями антиспуфинга, т. е. блокирования выхода за пределы сети пакетов с неправильным адресом отправителя. Если бы такие крупнейшие Web-узлы, как Yahoo! и Buy.com, были оснащены средствами антиспуфинга, то они не подверглись бы нашумевшим в феврале 2000 года атакам с применением технологии распределенного отказа в обслуживании. Пользователи комплекса WinRoute, в котором активизированы средства антиспуфинга, могут быть уверенными в том, что их сети никогда не станут источником таких атак.

Для чего нужен прокси-сервер?

Главным предназначением прокси-сервера является экономия пропускной способности канала подключения к Интернету. Когда пользователи подключаются к Интернету через прокси-сервер, то он сохраняет различные запрашиваемые объекты (страницы HTML, изображения, разного рода файлы) в своей кэш-памяти.

Если уже просмотренные страницы или изображения запрашиваются повторно тем же или другим пользователем, прокси-сервер извлекает их из своей кэш-памяти, снижая таким образом нагрузку на канал подключения к Интернету и одновременно значительно ускоряя повторную загрузку файлов, в особенности графических.

При этом нужно учесть, что объекты, сохраненные в кэш-памяти прокси-сервера, имеют свойство устаревать. Отсюда следует необходимость тщательно продумать значение параметра TTL (Time-to-Live, время жизни), сохраненного в кэше документов во избежание таких конфузов, как, например, предоставление к услугам пользователей последних известий за вчерашнее число.

Быстрая настройка

Прежде всего необходимо отметить, что применение программного комплекса WinRoute избавляет от необходимости использовать прокси-сервер для обеспечения доступа в Интернет, поскольку эти функции берет на себя NAT-маршрутизатор, встроенный в WinRoute, а технология NAT обеспечивает коллективное подключение к Интернету гораздо эффективнее, нежели прокси-сервер. Тем не менее в программный комплекс WinRoute встроен и прокси-сервер, обеспечивающий, при необходимости, расширенные функции кэширования.

Установка прокси-сервера программного комплекса WinRoute осуществляется предельно просто.

1. Из меню **WinRoute Administration** (Управление программой WinRoute) последовательно войдите в подменю **Setting | Proxy Server | General** (Настройки | Настройки прокси | Общие настройки) — рис. 3.62. Проверьте, активизирован ли параметр **Proxy Server Enabled** (Включить прокси-сервер). Номер порта (3128) оставьте без изменений.

Рис. 3.62. Общие настройки прокси-сервера

2. Откройте в вашем интернет-браузере MS Internet Explorer (Netscape Navigator, Opera и др.) меню настроек прокси-сервера, выберите настройку вручную, введите адрес головной машины WinRoute в качестве адреса прокси-сервера для протоколов HTTP, FTP и Gopher. Введите номер порта прокси-сервера `3128` для всех протоколов.
3. Проверьте функционирование настроек, загрузив в браузер любые Web-страницы.

Вкладка *General*

На вкладке **General** находятся следующие параметры:

- **Proxy Server Enabled** (Включить прокси-сервер).

  Используется для включения и отключения прокси-сервера;

- **Proxy port** (Номер порта).

  Это порт, через который в прокси-сервер поступают запросы. Как правило, нет необходимости менять установленный по умолчанию номер 3128;

- **Log access to proxy server** (Вести журнал доступа к прокси-серверу).

  Когда этот параметр активизирован, все URL, запрашиваемые браузерами у прокси-сервера, заносятся в протокол.

Контроль доступа пользователей в Интернет

Прокси-сервер программного комплекса WinRoute предоставляет администраторам возможность контролировать доступ к Web-узлам, позволяя запретить определенным пользователям и/или представителям возрастных групп доступ к отдельным Web-страницам или доменам.

Как побудить пользователей подключиться к прокси-серверу

Чтобы контролировать доступ в Интернет, прямой доступ необходимо заблокировать, чтобы у пользователей просто не было возможности просматривать Web-страницы иначе, как через прокси-сервер. Заблокировать прямой доступ можно путем активизации соответствующего правила фильтрации пакетов.

Настройка контроля доступа через прокси-сервер. Чтобы настроить конфигурацию контроля доступа через прокси-сервер программного комплекса WinRoute, откройте вкладку **Access** (Доступ) (рис. 3.63) меню настроек прокси-сервера.

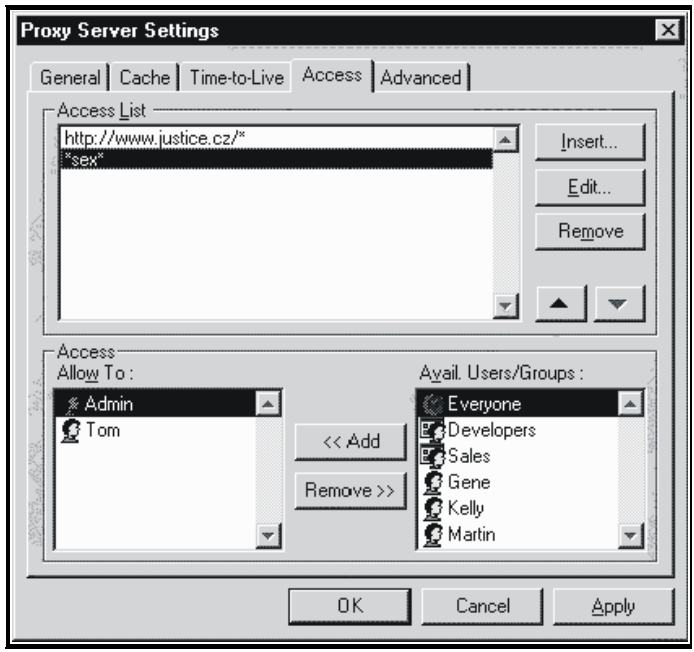


Рис. 3.63. Добавление пользователей в настройках прокси-сервера

- **Access List.** В списке перечисляются URL, доступ к которым ограничен. В качестве группового символа используйте значок `*`. Например, строка `*.somedomain.com` обозначает все компьютеры в домене **somedomain.com**.
- **Access.** Здесь перечисляются пользователи и/или группы пользователей, которым предоставлен доступ к тому или иному URL.
- **Avail. Users/Groups.** Список пользователей или групп, зарегистрированных программным комплексом WinRoute.

Пользователю, который обращается к Web-странице, входящей в список ограниченного доступа, браузер предложит пройти процедуру аутентификации. WinRoute произведет проверку подлинности идентификатора и пароля, а также права данного пользователя на доступ к соответствующей Web-странице.

Поскольку идентификатор и пароль пользователя сохраняются в памяти браузера, все дальнейшие запросы на аутентификацию удовлетворяются автоматически. Таким образом, пользователь избавлен от необходимости всякий раз вводить свой идентификатор и пароль.

Об этом необходимо ставить пользователей в известность. Если к компьютеру имеют доступ несколько пользователей, то по завершении интернет-сеанса им следует удалять свои опознавательные данные из памяти компьютера, закрывая браузер.

Дополнительные возможности. На вкладке **Advanced** (Дополнительно) окна настроек прокси-сервера можно настроить программный комплекс WinRoute на использование исходного прокси-сервера (рис. 3.64).

Рис. 3.64. Установка порта прокси-сервера

Иногда необходимо получить доступ к прокси-серверу, обладающему значительно большей емкостью кэш-памяти или подключенному к Интернету по быстрому каналу. При этом ваш собственный канал связи с этим сервером также будет сравнительно быстрым, например благодаря наличию вспомогательного канала в дополнение к основному.

В этом случае можно ускорить обмен данными, настроив прокси-сервер WinRoute на переадресацию запросов более мощному прокси-серверу, именуемому *исходным*. Для этого достаточно ввести имя и номер исходного прокси-сервера (**Parent proxy**) в соответствующие поля вкладки **Advanced** (Дополнительно).

Как происходит кэширование

В прокси-сервере программного комплекса WinRoute применяется чрезвычайно экономичный способ хранения данных: все кэшируемые объекты за-

писываются в единый файл фиксированного размера. Обычные прокси-серверы, как правило, сохраняют каждый объект в отдельном файле.

Если диск разбит на крупные блоки размещения (как, например, в FAT16), второй способ приводит к значительным потерям дискового пространства, поскольку большинство компонентов Web-страниц имеют небольшой размер. Как правило, 50% таких объектов не превышают 6 Кбайт, тогда как размер каждого блока размещения объемных дисков — 32 Кбайт (при использовании системы FAT).

Запись всех кэшируемых объектов в единый файл позволяет сэкономить колоссальный объем дискового пространства, потребление которого, по сравнению с традиционным подходом, снижается раз в десять. Иными словами, вы сможете сократить емкость своих дисковых массивов либо более эффективно использовать освободившийся объем.

Кроме того, единый файл фиксированного размера позволяет применить чрезвычайно действенную технологию индексации и, соответственно, значительно ускорить процесс кэширования в программном комплексе WinRoute.

Настройка кэширования

Кэширование можно настроить, открыв вкладку **Cache** (Кэширование) (рис. 3.65).

- **Cache Enabled** (Включить кэширование).

  Включение и отключение кэширования. При отключенном кэшировании Web-страницы всегда загружаются непосредственно из Интернета.

- **Cache directory** (Каталог кэширования).

  Каталог, где будут храниться кэшированные данные.

- **Cache size** (Размер кэша).

  Дисковое пространство, выделенное для данных, кэшируемых прокси-сервером. Размер кэша устанавливается с учетом количества пользователей, объема трафика на каждого из них и других факторов. Чем больше у вас дискового пространства, тем больший его объем вы можете выделить для кэша. Максимальный размер кэша составляет 3072 Мбайт (3 Гбайт).

- **Continue Aborted** (Продолжить после прерывания).

  Если этот пункт активизирован, прокси-сервер будет всегда скачивать объекты полностью даже в том случае, если пользовательский браузер от-

менит запрос (т. е. если пользователь нажмет кнопку **Stop** (Остановить) или перейдет по ссылке на другую страницу, не дожидаясь завершения загрузки текущей страницы). Это значительно ускорит повторную загрузку той же страницы в дальнейшем.

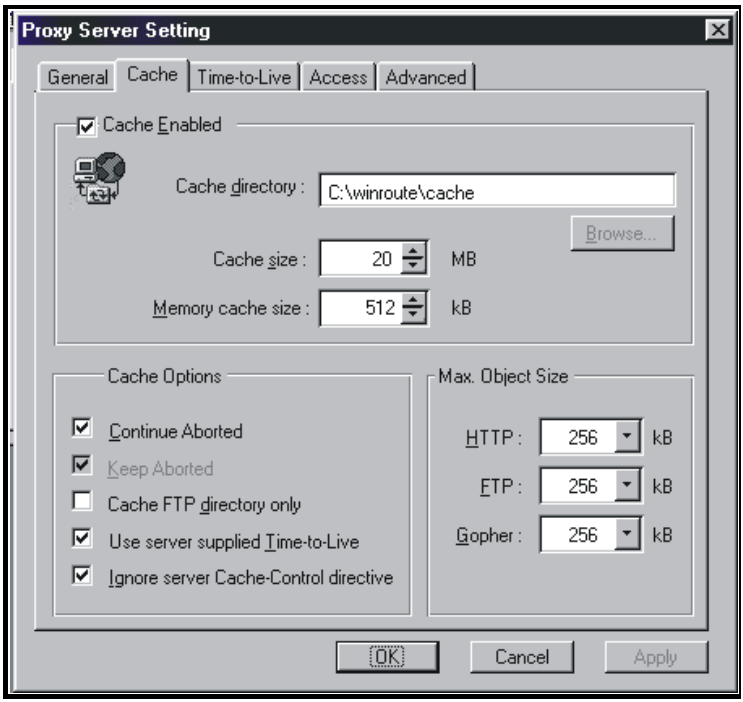


Рис. 3.65. Установка режимов кэширования

- **Keep Aborted** (Прекратить после прерывания).

  В этом случае прокси-сервер WinRoute доводит до конца кэширование только уже загружаемых объектов (Web-страницы или изображений), тем самым хотя бы частично ускоряя загрузку страницы при ее повторном посещении. При активизированном параметре **Continue Aborted** настройка **Keep Aborted** игнорируется.

- **Cache FTP directory only** (Кэшировать только FTP-каталог).

  Этот параметр следует активизировать, чтобы при просмотре FTP-серверов кэшировались только перечни объектов, находящихся в том или ином каталоге. Если вы хотите кэшировать и файлы, загружаемые с FTP-

серверов, отключите этот параметр. Решение о кэшировании того или иного файла зависит и от его размера.

- **Use server supplied Time-to-Live** (Время существования по сигналу сервера).

  Время жизни (Time-to-Live) — это тот отрезок времени, по истечении которого кэшированная Web-страница считается устаревшей, и ее содержание может быть удалено из кэша. Активизация этого параметра означает, что прокси-сервер должен соблюдать то значение TTL, которое указано на самой странице. Если оно не указано, применяется TTL по умолчанию.

- **Ignore server Cache-Control directive** (Игнорировать кэш-контроль сервера).

  Если содержание Web-страницы подвержено частым изменениям, ее автор может ввести команду **не кэшировать**. Такая возможность представляется весьма полезной, однако иногда авторы Web-сайтов ею злоупотребляют, что делает прокси-серверы практически бесполезными. Если вы хотите защитить себя от подобных злоупотреблений, активизируйте этот параметр.

- **Memory cache size** (Максимальный размер объекта).

  Обозначение максимального размера объекта, который можно сохранить в кэш-памяти. Объекты, превышающие это ограничение, загружаются браузером пользователя и не будут записываться в кэш. Как правило, необходимости в кэшировании крупных объектов (например, архивированных программных файлов) нет, ибо повторно их не загружают.

Значение времени жизни (Time-to-Live, TTL) по умолчанию следует вводить (рис. 3.66) на вкладке **Time-to-Live** (Время жизни), если оно на страницах не указывается или если вы решили игнорировать TTL, указанное удаленным сервером (см. параметр **Use server supplied Time-to-Live** (Время существования по сигналу сервера) на вкладке **Cache** (Кэширование)).

- **Protocol Specific Settings** (Особые настройки по протоколам).

  Здесь можно указать время существования в днях по умолчанию для протоколов HTTP, FTP и Gopher.

- **URL Specific Settings** (Особые настройки по URL).

  При необходимости настроить время существования для конкретных доменов, Web-серверов или отдельных страниц введите здесь соответствующие URL. TTL можно указывать в днях и/или часах.

  В качестве группового символа URL используйте значок `*`. Кроме того, в WinRoute 4.0 применяется подстрочное обозначение URL, иными сло-

вами, можно ввести просто `ftp` для обозначения всех серверов, в именах которых присутствует "ftp". (В предыдущих версиях WinRoute такая возможность отсутствовала.)

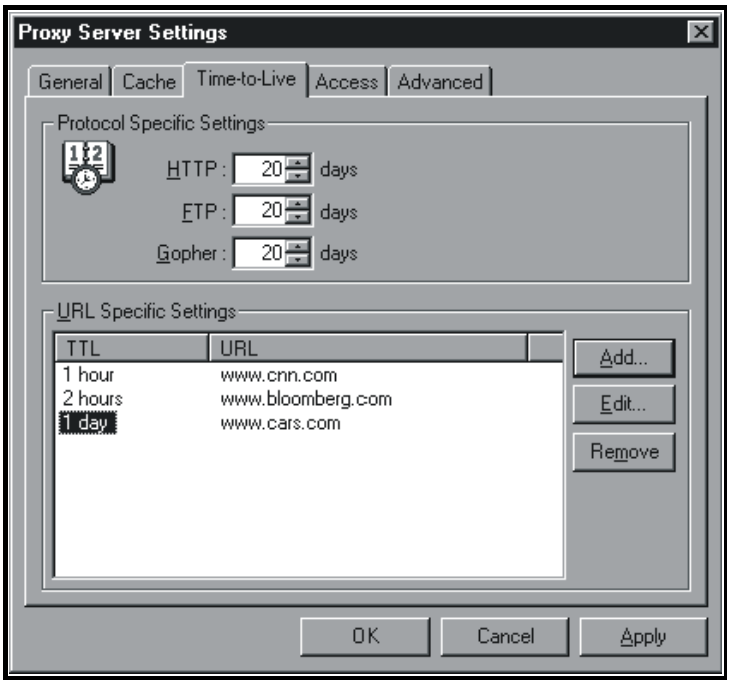


Рис. 3.66. Настройка времени жизни

Имейте в виду, что активизация параметра **Use server supplied Time-to-Live** (Время существования по сигналу сервера) на вкладке **Cache** (Кэширование) предоставляет TTL, указанному удаленным сервером, приоритет по сравнению с параметром **URL Specific Settings** (Особые настройки по URL).

Почтовый сервер WinRoute

В программный комплекс WinRoute встроен полнофункциональный почтовый сервер, поддерживающий протоколы SMTP/POP3. Пользоваться им можно точно так же, как и обычным почтовым сервером интернет-провайдера. Почтовый сервер WinRoute позволяет отправлять корреспонденцию как через Интернет, так и локальным пользователям внутри ЛВС. Кроме

того, он обеспечивает прием и сохранение электронных сообщений в почтовых ящиках пользователей системы WinRoute. Но и это еще не все: встроенный в WinRoute планировщик дает возможность обмениваться электронной почтой по заранее составленному вами графику.

Если вы не пользуетесь почтовым сервером

Пользоваться почтовым сервером WinRoute отнюдь не обязательно: вы можете, как и прежде, продолжать использовать почтовый сервер своего провайдера или какой-либо другой. В этом случае WinRoute действует просто как маршрутизатор и межсетевой экран, обеспечивающий связь вашей клиентской программы электронной почты с почтовым сервером провайдера.

> ***ВНИМАНИЕ!***
>
> Не настраивайте вашу клиентскую программу электронной почты на работу через прокси-сервер! Подключаться к Интернету необходимо через NAT. Кроме того, настройте ваше почтовое программное обеспечение на прямой выход в Интернет. Если вам не удается наладить обмен почтой, значит, конфигурация NAT настроена неправильно. Чтобы настроить ее надлежащим образом, см. *разд. "Краткий контрольный перечень параметров" данной главы.*

Учетные записи пользователей WinRoute

Учетные записи пользователей программного комплекса WinRoute можно запрограммировать как в индивидуальном, так и в групповом порядке (программирование осуществляется из меню **Setting | User Accounts** (Настройки | Учетные записи), вкладка **Users** (Пользователи)). Данные пользователей, зарегистрированных в Windows NT/2000, импортируются с помощью вкладки **Advanced** (Дополнительно) в меню **Setting | User Accounts** (Настройки | Учетные записи).

Полномочия пользователей

Пользователи программного комплекса WinRoute могут участвовать в управлении системой WinRoute, открывать почтовые ящики, участвовать в выработке правил ограничения доступа через прокси-сервер WinRoute.

Кроме того, пользователи вправе образовывать группы и применять к ним вышеупомянутые привилегии и ограничения.

Регистрация нового пользователя

Чтобы зарегистрировать нового пользователя (рис. 3.67), выполните следующие действия:

1. В меню **Setting** (Настройки) выберите команду **User Accounts** (Учетные записи).
2. Нажмите кнопку **Add** (Добавить).
3. Введите имя пользователя и пароль.

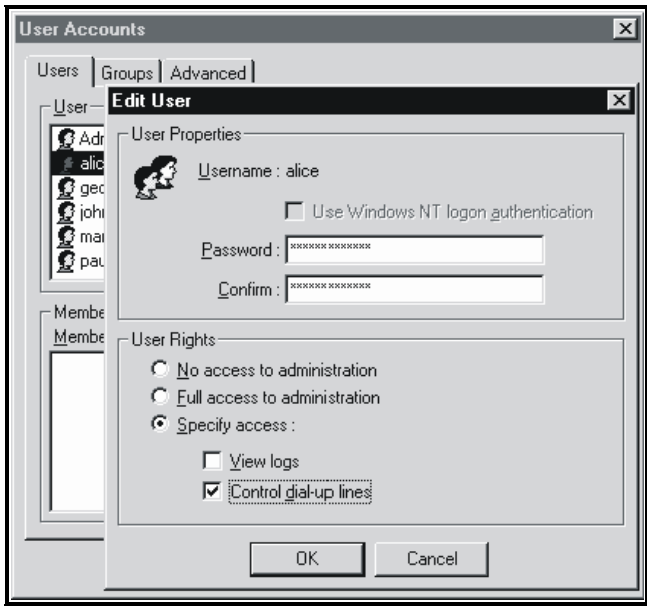


Рис. 3.67. Регистрация пользователя

4. Определите полномочия пользователя:
   - **No access to administration** — пользователь не обладает полномочиями на управление программным комплексом WinRoute;
   - **Full access to administration** — пользователь обладает неограниченными полномочиями на управление программным комплексом WinRoute;

- **View logs** — просмотр журналов. Данный пользователь обладает правом подключения к программе управления WinRoute только для просмотра содержания журналов (сведения по отладке, журнал прокси-сервера, почтовый журнал и т. п.) на экране. Права на изменение настроек данный пользователь не имеет;
- **Control dial-up lines** — контроль линий с вызовом по номеру. Данный пользователь вправе подключаться к программе управления WinRoute с целью установки/разрыва связи с Интернетом. Пользователь не обладает правом доступа к другим настройкам для внесения в них изменений.

Группы пользователей

Программный комплекс WinRoute позволяет группировать пользователей по различным признакам. Один и тот же пользователь может принадлежать одновременно к различным группам.

Группе предоставляются определенные полномочия.

> ***Примечание***
>
> Полномочия, выделенные группе, обладают приоритетом перед полномочиями того или иного ее участника.

Участники группы могут наделяться следующими полномочиями:

- **No access to administration** (Не администраторы) — данные пользователи не обладают полномочиями на управление программным комплексом WinRoute;
- **Full access to administration** (Администраторы) — данные пользователи обладают неограниченными полномочиями на управление программным комплексом WinRoute. Пользователи этой группы, если им выделены соответствующие полномочия, могут управлять межсетевым экраном из любой точки земного шара в безопасном режиме. При этом доступ к механизму (Engine) WinRoute надежно защищен мощными средствами криптографии и паролем;
- **View logs** (Просмотр журналов) — данные пользователи обладают правом подключения к программе управления WinRoute только для просмотра содержания журналов (сведения по отладке, почтовый журнал, журнал

прокси-сервера и т. п.) на экране. Права на изменение настроек данные пользователи не имеют;

- **Control dial-up lines** (Контроль линий с вызовом по номеру) — данные пользователи вправе подключаться к программе управления WinRoute с целью установки/разрыва связи с Интернетом. Пользователи не обладают правом доступа к другим настройкам для внесения в них изменений.

Компоненты комплекса WinRoute Pro

Программный комплекс WinRoute Pro 4.*x* состоит из трех модулей.

- **WinRoute Engine** (Движок).

  Выполняет все операции маршрутизации и анализа (NAT, пакетной фильтрации, распределения портов и др.). Запуск и завершение работы механизма WinRoute осуществляются либо из программы WinRoute Engine Monitor, либо, если ваша сеть работает под управлением Windows NT, непосредственно из ее раздела **Services** (Службы). Механизм WinRoute функционирует в скрытом режиме как служба ОС Windows 2000/NT/98 или 95.

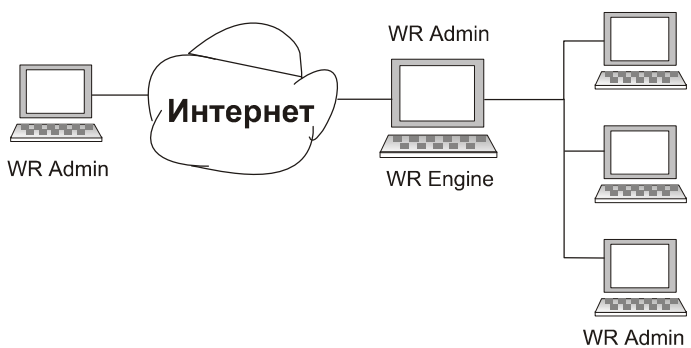


Рис. 3.68. WR Admin и WR Engine обеспечивают в WinRoute настройку и контроль

- **WinRoute Engine Monitor** (Монитор).

  Является диспетчерским приложением (рис. 3.68), непрерывно отслеживающим состояние механизма WinRoute. Значок программы отображается в правом нижнем углу рабочего стола.

- **WinRoute Administrator** (Программа управления).

  Обеспечивает настройку конфигурации и других параметров механизма WinRoute. Будучи самостоятельным приложением (wradmin.exe), программа WinRoute Administrator может работать на любом компьютере, подключая его к машине, на которой установлен механизм WinRoute, через TCP/IP-соединение. Сведения о настройках механизма WinRoute для подключения к удаленному узлу изложены в других разделах.

Временные интервалы

Временные интервалы (рис. 3.69) вводятся для выполнения по расписанию следующих действий:

- фильтрация пакетов;
- обмен электронной почтой (отправка и прием сообщений);

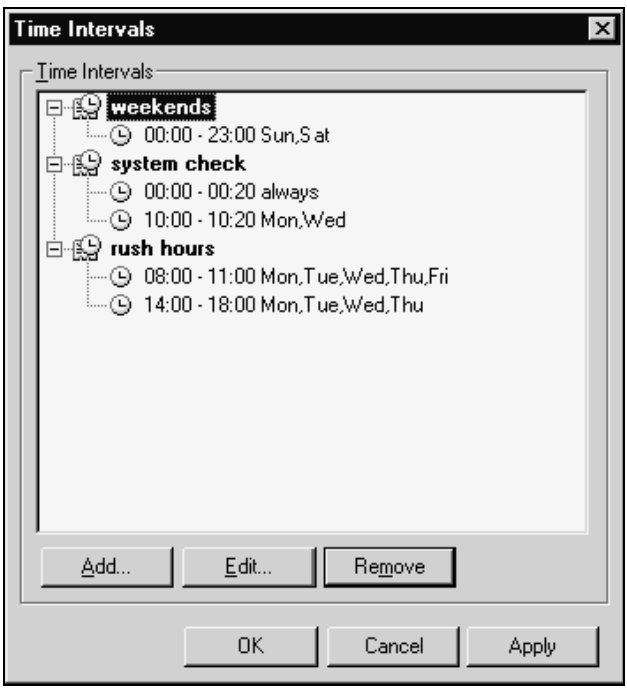


Рис. 3.69. Установка временных интервалов (расписание)

- подключение к Интернету;
- выполнение дополнительных настроек NAT.

> ***Примечание***
>
> Временные интервалы группируются по временным поясам, в результате чего формируется неоднородное временное пространство, состоящее из нескольких временных интервалов. Например, вы можете создать временной пояс под названием "Выходные и вечернее время", включив в него временные интервалы с 16:00 до 18:00 по субботам, воскресеньям и понедельникам, а также с 17:00 до 19:00 по вторникам.

Чтобы создать временной пояс, выполните следующие действия:

1. В меню **Setting** (Настройки) выберите команду **Advanced** (Дополнительно), откроется окно **Times Intervals** (Временные интервалы).
2. Введите название временного пояса.
3. Добавьте новые временные интервалы.

Системные требования

Минимальные системные требования к установке и обеспечению работоспособности программного комплекса WinRoute Pro 4.1:

- ПК класса Pentium (с одним или двумя процессорами);
- ОС Windows 95/98/NT 4.0/2000;
- память 32 Мбайт;
- 1 Мбайт свободного дискового пространства;
- наличие по меньшей мере двух интерфейсов, которыми могут быть: Ethernet, RAS, TokenRing, DirecPC.

Краткий контрольный перечень параметров

Существует перечень основных настроек и правил, единый для всех пользователей программного комплекса WinRoute. Его соблюдение обеспечит успешное подключение вашей сети к Интернету — разумеется, при наличии работоспособного канала для такого подключения.

Если вы намерены воспользоваться всеми преимуществами коллективного подключения к Интернету с использованием технологии преобразования сетевых адресов (Network Address Translation, NAT), нужно выполнить описанные далее настройки. В этом нет необходимости, если вы хотите подключиться через прокси-сервер (встроенный в программный комплекс WinRoute). В таком случае достаточно настроить ваш браузер и приложения на использование прокси-сервера WinRoute. Однако мы настоятельно рекомендуем пользоваться NAT, где только возможно, поскольку эта технология обеспечивает более высокое быстродействие, безопасность и надежность.

Настройки и правила

При настройке комплекса WinRoute следует соблюдать правила, приведенные далее:

1. *Проверьте наличие двух интерфейсов (сетевых адаптеров) в головном компьютере комплекса WinRoute.* Проверьте, имеется ли в головном компьютере комплекса WinRoute (хотя бы) два интерфейса: один для доступа в Интернет, второй для подключения к локальной сети или клиентским узлам. Интерфейсами могут служить сетевые адаптеры или линии подключения к серверу удаленного доступа (RAS). При этом один из интерфейсов должен применяться для подключения к Интернету (через Ethernet или RAS, либо по схеме коммутируемого доступа), а другой или другие (Ethernet, Token Ring...) — для установки связи с вашей локальной сетью (сетями).

2. *Обеспечьте возможность эхо-тестирования всех IP-адресов!* Эхо-тестирование (ping) как общедоступных, так и закрытых IP-адресов головной машины WinRoute с клиентских узлов является необходимым условием функционирования программного комплекса.

3. *Включите NAT в интернет-интерфейсе головного ПК комплекса WinRoute!* ВКЛЮЧИТЕ параметр преобразования сетевых адресов для интерфейса, обслуживающего подключение к Интернету (через Ethernet или линию RAS). Для этого войдите в меню **Setting | Interface Table** (Настройки | Таблица интерфейсов) и перейдите к свойствам соответствующего интерфейса.

4. *Отключите NAT во внутреннем интерфейсе головного ПК комплекса WinRoute!* Уберите флажок **Включить преобразование сетевых адресов** в интерфейсах, обеспечивающих подключение к внутренним сетям. В чрез-

вычайно специализированных конфигурациях NAT может быть оставлен *включенным* и во внутреннем интерфейсе.

5. *Отключите шлюз во внутреннем интерфейсе головного ПК комплекса WinRoute!* Убедитесь в том, что в свойствах сетевого подключения интерфейса (сетевого адаптера), обеспечивающего подключение к внутренней сети, шлюз по умолчанию *не установлен*. И конечно же, шлюз по умолчанию интерфейса подключения к Интернету необходимо включить и настроить в соответствии с указаниями вашего провайдера.

6. *Введите в головной ПК комплекса WinRoute параметры конфигурации DHCP-сервера!* В большинстве случаев вы будете пользоваться автоматизированной настройкой конфигурации сети с помощью DHCP-сервера программного комплекса WinRoute. Наряду с параметрами, в которых вы указываете сведения для ваших рабочих станций (например, данные DNS-сервера, шлюза по умолчанию и др.), дважды проверьте, определен ли диапазон (диапазоны) IP-адресов для DHCP-сервера.

7. *Установите внутренний IP-адрес головной машины комплекса WinRoute в качестве шлюза по умолчанию для клиентских ПК!* Головной ПК программного комплекса WinRoute играет роль *шлюза по умолчанию* для всех компьютеров локальной сети. Следовательно, IP-адрес (например, 192.168.1.1) сетевого адаптера головной машины WinRoute, обслуживающего внутреннюю сеть, должен быть установлен как шлюз по умолчанию на всех внутренних/клиентских компьютерах. Установите это значение на каждом клиентском узле или установите его один раз на DHCP-сервере комплекса WinRoute, который тогда автоматически назначит этот параметр для ваших рабочих станций. Если вы предпочитаете использовать по умолчанию другой шлюз, см. примеры дополнительных (меж)сетевых настроек.

8. *Проверьте DNS клиентских ПК!* В большинстве случаев вы будете пользоваться встроенным в WinRoute ретранслятором DNS в качестве DNS-сервера ваших сетевых компьютеров. Убедитесь в том, что встроенный в WinRoute ретранслятор DNS *активизирован* и правильно настроен. Чтобы пользоваться DNS-сервером вашего провайдера, введите его адрес в соответствующие поля конфигурации TCP/IP каждого подключенного к сети компьютера.

Примечание

Если программный комплекс WinRoute используется только как межсетевой экран или почтовый сервер (т. е. без организации коллективного подключе-

ния к Интернету), включать NAT в каком-либо из интерфейсов необходимости нет.

Если головной компьютер WinRoute обслуживает несколько локальных сетей, для интерфейса каждой из них необходимо назначить отдельный IP-адрес. Нельзя назначать IP-адреса одной и той же сети (например, 207.181.216.23 для одного интерфейса и 207.181.216.24 для другого). В большинстве случаев, когда имеется только один внутренний (ЛВС) интерфейс и один для подключения к Интернету, проблем не возникает. Однако, если у вас три интерфейса (два локальных и один для Интернета), внутренним интерфейсам необходимо назначать IP-адреса разных сетей (например, для одного 192.168.1.1, а для второго 192.168.2.1).

Невозможно пересказать все функции и настройки этой программы. Существующие варианты и версии WinRoute позволяют выбрать и подходящую по цене, и удовлетворительную по возможностям программу.

Но несмотря на множество достоинств WinRoute эта программа — продукт коммерческий. Версии, обладающие большими возможностями, стоят больших денег.

Интернет, тем не менее, предлагает нам и бесплатные программы, которые мы рассмотрим далее.

Extra Systems Proxy Server

На сайте **http://ln.com.ua/~vendor/** можно найти вариант прокси-сервера.

Предлагаемая версия прокси-сервера предназначена для работы на платформе Win32: Windows 95/98/ME/NT/2000. Рекомендуется, однако, использование исключительно серверных платформ: Windows NT Server и Windows 2000 Server. Также желательно, чтобы сервер, на котором работает данная программа, был выделенным (т. е. не использовался в качестве рабочей станции).

Назначением данной программы является обеспечение одновременного доступа в Интернет со стороны множества компьютеров локальной сети клиента через один имеющийся в его распоряжении канал связи с провайдером. В настоящий момент сервер поддерживает только протокол HTTP. В будущем планируется обеспечение поддержки и других протоколов (NNTP, SMTP, FTP и др.).

Данный сервер реализован в виде сервиса. Для его установки необходимо запустить на исполнение файл esps.exe с параметром командной строки

INSTALL, а для устранения данного сервиса из системы — тот же файл, но с параметром командной строки UNINSTALL. Имеется также еще один параметр командной строки — APPLICATION, предназначенный для запуска (без предварительной установки) данного сервера в качестве приложения, а не сервиса. Однако использование этого параметра не рекомендуется — запускать сервер как приложение, а не как сервис — нарушение общепринятых правил.

Данная программа может использоваться любым лицом или организацией для любых целей, не противоречащих закону, в том числе коммерческих, без какой-либо платы авторам. Ни сейчас, ни когда-либо в будущем никто не имеет права требовать какого бы то ни было вознаграждения за использование данной программы. Допускается лишь получение платы за оказание консультаций, проведение работ по установке, настройке и сопровождению данного сервера.

При создании сервера авторы прилагали все усилия по устранению обнаруженных ошибок, но в то же время полное отсутствие недоработок не гарантируется. Авторы не берут на себя никакой ответственности за возможный ущерб для файлов или оборудования любого лица или организации, который может наступить из-за использования данного сервера. В то же время авторы данного сервера гарантируют, что программные коды данного сервера не содержат в себе никаких деструктивных или шпионских функций.

Сведения об архитектуре

Данная версия прокси-сервера Extra Systems разработана на основе тех специфических подходов к программированию интернет-серверов, к которым разработчики пришли в результате многолетних поисков в данном направлении.

Основными моментами, которым уделялось внимание, являются скорость, стабильность и надежность работы сервера. Разработчики пришли к заключению, что единственным способом добиться этих целей является полный отказ от динамического создания каких-либо объектов по ходу работы сервера. Таким образом, все необходимые объекты (потоки, сокеты, буферы памяти и т. п.) создаются данным сервером однократно в момент запуска и в дальнейшем используются по мере необходимости. Многомесячные испытания данной концепции в ряде тестирующих организаций подтвердили правильность такого подхода.

Количество создаваемых объектов (ресурсоемкость сервера) задается пользователем посредством редактирования файла настроек и может меняться в

широких пределах в зависимости от потребностей и аппаратных возможностей того или иного клиента.

Сервер имеет в своем составе следующие подсистемы:

- ❒ модуль работы с сокетами;
- ❒ модуль управления потоками;
- ❒ модуль управления памятью;
- ❒ модуль анализа запросов и их выполнения;
- ❒ модуль учета работы клиентов;
- ❒ модуль кэширования в памяти адресов DNS;
- ❒ модуль кэширования в памяти успешно полученных из сети объектов (страницы, картинки и т. д.);
- ❒ модуль записи текущего состояния сервера;
- ❒ модуль управления доступом.

Настройки

Настройки программы размещаются в файле esps30.ini, который находится в каталоге Windows. Далее идет описание настроек по каждой подсистеме сервера. Каждая подсистема описывается соответствующей секцией указанного INI-файла.

При первом запуске формируется файл с настройками по умолчанию, которые в дальнейшем могут быть изменены пользователем программы. Для того чтобы новые настройки вступили в силу, необходимо перезапустить данный прокси-сервер с помощью сервис-менеджера операционной системы или же перезапустить саму систему (например, перезагрузив компьютер).

Основные настройки

Основные настройки сервера размещены в секции **Server**:

- ❒ **Port** (Порт) — номер порта, который принимает запросы от клиентов;
- ❒ **Threads** (Потоки) — количество рабочих потоков, выполняющих запросы клиентов;
- ❒ **Idle Thread Time** (Время бездействия потока) — время (в миллисекундах), на которое каждый поток освобождает процессор в отсутствие запросов от клиентов;

- **Master** (Главный) — адрес главного прокси-сервера, если данный сервер не является основным.

По умолчанию программа устанавливается на порт 3128. Если по каким-то причинам этот адрес не подходит, пользователь может назначить любой другой.

Количество потоков, устанавливаемое по умолчанию, равно 16. Для небольших сетей этого вполне достаточно. При необходимости можно установить 32, 64 или еще большее количество рабочих потоков. Достаточное для конкретной ситуации количество рабочих потоков легко определить, наблюдая карту использования потоков на странице статистики данного прокси-сервера. При недостаточном в данной конкретной ситуации количестве рабочих потоков запросы клиентов могут не обслуживаться (пропускаться). В этом случае необходимо увеличить количество рабочих потоков.

Время освобождения процессора каждым потоком по умолчанию устанавливается равным 100 мс. Рабочие потоки действуют следующим образом:

1. Определяют наличие активного клиентского запроса.
2. При отсутствии запроса — переход к п. 5, при наличии — к п. 3.
3. Выполняют запрос.
4. Переход к п. 1.
5. Освобождают процессор на заданное в настройках время.
6. Переход к п. 1.

Чем меньше время освобождения процессора, тем быстрее откликается сервер на поступающие запросы, но тем сильнее загружен процессор (особенно при большом количестве рабочих потоков). Поскольку каждый поток работает независимо, то время отклика сервера на поступающие запросы будет меньше того времени, на которое каждый поток освобождает процессор. Эта разница будет тем больше, чем больше рабочих потоков запущено. По теории вероятности, при наличии 16 потоков и времени освобождения процессора в 64 мс среднее время отклика будет равно 64/16 = 4 мс.

Адрес ведущего (главного) прокси-сервера задается в поле **Master** в виде адреса и порта, разделенных двоеточием, например `192.168.1.35:3080`. Если это поле оставить пустым (случай по умолчанию), то данный сервер сам будет получать все необходимые объекты прямо из сети, если же указать адрес другого прокси-сервера, то данный сервер не будет обращаться за объектами к сети, а будет все запросы переадресовывать к указанному прокси-серверу, передавая клиентам ответы главного (ведущего) прокси-сервера.

Модуль управления памятью

Как уже отмечалось ранее, вся память, используемая сервером, запрашивается у системы в момент запуска. В дальнейшем все временные данные (включая кэш полученных из сети объектов) размещаются в этой области.

Используемая сервером память имеет страничную организацию. Для каждого объекта выделяется одна или более страниц памяти в зависимости от размера объекта. При удалении объекта назначенные ему страницы памяти отмечаются свободными, так что в дальнейшем они могут использоваться для хранения вновь создаваемых объектов.

За настройки этого модуля отвечает секция **Memory Pool** (Пул памяти), имеющая два параметра:

- **Page Count** (Подсчет страниц) — количество используемых страниц памяти;
- **Page Size** (Размер страницы) — размер используемых страниц памяти.

По умолчанию программа устанавливает 4096 страниц по 1024 байт каждая. При наличии достаточного количества памяти в системе рекомендуется устанавливать не менее 65 536 страниц. Размер страниц менять не рекомендуется.

Страница статистики прокси-сервера позволяет в любой момент узнать общий и свободный объем области памяти, контролируемой данным модулем.

Модуль учета клиентов

Этот модуль состоит из таблицы, в которую заносятся адреса работающих клиентов и данные об их активности (количество используемых рабочих потоков, количество поступивших запросов, объем переданной информации и т. п.), и специального следящего потока, освобождающего таблицу от записей адресов, с которых давно не поступало никаких запросов (это бывает в том случае, если данный клиент отключился от сети). Информация из указанной таблицы доступна со страницы статистики данного прокси-сервера.

За настройки этого модуля отвечает секция **Users** (Пользователи), имеющая четыре параметра:

- **Enable** (Пуск) — включение (1) или выключение (0) этого модуля;
- **Count** (Количество) — наибольшее количество клиентов, которые могут одновременно работать с сервером;

- **Idle Thread Time** (Время бездействия потока) — время (в миллисекундах), на которое поток отслеживания клиентов освобождает процессор в промежутках между своей работой;
- **Time To Live** (Время жизни) — время (в миллисекундах), по истечении которого при отсутствии запросов клиент будет считаться отключившимся.

Модуль работы с сокетами

За настройки этого модуля отвечает секция **Wait Socket**, имеющая четыре параметра, определяющие допустимый тайм-аут при работе с локальными (через которые клиенты связываются с данным прокси-сервером) и удаленными (через которые данный прокси-сервер связывается с глобальной сетью или ведущим прокси-сервером) сокетами:

- **Write Local** — тайм-аут на запись (в секундах) для локальных сокетов;
- **Read Local** — тайм-аут на чтение (в секундах) для локальных сокетов;
- **Write Remote** — тайм-аут на запись (в секундах) для удаленных сокетов;
- **Read Remote** — тайм-аут на чтение (в секундах) для удаленных сокетов.

Малое время ожидания может помешать удовлетворению запросов при слабом внешнем канале или сильной загруженности сети, а чрезмерно большое — неоправданно удлинить время ожидания выдачи диагностики о неработоспособности того или иного хоста. По умолчанию локальный тайм-аут установлен на 5 с, а удаленный — на 15 с.

Модуль кэширования адресов DNS

Для экономии сетевого трафика данный прокси-сервер хранит в специальном буфере, размер которого регулируется, успешно полученные из сети адреса хостов. Время хранения этой информации также может регулироваться. Специальный поток в составе данного модуля устраняет из указанного буфера те записи, время хранения которых истекло.

За настройки этого модуля отвечает секция **DNS Cache**, имеющая четыре параметра:

- **Enable** — включение (1) или выключение (0) этого модуля;
- **Count** — размер буфера (в записях) для хранения адресов;

- **Idle Thread Time** — время (в миллисекундах), на которое поток отслеживания устаревших адресов освобождает процессор в промежутках между своей работой;
- **Time To Live** — время хранения записей (в миллисекундах).

Модуль кэширования успешно полученных из сети объектов

За настройки этого модуля отвечает секция **Memory Cache**, имеющая пять параметров:

- **Enable** — включение (1) или выключение (0) этого модуля;
- **Count** — предельное количество объектов, которые одновременно могут храниться в кэше;
- **Idle Thread Time** — время (в миллисекундах), на которое поток отслеживания устаревших объектов освобождает процессор в промежутках между своей работой;
- **Time To Live** — время хранения объектов (в миллисекундах);
- **Limit** — предельный размер всех объектов, которые могут находиться в кэше (в байтах).

Данный модуль помещает в кэш лишь успешно полученные из сети объекты, причем только те из них, которые подлежат кэшированию. В состав данного модуля входит специальный поток, который удаляет из кэша те объекты, время хранения которых истекло, а также следит за тем, чтобы не превышалось предельное количество объектов и предельное количество памяти, занимаемое всеми объектами. При достаточном количестве установленной в системе памяти рекомендуется устанавливать количество объектов не менее 8129, а суммарный размер объектов — не менее 32 Мбайт. Суммарный размер объектов рекомендуется устанавливать равным половине размера главного пула памяти, так как кэш объектов размещается именно в главном пуле памяти, но главный пул памяти используется сервером и для других целей.

Время хранения рекомендуется устанавливать равным 10—15 часам, что обеспечит эффективную экономию внешнего канала и в то же время не приведет к выдаче клиентам устаревшей информации.

Модуль записи текущего состояния сервера

За настройки этого модуля отвечают две секции, имеющие по два параметра с идентичным назначением. Это секции **Main Log** (Главная запись) и **Status Log** (Запись состояния). Первая секция отвечает за протоколирование процесса загрузки и выгрузки сервера, а вторая — за ежечасную фиксацию таких параметров сервера, как количество подключенных клиентов, количество обработанных запросов, объем переданной информации, текущий размер кэша и т. п.

Параметры указанных секций такие:

- **Enable** — включение (1) или выключение (0) записи по соответствующей секции модуля;
- **File Name** — полное имя файла, куда будет записываться информация по соответствующей секции модуля.

Модуль управления доступом

За настройки этого модуля прокси-сервера ESPS отвечает секция **Check** (Контроль), имеющая четыре параметра:

- **Enable** — включение (1) или выключение (0) этого модуля;
- **File Name** — имя файла, содержащего настройки доступа;
- **Default** — разрешение (1) или запрещение (0) доступа со стороны хостов, не поименованных в файле настроек;
- **Idle Thread Time** — периодичность (в миллисекундах) обновления информации об адресах клиентов, описания которых даются командой CD.

Если параметр **Enable** установлен в 0, то остальные параметры значения не имеют.

Файл настроек является обычным текстовым файлом, в котором команды размещены построчно: каждая команда размещена в отдельной строке. Некоторые строки могут быть пустыми (не содержать никаких печатных символов) и служить для визуального разделения смысловых блоков.

Файл настроек содержит строки нескольких типов: описание групп (`GD`, `CD`, `GN`), разрешение доступа к страницам (`PA`) и запрещение доступа к страницам (`PD`), описание запрещенных в URL слов и фрагментов (`BW`). Каждая команда имеет свои параметры, разделенные двоеточием. Строки, не содержащие команд, не учитываются. Пробелы в строке и дополнительные поля в расчет не

принимаются. Также не имеет значения и регистр символов, которыми написана та или иная строка (последовательность `Av6Hyu` во всех отношениях эквивалентна последовательности `av6hyU`). Дополнительные поля в командной строке можно использовать для комментариев.

Для настройки данного модуля необходимо выполнить два действия:

1. Определить группы клиентов сервера по их IP-адресам (`GD`) или именам (`CD`).
2. Определить права доступа для каждой такой группы клиентов.

С помощью команды `GN` можно (но необязательно) определить имена созданных групп.

Команда описания группы `GD` имеет три параметра: номер группы (от 1 до 64), адрес группы, маску. Например, команда

```
GD : 3 : 192.168.3.0 : 255.255.255.0 : Комментарий
```

определяет группу хостов с `192.168.3.0` по `192.168.3.255` как группу № 3.

Одна группа может быть подмножеством другой. Вхождение в подмножество считается приоритетным по сравнению с вхождением в надмножество. Иными словами, если задана группа № 1 для адресов с `192.168.0.0` до `192.168.255.255` и группа № 2 для адресов с `192.168.2.0` до `192.168.2.255`, то хост `192.168.2.45` считается принадлежащим к группе № 2, а не № 1, и права доступа для этого хоста будут определяться по данным для группы № 2, а не для группы № 1.

Можно также сказать, что приоритет определяется количеством установленных в маске битов — чем их больше, тем статус выше. В частности, маска `255.255.255.255`, определяющая один уникальный хост, имеет наивысший возможный статус (установлены все 32 бита). Другой крайний случай — маска `0.0.0.0` (при любом адресе) определяет все множество возможных адресов Интернета. Использование этой маски для образования группы в какой-то мере эквивалентно действию параметра **Default** из данного раздела INI-файла.

Команда `CD` имеет два параметра: номер группы (от 1 до 64) и имя компьютера, который необходимо отнести к данной группе. Например, команда

```
CD : 5 : rabbit : Комментарий
```

определяет принадлежность машины `rabbit` к группе № 5.

Отметим, что к одной группе можно одновременно отнести несколько диапазонов IP-адресов (командами `GD`) и несколько машин (командами `CD`), комбинируя эти команды в любой последовательности.

В момент запуска сервер (через службу имен) определяет IP-адреса машин, заданных с помощью команды CD, и в дальнейшем уточняет эту информацию с периодом, который задан параметром **Idle Thread Time**.

При поступлении от клиента первого запроса определение группы, к которой его следует отнести, начинается с просмотра команд CD. Если ни одна команда CD не определяет данную машину (и только в этом случае), просмотр продолжается по командам GD. Таким образом, любая команда CD имеет более высокий статус, чем любая команда GD.

Для именования групп служит команда GN, которая имеет два параметра: номер группы (от 1 до 64) и имя группы. Например, команда

```
GN : 8 : Администраторы :
```

определяет имя группы № 8 как "Администраторы". Это имя будет использоваться модулем вывода статистической информации для облегчения восприятия выводимой информации.

Перейдем теперь к рассмотрению команд разрешения (PA) и запрещения доступа (PD) к страницам Интернета.

Обе эти команды имеют одинаковый формат: код команды, номер группы, адрес страницы. Например, команда

```
PD : 4 : m.xyz.com : Комментарий
```

запрещает доступ к любой странице сервера **m.xyz.com** для всех клиентов, относящихся к группе № 4. Если на месте номера группы стоит 0, то данная запись имеет силу для всех групп клиентов. Если в поле адреса страницы ничего нет, то такая запись относится к любой странице Интернета.

Если для одной и той же группы имеется несколько сходных записей, то статус таких записей тем выше, чем больше длина адреса в той или иной записи. Например, пара записей

```
PD : 4 : m.xyz.com : Комментарий
PA : 4 : m.xyz.com/img : Комментарий
```

запрещает доступ клиентов группы № 4 ко всем страницам сервера **m.xyz.com**, за исключением тех, которые находятся в каталоге img.

Запись, в которой поле адреса пустое (обозначает, как это уже указывалось выше, любую страницу Интернета), имеет низший статус, который перекрывается любой записью с непустым адресом.

Если описана некоторая группа хостов, но для нее нет ни одной записи типа `PA` или `PD`, то для этой группы считается открытым доступ к любой странице Интернета.

Формат команды запрещенных слов `BW` включает номер группы и запрещенный в URL фрагмент. Например, команда

```
BW : 0 : photo : Комментарий
```

предотвращает доступ клиентам любой группы к странице, в полном имени которой в произвольном месте присутствует фрагмент `photo`. (Напомним, что номер группы 0, как всегда, означает применимость данной записи ко всем группам.)

Необходимо отметить, что команда `BW` имеет приоритет по сравнению с командой `PA`, так что если некий URL содержит в себе фрагмент, запрещенный командой `BW`, то никакая команда `PA` для данной группы уже не сможет обеспечить получение клиентом данной страницы.

Пример файла настроек

Листинг 3.2. Создаем группы пользователей

```
GD : 1 : 192.168.0.0 : 255.255.255.0 :
GD : 2 : 192.168.3.0 : 255.255.255.0 :
CD : 1 : dog :
CD : 2 : cat :
CD : 3 : fox :
```

Листинг 3.3. Даем группам имена (это необязательно)

```
GN : 1 : Клиенты :
GN : 2 : Администраторы :
```

Листинг 3.4. Открываем все

```
PA : 1 :                                        :
PA : 2 :                                        :
```

Листинг 3.5. Запрещаем плохие слова

```
BW : 0 : banner                    : Для всех
BW : 1 : porno                     : Только для юзеров
BW : 1 : sex                       : Только для юзеров
```

Листинг 3.6. Запрещаем баннеры

```
PD : 0 : m.doubleclick.net/viewad              :
PD : 0 : 4click.com.ua/cgi-bin/ps100.cgi       :
PD : 0 : reklama.utro.ru/bb.cgi                :
PD : 0 : images.rambler.ru/upl/ban_barter      :
PD : 0 : ad2.bb.ru/bb.cgi                      :
PD : 0 : www.bigbn.com.ua/bigbn                :
PD : 0 : ad.adriver.ru/cgi-bin/rle.cgi         :
PD : 0 : 217.170.71.61/users                   :
PD : 0 : ad.rambler.ru/ban.ban                 :
PD : 0 : ad2.rambler.ru/ban.ban                :
PD : 0 : ad.pbs.bb.ru/bb.cgi                   :
PD : 0 : ad1.lbe.ru/bb.cgi                     :
PD : 0 : reklama.port.ru                       :
PD : 0 : ad.mtu.ru/cgi-bin/a.cgi               :
PD : 0 : engine.awaps.net                      :
PD : 0 : adv.gorod.ru                          :
PD : 0 : image.linkexchange.com                :
PD : 0 : sle-pvt.com.ua                        :
PD : 0 : b.abn.com.ua/abn.php                  :
PD : 0 : reks.com.ua/b                         :
PD : 0 : www.gala.net/ads                      :
PD : 0 : ad.ir.ru/bb.cgi                       :
PD : 0 : www.aviso.com.ua/adverts              :
PD : 0 : finance.com.ua/bns                    :
PD : 0 : www.sle.com.ua                        :
PD : 0 : images.rambler.ru/other               :
PD : 0 : images.rambler.ru/n/                  :
PD : 0 : bs.yandex.ru/count                    :
PD : 0 : avanport.com/ban/                     :
```

```
PD : 0 : kiev2000.com/adver                    :
PD : 0 : sle-ent.com.ua                        :
PD : 0 : adfarm.mediaplex.com/ad/bn            :
```

Получение статистической информации

Система сбора статистики обеспечивает детальное наблюдение за следующими параметрами работы прокси-сервера:

- поступившие запросы;
- объем отправленной информации;
- состояние главного пула памяти;
- состояние рабочих потоков;
- список работающих с сервером клиентов;
- список элементов кэша DNS;
- список элементов кэша объектов;
- состояние памяти системы;
- запись поминутной, почасовой и посуточной статистики;
- список групп клиентов сервера с указанием прав доступа для каждой из групп.

Для перехода на страницу статистики необходимо в адресной строке браузера, работающего через данный прокси-сервер, запросить с любого хоста страницу /ESPS/MainServerStatus. Полный адрес, таким образом, может, например, выглядеть так: **http://192.168.0.1/ESPS/MainServerStatus**.

Загрузка программы

Программа доступна для загрузки в виде EXE-файла размером 123 392 байт. Это полноценная версия, не имеющая в работе никаких ограничений. Ни загрузка программы, ни ее последующее использование не требуют никакой регистрации.

В данный момент можно получить программу версии 3.43 от 12 февраля 2003 года по адресу **http://ln.com.ua/~vendor/esps30.htm**

С новостями версий программы можно ознакомиться на специальной странице **http://www.users.lucky.net.ua/~vendor/esps/history.htm**.

WinGate

Еще одна популярная программа — прокси-сервер. Ее саму и ее описание можно получить по адресу **ftp://ftp.cityline.ru/pub/wingate/** или на сайте **http://surf.to/wingaterus**.

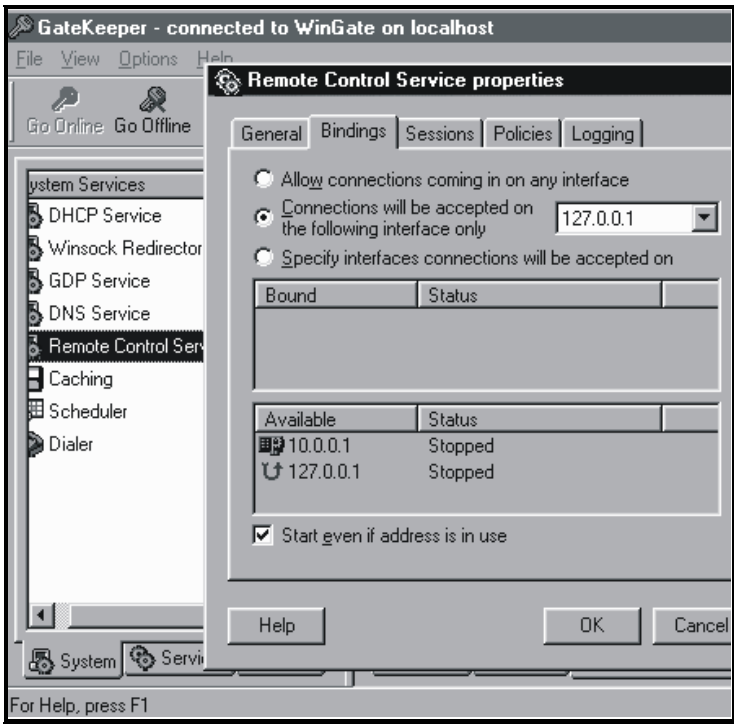


Рис. 3.70. Фрагмент панели **GateKeeper** — средства настройки WinGate

Программа позволяет настроить практически все необходимые сетевые службы (рис. 3.70).

Она может исполнять роль прокси-сервера, сервера DNS и DHCP, осуществлять маршрутизацию за пределы локальной сети, обеспечивая доступ нескольких компьютеров к Интернету, и надежно защищать сеть от проникновения извне. Позволяет вести мониторинг работы сети. Имеет в своем составе хорошо настраиваемую программу набора номера и планировщик, позволяющие программировать работу сервера соответственно требованиям сети. Есть несколько версий программы, рассчитанных на пользователей

разного уровня. Возможности программы меняются от версии к версии и наиболее широко представлены в Pro-версии.

По адресу **http://lan2inet.agava.ru/wg4install_9xdialup.htm** находится инструкция по установке сервера, сокращенный вариант которой приведен в этой книге.

Упрощенная инструкция по установке WinGate в Windows 95/98

Эту инструкцию следует использовать, если у вас имеются модем и dial-up-доступ к Интернету.

Для установки WinGate необходимо выполнить шаги, описанные далее. Приведены варианты установки программы для ПК, подключенного к Интернету, и компьютеров, подключаемых к Интернету через WinGate.

WinGate Server Computer (WG-сервер) — компьютер, подключенный к Интернету.

1. Установить соединение с Интернетом на WG Server.
2. Добавить TCP/IP на сетевом адаптере.
3. Настроить на сетевом адаптере статический IP-адрес — `192.168.0.1`.
4. Установить программное обеспечение WinGate.

WinGate Client Computer (WG-клиент) — компьютеры, подключаемые к Интернету через WinGate:

1. Проверить/установить Winsock 2 (для Windows 95).
2. Установить и настроить TCP/IP.
3. Установить WinGate Client.

   Вам необходимо установить соединение с WG Server согласно инструкциям вашего провайдера. Однако в процессе установки программного обеспечения WinGate необязательно должен быть подключенным к Интернету.
4. На следующем этапе необходимо настроить сетевой адаптер на WG Server, подключенный к локальной сети. Этому сетевому адаптеру *должен быть* присвоен статический IP-адрес. Адрес никогда не будет виден пользователям из Интернета или вашему провайдеру. Также он никак не повлияет на настройки интернет-соединения. Если у вас уже установлен

TCP/IP на сетевом адаптере, переходите к следующему пункту. Иначе необходимо произвести настройку TCP/IP:

- щелкните правой кнопкой мыши на значке **Network Neighborhood** (Сетевое окружение), чтобы открыть меню;

> ***ПРИМЕЧАНИЕ***
>
> Если вы используете Windows ME, щелкните на значке **My Network Places** (Мое сетевое окружение).

- выберите пункт **Properties** (Свойства) — откроется окно со списком протоколов. Найдите протокол TCP/IP. Возможно, у вас уже есть один для **Dial-Up Adapter** (Контроллер удаленного доступа) или другой сетевой адаптер в зависимости от типа подключения к Интернету;
- нажмите кнопку **Add** (Добавить);
- щелкните на строке **Protocol** (Протокол), затем нажмите кнопку **Add** (Добавить);
- в левом окне выберите в списке производителей **Microsoft**, затем в правом окне в списке протоколов отметьте **TCP/IP**;
- нажмите кнопку **OK**;
- нажмите кнопку **Cancel** (Отмена) в диалоговом окне **Select Network Component Type** (Выбор типа сетевого компонента), а затем кнопку **OK** для перезагрузки ПК.

5. На этом шаге нужно настроить TCP/IP на внутреннем сетевом адаптере. Щелкните правой кнопкой мыши на значке **Network Neighborhood** (Сетевое окружение) и выберите в раскрывающемся меню пункт **Properties** (Свойства). Найдите протокол TCP/IP, привязанный к внутреннему сетевому адаптеру (который вы добавили на втором шаге). Для настройки сетевого адаптера выполните следующие действия:

   - выберите протокол TCP/IP, привязанный к внутреннему сетевому адаптеру;
   - нажмите кнопку **Properties** (Свойства);
   - выберите вкладку **IP Address** (IP-адрес);
   - установите переключатель в положение **Specify an IP address** (Указать IP-адрес явным образом);

- в поле **IP address** (IP-адрес) введите `192.168.0.1`;
- в поле **Subnet Mask** (Маска подсети) введите `255.255.255.0`;
- выберите вкладку **DNS**. Не изменяйте никакие настройки DNS, отметьте только разрешен или запрещен DNS;
- нажмите кнопку **OK**;
- перезагрузите компьютер.

6. Установите WinGate на этот компьютер. В процессе установки выберите опцию **Configure this machine as a WinGate Server** (Настроить этот компьютер как WinGate-сервер). Продолжите процесс установки согласно **Installation Wizard** (Мастер установки). Тестовая версия позволяет пользоваться программой в течение 30 дней без ограничений. Загрузить тестовую версию можно по адресу **http://www.wingate.ru**.
7. Если на ПК с WG-клиентом установлена Windows 98, продолжите с шага 3. WG-клиент требует установки обновленного Microsoft Winsock 2. Если на ваших клиентах установлена Windows 95, необходимо выполнить следующие действия по обновлению Winsock:
   - загрузить Winsock 2 с сайта **www.microsoft.com/windows95/downloads/contents/WUAdminTools/S_WUNetworkingTools/W95Sockets2/Default.asp**;
   - установить Winsock 2 на ваши WG-клиенты с Windows 95.
8. Вам необходимо установить TCP/IP на ваших WG-клиентах. Если вы этого еще не сделали, вернитесь к шагу 2. Существует два варианта настройки TCP/IP на WG-клиентах. Вы можете выбрать **Obtain IP addresses automatically (DHCP)** (Получить IP-адрес автоматически) или **Specify an IP address (Static)** (Указать IP-адрес явным образом).

Настройка WG-клиента с применением **Obtain an IP Address Automatically/Dynamically** (Получить IP-адрес автоматически), используя DHCP, сводится к следующему:

1. Щелкните правой кнопкой на значке **Network Neighborhood** (Сетевое окружение).
2. Выберите пункт **Properties** (Свойства).
3. Выделите протокол TCP/IP, привязанный к сетевому адаптеру.
4. Нажмите кнопку **Properties** (Свойства).

5. Выберите вкладку **IP Address** (IP-адрес).
6. Установите переключатель в положение **Obtain an IP Address Automatically** (Получить IP-адрес автоматически).
7. Выберите вкладку **Wins Resolution** (Конфигурация WINS).
8. Установите переключатель в положение **Disable Wins Resolution** (Отключить распознавание WINS).
9. Выберите вкладку **DNS** (Конфигурация DNS).
10. Установите переключатель в положение **Disable DNS** (Отключить DNS).
11. Нажмите кнопку **OK**, перезагрузите компьютер и переходите к дальнейшим действиям.

Настройка WG-клиента с использованием статического IP-адреса — **Specify an IP Address** (Указать IP-адрес явным образом). Рекомендуется использовать WinGate DHCP, если у вас нет веских причин указывать IP-адрес вручную.

1. Щелкните мышью на значке **Network Neighborhood** (Сетевое окружение).
   - Выберите пункт **Properties** (Свойства).
   - Выделите протокол TCP/IP, привязанный к сетевому адаптеру.
   - Нажмите кнопку **Properties** (Свойства).
   - Выберите вкладку **IP Address** (IP-адрес).
   - Установите переключатель в положение **Specify an IP Address** (Указать IP-адрес явным образом).
   - В поле IP-адреса введите `192.168.0.2`.
   - В поле **Subnet Mask** (Маска подсети) введите `255.255.255.0`.
   - Выберите вкладку **Gateway** (Шлюз).
   - Введите в поле **Gateway** (Шлюз) IP-адрес WinGate `192.168.0.1`.
   - Нажмите кнопку **Add** (Добавить).
   - Выберите вкладку **DNS**.
   - Выберите опцию **Enable DNS** (Включить DNS).
   - Введите уникальное имя компьютера в сети в поле **Host** (Имя компьютера).
   - Оставьте *пустым* поле **Domain** (Домен).

- В поле **DNS server search order** (Порядок просмотра серверов DNS) введите IP-адрес WinGate `192.168.0.1`.
- Нажмите кнопку **Add** (Добавить).
- Оставьте пустым поле **Domain Suffix Search Order** (Порядок просмотра доменных суффиксов).
- Нажмите кнопку **OK**, перезагрузите компьютер и переходите к шагу 20.
- Установите WinGate Internet Client. Инсталляция осуществляется с помощью того же файла, что и для WG-сервера. Выберите Client-инсталляцию. После чего перезагрузите компьютер.

> ***ПРИМЕЧАНИЕ***
>
> Рекомендуется скопировать этот файл на клиентский компьютер, а не запускать его из сети.

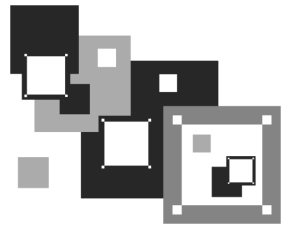
Установка WinGate завершена. Интернет-приложения на WG-клиент нужно настроить на подключение к Интернету, используя локальную сеть. E-mail-клиенты настраиваются согласно инструкциям провайдера. *Не настраивайте* приложения на подключение через прокси-сервер.

Настройка сервера вашей небольшой сети — дело ответственное. Чем тщательнее вы проведете настройку, чем полнее учтете особенности сети и специфику работы в ней пользователей, тем надежнее будет работать ваш сервер.

Правильная настройка — залог отсутствия конфликтов на аппаратном и программном уровнях, которые могут приводить к зависаниям и даже к краху системы.

В этой главе мы рассмотрели выход нашей сети в Интернет. Эта функция очень тесно связана с настройками сервера сети. В то же время можно организовать не только выход, но и санкционированный вход в вашу сеть. Такая возможность может оказаться чрезвычайно удобной, для получения доступа к ресурсам сети извне. Существуют, конечно, специально предназначенные для этого серверы, через которые многие из нас получают доступ к Всемирной паутине, а также FTP-серверы, хранилища данных с общим или ограниченным доступом. Наша сеть не входит в состав глобальной сети, но нам вполне по силам организовать доступ к сети извне по телефонной линии, и даже выход через нее в Интернет. Эти и некоторые другие возможности будут рассмотрены в следующей главе.

Глава 4



Изоляции — нет!

Создав сеть с выходом в Интернет, вы получили "государство", из которого можно попасть в окружающий мир. А к вам из этого мира можно попасть только через Интернет, если ваше соединение в данный момент активно.

В этой главе мы рассмотрим варианты подключения к вашей сети извне. В наше время практически везде, где бы мы ни находились, нас окружают телефоны. Телефонная линия может послужить отличным средством для связи компьютеров. Вход в сеть по телефонной линии имеет следующие преимущества:

- доступ к вашим данным из любой точки, где есть телефон и компьютер;
- возможность организовать информационную сеть, распределенную на большой территории и использующую в качестве каналов связи телефонные линии.

Такая сеть может состоять как из отдельных компьютеров, доступ к которым возможен по телефону, так и из небольших локальных подсетей с маршрутизаторами. Установив связь с такой локальной подсетью, даже компьютер, не имеющий доступа в Интернет, может подключиться к другой подсети или к глобальной сети. Соединение осуществляется по телефонной линии, подключенной к компьютеру подсети-посредника (рис. 4.1).

Собственно доступ к компьютеру по телефонной линии не требует какого-либо особого программного обеспечения. Все решается штатными средствами Windows 98.

Настройка компьютера, с которого будет производиться доступ, такова:

1. Создайте новое соединение. Задайте его имя и телефон (рис. 4.2).
2. На вкладке **Тип сервера** установите флажки **Войти в сеть**, **NetBEUI**, **TCP/IP**; все остальные флажки снимите.

Если компьютер, к которому производится подключение, не входит еще в какую-либо сеть, кроме образующейся при соединении, то IP-адрес будет получен автоматически (в любой версии Windows 98) и примет значение 192.168.55.2, вызываемый компьютер будет иметь адрес 192.168.55.1. Такие значения адресов приняты по умолчанию корпорацией Microsoft для подключения посредством сервера удаленного доступа. Если же вы подключаетесь к компьютеру, входящему в сеть и настроенному для работы в ней, то воспользуйтесь возможностью установить IP-адрес вручную. Для нашего случая значение адреса установим 192.168.1.2. Маска подсети в любом случае выбирается 255.255.255.0.

Настройка компьютера, с которым должно производиться соединение, такова:

1. Нажмите кнопку **Пуск**.
2. Выберите команду **Настройка | Панель управления**.
3. Запустите утилиту **Установка и удаление программ** и перейдите на вкладку **Установка Windows**.
4. Отметьте строку **Связь** и нажмите кнопку **Состав**.
5. Отметьте флажки **Сервер удаленного доступа**, **Телефон**, **Удаленный доступ к сети**.

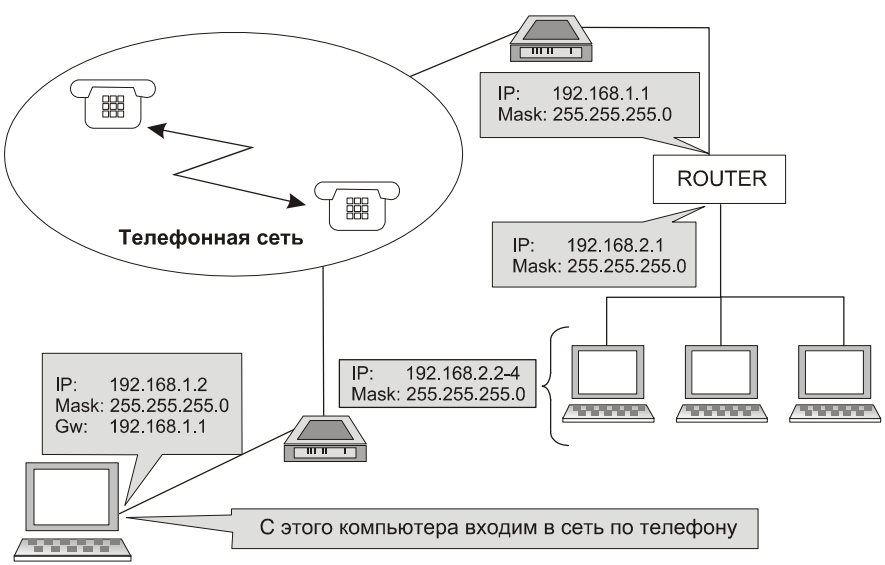


Рис. 4.1. Доступ по телефонной линии к одной из подсетей

6. Нажмите кнопку **OK** и вставьте диск с дистрибутивом ОС, если компьютер попросит это сделать. После установки компонентов потребуется перезагрузка Windows.

7. После перезагрузки в Панели управления дважды щелкните на значке **Сеть**. Если у вас нет компонентов **Клиент для сетей Microsoft**, **Протокол NetBEUI**, **Протокол TCP/IP**, **Служба удаленного доступа**, то их надо установить. Для этого нажмите кнопку **Добавить**, выберите из списка производителей **Microsoft** и таким образом установите необходимый клиент, протокол или службу.

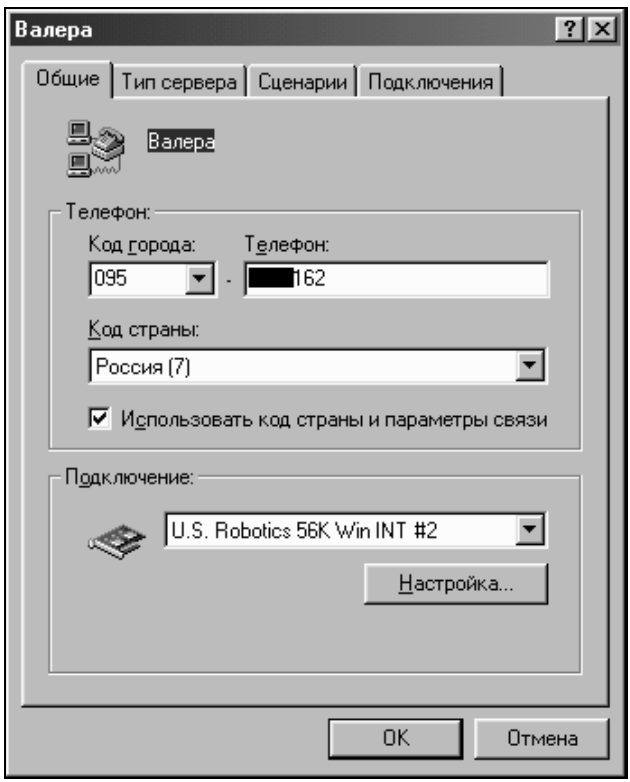


Рис. 4.2. Свойства соединения

8. Если не соглашаться с автоматическим присвоением IP-адреса для контроллера удаленного доступа, то необходимо установить адрес 192.168.1.1 и маску подсети 255.255.255.0.

9. Если компьютер является маршрутизатором и входит в другую сеть с помощью сетевой платы, то для IP-адреса сетевой платы значения уже настроены в соответствии с настройками локальной сети. Для нашего случая адрес сетевого адаптера — 192.168.2.1. При этом маска подсети — 255.255.255.0. Адрес в этом случае отличается от адреса контроллера удаленного доступа номером сети.
10. В свойствах компонента **Клиент для сетей Microsoft** установите переключатель **Быстрый вход**. Остальные параметры можно оставить по умолчанию.
11. Нажмите кнопку **Доступ к файлам и принтерам** и разрешите доступ к файлам и принтерам, отметив соответствующие флажки.
12. На вкладке **Управление доступом** выберите переключатель **На уровне ресурсов**.
13. Посмотрите на вкладку **Идентификация** и запомните имя компьютера или введите необходимое. Введите также имя рабочей группы.
14. Откройте папку **Мой компьютер**, а в ней — папку **Удаленный доступ к сети**. Раскрыв меню **Соединения**, обратите внимание на пункт **Сервер удаленного доступа**. Выбрав этот пункт, вы можете разрешить или запретить удаленные подключения к вашему компьютеру. Разрешив удаленное подключение, придумайте и введите пароль для подключения. Запишите его и не потеряйте! Если модем у вас постоянно подключен к телефонной сети и нет возможности отключить питание модема (для встроенных модемов), то пока не разрешайте удаленные подключения, так как компьютер будет ожидать звонка и на все входящие звонки будет отвечать. Если это обычный звонок, то звонящий услышит неприятный свист в трубке, а вы, подняв трубку, не сможете поговорить с человеком.
15. Теперь необходимо обеспечить доступ к дискам вашего компьютера. Для этого щелкните правой кнопкой на пиктограмме требуемого диска, выберите пункт **Доступ**, активизируйте переключатель **Общий ресурс**, заполните поле для сетевого имени, придумав это имя. Отметьте тип доступа — **Полный** или другой, по вашему выбору, придумайте и введите пароль для доступа к диску. После этого изображение диска в папке **Мой компьютер** изменится, приобретя "поддерживающую руку".
16. Если настройки закончены и требуется обеспечить доступ к компьютеру, разрешите удаленные подключения.

Можно заставить компьютер разрешать и запрещать удаленные подключения по расписанию. Для этого надо перекачать программу ServerOK с сайта

http://serverok.newmail.ru и настроить планировщик заданий, встроенный в Windows, на включение разрешения на доступ в определенное вами время. Автор программы предлагает ее бесплатно. Рекомендации по применению находятся на том же сайте. После этого вы сможете подключаться к удаленному компьютеру в заранее запланированное время. Если не применять ServerOK или другую подобную программу, то придется вручную каждый раз при необходимости обеспечивать удаленный доступ к компьютеру, открывать папки **Мой компьютер** и **Удаленный доступ к сети**, выбирать вкладку **Соединения**, открывать окно **Сервер удаленного доступа** и выбирать вариант **Разрешить/Запретить удаленные подключения**, устанавливая соответствующий переключатель.

Конечно, если вы отвели этот телефонный номер исключительно для связи с компьютером, переключать разрешение на удаленный доступ не надо. Можно управлять разрешением на подключение и путем выключения питания модема. Но такой вариант подходит в том случае, если с этого компьютера не осуществляется доступ к Интернету или другие соединения с использованием модема.

Доступ к ресурсам сервера и сети может быть защищен паролем. Тогда при соединении удаленного компьютера с сервером необходимо ввести имя пользователя и пароль для входа в Windows или для входа в сеть (в зависимости от настроек сервера), но иногда сервер требует ввести имя домена, несмотря на то что реально никакой домен не существует. В этом случае, проверив настройки и убедившись, что все сделано правильно, можно для входа на сервер применить следующий вариант процедуры аутентификации:

```
MSN/<имя_пользователя> <пароль_для_доступа_к_ресурсам>
```

Эта рекомендация дана самой корпорацией Microsoft в справке Windows 98, но обнаруживается она не с первого раза.

Связь двух компьютеров через модем в Windows XP

По приведенным далее ссылкам (возможно, что вам удастся найти и другие) можно найти статью Загитова Рифката "Связь двух компьютеров через модем в Windows".

- **http://www.winzone.ru/articles/284/**;
- **http://bugfix.ru/index.php?name=News&file=article&sid=1971**.

В статье рассматривается последовательность действий пользователя для настройки соединения двух компьютеров посредством телефонной линии и двух модемов. Никаких дополнительных затрат на прокладку кабеля не требуется. Нет необходимости согласовывать свой проект с местными органами управления. То есть этот вариант объединения двух компьютеров в сеть доступен любым пользователям персональных компьютеров, решившим объединить свои компьютеры в простую сеть.

Приведем изложение этой статьи, содержащее необходимый минимум информации, и некоторые комментарии.

Описанное в статье решение применимо, когда вы не имеете возможности решить задачу иным путем. У вас есть только два компьютера, два модема и телефонная линия. Несмотря на лаконичность поставленной задачи, возможны три варианта этого условия.

Варианты задачи:

- есть только два компьютера, два модема и телефонная линия;
- один из компьютеров подключен к локальной сети;
- один из компьютеров подключен к Интернету.

Естественно, что в каждом варианте задачи просматриваются варианты результатов решения этой задачи:

- получаем доступ каждого компьютера друг к другу;
- получаем доступ в удаленную локальную сеть;
- получаем доступ в Интернет через удаленный компьютер.

Таким образом, вы можете поставить перед собой одну из трех целей (или все три сразу!) и достичь поставленной цели, решив описываемую задачу.

Подготовка к соединению

Один из компьютеров, тот, к которому будем подключаться, назовем *сервером*, второй, с которого будем подключаться, — *клиентом*. Оба компьютера подключены к телефонной линии через модемы. Для установки связи между компьютерами необходимо, чтобы клиент позвонил на номер компьютера-сервера, а модем сервера в свою очередь "поднял трубку" и проверил имя и пароль звонящего пользователя. Если выполнение всех перечисленных операций прошло без ошибок, то соединение состоится. А если нет, то вы где-то допустили ошибку.

Настройка сервера

Компьютер-сервер, как мы уже выяснили, должен "ответить" на звонок клиента, для этого его нужно правильно настроить. Как это делается? А очень просто!

По следующей инструкции:

1. Если у вас меню **Пуск** в стиле Windows XP, то выполните следующие действия: **Пуск | Панель управления | Сетевые подключения | Создание нового подключения**. Если меню **Пуск** в классическом стиле, то: **Пуск | Настройка | Панель управления | Сетевые подключения | Создание нового подключения**.

   После выполнения указанных действий запустится мастер новых подключений. Нажмите кнопку **Далее**. Потребуется отметить указанные далее опции.

2. Выберите переключатель **Установить прямое подключение к другому компьютеру** и нажмите кнопку **Далее**.

3. Выберите переключатель **Принимать входящие подключения** и нажмите кнопку **Далее**.

4. Выберите ваш модем и нажмите кнопку **Далее**.

5. Отметьте флажок **Разрешить виртуальные частные подключения** и нажмите кнопку **Далее**.

6. В следующем окне — **Разрешения пользователей** — у вас есть несколько вариантов продолжения настройки, рассмотрим их все по порядку.

   - Вариант первый — выбрать из предлагаемого списка пользователей уже существующую учетную запись. Этот вариант приемлем, если на компьютере-сервере несколько учетных записей и клиент знает к одной из них имя входа и пароль. Такое бывает в тех случаях, когда клиент, к примеру, подключается из дома к своему рабочему месту.

   - Вариант второй — заранее создать пользователя для подключения.

     Для создания учетной записи входим в **Панель управления | Учетные записи пользователей | Создание учетной записи** и вводим имя новой учетной записи (оно же и имя нового пользователя). Тип учетной записи напрямую зависит от ее назначения. Учетная запись с правами администратора предназначена для опытных пользователей и, само собой, администраторов компьютера. Пользователь с правами

администратора может выполнять любые действия на компьютере. Пользователь с ограниченной учетной записью может изменять непосредственно свою учетную запись и окружающую его обстановку, но он не может повлиять на систему в целом.

Теперь следует разрешить новому пользователю вход через входящие подключения или включить его в уже созданное (в свойствах подключения).

Этот вариант подходит, если подключения будут производиться часто, и клиент хочет иметь на компьютере-сервере какие-либо права и собственные файлы.

- Вариант третий — создать нового пользователя здесь же. Для этого нажмите кнопку **Добавить** и заполните форму.
- И последний вариант — это выбрать учетную запись гостя. Этот вариант подходит тем, кто просто хочет поиграть с другом и не на что более не претендует.

  В свойствах учетной записи пользователя можно выбрать для него пароль или оставить его пустым (что и делается по умолчанию).

После того как вы определились с подходящим для вас вариантом, нажмите кнопку **Далее**.

7. В свойствах **Протокол Интернета (TCP/IP)** заранее установите IP-адреса для каждого компьютера.

   По умолчанию IP-адрес выделяется автоматически, т. е. каждый раз при новом подключении он может меняться. Но если отметить параметр **Указывать адреса TCP/IP явным образом**, то эта проблема исчезнет. Итак отмечаем указанный ранее параметр и в поле **С:** пишем что-то вроде `125.125.125.125`, а в поле **По:** — `125.125.125.126`. В итоге получаем два IP-адреса. Теперь IP-адрес сервера всегда будет 125.125.125.125, а IP-адрес клиента — 125.125.125.126.

   Вы можете назначить серверу и клиенту и другие IP-адреса по своему выбору.

8. Нажмите кнопку **Далее**.

А дальше-то и некуда. Все готово! Вот мы и настроили сервер. Теперь он готов принять звонок от клиента.

Настройка клиента (вариант 1)

Компьютер-клиент должен дозвониться до сервера и пройти проверку имени и пароля, но для этого нужно правильно настроить сетевое подключение.

Итак, делаем все то же самое, что и при настройке сервера на прием звонка, но только до запуска мастера новых подключений. После запуска мастера нажмите кнопку **Далее**.

Есть два варианта продолжения настройки. В обоих вариантах следует отмечать опции, указанные далее.

Рассмотрим первый вариант.

1. Выбираем переключатель **Подключить к Интернету** и нажимаем кнопку **Далее**.
2. Выбираем переключатель **Установить подключение вручную**, нажимаем кнопку **Далее**.
3. Выбираем переключатель **Через обычный модем** и нажимаем кнопку **Далее**.
4. **Имя поставщика услуг** вписываем любое (чтобы запомнить) и нажимаем кнопку **Далее**.
5. **Номер телефона** указываем тот, к которому подключен модем компьютера-сервера. Нажимаем кнопку **Далее**.
6. Теперь заполняем форму, вводим имя пользователя и пароль, которые мы указали в настройках сервера.

Вот и все! Настройка подключения по первому варианту завершена!

Настройка клиента (вариант 2)

Второй вариант не очень отличается от первого, но мы его все же рассмотрим. Описание начинаем с того места, где вы запустили мастер новых подключений. Нажмите кнопку **Далее**.

1. Теперь выбираем переключатель **Подключить к сети на рабочем месте** и нажимаем кнопку **Далее**.
2. Выбираем переключатель **Подключение удаленного доступа** и нажимаем кнопку **Далее**.

3. В поле **Организация** вводим любое понравившееся вам название. Нажимаем кнопку **Далее**.
4. **Номер телефона** указываем тот, к которому подключен модем компьютера-сервера. Нажимаем кнопку **Далее**.

Готово!

> ***Замечание***
>
> Обратите внимание на то, что имя и пароль пользователя мы не указывали. Их необходимо указать непосредственно перед звонком.

Возможные неполадки

Если модем компьютера-сервера не отвечает на звонок клиента, то, скорее всего, причину стоит искать в настройках модема и еще попробовать отключить из линии все телефоны.

Если модем клиента, начиная дозвон, "поднимает трубку" и не набирает номер, то стоит попробовать в настройках модема отключить опцию **Дождаться сигнала "линия свободна"**.

Бывает, что при подключении к серверу не удается пройти регистрацию. Сервер не узнает пользователя или пароль. В этом случае можно создать на нем подключение, аналогичное клиентскому, и запустить мастер настройки домашний сети или сети малого офиса, тот же мастер нужно запустить на компьютере-клиенте.

Соединяем компьютеры через Интернет

Вы спросите: зачем? Что ж, возможно, что у вас такой необходимости еще не возникало. Но многие администраторы сетей имеют возможность работать со своей сетью издалека. Зачем ехать для решения проблемы через многие километры, когда можно просто подключиться к сети через Интернет. Конечно, одно важное условие должно выполняться — и ваш компьютер, и сеть должны быть подключены к Интернету. Причем, желательно, чтобы сеть была подключена к Интернету всегда.

Но, возможно, вас заинтересует другой случай. Вы по ICQ или по e-mail договариваетесь о времени подключения и, имея обычные модемы, объединяете ваши компьютеры в маленькую локальную сеть, несмотря на расстояние, которое их разделяет.

> ***Примечание***
>
> Обратите внимание, что речь идет не об удаленном доступе к рабочему столу, а об объединении удаленных компьютеров в сеть.

Вообще говоря, вариантов для объединения компьютеров в сеть в Интернете много. Есть очень сложные способы, есть попроще, но совсем простых не существует. Нередко такую услугу предлагают интернет-провайдеры. Но нас интересует максимально простой способ.

Поиск компьютера в Интернете

Прежде всего, следует обратить внимание на то, что поиск компьютера в Интернете может оказаться непростым делом. Большинство провайдеров выдают выходящим в Интернет машинам динамические IP-адреса, которые меняются при каждом новом подключении. Это затрудняет подключение к такому компьютеру. Но не делает невозможным. Помощь можно получить от имеющихся в Интернете сервисов, которые позволяют определить текущий IP-адрес компьютера и найти его по символьному имени. Один из самых удобных сервисов такого рода можно найти по адресу **http://dyndns.org** или **http://www.dyndns.com**.

Подробное описание сервиса на русском языке есть по адресу **http://zyxel.ru/content/support/knowledgebase/KB-1257**.

Остается найти средство, позволяющее создать сетевое соединение через Интернет.

OpenVPN

По собственному опыту могу утверждать, что в данном случае лучше всего подойдет пакет OpenVPN (**http://openvpn.net/download.html**), все версии и варианты системы для скачивания можно найти на странице **http://openvpn.net/beta/**.

К сожалению, мне не удалось найти в Интернете лаконичное описание настройки этой программы для двух компьютеров под управлением Windows. Создана была эта программа как кроссплатформенная, и применяется она по большей части в мире Linux. Тем не менее ее с успехом можно применять для Windows-систем. Приведу здесь собственное описание настройки сети из двух компьютеров, "протянутой" через Интернет. Описание построено на основе материалов с сайта проекта OpenVPN и собственных экспериментов, которые завершились созданием постоянно действующего соединения двух компьютеров. Операционная система для обеих машин должна быть не ниже Windows 2000. Реально опробована работа сети, соответствующей описанию, на Windows XP и Windows Server 2003.

Серверная и клиентская части программы ничем не отличаются, кроме нескольких строчек в файле конфигурации программы. После установки программы на компьютере появляется виртуальный сетевой адаптер. Для нового адаптера автоматически создается и новое подключение, которое следует сразу переименовать в короткое и понятное имя, так как в файлах конфигурации программы OpenVPN нужно указать имя этого подключения. При этом программа работает в режиме командной строки, где короткие имена предпочтительны.

Файлы конфигурации для сервера и клиента в самом простом варианте приведены в листингах 4.1 и 4.2.

Листинг 4.1. Local.ovpn — файл конфигурации для клиента OpenVPN

```
# Имя компьютера, к которому осуществляем доступ.
# Приведен пример имени, созданного при использовании сервиса DynDNS
remote myserver.homeip.net
# Порт, через который осуществляется связь (любой свободный)
port 35000
# Указание на роль компьютера в VPN
proto tcp-client
dev tap
ifconfig 192.168.116.2 255.255.255.0
# Имя подключения
dev-node vpn
secret key.txt
ping-restart 60
ping-timer-rem
```

```
persist-key
resolv-retry 86400
ping 10
comp-lzo
verb 4
mute 10
```

Листинг 4.2. Server.ovpn — файл конфигурации для сервера OpenVPN

```
port 35000
proto tcp-server
dev tap
ifconfig 192.168.116.1 255.255.255.0
dev-node vpn
secret key.txt
ping 10
comp-lzo
verb 4
mute 10
```

В обоих файлах `vpn` — это имя сетевого подключения (`dev-node`). Сетевые подключения настройки не требуют, их параметры устанавливаются самой программой. Так в клиентском файле есть строка:

```
ifconfig 192.168.116.2 255.255.255.0
```

Эта строка устанавливает IP-адрес для подключения `vpn` 192.168.116.2, а маску подсети — 255.255.255.0. Файлы должны иметь расширение ovpn. При этом в контекстном меню данных файлов появится пункт **Start OpenVPN on this config file** (Запустить OpenVPN с этим файлом конфигурации).

Для того чтобы организация виртуальной частной сети была возможной, необходимо, чтобы со стороны удаленного компьютера можно было выполнить `ping` по адресу сервера, к которому делается попытка подключения. В локальном файле конфигурации указывается имя сервера (параметр `remote`). Связь имени и IP-адреса должна быть обеспечена любым из доступных способов.

OpenVPN-сервер, запущенный на сервере сети, ожидает попыток подключения извне. При удачной попытке сетевое подключение **VPN** активизируется.

OpenVPN-клиент после запуска предпринимает попытки определить доступность сервера по его имени. Как только сервер обнаружен, создается канал связи через виртуальные сетевые адаптеры.

Для обеспечения защищенности этого канала применяется шифрование. Для того чтобы сервер мог определить "своего" при подключении, применяется файл ключа (key.txt), который должен быть сформирован средствами самой программы с помощью пункта меню **Generate a static OpenVPN key** (Создать статический ключ) на одном из компьютеров и передан на другой любым доступным способом. Важно, чтобы на обеих машинах были копии одного и того же файла. Кроме того, связь осуществляется через выбранный вами порт, номер которого указывается в файлах конфигурации (параметр `port`).

Как серверная, так и клиентская части не имеют графического интерфейса. Работа программы видна в текстовом окне, в котором выводятся все сообщения о действиях и состоянии программы. Признаком установившегося соединения является сообщение, содержащее строку "Initialization Sequence Completed" ("Процедура инициализации завершена").

Сообщение клиентской программы "mute triggered" обозначает, что попытки связи неудачны, и программа ожидает изменений в настройках. При установившейся связи в сетевом окружении удаленного компьютера появится сервер (если компьютеры имеют одинаковое имя рабочей группы или домена). Для входа на него потребуется ввести имя пользователя и пароль учетной записи, имеющейся на сервере.

Если вход в локальную сеть защищен брандмауэром, то должен быть разрешен доступ к файлам и принтерам через виртуальный интерфейс, а основной интерфейс должен быть доступен для команды `ping`. Для этого следует включить параметр протокола ICMP (Internet Control Message Protocol, протокол управляющих сообщений Интернета) **Запрос входящего эха** для обеспечения возможности ответов компьютера на команду `ping` по его адресу. Настройки этого протокола доступны в дополнительных параметрах брандмауэра в ОС Windows XP и Windows Server 2003.

Можно обеспечить несколько подключений к серверу, запустив на нем несколько экземпляров OpenVPN-сервера. Каждый из экземпляров должен быть связан со своим виртуальным сетевым подключением. Виртуальные подключения могут создаваться средствами OpenVPN в любом необходимом количестве. Это позволяет для каждого подключения применять свой ключевой файл, что повышает защищенность сети.

Защищенный канал связи, создаваемый в Интернете, работает через порт, который мы зададим в файлах конфигурации OpenVPN, этот порт должен быть открыт. В примере показано применение порта 35 000, но можно выбрать любое значение, неиспользуемое на вашем сервере. Если есть сомнения в том, что выбранный вами порт открыт на каком-либо участке предполагаемого канала, его можно изменить.

На рабочей станции обычно специальных настроек не требуется. Должна быть установлена программа OpenVPN, а в папку с конфигурационными файлами программы, помещены файл конфигурации клиента и секретный ключ.

На рабочей станции устанавливаем соединение с Интернетом через обычный модем и запускаем OpenVPN с использованием локального (клиентского) файла конфигурации, программа делает несколько попыток соединения, и, если все настроено верно, соединение устанавливается. Вы можете определить момент установки соединения по сообщению "Initialization Sequence Completed" ("Процедура инициализации завершена"). В противном случае проверяем настройки и качество соединения.

После установления соединения VPN откройте сетевое окружение на рабочей станции. Вы должны увидеть компьютер, к которому производилось подключение.

Если вместо сообщения "Initialization Sequence Completed" на экране будет появляться "Initialization Sequence Completed with Errors" ("Процедура инициализации завершена с ошибками"), то работа с сетевыми ресурсами может быть затруднена или невозможна. В этом случае следует проверить качество соединения и правильность настроек.

Если вам удалось настроить OpenVPN и получить доступ к удаленному компьютеру, то при желании вы можете запустить службу OpenVPN, которая появилась в перечне служб операционной системы после установки программы. Теперь связь будет устанавливаться автоматически при каждом совместном выходе в Интернет обоих компьютеров.

Число подключений, созданных с помощью OpenVPN, может быть практически любым. Потребуется только создать необходимое число виртуальных сетевых адаптеров, а затем запускать соответствующее количество экземпляров программы.

Один экземпляр программы может обслужить одну пару компьютеров.

Воспользовавшись приведенными рекомендациями, можно создать маленькую сеть, не прокладывая сетевой кабель и не заботясь о соблюдении предельного расстояния между компьютерами.

Модем

Этот материал поможет вам более сознательно подойти к выбору оборудования, от которого во многом зависит качество связи по телефонной линии, а также качество работы в Интернете. Учитывая, что предполагается коллективный доступ к Интернету, а также доступ к сети извне по телефонной линии, модем становится одним из важнейших элементов сети. Знание принципов его работы и технологий, применяемых для модемных соединений, поможет выбрать модем и настроить его для конкретных условий работы в вашей сети.

Принципы работы модема

Необходимость организации соединения между удаленными компьютерами без прокладки дорогостоящих специальных линий связи заставила разработчиков коммуникационного оборудования создать модем (модулятор/демодулятор), устройство, которое может преобразовать на передающем конце дискретный сигнал в аналоговый, а на приемном произвести обратное преобразование.

Чтобы модемы могли обмениваться друг с другом информацией, их способы преобразования цифровых данных в аналоговые и обратно должны быть одинаковыми, т. е. модемы должны применять одинаковые способы модуляции и демодуляции сигналов. Чтобы все модемы, производимые различными фирмами, могли соединяться друг с другом, было решено определить ряд рекомендаций, которым они должны соответствовать.

Для разработки стандартов передачи данных был создан специальный Международный консультативный комитет по телефонии и телеграфии (International Consultative Committee for Telegraphy and Telephony, CCITT).

Модем обменивается данными с компьютером через последовательные порты (COM). Данные передаются последовательно бит за битом. Скорость, с которой происходит этот обмен, измеряется в битах в секунду — бит/с. Обычно на байт полезной информации передается два служебных бита. Очень приблизительно реальную скорость передачи информации можно определить, разделив скорость передачи данных на десять. Реальная скорость передачи информации будет зависеть от качества телефонного канала, алгоритма сжатия, а также многих других факторов. Скорость в бодах определя-

ется числом изменений сигнала, передаваемого модемом по телефонной линии, произошедших за одну секунду.

Для модуляции сигнала обычно используются методы, перечисленные далее.

- Метод амплитудной модуляции.

  Наименее эффективный метод модуляции, при котором информация кодируется за счет изменения амплитуды передаваемого сигнала. Применяется только на очень маленьких скоростях — до 100 бит/с.

- Метод частотной модуляции.

  Информация кодируется за счет изменения частоты передаваемого сигнала. Применяется на скоростях до 1200 бит/с. При частотной модуляции (FSK, Frequency Shift Keying) значениям 0 и 1 информационного бита соответствуют свои частоты физического сигнала при неизменной его амплитуде. Частотная модуляция весьма помехоустойчива, поскольку искажению при помехах подвергается в основном амплитуда сигнала, а не частота. При этом достоверность демодуляции, а значит, и помехоустойчивость тем выше, чем больше периодов сигнала попадает в "бодовый" интервал. Но увеличение этого интервала по понятным причинам снижает скорость передачи информации. С другой стороны, необходимая для этого вида модуляции ширина спектра сигнала может быть значительно у́же всей полосы канала. Отсюда вытекает область применения FSK — низкоскоростных, но высоконадежных стандартов, позволяющих осуществлять связь на каналах с большими искажениями амплитудно-частотной характеристики или даже с усеченной полосой пропускания.

- Метод фазовой модуляции.

  Применяется на скоростях до 4800 бит/с. Информация кодируется за счет изменения фазы передаваемого сигнала. При фазоразностной модуляции (DPSK, Differential Phase Shift Keying) изменяемым в зависимости от значения информационного элемента параметром является фаза сигнала при неизменных амплитуде и частоте. При этом каждому информационному элементу ставится в соответствие не абсолютное значение фазы, а ее изменение относительно предыдущего значения. Если информационный элемент двухбитовый (дибит), то в зависимости от его значения (00, 01, 10 или 11) фаза сигнала может измениться на 90, 180, 270 градусов или не измениться вовсе. Из теории информации известно, что фазовая модуляция наиболее информативна, однако увеличение числа кодируемых битов выше 3 (8 позиций поворота фазы) приводит к резкому снижению поме-

хоустойчивости. Поэтому на высоких скоростях применяются комбинированные амплитудно-фазовые методы модуляции.

- Метод квадратурно-амплитудной модуляции (Quadrature Amplitude Modulation, QAM).

  Здесь помимо изменения фазы сигнала используется манипуляция его амплитудой, что позволяет увеличивать число кодируемых битов. В настоящее время используются модуляции, в которых количество кодируемых на одном "бодовом" интервале информационных битов может доходить до 8, а, соответственно, число позиций сигнала в сигнальном пространстве — до 256. Однако применение многоточечной QAM в чистом виде сталкивается с серьезными проблемами, связанными с недостаточной помехоустойчивостью кодирования. Поэтому во всех современных высокоскоростных протоколах используется разновидность этого вида модуляции, так называемая модуляция с решетчатым кодированием, или треллис-кодированием (Trellis Coded Modulation, TCM), которая позволяет повысить помехозащищенность передачи информации — снизить требования к отношению сигнал/шум в канале на величину от 3 до 6 дБ. Суть этого кодирования заключается во введении избыточности. Пространство сигналов расширяется вдвое путем добавления к информационным битам еще одного, который образуется посредством сверточного кодирования над частью информационных битов и введения элементов запаздывания. Расширенная таким образом группа подвергается все той же многопозиционной амплитудно-фазовой модуляции. В процессе демодуляции принятого сигнала производится его декодирование по весьма изощренному алгоритму Виттерби, позволяющему за счет введенной избыточности и знания предыстории выбрать по критерию максимального правдоподобия из сигнального пространства наиболее достоверную точку и тем самым определить значения информационных битов.

Все современные модемы обеспечивают при передаче информации по телефонным линиям автоматическую коррекцию ошибок и компрессию данных. Это позволяет резко повысить качество связи и скорость передачи информации.

При передаче данных по зашумленным телефонным линиям существует большая вероятность, что данные, переданные одним модемом, будут приняты другим модемом в искаженном виде.

Общая форма передачи данных по протоколам с коррекцией ошибок следующая: модем передает данные отдельными блоками по 16—20 000 байт, в зависимости от качества связи. Каждый блок снабжается заголовком, в ко-

тором указана проверочная информация, например контрольная сумма блока. Принимающий модем самостоятельно подсчитывает контрольную сумму каждого блока и сравнивает ее с контрольной суммой из заголовка блока. Если эти две контрольные суммы совпали, то считается, что блок принят без ошибок. В противном случае принимающий модем отсылает передающему модему запрос на повторную передачу этого блока. Передача сбойного блока продолжается до тех пор, пока он не будет принят правильно.

Протоколы коррекции ошибок могут быть реализованы как на аппаратном, так и на программном уровне. Аппаратный уровень реализации эффективнее. Современные модемы для ускорения передачи данных используют специальные протоколы, позволяющие производить сжатие передаваемой информации. Передающий модем сжимает данные, они в сжатом виде проходят через телефонный канал и принимаются удаленным модемом, который производит их восстановление и дальнейшую передачу компьютеру.

При использовании модемов с аппаратной поддержкой протоколов сжатия информации следует установить скорость работы COM-порта, к которому подключен модем, выше скорости работы модема.

Модем может работать в двух основных режимах — командном режиме и режиме обмена данными. В режиме обмена данными он может принимать и передавать данные между компьютером и удаленным модемом. При этом компьютер принимает и передает данные от модема через асинхронный порт, на котором установлен модем.

В командном режиме можно передавать модему команды, управляющие его работой. Компьютер передает модему команды через COM-порт точно так же, как данные для обмена с удаленным модемом.

При помощи команд можно изменять характеристики обмена данными, изменять условия связи, записывать и считывать данные из внутренних регистров модема. В этих регистрах хранятся различные числовые параметры, определяющие временные и некоторые другие характеристики работы модема.

Сразу после включения питания модем находится в командном режиме. Переключение из командного режима в режим обмена данными осуществляется в следующих случаях:

- при удавшейся попытке установления связи с другим модемом;
- при выполнении модемом процедур самотестирования.

Переход из режима передачи данных в командный режим происходит:

- после неудачной попытки связаться с удаленным модемом, например, когда модемы не смогли согласовать общий протокол обмена данными. Обычно это происходит при плохом качестве связи;
- при потере несущей во время передачи данных. Причиной потери несущей может быть плохое качество связи, повреждение линии связи, "зависание" удаленного модема;
- при поступлении модему от компьютера команды в момент набора модемом номера;
- при передаче от компьютера модему специальной Escape-последовательности.

Модемы с аппаратной коррекцией ошибок обеспечивают нижеприведенные режимы передачи данных.

- *Стандартный режим.* Обеспечивает буферизацию данных, что позволяет работать с различными скоростями передачи данных между компьютером и модемом и между двумя модемами. В результате для повышения эффективности передачи данных можно установить скорость обмена компьютер — модем выше, чем модем — модем. В стандартном режиме работы модем не выполняет аппаратной коррекции ошибок.
- *Режим прямой передачи.* Данный режим соответствует режиму обычного модема. Передаваемые данные не буферизуются, аппаратная коррекция ошибок не выполняется.
- *Режим с коррекцией ошибок и буферизацией.* Это стандартный режим при связи двух модемов, поддерживающих коррекцию ошибок. Если удаленный модем не поддерживает коррекцию ошибок, связь не устанавливается и модем освобождает телефонную линию.
- *Режим с коррекцией ошибок и автоматической настройкой.* Используется, если заранее неизвестно, поддерживает ли удаленный модем протоколы MNP, CCITT V.32, CCITT V.32bis и др. В начале сеанса связи, после определения режима удаленного модема, устанавливается один из трех описанных ранее режимов.

Внутренние и внешние модемы

Модем может быть выполнен в виде платы расширения, устанавливаемой внутри компьютера, подобно любым другим платам расширения (рис. 4.3),

или как отдельное устройство, подсоединяемое к компьютеру через последовательный порт (рис. 4.4).

Работают оба типа модемов одинаково, а различия заключаются в следующем:

- внешние модемы являются более мобильными, чем внутренние. Внешний модем легко можно отсоединить от одного компьютера и подключить к другому (для этого нужно переключить только один разъем);
- внутренний модем увеличивает нагрузку на блок питания компьютера. Внешний модем имеет отдельный блок питания;

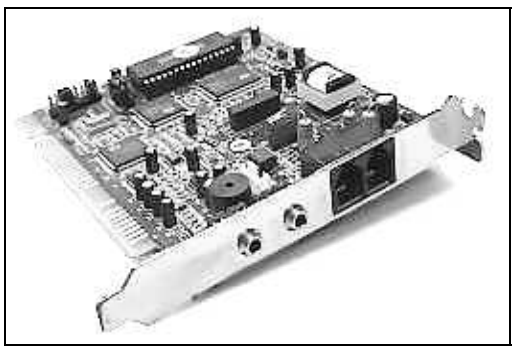


Рис. 4.3. Внутренний модем

Рис. 4.4. Внешний модем

- большинство внешних модемов имеют на лицевой панели несколько световых индикаторов. По ним можно в любой момент времени определить состояние модема: включен ли он, производит ли он передачу или прием данных и т. д.;
- модемы имеют обыкновение время от времени "зависать". Для вывода модема из этого состояния надо выполнить его перезагрузку, иными словами, произвести выключение и включение модема (в случае внутреннего модема потребуется перезагрузка компьютера). При наличии внешнего модема эта операция займет приблизительно 1 с, в то же время при наличии внутреннего модема, работающего под такой операционной системой, как Windows NT, на перезагрузку модема может понадобиться до 5 мин.

Из представленных в настоящее время на российском рынке модемов рекомендуют выбирать внешние модемы компании USRobotics — Courier, адаптированные под российские телефонные линии.

Протоколы

- **V.21**

  Это дуплексный протокол с частотным разделением каналов и частотной модуляцией FSK. На нижнем канале (его обычно использует для передачи вызывающий модем) "1" передается частотой 980 Гц, а "0" — 1180 Гц. На верхнем канале (передает отвечающий) "1" передается частотой 1650 Гц, а "0" — 1850 Гц. Модуляционная и информационная скорости равны 300 бод и 300 бит/с соответственно. Несмотря на невысокую скорость, данный протокол находит применение, прежде всего, в качестве "аварийного", при невозможности вследствие высокого уровня помех использовать другие протоколы физического уровня. Кроме того, ввиду своей неприхотливости и помехоустойчивости, он используется в специальных высокоуровневых приложениях, требующих высокой надежности передачи. Например, при установке соединения между модемами по новой рекомендации V.8 или для передачи управляющих команд при факсимильной связи (верхний канал).

- **V.22**

  Это дуплексный протокол с частотным разделением каналов и модуляцией DPSK. Несущая частота нижнего канала (передает вызывающий) — 1200 Гц, верхнего (передает отвечающий) — 2400 Гц. Модуляционная скорость — 600 бод. Имеет режимы двухпозиционной (кодируется бит) и четырехпозиционной (дибит) фазоразностной модуляции с фазовым расстоянием между точками, равным 180° и 90°. Соответственно, информационная скорость может быть 600 или 1200 бит/с. Этот протокол фактически поглощен протоколом V.22bis.

- **V.22bis**

  Это дуплексный протокол с частотным разделением каналов и модуляцией QAM. Несущая частота нижнего канала (передает вызывающий) — 1200 Гц, верхнего — 2400 Гц. Модуляционная скорость — 600 бод. Имеет режимы четырехпозиционной (кодируется дибит) и шестнадцатипозиционной (кодируется квадробит) квадратурной амплитудной модуляции. Соответственно, информационная скорость может быть 1200 или 2400 бит/с. Режим 1200 бит/с полностью совместим с V.22, несмотря на другой тип модуляции. Дело в том, что первые два бита в режиме 16-QAM (квадробит) определяют изменение фазового квадранта относительно предыдущего сигнального элемента и потому за амплитуду не отвечают, а последние два бита определяют положение сигнального

элемента внутри квадранта с вариацией амплитуды. Таким образом, DPSK можно рассматривать как частный случай QAM, где два последних бита не меняют своих значений. В результате из шестнадцати позиций выбираются четыре в разных квадрантах, но с одинаковым положением внутри квадранта, в том числе и с одинаковой амплитудой. Протокол V.22bis является стандартом де-факто для всех среднескоростных модемов.

- **V.32**

Это дуплексный протокол с эхо-подавлением и квадратурной амплитудной модуляцией или модуляцией с решетчатым кодированием. Частота несущего сигнала — 1800 Гц, модуляционная скорость — 2400 бод. Таким образом, используется спектр шириной от 600 до 3000 Гц. Имеет режимы двухпозиционной (бит), четырехпозиционной (дибит) и шестнадцатипозиционной (квадробит) QAM. Соответственно, информационная скорость может быть 2400, 4800 и 9600 бит/с. Кроме того, для скорости 9600 бит/с имеет место альтернативная модуляция — 32-позиционная TCM.

- **V.32bis**

Это дуплексный протокол с эхо-подавлением и модуляцией TCM. Используются те же, что в V.32, частота несущего сигнала — 1800 Гц и модуляционная скорость — 2400 бод. Имеет режимы 16-TCM, 32-TCM, 64-TCM и 128-TCM. Соответственно, информационная скорость может быть 7200, 9600, 12 000 и 14 400 бит/с. Режим 32-TCM полностью совместим с соответствующим режимом V.32. Протокол V.32bis является стандартом дефакто для всех скоростных модемов.

- **V.23**

Это полудуплексный протокол с частотной модуляцией FSK. В нем имеются два скоростных режима: 600 и 1200 бит/с. Модуляционная и информационная скорости равны 600 и 1200 бод соответственно. В обоих режимах "1" передается частотой 1300 Гц. В режиме 600 бит/с "0" передается частотой 1700 Гц, а в режиме 1200 бит/с — частотой 2100 Гц. Реализация протокола опционально может включать обратный канал, работающий на скорости 75 бит/с, что превращает протокол в асимметричный дуплексный. Частота передачи "1" в обратном канале — 390 Гц, "0" — 450 Гц. Этот протокол практически вышел из употребления в качестве стандартного протокола межмодемной связи, и далеко не всякий стандартный модем им оснащен. Однако он до сих пор остается базовым для реализации нестандартных модемов, получивших широкое распространение в нашей

стране (типа LEXAND). Видимо, благодаря простоте, высокой помехоустойчивости и приличной (по сравнению с V.21) скорости. Кроме того, в ряде европейских стран этот протокол применяется в информационной системе Videotex.

- **V.26, V.26bis, V.26ter**

Эти три протокола объединяет тип модуляции — DPSK, частота несущей — 1800 Гц и модуляционная скорость — 1200 бод. Разница между ними заключается в возможностях и способах обеспечения дуплексной связи и в информационной скорости. V.26 обеспечивает дуплекс только по четырехпроводной выделенной линии, V.26bis — это полудуплексный протокол, предназначенный для работы по двухпроводной коммутируемой линии, а V.26ter обеспечивает полный дуплекс с помощью технологии эхоподавления. Кроме того, первые два протокола могут быть асимметричными дуплексными, опционально включая обратный канал, работающий на скорости 75 бит/с в соответствии с V.23. Все три протокола обеспечивают скорость передачи информации 2400 бит/с посредством четырехпозиционной (дибит) DPSK. V.26bis и V.26ter, кроме того, имеют режим двухпозиционной (бит) DPSK, обеспечивая скорость 1200 бит/с.

- **V.33**

В этом протоколе используется модуляция с решетчатым кодированием TCM. Он предназначен для обеспечения дуплексной связи на четырехпроводных выделенных каналах. Имеет частоту несущего сигнала 1800 Гц и модуляционную скорость 2400 бод. Работает в режимах 64-TCM и 128-TCM. Соответственно, информационная скорость может быть 12 000 и 14 400 бит/с. Этот протокол очень напоминает V.32bis без эхо-подавления. Более того, если модем с протоколом V.33 установить на четырехпроводное окончание до дифференциальной системы АТС, то он вполне сможет связаться с удаленным модемом V.32bis, установленным на двухпроводной линии.

- **V.27ter**

В этом протоколе применяется фазоразностная модуляция с частотой несущего сигнала 1800 Гц. Могут использоваться два режима с разными информационными скоростями: 2400 и 4800 бит/с. Информационная скорость 2400 бит/с достигается модуляционной скоростью 1200 бод и кодированием дибита (4-позиционный DPSK), а 4800 бит/с — скоростью 1600 бод и кодированием трибита (8-позиционный DPSK). Стоит отметить, что существуют еще малоупотребительные модемные протоколы

данного семейства — V.27 и V.27bis, которые отличаются от V.27ter главным образом типом канала (выделенный четырехпроводный), для которого они предназначены.

- **V.29**

В этом протоколе применяется квадратурная амплитудная модуляция. Частота несущего сигнала — 1700 Гц, модуляционная скорость — 2400 бод. Имеет режимы 8-позиционной (трибит) и 16-позиционной (квадробит) QAM. Соответственно, информационная скорость может быть 7200 и 9600 бит/с.

- **V.17**

Этот протокол по своим параметрам очень напоминает V.32bis. В нем используется модуляция с решетчатым кодированием. Частота несущего сигнала — 1800 Гц и модуляционная скорость — 2400 бод. Имеет режимы 16-TCM, 32-TCM, 64-TCM и 128-TCM. Соответственно, информационная скорость может быть 7200, 9600, 12 000 и 14 400 бит/с.

- **V.32terbo**

Этот протокол, разработанный фирмой AT&T, является открытым для реализации разработчиками модемов. В частности, помимо БИС фирмы AT&T данный протокол реализован в некоторых модемах компании USRobotics. Протокол фактически является механическим развитием технологии V.32bis: дуплекс с эхо-подавлением, модуляция с решетчатым кодированием, модуляционная скорость — 2400 бод, несущая — 1800 Гц, расширение информационных скоростей значениями 16 800 и 19 200 бит/с за счет 256-TCM и 512-TCM. Следствием такого подхода являются весьма жесткие требования, предъявляемые данным протоколом к линии. Так, например, для устойчивой работы на скорости 19 200 бит/с отношение сигнал/шум должно быть не менее 30 дБ.

- **ZyX**

Протокол разработан фирмой ZyXEL Communications Corporation и реализован в ее собственных модемах. Этот протокол так же, как и V.32terbo, расширяет V.32bis значениями информационных скоростей 16 800 и 19 200 бит/с с сохранением технологии эхо-подавления, модуляции с решетчатым кодированием и несущей 1800 Гц. Модуляционная же скорость 2400 бод сохраняется лишь для информационной скорости 16 800 бит/с. Скорость 19 200 бит/с обеспечивается повышением модуляционной скорости до 2743 бод при сохранении режима модуляции 256-TCM для обеих скоростей. Такое решение позволяет снизить требование к отношению

сигнал/шум на линии на 2,4 дБ, однако расширение полосы пропускания может негативно сказываться при больших искажениях амплитудно-частотной характеристики канала.

- **HST**

Протокол HST (High Speed Technology) разработан компанией USRobotics и реализован в модемах серии Courier. Это асимметричный дуплексный протокол с частотным разделением каналов. Обратный канал имеет режимы 300 и 450 бит/с. Основной канал — 4800, 7200, 9600, 12 000, 14 400 и 16 800 бит/с. Применяется модуляция с решетчатым кодированием и модуляционной скоростью 2400 бод. Характеризуется сравнительной простотой и высокой помехоустойчивостью вследствие отсутствия необходимости в эхо-компенсации и отсутствия взаимовлияния каналов.

- **PEP, TurboPEP**

Полудуплексные протоколы семейства PEP (Packetized Ensemble Protocol) разработаны фирмой Telebit и реализованы в модемах фирмы серий TrailBlazer (PEP) и WorldBlazer (TurboPEP). По этим протоколам принципиально иным образом используется вся полоса пропускания канала тональной частоты для высокоскоростной передачи данных. Весь канал разбивается на множество узкополосных частотных подканалов, по каждому из которых независимо передается своя порция битов из общего потока информации. Такого рода протоколы называют многоканальными, или параллельными, или протоколами с множеством несущих (multicarrier). По протоколу PEP канал разбивается на 511 подканалов. В каждом подканале шириной около 6 Гц с модуляционной скоростью от 2 до 6 бод с помощью квадратурной амплитудной модуляции кодируются от 2 до 6 бит на бод. Есть несколько степеней свободы для обеспечения максимальной пропускной способности каждого конкретного канала, имеющего свои характеристики по части искажений и помеховой обстановки. В процессе установки соединения каждый частотный подканал независимо тестируется и определяется возможность его использования, а также параметры: модуляционная скорость подканала и число позиций модуляции. Максимальная скорость передачи по протоколу PEP может достигать 19 200 бит/с. В процессе сеанса при ухудшении помеховой обстановки параметры подканалов могут меняться, а некоторые подканалы — отключаться. При этом декремент понижения скорости не превышает 100 бит/с. Протокол TurboPEP за счет увеличения числа подканалов, а также количества кодируемых на одном бодовом интервале битов, может достигать

скорости 23 000 бит/с. Кроме того, в протоколе TurboPEP применяется модуляция с треллис-кодированием, что увеличивает помехоустойчивость протокола.

- **V.34**

Отличается от протокола V.32 тем, что по результатам тестирования линии связи вместо коррекции усиления на приемной стороне проводится коррекция АЧХ на передающей стороне путем дополнительного усиления затухающих в линии частотных полос. Этим достигается увеличение отношения сигнал/шум, которое существенно влияет на качество связи.

- **V.90**

По этому протоколу данные от модема к модему передаются с использованием разного вида преобразований. Информация от пользователя передается по протоколу V.32 или V.34, а обратно с применением цифрового преобразования, которое позволяет при соответствующем оборудовании у провайдера достичь скорости передачи данных 56 Кбит/с. Таким образом, скорость передачи в разных направлениях существенно отличается, что позволяет получать информацию большого объема за небольшие (по сравнению с работой обычных модемов) промежутки времени. При этом передача запросов, не требующая большого объема данных, происходит на обычных скоростях.

- **V.92**

Новый стандарт импульсно-кодовой модуляции для аналоговых модемов включает в себе три новые функции, повышающие производительность: увеличение скорости передачи данных (PCM Upstream), ускорение установки соединения (Quick Connect) и возможность перевода модемного соединения на режим ожидания вызова (Modem-on-Hold). PCM Upstream — увеличивает скорость передачи данных до 48 Кбит/с (для сравнения: модемы V.90 позволяли выгружать данные с максимальной скоростью 31,2 Кбит/с). При этом скорость загрузки остается прежней — 56 Кбит/с, но повышается скорость отправки факсимильных сообщений с 14,4 до 33,6 Кбит/с. Quick Connect — сокращает время установки соединения благодаря запоминанию модемом характеристик телефонной линии. Все это позволяет сократить обычное время установки соединения (около 30 с) до 10 с. Modem-on-Hold — позволяет модему прерывать соединение на некоторое время, одновременно оставаясь на линии — пока вы пользуетесь телефоном, получив специальный входящий голосовой вызов. Если вам необходимо срочно позвонить по телефону, когда линия занята модемом, вы

просто запускаете специальную программу, которая ставит ваш модем в режим ожидания, приостанавливая сеанс обмена данными между модемом и сервером.

Управление модемом

После выпуска американской фирмой Hayes модемов серии Smartmodem система команд, использованная в ней, стала стандартом, которого придерживаются остальные разработчики модемов. Система команд, примененная в этих модемах, носит название hayes-команд, или AT-команд. Со времени выпуска первых AT-совместимых модемов набор их команд дополнился и стал называться расширенным набором AT-команд. Подробное описание каждой команды можно найти в документации к модему.

Hayes-совместимые модемы имеют набор регистров, определяющих различные характеристики модема. Содержимое большинства этих регистров можно считывать и изменять программным способом. Для чтения и записи значений регистров модема можно использовать AT-команды: `ATS`*r* и `ATS`*r*`=`*n*, где *r* — номер регистра модема, а *n* — число, которое в него записывается. Описание каждого регистра (диапазон возможных значений, значение, записываемое в регистр по умолчанию, и т. д.) можно найти в документации на модем.

"Пообщаться" с модемом можно используя программу HyperTerminal.

В табл. 4.1 приведены стандартные Hayes-команды и регистры.

Таблица 4.1. *Стандартные Hayes-команды*

Команда	Значение
`A\`	Повтор последней введенной команды
`AT`	Префикс `AT` (от англ. *attention*) может быть общим для нескольких команд. Например, команды `ATE1` и `ATV1` можно ввести так: `ATE1V1`
`A`	Поднять трубку и ответить на входящий звонок. В некоторых модемах выполнение этой команды возможно, только если регистр S1 (счетчик входящих звонков) не равен 0
`D`	Набор номера и соединение с удаленным модемом. Формат команды D*xxxxxxxx*, где *x* — цифры номера

Таблица 4.1 *(продолжение)*

Команда	Значение
E	E1 — включить эхо, E0 — выключить эхо. В зависимости от этой команды модем возвращает в терминал посланные в модем символы
Q	Контролирует вывод результатов выполнения команд модемом. Q0 — результаты разрешены, Q1 — результаты запрещены
V	Контролирует вид выводимых результатов. V0 — числовые результаты (1, 0 и т. д.), V1 — текстовые результаты (OK, ERROR и т. д.)
S0	Переводит модем в режим автоматического ответа на звонок и указывает ему, после какого звонка "поднимать трубку"
S1	Подсчитывает и хранит число звонков входящего звонка (только для чтения)
S2	Хранит десятичный ASCII-код символа Escape-последовательности
S3	Хранит десятичный ASCII-код символа "возврат каретки"
S4	Хранит десятичный ASCII-код символа "перевод строки"
S5	Хранит десятичный ASCII-код символа "удаление предыдущего символа"
S6	Устанавливает, сколько времени модем ждет сигнала "диалтон" (сигнал готовности телефонной сети к приему сигналов набора номера) до набора номера
S7	Устанавливает, сколько времени модем "ждет несущей", прежде чем "положить трубку" и выдать "NO CARRIER"
S8	Устанавливает время ожидания по команде (,) в команде набора номера
S9	Время определения стабильного сигнала несущей вашим модемом
S10	Время, через которое модем отсоединится от линии после потери несущей
S11	Устанавливает длительности и задержки для тонального набора
S12	Устанавливает время ожидания нажатия следующего символа Escape-последовательности
S13	Битовый регистр

Таблица 4.1 *(окончание)*

Команда	Значение
S14	Зарезервирован
S15	Битовый регистр
S16	Битовый регистр
S17	Зарезервирован
S18	Время тестирования модема командами &T, по истечении этого времени модем сам закончит тестирование и прервет тест
S19	При отсутствии активности на линии по истечении этого времени модем разорвет соединение (S19=0 отменяет эту функцию)
S20	Зарезервирован
S21	Зарезервирован
S22	Хранит десятичный ASCII-код символа XON
S23	Хранит десятичный ASCII-код символа XOFF
S24	Зарезервирован
S25	Устанавливает время, в течение которого сигнал DTR должен быть опущен, чтобы модем определил это как потерю DTR
S26	Зарезервирован
S27	Битовый регистр

Запустив HyperTerminal и набрав ATE1, включим отображение набираемых команд. Набрав ATA, услышим гудок — сигнал из телефонной линии (модем должен быть подключен к телефонной линии), говорящий о том, что модем "поднял трубку". Чтобы "опустить трубку", необходимо нажать любую клавишу, гудок прекратится, а на экране появится сообщение "NO CARRIER" — соединение не удалось.

Знак $ используется для отображения перечня основных команд, а также для получения подсказки по любой команде. Перед командой, в том числе и перед символом $, должна быть набрана команда AT.

Более подробный перечень команд приводится в описании вашего модема. AT-команды позволяют программно управлять модемом. Некоторые про-

граммы требуют ввода строки инициализации, которая включает последовательность AT-команд, необходимых для начала работы модема.

Модемы и доступ к Интернету

Производители модемов предлагают все новые и новые решения для обеспечения стабильной и высокоскоростной связи:

- семейство технологий ADSL;
- многоканальные (сдвоенные и строенные) модемы;
- цифровая связь ISDN;
- радио-Ethernet;
- спутниковое вещание типа DirecPC.

Технология ADSL

Аббревиатура ADSL расшифровывается как Asymmetric Digital Subscriber Line — асимметричная цифровая абонентская линия. Эта технология позволяет поставщикам информационных услуг использовать все возможности имеющейся коммуникационной инфраструктуры и обеспечить высокоскоростной доступ к Интернету по обычным медным кабелям.

ADSL позволяет обмениваться большими объемами данных по телефонным линиям со скоростью до 6 Мбит/с. В силу асимметричности линий скорость обратной передачи данных — от клиента к провайдеру — не превышает 640 Кбит/с. Рассматриваемая технология ориентирована прежде всего на малые рабочие группы. Модем ADSL представляет собой устройство со встроенным сетевым адаптером Ethernet и интерфейсом 10Base-T, обеспечивающим возможность подключения к локальной сети. При наличии концентратора модемом без заметной задержки трафика могут пользоваться до 10 человек. В качестве среды информационного обмена используется витая пара. Разработчиком стандарта является фирма Motorola. Данная технология позволяет с минимальными затратами эффективно решать проблему "последней мили", обеспечивая высокоскоростной доступ к опорной сети интернет-провайдера.

Многоканальные модемы

На рынке оконечного коммуникационного оборудования (высокоскоростные решения, не выходящие за рамки традиционных модемных технологий) сформировалось новое направление: недорогие устройства, обеспечивающие передачу данных со скоростью выше 56 Кбит/с. Это модемы с параллельным информационным обменом, алгоритм работы которых предусматривает передачу данных по двум и более линиям одновременно. Например, в июле 1997 года компания Transend выпустила на рынок США модем Transend Sixty-Seven со скоростью передачи данных 67 Кбит/с, использующий две обычные телефонные линии (33,6 Кбит/с — по каждой), поддерживающий технологию Plug and Play и работающий в стандарте V.34. Другой пример, на выставке Comdex/Fall'97 компания Boca Research представила двухканальный модем, работающий по технологии 56К и обеспечивающий соединение со скоростью до 112 Кбит/с.

Технология ISDN

Описанные ранее технологии частично решают проблему повышения скорости обмена данными, но, оставаясь аналоговыми, не гарантируют их надежного приема/передачи. В качестве альтернативы выступает более дорогое решение, реализующее гарантированную высокоскоростную связь — цифровая связь с интеграцией услуг ISDN (Integrated Services Digital Network). Интеграция услуг предполагает, что данная технология позволяет передавать по цифровым телефонным линиям не только сетевой трафик, но и другие данные, например оцифрованные звук и видео. Реализованы дополнительные виды сервиса: распознавание типа сигнала (факс/модем/голос), получение вызова во время разговора с другим абонентом и т. п. Но особенно удобна ISDN именно для передачи данных. Слово "модем" в этом случае используется скорее по привычке, никакой модуляции/демодуляции здесь не происходит: цифровой сигнал от ПК до сервера провайдера Интернета не претерпевает ни одного преобразования, а следовательно, и не искажается. При этом пользователь имеет возможность выбирать между скоростью 128 и 64 Кбит/с с одновременным использованием второго канала для телефонных разговоров.

Устройства ISDN часто называют терминальными адаптерами. АТС типа ISDN соединяются с модемом по трем логическим каналам по стандарту BRI (интерфейс базового уровня). Данные передаются по двум каналам со скоростью 64 Кбит/с и затем коммутируются на АТС. Третий канал с пропускной способностью 16 Кбит/с является служебным, по нему согласуются протоколы связи

и осуществляется передача различной сервисной информации. В нашей стране развитие рассматриваемой технологии пока сдерживается ее высокой ценой.

Два dial-up-соединения

Как вы уже догадались, речь пойдет о работе двух модемов на одной машине. Один для связи с Интернетом, другой для обеспечения удаленного доступа к этому компьютеру. Польза от такого варианта подключения заметна, когда к серверу дотягиваются две телефонные линии. Одна из них может быть местного значения, и по ней может осуществляться связь компьютеров, другая — с выходом в город. Еще лучше, когда есть две городские линии. Одновременное использование двух dial-up-соединений требует установить на сервер кроме контроллера удаленного доступа адаптер виртуальной частной сети (рис. 4.5 и 4.6).

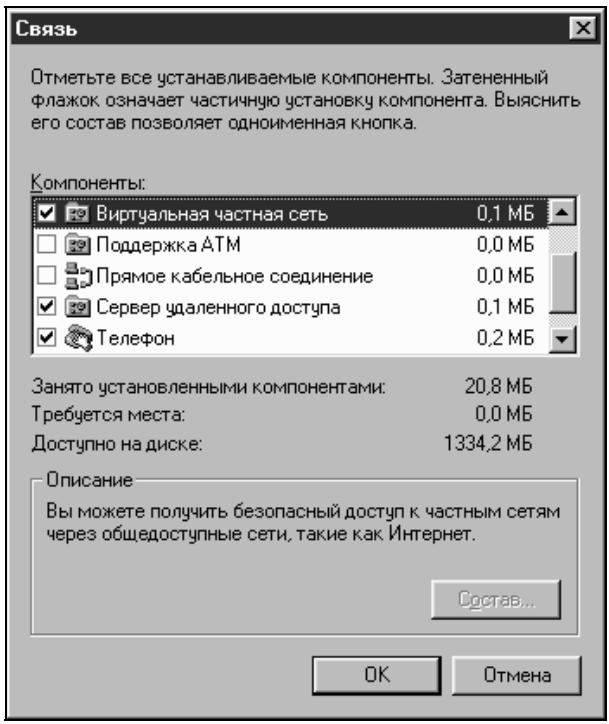


Рис. 4.5. Добавление поддержки виртуальной частной сети через установку Windows

После этих дополнений компьютер сможет одновременно использовать два модема. При недостатке внешних портов для подключения модемов один из них или оба могут быть внутренними.

Может случиться так, что после установки двух модемов вызываемый модем не будет отвечать на звонки. В этом случае необходимо в строку инициализации модема вписать `ATS0=1` (рис. 4.7). Для этого надо открыть **Панель управления | Система | Устройства | Модемы | <Ваш модем> | Свойства | Дополнительно**.

Настройки сервера удаленного доступа остаются по умолчанию. IP-адрес назначается автоматически (192.168.55.2 на стороне клиента и 192.168.55.1 на стороне сервера), но на всякий случай установите пароль на доступ к серверу. При этом разрешение на доступ удобнее включать автоматически с помощью ServerOK.

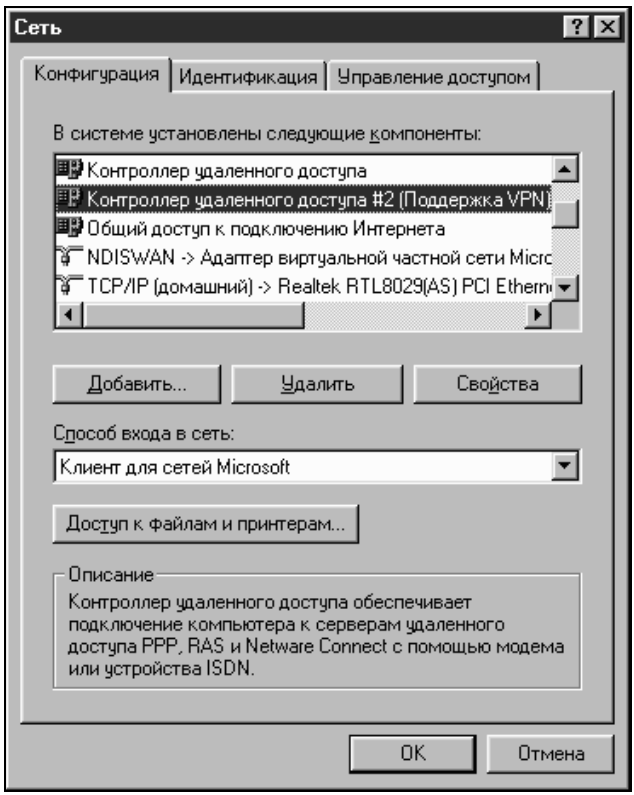


Рис. 4.6. В свойствах сети должен появиться контроллер удаленного доступа № 2

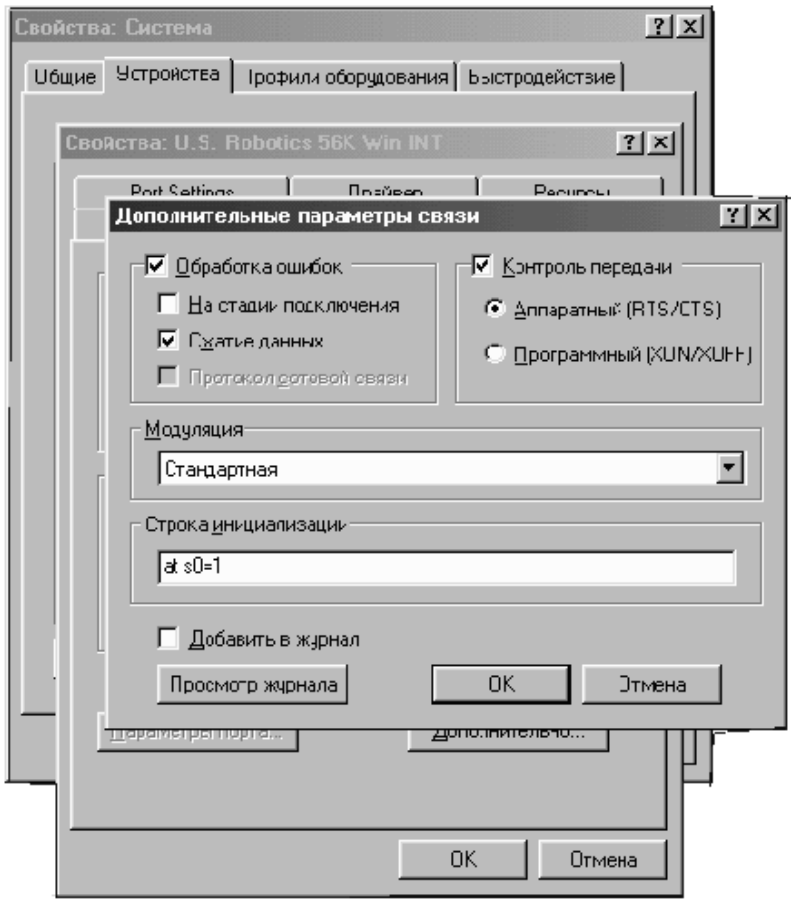


Рис. 4.7. Строка инициализации модема

Еще немного о маршрутизации

Открыв окно сеанса DOS и набрав команду `C:\WINDOWS>route print` в окне сеанса MS-DOS, можно получить таблицу маршрутов, определенную для данного компьютера (табл. 4.2).

Далее приводится расшифровка строк маршрутизации.

- Сетевой адрес:
  - 0.0.0.0 — маршрутизация (routing) по умолчанию;

- 127.0.0.0 — loopback-адрес (loopback — обратный);
- 157.57.11.169 — адрес сетевой карты;
- 157.57.255.255 — подсетевой "широковещательный" адрес;
- 224.0.0.0 — multicast-адрес (multicast — широковещательный);
- ограниченный подсетевой "широковещательный" адрес.

❒ Маска подсети определяет пространство IP-адресов, используемых при маршрутизации. Например, маска 255.255.255.255 позволяет использовать весь спектр IP-адресов.

❒ Адрес шлюза определяет направление пересылки пакетов. Им может быть адрес сетевой карты или маршрутизатора в сети.

❒ Интерфейс определяет сетевую плату, через которую идет посылка пакетов.

127.0.0.1 — программный loopback-адрес.

❒ Метрика — весовой коэффициент, определяет количество шагов для достижения заданной точки.

Таблица 4.2. *Активные маршруты*

Сетевой адрес	Маска	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	157.57.8.1	157.57.11.169	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
157.57.11.169	255.255.255.255	127.0.0.1	127.0.0.1	1
157.57.255.255	255.255.255.255	157.57.11.169	157.57.11.169	1
224.0.0.0	224.0.0.0	157.57.11.169	157.57.11.169	1
255.255.255.255	255.255.255.255	157.57.11.169	157.57.11.169	1

При включенной маршрутизации (изменение в реестре, рассмотренное в *главе 3*) можно добавить нужное число маршрутов для обеспечения комфортной работы с сетью. Тогда не придется для обнаружения требуемого ресурса использовать поиск, а все необходимое будет видно в сетевом окружении. Для всех машин подсетей, конечно, должны быть указаны шлюзы по умолчанию.

Удаленное управление и администрирование

Организовав доступ к любой машине вашей сети (или сетей), было бы разумно получить возможность удаленного управления сетевыми компьютерами. Удаленное управление сетевыми компьютерами позволяет:

- управлять сервером, не подходя к нему, даже находясь на значительном удалении от него;
- получать доступ к приложениям, установленным на удаленных компьютерах;
- совместно работать над одним документом, в одном приложении, в одно время, находясь на расстоянии от коллеги;
- организовывать систему помощи пользователям сети, непосредственно включаясь в их работу и корректируя их действия;
- получать удобный доступ к своему компьютеру, используя его рабочий стол на удаленной машине, при этом результаты работы (файлы) могут как оставаться на вашей машине, так и перемещаться или копироваться на удаленную;
- устанавливать постоянный контроль над несколькими машинами, находящимися в территориально удаленных местах, поместив изображения их экранов на экране вашей машины. При этом вы не будете мешать работе машин, над которыми установлен контроль, а на экране вашей машины можно разместить шесть-восемь экранов удаленных рабочих станций одновременно...

Каждый сможет продолжить этот список в соответствии со своими потребностями и желаниями. Что же требуется для обеспечения удаленного администрирования? Почти все мы уже сделали. К компьютеру должен быть доступ по протоколу TCP/IP. Кроме этого, нужна какая-либо из программ удаленного администрирования.

Программы удаленного администрирования

В настоящее время существует много таких программ, разработанных зарубежными и отечественными программистами.

Среди них можно выделить три продукта:

- RA (Remote Anything). Разработчик: компания TWD Industries. Размер файлов 520 Кбайт, PDF-руководство 780 Кбайт (**http://twd-industries.com**).
- PcAnywhere. Разработчик: компания Symantec. Размер файла 34,7 Мбайт.
- Radmin. Разработчик: компания "Фаматек". Размер файла 1,72 Мбайт (**www.radmin.com**).

Все три программы обладают в основном одинаковыми возможностями. Мы рассмотрим подробно работу последней из них. Наш выбор определен тем, что это:

- отечественная программа;
- относительно недорогая (1250 р.);
- ее пробная версия полнофункциональна и ограничена лишь временем использования;
- есть русскоязычная версия;
- в использовании чрезвычайно проста и понятна;
- работает в Windows 95/98/2000/2003/XP/Vista.

Radmin (Remote Administrator)

Программа позволит вам подключаться, не отходя от своего компьютера, к любому компьютеру сети для помощи пользователю или контроля правильности его работы, а также для дистанционной установки программного обеспечения и настройки клиентских машин. Ее применение требует наличия клиентской части на вашем компьютере и серверной — на удаленных. При этом вы видите экран удаленного компьютера на своем рабочем столе. Окно, в котором отображается экран удаленного компьютера, может быть полностью развернуто. А ваши мышь и клавиатура подменяют мышь и клавиатуру на удаленном компьютере, если управление осуществляется в полноэкранном режиме или окно удаленного экрана активно. Но можно и просто наблюдать за происходящим. Программа поддерживает LAN, WAN, а также соединение dial-up — модемное соединение через Интернет или с использованием сервера удаленного доступа, так как она не требует высокоскоростного соединения. При подключении через модем вы можете получить приемлемую частоту обновления экрана (около 5—10 обновлений экрана в секунду). При работе внутри локальной сети экран обновляется в режиме реального

времени (около 100—500 обновлений экрана в секунду). Иногда, используя Radmin в полноэкранном режиме, вы можете даже забывать, что работаете на удаленном компьютере!

Radmin состоит из двух частей:

- серверной части, которая генерирует изображение экрана;
- клиентской части (программа просмотра), которая постоянно отображает экран удаленного компьютера на экране вашего компьютера.

Для старта Radmin вы должны запустить сервер, а также установить соединение с помощью клиентской части (программы просмотра).

Возможности программы

Radmin-сервер может работать как сервис под Windows XP/2000/2003 и Windows 9*x*/ME, что позволяет вам выполнять команды: `logon` и `logoff` дистанционно, поддерживает одновременно несколько сессий дистанционного управления и просмотра на одном рабочем месте. Полноэкранный режим позволяет вам видеть экран удаленного компьютера во весь экран вашего компьютера, а масштабируемый режим — изменять размер окна-экрана удаленного компьютера.

Radmin использует *драйвер видеозахвата* для изменения экрана. Это позволяет вам работать на удаленном компьютере в режиме реального времени с потрясающей скоростью (сотни обновлений экрана в секунду), обмениваться файлами с удаленным компьютером и даже выключить компьютер дистанционно без необходимости соединения, в режиме просмотра. Radmin-сервер предоставляет Telnet-доступ к удаленному компьютеру, если этот сервер работает под Windows 2000 и более новой ОС семейства Windows. Вы можете разрешить удаленное управление, просмотр, обмен файлами, а также Telnet-доступ определенным пользователям или группам пользователей. Если пользователь принадлежит к домену Windows 2000/2003, то Radmin будет использовать текущие регистрационные данные (пользователь/пароль) для предоставления доступа к Radmin-серверу. Если система безопасности Windows 2000/2003 выключена, то доступ контролируется паролем. Radmin определяет пользователя методом "запрос-ответ", основанном на 128-битовом шифровании, которое применяется для всех передаваемых данных. Начиная с версии программы 2.1 шифрование невозможно отключить. IP-фильтр предоставляет доступ к Radmin-серверу только определенным IP-адресам и подсетям. Мак-

симальное разрешение экрана, поддерживаемое Radmin, до 2048×2048 при 32-битовом цвете.

Radmin требует соединения между серверной и клиентской частями по протоколу TCP/IP.

Системные требования

Программа работает даже на P386 с 8 Мбайт RAM под управлением Windows 95. Может работать без дисплея, мыши или клавиатуры. Для всех операционных систем (Windows 9*x*/ME/NT/2000/2003/XP/Vista) необходим установленный протокол TCP/IP. Один из серверов нашей сети с операционной системой Windows 2000 именно так и работает. Он применяется как архивное хранилище файлов и работать на нем в локальном режиме нет необходимости, но когда требуется изменить какие-либо настройки этого сервера или перезагрузить его, то достаточно удаленного подключения.

Установка

Для работы с Radmin вам необходимы два компьютера, соединенные через сеть. Установите протокол TCP/IP и Radmin на оба компьютера. Перед инсталляцией для всех пользователей деинсталлируйте предыдущие версии Radmin, если таковые присутствуют.

> ***Рекомендации для пользователей Windows 2000***
>
> Для установки сервиса Remote Administrator вы должны иметь права администратора.

1. Распакуйте установочные файлы.
2. Запустите rserv30ru.exe, чтобы установить Radmin Server, или rview30ru.exe, чтобы установить Radmin Viewer.
3. Следуйте инструкциям программы установки.

После установки программы вы можете запустить из меню **Пуск** серверную или клиентскую часть программы или команду **Установочная служба** из меню **Настройка сервера**, в котором можно настроить Radmin-сервер для автоматической загрузки при старте Windows, изменить пароль для сетевого доступа и выполнить другие настройки.

Установка соединения

1. Запустите Radmin-сервер на удаленном компьютере. При этом должен появиться значок Radmin-сервера на панели задач Windows.
2. Подведите мышь к значку — появится IP-адрес компьютера. Двойной щелчок кнопкой мыши по значку выводит на экран список текущих соединений. Значок может быть отключен в настройках Radmin-сервера.
3. На локальном компьютере запустите обозреватель Radmin Viewer.
4. Выберите из меню обозревателя **Соединение/Соединение с**.
5. В поле **IP адрес или имя DNS** введите IP-адрес (например, `10.0.0.1`) или DNS-имя (например, `comp1.company.com`) удаленного компьютера, на котором запущен Radmin-сервер.

Подключение "модем — модем"

Radmin не работает непосредственно с модемами. Для соединения "модем — модем" вы должны настроить удаленный доступ на клиенте и сервере. Протокол TCP/IP нужно установить на обоих компьютерах. На серверной стороне вы должны установить сервер удаленного доступа (это стандартный компонент для Windows 98 и компонент из MS Plus! для Windows 95), если вы используете Windows 9*x*, или же RAS (Remote Access Server — сервер удаленного доступа в Windows 2000/NT), если вы используете Windows 2000/NT. Кроме того, следует настроить сервер для работы с протоколом TCP/IP. На клиентской стороне вы также должны установить Контроллер удаленного доступа и настроить его на применение протокола TCP/IP. Далее нужно сделать звонок, используя соединение dial-up. После подключения вы можете найти IP-адрес удаленного сервера в свойствах подключения или в Мониторе подключения, находящемся на Панели управления. Используйте этот IP-адрес для подключения Radmin-клиента к удаленному серверу. Как правило, при данном типе соединения он равен 192.168.55.1. Если соединяемые компьютеры входят в локальные сети, то могут быть присвоены и другие адреса из диапазона 192.168.*X.X*.

Конечно, скорость соединения очень зависит от качества связи. Но, например, мне из дома удается контролировать некоторые долго идущие процессы в сети несмотря на то, что расстояние до сервера — 40 км.

Подключение через Интернет

Установить соединение через Интернет так же просто, как соединение "модем — модем". Единственная проблема заключается в том, что IP-адрес удаленного компьютера, на котором выполняется Radmin-сервер, не всегда известен до подключения. Он может назначаться провайдером (ISP) динамически или статически. В первом случае IP-адрес становится известен только после подключения к Интернету и необходимо каким-либо образом "передать" его на клиентскую сторону.

1. Установите Radmin на оба компьютера.
2. Запустите Radmin-сервер на удаленном компьютере.
3. Подключите удаленный компьютер к Интернету.
4. Любым способом получите информацию об IP-адресе компьютера, к которому вы хотите подключиться.
5. Подключите ваш компьютер к Интернету.
6. Запустите Radmin-клиент на локальном компьютере, выберите в меню **Соединение/Соединение с**, введите IP-адрес удаленного компьютера, который вам уже известен.

Соединение через прокси-сервер

Программа Radmin использует по умолчанию порт 4899 TCP. Вы можете открыть данный порт на вашем прокси-сервере. Другим решением этой проблемы является изменение номера порта (на обеих сторонах соединения) на уже открытый на вашем прокси-сервере. Если ваш прокси работает под управлением Windows, вы можете установить Radmin-сервер на этом же компьютере. Далее вы сможете подключаться, используя **Соединение через**. Сказанное ранее относится и к firewall/router (сетевой экран и маршрутизатор).

Иногда только firewall/router имеет "настоящий" IP-адрес. Сконфигурируйте маршрутизатор так, чтобы он перенаправлял соединения на сетевые интерфейсы компьютеров, находящихся в локальной сети (forwarding). После этого вы должны указывать IP-адрес маршрутизатора, для того чтобы подключиться к компьютеру во внутренней сети.

Если используется совместное интернет-соединение, входящее в Windows 98SE, обозреватель Radmin Viewer не найдет ваш сервер. Проблема

заключается в том, что порт должен быть открыт, чтобы обозреватель мог найти сервер. Далее приводится ссылка на программу, которая позволяет это делать: **www.practicallynetworked.com/sharing/ics.htm**.

Пример настроек TCP/IP для сегмента локальной сети

Для задания IP-адреса одного сегмента локальной сети в установках TCP/IP сетевой карты на первом компьютере введите IP-адрес: `10.0.0.1` (адреса этого типа часто применяют в одноранговых сетях) и сетевую маску: `255.255.255.0`.

На втором компьютере установите IP-адрес: `10.0.0.2`, сетевую маску: `255.255.255.0`.

Попробуйте выполнить следующую команду `ping` со второго компьютера:

```
ping 10.0.0.1
```

Если компьютеры сети получают адреса автоматически, то применяя программу SuperScan, которая будет описана в *разд. "SuperScan — программа для сканирования сетей" данной главы*, вы без труда определите адрес нужного вам компьютера. Можно использовать и команду `ping`.

Настройка Radmin-сервера

Log-файл. Все действия могут быть записаны в Log-файл из окна параметров настройки **Настройки** программы Remote Administrator.

IP-фильтр. Эти настройки позволят вам предоставлять доступ к Radmin-серверу только с определенного IP-адреса или подсети. Установить IP-фильтр можно, используя **Настройки** в меню **Настройка Remote Administrator Server** (доступно из меню **Пуск**).

Например:

подсеть 192.168.1.*xx*

компьютер 192.168.1.67

Для доступа к целой подсети установите:

фильтр IP — 192.168.1.0

маска — 255.255.255.0

Если IP-адрес и маска подсети не соответствуют фильтру IP, вы получите сообщение: "Client I/O error".

Установка/изменение пароля для Radmin-сервера. Вы можете установить или изменить пароль для Radmin-сервера непосредственно из меню **Настройка Remote Administrator Server**. При открытии соединения для ввода пароля будет появляться отдельное окно. На рис. 4.8 показано это окно на фоне обозревателя Radmin.

Если вы пользуетесь Windows NT/2000, то можно включить в настройках Radmin-сервера поддержку системы безопасности NT. После чего следует предоставить соответствующие права доступа (**Полный контроль**, **Обзор**, **Телнет**, **Перепись файлов**, **Выключение**) к Radmin-серверу.

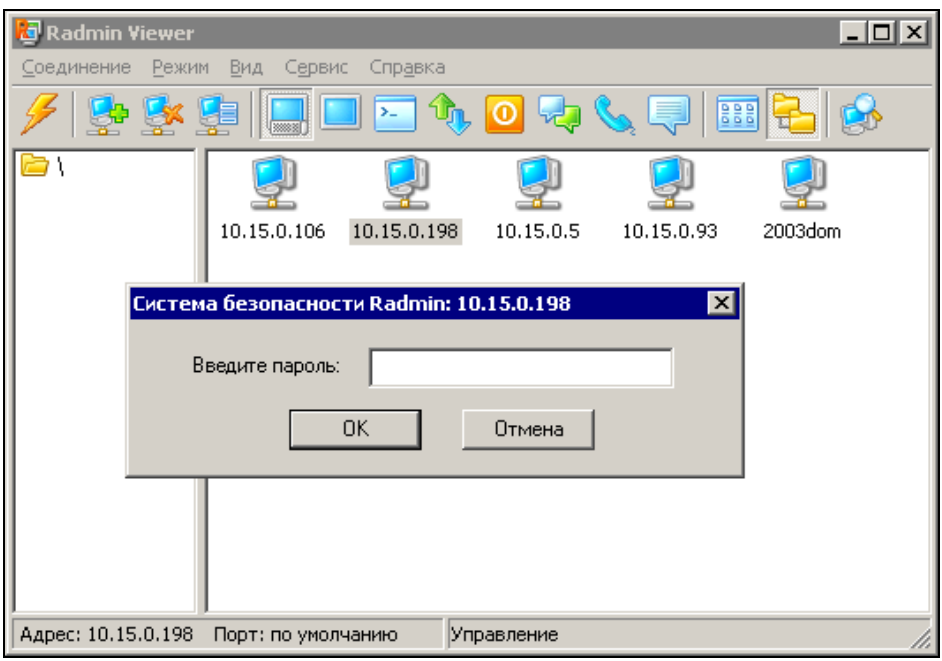


Рис. 4.8. Окно ввода пароля при открытии соединения на фоне окна обозревателя

Установки порта. Номер и адрес порта сервера могут быть изменены из меню **Настройка Remote Administrator Server**. Номер порта по умолчанию — 4899.

Меню *Соединение*

Вы можете создать новое соединение, использовать уже установленное, а также выбрать вид соединения непосредственно из меню клиента Remote Administrator.

Окно обозревателя Radmin

Команды меню обозревателя Remote Administrator **Соединение с** или **Создать** используются для создания соединения. Команда **Соединение с** позволяет выбирать компьютер, через который производится подключение (поле **Соединение через**), а также устанавливать тип соединения и номер порта.

Меню режимов

С помощью этого меню можно выбрать режим контроля за удаленным компьютером. Вы можете использовать **Полный контроль**, **Обзор**, **Телнет**, **Перепись файлов**, **Выключение** и разные режимы соединения. Если режим **Обзор** позволяет только видеть экран удаленного компьютера, то использование режима **Полный контроль** позволяет вам управлять удаленным компьютером с помощью мыши и клавиатуры и т. д.

Работа с файлами

Этот режим включен в Radmin начиная с версии 2.0. Вам необходимо выбрать пункт **Перепись файлов** из меню **Контроль** или нажать кнопку на панели инструментов.

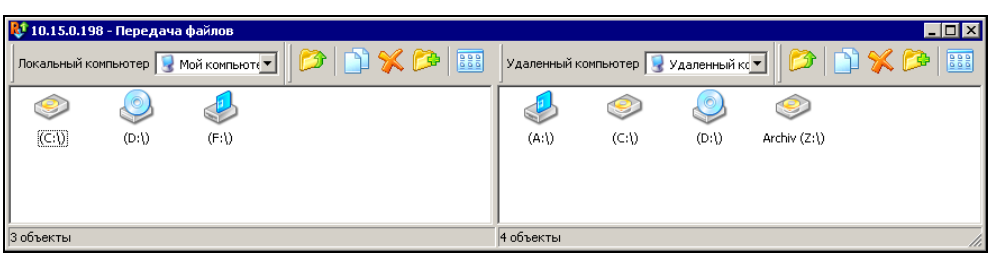


Рис. 4.9. Панели перемещения файлов

Интерфейс передачи файлов в Radmin похож на интерфейс обозревателя Windows (рис. 4.9), однако он работает с двумя окнами — локальным и удаленным. Вы можете выбрать вид просмотра файлов, используя кнопки на панели инструментов. Для копирования файлов можно применять технологию Drag and Drop ("перетащить и оставить"), нажать кнопку **Копировать** на панели инструментов или щелкнуть правую кнопку мыши и выбрать команду **Копировать** в появившемся меню. Команда **Стоп** отменяет операцию.

Примечание

В этом режиме Radmin не поддерживает сетевые диски.

Переключение между нормальным и полноэкранным режимом

Переключение между нормальным, растянутым (в этом режиме экран удаленного компьютера вписывается в окно программы) и полноэкранным режимами производится нажатием клавиши <F12>. Если вы хотите передать клавишу <F12> удаленному компьютеру, используйте команду **Передать F12** из меню **RScreen window**. Иногда режим нормального просмотра не подходит (например, экран удаленного компьютера больше). Тогда можно сжать или растянуть окно **RScreen** на полный экран. Меню удаленного экрана вызывается комбинацией клавиш <Ctrl>+<F12>.

Полноэкранный текстовый режим

Radmin не регистрирует экранные изменения, если удаленный компьютер находится в полноэкранном текстовом режиме. В таком режиме GDI (Graphic Display Interface — графический интерфейс) не выполняет прорисовку экрана. Это связано с тем, что в Windows работа драйвера видеопорта не документирована, и разработчики программ не могут применить возможности этого драйвера. Обеспечить текстовый режим на удаленной машине можно в оконном режиме.

Послать <Ctrl>+<Alt>+<Del>

Если вы хотите послать команду <Ctrl>+<Alt>+<Del> на удаленный компьютер, то можно воспользоваться пунктом меню окна обозревателя **Послать** <Ctrl>+<Alt>+<Del>. Эта возможность у вас появится только при подключе-

нии в режиме полного контроля и работе Radmin-сервера как системного сервиса под управлением Windows NT/2000. Эту команду на удаленный компьютер можно послать и с помощью комбинации "горячих" клавиш <Ctrl>+<Alt>+<F12>.

Послать команду

Вы можете использовать этот пункт меню для отправки на удаленный компьютер следующих "горячих" клавиш:

- <Ctrl>+<Esc> — для вызова главного меню;
- <F12> — для изменения размеров окна клиентской части программы Radmin, если она запущена на удаленном компьютере;
- <Ctrl>+<F12> — для вызова меню в окне клиентской части программы Radmin, если она запущена на удаленном компьютере;
- <Alt>+<F12> — аналог команды <F12>, <Ctrl>+<Alt>+<F12> — для вызова окна завершения работы на удаленном компьютере.

Команды для получения и установки буфера обмена

Эти команды меню **RScreen** позволяют изменять содержимое буфера обмена.

Для того чтобы скопировать буфер обмена:

1. Выделите текст в удаленном окне.
2. Выполните стандартную команду **Копировать** (можно просто нажать клавиши <Ctrl>+<C>).
3. Щелчком кнопки мыши выполните команду **Получить буфер**. Она доступна в меню окна удаленного компьютера **RScreen**, которое вызывается нажатием клавиш <Ctrl>+<F12>.
4. Выполните стандартную команду **Вставить** (<Ctrl>+<V>), предварительно переключившись для работы в локальном окне.

> ***Примечание***
>
> Через буфер обмена Radmin нельзя работать с файлами.

Перезагрузка

Radmin позволяет вам перезагрузить и выключить удаленный компьютер, завершать и возобновлять сеанс пользователя на этом компьютере. Сделать это можно из меню окна удаленного компьютера **RScreen**.

Настройки окна удаленного компьютера (RScreen)

Если процессор на удаленном компьютере сильно загружен — установите меньшее значение максимальной скорости обновлений в минуту в настройках **RScreen**. Если удаленный компьютер работает под Windows 95/98 (или под Windows NT, без установленного драйвера видеозахвата), Radmin-сервер может стать причиной большой загрузки процессора при установке максимальной скорости более 50 обновлений в минуту.

Отключение сбоев на рабочем столе приводит к увеличению скорости взаимодействия между локальным и удаленным компьютерами. Кроме того, можно установить **Формат цвета** в режим **16 цветов** (доступно в меню свойств соединения). Если вы подключены через dial-up-модем, то не сможете установить более 10 обновлений экрана в секунду, потому что сигнал не способен пройти туда и обратно более 10 раз в секунду (ping > 100 ms).

Если на удаленной стороне применяется операционная система Windows 95/98, скорость будет зависеть от разрешения экрана удаленного компьютера. Устанавливайте невысокие разрешения на удаленном компьютере. Кроме того, пользуйтесь пониженными цветовыми форматами 8bpp (256 цветов) или 16bpp (65 536 цветов). В некоторых системах быстрее формат 8bpp, в некоторых — 16bpp. Убедитесь, что скорость обновления не ограничена полем **Максимальная скорость обновлений в минуту** в настройках окна **RScreen**.

Если на удаленной машине используется Windows NT без установленного драйвера видеозахвата, помните, что с этим драйвером Radmin работает примерно в 10 раз быстрее и намного меньше использует процессорного времени.

Статистика соединения

Используйте окно **Информация о соединении**, вызываемое из меню **RScreen**, предоставляющего окно для получения информации о количестве прорисовок в секунду, байтов, переданных в секунду, и т. д.

Управление из командной строки (Command line)

Radmin-клиент может управляться из командной строки, которая позволяет создавать соединение с хостом без использования адресной книги.

Далее приводится формат такой командной строки:

```
radmin.exe /connect:xxxxx:nnnn other_options
```

Например:

```
radmin.exe /connect:server:1000 /fullscreen /encrypt
radmin.exe /connect:10.0.0.100:4000 /telnet
radmin.exe /connect:server /through:gate
```

Для выполнения настроек в командной строке используются следующие ключи:

- `/connect:xxxxx:nnnn` — указывает сервер и порт для подключения. Этот ключ обеспечивает соединение с сервером даже при отсутствии записи в адресной книге;
- `/through:xxxxx:nnnn` — указывает адрес и порт промежуточного сервера.

По умолчанию устанавливается режим соединения **Полный контроль** (видеть удаленный экран, управлять мышью и клавиатурой).

Для указания других режимов соединения используются следующие ключи:

- `/noinput` — режим просмотра (видишь только экран);
- `/shutdown` — режим удаленного выключения компьютера;
- `/file` — режим пересылки файлов;
- `/telnet` — Telnet-режим.

Следующие ключи работают только в режимах **Полный контроль** и **Просмотр**:

- `/fullscreen` — устанавливает полноэкранный режим просмотра;
- `/hicolor` — устанавливает формат цвета, равный 65 536 цветам, для передачи по сети;
- `/locolor` — устанавливает формат цвета, равный 16 цветам, для передачи по сети;
- `/updates:nn` — указывает максимальное количество прорисовок для просмотра;
- `/encrypt` — включает шифрование всех данных при работе.

Другие ключи:

- `/unregister` — удаляет все уже введенные ключи для Radmin;
- `/?` — показывает окно помощи.

Но, конечно, лучше всего, если все настройки вы будете производить, следуя указаниям программы установки или используя меню **Настройка Remote Administrator Server**. В этом случае вам не придется вводить ключи настройки в командную строку.

Есть еще несколько команд для системных администраторов, позволяющие вручную инсталлировать и деинсталлировать Radmin-сервер, а также изменять его настройки (номер порта, пароль и т. д.). Рассмотрим одну из них:

```
r_server.exe
```

Программу `r_server.exe` можно выполнять со следующими ключами:

- `/setup` — запускает диалог (мастер), который вам поможет установить сервис и драйвер, а также указать пароль и номер порта для Radmin-сервера. Например:

  ```
  r_server.exe /setup
  ```

- `[/port:xxxx] [/pass:xxxxx]` — если в командной строке нет никаких других ключей, кроме `/port` и `/pass`, программа `r_server` выполняется как Radmin-сервер. Далее приведены примеры возможных вариантов командной строки:

  ```
  r_server.exe
  ```

  - `r_server.exe /pass:mypass` — устанавливает пароль "mypass" для сервера Radmin;
  - `r_server.exe /port:5505` — устанавливает номер порта "5505" для сервера Radmin;
  - `r_server.exe /port:3333 /pass:qwerty` — устанавливает пароль "qwerty" и номер порта "3333" для сервера Radmin;

- `/save [/port:xxxx] [/pass:xxxxx]` — позволит вам изменить номер порта и/или пароль в реестре. Например, для сохранения пароля и номера порта в реестре следует ввести команду:

  ```
  r_server.exe /port:5505 /pass:qwerty /save
  ```

  Для записи в реестр номера порта по умолчанию и пустого пароля выполните команду:

  ```
  r_server.exe /save
  ```

- `/install` — позволяет установить как сервис, так и драйвер (Windows NT);
- `/uninstall` — деинсталлирует программу;
- `/installservice` — устанавливает только сервис (Win95/98 или WinNT);
- `/uninstallservice` — деинсталлирует сервис;
- `/uninstalldrv` — деинсталлирует драйвер;
- `/silence` — запрещает сообщения об ошибках (`error`) или успешно выполненных операциях `(ok)` при запуске с ключами: `/install`, `/uninstall` или `/save`;
- `/stop` — останавливает Radmin-сервер. Применение этого ключа останавливает сервис и завершает приложение. Для остановки сервиса под Winows NT требуется наличие соответствующих прав;
- `/?` — показывает окно помощи.

Остановка Radmin-сервера

Для остановки сервера вы можете использовать соответствующий ярлык в папке Remote Administrator или просто ввести в командную строку:

```
r_server.exe /stop
```

Адресная книга Radmin

Вся информация об удаленных подключениях содержится в адресной книге. Ваша адресная книга хранится в системном реестре (registry). Все операции с ней можно выполнять с помощью regedit.exe. Экспортируйте в файл все ключи, находящиеся в разделе реестра `HKEY_CURRENT_USER\Software\Radmin\v2.0\Clients`.

Далее вы можете импортировать этот файл (собственно, адресную книгу) в реестр на другом компьютере. Если вы хотите воспользоваться старой (из прошлой версии программы) адресной книгой, то выполните следующую команду, создающую адресную книгу Radmin2.x из Radmin1.11:

```
radmin.exe /copyphonebook
```

Несмотря на то что Windows имеет некоторые встроенные средства для работы с удаленным рабочим столом, они не идут ни в какое сравнение с описанной программой. Более того, используя эту программу, вы можете работать с

каталогами, доступ к которым по сети запрещен для пользователей. Никто, кроме вас, к этим каталогам не сможет подключиться из сети. Единственное средство, встроенное в Windows 2000 Server и Windows Server 2003, которое может заменить Radmin при удаленной работе с самим сервером, — это сервер терминалов. Но с его помощью вы не получите доступ к компьютерам сети. Интересной может быть и возможность одновременной работы двух администраторов или пользователей, находящихся за разными компьютерами, с рабочим столом третьей машины одновременно. Но такая задача потребует дополнительной лицензии на программу, цена которой, впрочем, не так уж и высока — 750 рублей.

VNC — Virtual Network Computing

Эта программа существует в нескольких платных и бесплатных версиях. Имеет версии для Windows, Linux и практически для всех существующих ОС для настольных и даже карманных компьютеров. **http://www.realvnc.com/** — это адрес, где можно узнать о программе подробно и скачать ее.

На рис. 4.10 и 4.11 показаны окна программы, доступные при установлении подключения к другому компьютеру. После первоначальной установки программы вы можете не изменять никаких установок. Просто наберите адрес удаленного компьютера в поле **Server** и нажмите кнопку **OK**. Если программа установлена на удаленном компьютере, вы увидите его экран.

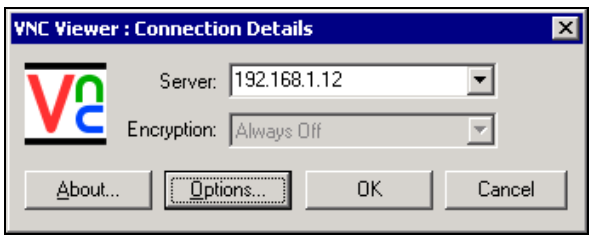


Рис. 4.10. Окно **VNC Viewer: Connection Details**

По сравнению с другими программами подобного назначения VNC в бесплатной версии не содержит некоторых полезных функций, например передачи файлов. Если вам эта функция нужна, придется купить более сложную версию этой программы или воспользоваться программой другого разработчика. Но у VNC есть интересная возможность: к серверу VNC можно подключиться, не

имея установленной программы на компьютере. Достаточно иметь поддержку Java в браузере. Установив на компьютеры пользователей серверную часть программы, вы сможете с любого другого компьютера подключиться к рабочему столу (рис. 4.12). Желательно только, чтобы разрешение экрана у компьютера, с которого вы подключаетесь, было выше, чем у подключенного. Иначе появятся полосы прокрутки, с которыми не очень удобно работать.

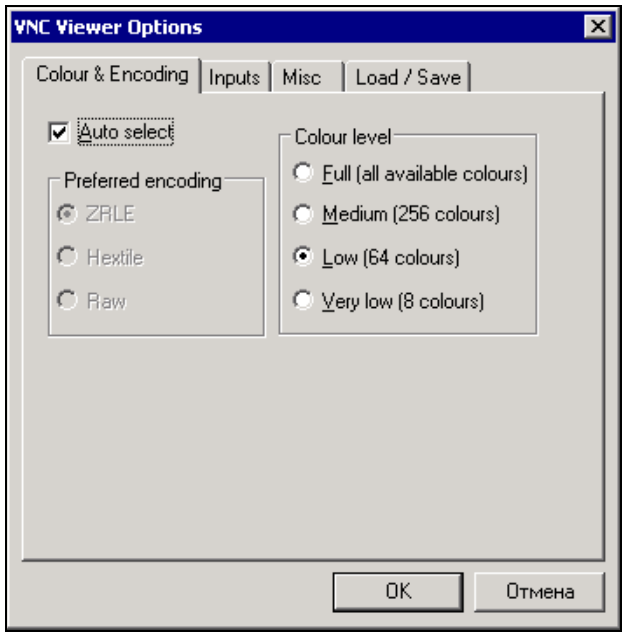


Рис. 4.11. Окно **VNC Viewer Options**

Естественно, что на компьютерах должна быть установлена поддержка Java. Может возникнуть вопрос: как же подключиться к рабочему столу пользователя, если сеть находится за маршрутизатором с NAT и реальный IP-адрес в Интернете один? Есть несколько вариантов, которые использовались или используются автором. Самый надежный из них — это организация терминального доступа к серверу, а уже с него подключения к рабочим столам пользователей. В этом случае возможны варианты при подключении к рабочим столам пользователей, могут быть применены различные программы, различные порты. Внутри сети это не станет помехой для организации доступа. В то же время, через Интернет доступно всего одно хорошо защищенное подключение к серверу или специально выделенному компьютеру. Но при

желании вы можете настроить маршрутизатор и программы администрирования таким образом, чтобы можно было выделить диапазон портов, подключаясь через которые вы могли бы попасть на ту или иную рабочую станцию. Но это снизит общую защищенность вашей сети от атак из Интернета, если придется открыть много портов.

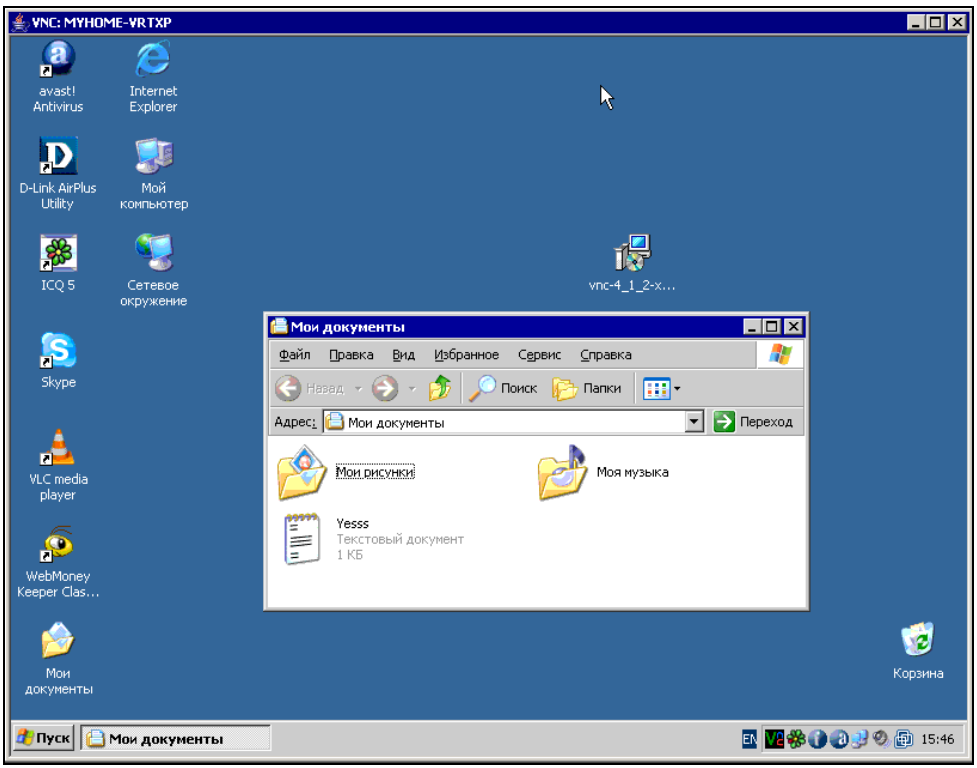


Рис. 4.12. Окно VNC Viewer (Java)

В области создания программ удаленного администрирования и доступа к рабочему столу существует некоторая конкуренция. Есть варианты бесплатные, есть очень дорогие. Но у каждого свои преимущества и недостатки. По следующим ссылкам вы сможете найти подходящий вам вариант:

- **http://www.cybercontrol.ru/products/nrc/index.html**;
- **http://rus.jmpager.com/index.htm**;
- **http://www.anyplace-control.com/ru/index.shtml**;

- **http://www.famatech.ru/**;
- **http://www.oszone.net/219/**;
- **http://www.opennet.ru/prog/info/131.shtml**;
- **http://ipesin.linux.kiev.ua/translations/rhm/vnc1.html**;
- **http://www.hidadmin.ru/**;
- **http://forum.ru-board.com/topic.cgi?forum=8&topic=1696**;
- **http://www.teamviewer.com/download/portable.aspx**.

Программа, доступная по последней ссылке, может быть применена без установки на компьютер, ее можно запускать со съемного носителя. Программа использует некоторый сервер, расположенный в Интернете, что позволяет подключаться к любому компьютеру имеющему выход в Интернет, если на нем запущен экземпляр программы. При этом не требуется выполнять никаких настроек в сети. Возможна и работа внутри локальной сети без обращения к внешнему серверу. Программа работает в любой ОС Windows.

SuperScan — программа для сканирования сетей

В качестве вспомогательного средства при работе с программами удаленного управления можно использовать бесплатную утилиту SuperScan (рис. 4.13), которую можно найти по адресу **http://www.openproj.ru/42/909/** или более новую версию по адресу **http://www.webattack.com/get/superscan.html**.

Эта утилита позволяет определить активные в данный момент компьютеры сети. Сеть сканируется в заранее заданном диапазоне адресов и портов. Поскольку в вашей сети большинство адресов не выходит за пределы заранее определенных значений, найти активные машины не составит труда. Программа может использоваться и для зондирования адресов в Интернете.

LanSchool

Если ваша сеть используется преимущественно для обучения (студентов, школьников) и есть оборудованные компьютерами классы или предполагается их организовать, то полезна будет программа LanSchool с сайта

www.lanschool.com. Программа разработана специально для учебного класса. Предусмотрено размещение учебных мест в различных помещениях. LanSchool содержит две составляющих: Teacher.exe и Student.exe. Названия составляющих говорят сами за себя.

Большое количество настроек позволяют конфигурировать программу в соответствии с требованиями учебного процесса. Компьютер преподавателя связан с компьютерами студентов шестнадцатью каналами, подобно каналам телевидения. Каждый из компьютеров студентов представлен на экране преподавателя значком, который может быть развернут в окно. На экранах студентов окно преподавателя может быть развернуто на полный экран, а может быть свернуто для освобождения места для работы. При этом преподаватель имеет возможность руководить работой, показывать и объяснять учебный материал как всем студентам, так и индивидуально, взяв управление экраном студента на себя.

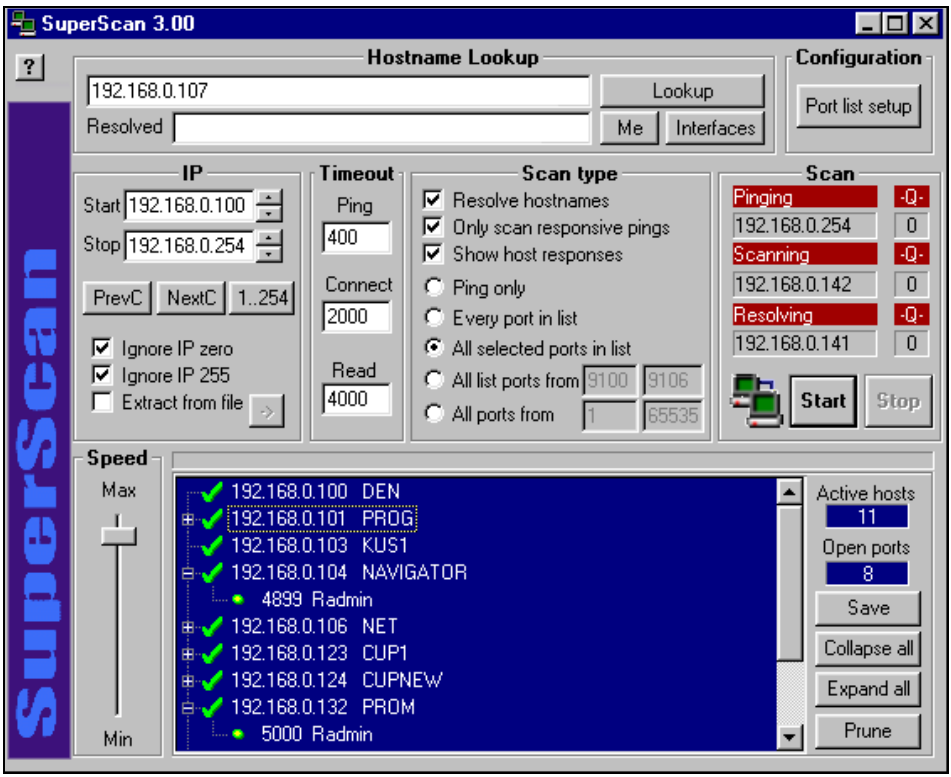


Рис. 4.13. Окно программы SuperScan 3.00

Для учебного класса актуальным является вопрос защиты программы и сети от несанкционированных действий учащихся. В LanSchool этот вопрос решен достаточно хорошо. Предусмотрена возможность установки защиты. Кроме того, создатели программы предположили, что особенно "продвинутые" учащиеся смогут обойти защиту. Но в этом случае действия нарушителя будут зафиксированы в *реестре* компьютера студента. Преподаватель может просмотреть эту информацию на любом из компьютеров студентов дистанционно и выявить нарушителя, применив к нему меры административного воздействия.

Системные требования и установка:

- операционная система — Windows 95/98, Windows ME, Windows NT 4.0 с SP4 или Windows 2000, Windows XP
- процессор — 166 МГц Intel Pentium или выше;
- оперативная память — 32 Мбайт для Windows 95, 48 Мбайт для Windows 98 и Windows ME, 64 Мбайт для Windows NT 4.0 и 96 Мбайт для Windows 2000;
- экранное разрешение компьютеров может составлять 800×600, 1024×768 или 1280×1024. Все компьютеры должны использовать TCP/IP-протокол.

Дистрибутив программы занимает немногим более 1 Мбайт вместе с файлами PDF с описанием установки программы.

В самом начале установки выбирается режим установки — преподаватель или студент. Сама установка программы занимает несколько секунд, как и деинсталляция. Незарегистрированная версия по окончании времени демонстрационной работы перед каждым рабочим запуском предупреждает о завершении demo-периода и просит прекратить использование программы.

С точки зрения конфигурации сети должно выполняться одно требование: компьютер преподавателя и компьютеры студентов должны находиться в пределах одной подсети.

Компьютер — сеть — компьютер. Transmitter Lite

Настроенная иерархическая сеть позволяет организовать общение между пользователями более гибко, чем одноранговая. Каналом связи может служить как сама сеть, через сетевые карты, так и Интернет или телефонная линия. В некоторых случаях возможно использование всех этих каналов одновременно. Соб-

ственно вид канала связи не имеет большого значения, важно только, чтобы этот канал поддерживал работу по протоколу, который использует программа связи. Одна из таких программ называется Transmitter Lite (**http://pcutils.narod.ru/svaz.html**). Программа распространяется бесплатно, но обладает очень широкими возможностями и имеет русский интерфейс.

Программа Transmitter Lite (рис. 4.14) — приложение для связи между двумя компьютерами по протоколу TCP/IP. Связь возможна по Интернету, по локальной сети, и даже напрямую через модемы компьютеров. Программа позволяет передавать речь (предусмотрена возможность полнодуплексного разговора), отсылать/получать сообщения, файлы, вести диалоговое взаимодействие. Это своего рода многофункциональный интернет-телефон. Также возможно предоставить определенные ресурсы (каталог, диск) для удаленного использования. Вся передаваемая информация шифруется.

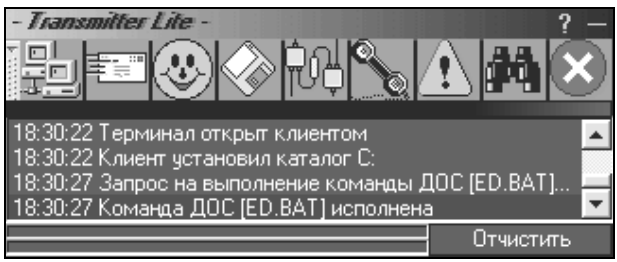


Рис. 4.14. Вид главной панели программы

Если вы желаете использовать программу для связи через сеть Интернет, то вам необходимо сначала зарегистрироваться на главном сервере — Координаторе. Он работает как своего рода АТС, посредник между пользователями программы. IP-адреса обычно раздаются сервером провайдера на сеанс связи и каждый раз бывают разными. Для определения текущего адреса пользователя, с которым предполагается установить соединение через Интернет, необходим Координатор. Для того чтобы сервер вас обслужил, надо зарегистрироваться на нем. Регистрация производится из меню программы Координатор — **Регистрация нового пользователя**. После заполнения формы регистрации у вас будут регистрационное имя в сети Transmitter и пароль, которые вы сами выберете. Откройте панель настроек, выберите пункт **Параметры связи** и введите в соответствующих полях новые регистрационное имя и пароль. Также настройте все остальные пункты, руководствуясь справкой программы.

Чтобы связаться с другим пользователем программы, надо знать его регистрационное имя в сети Transmitter. Связь устанавливается с помощью кнопки **Соединение** после ввода регистрационного имени вызываемого абонента. Вы можете связаться с удаленным компьютером напрямую, зная его IP-адрес. Для этого надо открыть в окне соединения дополнительные свойства и установить флажок **Связь напрямую**. Это может быть необходимо, когда вызываемый абонент находится в локальной сети без выхода в Интернет или при связи между двумя компьютерами через модемы по телефону с помощью сервера удаленного доступа. Transmitter может работать и через прокси-сервер. Transmitter является однопоточной, одноканальной коммуникационной программой, т. е. все действия по передаче файлов, сообщений и т. п. происходят всего по одному порту, и обслуживать она может в одно время или одного клиента, или работать с одним сервером. Программа несовместима с другими программными продуктами подобного рода, только с серией Transmitter.

Чтобы установить соединение с другим компьютером, вам надо знать либо регистрационное имя нужного пользователя (регистрационное имя в сети Transmitter), либо IP-адрес его машины и входящий порт. Нажмите кнопку **Соединение**, затем введите нужные данные и нажмите кнопку **ОК**. Если вы ввели регистрационное имя сети Transmitter нужного пользователя, то программа свяжется сначала с главным сервером — Координатором, выяснит местонахождение требуемого пользователя (его адрес IP), а затем свяжется с ним напрямую. Для этого вызываемый пользователь должен быть зарегистрирован на сервере Координатора. Если вы знаете адрес IP нужного абонента, то можете связаться с ним сразу напрямую. Для этого нажмите кнопку (в окне установки связи) **Дополнительно** и установите флажок **Связь напрямую**, введите в поле **Логин** адрес IP вызываемого абонента. Если на сервере абонента для входа требуется пароль, то введите его в соответствующем поле. При связи через Координатор указанный для связи порт игнорируется, так как на сервере Координатора указан текущий порт вызываемого абонента. Значение порта имеет смысл только при соединении напрямую. По мере соединения с разными адресами, они запоминаются программой. Запоминаются последние 50 введенных адресов. Если соединение прошло успешно, то программа отсылает удаленному компьютеру (серверу) ваше имя и, если есть, пароль. Если же пароль неверный или пользователь на сервере не захотел вас принять, то Transmitter закроет соединение и установит режим ожидания. Если же вы пытаетесь связаться с сервером, который в данный момент обслуживает другого клиента или сам является клиентом, то программа сообщит вам, что невозможно связаться по данному адресу.

Когда программа выступает в качестве серверного приложения, при запуске сразу устанавливается режим ожидания по определенному в настройках параметров связи порту. Теперь она может выступать в качестве сервера для такой же программы. Установите в настройках параметров безопасности условия входа на ваш сервер.

В зависимости от указанных ранее установок Transmitter, чтобы принять клиента, спросит разрешения у вас, проверит пароль или просто допустит клиента на сервер.

Если требуется ваше разрешение, то будет мерцать кнопка **Соединение** и пиктограмма на системной панели. Также вы услышите звук (схожий со звуком телефона). Нажмите кнопку, появится окно с данными клиента, его имя и адрес IP. Затем сделайте выбор: принять или игнорировать. Если вы выберете второе, то Transmitter закроет соединение и установит режим ожидания. При выборе значения **Принять** связь установится, и клиент сможет с вами общаться так же, как и вы с ним.

Если же установленный пароль не совпадает с паролем, присланным клиентом, то программа отключит его, запишет в окно статистики "Пароль неверный" и установит режим ожидания.

Когда связь установлена, безразлично, находитесь ли вы на стороне клиента или сервера. Обе стороны полноценно могут использовать возможности программы, в соответствии с настройками параметров безопасности каждой стороны.

Для связи двух компьютеров напрямую через модемы вам потребуется сервер удаленного доступа (Windows 98/NT). Если же у вас Windows 95, можно воспользоваться прилагаемым к программе сервером. Для этого выберите в меню **Открыть | Сервер удаленного доступа**. Установите опцию **Разрешить удаленные подключения** (Allow caller access). Теперь можно установить связь с этим компьютером по протоколу TCP/IP (как в Интернет). В большинстве случаев после соединения у сервера будет адрес IP 192.168.55.1, а у клиента — 192.168.55.2. Если же протокол TCP/IP настроен не по умолчанию, то сервер получит адрес, который вы сами установили в настройках сети (**Панель управления | Сеть**).

Прием и передача сообщений

Чтобы передать сообщение противоположной стороне, нажмите кнопку **Сообщение** и в появившемся окне (рис. 4.15) введите сообщение и нажмите

кнопку **Послать**. Максимальный размер сообщения — 32 Кбайт. Пустое сообщение не отсылается.

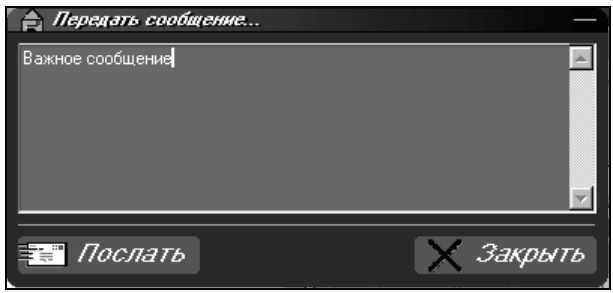


Рис. 4.15. Панель передачи сообщений

При получении сообщений от противоположной стороны будет изменяться фон кнопки **Сообщение**, мерцать значок на системной панели. Для того чтобы прочитать полученное сообщение, нажмите данную кнопку. Если пришло несколько сообщений, то в окне **Получено сообщение** появится кнопка **Следующее**.

Для записи приходящих сообщений в файл выставите соответствующий пункт в меню **Настройки параметров связи**.

Чат

Пользование этим режимом аналогично работе с сообщениями. Разница лишь в том, что окно чата (рис. 4.16) появится на обоих связанных компьютерах, и вся информация будет доступна для просмотра до закрытия сеанса связи.

Удаленный терминал

Один из полезных режимов работы программы — **Удаленный терминал** (рис. 4.17).

В этом режиме возможны прием, передача и переименование файлов, создание и удаление папок на удаленном компьютере, а также выполнение на нем команд DOS. Доступные возможности зависят от настроек разрешений на удаленной машине.

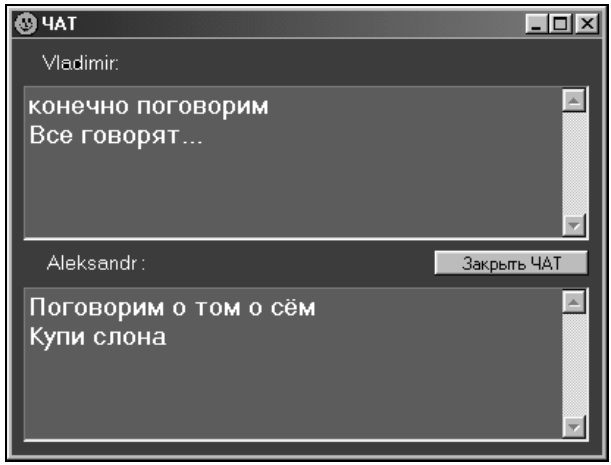


Рис. 4.16. Чат

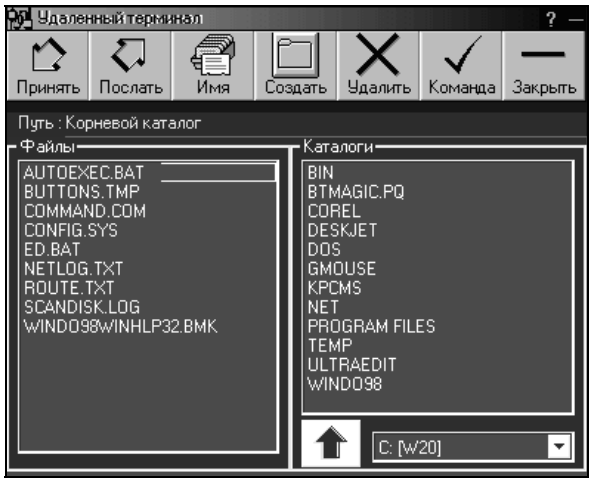


Рис. 4.17. Удаленный терминал

Голосовая связь

Возможна при нажатии кнопки с изображением телефонной трубки и удержании ее. При этом на кнопке появится изображение микрофона, а все сказанное вами в микрофон, подключенный к звуковому адаптеру, с некоторой задержкой будет передано на удаленный компьютер.

Дополнительные возможности

Заслуживает внимания возможность оставить сообщение для первого соединившегося пользователя. Выберите правой кнопкой мыши значок программы в системном лотке и укажите на пункт меню **Оставить сообщение**. Откроется окно, в котором вы сможете ввести текст сообщения. При соединении сообщение будет передано. Можно также автоматически отключиться от установившего соединение пользователя сразу после передачи сообщения.

Если у вас локальная сеть и для доступа в Интернет используется прокси-сервер (proxy или firewall), то вам потребуется дополнительно настроить программу. Нужно создать TCP-связь (TCP link, TCP mapping) от прокси-сервера к программе в локальной сети (на ее локальный адрес и порт). Порт связи на прокси должен обязательно быть такой же, как локальный порт программы, так как Transmitter отошлет Координатору свой текущий порт и адрес прокси-сервера.

Например, если программа установлена в локальной сети на компьютере с адресом 192.168.0.3, порт 20 000, то вам надо создать связь на прокси: порт ожидания (Listen port, accept port) такой же, как у программы — 20 000.

Связь по указанному адресу и на указанный порт должна быть разрешена для всех внешних подключений. И так для каждого пользователя в локальной сети. Причем порты у каждого пользователя в одной сети должны быть разные, так как для каждого пользователя будет своя TCP-связь.

Данная TCP-связь служит для приема звонков, а для связи с другими пользователями Интернета программа будет использовать протокол SOCKS4. Если вы не установите TCP-связь, то прием звонков будет невозможен, однако программа сможет связываться с пользователями вне вашей локальной сети. И наоборот, если установите TCP-связь и у вас не будет сервиса SOCKS4, то программа сможет принимать звонки, однако не сможет соединяться с внешней сетью (Интернет).

Для настройки на сервис SOCKS4 откройте панель настроек **Параметры связи**, нажмите на изображение пары компьютеров и введите в соответствующих полях адрес прокси-сервера и порт, на котором установлен сервис SOCKS4.

Также в данном окне можно изменить адрес Координатора, если он перенесен на другой сервер. Не рекомендуется изменять данные Координатора без обращения к службе технической поддержки программы.

Такие программы, как Radmin, SuperScan и Transmitter, могут применяться и совместно. Каждая из них обладает возможностями, дополняющими друг друга. Комплекс этих программ может обеспечить надежную и оперативную связь между компьютерами, которая удовлетворит самого требовательного пользователя.

ICQ (I Seek You)

Следующая рассматриваемая программа предназначена исключительно для работы в Интернете. Часто ее называют "Аська" (рис. 4.18). Существуют как англоязычные, так и русскоязычные версии этой программы. Программа обладает широчайшими возможностями. После регистрации и получения регистрационного номера (UIN) пользователи Интернета и ICQ смогут найти вас и подключиться для разговора или передачи файлов. Если запущен NetDetect Agent — программка, обнаруживающая наличие соединения с Интернетом, то ICQ может стартовать автоматически при обнаружении соединения с Интернетом. Работая в фоновом режиме, программа требует мало ресурсов и не мешает работе других приложений. При обнаружении соединения программа "объявит" о вашем присутствии в Интернете и покажет вам, кто из ваших знакомых доступен для связи в настоящий момент.

Для начала работы в ICQ после регистрации необходимо уметь:

- ❒ добавлять пользователя к вашему списку контактов;
- ❒ посылать сообщения;
- ❒ получать сообщения;
- ❒ отвечать на сообщение;
- ❒ разговаривать с другим пользователем;
- ❒ передавать файлы.

Это основные функции, доступные в ICQ.

Кроме того, программа позволяет вести наблюдение за состоянием активности пользователей. Если какой-либо ваш знакомый зарегистрировал ICQ и сообщил вам свой номер, вы можете внести его в список пользователей, а когда он подключится к Интернету, программа подскажет вам, что знакомый доступен для связи с ним. Поддержка программы включает создание вашей

страницы на сервере ICQ, где будут представлены сведения о вас, которые вы внесли при регистрации. С этой же страницы можно посылать сообщения, искать пользователей, получать обновления. Вы можете также добавлять и изменять сведения о себе, которые помогут другим пользователям найти вас.

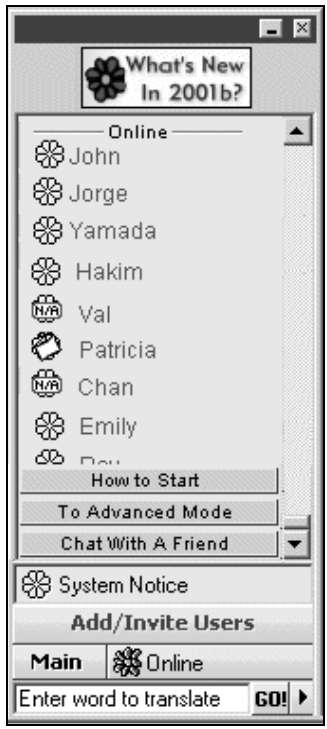


Рис. 4.18. ICQ в развернутом виде

Примечание

Сообщение, посланное из Outlook Express, не может быть понято ICQ: его текст посмотреть невозможно.

Примечание

Программа не позволяет использовать ее в локальной сети без подключения к серверу ICQ. Поэтому более подробно работу с программой мы не рассматриваем.

Courier Mail Server

Пришла пора организовать в вашей сети почтовое отделение. Windows 2000 Server не имеет в своем составе средств для его создания, другие, рассмотренные ранее варианты почтовых серверов сложны в настройке, поэтому воспользуемся очень удобной и к тому же бесплатной программой Courier Mail Server (CMS). Ее можно найти на сайте **http://courierms.narod.ru**. Разработчики программы — Роман Ругаленко и Валерий Пиго — постоянно работают над ее обновлением и оказывают оперативную техническую поддержку пользователям (их e-mail: **courierms@narod.ru**). Практика применения программы в локальной сети показала ее высокую надежность и удобство эксплуатации при наличии вспомогательного компьютера, который выполняет функции почтового отделения локальной сети. Если ваш основной сервер не слишком загружен, то программа может работать и на нем. Несмотря на относительную простоту интерфейса, следует внимательно познакомиться с процедурой установки и настройки почтового сервера.

CMS представляет собой сервер электронной почты, работающий под управлением операционной системы Windows 9*x*/ME/NT/2000/XP. Программа предоставляет возможность пользователям локальной сети обмениваться электронной почтой друг с другом, а так же получать и отправлять письма через Интернет.

В состав CMS входят:

- SMTP-сервер
- POP3-сервер
- IP-фильтр
- SMTP-клиент
- POP3-клиент
- Планировщик
- Сортировщик почты
- Удаленный доступ

Почтовый сервер CMS предназначен для организации обмена электронной почтой между компьютерами. Основными его функциями являются прием почтовых сообщений от клиентов и доставка их по адресам, указанным в сообщении. В качестве клиентов могут выступать как сетевые компьютеры, так и другие почтовые серверы. Пользователи с помощью программы — почтового клиента, могут создавать сообщения, отправлять их на сервер и забирать почту из своих почтовых ящиков.

Для связи между сервером и клиентом применяются следующие почтовые протоколы:

- Simple Mail Transfer Protocol (SMTP — простой почтовый протокол передачи данных) — для передачи сообщений на сервер;

- Post Office Protocol version 3 (POP3 — протокол почтовой связи третьей версии) — для приема сообщений из почтового ящика.

В программе используются стандартные порты: для SMTP — порт 25, для POP3 — порт 110.

Для блокирования нежелательных подключений в CMS имеется IP-фильтр.

Сообщения, полученные SMTP-сервером, помещаются в очередь входящих сообщений. Они последовательно обрабатываются и направляются в почтовые ящики (для локальных получателей) и в очередь исходящих сообщений (для внешних получателей).

Получатель считается локальным, если домен в его адресе электронной почты (строка после @) совпадает с именем локального домена сервера.

Накопившиеся исходящие сообщения SMTP-клиент периодически отправляет в Интернет на другой почтовый сервер, который берет на себя ответственность за дальнейшую доставку сообщений.

Сеансы обмена почтой через Интернет могут выполняться в автоматическом режиме по расписанию с помощью планировщика. При этом подключение к Интернету может осуществляться как по локальной сети, так и через модем (удаленный доступ).

POP3-клиент обеспечивает возможность забирать почту из почтовых ящиков, находящихся на других серверах, и доставлять ее локальным или внешним получателям.

Сортировщик почты позволяет на основе задаваемых правил перенаправлять определенным получателям сообщения, принятые из внешних ящиков.

Системные требования

- Операционная система: Windows 9*x*/ME/NT/2000/XP.
- Свободное место на жестком диске: 1 Мбайт и несколько мегабайт для хранения почты пользователей.
- Установленный сетевой протокол TCP/IP.
- Если предполагается обмен электронной почтой через Интернет, то необходимо непосредственное соединение компьютера с Интернетом через сетевую плату, модем или другое устройство.
- При подключении к Интернету с помощью модема необходим установленный компонент Windows **Удаленный доступ к сети**.

- При наличии локальной сети на всех компьютерах для работы с электронной почтой через CMS должен быть установлен сетевой протокол TCP/IP и клиентские программы, способные работать с почтовыми серверами по протоколам SMTP и POP3 (Outlook Express, The Bat! или аналогичные).

Установка и удаление

CMS поставляется в виде архива ZIP, содержащего исполняемый файл и документацию. Для установки сервера создайте папку, в которой он будет функционировать, переместите файлы из архива в эту папку и запустите приложение CourierMS.exe. При первом запуске сервер внутри своей папки автоматически создаст необходимые для его работы подкаталоги и файлы. За пределами своей папки сервер не производит никаких изменений. Системный реестр Windows меняется только при регистрации в качестве службы.

Если запуск прошел нормально, то на экране появится главное окно сервера, а в системном лотке (System Tray) рядом с часами — его значок.

Для того чтобы сервер запускался автоматически при загрузке Windows, его можно зарегистрировать как службу.

Для удаления сервера остановите его, после чего удалите папку, в которой он находится, а также папки почтовых ящиков, очередей или журналов, если вы разместили их за пределами рабочей папки сервера. Если сервер запускался как служба, то перед его удалением надо отменить запуск в качестве службы.

Работа в качестве службы

Помимо ручного запуска CMS может автоматически запускаться как служба (сервис) Windows NT/2000/XP/9*x*/ME.

Для функционирования в качестве службы запустите CMS и в меню **Настройки** выберите команду **Запускаться службой**. При этом произойдет регистрация службы Courier Mail Server в системе.

Теперь при загрузке Windows CMS будет автоматически запускаться как служба до входа пользователя в сеть. При завершении сеанса пользователя сервер будет продолжать работу.

Можно запустить службу и вручную. Для этого в Windows NT/2000/XP используйте диспетчер служб (Service Control Manager), а в Windows 9*x*/ME запустите из командной строки CourierMS.exe с ключом `/service`.

Для прекращения запуска в качестве службы в меню **Настройки** повторно выберите команду **Запускаться службой**.

Главное окно

Главное окно сервера (рис. 4.19) содержит четыре панели:

- панель компонентов (вверху слева) содержит список компонентов сервера;
- панель подключений (вверху справа) включает в себя список текущих клиентских подключений к серверу, а также исходящих подключений к внешним SMTP- и POP3-серверам;
- панель статистики (внизу слева) отображает количество имеющихся учетных записей и состояние SMTP/POP3-серверов. Она также служит для запуска/остановки серверов с помощью контекстного меню;
- панель журнала (внизу справа) отображает журнал работы сервера.

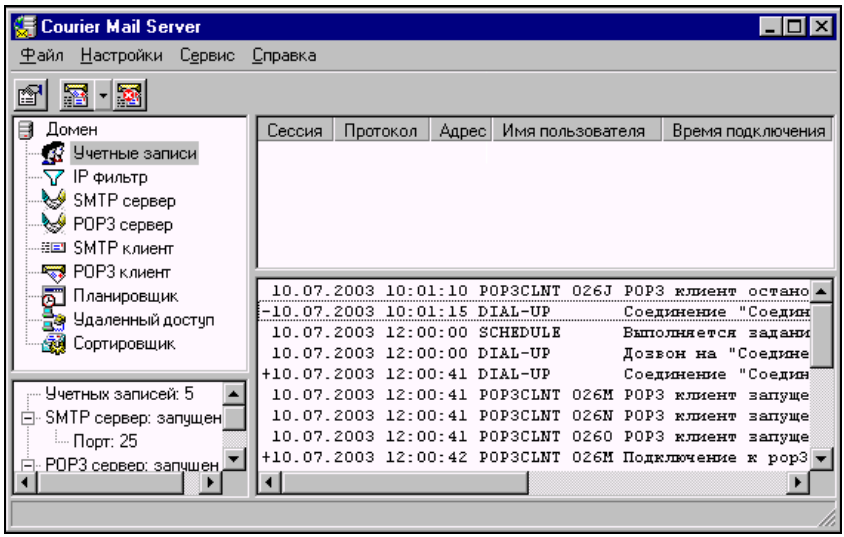


Рис. 4.19. Главное окно Courier Mail Server

Для настройки параметров главного окна в меню **Настройки** выберите команду **Интерфейс**. С помощью этой команды можно установить следующие режимы работы программы:

- **Показывать главное окно при запуске** — если флажок установлен, то главное окно будет показываться при запуске CMS;
- **Отображать значок в системном лотке** — назначение следует из названия;
- **Запоминать состояние главного окна** — если флажок установлен, то при выходе из CMS будут сохранены размер и положение главного окна, а также размеры панелей;
- **Задавать пароль главного окна** — пароль, запрашиваемый перед открытием главного окна. Если пароль пустой, запрашиваться он не будет;
- **Устанавливать клавиши быстрого вызова** — комбинация клавиш для быстрого вызова главного окна;
- **Указать количество строк экранного журнала** — максимальное количество строк, отображаемых одновременно в экранном журнале.

Настройка сервера

Настройка сервера заключается в последовательной настройке всех его компонентов. Для задания свойств компонента выберите его в дереве компонентов, после чего в меню **Файл** или в контекстном меню выберите команду **Свойства**. Для настройки свойств журнала в меню **Настройки** выберите команду **Журнал**. В каждом окне настройки компонентов можно вызвать контекстную справку клавишей <F1>.

Домен

Вкладка **Общие** (рис. 4.20) в окне свойств домена позволяет задать в текстовом поле **Имя** имя локального домена, например **mycompany.ru**.

Теперь, если SMTP-сервер CMS получит сообщение, адресованное, например, **user@mycompany.ru**, он поместит его в почтовый ящик user, так как получатель принадлежит локальному домену. Если адрес получателя будет **user@yourcompany.ru**, то письмо будет отправлено в Интернет, так как домен **yourcompany.ru** не является локальным для этого сервера.

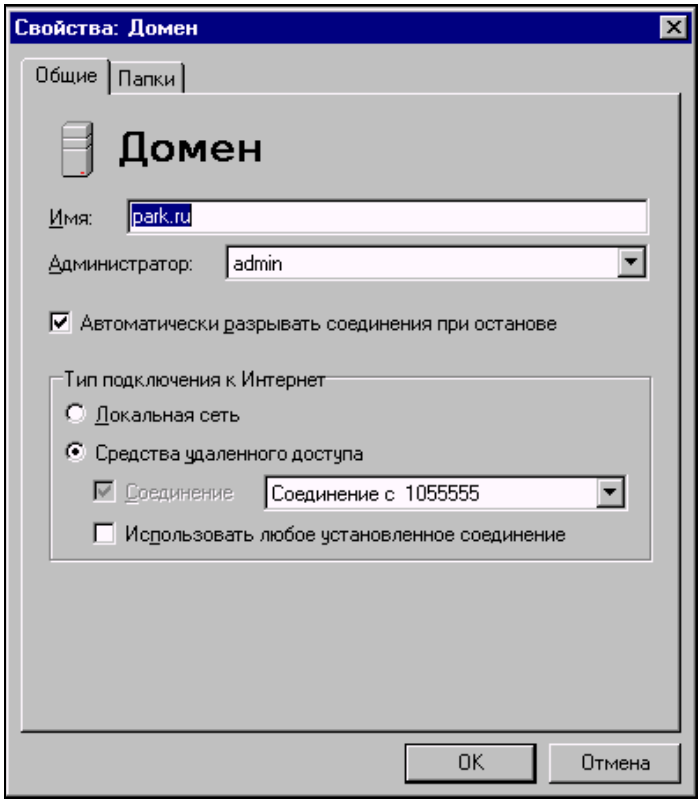


Рис. 4.20. Окно **Свойства: Домен**, вкладка **Общие**

Получатель, домен которого не указан, считается локальным. То есть, если SMTP-сервер примет сообщение с адресом получателя **user**, он поместит его в локальный почтовый ящик user, как и в случае полного адреса **user@mycompany.ru**.

Текстовое поле **Администратор** служит для указания почтового ящика администратора. Согласно стандарту Интернета любой почтовый сервер должен иметь почтовый ящик postmaster, служащий для приема сообщений о проблемах, связанных с работой сервера. Если сервер получит сообщение, адресованное **postmaster@mycompany.ru** или просто **postmaster**, оно будет доставлено администратору.

Если флажок **Автоматически разрывать соединения при останове** установлен, то при остановке сервера клиентские соединения будут разорваны автоматически без подтверждения администратора. Если CMS запущен как

служба, то соединения разрываются автоматически независимо от состояния данного флажка.

Группа **Тип подключения к Интернет** предназначена для указания способа подключения почтового сервера. Можно выбрать один из переключателей: **Локальная сеть** или **Средства удаленного доступа**, чтобы использовать для подключения локальную сеть или средства удаленного доступа соответственно.

Если установить флажок **Соединение**, то для подключения будет применяться соединение, указанное в расположенном рядом раскрывающемся списке.

Для подключения через любое уже установленное соединение можно установить флажок **Использовать любое установленное соединение**.

Вкладка **Папки** предназначена для настройки папок почтовых ящиков, очередей входящих и исходящих сообщений и файлов журнала.

Учетные записи

Редактор учетных записей (рис. 4.21) предназначен для ведения списка учетных записей пользователей сервера. При создании учетной записи создается также соответствующая папка почтового ящика. При удалении учетной записи папка почтового ящика удаляется автоматически со всем содержимым.

При первом запуске сервера автоматически создается учетная запись postmaster (пароль — 1).

Каждая учетная запись (рис. 4.22) имеет параметры, приведенные далее.

- **Реальное имя** — имя владельца почтового ящика.
- **Имя почтового ящика** — наименование почтового ящика. Оно же является и именем пользователя при подключении к серверу. В имени ящика не используйте русские буквы и специальные символы, так как некоторые почтовые программы работают с ними некорректно. Если имя ящика user, локальный домен mydomain.ru, то адрес электронной почты данного пользователя **user@mydomain.ru**.
- **Пароль** — пароль для подключения к серверу.
- **Доступ POP3 клиентам разрешен** — если флажок установлен, то доступ к почтовому ящику разрешен.
- **Почтовая папка** — папка, в которой будут храниться сообщения данного ящика.

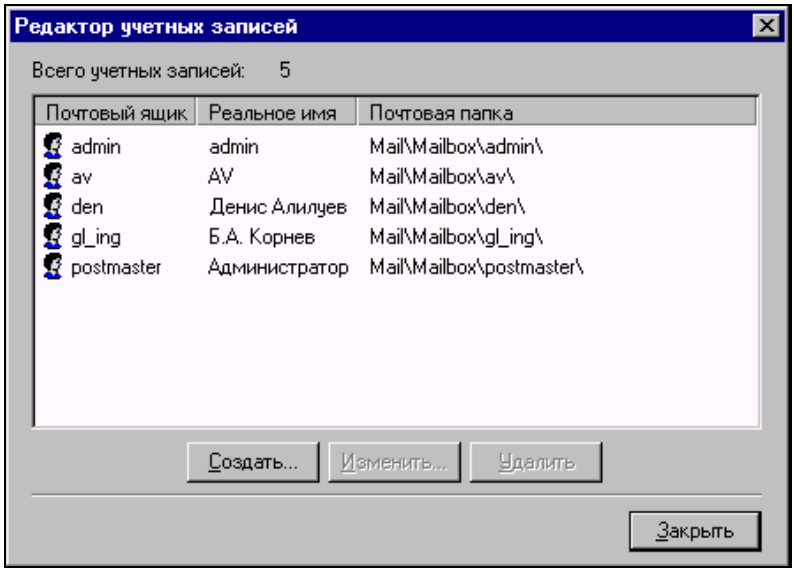


Рис. 4.21. Редактор учетных записей

- **Внешний адрес e-mail** — адрес электронной почты, которым будет заменяться локальный адрес отправителя при отправке сообщений в Интернет. Если поле пусто, то замена производиться не будет. Функция замены необходима, например, в том случае, если локальный домен официально не зарегистрирован. Предположим, что локальный домен называется **mycompany.ru** и не зарегистрирован. Локальный пользователь с адресом **user@mycompany.ru** отправил сообщение через Интернет. Возможны два варианта:

  - SMTP-сервер, через который производится отправка, откажется принимать такое сообщение, так как домен mycompany.ru ему неизвестен;
  - сообщение будет принято и доставлено получателю, но ответ на него не дойдет до адресата, так как в его адресе — **user@mycompany.ru** — указан домен, который не зарегистрирован, и, соответственно, неизвестен почтовым серверам Интернета.

  Таким образом, в описанных ситуациях необходимо использовать замену адреса. Если в поле ввести реально существующий адрес электронной почты (например, почтовый ящик, размещенный у провайдера), то сервер, принимающий сообщение, будет считать, что оно отправлено с этого адреса. Ответ на сообщение будет также доставлен на указанный адрес.

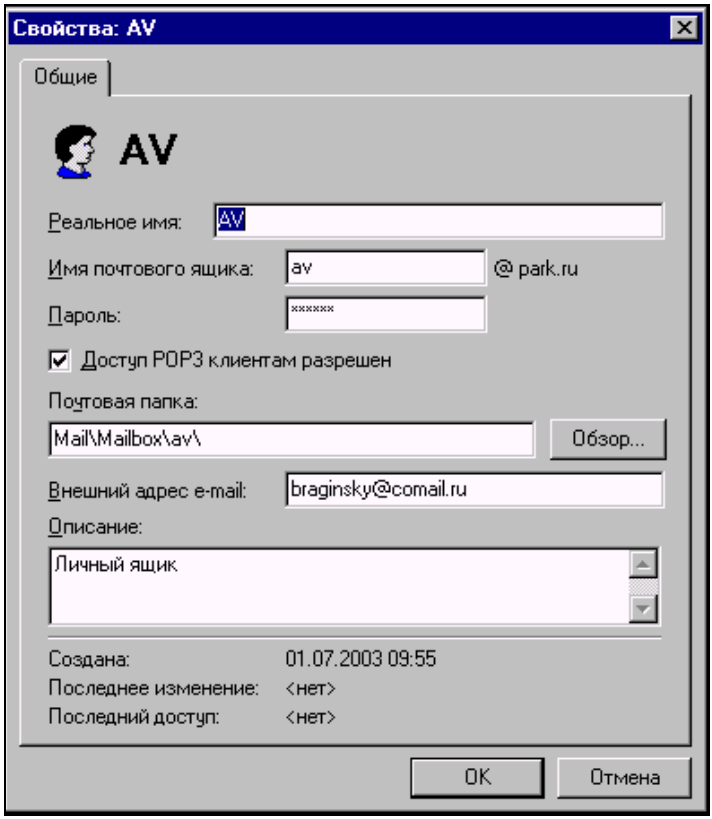


Рис. 4.22. Окно свойств учетной записи

- **Описание** — любой текстовый комментарий.
- **Создана** — дата и время создания учетной записи.
- **Последнее изменение** — дата и время последней модификации.
- **Последний доступ** — дата и время последнего подключения к почтовому ящику.

IP-фильтр

Окно свойств фильтра с правилами фильтрации изображено на рис. 4.23.

При выборе переключателя **Разрешить все подключения** фильтрация подключений производиться не будет.

Если установить переключатель **Фильтровать на основе списка правил** — для фильтрации будет использоваться список правил фильтра. В каждом правиле можно указывать либо конкретный IP-адрес, либо диапазон, при этом фильтрации подвергаются все адреса, входящие в диапазон. Правило распространяется на протоколы, отмеченные флажками. Подключения, не удовлетворившие ни одному правилу, блокируются. Правила при фильтрации просматриваются сверху вниз, поэтому более общие правила должны находиться ниже более конкретных.

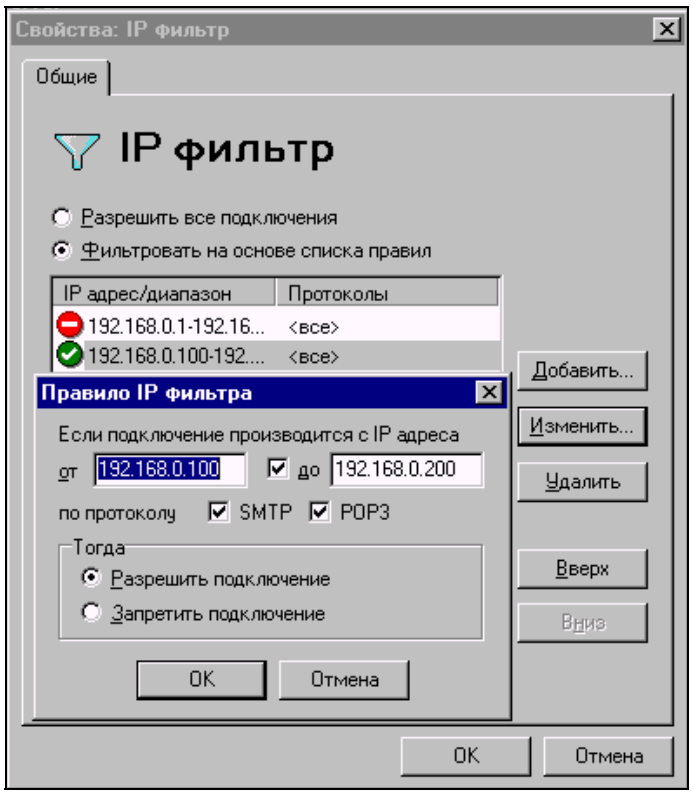


Рис. 4.23. Окно свойств фильтра с правилами фильтрации

Группа **Для адресов, не указанных в списке** используется для задания прав подключения с адресов, не попавших в список.

Рассмотрим пример. Необходимо разрешить подключение к серверу с локального компьютера (127.0.0.1) и из локальной сети (192.168.10.*x*). С адреса

192.168.10.12 запретить подключение к SMTP-серверу. С остальных адресов запретить любые подключения.

Выбираем переключатель **Фильтровать на основе списка правил** и создаем по порядку три правила:

1. 127.0.0.1, SMTP и POP3, разрешить.
2. 192.168.10.12, SMTP, запретить.
3. 192.168.10.1-192.168.10.255, SMTP и POP3, разрешить.

SMTP/POP3-серверы

Окна свойств SMTP- и POP3-серверов показаны на рис. 4.24 и 4.25.

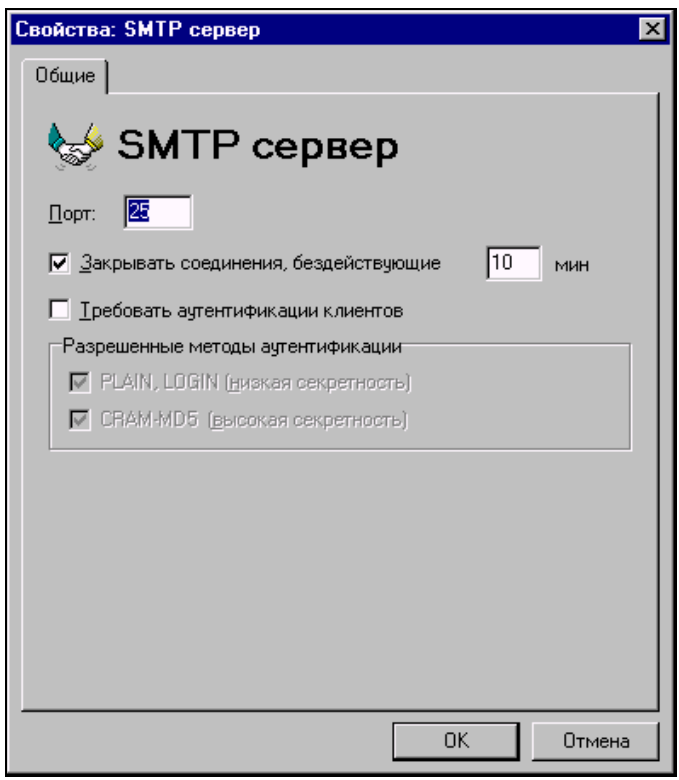


Рис. 4.24. Окно **Свойства: SMTP сервер**

В поле **Порт** указывается номер порта, на котором будет работать сервер. Стандартные значения: для SMTP — 25, для POP3 — 110. При изменении порта сервер начнет работать на нем только после перезапуска (изменение выполняется на панели статистики через контекстное меню, которое появляется при щелчке правой кнопкой мыши по значку соответствующего сервера).

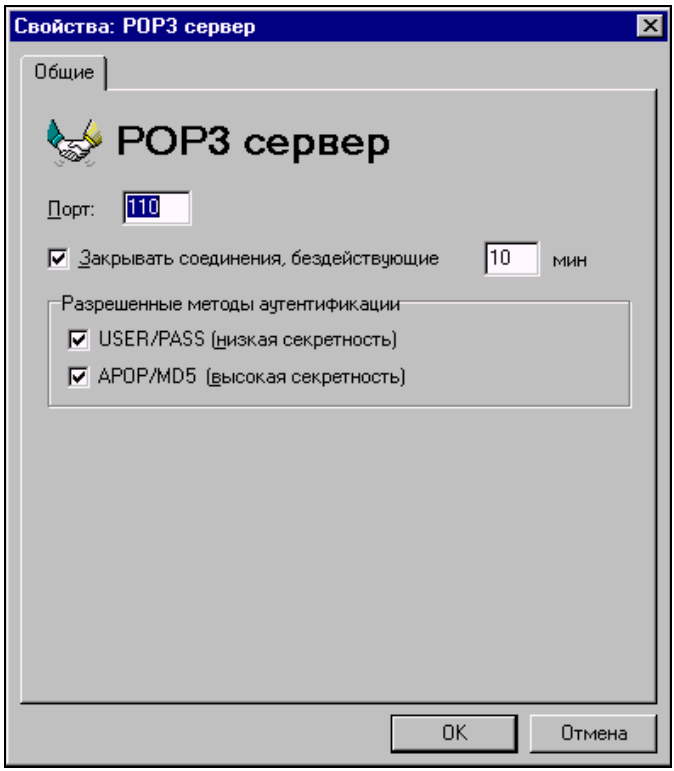


Рис. 4.25. Окно **Свойства: POP3 сервер**

Установленный флажок **Закрывать соединения, бездействующие** и поле **мин** применяются для задания промежутка времени, по истечении которого соединение принудительно разрывается, если клиент не отправил на сервер никаких данных. Стандартное значение — 10 мин, но для локальной сети можно указать меньшее значение, так как поддержка бездействующих соединений отнимает ресурсы сервера.

В группе **Разрешенные методы аутентификации** перечислены методы аутентификации, поддерживаемые сервером. Методы, отмеченные флажка-

ми, разрешено использовать. На SMTP-сервере обязательная аутентификация клиентов может быть отключена, если сброшен флажок **Требовать аутентификации клиентов**.

SMTP-клиент

Для связи с SMTP-сервером провайдера служит SMTP-клиент (рис. 4.26).

В текстовое поле **SMTP сервер** вводится имя или IP-адрес SMTP-сервера, через который будет отправляться почта в Интернет. Обычно указывается почтовый сервер провайдера.

Поле **Порт** содержит номер порта подключения к серверу. Стандартное значение — 25.

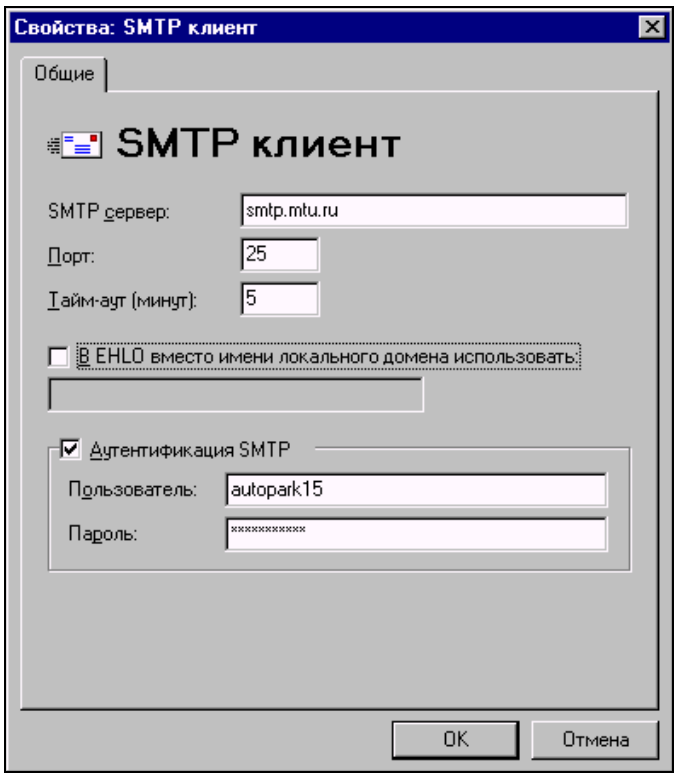


Рис. 4.26. Окно **Свойства: SMTP клиент**

Если в течение времени, указанного в поле **Тайм-аут (минут)**, сервер не вернул никаких данных, соединение принудительно разрывается. Стандартное значение — 5 мин.

Если флажок **В EHLO вместо имени локального домена использовать** установлен, то при подключении к серверу в команде `EHLO` (Extended hello — одна из команд протокола ESMTP, которая поддерживается большинством современных почтовых серверов и заменяет старую команду `HELLO` протокола SMTP. По этой команде сервер сообщает о поддерживаемых им сервисах. Если команда не поддерживается сервером, то она заменяется на `HELLO`. При получении этой команды опрашиваемый сервер пытается опознать клиента.) будет указана заданная строка, иначе — имя локального домена.

Группа **Аутентификация SMTP** используется при необходимости аутентификации на SMTP-сервере.

POP3-клиент

Для связи с POP3-сервером провайдера служит POP3-клиент (рис. 4.27).

POP3-клиент содержит список внешних почтовых ящиков (учетных записей), из которых необходимо забирать почту.

Параметры внешней учетной записи

На рис. 4.28 показано окно для ввода параметров внешней учетной записи.

Если установлен флажок **Получать сообщения этой учетной записи**, почта из данного ящика будет забираться.

В текстовое поле **POP3 сервер** вводится имя (или IP-адрес) POP3-сервера, на котором расположен внешний почтовый ящик.

Номер порта подключения к серверу задается в поле **Порт**. Стандартное значение — 110.

Поле **Пользователь** предназначено для указания имени пользователя почтового ящика. Обычно оно совпадает с именем почтового ящика (слева от символа @ в адресе электронной почты).

Можно установить пароль почтового ящика в поле **Пароль**.

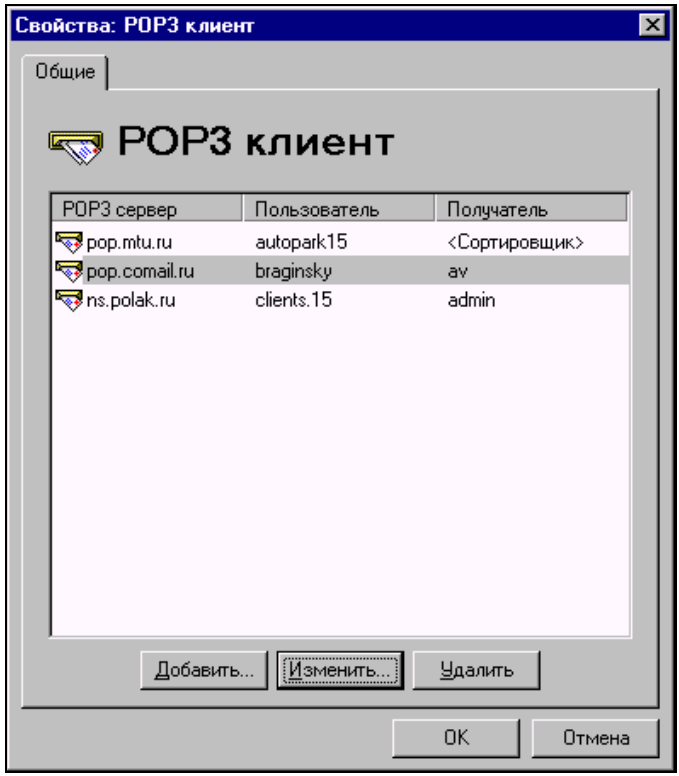


Рис. 4.27. Окно **Свойства: POP3 клиент**

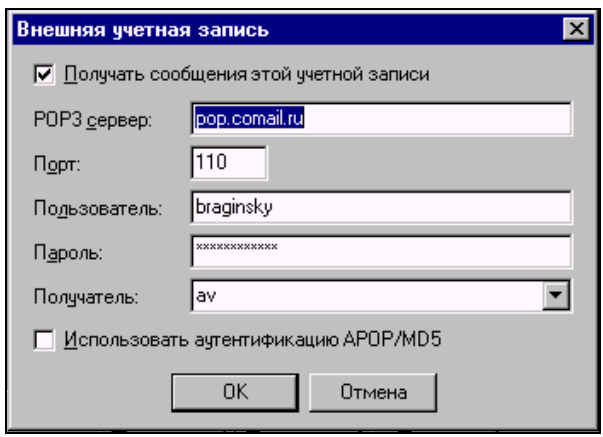


Рис. 4.28. Окно **Внешняя учетная запись**

Текстовое поле **Получатель** содержит адрес, на который будут доставляться принятые письма. Из списка можно выбрать любой локальный почтовый ящик, Домен или Сортировщик.

> ***Примечание***
>
> Можно не выбирать значение из списка, а ввести список адресов (в том числе и внешних), перечисленных через запятую. Сообщения будут перенаправлены на эти адреса. При указании в качестве получателя <Домен> адрес получателя для локального домена ищется сначала в полях **Received:**, а в случае неудачи — в полях **To:** и **Cc:**.

Если установлен флажок **Использовать аутентификацию APOP/MD5**, то при подключении к серверу вместо стандартной аутентификации USER/PASS будет использоваться безопасный метод APOP/MD5. Некоторые POP3-серверы могут не поддерживать этот метод аутентификации.

Планировщик

Планировщик (рис. 4.29) CMS управляет получением и отправкой сообщений в соответствии с расписанием.

Если в этом окне установлен флажок **Выполнять задания планировщика**, то задания будут выполняться. Список содержит задания планировщика.

Параметры задания

Параметры для каждого задания (рис. 4.30) устанавливаются индивидуально и очень гибко.

Вкладка *Общие*. На этой вкладке задается наименование задания (поле **Имя**) и выбирается из списка в поле **Задание** действие, которое должно быть выполнено.

Группа **Время выполнения** устанавливает временные характеристики задания:

- **однократно** — задание выполнится один раз, время выполнения указывается в поле **в** (в формате ЧЧ:ММ);
- **периодически** — задание будет выполняться периодически, период указывается в поле **каждые** (в формате ЧЧ:ММ). Если установлен флажок

круглосуточно, то задание будет выполняться с 00:00 до 23:59, иначе следует задать поля **с** и **до**;

- **По следующим дням** — установите флажки у тех дней недели, в которые задание должно выполняться.

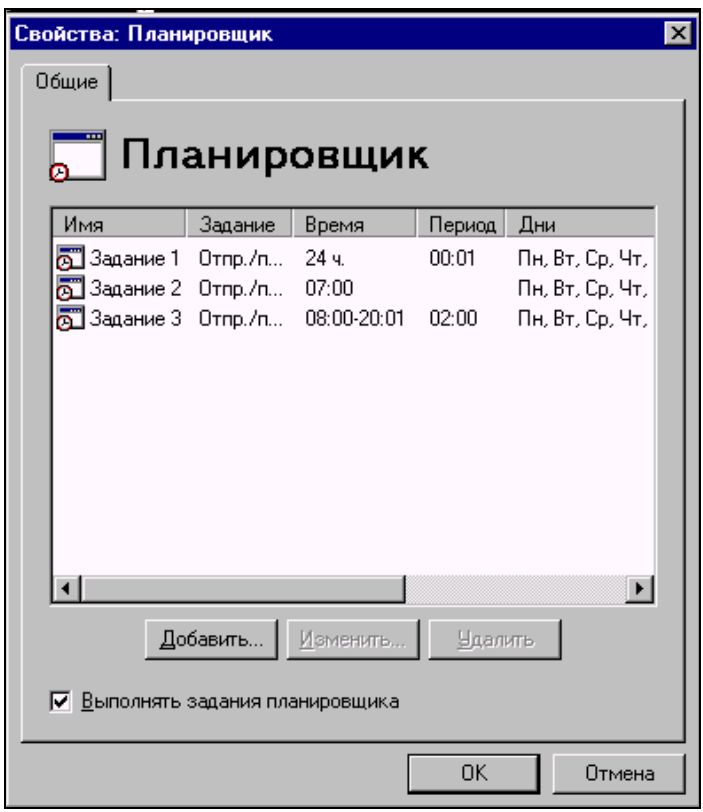


Рис. 4.29. Окно **Свойства: Планировщик**

Если флажок **Собственные настройки для подключения к Интернет** установлен, то на дополнительной вкладке **Подключение** можно задать параметры подключения для данного задания. Если флажок не установлен, то для подключения используются настройки домена.

Отмеченный флажок **Выполнять задание** свидетельствует о том, что задание будет выполняться.

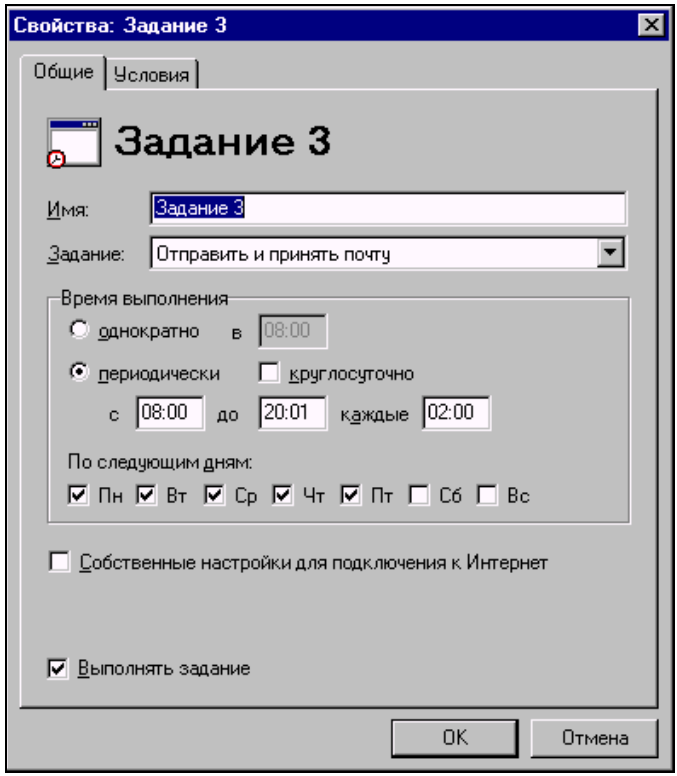


Рис. 4.30. Окно **Свойства: Задание 3**

Условия задания

Вкладка *Условия*. Группа **Условия выполнения** этой вкладки содержит перечень условий, которые проверяются перед выполнением задания. Условия с установленными флажками — активные. Они проверяются в тот момент, когда должно начаться выполнение задания. Если хотя бы одно из активных условий выполняется, то задание запускается. Далее приводится список условий:

- **если число исходящих сообщений** — условие выполнено, если количество сообщений в очереди исходящих не меньше указанного значения;
- **если объем исходящих сообщений** — условие выполнено, если совокупный объем всех сообщений в очереди исходящих не меньше указанного значения;

- **если сообщения ожидают отправки** — условие выполнено, если самое старое сообщение в очереди исходящих находится там не меньше указанного времени;
- **если существует файл** — условие выполнено, если существует указанный файл. В имени файла можно использовать символы маски "?" и "*" (например, Mail\Mailbox\scheduler*.msg);
- **удалить файл после запуска задания** — если флажок установлен, то после выполнения задания файл удаляется.

Удаленный доступ

В окне программы CMS **Свойства: Удаленный доступ** (рис. 4.31) выводится список соединений удаленного доступа.

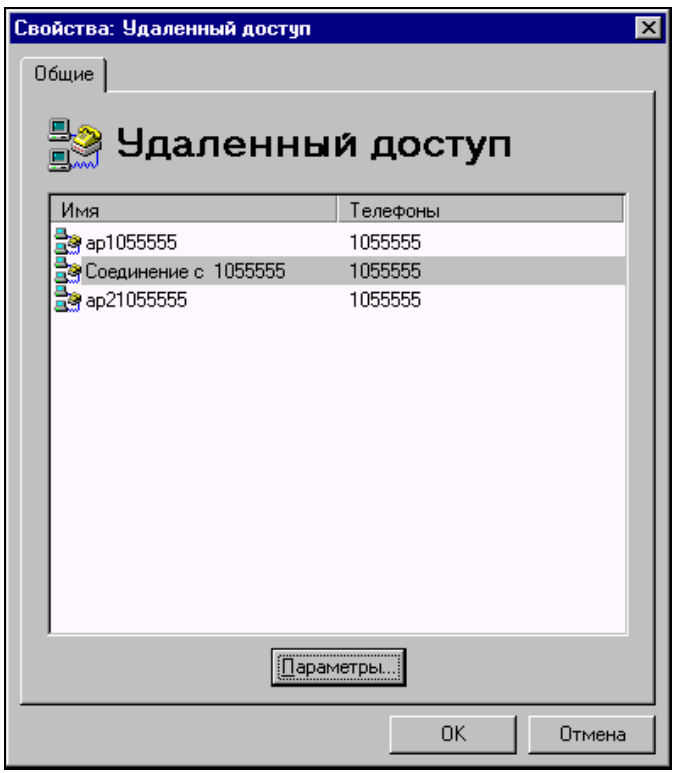


Рис. 4.31. Окно **Свойства: Удаленный доступ**

Для каждого соединения можно установить не зависящие от настроек Windows параметры (рис. 4.32).

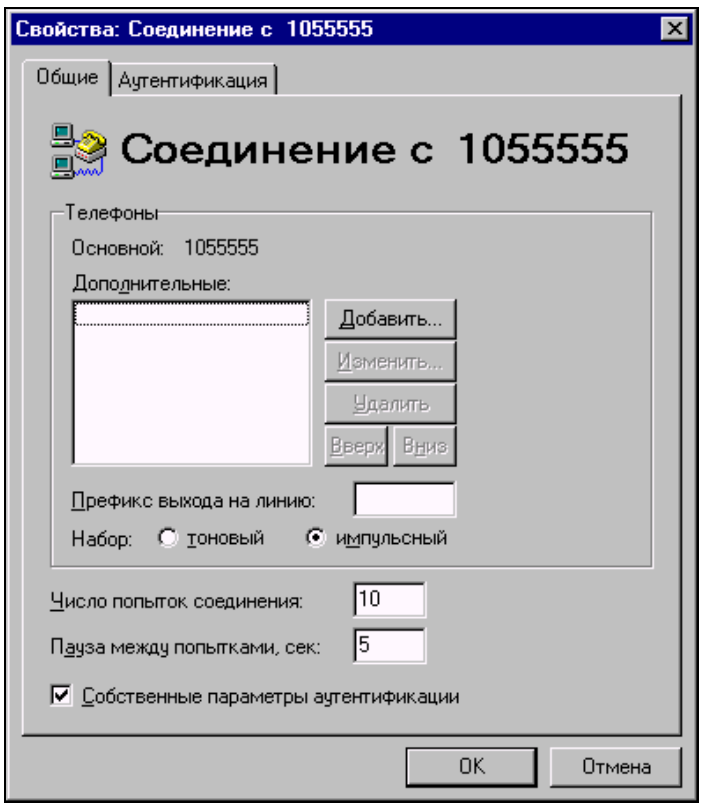


Рис. 4.32. Окно **Свойства: Соединение с <номер телефона>**

Группа **Телефоны** на вкладке **Общие** включает в себя следующие параметры:

- **Основной** — основной номер телефона соединения;
- **Дополнительные** — список дополнительных номеров телефонов;
- **Префикс выхода на линию** — назначение следует из названия;
- **Набор тоновый/импульсный** — тип набора номера.

В поле **Число попыток соединения** можно указать число попыток установки соединения.

Задержка в секундах перед следующей попыткой задается в поле **Пауза между попытками, сек**.

При соединении с провайдером сначала используется основной номер телефона, а затем дополнительные номера по порядку. Если попытка соединения не удалась, выдерживается пауза и производится попытка соединения по следующему номеру. При достижении конца списка номеров попытки соединения повторяются, начиная с основного номера и т. д. до исчерпания попыток.

Если установлен флажок **Собственные параметры аутентификации**, то на дополнительной вкладке **Аутентификация** можно задать параметры аутентификации для данного соединения. Если флажок не установлен, для аутентификации используются данные Windows.

Вкладка *Аутентификация*. Эта вкладка содержит параметры для аутентификации на удаленном компьютере после установления связи. Если провайдер не требует указания домена при подключении, то поле **Домен** можно оставить пустым.

Сортировщик

Сортировщик почты в составе программы CMS на основе задаваемых правил перенаправляет определенным получателям сообщения, пришедшие из внешних почтовых ящиков.

Список правил сортировки

Сортировщик содержит список правил (рис. 4.33), на основе которых и происходит сортировка сообщений.

В текстовое поле **Доставлять неотсортированную почту по адресам** через запятую вводится список адресов, по которым будут доставляться сообщения, не удовлетворившие ни одному правилу. Если не указан ни один адрес, сообщения будут доставляться администратору.

Если установить флажок **Дублировать проходящую почту на адреса**, то в расположенном ниже текстовом поле можно через запятую указать список адресов, на которые будут направляться копии всех сообщений, получаемых SMTP-сервером.

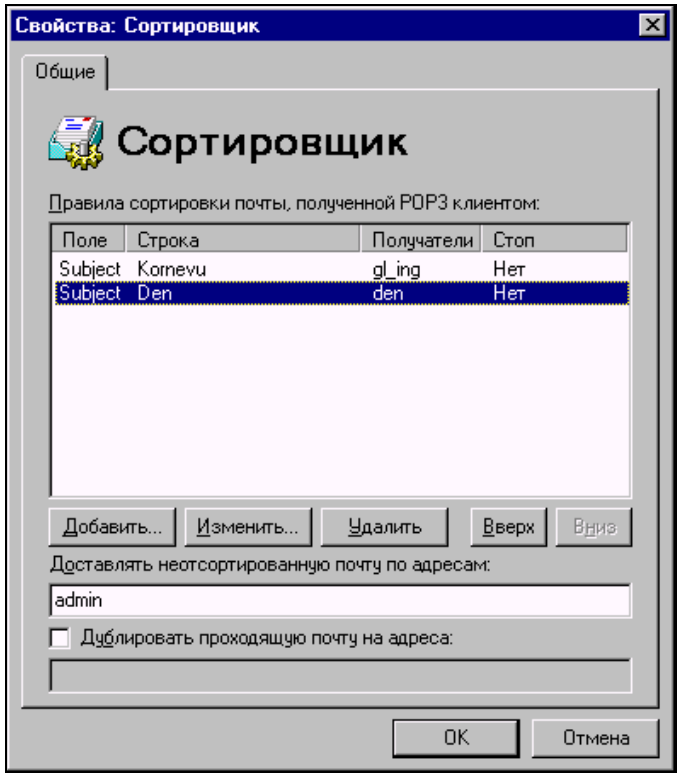


Рис. 4.33. Окно **Свойства: Сортировщик**

Параметры правил сортировки

Правила сортировки задаются в отдельном окне (рис. 4.34).

В списке **Если поле заголовка** выбирается анализируемое поле заголовка сообщения. Кроме того, можно ввести значение вручную, если оно отсутствует в списке.

В поле **Содержит текст** вводится текст для поиска в значениях анализируемого поля заголовка сообщения.

Список получателей, которым будет доставлено данное сообщение, если правило выполняется, включается в многострочное поле **Тогда доставить сообщение по следующим адресам**. Можно указывать как локальных, так и внешних получателей.

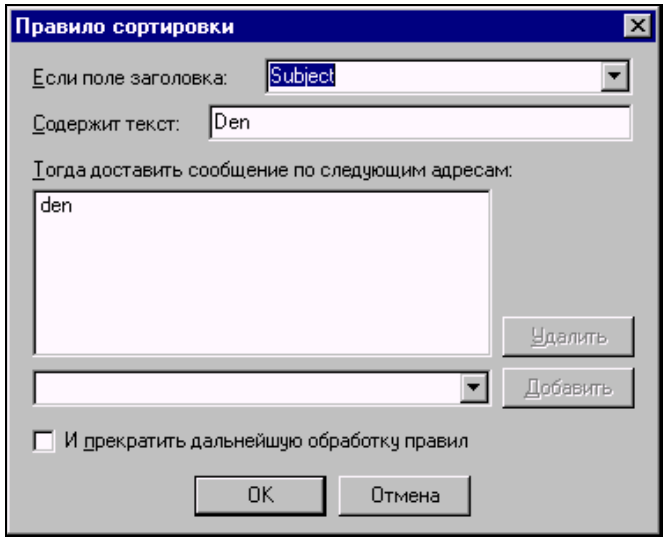


Рис. 4.34. Окно **Правило сортировки**

Если установить флажок **И прекратить дальнейшую обработку правил**, то все остальные правила не будут проверяться для данного сообщения.

Для каждого сообщения проверяются последовательно все правила до тех пор, пока не будет достигнут конец списка или не выполнится правило, у которого установлен флажок прекращения дальнейшей обработки. Правило выполняется, если в заголовке сообщения имеется указанное поле и оно содержит указанный текст. В этом случае происходит доставка сообщения указанным получателям.

Журнал

Управление журналом доступно из окна, открывающегося при выборе подпункта **Журнал** из пункта **Настройки** меню программы.

В группу **Режим сохранения в файл** входят следующие переключатели:

- **Не сохранять** — журнал не будет сохраняться в файл (только отображение на экране);
- **Отдельный файл для каждой даты** — журнал за каждую дату сохраняется в файл с именем вида ГГГГДДММ.log;

- **Отдельный файл для каждого дня недели** — журнал за каждый день недели сохраняется в файл с названием дня недели (Monday.log, Tuesday.log и т. д.);
- **Один общий файл** — журнал записывается в один файл с именем, указанным в поле **Имя файла**. В этом поле нужно указывать только имя файла, без папки. Папка журнала настраивается с помощью окна свойств домена.

Если установлен входящий в группу флажок **Ограничить размер файла**, то при достижении файлом журнала размера, указанного в поле **NN Кб**, он закрывается и его расширение меняется на old. Если файл с расширением old существует, он удаляется. Журнал продолжает сохраняться во вновь созданный файл с расширением log.

Группа **Уровень подробности** содержит три уровня:

- **Низкий** — записываются сообщения об ошибках и наиболее важные системные сообщения;
- **Средний** — кроме сообщений низкого уровня записываются сообщения о запуске/остановке компонентов, подключении/отключении клиентов, работе сортировщика;
- **Высокий** — записываются сообщения обо всех событиях сервера.

Настройки почтовых клиентов

Эти настройки необходимо произвести на компьютерах пользователей, которым нужен доступ к электронной почте посредством CMS. Для того чтобы почтовый клиент мог отправлять и принимать почту, в его настройках нужно указать адреса серверов входящей и исходящей почты, а также параметры учетной записи для подключения к почтовому ящику. Настройки в разных почтовых клиентах могут иметь различные названия, но обычно применяются следующие параметры: **SMTP сервер**, **POP3 сервер, Пользователь (Учетная запись)**, **Пароль**.

В поля **SMTP сервер** и **POP3 сервер** введите адрес компьютера, на котором запущен CMS. Рекомендуется вводить IP-адрес, а не сетевое имя, так как при этом сервер не будет тратить дополнительное время на определение IP-адреса по сетевому имени (что, кстати сказать, не всегда возможно). IP-адрес компьютера вы можете узнать, запустив на нем программу ipconfig.exe или winipcfg.exe.

Если клиент запущен на том же компьютере, что и сервер, то для этого клиента в качестве IP-адреса серверов можно указать 127.0.0.1 (соответствующее сетевое имя — localhost). В поля **Пользователь (Учетная запись)** и **Пароль** введите имя и пароль почтового ящика, которые указаны в свойствах этого ящика на сервере. Если сервер использует нестандартные номера портов, то в клиентской программе укажите соответствующие значения (для этого обычно имеется поле **Порт**). Тип подключения к серверу — с помощью локальной сети.

Эксплуатация

Правильно установленный и настроенный сервер не требует постоянного внимания администратора и работает в автоматическом режиме. Текущие подключения клиентов к серверу, а также исходящие подключения к внешним SMTP- и POP3-серверам выводятся на панель подключений.

Для каждого подключения отображаются следующие параметры:

- значок, обозначающий тип подключения;
- **Сессия** — идентификатор почтовой сессии;
- **Протокол** — протокол, по которому выполнено подключение;
- **Адрес** — имя или IP-адрес клиента/сервера, с которым идет обмен;
- **Имя пользователя** — для SMTP-подключений отображается аргумент команды `EHLO` и имя пользователя. Для POP3-подключений отображается имя пользователя (для клиентских подключений имя пользователя отображается только после аутентификации);
- **Время подключения** — дата и время подключения. Для принудительного отключения клиента выделите соответствующий элемент в списке и в контекстном меню выберите команду **Удалить**.

Для остановки CMS в меню **Файл** выберите команду **Остановить**.

События, происходящие на сервере, записываются в журнал. Журнал ведется одновременно в файле и на экране. Строки экранного журнала можно копировать, вырезать в буфер обмена и удалять с помощью команд контекстного меню.

Формат строки журнала следующий:

- тип события: `" "` — информация, `"!"` — ошибка, `"*"` — предупреждение, `"+"` — подключение, `"-"` — отключение, `"x"` — подключение клиента

заблокировано IP-фильтром, `">"` — отправка строки, `"<"` — прием строки, `"@"` — действие с почтовым сообщением;

- ❒ дата и время события;
- ❒ имя компонента, к которому относится событие;
- ❒ идентификатор почтовой сессии;
- ❒ описание события.

Сеансы обмена почтой через Интернет можно инициировать вручную. Для отправки почты в меню **Сервис** выберите команду **Отправить почту**, а для приема — команду **Принять почту**.

Имеется возможность удаленного запуска заданий планировщика. Для этого создайте отдельную учетную запись, например scheduler. В планировщике создайте задание на отправку/прием почты круглосуточно каждую минуту, с условием **если существует файл**. В качестве имени файла укажите путь к почтовой папке созданной учетной записи — Mail\Mailbox\scheduler*.msg. Установите флажок **Удалить файл после запуска задания**. Теперь отправьте любое сообщение на адрес созданной учетной записи (например, scheduler@<локальный_домен>). После того как оно попадет в почтовый ящик scheduler, в течение минуты запустится задание планировщика.

Для раздельного управления отправкой/приемом почты создайте, соответственно, две учетные записи (например, scheduler_send и scheduler_recv) и настройте два задания планировщика.

Если при попытке отправки сообщения в Интернет удаленный SMTP-сервер не принял ни одного адреса получателя или вернул код постоянной ошибки (5xx), файл сообщения получает расширение bad и попыток его отправить больше не производится. Постоянная ошибка сервера означает, что данное сообщение не может быть отправлено без корректировки. Причину отказа сервера и код ошибки можно найти в журнале (искать лучше всего по имени файла сообщения — *.msg).

Для повторной попытки отправить такое сообщение дайте файлу расширение msg. Вероятнее всего, повторная попытка будет также неудачной.

Если в свойствах домена не указан администратор или его почтовая папка недоступна, то сообщения, направленные ему, будут удаляться.

Безопасность

В программе есть две ступени защиты сервера от несанкционированного доступа:

- фильтрация клиентских подключений;
- аутентификация подключившихся пользователей.

При подключении клиента его IP-адрес анализируется IP-фильтром и, если подключение запрещено, соединение принудительно разрывается. Данный факт отражается в журнале.

Если круг компьютеров, которым разрешен доступ к CMS, ограничен, настройте IP-фильтр таким образом, чтобы он разрешал подключение только с этих компьютеров и блокировал прочие подключения. Тем самым пресекаются попытки подключения к серверу с несанкционированного компьютера.

Однако возможны ситуации, когда с разрешенного компьютера осуществляется попытка несанкционированного доступа к серверу. Это могут быть, например, действия вируса. Для защиты от подобных действий используется аутентификация (проверка имени пользователя и пароля). Если она выполнена успешно, клиент получает доступ к серверу.

Методы аутентификации SMTP- и POP3-серверов можно условно разделить на две группы: с низкой секретностью и с высокой.

При использовании *методов с низкой секретностью* (для SMTP — это PLAIN и LOGIN, для POP3 — USER/PASS) пароль на сервер передается в открытом виде.

При использовании *методов с высокой секретностью* (для SMTP — это CRAM-MD5, для POP3 — APOP/MD5) на сервер передается результат преобразования пароля, объединенного с другими данными, специальной хэш-функцией. Восстановить исходный пароль, зная результат преобразования, невозможно. Поэтому, даже если злоумышленник перехватит аутентификационные данные, передаваемые по сети, пароль он раскрыть не сможет.

Таким образом, рекомендуется использовать только методы с высокой секретностью, если их поддерживают почтовые клиенты, которые будут подключаться к серверу (это можно определить экспериментальным путем).

Проверка работоспособности

После установки и настройки сервера и клиентов необходимо проверить их взаимодействие.

Предположим, что локальным доменом является **mydomain.ru**, порты SMTP/POP3-серверов — стандартные (25 и 110 соответственно) и на сервере имеются два почтовых ящика — user1 и user2. Запустите почтовый клиент на компьютере пользователя user1 и создайте новое сообщение. В поле **Кому (To)** введите адрес **user2@mydomain.ru**. Введите любую тему и содержание письма. Отошлите письмо. Оно должно без ошибок отправиться на сервер.

Запустите почтовый клиент на компьютере пользователя user2 и примите почту. Должно прийти сообщение от user1. (Если сообщение не принято, подождите несколько секунд, пока оно попадет в почтовый ящик, и примите почту снова.) Создайте и отправьте ответ на сообщение. Примите почту для user1.

Если оба письма нормально отправлены и приняты, можно считать почтовую систему в локальной сети работоспособной.

Устранение неполадок

В случае возникновения проблем с отправкой или получением почты придерживайтесь следующего порядка действий:

1. Убедитесь, что при загрузке CMS запускаются SMTP/POP3-серверы (это отражается в журнале). Если они не запускаются, это означает, что какое-то другое запущенное приложение использует данные порты. Либо остановите это приложение, либо настройте серверы CMS на другие порты и запустите их.
2. Если SMTP/POP3-серверы запускаются нормально, нужно попробовать подключиться к ним с компьютера пользователя при помощи служебной программы Telnet. Для этого в меню **Пуск** выберите команду **Выполнить** и введите: `telnet <адрес> <порт>`, где адрес — это IP-адрес или сетевое имя компьютера, на котором запущен CMS. Порт — это порт SMTP- или POP3-сервера CMS (стандартные значения 25 и 110).
3. После выполнения команды `telnet <адрес> <порт>` в окне программы Telnet должна появиться строка, начинающаяся с символов "220" для SMTP-сервера и "+OK" для POP3-сервера. В строке должно также содер-

жаться имя локального домена, назначенное в CMS. В этом случае соответствующий сервер доступен с данного компьютера.

Если серверы доступны, а почта не принимается или не отправляется, скорее всего, неправильно настроен почтовый клиент. Проверьте его настройки, возможно, указано неправильное имя пользователя или пароль.

Если сервер недоступен из программы Telnet, то причина либо в настройке сервера (или он не запущен), либо в проблемах сети. Проверьте настройки сервера, просмотрите файл журнала — там должны отражаться факты подключений/отключений и обмен данными по почтовым протоколам. Возможно, потребуется повысить уровень подробности журнала, чтобы детально разобраться в проблеме.

Для более комфортной работы с журналом разработчики предлагают дополнительную утилиту CMS Log Viewer (рис. 4.35), которую можно скопировать с сайта программы.

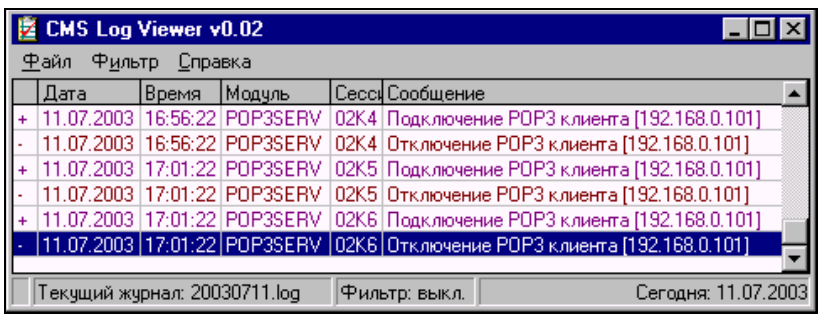


Рис. 4.35. Окно дополнительной утилиты CMS Log Viewer

Почтовый сервер из состава Windows Server 2003

Для того чтобы настроить сервер для работы в качестве почтового сервера, можно воспользоваться различными средствами, в том числе и встроенными в операционную систему. Эти средства в большинстве случаев обеспечивают основные потребности сети. В тех случаях, когда работа с электронной почтой составляет одно из основных занятий пользователей сети, лучше приме-

нять программы, разработанные для этой цели. Пользователи нашей сети не испытывают никаких неудобств при работе с почтовым сервером, который входит в состав Windows Server 2003. Почта у нас используется по своему прямому назначению — пользователи общаются с внешним миром. Для того чтобы иметь возможность получать почту на ваш почтовый сервер, необходимо зарегистрировать ваш домен в Интернете. Для этого есть много возможностей. Одна из них — получить домен второго уровня. Очень часто это предлагается сделать бесплатно. Если ваш провайдер выдает вам динамический IP-адрес, который изменяется с каждым подключением или просто периодически, то можно воспользоваться службами типа DinDNS (**http://www.dyndns.org**) или другими подобными. При условии, что ваш сервер практически постоянно подключен к Интернету, вы сможете всегда найти его из Интернета по символьному адресу. А для работы почты большего и не требуется. Мы не будем рассматривать технологии, которые используются для этих целей, но отметим, что подобные услуги часто бесплатны в объеме, достаточном для наших целей.

Перед настройкой собственно почтового сервера немного подправим работу маршрутизатора (рис. 4.36) — в уже известном нам окне **Routing and Remote Access**, но на этот раз следует добавить **Статические маршруты**. Это маршруты, которые будет использовать сервер для общения с внешним миром — Интернетом.

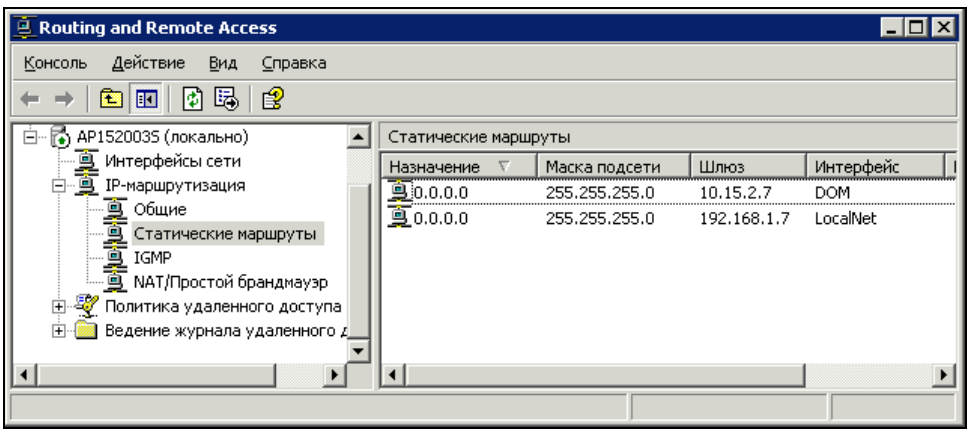


Рис. 4.36. Окно **Routing and Remote Access**

Для каждого из двух сетевых интерфейсов противоположный интерфейс становится шлюзом. Адрес назначения 0.0.0.0 обозначает, что нет никаких ограничений для адресов с обеих сторон маршрутизатора. Ограничения накладываются лишь адресом шлюза и маской подсети. В данном примере интерфейс DOM имитирует внешний интерфейс, смотрящий в Интернет. Скорее всего, для такого интерфейса маска подсети будет иной (255.255.255.252 — наиболее частый вариант), а адрес интерфейса будет соответствовать допустимому в Интернете.

Почтовый сервер начнем настраивать так же, как настраивали доступ в Интернет — воспользуемся мастером настройки сервера. На странице ролей (см. рис. 3.35) выберем **Почтовый сервер**. На следующем шаге нам будет предложено выбрать метод проверки подлинности пользователей и имя домена электронной почты. Для проверки подлинности выберем **Локальные учетные записи Windows**. Это позволит идентифицировать пользователя почты как учетную запись на сервере. Имя домена электронной почты может быть любым, если предполагается только внутреннее применение сервера, и совершенно определенным, зарегистрированным в Интернете, если сервер будет применяться для внешней связи. Для настройки примера я зарегистрировал с помощью DinDNS домен **okobox.homeip.net**. Поскольку в сети, где настраивается этот пример, почтовые серверы уже есть, мы воспользуемся нестандартным значением порта для SMTP-сервера. Это может быть полезно и в случае, когда вы хотите сделать почтовый сервер недоступным для большинства пользователей Интернета, применяя его в каких-либо специальных целях. Итак, в примере почтовый домен **okobox.homeip.net**. После ввода данных и нажатия кнопки **Далее** начнется процесс установки, во время которого может понадобиться дистрибутив системы. После завершения установки необходима ручная подстройка сервера. Для ручной настройки потребуется открывать отдельно SMTP- и POP3-серверы. SMTP открывается через **Администрирование | Диспетчер служб IIS** (рис. 4.37), а POP3 — через **Администрирование | Служба POP3** (рис. 4.38).

Для настройки порта SMTP-сервера откройте из окна **Internet Information Servise (IIS) Manager** (см. рис. 4.37) окно свойств виртуального SMTP-сервера (из контекстного меню), а в этом окне выберите вкладку **Доставка**. В нижней части этой вкладки есть кнопки **Подключения** и **Дополнительно**. Нажав кнопку **Подключения**, вы откроете окно **Исходящие подключения** (рис. 4.39).

В этом окне при необходимости можно изменить значение порта для этого сервера. В примере стандартный порт 25 заменен значением 6525.

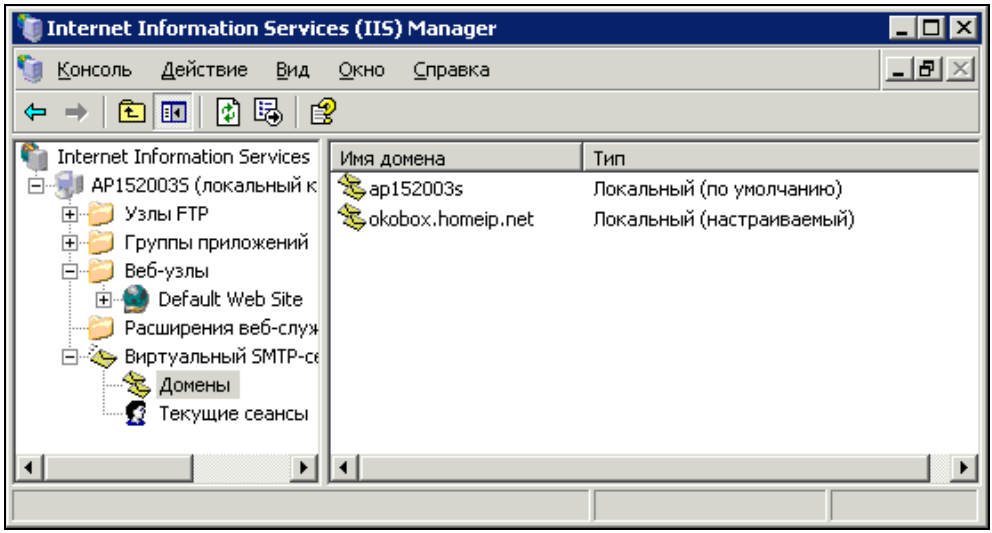


Рис. 4.37. Окно **Internet Information Services (IIS) Manager** (управление SMTP-сервером)

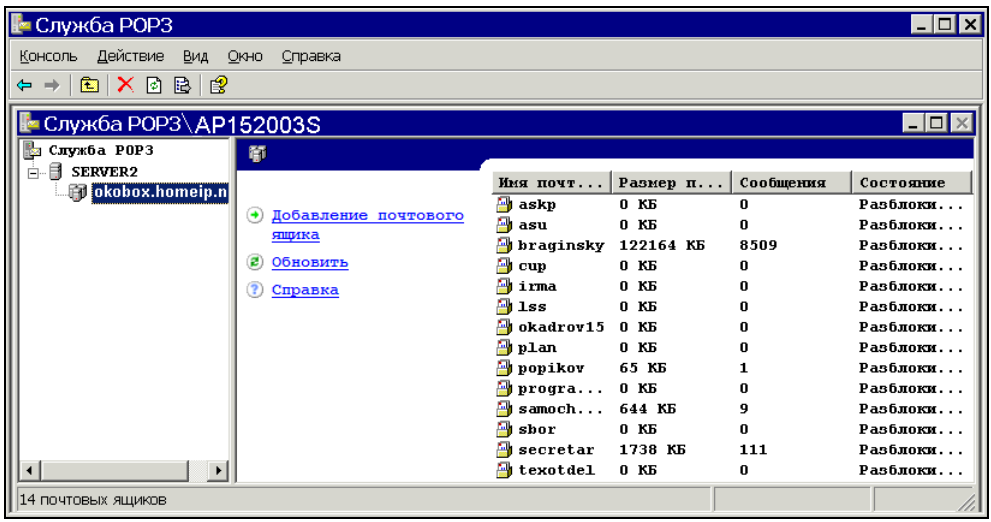


Рис. 4.38. Окно **Служба POP3** (**POP3 Service | AP152003S**)

Нажав кнопку **Дополнительно** на вкладке **Доставка**, вы откроете окно **Дополнительная настройка доставки** (рис. 4.40), в котором можно указать **Имя подменяющего домена**, предназначенное для замены имени компьюте-

ра зарегистрированным именем почтового домена. Внеся изменения в настройки SMTP-сервера, настроим POP3-сервер. Если к SMTP-серверу пока метод доступа анонимный, то POP3-сервер мы настроили для проверки подлинности по локальным учетным записям Windows. Значит, для каждого пользователя почтового сервера должна создаваться учетная запись на этом компьютере. К счастью, этот процесс автоматизирован, и учетная запись может создаваться вместе с почтовым ящиком. Для создания почтового ящика достаточно в окне **Служба POP3** (**POP3 Service | AP152003S**) (см. рис. 4.38) выделить значок почтового домена в левой части окна, а в правой выбрать пункт меню **Добавление почтового ящика** (Add Mailbox).

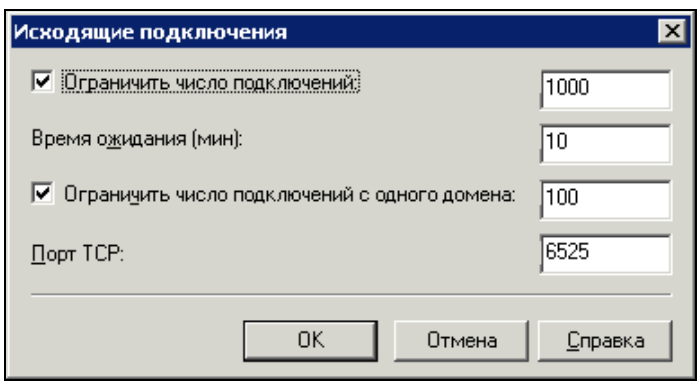


Рис. 4.39. Окно **Исходящие подключения**

При этом откроется окно **Добавление почтового ящика** (рис. 4.41). Внесите в соответствующие поля необходимые данные.

Все. Почтовый ящик для учетной записи braginsky создан. Остается совсем немного. Следует открыть порт 110 для доступа к почтовому серверу из Интернета или из первой сети.

Для этого в окне **Routing and Remote Access** (см. рис. 4.36) откройте окно свойств общего интерфейса и на вкладке **Службы и порты** (рис. 4.42) отметьте **Протокол Post-Office Protocol, версия 3 (POP3)** и укажите IP-адрес сервера, когда соответствующее поле станет доступно. Для доступа к SMTP-серверу придется создать новую службу SMTP с измененным значением порта с помощью кнопки **Добавить**. После выполнения этих действий сервер станет доступным из Интернета.

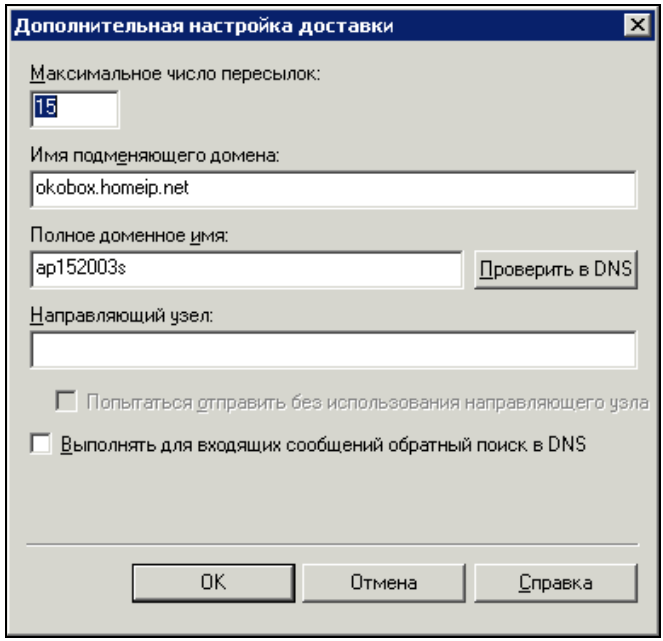


Рис. 4.40. Окно **Дополнительная настройка доставки**

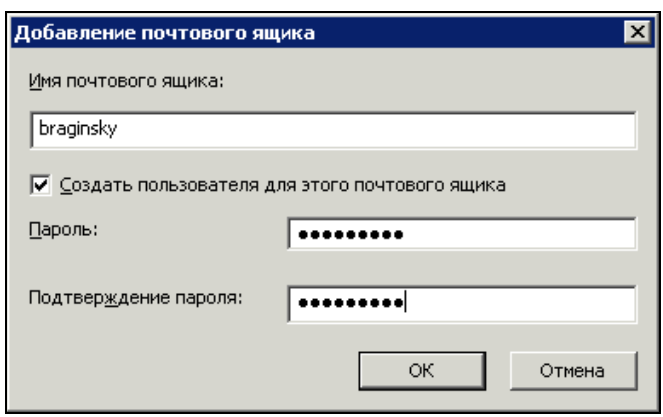


Рис. 4.41. Окно **Добавление почтового ящика**

Настраивая работу почтовых служб, обратите внимание на способ авторизации пользователей на сервере. Для SMTP-сервера есть возможность работать анонимно. Но для работы в Интернете такой вариант не годится. Вы сразу почувствуете, что вашим сервером пользуются. Доступ к SMTP-серверам в

Интернете их хозяева стараются ограничить с целью недопустить массовые несанкционированные рассылки через него (спам). Используют ограничения по IP-адресам или авторизацию.

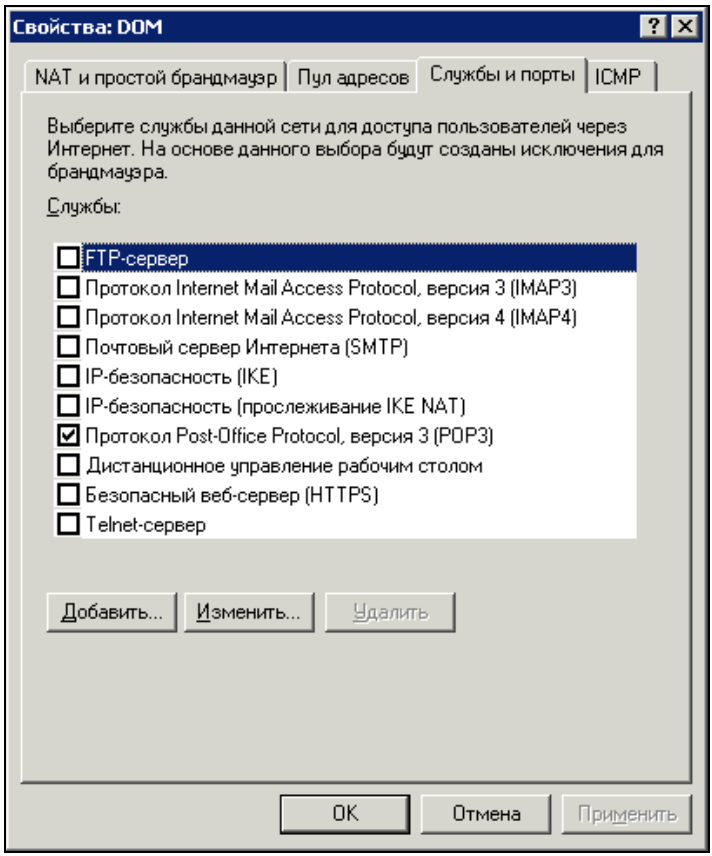


Рис. 4.42. Окно **Свойства: DOM**
(свойства интерфейса подключения к Интернету)

В рассмотренном примере сервер находится внутри сети и не имеет прямого выхода в Интернет. Почтовый сервер в таком случае будет действовать только в пределах локальной сети, для которой он настроен. Для работы сервера в Интернете, для обеспечения возможности обмена почтовыми сообщениями с пользователями Интернета необходимо, чтобы внешний интерфейс сервера был действительно внешним (рис. 4.43). Кроме того, подключение через "Срим" (ADSL для физических лиц в Москве) затрудняет полноценно ис-

пользовать почтовый сервер. Динамический IP-адрес невозможно прописать в маршрутизаторе Windows Server 2003. Доступ в Интернет для компьютеров сети, тем не менее, возможен в рассмотренном примере при любом способе подключения.

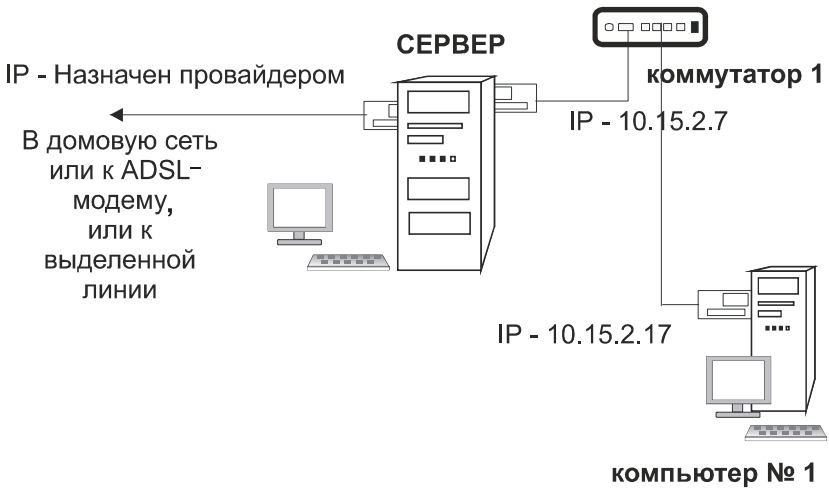


Рис. 4.43. Вариант подключения сети к Интернету через сервер

Управление почтовым сервером

SMTP-сервер обычно не требует специального управления. Все пользователи почтового сервера могут использовать SMTP-сервер для отправки сообщений. Другое дело POP3-сервер. Он используется для получения почты, а значит, должен знать своих клиентов. Как создавать почтовые ящики в локальном интерфейсе сервера, мы уже рассмотрели. Но у Windows Server 2003 есть и Web-интерфейс для управления почтовым сервером. Проверьте компоненты E-mail Services (рис. 4.44), которые установлены в вашей системе. Если не установлен компонент **POP3 Service Web Administration**, то доустановите его.

После установки этого компонента вы получите возможность управлять почтовым сервером из Интернета через Web-интерфейс. Управление сервером через этот интерфейс несколько удобнее, чем через локальный интерфейс. Поэтому на своих серверах мы часто используем Web-интерфейс даже при

локальной работе с сервером. Через этот интерфейс вы можете получить доступ к управлению не только программным почтовым сервером, но и по многим параметрам сервером в целом. Это один из способов удаленного администрирования сервера, причем хорошо защищенный.

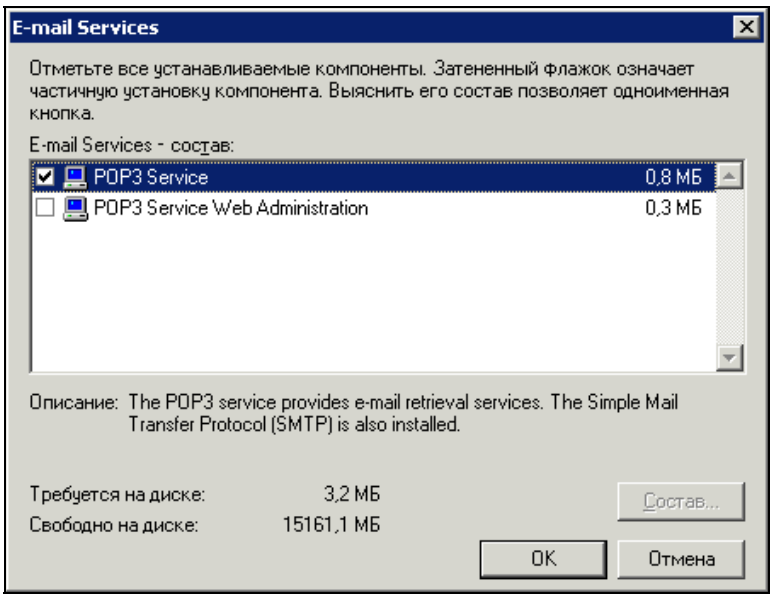


Рис. 4.44. Окно **E-mail Services**

Web-интерфейс

К сожалению, Web-интерфейс почтового сервера не имеет локализованного варианта. Даже в русской версии Windows Server 2003 он выполнен на английском языке. Тем не менее после предварительного знакомства с этим инструментом он становится абсолютно понятным и удобным.

Web-интерфейс управления сервером — это Web-сайт на вашем сервере. Для того чтобы вы имели возможность поместить на сервер и свой собственный сайт, доступ к интерфейсу управления организован по специально выделенному для этого порту. Набирая в браузере адрес своего сервера без указания номера порта, вы сможете подключаться к Web-сервисам, работающим на порту номер 80. Для управления сервером следует после адреса указать порт

8098, а протокол HTTP изменить на HTTPS. Пример адреса для подключения к интерфейсу управления сервером: **https://www.myserver.ru:8098**. Адрес, конечно, должен быть вашим, причем, может быть и внутренним из имени компьютера в сети или просто IP-адрес.

Сразу после перехода по этому адресу и прохождения авторизации вы увидите страницу, на которой может быть какое-либо сообщение. Если все работает нормально, то сообщений обычно нет и можно выбрать вкладку с необходимыми средствами управления. Например, вкладку **E-Mail** (рис. 4.45).

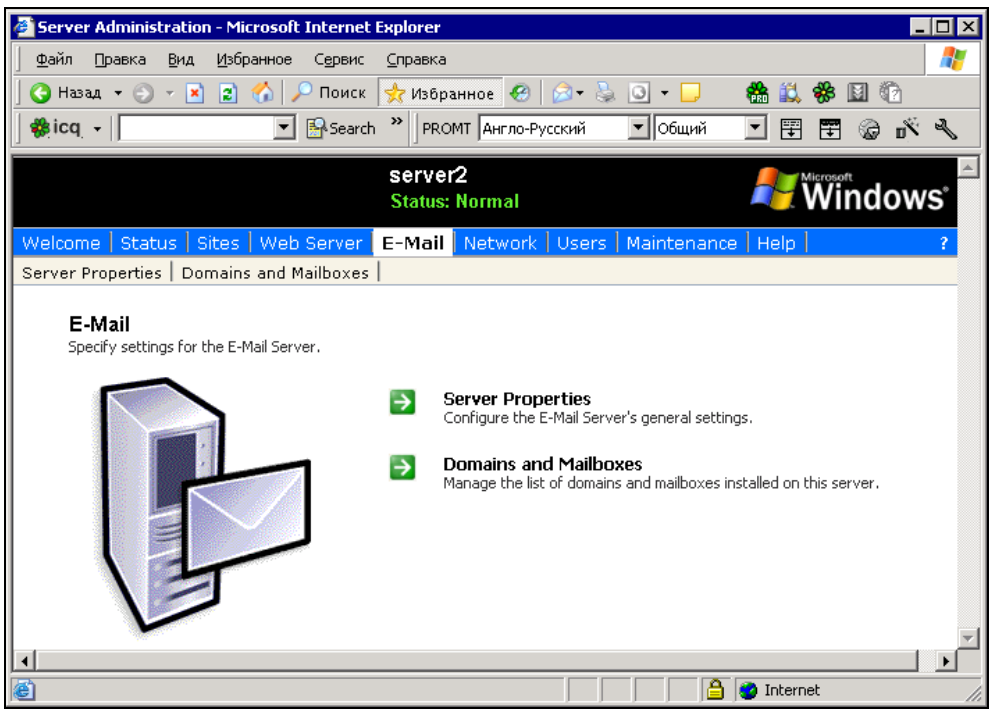


Рис. 4.45. Окно **Server Administration – Microsoft Internet Exporer**, вкладка **E-Mail**

На этой вкладке доступны два пункта меню: **Server Properties** (Свойства сервера) и **Domains and Mailboxes** (Домены и почтовые ящики). В большинстве случаев этих пунктов достаточно для повседневного администрирования почтового сервера. Выберем пункт **Server Properties** (рис. 4.46).

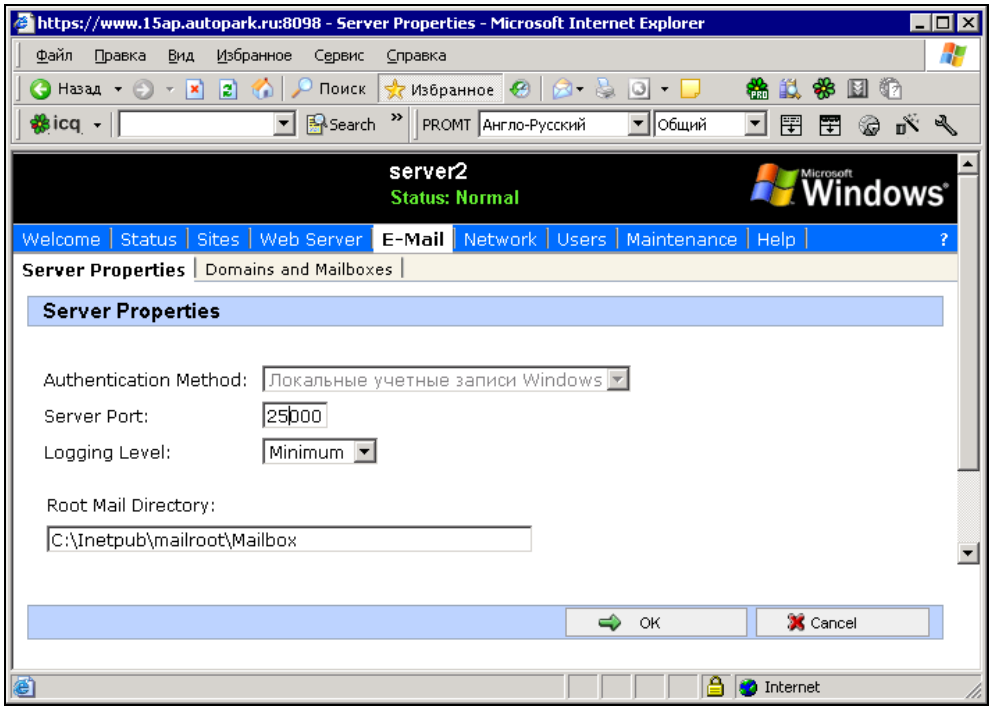


Рис. 4.46. Вкладка **Server Properties**

На открывшейся странице мы можем изменить каталог, содержащий почтовые ящики, изменить уровень протоколирования событий сервера и изменить порт, используемый сервером POP3. Изменив порт относительно стандартного значения, мы повысим защищенность сервера, поскольку только посвященные пользователи будут его знать. Кроме того, мы получаем возможность применения в той же сети и даже на том же сервере еще одного почтового сервера. Зачем это нужно? Таких ситуаций может быть много. Это и различные серверы для внешней и внутренней почты, и серверы управления, позволяющие передавать в виде почтовых сообщений команды управления сервером сети. Само собой, такой сервер должен быть лучше защищен, чем обычный почтовый сервер. Адреса и учетные записи такого сервера не должны быть доступны всем пользователям сети. Необходимость во втором почтовом сервере может никогда не возникнуть у многих пользователей и администраторов сети, но когда она возникнет, мы можем беспрепятственно устанавливать его, не опасаясь, что возникнет конфликт с уже существующим почтовым сервером.

Примечание

Работая с несколькими почтовыми серверами, расположенными на одном компьютере, следует помнить, что два POP3-сервера должны иметь различные значения портов. Нельзя установить два сервера, применив для их работы стандартные порты. В то же время два SMTP-сервера могут сосуществовать, используя один и тот же стандартный или нестандартный порт.

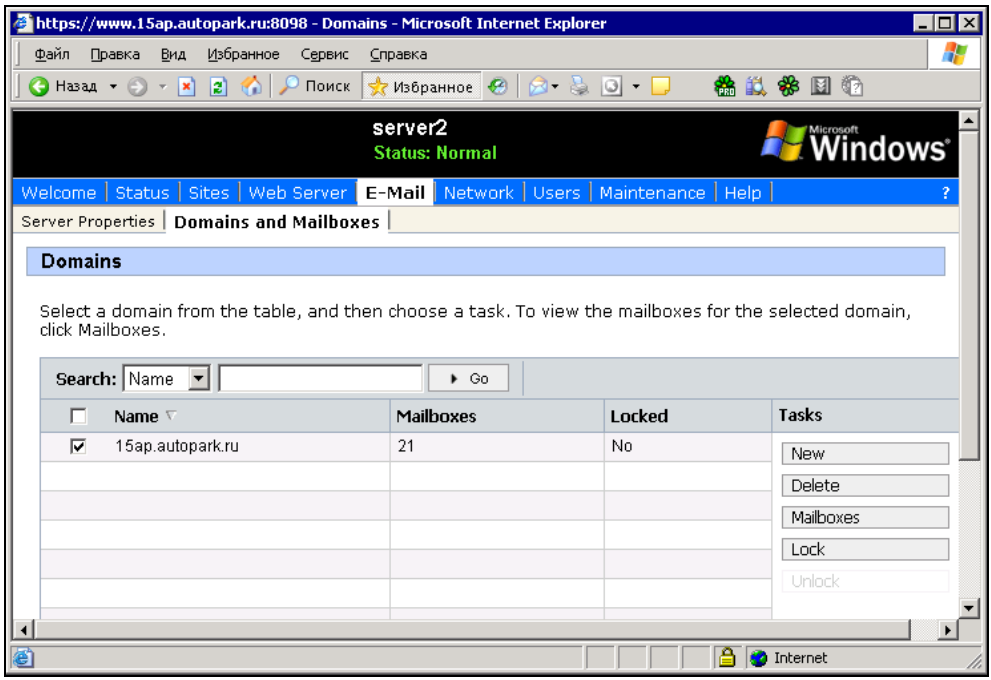


Рис. 4.47. Вкладка **Domains and Mailboxes**

На странице **Domains and Mailboxes** (рис. 4.47) мы можем получить доступ к созданию или удалению и блокированию почтовых доменов, а также можем перейти на страницу управления самими почтовыми ящиками. Интерфейс этих страниц настолько понятен, что нет смысла подробно его рассматривать. Кроме управления доменами и почтовыми ящиками через Web-интерфейс мы можем получить доступ к управлению локальными учетными записями пользователей сервера, перейдя на вкладку **Local Users on Server** (Пользователи) (рис. 4.48).

Здесь мы можем создавать, удалять и модифицировать учетные записи. Если сервер работает только как почтовый сервер, то этот интерфейс обеспечивает доступ ко всем необходимым свойствам учетных записей пользователей почты. Но не только учетными записями пользователей почты можно управлять с этой вкладки. Вы можете создавать учетные записи, наделяя их любыми правами, или предоставлять и ограничивать права для существующих учетных записей.

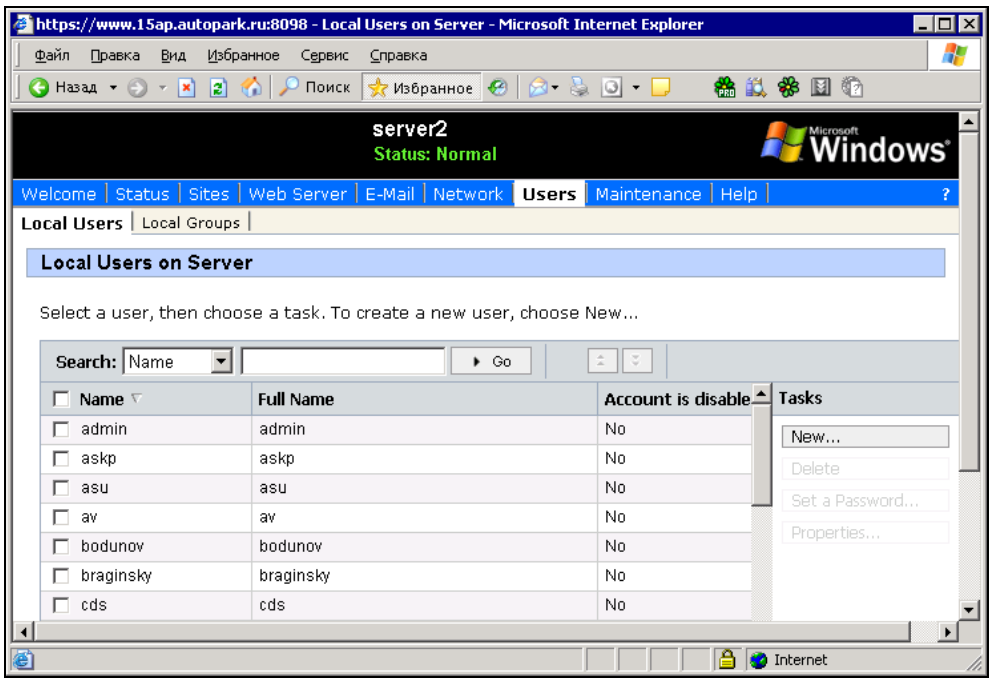


Рис. 4.48. Вкладка **Local Users on Server**
(Локальные пользователи сервера)

Кроме управления почтовым сервером Web-интерфейс позволяет управлять и Web-серверами с вкладки **Web Site Configuration** (рис. 4.49).

А с вкладки **Date and Time Settings** (Установка даты и времени) можно контролировать работу системных часов сервера.

Вкладка **Shutdown** (рис. 4.51) позволяет выполнять перезагрузку, выключение и планирование выключения или перезагрузки сервера.

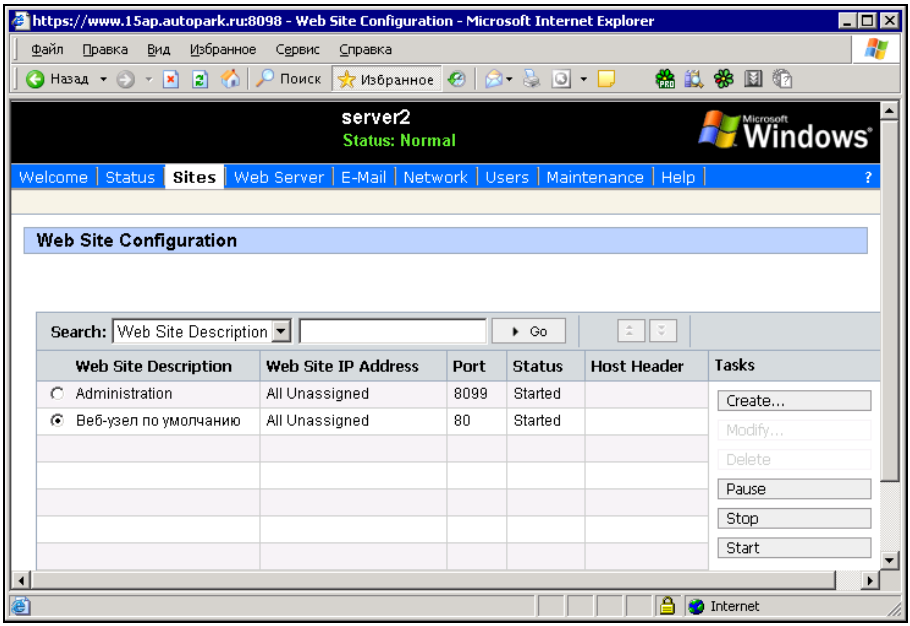


Рис. 4.49. Вкладка **Web Site Configuration** (Конфигурация Web-сайтов)

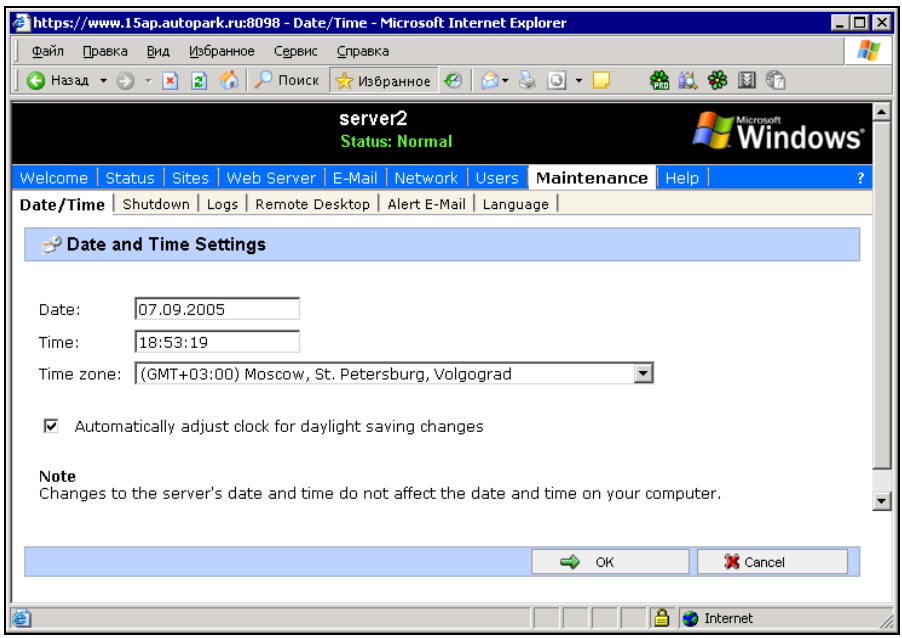


Рис. 4.50. Вкладка **Date and Time Settings** (Установка даты и времени)

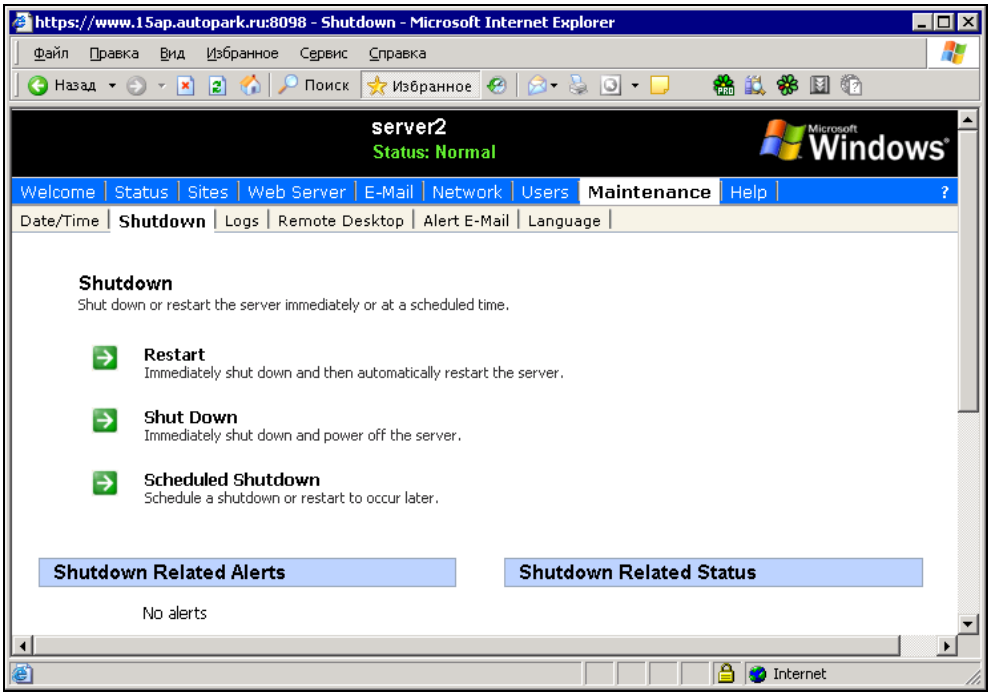


Рис. 4.51. Вкладка **Shutdown** (Выключение)

Эти операции довольно рискованны, если вы не уверены, что после перезагрузки работа сервера восстановится, а выключение действительно необходимо в данный момент.

Но если вы точно знаете, что перезагрузка необходима и вызвана изменением каких-либо настроек или иной ситуацией, а сами вы находитесь на значительном удалении от сервера, то этот инструмент очень удобен. Кроме собственно перезагрузки и выключения, вы можете назначить сообщения, которые сервер будет отсылать вам при перезагрузке или выключении.

Установить связь сообщений с различными типами событий, указать адрес для их отправки и SMTP-сервер, которым необходимо при этом воспользоваться, вы можете на вкладке **Alert E-Mail** (Сообщения по электронной почте) (рис. 4.52).

Рассмотрите самостоятельно остальные возможности этого интерфейса. Возможно, что именно вас заинтересуют и другие его функции. Их достаточно, чтобы иметь возможность в удаленном режиме выполнять необходимые опе-

рации на вашем почтовом сервере. Если вы сталкивались ранее со средствами управления маршрутизаторами и другими сетевыми устройствами по HTTP-протоколу и вам нравился такой метод управления этими устройствами, то Web-интерфейс управления сервером вам обязательно понравится.

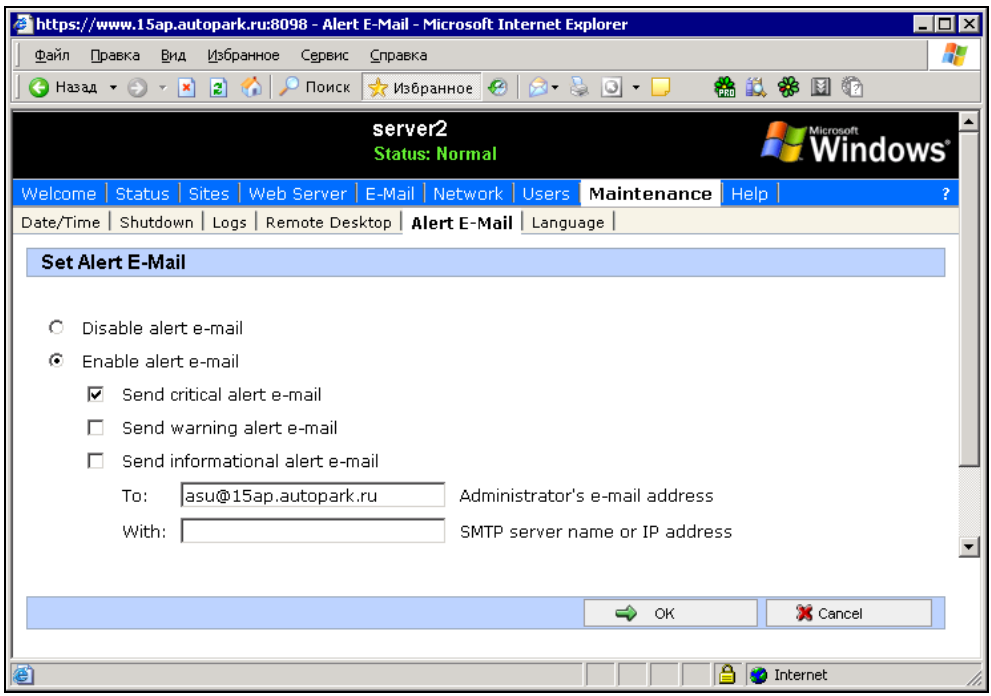


Рис. 4.52. Вкладка **Maintenance | Alert E-Mail | Set Alert E-Mail** (Настройка сообщений по электронной почте)

В заключении описания Web-интерфейса для управления сервером посмотрим еще на одну вкладку — **Set Server Name | Server Identity** (Начальные настройки | Идентификация сервера (рис. 4.53). В этом окне вы имеете возможность переименования сервера, изменения его принадлежности к тому или иному домену или рабочей группе.

Таким образом, в ваших руках мощнейшее средство для управления сервером, применяя которое необходимо соблюдать осторожность и не пытаться экспериментировать, если вы находитесь на значительном удалении от сервера и не сможете исправить ошибку при потере связи с сервером.

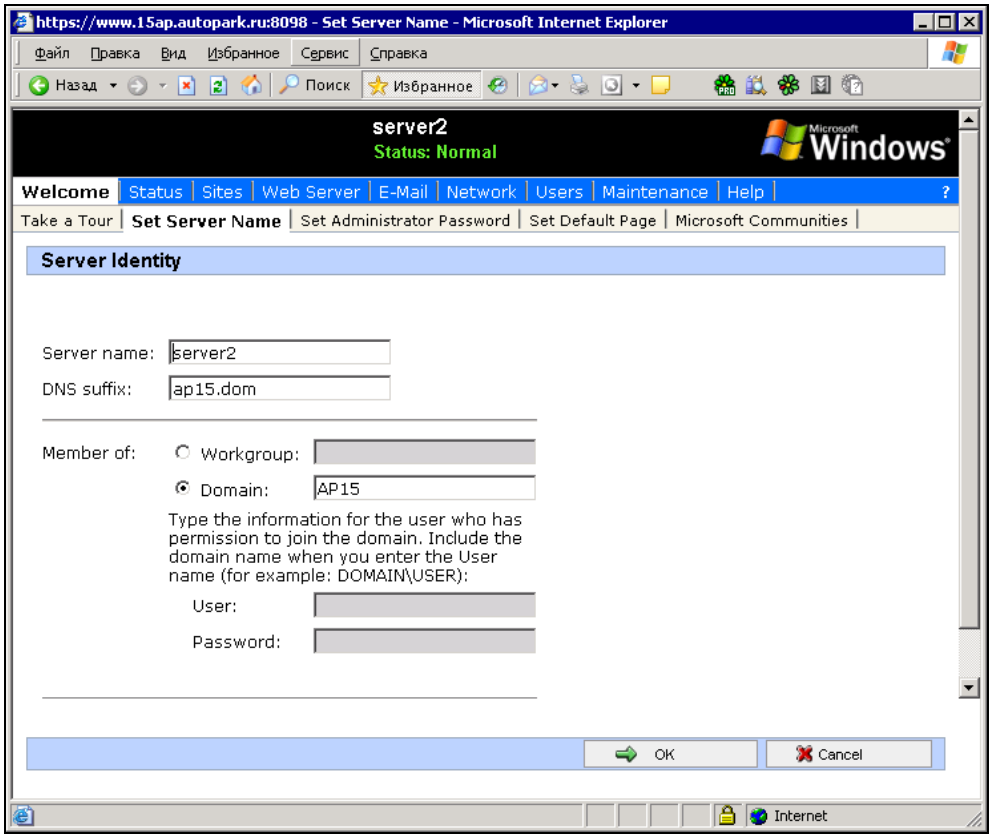


Рис. 4.53. Вкладка **Set Server Name | Server Identity** (Начальные настройки | Идентификация сервера)

FTP-сервер

Значительный интерес для использования в сети может представлять FTP-сервер. Для тех, кто часто ищет файлы в Интернете и перекачивает их, FTP-протокол не является тайной за семью печатями. Множество FTP-клиентов можно найти как в Интернете, так и на распространяемых компакт-дисках. Обычно клиенты рассчитаны на работу с UNIX-серверами. В нашем случае нужен сервер, эмулирующий работу UNIX-сервера, но реально работающий под Windows. Такое программное обеспечение существует и, более того, оно бесплатно. Примером такого сервера может быть WarDaemon FTP-сервер

(рис. 4.54), который можно найти на сайте **www.jgaa.com** или на сайтах, поддерживающих создание домашних сетей, например на **telecom.sins.ru**.

WarDaemon FTP-сервер считается одним из лучших серверов FTP для Windows. Сервер содержит порты UNIX и Linux, поддерживает большинство соответствующих команд. Последняя версия программы — 1.70 — обеспечивает возможность удаленного управления. Это значит, что можно управлять сервером с любого компьютера сети.

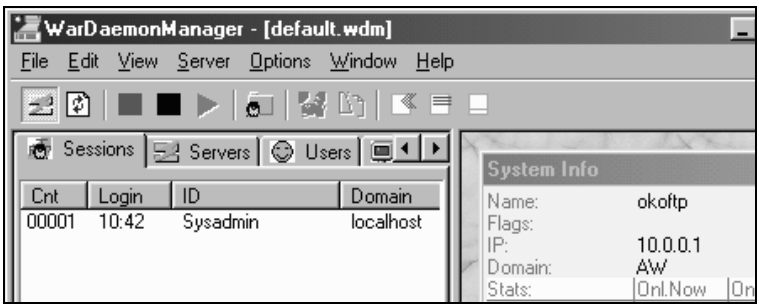


Рис. 4.54. Окно **WarDaemonManager**

Устанавливается сервер достаточно легко и может быть запущен как приложение или как сервис. При этом он будет запускаться одновременно с Windows. При первом старте будет запрошен пароль администратора, который надо ввести и подтвердить. При следующих запусках будут запрашиваться имя сервера и пароль.

Сервер имеет большое количество настроек, позволяющих управлять доступом и повышающих удобство работы с ним.

С помощью окна **User manager** (рис. 4.55) можно управлять доступом к серверу, разграничивая права между пользователями и гостями. В дереве пользователей может быть создано произвольное количество групп пользователей, наделенных специфическими правами.

Соединение с сервером может быть осуществлено, как и обычно, по IP-адресу (например, 193.91.161.12) или адресу DNS (имени домена — **ftp://ftp.<ваш сервер>.<домен2>.<домен1>**).

Что касается номера порта, то обычно по умолчанию используется 21, но если задать различные номера портов, то на одном физическом сервере можно использовать несколько экземпляров FTP-сервера.

Сведения о пользователях могут сохраняться в базе данных. Поддерживаются несколько типов баз данных, но для Microsoft Windows наиболее актуально использование формата MDB (Microsoft Access входит в состав Microsoft Office Professional). Заготовка такой базы данных содержится в папке с установленной программой.

На просторах Интернета можно найти и другие программы такого же назначения.

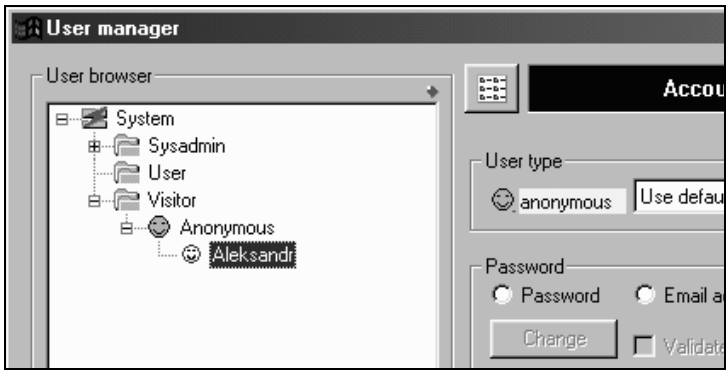


Рис. 4.55. Окно **User manager**

Рис. 4.56. Диалоговое окно простого FTP-сервера

Например, ST FTP Server v1.6. Это простой FTP-сервер (рис. 4.56). Он поддерживает основной набор FTP-команд, "докачку" файлов в оба направления,

идентификацию и аутентификацию пользователей, анонимные подключения. Возможна настройка рабочих каталогов и прав доступа для каждого пользователя в отдельности.

Сервер может работать как обычная программа для Windows 9*x* и NT (STFTP.EXE), а также как служба Windows NT (STFTPSrv.EXE).

Web-сайт без подключения к Интернету

Один из вариантов хранения внутреннего Web-сайта — это размещение его на сервере средствами операционной системы. В Windows 2000 Server встроена такая возможность. Web-сервер на основе этой операционной системы поддерживает практически все технологии программирования, применяемые при создании Web-страниц. Следовательно, вы можете заказать изготовление вашего сайта любому специалисту, не ограничивая его в средствах разработки. Но важно помнить, что страницы разрабатываются человеком, который не слишком заинтересован в информационной безопасности вашей сети. Поэтому вам следует проконтролировать качество разработанной страницы или сайта с точки зрения ее безопасности. Для этого, возможно, придется привлечь другого, независимого специалиста. Можно обойтись и простыми страницами, создание которых доступно и вам.

Что же необходимо для размещения страницы на сервере? Прежде всего, нужно убедиться, что на сервере установлен компонент Internet Information Services (IIS — служба информации Интернета — Web-сервер разработки Microsoft). Если вы сами инсталлировали операционную систему, выбрав вариант установки по умолчанию, то этот компонент должен быть уже установлен. Если нет, то добавить его несложно с помощью диалогового окна **Установка и удаление программ** (его значок находится на Панели управления). Мы будем считать, что основные составляющие этого компонента уже установлены. Для того чтобы удостовериться в этом:

1. Выберите **Пуск | Настройка | Панель управления**.
2. Двойным щелчком мыши на значке **Установка и удаление программ** откройте одноименное окно.
3. Нажмите левой кнопкой мыши область **Добавление и удаление компонентов Windows**.

4. В открывшемся окне (рис. 4.57) мастера компонентов Windows проверьте наличие флажка в строке **Internet Information Services (IIS)**. Если флажок не установлен, то установите его и нажмите кнопку **Далее**.

5. С помощью кнопки **Состав** выберите все составляющие компонента **Internet Information Services**.

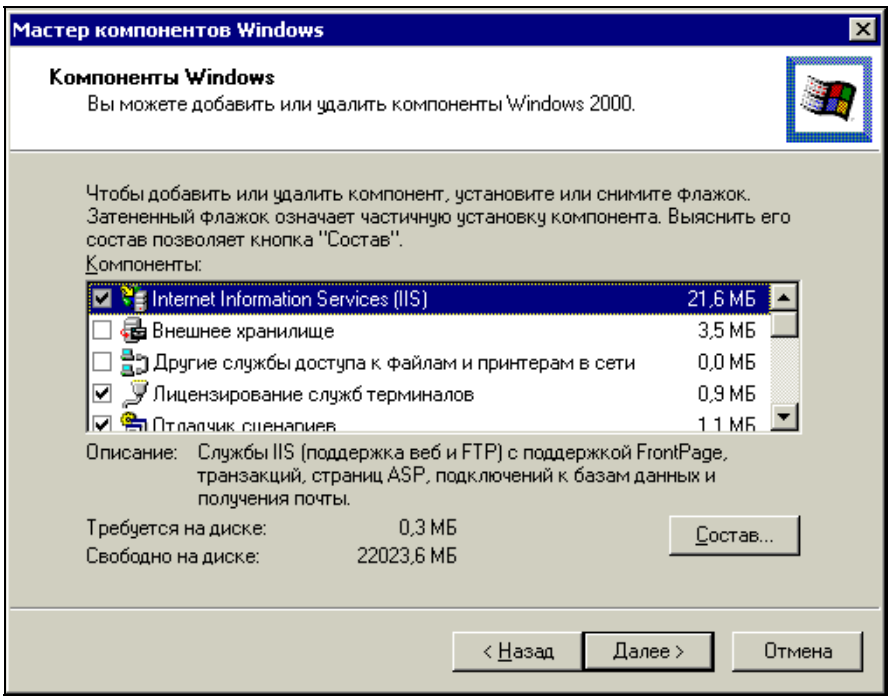


Рис. 4.57. Мастер компонентов Windows

После установки IIS, как и в случае обнаружения этого компонента в системе, можно приступить к его настройке. Для настройки ISS следует выполнить следующее:

1. Откройте консоль управления Internet Information Services (рис. 4.58). Для этого необходимо выполнить команду **Пуск | Программы | Администрирование | Диспетчер служб Интернета**.

2. Щелкнув правой кнопкой мыши по имени вашего сервера в левой части консоли, выберите пункт меню **Свойства**. Откроется окно свойств сервера (рис. 4.59).

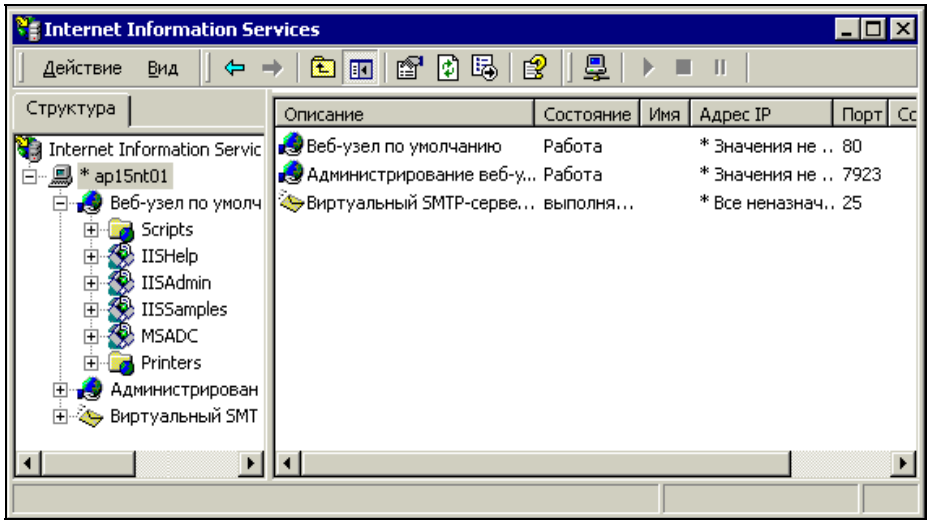


Рис. 4.58. Окно **Internet Information Services**

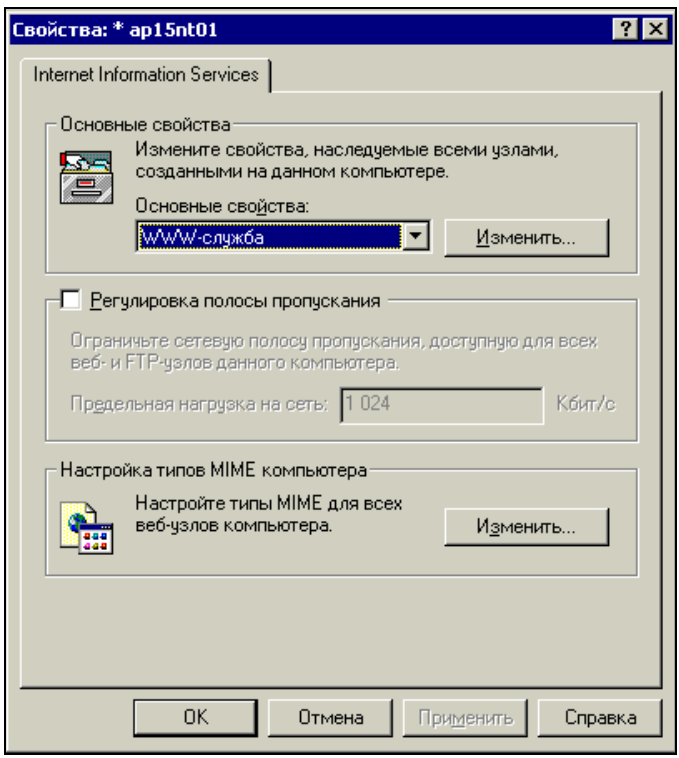


Рис. 4.59. Окно **Свойства: <Имя сервера>**

3. Если в поле **Основные свойства** стоит значение **WWW-служба** — нажмите кнопку **Изменить**. Иначе выберите из раскрывающегося списка поля это значение и нажмите кнопку **Изменить**.
4. Практически все свойства в открывшемся окне **Основные свойства WWW-службы для <Имя сервера>** по умолчанию уже установлены верно, вам следует перейти на вкладку **Документы** (рис. 4.60).
5. Установите флажок **Задать документ, используемый по умолчанию**.

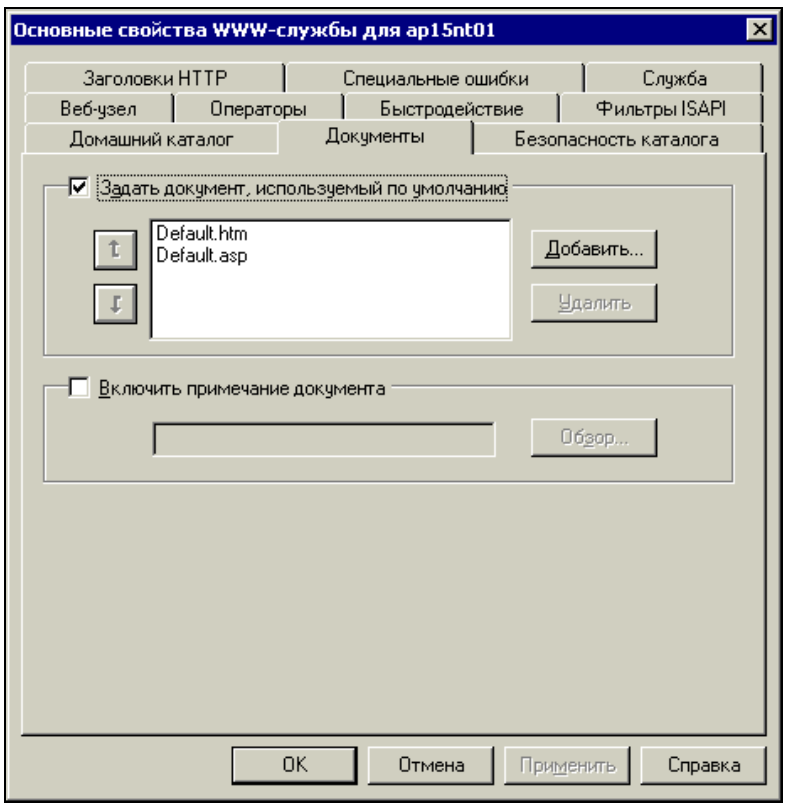


Рис. 4.60. Окно **Основные свойства WWW-службы для <Имя сервера>**, вкладка **Документы**

6. Нажмите кнопку **Добавить**.
7. В открывшемся диалоговом окне с единственным полем введите **Default.htm** и нажмите кнопку **ОК**. Закройте все открытые окна.

8. По умолчанию домашним каталогом для вашей страницы назначен \InetPub\wwwroot. Найдите его на диске и поместите в него файл Default.htm. Это может быть любая созданная вами HTML-страница, названная Default.htm.

9. Если подготовленной страницы нет, вы можете создать временную, используя текстовый редактор Блокнот. Для этого откройте Блокнот и введите следующий текст:

```
<html>
<head>
</head>
<body>
<h1>
На этом месте будет размещена страница
нашей организации.
В настоящее время сайт находится в стадии разработки.
</h1>
</body>
</html>
```

10. Сохраните файл как Default.htm в каталоге \InetPub\wwwroot.

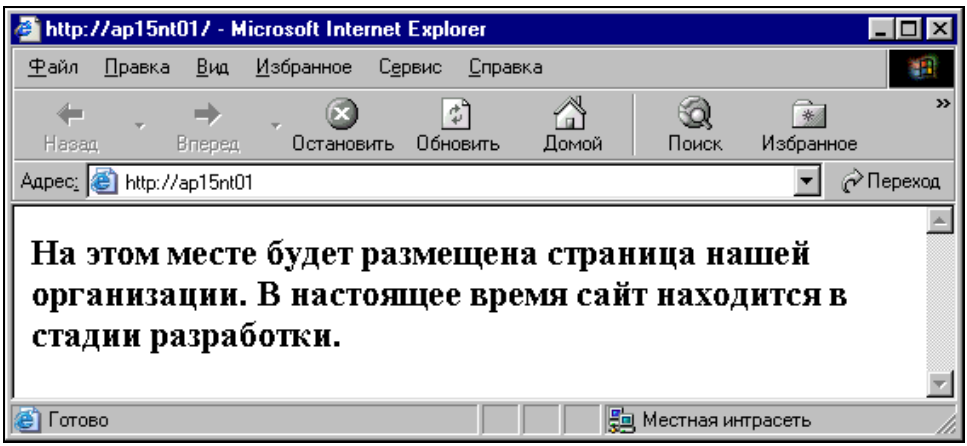


Рис. 4.61. Окно **Microsoft Internet Explorer** с изображением только что созданной страницы

11. Теперь с любого компьютера сети подключитесь к вашему Web-серверу, набрав в строке адреса имя или IP-адрес вашего сервера. На экране должна появиться страница, показанная на рис. 4.61.

Можно увидеть эту страницу и на экране консоли сервера, введя в качестве адреса `http://127.0.0.1/`.

Если у вас все получилось, то дальнейшую работу по созданию страницы поручите специалисту.

Web-сервер не на сервере

Рассмотрим еще один вариант создания локального (внутри сети) Web-сервера.

Для этого необходимо скопировать бесплатную программу AnalogX Simple Server, которая находится по уже известному вам адресу **www.analogx.com**. Она позволяет создать Web-сервер на любом компьютере вашей сети, если на нем установлена операционная система семейства Windows. Перед установкой программы создайте на диске компьютера каталог Web и поместите в него уже созданную страницу, но под именем Index.htm.

Установите программу. Установка ее настолько проста, что описания не требует. От регистрации программы можно отказаться, особенно если с данного компьютера нельзя подключиться к Интернету. После установки программы перезагрузите компьютер.

Далее выполните следующее:

1. В меню **Пуск** выберите пункты **Программы | AnalogX | SimpleServer | WWW | SimpleServer.WWW**. Откроется окно программы (рис. 4.62), в котором вы увидите логотип программы и четыре кнопки.
2. Нажав нижнюю длинную кнопку, выберите в окне проводника файл вашей страницы и нажмите кнопку **ОК**.
3. Затем нажмите кнопку **Start**, надпись на которой изменится на **Stop**.
4. На верхней кнопке вы можете прочитать IP-адрес компьютера. Сверните окно (не закрывайте).
5. В строке адреса в окне интернет-браузера на любом компьютере сети наберите имя или IP-адрес компьютера с установленным Web-сервером. В результате вы увидите созданную вами страницу.

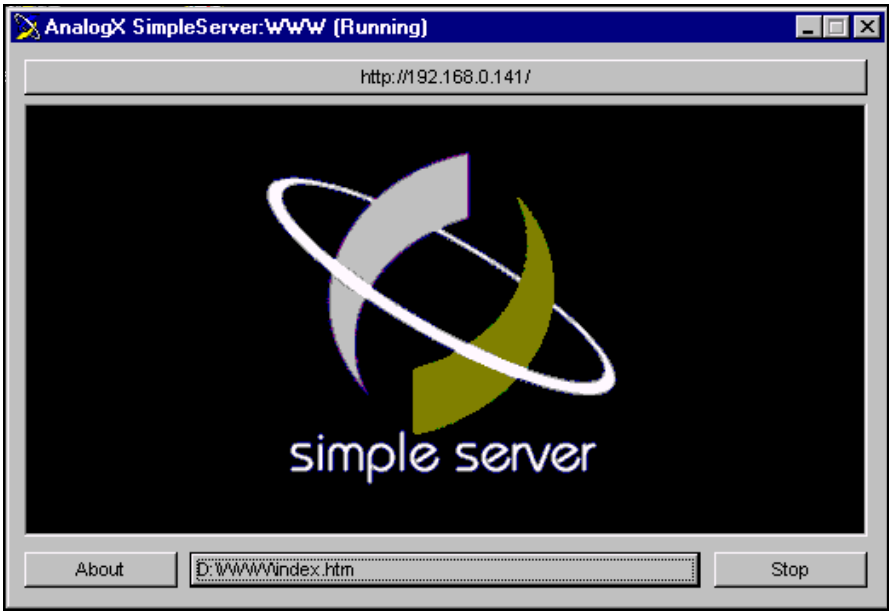


Рис. 4.62. Окно **AnalogX Simple Server**

Если все получилось, то создание Web-сервера можно считать завершенным. Этот сервер обладает несколько меньшими возможностями, чем тот, что мы создавали ранее, но тем не менее с успехом может применяться в качестве внутреннего Web-сервера. Сервер поддерживает работу с некоторыми видами скриптов. Сохранив полностью Web-страницу, на которой был размещен калькулятор для расчета стоимости услуг некоторой фирмы, и создав ссылку на нее с основной страницы внутреннего сайта, я мог пользоваться этим калькулятором, не подключаясь к сайту фирмы.

Итак, в вашем распоряжении два действующих Web-сервера. С помощью AnalogX Simple Server вы можете создать по серверу на каждом компьютере вашей сети!

Web-сайт и FTP-сервер для компьютеров под управлением DOS

Для подключения к компьютеру из сети применяется Web/FTP-сервер на одной дискете! Пользователи локальной сети могут через любой Web-браузер

или FTP-клиент обратиться к ресурсам того компьютера, где запущен описываемый сервер. Дистрибутив Web/FTP-сервера на одной дискете можно найти по адресу **http://386.eznos.org/** или воспользоваться файлом diskwww.zip (**www.okobox.narod.ru**), содержащим образ дискеты и программу diskdupe.exe, позволяющую преобразовать этот образ в рабочую дискету. Последняя включает почти все необходимое для запуска сервера на машинах, начиная с процессора 80386, но, в отличие от оригинальной, она содержит операционную систему MS-DOS 7 (русифицированную) и при старте на экране появляется сообщение о запуске Windows 98. Учтите, каким бы дистрибутивом вы не воспользовались, все равно придется настраивать сервер в соответствии с параметрами сети и применяемым сетевым адаптером.

Настройка сервера проста, но требует внимания. Она заключается в изменении записей в файлах конфигурации. Прежде всего заглянем в файл A:\nos\autoexec.nos. Как и другие подобные файлы сервера, этот текстовый файл можно редактировать любым текстовым редактором. На дискете, полученной из образа архива diskwww.zip, уже есть необходимый редактор (edit.com), который известен практически всем пользователям ПК, хотя бы иногда работающим в среде MS-DOS. Далее приведено содержание данного и других файлов из diskwww.zip. Для тех, кто будет пользоваться прочими дистрибутивами, эти описания также подойдут — отличия не принципиальны.

Файл Autoexec.nos

Сразу отмечу, что символ # предваряет все комментарии и неисполняемые команды.

Итак,

```
# =============
# autoexec.nos
# =============
hostname webbserver #Имя вашего сервера.
ip address 192.168.0.111 #IP-адрес сервера должен быть заменен на другой,
#допустимый в вашей сети.
#Следующие значения параметров TCP/IP лучше не изменять, если вы не
#знаете, зачем это делаете.
tcp mss 1460
tcp window 4096
tcp syn off
```

```
tcp maxwait 60000
tcp irtt 1000
tcp timer linear
ip ttl 50
isat 1


attach packet 0x62 en0 5 1500
#Данная команда подключает пакетный драйвер вашей сетевой платы. На
#рабочей дискете есть драйверы для двух плат, с которыми проверялась
#работа сервера.
#Устанавливать прерывания обычно не требуется, но если устройства
#конфликтуют, компьютер придется настроить. Если не знаете как, то
#обратитесь к опытным пользователям или доступным описаниям.


route add 192.168.0/24 en0
#Маска подсети. Возможны варианты 192.168/16; 172.16/16; 10/8. Если
#возникают трудности с определением маски подсети в этом формате, то на
#дискете в каталоге WWW можно воспользоваться файлом Netmask.htm.


route add default en0 192.168.0.15
#Адрес вашего маршрутизатора или основного сервера.
#Add domain name server
#Замените адреса в следующих двух строках значениями, соответствующими
#используемым вами DNS-серверам. Если таких нет или вы не хотите их
#применять, то не удаляйте символ комментария перед этими строками:
#domain addserver 192.168.0.15
#domain addserver 192.168.1.254


# ===Start Services===
# FTP services


#Для работы FTP-сервера необходимо сохранить записи о пользователях
#в файле ftpusers.
#Следующие четыре строчки можно не изменять.
ftype image
ftptdisc 900
ftpmax 10
start ftp
#Сервер может использовать страницы как с дискеты, так и с жесткого
#диска, если он есть. Для настройки запуска с применением порта 80 и
#каталога документов c:\nos\www следует написать:
#start http 80 c \nos\www (после буквы диска двоеточие не ставить).
```

```
#Измените следующую строку в соответствии с этим описанием:
start http 80 a \www
#В следующих двух строках приведены варианты настройки выключения (exit)
#или перезагрузки (reboot) сервера. Автор рекомендует перезагружать его
#ежедневно, однако сервер может работать и без перезагрузки.
#Параметр 0500 обозначает время в часах и минутах.


# at 0600 exit
at 0500 reboot
```

Файл HTTPD.BAT

Файл HTTPD.BAT содержит указание на используемый пакетный драйвер, который должен быть помещен в каталог A:\NOS\BIN. Как и обычно в BAT-файлах, REM — комментарий.

```
@echo off
REM Настройка сети. Оба драйвера есть на дискете. Если у вас установлена
REM другая сетевая плата, то возьмите ее пакетный драйвер с дискеты,
REM прилагающейся к плате, или найдите в Интернете. В строке указывается
REM только имя файла без расширения, 0x62 пропускать нельзя.
REM \nos\bin\Rtspkt 0x62
\nos\bin\Hppclanp 0x62
REM Старт сервера
\nos\bin\nos.exe -f\nos\nos.cfg
REM Отключение от сети при выключении сервера
\nos\bin\termin 0x62
echo\
```

Файл Ftpusers

В файле A:\NOS\Ftpusers представлены настройки доступа к FTP-серверу. Именно с его помощью удобно загружать необходимые файлы на компьютер из сети.

```
admin parol \ 127;ftp\user 127;ftp\univ 127
univperm * c:\doc 3
user secret c:\arx 7
```

Цифры обозначают уровень доступа:

- 1 — только чтение;
- 3 — чтение и запись без возможности удаления;
- 7 — полный;
- 127 — системного администратора;
- 128 — запрещение доступа.

Формат записи:

```
<Пользователь> <Пароль> [Буква диска:] \<Путь1> <Доступ>;\<Путь2>
<Доступ>.
```

Звездочка обозначает пустой пароль. Буква для диска A: может быть опущена. С указанными настройками сервер работает в сети с сервером Windows 2000 Server 192.168.0.15, с маской подсети — 255.255.255.0. Причем независимо от операционной системы всегда возможен вход через браузер с любой рабочей станции. Для предоставления доступа берется числовой формат IP-адреса **http://192.168.0.111**, а для пропуска через FTP нужно ввести **ftp://имя_пользователя@192.168.0.111**. Пароль будет запрошен автоматически, но его можно ввести сразу же в адресе:

```
ftp:// имя_пользователя:пароль @192.168.0.111.
```

При удачном соединении с сервером на экране компьютера, с которого устанавливалось соединение, появится страница приветствия: на русском языке — для дискеты, на английском — для оригинальных файлов.

Краткий список команд для управления сервером

- `?` — вывод перечня команд на экран;
- `cls` — очистка экрана;
- `exit` — закрытие (выключение) сервера;
- `help` — помощь;
- `http status` — статус сервера;
- `info` — информация о сервере;

- `multitask on` — включение многозадачного режима (в этом режиме можно работать на рабочей станции с установленным и запущенным сервером);
- `ping w.x.y.z` — ping по сетевому адресу;
- `pkstat` — детализация трафика;
- `route` — вывод таблицы маршрутизации на экран;
- `shell` — сеанс DOS, для возврата — `exit`.

После однократной настройки сервера на дискете вы сможете применить его на любом компьютере, изменив лишь драйвер сетевой платы, если это необходимо. Быстродействие сервера не велико, но для первоначальной загрузки файлов дистрибутива операционной системы вполне достаточно.

Связь через HyperTerminal

Наверняка многие знают или слышали о BBS (Bulletin Board System — система электронных досок) электронных досках объявлений и FIDO — глобальной некоммерческой сети. Подробно вникать в принципы работы этих сетей и описывать программное обеспечение, необходимое для работы с BBS, мы не будем. Для этого есть масса источников в Интернете, а также знакомые, уже работающие с этими сетями. Для нас достаточно знать, что сети имеют иерархическую структуру, и в один момент времени к станции BBS может получить доступ только один пользователь. Почта или сообщение, оставленные этим пользователем, могут быть переданы в любую точку мира, где есть телефон и пользователи FIDO. Файлы, имеющиеся на BBS, пользователь может перекачать на свою машину (в пределах отведенного ему на это времени), а также забрать адресованную ему почту. Неоспоримое преимущество таких сетей перед Интернетом — это бесплатность, не считая платы за телефонное время, если она взимается. Конечно, в этом случае невозможна организация каких-либо выделенных каналов, режима онлайн, мультимедиа и игр по сети. Но информацией можно обмениваться, "софт" можно перекачивать и заказывать, если нет на данной BBS. Время связи со станцией BBS ограничено интервалом, указанным в нодлисте, который представляет из себя реестр действующих станций с расписанием их работы. В другое время телефоны используются по своему прямому назначению.

Организуя свою сеть, можно использовать опыт работы BBS и FIDO, творчески переработав его. Предположим, что часть пользователей ПК, с которыми

необходимо поддерживать регулярные контакты, находятся на таком удалении от вашей сети, что непосредственное подключение к сети проблематично. В этом случае возможно использование электронной почты и других средств связи, доступных через Интернет. Для этого необходимо подключение к глобальной сети всех пользователей, участвующих в обмене информацией. Это возможно не всегда. В то же время Интернет на просторах нашей страны — явление, встречающееся реже, чем телефон. Попробуем организовать регулярную связь между пользователями, имеющими телефон и модем, но не подключенными к Интернету.

Наиболее простым средством связи компьютеров через телефонно-модемную линию может быть HyperTerminal — программа связи, входящая в комплект поставки Windows 95/98/ME/2000. Эта программа позволяет передавать файлы между связанными машинами, а также проводить сеансы текстового общения. Если на вашей машине вы не обнаружили эту программу, то ее не трудно установить, имея дистрибутив Windows той версии, которая находится на компьютере.

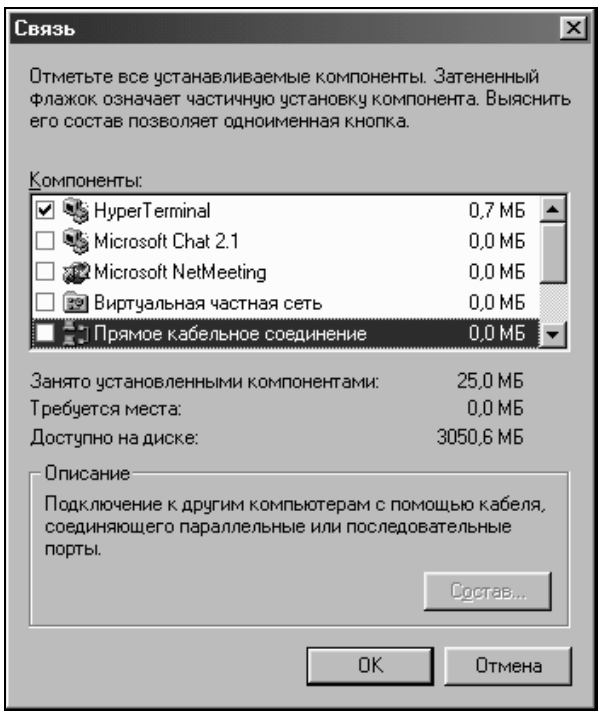


Рис. 4.63. Установка программы HyperTerminal

Для этого надо открыть папку Панель управления, выбрать значок **Установка и удаление программ**, перейти на вкладку **Установка Windows**, выбрать компонент **Связь**, нажать кнопку **Состав** и выставить флажок **HyperTerminal** (рис. 4.63).

Потребуется указать расположение дистрибутивных файлов, и программа будет установлена. После этого ее можно открыть через меню **Пуск**, выбирая последовательно **Программы | Стандартные | Связь | HyperTerminal**. В папке с программой можно создать новое подключение подобно тому, как это делается для удаленных соединений, но настроек существенно меньше. Некоторые из настроек показаны на рис. 4.64.

Каждое подключение может быть сохранено со своей картинкой, выбор которой предоставлен при сохранении самой программой (рис. 4.65).

В рабочем окне (рис. 4.66) можно набирать текст, а в меню выбирать режимы работы, устанавливать режим ожидания связи или передачи/приема файла, или режим связи, когда после выбора соединения HyperTerminal набирает номер и устанавливает связь.

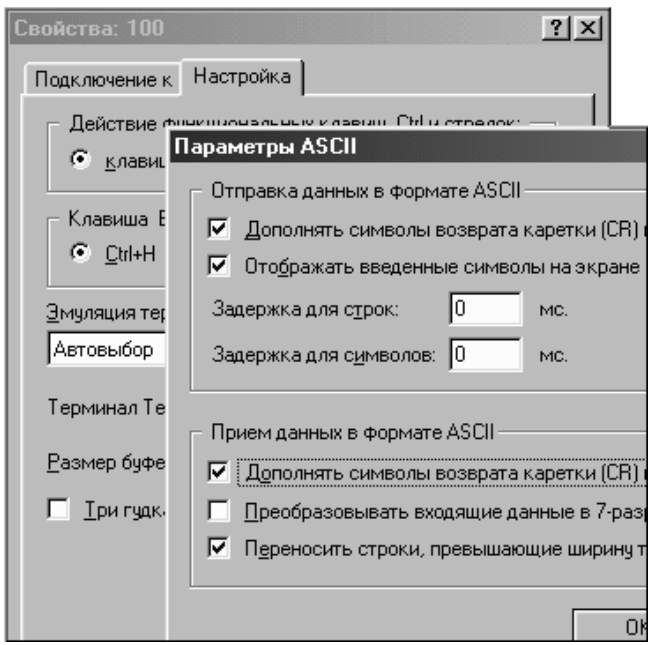


Рис. 4.64. Некоторые настройки программы HyperTerminal

Во время запуска программы появляется заставка, приглашающая обновить текущую версию на более новую. Версия 6.3, которую можно получить бесплатно, позволяет использовать макросы (рис. 4.67), дающие возможность во время сеанса связи нажатием одной-двух клавиш вводить заранее заготовленные строки большой длины.

Рис. 4.65. Внешний вид папки с программой и сохраненными подключениями

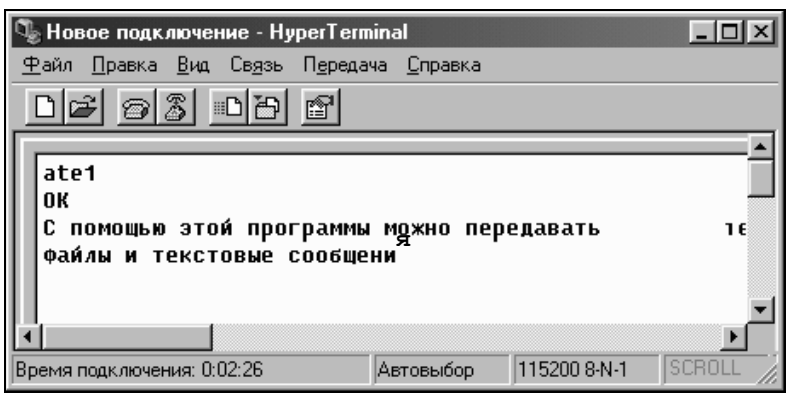


Рис. 4.66. Рабочее окно терминала

Текст, набираемый кириллицей, будет отображаться кодами символов. А в окне программы при установке шрифта с кириллицей — нормальный текст. Надо только помнить, что в режиме русского текста нельзя вводить команды для модема. Возможно, что более удобным будет написание текста транслитерацией.

В вашей сети количество машин не настолько велико, чтобы придумывать особую систему адресов. Каждая машина имеет свое имя, которое отражено в названии подключения. А в параметрах подключения телефонный номер однозначно определяет компьютер, к которому производится подключение. Выделив один из компьютеров (желательно, чтобы он был подключен к вашей сети Ethernet или имел соединение с Интернетом), можно организовать на нем "почтовое отделение" и хранить персональную почту в виде файлов с именем, соответствующим имени адресата. Владелец ПК в определенное время по договоренности может включить HyperTerminal в режим ожидания и принимать почту для всех членов сети, которые не имеют возможности общаться иным способом. Каждый сможет, подключившись, забрать свою почту или послать сообщение другому пользователю.

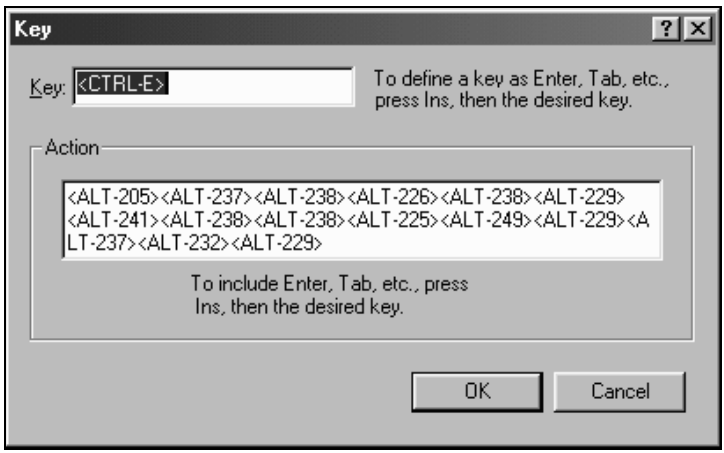


Рис. 4.67. Диалоговое окно создания/модификации макроса в новой версии программы HyperTerminal

Использование сервера удаленного доступа позволяет сделать подключения более наглядными. Применив Radmin, можно воспользоваться программным обеспечением "почтового отделения" для дистанционной обработки файлов.

Протокол NetBEUI (его назначение и установка уже рассмотрены) позволяет при подключении удаленных компьютеров использовать возможности Windows по разграничению доступа к файлам и папкам и выделить каталог для общего пользования. При этом каталоги пользователя машины, выполняющей функции "почтового отделения", будут недоступны другим пользователям, что уменьшит риск несанкционированных действий, направленных на повреждение системы или вызванных неопытностью.

Конкретная реализация сети без кабеля зависит от ваших потребностей, желания и фантазии. Существенные удобства в работе с удаленными машинами по телефонной линии может предоставить программа АОН (автоматический определитель номера). Такие программы способны выявлять заранее записанные номера и разрешать для них соединение, а другие номера игнорировать. Если сеансы связи с использованием сервера удаленного доступа проводятся в ночное время, АОН может избавить вас от "лишних" звонков абонентов, случайно позвонивших вам. Все звонки от пользователей сети будут опознаваться, и с ними будет устанавливаться соединение. К сожалению, программы АОН работают не со всеми модемами. Более подробно об этих программах можно узнать, установив пробные версии с адресов **www.srg-kiev.chat.ru/aon.htm**, **http://www.cyteg.com/prg/aon/downld_r.htm**, **http://www.voicecallcentral.com/rus/advancedcallcenter.htm**.

Если нет хаба

Материал этого раздела полезен в случаях, когда крайняя нужда заставляет создавать сеть практически без средств. Как говорят: голь на выдумки хитра.

Рассмотрим, каким образом можно построить пассивный хаб для витой пары.

Сетевая карта Ethernet с интерфейсом "витая пара" и скоростью 100 (или 10) Мбит имеет 8-контактный разъем. Из них используются только четыре контакта: первый, второй, третий и шестой (рис. 4.68).

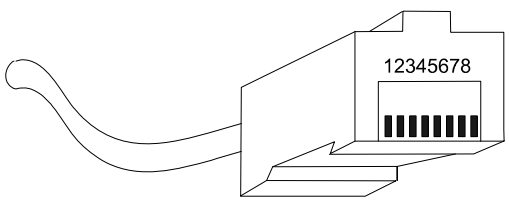


Рис. 4.68. Нумерация контактов

Из них парами являются контакты 1, 2 и 3, 6. При обжимании концевых разъемов им должны соответствовать свитые вместе провода, т. е. собственно витые пары. Отличить пары очень просто — они состоят из цветного провода (однотонный цвет) и белого провода, окрашенного полосками этого цвета.

Интерфейс построен следующим образом: одна из пар передает в одну сторону, вторая — в другую. "Навороченные" сетевые карты умеют одновременно передавать и принимать информацию (это называется режимом full duplex — полный дуплекс). Однако в нашем случае он не будет использоваться — карта будет работать в полудуплексном режиме. При включении сетевая карта "договаривается" с удаленным устройством о том, есть ли полный дуплекс или нет. При наличии хаба она сразу "поймет", что дуплекса нет.

Полудуплексный режим функционирует так: когда карта передает информацию, поступивший на вход сигнал дает ей понять, что какая-то еще карта отправила информацию одновременно с ней — т. е. возникла коллизия. В этом случае передача останавливается и повторяется через некоторый случайный промежуток времени. Существует большая вероятность того, что адаптеры начнут вторую попытку передачи в разное время. В этом случае запоздавшая с передачей сетевая карта "увидит", что началась передача другим адаптером, и будет принимать информацию, отложив передаваемые данные в свой буфер до следующей попытки.

В сети по физической топологии "общая шина" информация, передаваемая одним компьютером, должна достичь всех остальных. Таким образом, хаб должен обеспечить распространение информации. Но одновременно с этим передаваемая информация не должна попасть на вход передающего ее компьютера, иначе он примет ее за коллизию и не сможет ничего передать вообще.

Итак, мы можем сформулировать задачу хаба: он должен распространять передаваемую информацию на все подключенные к нему компьютеры, кроме передающего (чтобы не было эха).

Простейший случай: два компьютера. Тогда они просто соединяются напрямую: 1 и 2 контакты — к 3 и 6 контактам соседа. Кроме того, будет полный дуплекс (если обе карты его поддерживают).

Теперь переходим к случаям, когда вместе соединяются три компьютера и более. В этом случае необходимо обеспечить, чтобы передаваемый сигнал не возвращался обратно.

Рассмотрим резистивный мост, состоящий из четырех резисторов одинакового сопротивления, образующих квадрат. Если на противоположные вершины этого квадрата подать сигнал, то разность потенциалов на оставшихся двух

вершинах будет равна нулю. К противоположным вершинам подключаем выход сетевой карты, к оставшимся двум (тоже противоположным) — вход. Адаптер не "увидит" собственного сигнала, т. е. наша цель достигнута. В действительности сигнал может быть — вследствие разброса сопротивлений резисторов. Поэтому, чем на большее количество интерфейсов делается пассивный хаб, тем меньше должен быть разброс параметров резисторов. Их сопротивление должно быть вполне определенным: подключив омметр к любым двум противоположным вершинам, мы должны получить 100 Ом. Это волновое сопротивление применяющейся в Ethernet витой пары. Если сопротивление будет отличным от 100 Ом, будут возникать эффекты отражения сигнала, которые сделают сеть неработоспособной.

Практического смысла рассмотренная конструкция не имеет и приведена лишь для иллюстрации принципа работы пассивного хаба.

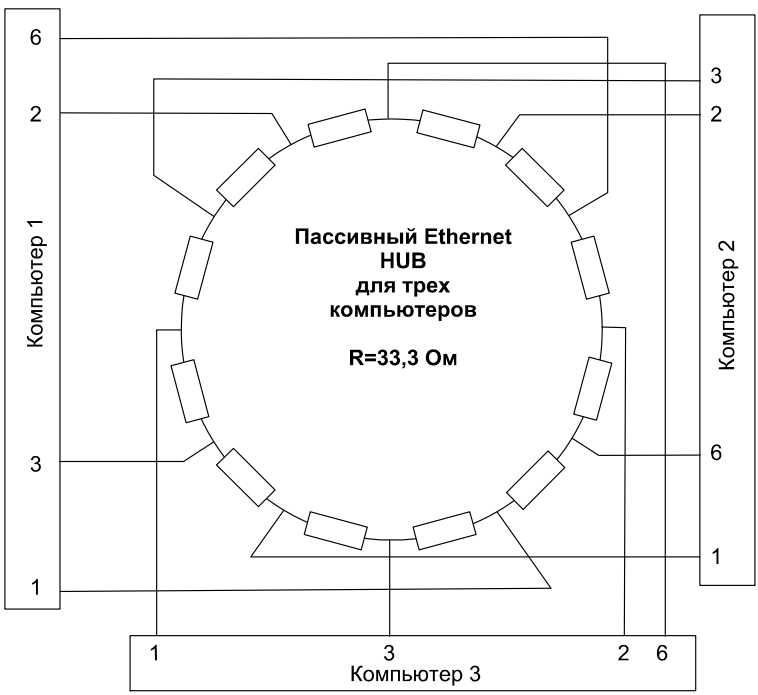


Рис. 4.69. Пассивный хаб для витой пары

Теперь рассмотрим хаб на *N* компьютеров. В общем случае это такая схема, которая с точки зрения каждого из интерфейсов (входа и выхода для кон-

кретной машины) представляет собой резистивный мост. Сигнал от любого компьютера, претерпевая полное ослабление для своего входа, остается достаточно сильным, достигнув входа любой другой машины.

Простейший вариант такой схемы — кольцо из резисторов (мост из 4 резисторов — частный случай кольца). Количество резисторов должно быть равно $N \times 4$, а сопротивление каждого резистора соответственно $100/N$.

Для трех компьютеров это будет 12 резисторов по 33,33 Ом каждый. Кольцо делается таким образом, что каждая пара "выход/вход" подключается к вершинам квадрата, сторона которого образована равным количеством резисторов. Для трех компьютеров это означает, что подключение производится в точках, отстоящих друг от друга на три резистора. Остальные машины подключаются со смещением на один резистор (рис. 4.69).

Что мы теперь можем сделать?

Рассмотренный нами материал позволяет создавать сети комбинированной структуры, исходя из требований к связи и возможностей пользователей. Операционные системы, применяемые при построении сети, могут быть выбраны по вашему желанию. Если ресурсы компьютеров ограничены, то вполне достаточно Windows 95/98 и даже DOS, но лучше версии PTS-DOS 2000. Требуя очень незначительных по нынешнему времени ресурсов, система PTS-DOS 2000 позволяет, не выходя из DOS, работать с Интернетом, устанавливать сетевые соединения, причем браузер, входящий в состав системы (к сожалению, не русифицирован), позволяет организовать рабочий стол, а для файлов применять значки.

Попробуем, используя имеющиеся у нас возможности, составить эскизный проект сети, который вам не предложит ни одна компания (рис. 4.70), специализирующаяся на организации сетей. Процедуры настройки были рассмотрены ранее и теперь предполагается, что вы можете их выполнить самостоятельно.

Необходимо обеспечить связь между компьютерами семи пользователей:

- пользователь 1 — администратор сети, сервер, есть выход в Интернет;
- пользователи 2, 3, 7 — территориально в пределах досягаемости кабельной сети;
- пользователи 4, 5 — возможен доступ по телефонной линии;
- пользователь 6 — удаленный доступ через Интернет.

Рассмотрим средства связи, установленные на компьютерах пользователей (табл. 4.3).

Таблица 4.3. *Средства связи в "композиционной" сети*

	Пользователь 1	**Пользователь 2**	**Пользователь 3**	**Пользователь 4**	**Пользователь 5**	**Пользователь 6**	**Пользователь 7**
Сетевая плата	+	+	+	–	–	–	–
Модем	+	+	+	+	+	+	–
COM-порт, свободный для связи	–	–	+	–	–	–	+
WinRoute или WinGate	+	+	+	–	–	–	–
Radmin	+	+/–	+/–	+/–	+/–	+/–	+/–
Transmitter	+	–	–	+/–	+/–	+/–	+/–
HyperTerminal	+/–	+	+	+	+	–	–
Система Windows	95/98	95/98	95/98	95/98	95/98	95/98	95/98
Скорость связи с Пользователем 1	–	Высокая	Высокая	По расписанию. Низкая	По расписанию. Низкая	По расписанию. Высокая	Определяется портом
Постоянный IP-адрес	Со стороны Ethernet	+	+	+	+	–	–
NetBEUI	+/–	+	+	+	+	–	–

"+" — желательно.
"–" — не требуется.
"+/–" — по желанию.

В соответствии с расписанием возможны периоды, когда все пользователи находятся в активном состоянии. В это время может быть обеспечена связь — "каждый с каждым". Но в большинстве случаев достаточно того, что каждый пользователь может получить доступ к ресурсам сети.

Пользователь 6, получающий возможность связи с сетью через Интернет, может использовать комплексно Transmitter и Radmin. Это позволит ему, установив связь через Transmitter или любую другую программу связи, передать значение своего IP-адреса или запросить адрес сервера, и использовать для соединения Radmin. В этом случае он получает доступ ко всем ресурсам сети, используя прямые соединения и соединения через промежуточный компьютер, работающий подобно маршрутизатору для Radmin. В сети может использоваться одновременно несколько телефонных линий, к которым имеют выход различные машины сети, что расширяет информационный канал для входа извне. Крупные организации могут позволить себе многоканальные телефоны. В нашем случае нет необходимости обеспечивать возможность одновременной связи для многих пользователей. Но для двух-трех входящих звонков (пусть и в определенное расписанием время) наша сеть готова.

Участок сети Ethernet, изображенной на рис. 4.70, выполнен на коаксиальном кабеле, но ничего не изменится с точки зрения функциональности сети, если применить витую пару. Поменяется только состав оборудования — добавится хаб.

Вообще говоря, наша сеть — это не только стандартные средства связи, строго соответствующие ГОСТам и ТУ. Это еще искусство применить минимальные средства для получения максимального или достаточного эффекта. Не все средства и методы, рассмотренные нами, пригодны для предприятий. Для них, особенно для крупных организаций, существуют определенные нормы, связанные с необходимостью совмещения с другими сетями и высокой надежностью. Такие сети требуют применения дорогостоящего оборудования. Но к строительству домашних сетей, сетей небольших офисов и предприятий, которые не входят в сети корпораций, вполне можно подойти творчески и применить нестандартные варианты. Постепенная доводка сети и определение наиболее удобных и надежных решений приведут к результату, который по соотношению надежности, быстродействия и стоимости недостижим для стандартных сетей.

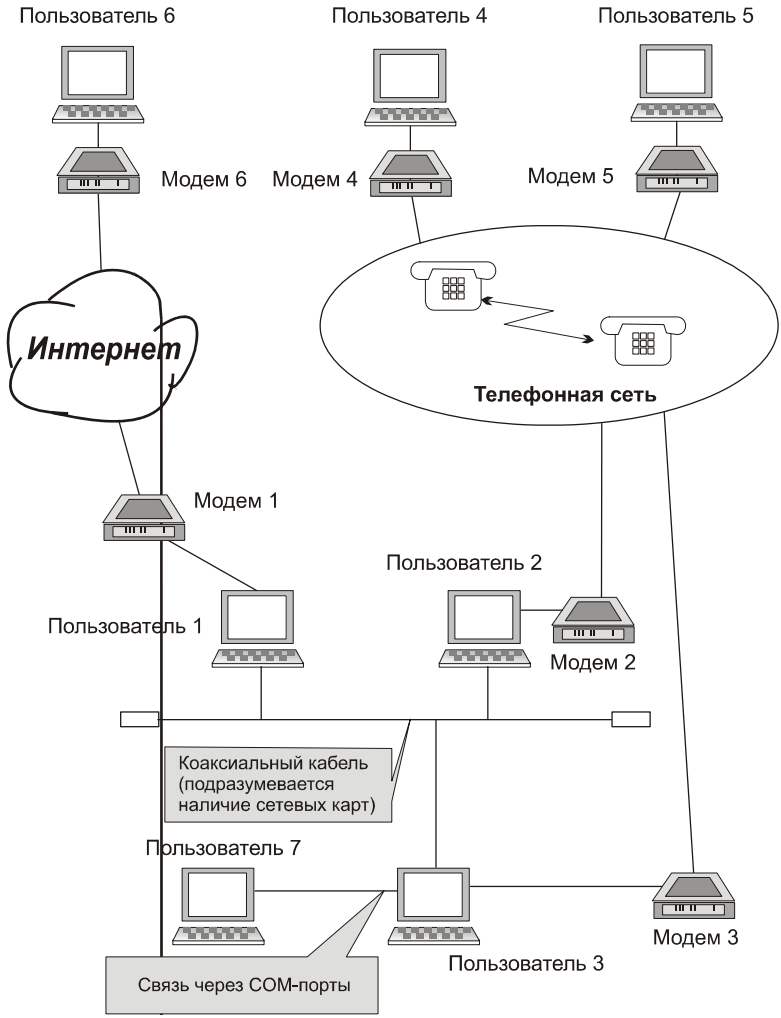
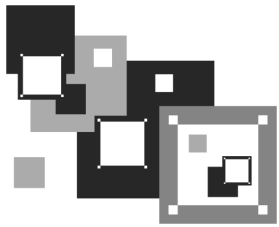


Рис. 4.70. Одна из возможных "композиций" на тему "Наша сеть"

Глава 5



Защити свою сеть

Прошла пора экспериментов и время кропотливой настройки. Сеть работает и, возможно, расширяется. Подключаются новые пользователи, заглядывают гости, разрастается файловый архив, растут базы данных... Но ничто не вечно под Луной. Однажды "доброжелатель" не сможет противостоять жгучему желанию напакостить или пару раз отключится напряжение. Все может быть. Но мы не привыкли думать заранее.

Пока гром не грянет...

Да, да — не перекрестится! Если уже произошло, то следует временно остановить работу сервера, проверить *все* диски на наличие инфекции, и если ваш антивирус не зарегистрирован и не лечит заразу, а лишь указывает на ее наличие, то удалить файлы или собрать их в один каталог, доступ к которому будет только у вас. Позже вы сможете вылечить файлы.

Есть вирусы, которые терпеливо ждут своего часа, а пользователи, не задумываясь о последствиях, работают с зараженными файлами. Иногда такой файл с макровирусом лежит себе в какой-либо папке год или больше, а папка на дискете... Сеть чистая, вы спокойны, а пользователю понадобился файл, он его достал и открыл. Зараза попала на его машину. Результаты работы с файлом пользователь 1 послал пользователю 2, а тот поместил жутко интересную информацию в общедоступный архив и *всем* об этом объявил. А завтра наступает час "икс". Машины "виснут", пользователи их перезагружают, но бедные компьютеры перезагружаются... а на черном экране появляется сообщение о том, что диск не системный, следует заменить его и нажать любую клавишу. Только в сообщении не говорится, на что надо заменить диск.

Кое-кто додумался вставить загрузочную дискету, перейти на диск C: и набрать команду `dir`. И что же этот кое-кто увидел? Да ничего особенного — несколько пустых каталогов и несколько бесполезных файлов, разбросанных там и сям. Зараза уничтожила все труды пользователя, и не только его.

Я не придумал эту историю, она произошла несколько лет назад в одной из сетей. Но самое интересное еще впереди. Прошел год. Дата активизации вируса выпала на выходной и прошла незамеченной. Еще через год вирус "съел" данные с нескольких винчестеров. *Все* помнили о вирусе, со всеми была проведена разъяснительная работа, регулярно сеть сканировалась антивирусом, но к часу "икс" снова была потеряна информация на части машин. Коварный вирус всплыл и активизировался несмотря на то, что его ждали. Плохо ждали, беспечно.

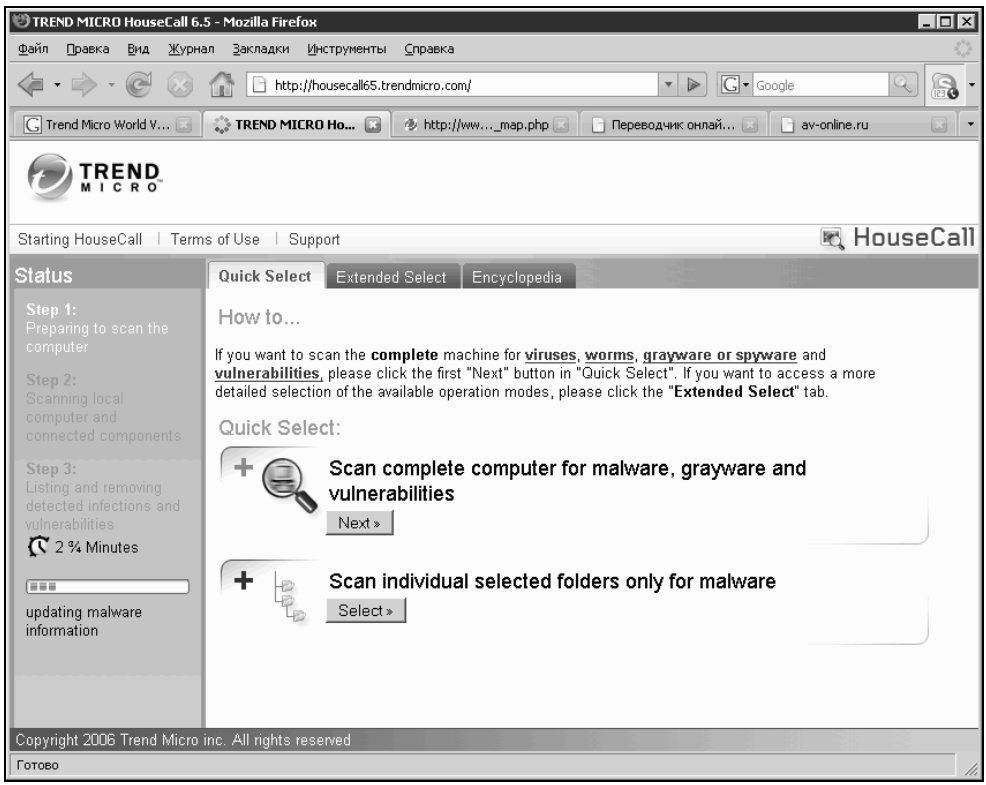


Рис. 5.1. Окно входа
в программу online-антивирусного сканера

Посещая время от времени архивы домашних сетей, доступ к которым возможен через Интернет, я обнаруживаю зараженные файлы и в некоторых из них.

Что же делать? Не жалейте времени и денег на борьбу с вирусами. Имейте в своем распоряжении работоспособную антивирусную программу. Часто производители таких программ предлагают бесплатно версию, которая не может проверять сетевые диски, но отлично работает на локальной машине, обнаруживая и вылечивая зараженные файлы. Иногда борьба с вирусом возможна даже без такой программы.

Рис. 5.2. Online-антивирусный сканер проверяет выбранные вами файлы

Так, если вы получили и прочитали уже в MS Word DOC-файл, а следом получили информацию о том, что этот файл заражен макровирусом, можно не беспокоиться. Достаточно удалить этот файл(ы), который вы читали или создавали позже, и обязательно удалить шаблон Normal.dot. Шаблон будет вос-

становлен автоматически, а зараза будет удалена. Бывает, что недостаток памяти слабой машины не позволяет запустить на ней антивирус. В этом случае периодическое удаление шаблона Normal.dot позволит резко снизить вероятность заболевания. К несчастью, не все макровирусы удаляются так просто, и надо иметь версии антивирусных программ, которые запускаются и на самых слабых машинах. Большой популярностью пользуются различные версии антивирусов "Лаборатории Касперского" (**www.kaspersky.ru**).

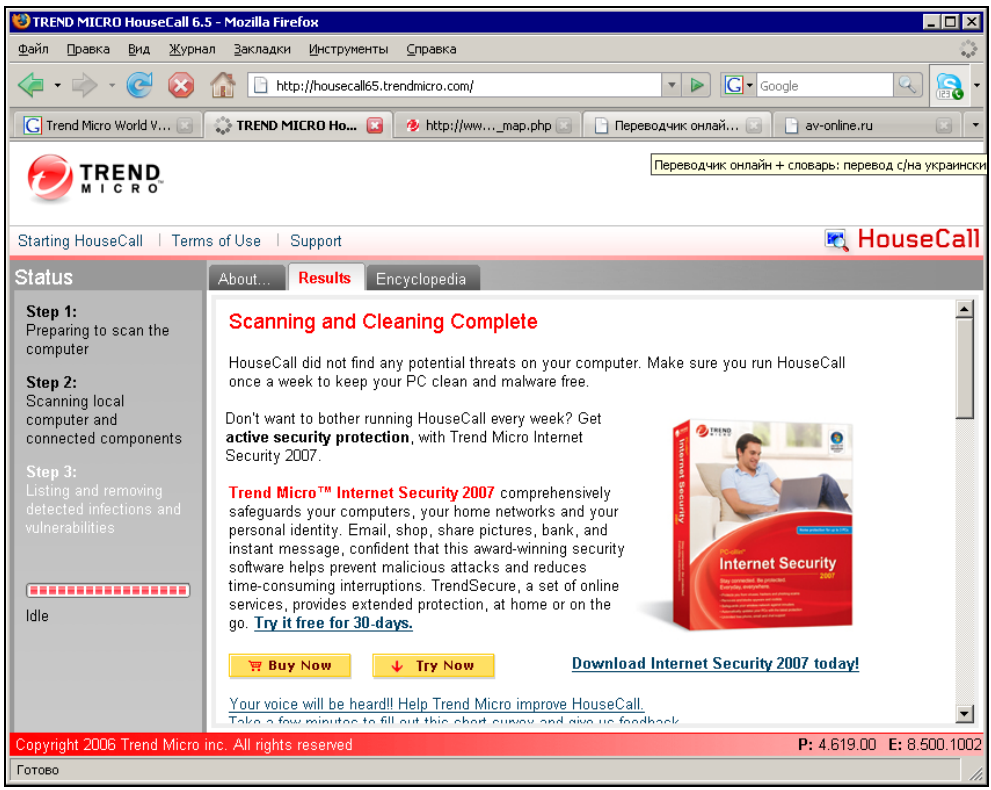


Рис. 5.3. Online-антивирусный сканер завершил проверку компьютера

Некоторые провайдеры помещают у себя ссылку на сайт, откуда может быть запущена дистанционная проверка вашей машины на вирусы с помощью компании Trend Micro World Virus Tracking Center (**http://housecall.trendmicro.com/**) (см. рис. 5.1).

В процессе проверки вы будете видеть оставшееся до завершения процедуры время (см. рис. 5.2). Само собой, сканирование и лечение может занять продолжительное время — перед запуском online-антивируса оцените запасы времени вашего доступа к Интернету. Если на вашем компьютере не будет обнаружено вирусов, то об этом также будет сообщено (рис. 5.3).

Еще один полезный online-сканер для поиска и уничтожения троянских программ — Free online Trojan Scanner (рис. 5.4) — можно найти в Интернете по адресу **http://www.windowsecurity.com/trojanscan/**.

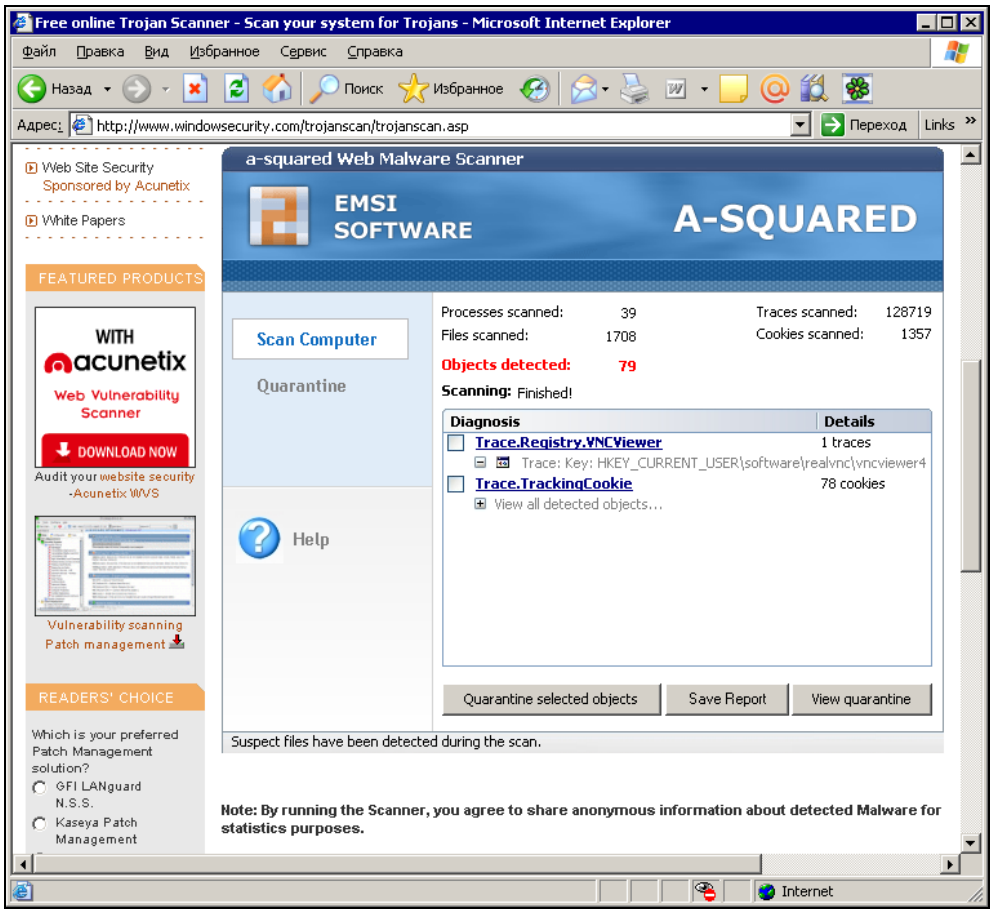


Рис. 5.4. Free online Trojan Scanner (Сканер троянов)

Сам сканер не уничтожает троянские программы, но выводит перечень найденных файлов с вредоносным кодом, а вам уже решать, что удалить, а что оставить. На приведенном рисунке сканер обнаружил VNCViewer, который принял за троянскую программу. Но лучше перестраховаться и подозревать некоторые безобидные файлы, чем пропустить настоящий вирус.

Подобных средств для обнаружения и лечения вирусов в Интернете можно найти немало, далее приведены некоторые из адресов, где их можно найти.

- Panda ActiveScan: **http://www.pandasoftware.com/activescan/ru/activescan_principal.htm**.
- BitDefender Online Scanner: **http://www.bitdefender.com/scan8/**.
- Symantec Security Check: **http://www.symantec.com/home_homeoffice/security_response/index.jsp**.
- McAfee VirusScan: **http://virusscan.nl.nu/**.
- F-Secure Online Virus Scanner: **http://support.f-secure.fi/fin/home/ols.shtml**.
- eTrust Antivirus Web Scanner: **http://www.ca.com/ru/**.
- Free online Trojan Scanner: **http://www.windowsecurity.com/trojanscan/**.
- Kaspersky Online Scanner: **http://www.kaspersky.ru/virusscanner**.
- Dr.Web: **ftp://ftp.drweb.com/pub/drweb/cureit/cureit.exe**.

Во всех случаях для проверки компьютера на вирусы online-средствами требуется установка каких-либо компонентов антивирусных программ или утилит, которые отличаются от полных версий невозможностью обновления антивирусных баз. Ход проверки можно видеть в окне браузера или в отдельном окне утилиты.

Если у вас установлена версия антивирусной программы, которая поддерживает проверку сетевых дисков (из приведенных выше — Dr.Web), то вы сами можете периодически контролировать удаленные компьютеры. Конечно, во время такой проверки нагрузка на проверяемый компьютер возрастет, и он может немного "притормаживать", но из двух бед выбирают меньшую. Можно установить и DOS-версию антивируса, запуская его перед загрузкой Windows. Дольше происходит загрузка, но самозапускающиеся вирусы могут быть уничтожены перед началом работы.

Примечание

DOS-версии антивирусов не смогут работать в операционных системах, выпущенных после Windows ME.

Чем чаще вы будете проверять на наличие вирусов ваш компьютер и машины пользователей сети, тем безопаснее будет ваша сетевая жизнь.

К сожалению, не все вредоносные программы могут определяться как вирусы. Обычный BAT-файл, доступ к которому на пару секунд может получить злоумышленник, может стать коварным оружием в его руках. Представьте себе, что такой файл содержит одну команду `Format C:`. Вы оставили свой любимый компьютер на полчаса, решив попить чаю, а вернувшись обнаружили процесс в стадии завершения...

Правда, в этом случае нет причин сильно расстраиваться. Существует множество средств, позволяющих вернуть все на свои места. Эти средства содержатся в распространенных комплектах утилит типа Norton Utilities или Fix-It Utilities фирмы Ontrack.

Но форматирование винчестера — не самая большая пакость, на которую способны вирусы и резидентные программы, засланные к вам хакерами. Возможно похищение информации с вашей машины, кража паролей, а затем времени доступа в Интернет. Вполне вероятна порча файлов, когда они не уничтожаются, а переписываются в виде, не пригодном для дальнейшего использования. В этом случае восстановление информации при отсутствии резервных копий, хранящихся в надежном месте, становится проблематичным. Причем портиться могут системные файлы, что приведет к невозможности загрузки системы в следующий раз. Некоторые несанкционированные действия хакеров или проявления деятельности вирусов носят совсем безобидный характер. Например, в случайные моменты времени может появляться сообщение с приветствием или угрозой от хакера или совсем отвлеченного характера вроде "Я не люблю брюки в клеточку" (это сообщение появлялось на компьютере секретаря одной уважаемой организации при загрузке MS Office, но не каждый раз, а по случайному закону). Но появление такого сообщения и даже просто необычное поведение компьютера должно вас обеспокоить и заставить провести проверку на вирусы.

AnVir Virus Destroyer

По адресу **http://anvir.com** можно найти очень компактную (всего 153 Кбайт), работающую под всеми операционными системами семейства Windows программу, позволяющую уничтожать многие известные вредоносные вирусы. Вирусы, не известные программе, могут быть обнаружены до начала их разрушительной деятельности в момент проникновения в ваш компьютер и/или

внесения изменений в реестр с целью самозапуска при очередной загрузке компьютера. При изменении записей в реестре программа предупреждает пользователя об этом событии. Остается средствами самой программы просмотреть измененные записи, запретить запуск вредоносной программы, удалить файл вируса. Во время эпидемии вируса MSBlast программа исправно обнаруживала его проникновение в компьютер, и заражение ни разу не произошло.

Если предприняты меры предосторожности при работе с электронной почтой, когда вы сами не открываете подозрительные файлы и удаляете их, то вирусам остается надеяться лишь на автоматический запуск, который и исключается этой программой.

Кроме того, программа позволяет управлять процессами, идущими на компьютере. В любой момент любой процесс можно остановить, например для освобождения памяти. Для каждого запущенного процесса можно определить связанные с ним файлы. В некоторых случаях только эта возможность позволяет удалить вредоносные программы с компьютера.

Программа имеет русскую бесплатную версию. Интерфейс абсолютно понятен.

Если ваш компьютер имеет непосредственный выход в Интернет, то наличие на нем антивирусной программы обязательно, но недостаточно, чтобы обеспечить его безопасность и безопасность сети. Необходима программа, которая сможет стать заслоном от любых подозрительных файлов, приходящих извне. Одна из таких программ — AtGuard.

AtGuard

Это один из лучших персональных firewall. Слово это можно перевести как "передний край" в контексте боевых действий, или "занавес", или "экран". Программа принимает на себя все удары неприятеля, защищая ваш компьютер. В настоящее время программа приобретена корпорацией Symantec и встроена в Norton Internet Security 2000. Этот пакет продолжает совершенствоваться и теперь существует Norton Personal Firewall 2002, который поддерживается Windows XP. Тем не менее до сих пор пользуется популярностью более старая версия AtGuard 3.22, существующая в частично русифицированном виде. Частично русифицированный вариант программы и описывается далее. (Такая версия была доступна автору в момент написания этих строк.)

Помимо функций firewall программа также блокирует большинство баннеров, файлы cookie, JavaScript и апплеты, а также элементы ActiveX. Также возможна защита информации, которую ваш браузер может передать серверу.

Первый этап — настройка программы

После установки и перезагрузки компьютера необходимо запустить программу — в системном лотке появится значок в виде шлагбаума. Щелкнув по нему правой кнопкой мыши и выбрав команду **Settings** (Настройки), можно получить доступ ко всем настройкам программы (рис. 5.5).

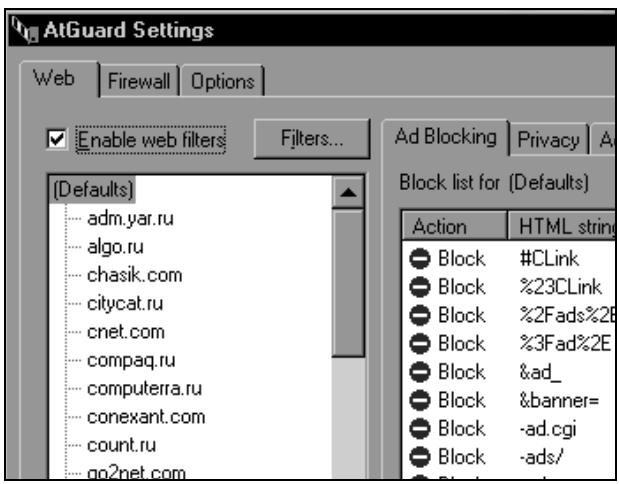


Рис. 5.5. Фрагмент окна программы AtGuard Settings 3.22, вкладка **Web**

На вкладке **Web** можно просмотреть, какие пути для загрузки баннеров будет блокировать AtGuard, и при необходимости добавить свои (нажав кнопку **Add** (Добавить)). Переключившись на вкладку **Privacy** (Защита), необходимо установить, что именно будет блокироваться по умолчанию.

Рекомендуется в начале заблокировать (**Block**) файлы cookies, а позднее разрешать их использование для тех сайтов, на которых они необходимы, например для чатов и почты на основе Web-интерфейса типа Mail.Ru, страницы провайдеров с персональной информацией пользователя — иначе они просто не будут работать.

Далее нужно заблокировать поля **Referer** и **E-mail from** и разрешить (**Permit**) **User-Agent**. Поле **Referer** позволяет удаленному компьютеру определить, с какого сайта вы пришли, поле **E-mail from** — ваш почтовый адрес, и, естественно, раскрывать кому ни попадя эту информацию нет никакой нужды. А вот поле **User-Agent** указывает серверу, каким браузером вы пользуетесь, и, поскольку на большинстве сайтов HTML-код адаптирован под разные версии и типы браузеров, отправку этой информации необходимо разрешить.

На вкладке **Active Content** (Активное содержание) можно заблокировать загрузку потенциально опасных элементов ActiveX, JavaApplet и т. д. Но делать это нежелательно, так как многие странички будут работать некорректно. Если вас раздражает, когда выскакивают сообщения при просмотре страничек или открываются новые окна, — отметьте **Запрет всплывающих окон**.

На вкладке **Firewall** желательно отметить оба флажка — запустить сам firewall (**Вкл. firewall**) и держать его в режиме "обучения" (**Режим обучения**). Уже заранее по умолчанию выставлены несколько правил, которые прежде всего разрешают отдельные служебные запросы и защищают вас от таких известных программ, как BackOffice и NetBus. При первоначальной настройке, кроме двух верхних флажков, ничего здесь трогать не надо.

На вкладке **Options** (Опции) включите все флажки, **Privacy | To place the password** (Секретность | Запоролить) (не очень удобно — приходится постоянно вводить все пароли), и отметьте переключатель **At network** (При входе в сеть), чтобы запускать программу при установке соединения. Если связь у вас плохая или компьютер все время подключен к сети, то выберите **With the system** (Запускать при загрузке системы). Настройки первого этапа завершены.

Временно придется потерпеть на экране панель **DashBoard** (Инструментальная панель). Она позволяет оценивать число установленных соединений и другую статистику. Убедившись в эффективности AtGuard, ее можно отключить, но пока установите на ней все флажки.

Второй этап — настройка браузера

Подключаетесь к сети и запускаете свой браузер, почтовую программу и все остальное, что вы используете для работы в сети. Набираете в адресной строке браузера `www.aport.ru` и нажимаете клавишу <Enter>. Если все в порядке, то на экране появляется окно с четырьмя кнопками: **Always to prohibit** (Всегда запрещать), **Always to permit** (Всегда разрешать), **To prohibit** (Запрещать для этой

попытки), **To permit** (Разрешать для этой попытки). Нажимаете кнопку **Always to permit** (Всегда разрешать) и настраиваете первое правило (самое важное) — разрешаете браузеру устанавливать HTTP-соединение с сервером, причем не только с **www.aport.ru**, а с любым адресом. Пройдя через ряд окошек и создав правило, вы через некоторое время увидите запрошенную страничку. Теперь на экране возникает такая же табличка с четырьмя кнопками, но уже говорящая о том, что программе встретился cookie. Здесь выбор за вами — разрешать их или блокировать (рис. 5.6). Для сайта **www.aport.ru** их стоит разрешить, потому что cookie на нем используются для удобства вашей работы с сайтом. В таком же духе работаете и с остальными сайтами (предупреждение о новом соединении появляться более не будет).

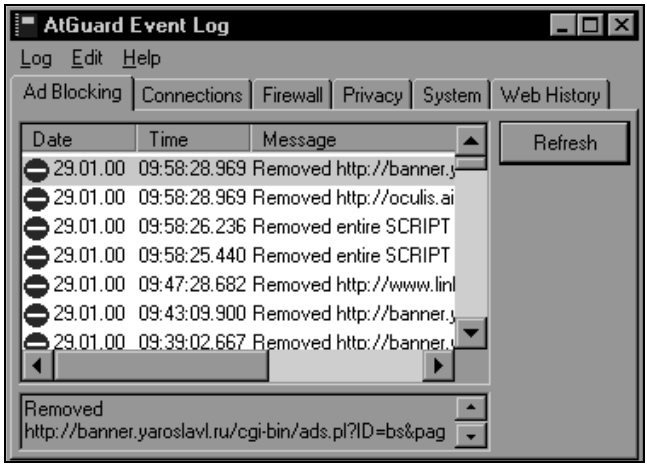


Рис. 5.6. Второй этап настройки

Третий этап — настройка работы с почтой

Отправляем и принимаем почту. При этом необходимо настроить два правила: разрешить POP3-соединение с почтовым сервером и SMTP — с SMTP-сервером, но только для серверов, которыми вы пользуетесь (рис. 5.7).

Точно так же настраиваются и другие программы. Самое главное — понимать, какие соединения характерны для этих программ.

При работе через прокси-сервер понадобится http-proxy.

В программе предусмотрено ведение многочисленных Log-файлов. Проанализировать можно все, от истории посещения страниц (Web-history) и до объема трафика, который был сэкономлен из-за блокирования баннеров. Простейшая статистика ведется прямо на **DashBoard**, остальная доступна через меню **Statistics** (Статистика) и **EventLog** (журнал событий).

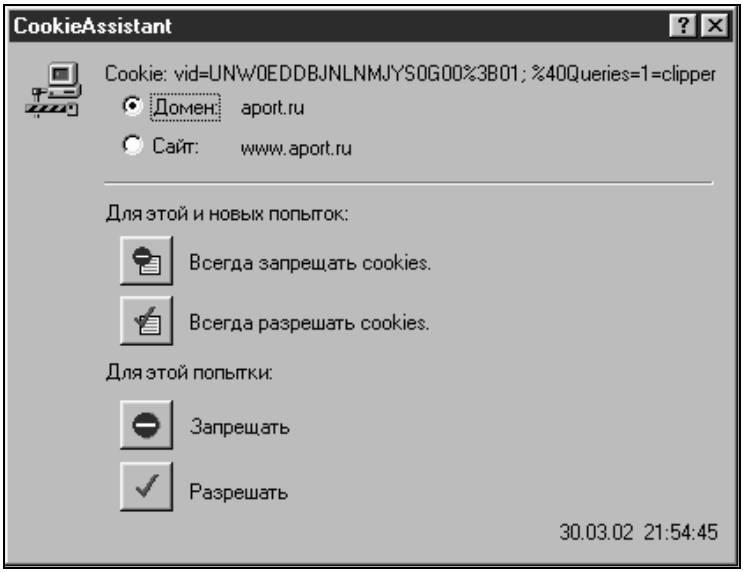


Рис. 5.7. Окно разрешения/запрещения правила соединений

Несколько рекомендаций

Создавайте конкретные правила, а не "Разрешить все всем" (**Permit all to all**).

Иногда просматривайте все правила на предмет обнаружения явных ошибок.

Если у вас не работает какая-то программа (не может установить соединение), отключите firewall прямо с **DashBoard**.

Если же упорно не работает любимый чат или электронная почта, попробуйте отключить блокировку cookies. Впоследствии (отключившись от сети) проверьте, что вы блокируете для данного сайта и не закрыт ли доступ в сеть вашей любимой программе.

Если на вашем компьютере начнет работать вирус-троян, неожиданно возникнет окошко с четырьмя кнопками, извещающее, что неизвестная программа собирается установить соединение с неизвестным вам адресом. Заблокируйте эти действия, немедленно отключитесь от сети и проверьте список программ, запущенных на вашей машине.

Настройка закончена.

Правильно настроенная AtGuard плюс антивирус с последними обновлениями позволят работать в глобальной сети, не опасаясь атак хакеров и других недоброжелателей.

Версия 3.22 встречается на некоторых сайтах, авторы которых считают необходимым сохранять ее для пользователей. Один из адресов — **www.okobox.narod.ru**, другие можно найти, воспользовавшись любой поисковой машиной. В очень удобном виде представляет информацию **Google.ru**. AtGuard — не единственная программа-firewall. При желании можно найти программы других производителей, более простые, но помогающие защитить ваш компьютер от нежелательных контактов в Интернете.

Для защиты от непрошеных страниц в Интернете есть очень простая в использовании бесплатная программа NoAds (**www.southbaypc.com/NoAds**).

NoAds останавливает открытие всплывающих окон во время переходов со страницы на страницу. Настройки программы позволяют определить адреса URL, доступ к которым будет прерываться программой. Программа поддерживает все популярные средства просмотра Интернета — Microsoft Internet Explorer, Netscape Navigator, America Online и Opera. Программа очень проста в использовании, после запуска ее значок находится в системном лотке. Обнаружив новое нежелательное окно, вы его включаете в список неблагонадежных, и программа прекратит к нему доступ в следующий раз.

Не хакер единый

Казалось бы, что достаточно правильно организовать защиту от внешнего и внутреннего врага и можно спокойно работать. Но неприятности часто поджидают совсем не с той стороны, откуда их ждешь. Даже если ваш компьютер не старый, даже если на все его составляющие еще есть гарантия, вы не застрахованы от потери данных из вашей сети. Всегда есть вероятность выхода из строя винчестера, на котором хранится огромный объем чрезвычайно важной для вас информации.

Можно ли предугадать или предсказать момент выхода винчестера из строя? Да, можно. По адресу **www.acelab.ru** вам окажут помощь, если ваш винчестер уже вышел из строя. Для этого необходимо перекачать программу, которая будет постоянно контролировать параметры всех винчестеров, установленных на вашей машине. S.M.A.R.T. vision — так называется программа диагностики винчестеров. Ее можно найти по адресу **http://softportal.com/?id=17** или **http://www.acelab.ru/dep.pc/resource.php#PC**.

Программа будет извещать вас о всех отклонениях параметров дисков, которые могут привести к потере данных. Значок программы будет находиться в системном лотке на панели задач и в зависимости от состояния дисков менять цвет от зеленого, когда все работает нормально, до красного, когда параметры дисков перешагнули некоторое пороговое значение и не за горами крах системы. Желтый цвет значка предупреждает о необходимости разобраться подробнее, какие параметры изменились, и пока не поздно принять меры к сохранению данных.

S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technolodgy) — технология самотестирования, разработанная производителями HDD для повышения степени надежности хранения информации. Суть S.M.A.R.T. заключается в том, что сам винчестер отслеживает состояние своей работоспособности и может заранее предупредить пользователя о предаварийном состоянии. Пользователь компьютера, оснащенного S.M.A.R.T.-винчестером и специальной программой S.M.A.R.T.-диагностики, извещенный о состоянии диска, сможет избежать потери данных, хранящихся на винчестере. В настоящее время технологию S.M.A.R.T. поддерживают все производители жестких дисков: Seagate, Western Digital, Quantum, Fujitsu, Maxtor, Samsung, Hitachi, IBM.

Состояние работоспособности оценивается по нескольким параметрам работы накопителя, которые называются *атрибутами надежности* (attributes). Каждый атрибут имеет свой номер — ID (идентификатор). Атрибутам надежности соответствуют параметры работы накопителя, которые могут характеризовать его естественный износ и состояние:

- количество старт/стоповых циклов, выполненных накопителем;
- количество оборотов, совершенных шпиндельным двигателем;
- количество позиционирований, совершенных головками чтения/записи;
- высота полета головки чтения/записи над поверхностью диска;

- скорость передачи данных с магнитных поверхностей в кэш-буфер накопителя;
- время выхода накопителя в состояние готовности;
- подсчет переназначений bad-секторов;
- подсчет совершенных накопителем ошибок позиционирования;
- подсчет случаев коррекции данных при операциях "чтение/запись";
- подсчет повторных рекалибровок накопителя и т. д.

Например, для накопителей Western Digital применяются атрибуты — контролируемые параметры, приведенные в табл. 5.1.

Таблица 5.1. *Атрибуты надежности, применяемые для накопителей Western Digital*

ID	Контролируемый параметр
1	Read Error Rate
4	Start/Stop Count
5	Relocated Sector Count
10	Spin up Retry Count
11	Drive Calibration Retry Count
199	ULTRA DMA CRC Error Rate
200	Multi-zone Error Rate

Большинство S.M.A.R.T.-винчестеров имеют от 3 до 15 атрибутов надежности. Максимально возможное их количество — 30. Состав и количество атрибутов надежности определяются самими производителями индивидуально для каждого типа HDD.

Значения атрибутов надежности могут лежать в диапазоне от 1 до 253. Первоначально атрибуты имеют максимальные значения. По мере износа винчестера или в случае возникновения предаварийного состояния значения атрибутов надежности уменьшаются. Следовательно, высокое значение атрибутов говорит о малой вероятности выхода накопителя из строя и, соответственно, низкое значение атрибутов — о снижении надежности накопителя и возрастании вероятности выхода его из строя. Как правило, верх-

ние границы атрибутов надежности имеют значение 100 (IBM, Quantum, Fujitsu) или 253 (Samsung). Но есть и исключения. Так у HDD Western Digital моделей WDAC34000, WDAC33100, WDAC31600 первый атрибут надежности имеет максимальное значение 200, а остальные — 100.

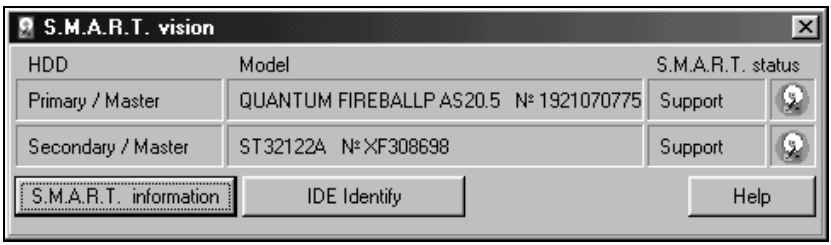


Рис. 5.8. Информация о HDD

Для того чтобы получить расширенную информацию, дважды щелкните мышью по значку S.M.A.R.T.-состояния. В раскрывшемся окне (рис. 5.8) вы увидите таблицу представленных в системе HDD, состоящую из четырех столбцов

- **HDD** — место винчестера в системе: Primary/Master, Primary/Slave, Secondary/Master, Secondary/Slave;
- **Model** — тип винчестера;
- **S.M.A.R.T** — поддержка накопителем технологии S.M.A.R.T. Возможные варианты:
  - **Support** — HDD поддерживает S.M.A.R.T-технологию;
  - **Not Support** — HDD не поддерживает S.M.A.R.T-технологию;
  - **Error** — HDD поддерживает S.M.A.R.T-команды, но контрольная сумма S.M.A.R.T.-параметров не сходится. В этом случае результаты S.M.A.R.T.-диагностики могут быть ложными;
- **status** — результат S.M.A.R.T-диагностики HDD. Если компьютер оснащен несколькими S.M.A.R.T.-винчестерами, то значок общего S.M.A.R.T.-состояния на панели задач соответствует накопителю с худшим результатом S.M.A.R.T.-диагностики.

Для того чтобы получить расширенную информацию о значениях каждого из атрибутов надежности, нажмите кнопку **S.M.A.R.T. information** и выберите

нужный жесткий диск. Вы увидите значения атрибутов надежности и соответствующие им пороговые значения в графическом представлении (рис. 5.9).

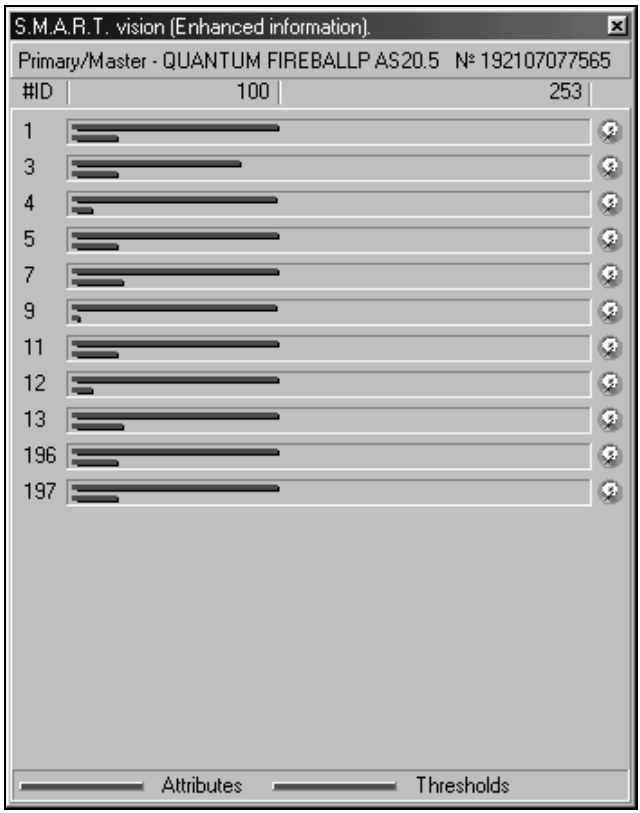


Рис. 5.9. Подробно о параметрах винчестера

На рис. 5.9 короткие индикаторные линии соответствуют пороговому значению параметров, а длинные — их действительному значению.

В настоящее время не все производители HDD предоставляют сведения о том, какие параметры характеризуются атрибутами надежности. Считается, что достаточно знать, не вышел ли какой-нибудь из контролируемых атрибутов за установленные пределы.

Нажав кнопку **IDE Identify**, можно получить подробную информацию о характеристиках HDD (паспорт диска), соответствующую спецификации ATA-4.

Для примера приведем паспорт QUANTUM FIREBALL PAS20.5 (табл. 5.2).

Таблица 5.2. *Паспорт диска*

Параметр	**Значение**
Интерфейс	ATA
Тип	Несъемное устройство и/или контроллер
Логических цилиндров	16 383
Логических головок	16
Логических секторов в треке	63
Модель	QUANTUM FIREBALL PAS20.5
Серийный номер	192107077565
Версия микропрограммы	A1Y.1500
Количество байтов, доступных при командах READ/WRITE LONG	4
Максимальный размер блока для команд READ/WRITE MULTIPLE	16
Таймер остановки	Значения таймера остановки определены производителем
Поддержка IORDY	Да, может быть отключен
Поддержка LBA	Да
Поддержка DMA	Да
Емкость	16 514 064 секторов (8063 Мбайт)
Емкость, доступная в режиме LBA	40 132 503 секторов (19 595 Мбайт)
Текущий размер блока для команд R/W Multiple	16
Multiword DMA Mode 0	Доступен
Multiword DMA Mode 1	Доступен

Таблица 5.2 *(окончание)*

Параметр	**Значение**
Multiword DMA Mode 2	Доступен, активный
Ultra DMA/33 Mode 0	Доступен
Ultra DMA/33 Mode 1	Доступен
Ultra DMA/33 Mode 2	Доступен (текущий)
Поддержка PIO Mode : 2	Да
Поддержка PIO Mode : 3	Да
Поддержка PIO Mode : 4	Да
Минимальное время цикла Multiword DMA	120 нс
Рекомендуемое время цикла Multiword DMA	120 нс
Минимальное время PIO-цикла без управления потоком	120 нс
Минимальное время PIO-цикла с IORDY	120 нс
Поддержка ATA-1	Да
Поддержка ATA-2	Да
Поддержка ATA-3	Да
Поддержка ATA-4	Да
Поддержка ATA-5	Да
Поддержка управления питанием	Да
Поддержка управления безопасностью	Да
Поддержка S.M.A.R.T-функции	Да

Для кого-то эта программа будет только индикатором состояния винчестеров, для других она окажется полезной и при настройке всей системы в целом, поскольку не всегда информация, которую выдает программа, бывает легко доступна в другом месте.

Если данные все же потеряны, можно обратиться по приведенному ранее адресу или на сайт **www.antivirus.ru**.

На этом сайте находится компьютерная скорая помощь, которая восстанавливает информацию в режиме online или выезжает на место. Винчестеры становятся все более сложными устройствами. Объем их быстро увеличивается, и программы, воспользовавшись которыми можно было раньше в домашних условиях восстановить информацию после сбоя, быстро устаревают. Описанная далее программа позволяла восстанавливать информацию на винчестерах размером до 8 Гбайт.

Если вы не имеете возможности получить помощь по этим адресам или хотите восстановить информацию самостоятельно, то во многих случаях это можно сделать. Важно, чтобы восстанавливаемый винчестер вращался, а электроника, установленная на нем, была исправна. Любое удаление файлов или форматирование диска не приводят к полной потере информации. Для того чтобы действительно удалить *всю* информацию с диска, применяют специальные программы, которые могут на удаление данных потратить очень продолжительное время (часы). Потеря элементов информации, которая не дает возможности прочитать данные с диска, не приводит к их полному уничтожению. Один из наиболее эффективных путей восстановления данных — применение программ Tiramisu, Easy Recovery. Это названия одной и той же программы фирмы Ontrack Data International, Inc. (**www.ontrack.com**), существующей в разных версиях. В комплекте Fix-It Utilities 3.0 создается загрузочная дискета, содержащая программу, работающую под MS-DOS. Tiramisu — более старая версия программы, не работающая с дисками емкостью более 10 Гбайт. В незарегистрированном виде она способна восстановить несколько файлов, после чего ее необходимо перезапустить. Зарегистрированные полнофункциональные версии программы способны восстановить практически всю информацию с отформатированного винчестера. Но сохранять данные в процессе восстановления необходимо на другой, исправный диск. Новые версии программы обычно носят название EasyRecovery.

Интерфейс программы может существенно отличаться, но суть работы остается одна. Программа может восстанавливать данные с диска, где уже отсутствует FAT и ее копия. Проанализировав винчестер, программа создает виртуальную FAT и показывает виртуальное дерево каталогов и файлов, которые удалось восстановить. Пользователь имеет возможность сохранить на другом носителе все или часть найденных файлов. Имена каталогов могут не соответствовать реальным, но файлы, содержащиеся в них, обычно восстанавливаются очень корректно.

Принцип работы программы не изменился, поэтому рассмотрим старую версию, которую часто еще можно встретить у "продвинутых" пользователей.

После запуска командой **Start Recovery** программа Tiramisu довольно продолжительное время анализирует выбранный диск (рис. 5.10).

Рис. 5.10. Интерфейс программы Tiramisu

В ходе анализа производится выделение подсветкой надписей, указывающих вид текущего процесса. Текущие операции отображаются в отдельном окне. На протяжении всей работы программа не делает ни одного изменения записи на диске. Вся работа происходит в оперативной памяти. Поэтому диски большого размера потребуют соответствующего количества свободной памяти, но независимо от результатов работы программы (рис. 5.11) состояние диска не изменится, что позволит повторить процесс восстановления, изменив настройки программы или применив другие средства.

В верхнем правом углу отображается текущее время, а в нижнем правом — объем свободной оперативной памяти. Работая как с файловым менеджером, выбираем необходимый файл или каталог и копируем на второй винчестер или дискету (рис. 5.12).

Программа позволяет выбрать файлы по маске и скопировать требуемый тип файлов со всего диска. Продолжительность процесса восстановления зависит от многих факторов, но для машины с частотой процессора 266 МГц составляет около 15 мин на 1 Гбайт (без учета времени копирования файлов). Команда **File | Create Longname Batch** позволяет создать файл, содержащий длинные имена файлов. Кириллица в этом случае не поддерживается, и короткие имена, если они не испорчены, понятнее длинных. Следует учесть, что Tiramisu, в отличие от новых версий (EasyRecovery V5.0), не видит логических дисков. Она работает с физическим диском — винчестером. Как старые, так и новые версии не отображают кириллицу в именах файлов. Последние версии EasyRecovery имеют новый интерфейс, значительное число настроек, но их (в отличие от Tiramisu) нельзя запустить из-под Windows в окне сеанса MS-DOS.

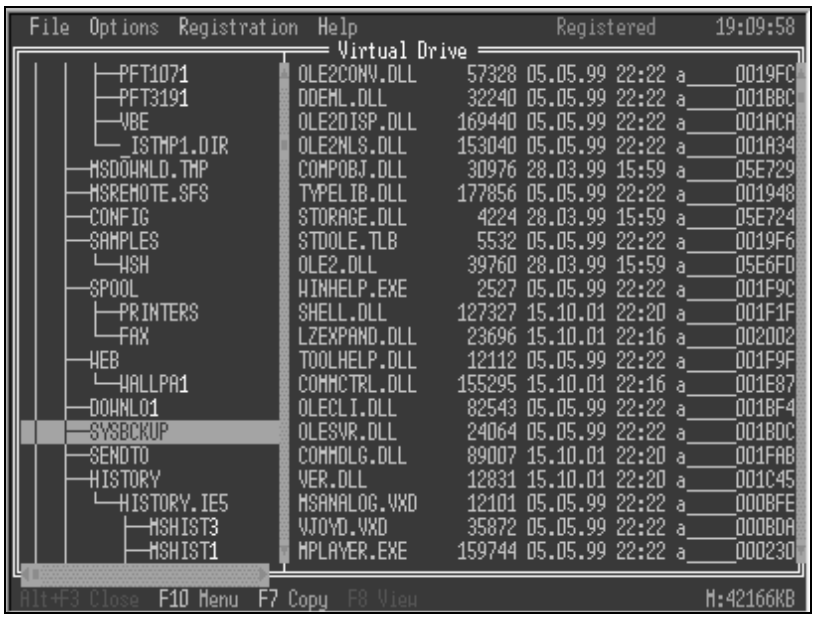


Рис. 5.11. Результат работы Tiramisu

Существуют и другие программы, позволяющие восстанавливать информацию на винчестере. HDD Regenerator (**http://dposoft.net**), например, позволяет восстанавливать намагниченность диска не обращая внимания на его логическую структуру. Программа работает со всеми современными винче-

стерами, запускается в среде Windows, но не работает на некоторых старых компьютерах. Мне не удалось запустить ее на компьютере HP Vectra 1996 года выпуска.

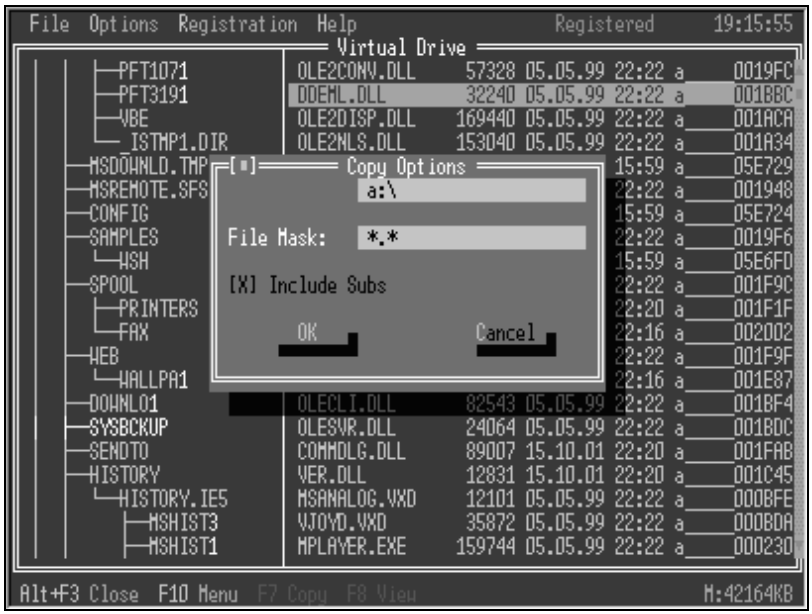


Рис. 5.12. Выбор диска — получателя копии восстановленного файла или файлов

Испорченные файлы

К сожалению, действия по восстановлению файлов после разрушения файловой системы не всегда приводят к восстановлению драгоценной информации. После воздействия вируса или других случайных факторов файлы могут быть повреждены так, что программы, предназначенные для работы с ними, не смогут их открыть. Файлы простой структуры, например текстовые в кодировке DOS, при повреждении потеряют часть своего содержания, но остальная часть будет доступна для просмотра. Файлы более сложной структуры, например файлы офисных приложений, окажутся недоступны для чтения, если в них пропадет даже один байт информации. При этом может пропасть информация о форматировании элементов содержания или другая

часть информации не первостепенного значения. Но файл окажется недоступен полностью, так как будет нарушена его структура, и приложение не распознает его. К счастью, существуют средства для восстановления структуры поврежденных файлов практически для всех офисных приложений. Их можно найти на сайте **OfficeRecovery.com**. Существуют как отдельные приложения типа ExcelRecovery или WordRecovery, так и программы комплексного восстановления файлов офисных приложений. Рассмотрим последовательность действий пользователя при работе с программой восстановления XLS-файлов — ExcelRecovery.

1. Перед началом работы с поврежденным файлом необходимо создать его резервную копию, используя надежные средства для ее сохранения. Лучше, если копия будет храниться на отдельном носителе.
2. Запускаем ExcelRecovery.
3. В меню **File** выбираем пункт **Recover**.
4. Выбираем файл для восстановления.
5. Нажимаем кнопку **Recover**.
6. Ждем, пока завершится процесс обработки, который может занять продолжительное время, если файл большого размера.
7. По завершении восстановления файла появится запрос на сохранение восстановленной копии. Вводим новое имя или соглашаемся с предложенным и сохраняем файл.

Интерфейс программы настолько прост, что нет смысла его здесь приводить. Программы можно получить в демо-версии, при этом они смогут восстанавливать небольшие файлы и будут оставлять в восстановленном файле информацию о себе. Зарегистрированная версия работает с файлами любого размера (проверено на файле размером 8 Мбайт).

Работа с файлами других приложений не отличается от рассмотренной схемы.

Человеческий фактор

Заботясь о сохранении данных, обязательно следует обратить внимание на человеческий фактор. Атаки снаружи или дефекты оборудования при внимательном отношении к процессу защиты данных не принесут столько вреда, как действия разозлившегося или обидевшегося пользователя, который имеет "лишние" права в сети. Доступ к жизненно важным файлам сервера вообще

должен быть закрыт для пользователей сети. Лучше всего, когда доступная по сети информация находится на отдельном винчестере. Это не абсолютная, но достаточно высокая гарантия того, что в систему никто не проникнет и ее не испортит. Эту рекомендацию полезно выполнять не только для сервера, но и для любой машины, работающей в сети. При отсутствии второго винчестера следует создать логический диск, на котором можно разместить необходимую информацию.

Конечно, Windows 95/98 обладают меньшими возможностями разграничения доступа, чем Windows NT/2000, но, установив пароли для доступа к ресурсам сервера, вы существенно повысите безопасность работы. Бóльшая часть файлов должна быть доступна лишь для чтения, что обезопасит даже от непреднамеренного искажения информации. Пароль для полного доступа должен быть по возможности максимально сложным, а знать его может *только* администратор. Пароль, рассказанный по секрету другу, станет известен всей сети очень быстро.

И еще об операционной системе

Разрабатываемые хакерами средства часто предполагают использование в сети ОС Windows, с присущим ей реестром и каталогами Windows и Program Files. Даже переименование папки Windows при установке системы приводит к повышению "хакероустойчивости". А если этих каталогов нет вообще, как и реестра?.. Операционная система, которая редко применяется большинством пользователей, оказывается лучше защищена, чем широко распространенная. Если учесть, что часто сетевое соединение требуется лишь для передачи файлов, то MS-DOS 6.22 или PTS-DOS 2000/32 будет вполне достаточно в качестве операционной системы клиента. Применение PTS-DOS 32 может быть интересно тем, что, установив ее на один диск с Windows, мы спрячем во время работы в DOS каталоги Program Files и Windows (или соответствующие им, если вы используете другие имена). Программа Acronis OS Selector, о которой поговорим немного позже, прячет эти каталоги в скрытый каталог Bootwiz, что способствует сохранению их от повреждения.

Установка PTS-DOS 32 имеет некоторые особенности, о которых следует упомянуть. В то время, когда писались эти строки, были доступны PTS-DOS 2000 с входящими в комплект командным процессором CP (рис. 5.13), поддержкой сети LotLAN и интернет-браузером Arachne. PTS-DOS 32 не комплектовалась ничем.

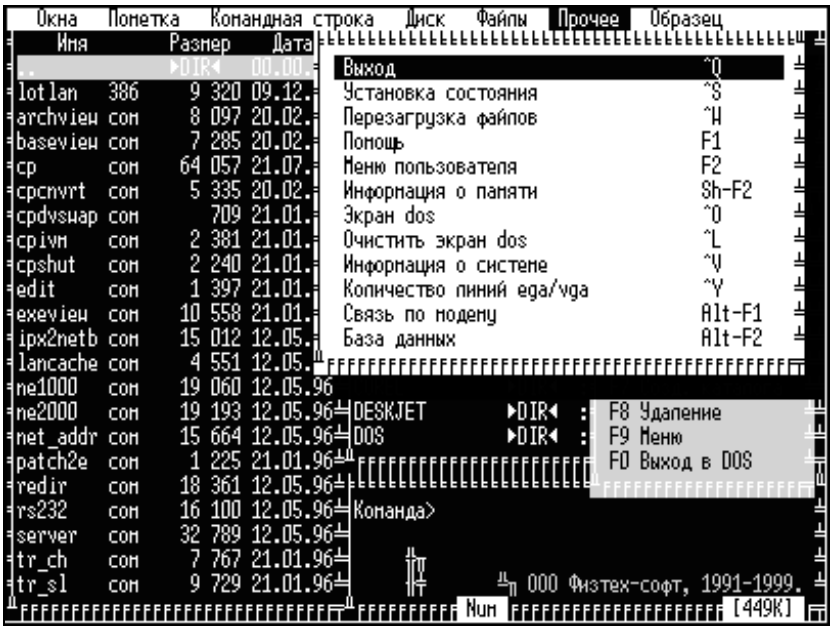


Рис. 5.13. Вид окна командного процессора в PTS-DOS

Но, приобретя PTS-DOS 32, можно перенести из демо-версии PTS-DOS 2000 все дополнительные программы. Arachne, правда, продукт импортный и предупреждает о том, что это не коммерческая версия, тем не менее прекрасно работает, а на сайте **http://home.arachne.cz** доступна и обновленная версия программы. PTS-DOS имеет встроенный менеджер загрузки, хотя более удобным может быть применение Acronis OS Selector (**www.Acronis.com**). Этот менеджер позволяет устанавливать практически неограниченное число операционных систем, в том числе на расширенные разделы. В его состав входит Администратор дисков (в демо-версии отключен), который может заменить Diskedit из NU, PartitionMagic и BootMagic вместе взятые. Но окончательный выбор менеджера загрузки за вами.

Установленная PTS-DOS 32, с перенесенным комплектом сетевых программ, позволяет работать в локальной сети, в Интернете, принимать и отправлять e-mail, а также устанавливать связь с удаленным компьютером по телефону. Важное условие осуществимости всего вышеперечисленного — возможность работы вашего модема под DOS.

Допустимо применение и других, менее распространенных операционных систем. В Интернете можно найти информацию даже о любительских разра-

ботках. Но в каждом конкретном случае необходимо исследовать совместимость вашего оборудования и программного обеспечения с операционной системой.

Контроль

В Windows NT/2000 есть средства постоянного мониторинга сети. Но и в Windows 95/98 можно успешно контролировать процессы, происходящие в системе. При анализе причин, происходящих в сети событий, полезно иметь информацию о запускавшихся программах и открывавшихся файлах. Для постоянного слежения за работой программ на компьютере можно применить программу Alot Nanny (рис. 5.14), которая находится по адресу **http://www.5star-shareware.com/Windows/Hobby/Kids-Parenting/alot-nanny.html**.

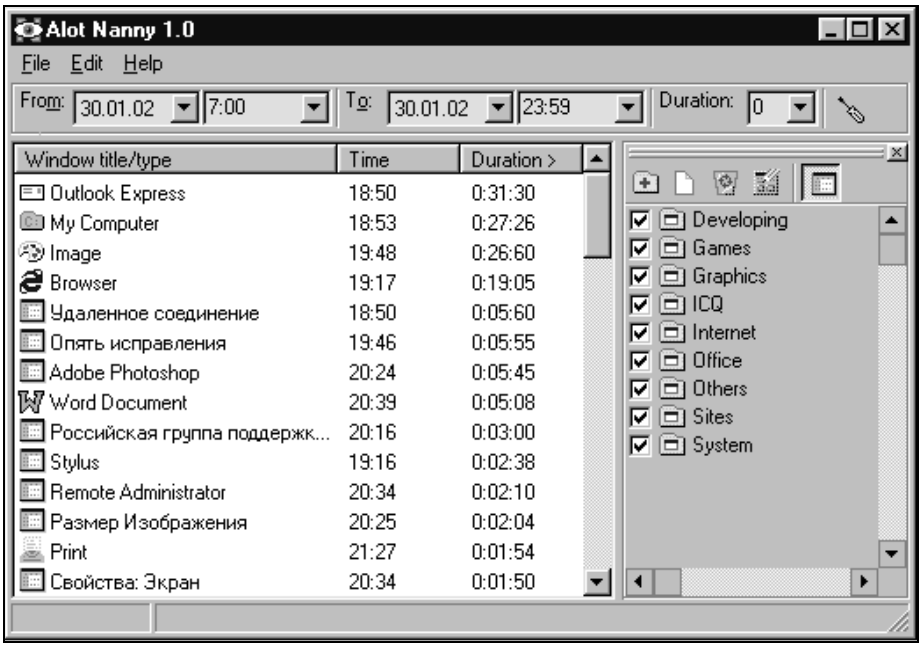


Рис. 5.14. Окно **Alot Nanny**

После запуска программа начинает фиксировать все события, происходящие на машине, где она установлена, отмечая типы открываемых файлов, вре-

мя их открытия, продолжительность процесса работы с ними. Вся информация сохраняется и может быть просмотрена в любой момент времени (рис. 5.15).

Программа имеет две составляющие:

- Eye — программа, которая записывает отчеты на диск в фоновом режиме;
- Nanny — программа, используемая для чтения файла Eye. Отчеты, создаваемые программой, могут обрабатываться (сортироваться и фильтроваться) и просматриваться.

В первый раз прочитав информацию, предлагаемую программой, вы удивитесь подробности и тщательности, с которой она фиксирует все события, происходящие в машине.

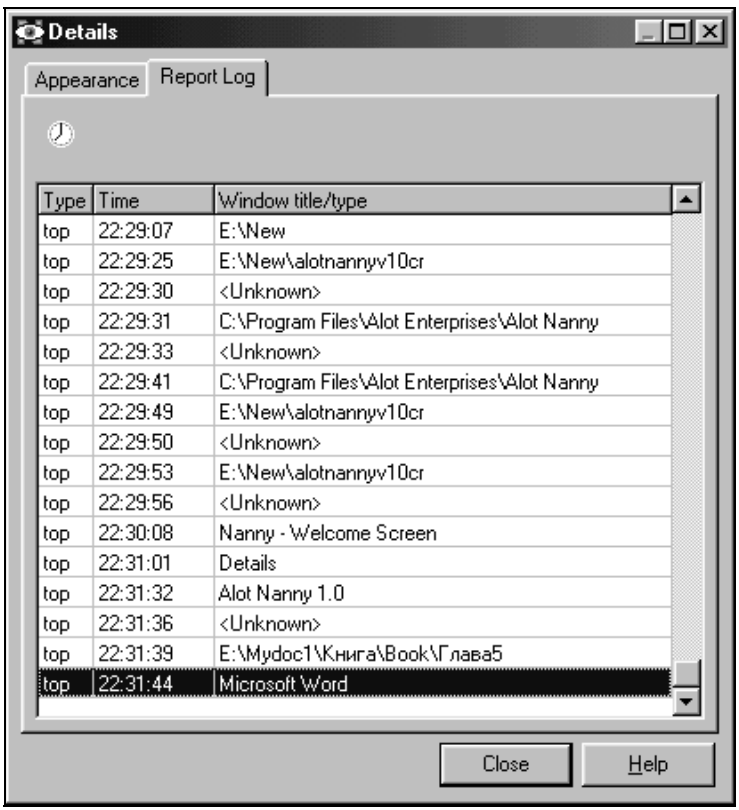


Рис. 5.15. Подробная информация о событиях в системе

Традиционные средства

Как и при работе на обычном ПК, работая в сети, необходимо быть готовым к устранению неполадок, которые возникают, как правило, неожиданно. Необязательно неполадка приведет к разрушениям и потребует мер, рассмотренных ранее. Многие мелкие неполадки проявляются не сразу, и лучше, если вы обнаружите их во время профилактических работ. Профилактика сервера, как и любого ПК, должна проводиться регулярно. Это позволит избежать накопления "критической массы" ошибок, достижение которой приводит к быстрому выходу системы из строя. Для проведения профилактических работ потребуется комплект дискет для диагностики и обслуживания компьютера. В этот комплект должна входить загрузочная дискета, содержащая файловый менеджер, текстовый редактор, стандартные программы для обслуживания дисковой системы. Желательно также иметь дискеты с редактором диска (лучше не одним), программу для восстановления удаленных файлов, программу проверки и исправления ошибок на дисках, антивирусную программу, архиватор, неплохо запастись программой для запоминания содержимого CMOS-памяти и восстановления ее в случае сбоя или преднамеренного искажения.

Рассмотрим подробнее состав аварийного комплекта.

Загрузочная дискета может быть обычной, предложенной Windows при установке, или созданной позже. Можно создать более удобный вариант, учитывающий ваши условия работы и конфигурацию оборудования.

Так, в состав программ, входящих в дискету, резонно включить файловый менеджер. Это может быть VC (Volkov Commander). В последних версиях этого менеджера достаточно одного файла VC.COM для использования программы с минимальными возможностями. В более старых версиях требуется также VC.OVL.

Приведем содержание реальной дискеты, применяемой автором, полученное командой `DIR /S`.

Содержание дискеты

```
Том в устройстве A имеет метку RESTORE
Серийный номер тома: 1F09-0A13
Содержимое папки A:\
MSDOS.SYS        SYS.COM          COMMAND.COM      AUTOEXEC.BAT
```

```
CONFIG.SYS      HIMEM.SYS       FORMAT.COM      IFSHLP.SYS
SETVER.EXE      DISPLAY.SYS     KEYB.COM        MODE.COM
COUNTRY.SYS     KEYBRD3.SYS     MEM.EXE         EGA3.CPI
RKM.COM         EMM386.EXE      LOGO.SYS        [CMOSSA~1]
[VC]            MOUSE.COM       FDISK.EXE
       21 файлов        837 019 байт
Содержимое папки A:\CMOSSA~1
CMSSV4_1.EXE    CMOSSAVE.TXT    CMOS.BAK
CMOS.SAV
4 файлов          7 893 байт
Содержимое папки A:\VC
VC.COM          VC.INI          VCEDIT.EXT      VCVIEW.EXT
VC.MNU          HIEW.EXE        HIEW.INI        HIEW.XLT
HIEW.HLP        HIEW.ORD        HIEW.VMM        EDIT.EXE
EDIT.HLP        NCMENU.COM      TXT.TXT
       15 файлов        308 209 байт
Итоговые данные
       40 файлов      1 153 121 байт
        2 папок          65 536 байт свободно
```

Большинство файлов получены из папки Windows\Command, к ним добавлен файловый менеджер VC, русификатор RKM и программа, сохраняющая содержимое CMOS-памяти, где хранятся сведения о параметрах, которые мы можем установить в BIOS Setup. Для индивидуализации дискеты добавлена заставка Logo.sys — файл формата BMP размером 320×400 точек (пикселов).

Найти необходимые для составления дискеты программы не составит труда. Русификаторы, CMOS-сейверы (программы для сохранения информации из CMOS-памяти), файловые менеджеры разработаны известными фирмами и программистами-индивидуалами в достаточном количестве, чтобы выбрать программу по своему вкусу.

Системные файлы дискеты приведены далее.

AUTOEXEC.BAT

```
lh mouse
lh a:\vc\vc
```

CONFIG.SYS

```
[menu]
Menuitem=D, SuperDisk
Menudefault=D,1
Menucolor=14,1
[D]
dos=high,umb,noauto
Device=himem.sys/testmem:off
Device=emm386.exe ram
Devicehigh=A:\display.sys con=(ega,,1)
Country=007,866,country.sys
Install=mode.com con cp prepare=((866) ega3.cpi)
Install=mode.com con cp select=866
Installhigh=keyb.com ru,,keybrd3.sys
[COMMON]
Fileshigh=30
Buffershigh=20
Stackshigh=9,256
Lastdrivehigh=z
Shell=command.com /E:512 /P
FCBSHIGH=1
```

MSDOS.SYS

```
[Paths]
WinDir=a:\
WinBootDir=a:\
WinBootDir=a:\
HostWinBootDrv=a:
[Options]
BootMulti=0
BootGUI=0
Network=1
```

На других дискетах желательно иметь редактор дисков Diskedit и NDD (Дисковый доктор) из комплекта Norton Utilites. Хорошо, если есть DOS-версии PartitionMagic v.5—7, EasyRecovery v.5 и выше, комплект архивато-

ров и программа-антивирус. Можно обратить внимание и на продукты Acronis (сайт **www.acronis.com**), среди которых есть практически все необходимые средства.

Неплохо, если на дискетах будут сохранены резервные копии системных файлов и образы важнейших областей винчестеров.

Если вы вооружены таким аварийным комплектом, то восстановление системы после практически любого неблагоприятного воздействия не займет у вас слишком много времени, а потери данных будут минимальны. Соответственно, исправная работа сети будет гарантирована.

Не перегружайте систему

Компьютер, конечно, железный, и выдержать он может много, но не все. Если у вас в сети есть выделенный сервер, то на нем не должны производиться какие-либо работы, не связанные с работой сети. А если сервера нет? Как обеспечить бесперебойную работу компьютера в сети? Невозможно удержаться и не поставить новую игрушку или, и того круче, операционную систему. При этом ни один производитель программного обеспечения не берет на себя ответственность за последствия установки нового продукта на ваш компьютер. Вся ответственность ложится на вас. Следовательно, не повредит подложить соломки, хотя бы там, где можем упасть.

Как обезопасить себя от последствий некорректной работы новой программы или собственной ошибки? Такое средство есть.

Резервирование всей системы

Само собой разумеется, что резервные копии системных и других важных файлов вы храните отдельно от компьютера (на внешних носителях). Но нарушения в работе операционной системы, даже не будучи катастрофическими, могут потребовать продолжительного времени для восстановления работоспособности. Если ваша машина должна к определенному часу быть готовой для связи с пользователями, то такие нарушения могут не позволить выполнить эти обязанности. Для гарантированного обеспечения постоянной готовности компьютера к связи (задержка может быть 1—3 минуты) можно дублировать всю систему. Это позволит в системе 1 проводить эксперименты на совместимость, испытывать новые продукты, а система 2 будет всегда го-

това к работе в сети. Потребуется лишь перезагрузка для перехода в рабочую ОС. Все, что отработано и не может вызвать нарушений в работе компьютера, может переноситься в систему 2. Неполадки в системе 1 могут быть такими, что простейшим путем к их устранению будет "снос" системы и установка ее заново. Вторая система, как ни в чем не бывало, будет работать.

Установка двух операционных систем на одной машине может быть реализована следующими путями:

1. Установка ОС на два различных винчестера с выбором загружаемой системы с помощью менеджера загрузки или в BIOS Setup.
2. Установка ОС на разные логические диски с помощью менеджеров загрузки.
3. Установка ОС на один логический диск с ручным выбором загружаемой системы.

Третий вариант может пригодиться, когда винчестер один, размер его небольшой, система уже установлена и хорошо работает. Рассмотрим его подробно.

Для загрузки двух Windows 95/98 необходимо следующее:

1. Подготовьте файлы Autoexec.bat и Config.sys, которые будут использоваться во второй системе, и сохраните их на диске с именами, например Autoexec.sec и Config.sec.
2. Создайте BAT-файлы Winsec.Bat и Winprim.Bat.

Winsec.Bat

```
@ echo off
echo Смена Windows
choice /C:YN /T:N,7 Перейти во вторую ОС?
If ERRORLEVEL 2 goto exit
rename c:\windows winprim
rename c:\winsec windows
ren c:\autoexec.bat autoexec.pri
ren c:\config.sys config.pri
ren c:\autoexec.sec autoexec.bat
ren c:\config.sec config.sys
ren c:\logo.sys logo.pri
ren c:\logo.sec logo.sys
```

```
echo Перезагрузка
restart
:exit
```

Winprim.Bat

```
@ echo off
echo Смена Windows
choice /C:YN /T:N,7 Перейти в первую ОС?
If ERRORLEVEL 2 goto exit
rename c:\windows winsec
rename c:\winprim windows
ren c:\autoexec.bat autoexec.sec
ren c:\config.sys config.sec
ren c:\autoexec.pri autoexec.bat
ren c:\config.pri config.sys
ren c:\logo.sys logo.sec
ren c:\logo.pri logo.sys
echo Перезагрузка
restart
:exit
```

3. Из файла Ebd.cab — (C:\Windows\Command\Ebd\) — извлеките Restart.com и поместите его вместе с Winsec.Bat и Winprim.Bat в корневой каталог диска C:.
4. Для повышения наглядности процесса перехода скопируйте файл Logos.sys — (C:\Windows\) — в любое удобное место на диске, переименовав в Logo.bmp. С помощью графического редактора Paint отредактируйте файл: оформите изображение по своему вкусу и вставьте в него цифру 1. Сохраните Logo.bmp в корневом каталоге диска C: и переименуйте в Logo.sys. Замените в Logo.bmp цифру 1 на 2. Сохраните полученный файл в корневом каталоге и переименуйте в Logo.sec. Резервные копии этих файлов следует сохранить, поскольку при переустановке Windows они будут уничтожены.
5. Сделайте резервные копии всех полученных файлов.
6. Подготовьте дистрибутив с Windows 98.
7. Перезагрузите ПК в режиме командной строки.

8. Запустите файл Winsec.Bat.
9. Установите вторую ОС Windows 98 в каталог Windows при запуске файла Winprim.Bat, т. е. при переходе в первую систему каталог будет переименован в Winsec.

Теперь, перезагружая ПК в режиме **command prompt only**, с помощью команды `winsec` или `winprim` можно переходить из одной системы в другую. Такой вариант установки двух систем интересен тем, что применяется один загрузчик, не требуется Boot Manager, из одной системы всегда есть доступ к файлам другой для внесения исправлений и корректировки. Используются одни и те же файлы Io.sys, Msdos.sys, что позволяет применять одинаковые настройки системы при загрузке. Впрочем, при желании можно заменять и эти файлы, что позволит устанавливать две разные системы (Windows 95 и Windows 98), но наша задача — резервирование системы и обеспечение бесперебойной работы в сети.

Папка Program Files — общая для двух систем. Обычно это не мешает, но если есть подозрение, что какой-либо файл устанавливаемой программы может "не ужиться" со второй системой, следует устанавливать программу в другую папку. Такую возможность обычно оставляют пользователю производители программного обеспечения.

Этот метод установки второй системы позволяет сделать ее полной копией первой. При этом перезагрузка может потребоваться только в случае неполадок. Но следует регулярно обновлять вторую систему, приводя ее в соответствие с первой.

Компьютеры обычных пользователей сети тоже могут иметь более одной работоспособной операционной системы, переход между которыми обеспечен любым доступным методом. При внешней атаке на такую машину и даже повреждении ее системы вы сохраните возможность работы с компьютером и восстановления работоспособного соединения с сетью в удобное для вас время.

Резервирование файлов системы

Надо сказать, что операционные системы Windows 2000/XP/Vista имеют в своем составе средства для создания резервной копии системы и для восстановления после сбоев. Наиболее совершенна система резервирования в ОС Vista Ultimate.

Откройте из Панели управления окно **Центр архивации и восстановления**. В нем представлены следующие возможности резервирования:

1. Традиционное для Windows XP создание точки восстановления системы.
2. Создание архивных копий файлов и папок.
3. Создание архивного образа всего содержимого компьютера для восстановления в случае отказа оборудования.

   Заранее позаботившись о создании архивов файлов, папок или всей системы, вы можете быть уверенными в сохранности всех ваших данных и в возможности восстановления работоспособности компьютера при серьезных неполадках. Следует иметь в виду, что архивы не должны располагаться на том же диске, что и система. В случае выхода из строя винчестера, например, вы можете заменить его на новый, а из образа системы восстановить ее в работоспособное состояние. Для восстановления системы достаточно нажать клавишу <F8> при загрузке с установочного диска и выбрать соответствующий пункт меню.

ПРИМЕЧАНИЕ

Не следует экспериментировать с возможностями восстановления системы на рабочем винчестере. Все данные на диске будут уничтожены, он будет отформатирован.

Безопасность в Windows Vista

Современные операционные системы существенно стабильнее, чем Windows 98. Кроме того, есть возможность штатными средствами устанавливать несколько операционных систем на одну машину. Это позволит использовать особенности той или иной системы наилучшим образом. Системы безопасности современных операционных систем развивались очень активно от Windows 2000 до Windows Vista. Последняя вобрала в себя все лучшее от своих предшественниц, но есть в ней и совершенно новые для Windows решения.

Система безопасности Windows Vista позволяет надеяться, что при соблюдении элементарных требований вы сможете спокойно работать и не слишком задумываться о возможных атаках вирусов и хакеров на ваш компьютер.

Давайте рассмотрим средства, которые призваны обеспечить наше спокойствие за сохранность наших данных.

Центр обеспечения безопасности

В Панели управления не сложно найти значок **Центр обеспечения безопасности**.

Открыв этот апплет, вы увидите окно (рис. 5.16), из которого можно получить доступ к различным настройкам безопасности компьютера и получить информацию о замечаниях к состоянию системы безопасности. Например, если вы не установите антивирусный пакет (в состав Windows Vista антивирусные программы не входят), Центр обеспечения безопасности обратит ваше внимание на его отсутствие.

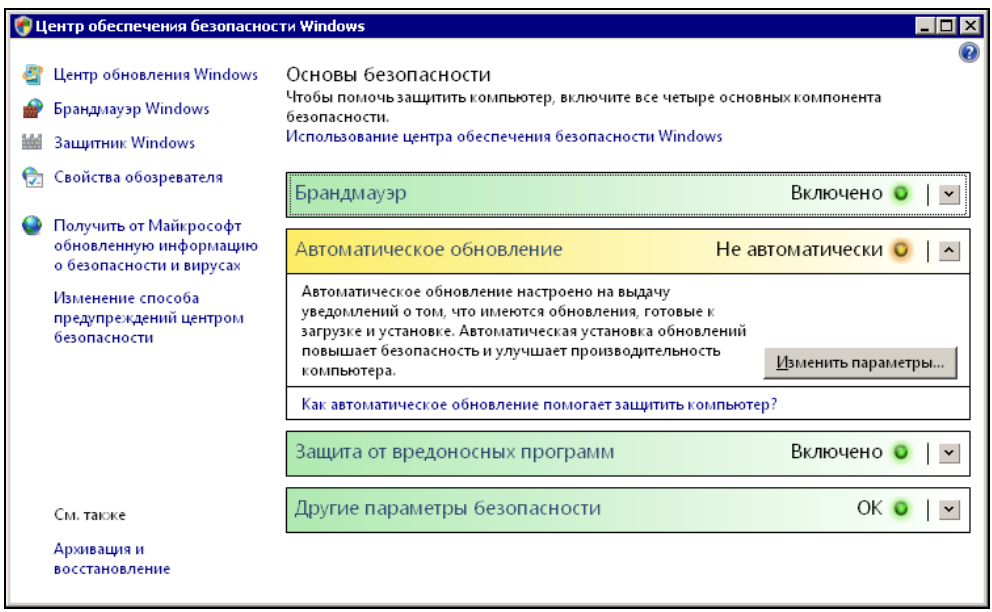


Рис. 5.16. Окно
Центр обеспечения безопасности Windows

Примечание

Если нет подключения к Интернету, можно прожить и без антивирусной программы, но при наличии высокоскоростного подключения к Интернету отсутствие антивирусной защиты может привести к катастрофе для вашего компьютера. Обязательно загрузите антивирусный пакет с сайта разработчика. Практически все разработчики таких программ предлагают бесплат-

ные версии на более или менее длительный срок. Воспользовавшись этим, вы можете выбрать со временем наиболее понравившуюся программу.

Конечно, если вы намеренно решили снизить защищенность вашего компьютера, вы можете избавить себя от предупреждений системы, выбрав в левой части окна **Изменение способа предупреждений центром безопасности**.

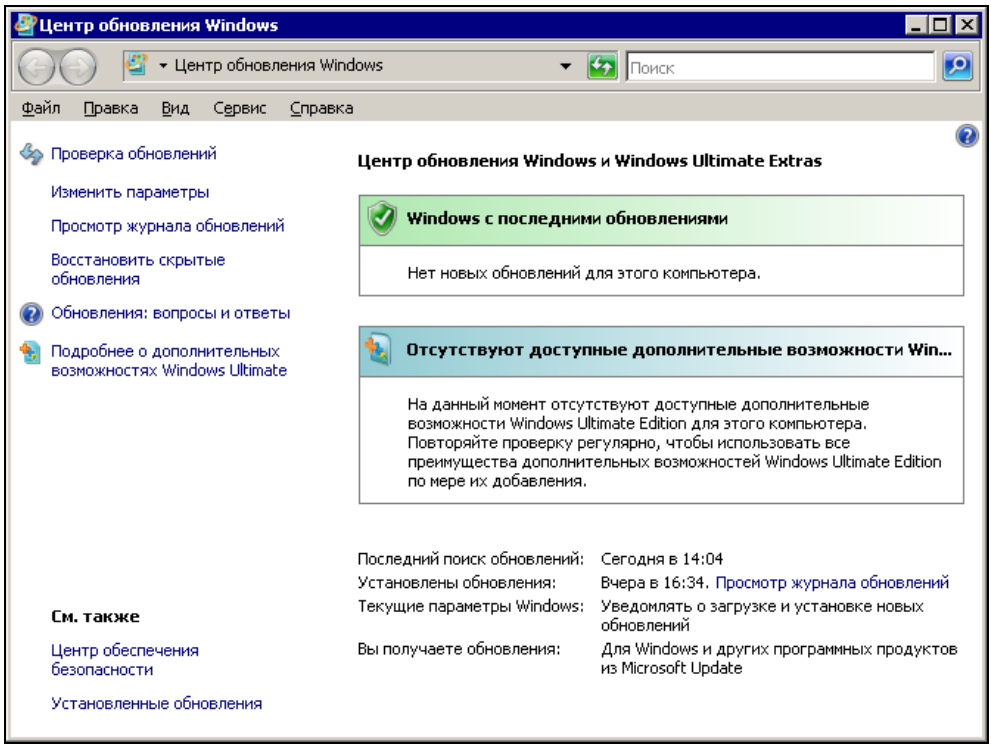


Рис. 5.17. Окно **Центр обновления Windows**

Но все же не стоит этого делать, если только вы не занимаетесь тестированием системы в незащищенном режиме, — "береженого Бог бережет". Если все ячейки с диагностическими сообщениями Центра обеспечения безопасности зеленого цвета, значит, все настройки в основном соответствуют современным требованиям к защите компьютера. Желтые предупреждения требуют обратить на себя внимание, но еще не сообщают о серьезных проблемах. Например, вместо автоматического обновления может быть настроена выдача

уведомлений о наличии обновлений. Это может иметь смысл при условии ограниченного трафика Интернета, доступного вам.

Для изменения режима автоматического обновления достаточно выбрать в левой части окна **Центра обеспечения безопасности** пункт **Центр обновления Windows**, после чего откроется одноименное окно (рис. 5.17).

В этом окне вы также увидите сообщения, говорящие о состоянии системы, наличии обновлений для нее. Конечно, сообщения о доступности обновлений возможны только при работающем подключении к Интернету.

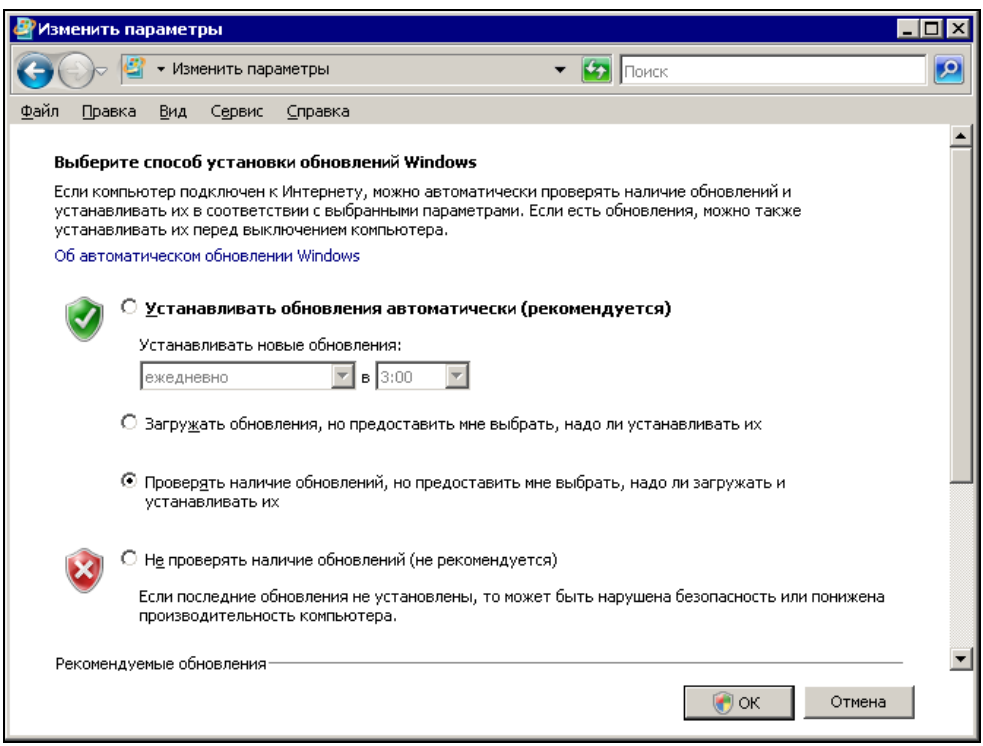


Рис. 5.18. Окно **Изменить параметры**

Выбрав в левой части этого окна пункт меню **Изменить параметры**, вы сможете в открывшемся одноименном окне (рис. 5.18) изменить режим получения обновлений или отказаться от них совсем.

Брандмауэр Windows

Работа в Интернете или в небезопасных сетях всегда сопряжена с риском проникновения на ваш компьютер вредоносных программ. Для того чтобы защитить компьютер от несанкционированного доступа к нему, в состав Windows Vista включено средство, которое закрывает доступ к компьютеру извне во всех случаях, кроме явно разрешенных пользователем. Брандмауэр настраивается системой автоматически при первом указании пользователем вида сети, в которую входит компьютер. В дальнейшем можно изменить настройки защиты.

Получить доступ к настройкам брандмауэра Windows можно, открыв из окна Центра обеспечения безопасности Windows окно **Брандмауэр Windows** (рис. 5.19), воспользовавшись соответствующим пунктом меню.

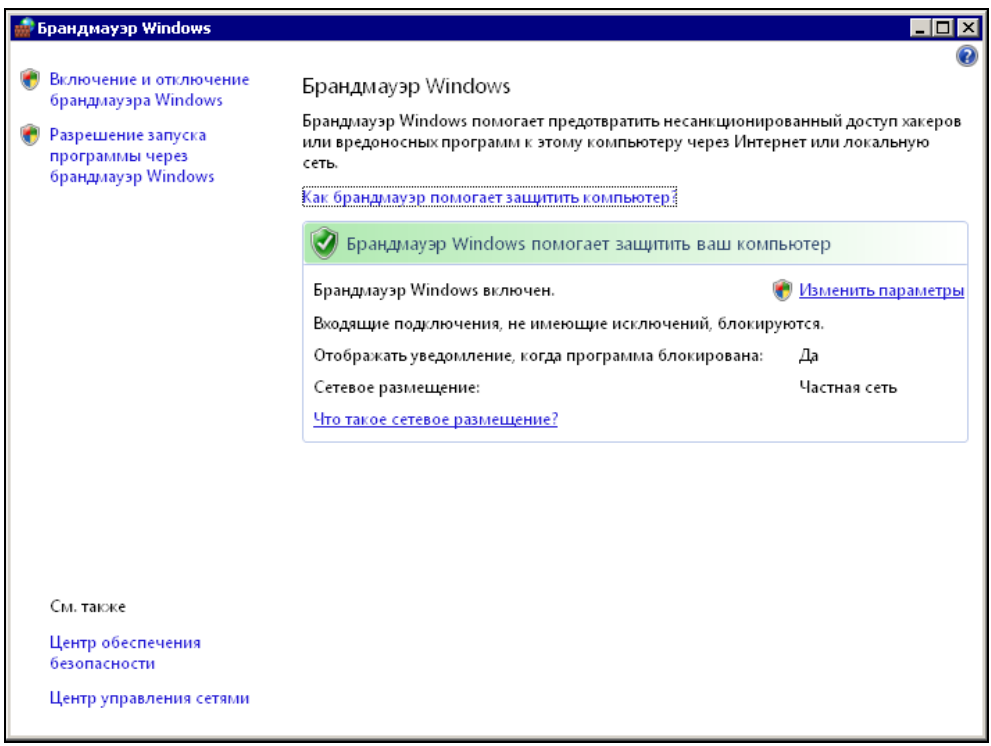


Рис. 5.19. Окно **Брандмауэр Windows**

Воспользовавшись ссылкой **Изменить параметры**, имеющейся в этом окне, можно открыть окно **Параметры брандмауэра Windows** (рис. 5.20), которое имеет три вкладки, на каждой из которых можно выполнить определенные настройки.

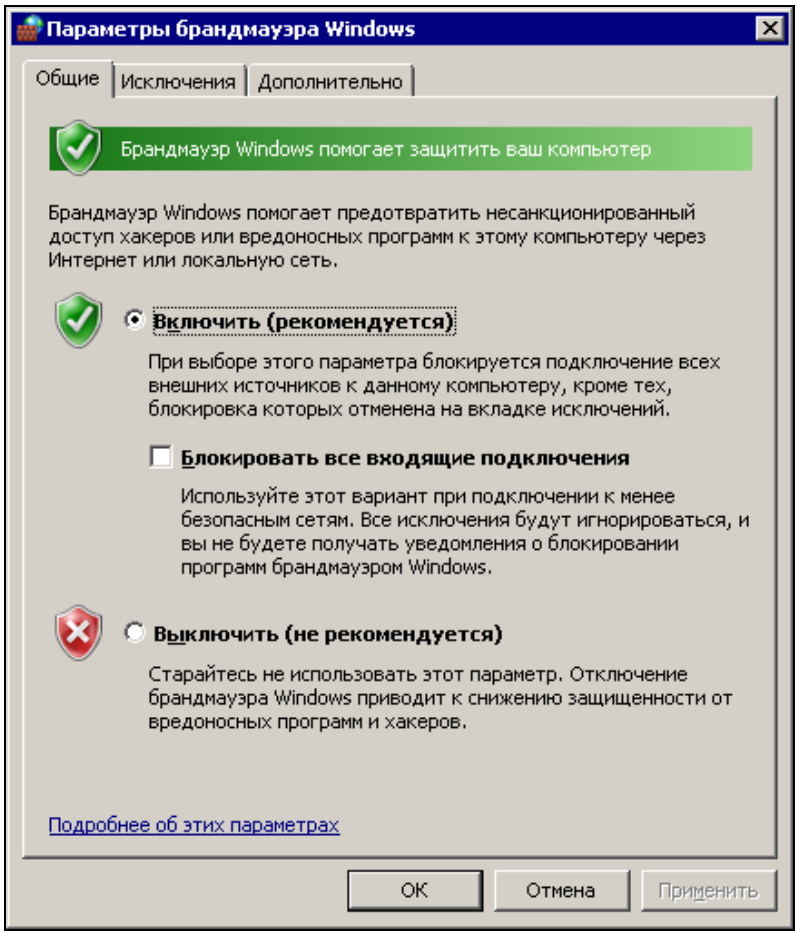


Рис. 5.20. Окно **Параметры брандмауэра Windows**, вкладка **Общие**

Так, на вкладке **Общие** можно выключить брандмауэр Windows или включить, выбрать режим **Блокировать все входящие подключения**, который может быть полезен при работе в неизвестных вам и небезопасных сетях.

На вкладке **Дополнительно** (рис. 5.21) можно указать те сетевые подключения, которые должны быть защищены брандмауэром. Вполне возможно, что одно из подключений используется вами для связи со вторым своим компьютером. Защищать себя от себя вам, возможно, не потребуется.

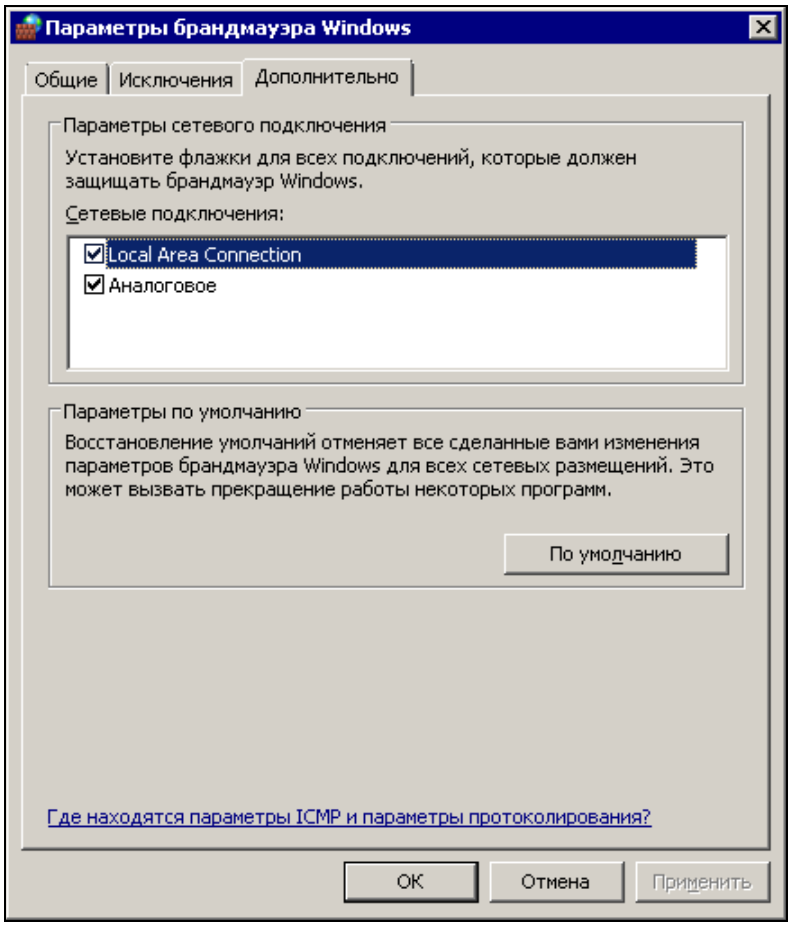


Рис. 5.21. Окно **Параметры брандмауэра Windows**, вкладка **Дополнительно**

На вкладке **Исключения** (рис. 5.22) можно указать программы или отдельные порты, к которым необходимо обеспечить беспрепятственный доступ из сети или Интернета. Автор использует, например, удаленный доступ к рабочему столу своего компьютера. Конечно, **Дистанционное управление рабо-**

чим столом должно быть исключено из числа блокируемых внешних обращений к компьютеру.

Исключения вы можете добавлять самостоятельно, указав, например, порт, используемый программой (рис. 5.23). Но исходя из соображений безопасности, вы можете ограничить число компьютеров, с которых будет возможен доступ к этому порту, указав конкретные значения разрешенных IP-адресов, воспользовавшись кнопкой **Изменить область**. Можно, конечно, разрешить доступ для всех или для определенной сети (рис. 5.24).

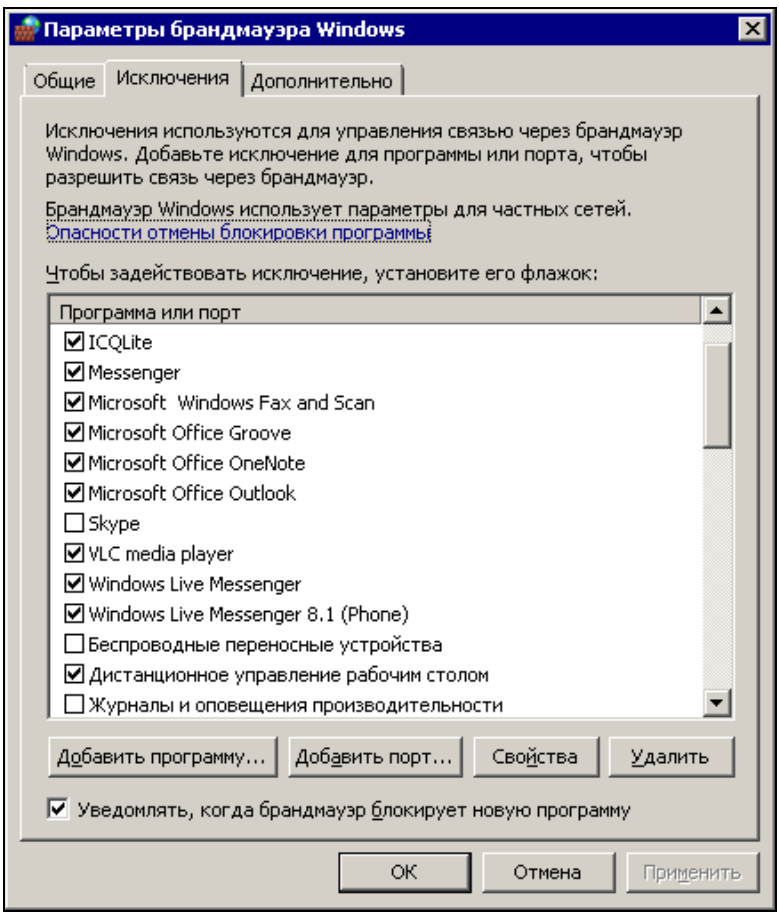


Рис. 5.22. Окно **Параметры брандмауэра Windows**, вкладка **Исключения**

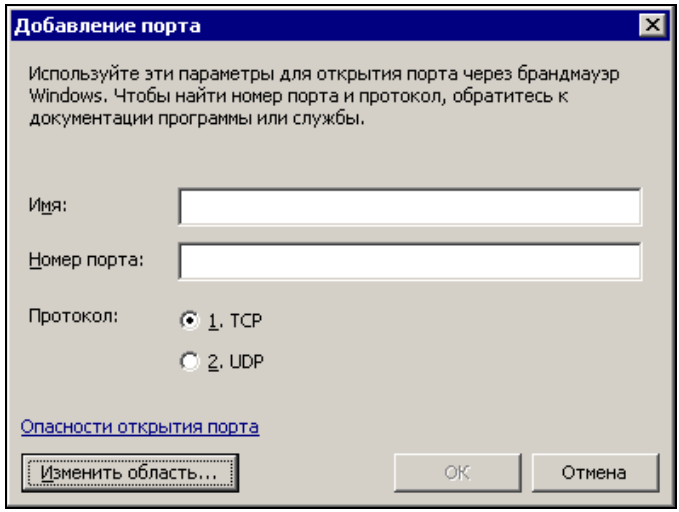


Рис. 5.23. Окно **Добавление порта**

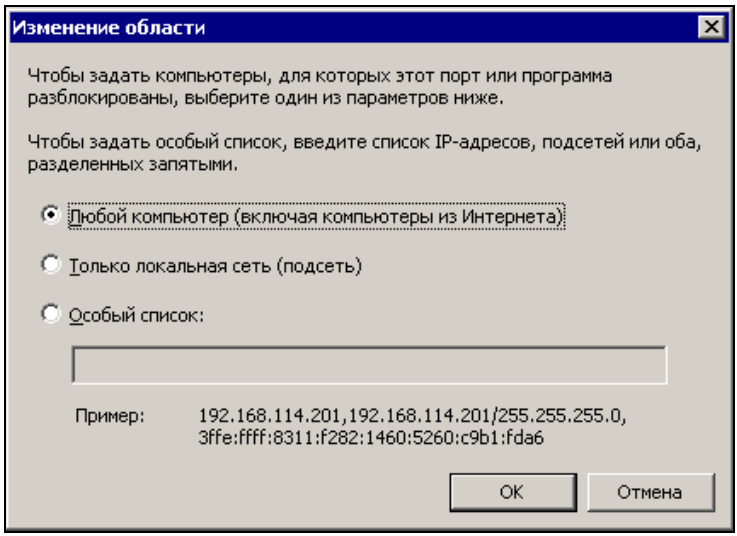


Рис. 5.24. Окно **Изменение области**

Защитник Windows

Это еще одно средство защиты вашего компьютера, которое предназначено для обнаружения вредоносных программ.

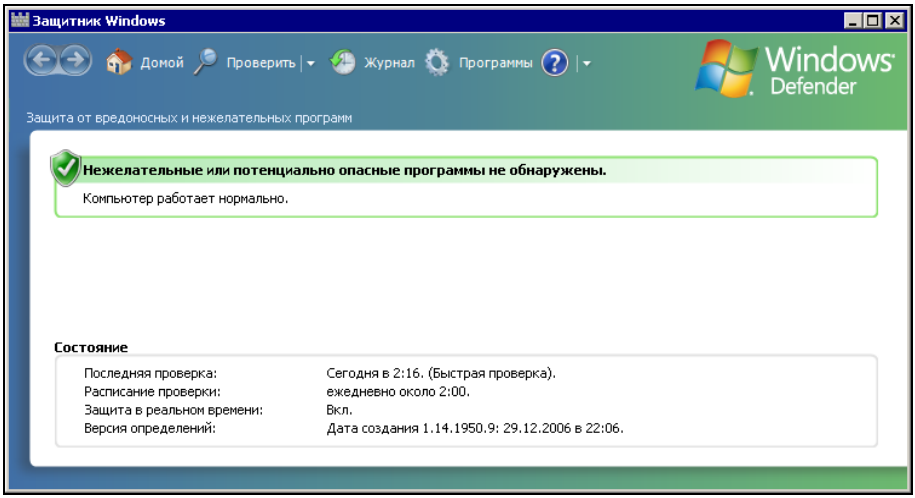


Рис. 5.25. Окно **Защитник Windows**

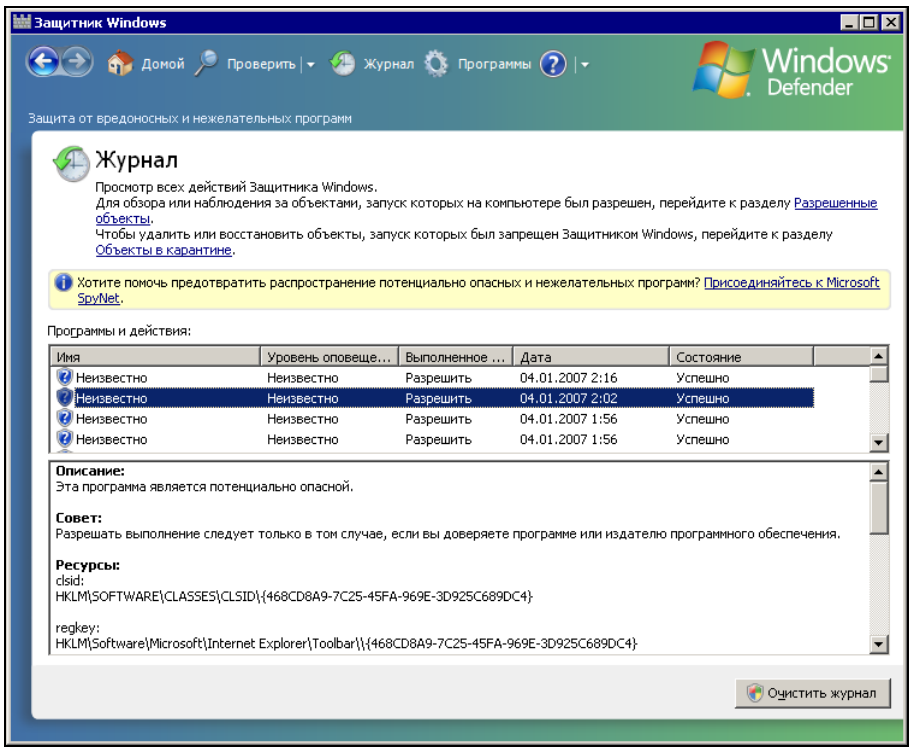


Рис. 5.26. Окно **Защитник Windows**, вкладка **Журнал**

Открыть его окно (рис. 5.25) вы можете также из окна **Центр обеспечения безопасности Windows**. Защитник Windows (Windows Defender) работает почти незаметно для пользователя, до тех пор пока не появится подозрительная программа. В этом случае защитник спросит о дальнейших действиях. Если вы уверены, что эта программа запущена вами сознательно и не представляет угрозы для компьютера, вы дадите согласие на ее запуск.

Информацию обо всех действиях программы можно посмотреть в Журнале (рис. 5.26), который ведет программа.

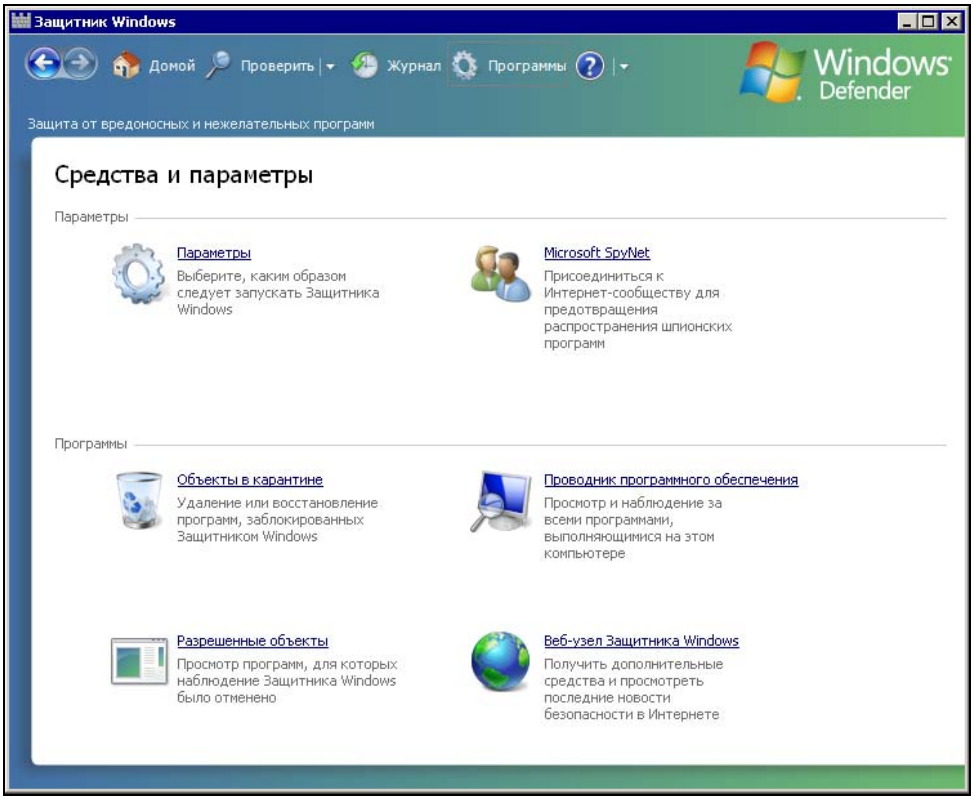


Рис. 5.27. Окно **Защитник Windows**, вкладка **Средства и параметры**

Как и другие средства защиты компьютера, Защитник Windows можно настраивать по своему усмотрению (рис. 5.27), выбрав в меню его окна **Программы**. При этом откроется страница, где можно выбрать средства управ-

ления Защитником. При выборе меню **Параметры** возможны достаточно тонкие настройки программы (рис. 5.28).

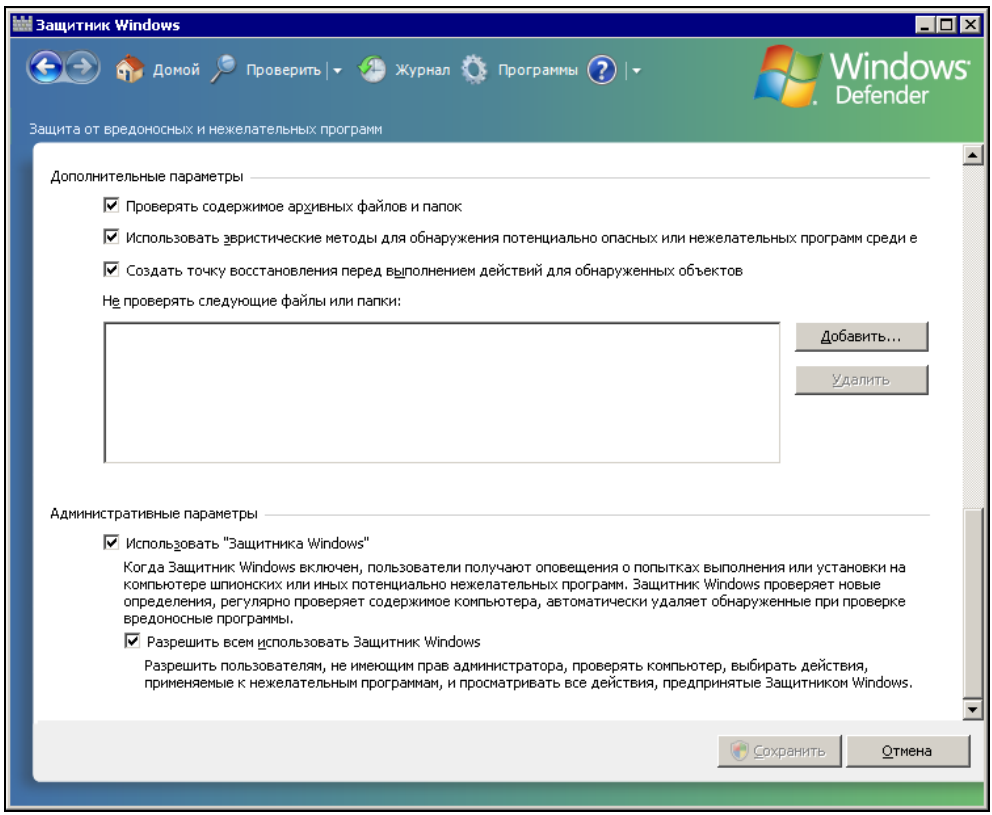


Рис. 5.28. Окно **Защитник Windows**, вкладка **Дополнительные параметры**

В этом окне вы можете запретить проверять отдельные файлы или папки, можете вообще запретить использование Защитника Windows или запретить использование программы пользователям, не обладающим административными полномочиями.

Свойства обозревателя

Это тоже один из пунктов меню в окне **Центр обеспечения безопасности Windows**. Значительная часть информации попадает на ваш компьютер

именно из Интернета. Поэтому защита браузера Internet Explorer, обеспечение безопасного перемещения по Интернету имеют не меньшее значение, чем защита от вредоносных программ. Web-страницы могут содержать программный код, который, будучи выполнен на вашем компьютере, может привести к различным неприятным последствиям. Фильтр фишинга, встроенный в Internet Explorer, позволяет распознать поддельные сайты. Но не только поддельный сайт может быть опасен.

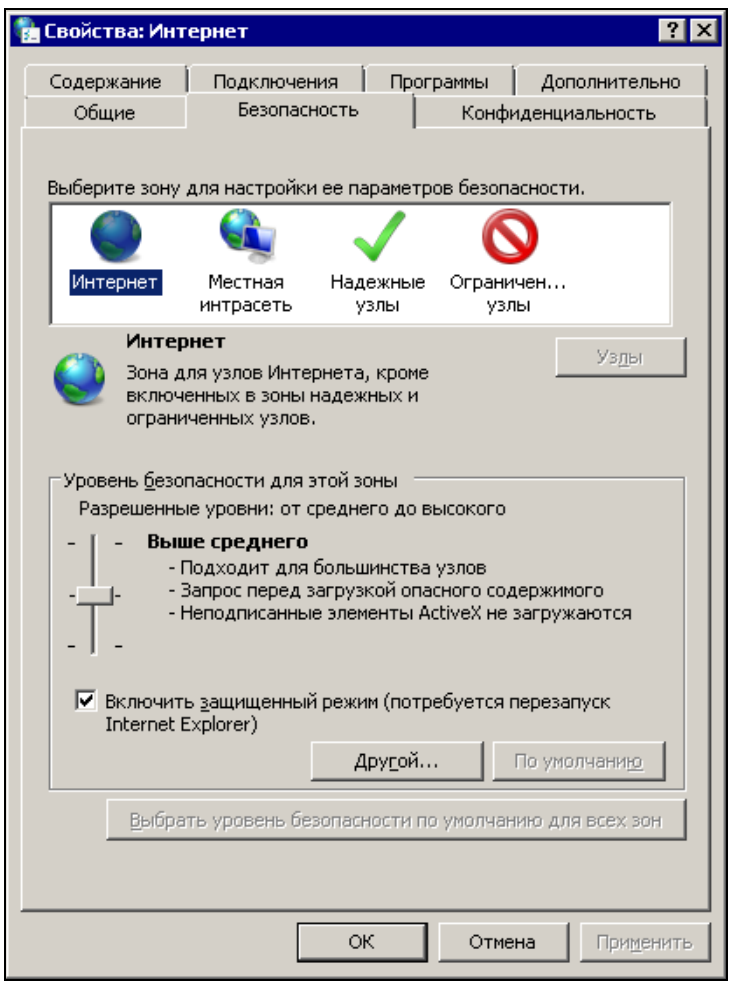


Рис. 5.29. Окно **Свойства: Интернет**, вкладка **Безопасность**

Открыв окно свойств обозревателя (рис. 5.29), вы можете настроить Internet Explorer наиболее оптимальным для вас образом. Безопасность прогулок по Интернету, и в то же время их комфортность, можно существенно повысить, распределив посещаемые узлы по зонам безопасности. Если вы сами поддерживаете какой-либо сайт, естественно его поместить в зону надежных узлов вместе с другими доверенными узлами. Потенциально опасные адреса могут быть отнесены к зоне ограниченных узлов.

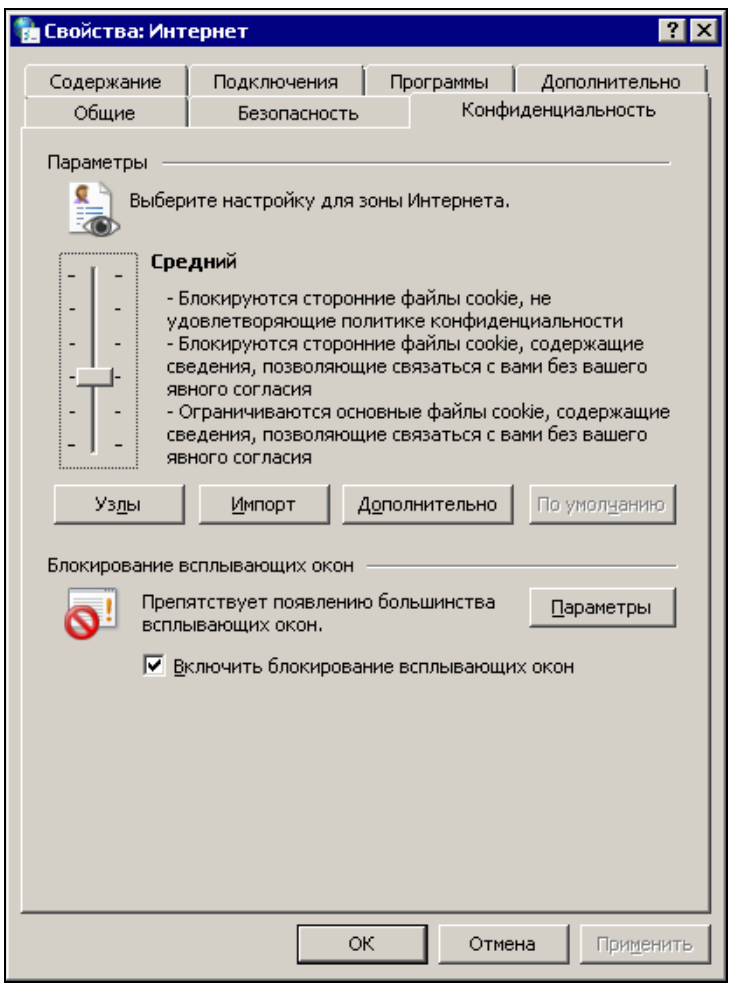


Рис. 5.30. Окно **Свойства: Интернет**, вкладка **Конфиденциальность**

Даже вполне благонадежные узлы в Интернете собирают определенную информацию о своих посетителях. Она бывает необходима для сохранения статистики посещений сайта, определения контингента пользователей, посещающих сайт, для формирования интерфейса сайта по вашему желанию и в ряде других вполне законных случаев. Возможно, что вы не хотите, чтобы информация о вас попала на какой-либо сайт. Несмотря на то что в большинстве случаев это совершенно безопасно, вы имеете право не давать о себе никаких сведений. На вкладке **Конфиденциальность** (рис. 5.30) вы можете настроить уровень конфиденциальности для различных узлов Интернета. Пояснения, которые показываются при изменении настроек, вполне достаточны, чтобы сознательно установить необходимые вам настройки.

Настройки для опытных

Не все, что касается безопасности вашего компьютера, может быть настроено из Центра обеспечения безопасности.

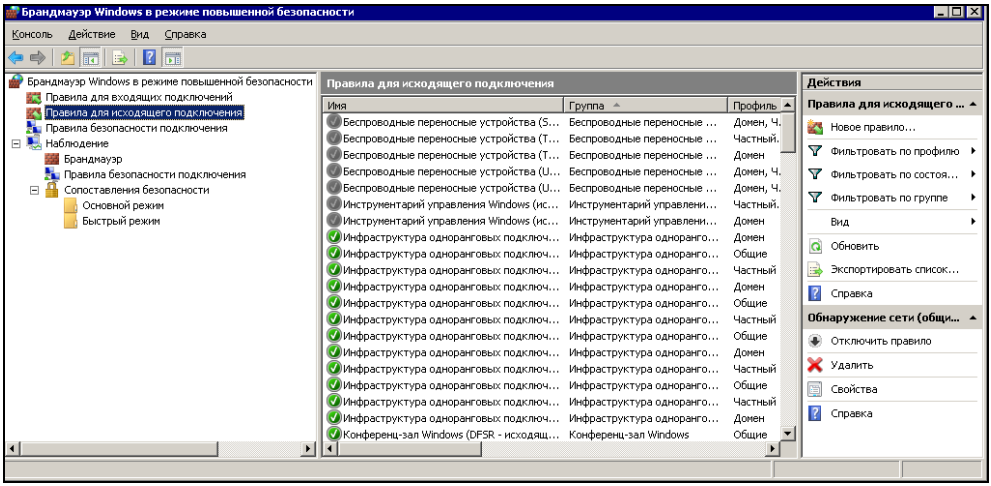


Рис. 5.31. Окно **Брандмауэр Windows в режиме повышенной безопасности**

Опытные пользователи, являющиеся администраторами своих компьютеров, могут настроить параметры безопасности более точно. До сих пор, когда мы настраивали брандмауэр, разговор шел о входящих подключениях. Но представьте себе, что какая-либо программа попала на ваш компьютер легальным

путем, не была опознана системой защиты, как неблагонадежная, а в один прекрасный момент начала передавать сведения о вашем компьютере, подключившись по известному ей адресу в Интернете. Такими свойствами наделены многие бесплатные программы, которые должны в качестве компенсации своей бесплатности показывать вам рекламу, причем соответствующую вашим интересам.

Не пугайтесь. Это не шпионаж, но в отдельных случаях и это может не устраивать пользователя компьютера. Для защиты от действий подобных программ следует более тонко настроить брандмауэр Windows. Для этого откройте **Пуск | Администрирование | Брандмауэр Windows в режиме повышенной безопасности** (рис. 5.31).

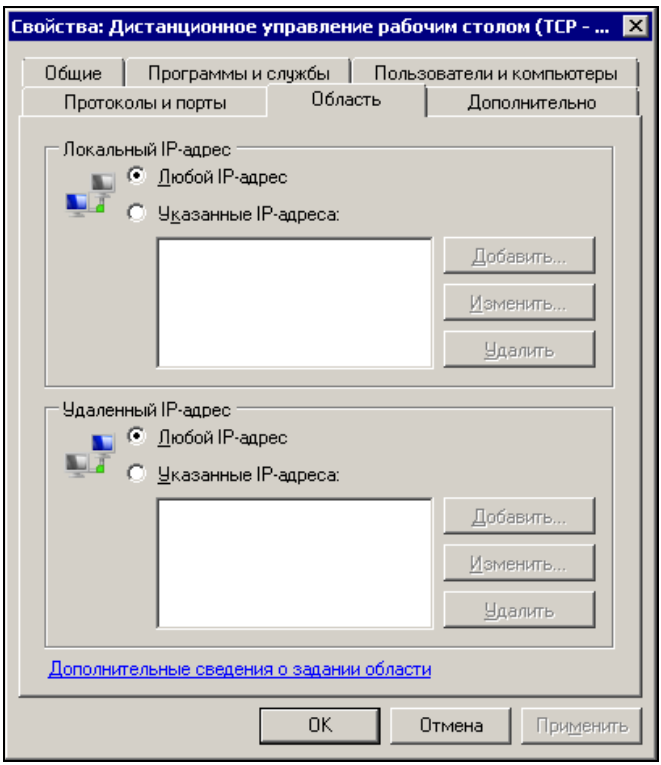


Рис. 5.32. Окно **Свойства: Дистанционное управление рабочим столом**

Выберите **Правила для исходящего подключения** и выберите необходимое для настройки. Если в перечне правил еще нет требуемого, вы самостоятель-

но можете создать новое правило. Конечно, такие настройки требуют более глубокого понимания процессов, идущих в компьютере. Но "не боги горшки обжигают". Имея желание, вы всегда разберетесь и в более потаенных настройках системы.

Ограничения для входящих и исходящих подключений можно установить и по IP-адресам компьютеров (рис. 5.32). Обратите внимание, что используя тонкие настройки безопасности, мы можем ограничить возможность подключения к нашему компьютеру, если он имеет определенный IP-адрес или диапазон адресов. Для другого диапазона, наоборот, разрешить. Зачем, спросите вы? Все очень просто.

Автор, например, пользуется ноутбуком, который получает свой IP-адрес в каждой из сетей, где ему приходится работать. Так вот, доступ к нему возможен только в домашней сети, в которой он всегда получает один и тот же IP-адрес. Возможны и другие ситуации, обнаружив которые вы увидите полезность настроек брандмауэра Windows в режиме повышенной безопасности.

Управление учетными записями

Это окно (рис. 5.33) найти очень просто. В правой части меню **Пуск** находите **Компьютер** и в контекстном меню выбираете **Управление**.

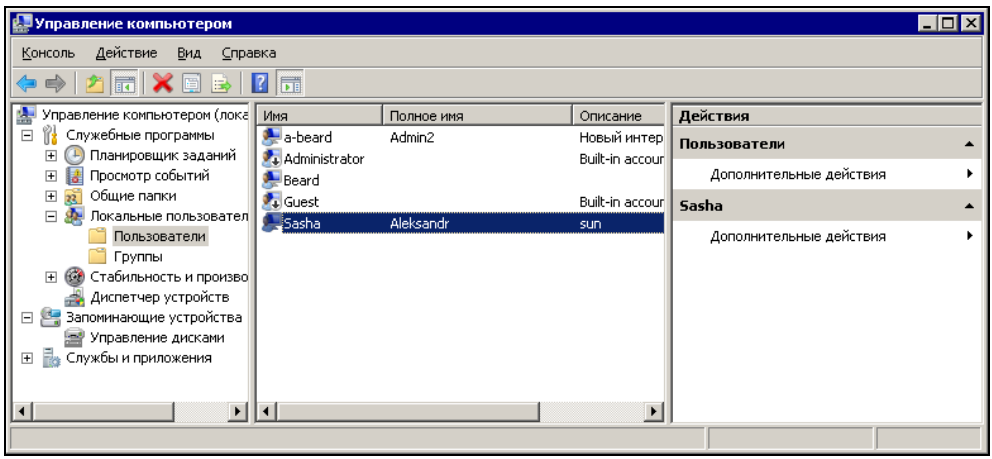


Рис. 5.33. Окно **Управление компьютером**

Оно вам может пригодиться во многих случаях, когда требуется работа с системой в качестве администратора. Доступ к элементам системы, представленным в этом окне, возможен и другими путями, но окно **Управление компьютером** содержит набор объектов, действительно достаточный для управления компьютером.

Завершая короткий обзор настроек безопасности системы, обратим внимание на узел **Локальные пользователи | Пользователи** в левой части окна. Выбрав его, вы увидите в средней части окна все учетные записи локальных пользователей. Безопасность компьютера определяется не только внешними причинами, но и просто случайными или неумелыми действиями пользователя, имеющего слишком высокие права в системе. Откройте окно свойств (рис. 5.34) учетной записи, для которой вы хотели бы ограничить права.

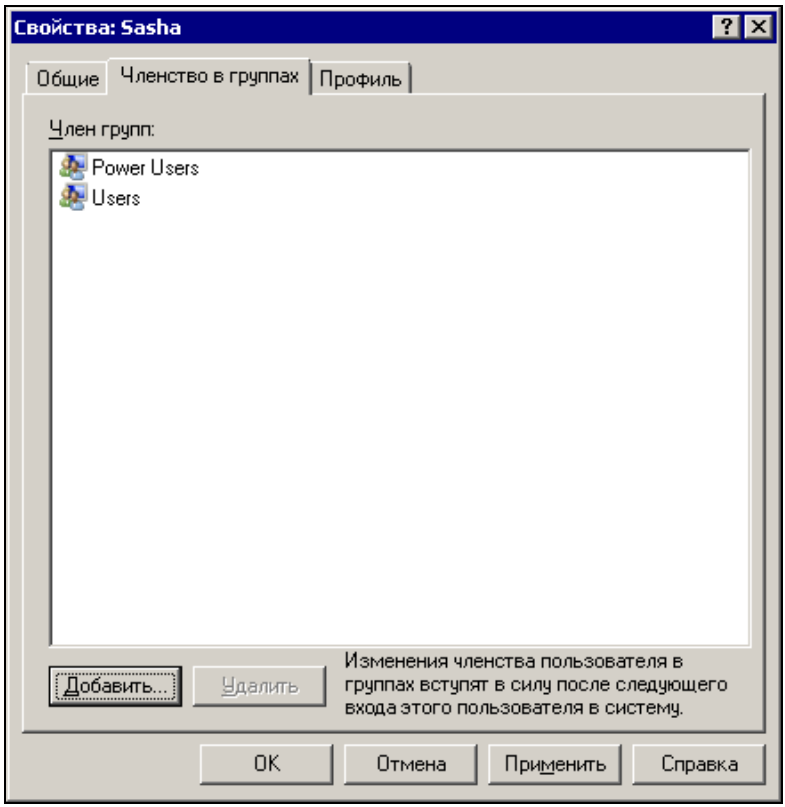


Рис. 5.34. Окно **Свойства: <Имя_учетной_записи>**

В большинстве случаев достаточно вывести учетную запись из группы администраторов, чтобы обезопасить компьютер от неквалифицированных действий пользователя. В то же время, если случился редкий момент, когда потребовались права администратора компьютера при работе в сеансе этой учетной записи, вы можете ввести пароль администратора, который будет запрошен системой при попытке выполнить критичные для состояния системы действия. Это действует Контроль учетных записей пользователей (UAC), функция Windows, позволяющая предотвратить несанкционированные изменения в компьютере. UAC обеспечивает защиту, запрашивая разрешение или пароль администратора перед совершением потенциально опасных для компьютера действий или при изменении параметров, которые могут оказать влияние на работу других пользователей. Появившееся UAC-сообщение следует внимательно прочитать, проконтролировать, соответствует ли название выполняемого действия (программы) тому, которое действительно производится (запускается).

Командная строка и программа NETSTAT

Операционная система содержит множество средств, которые не видны обычному пользователю. Нет к ним доступа из меню **Пуск** или из Панели управления. Но они есть, и их применение может принести очень большую пользу. Это относится ко всем ОС семейства Windows и еще более к Linux.

Рассмотрим некоторые возможности анализа безопасности вашего компьютера с ОС Windows Vista. С небольшими коррективами метод может быть использован во всех операционных системах.

Введите в поле поиска над кнопкой **Пуск** символы `cmd`. В открывшемся окне командной строки введите `help`. Вы увидите окно, показанное на рис. 5.35.

В окне командной строки вы видите все команды, которые можно выполнить в нем. Конечно, можно и запускать обычные приложения, но они будут открываться в своих окнах. Командная строка — это текстовый интерфейс операционной системы. С ним вы можете встретиться и при решении проблем с работоспособностью системы, когда при загрузке системы по нажатию клавиши <F8> выберете режим командной строки.

Но у нас система в рабочем состоянии, и командную строку мы можем использовать как удобный интерфейс для выполнения различных задач по обслуживанию системы.

Каждая команда из списка, выведенного по команде `help`, имеет свою справку по ее использованию. Обычно для вывода справки достаточно ввести имя команды и параметр `/?`.

Описание всех команд заняло бы много места, да и нет смысла описывать то, что легко можно увидеть на экране, вызывая справку по команде. Мы рассмотрим один пример использования командной строки для выяснения некоторых сетевых проблем.

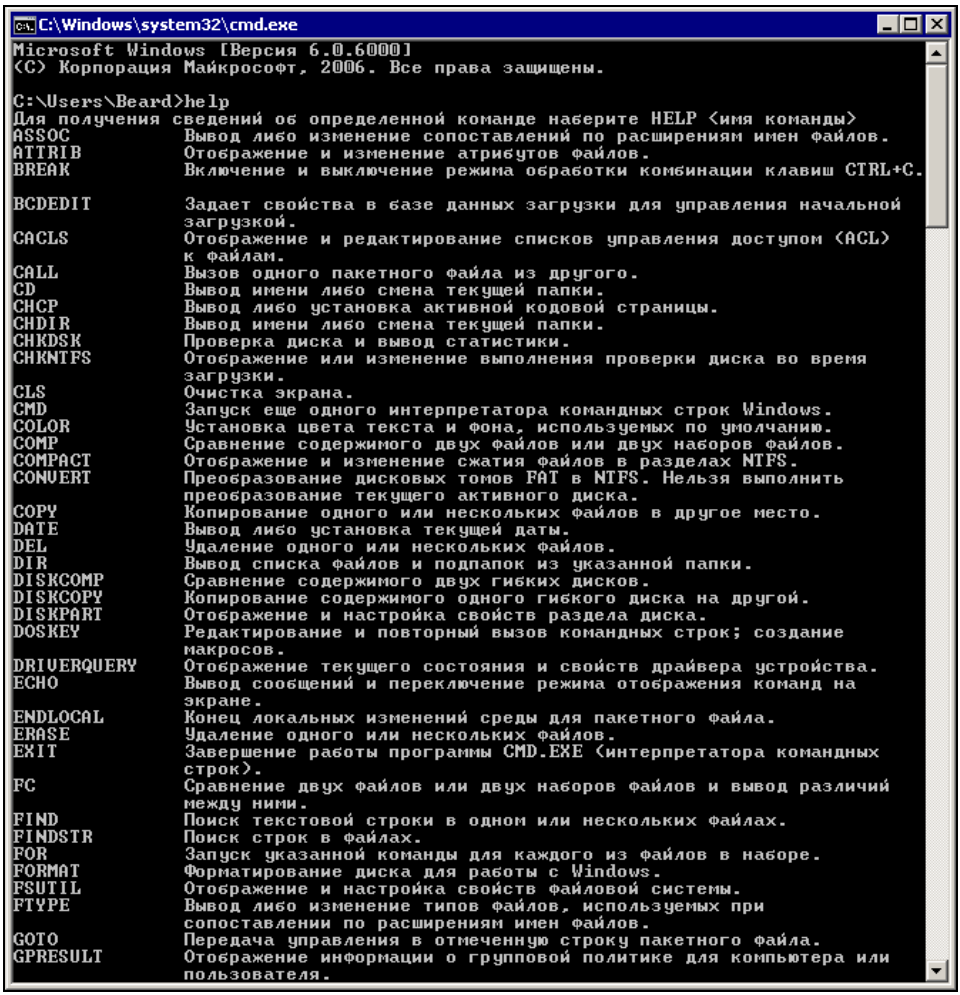


Рис. 5.35. Окно командной строки

В составе системы есть программы, которые не имеют оконного интерфейса, а предназначены для работы в окне командной строки. Постепенно, интересуясь вопросами администрирования системы, вы узнаете о многих подобных программах. А сейчас рассмотрим программу NETSTAT. Одна из возможностей, которую предоставляет эта команда, — выявление источников трафика Интернета. Увидеть наличие трафика не сложно. Посмотрев на окно **Состояние** сетевого подключения (для этого следует открыть **Центр управления сетями и общим доступом | Управление сетевыми подключениями** и выбрать в контекстном меню действующего подключения к Интернету пункт **Состояние**), вы увидите изменяющиеся числа **Отправлено** и **Принято**. Но определить источник трафика, узнать какая программа его генерирует, если трафик исходящий, таким путем не удастся. Попробуем узнать подробности о существующих источниках трафика, определим их лояльность к нашей системе.

В окне командной строки введите команду `CLS` для очистки экрана, а затем команду `NETSTAT -n`, где "–n" — параметр, который заставляет программу показывать IP-адреса, а не имена узлов, к которым подключается наш компьютер.

На экране вы увидите результат выполнения этих команд (рис. 5.36).

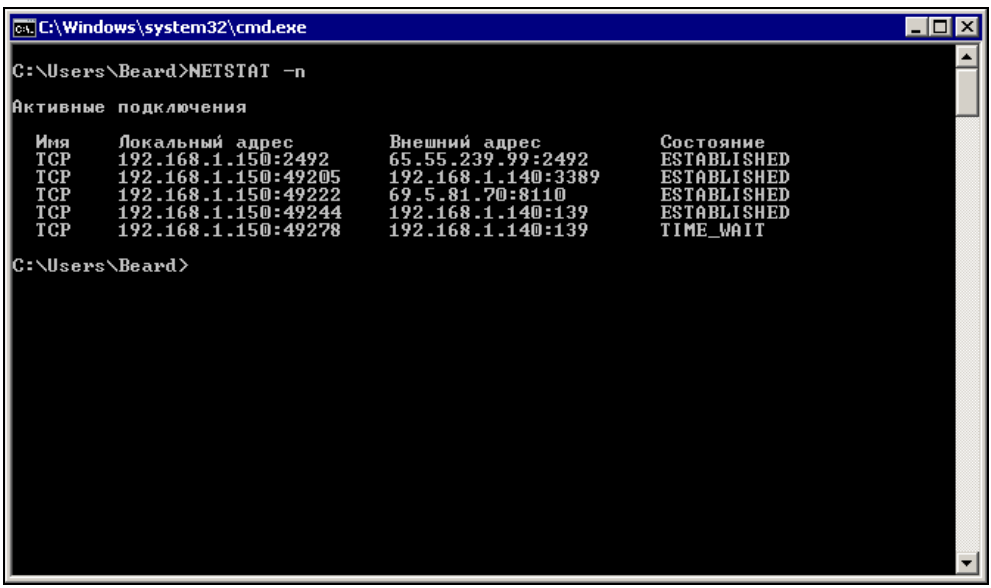


Рис. 5.36. Результат выполнения команды `NETSTAT -n`

У вас в этом окне будет другая информация, но мы проанализируем сетевую активность компьютера автора (интересно подсмотреть, чем это там автор занимается в своей сети).

Сначала отметим известные адреса. 192.168.1.150 — это IP-адрес самого компьютера в домашней сети. Рядом с адресом номера портов, которые система использует в данный момент. Переходим к внешним адресам (снизу вверх).

192.168.1.140:139 — адрес ноутбука, включенного в сеть и порт, который используется при обмене файлами. TIME_WAIT — говорит об ожидании активности. То есть в настоящее время обмен файлами не происходит. Этот сетевой процесс нам известен и нужен, переходим к следующему.

192.168.1.140:139 — тот же адрес и тот же порт, но в рабочем состоянии. ESTABLISHED — значит, подключен. Открыта доступная по сети папка, с которой можно будет обменяться файлами. Тоже все ясно.

69.5.81.70:8110 — адрес и порт интернет-радиостанции. ESTABLISHED — автор слушает радио.

192.168.1.140:3389 — снова адрес ноутбука, но используется порт удаленного рабочего стола. ESTABLISHED — открыт сеанс работы с удаленным рабочим столом. Тоже понятно. Автор часто использует возможность работы сразу на двух компьютерах.

65.55.239.99:2492…. А вот и неизвестное активное подключение. Чем оно вызвано? Какая программа его использует? Проведем следствие, а поможет нам Интернет.

Следствие

Откроем Internet Explorer и введем в строку адреса **http://www.nic.ru/whois/**. Это один из ресурсов в Интернете, который позволяет определить принадлежность IP-адреса. В открывшейся форме в поле для ввода IP-адреса вводим тот, что мы обнаружили и в результате видим страницу, показанную на рис. 5.37.

Внимательно читаем полученные данные:

- наименование организации (OrgName) — Microsoft Corp (Корпорация Microsoft);
- город (City) — Redmond.

Как вы, наверное, уже поняли, компьютер зачем-то связан с одним из серверов корпорации Microsoft.

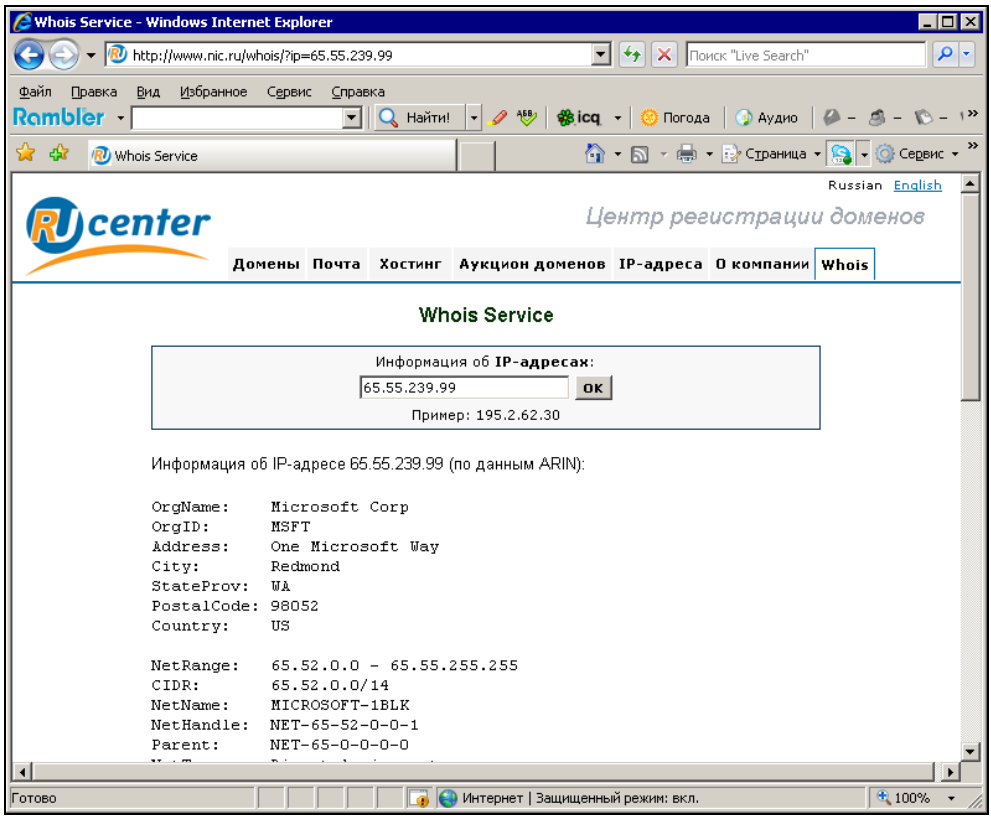


Рис. 5.37. Окно **Whois Service — Windows Internet Explorer**

Попытаемся определить, зачем он установил этот контакт. Проведя поиск в Интернете относительно применения порта 2492, удалось найти такую информацию на странице **http://www.pimswiki.org/index.php?title=PIMS_Software_-_Network_Port_Requirements/Recommendations**.

Страница на английском языке, в ней есть следующая информация: Port 2492 is the port used by Groove's native Simple Symmetrical Transfer Protocol (SSTP).

Port 2492 — порт, используемый в Groove's native Simple Symmetrical Transfer Protocol (SSTP).

Groove — это целая система приложений и протоколов. Основная функция Groove состоит в синхронизации двух или более ПК по Интернету. Система используется в новой версии Microsoft Office 2007, которая установлена у автора, а взаимодействие компьютеров в системе поддерживается сервером, принадлежащим Microsoft.

Вот и разгадка. Не вдаваясь в подробности, приведу окно Диспетчера взаимодействия, который запущен на компьютере (рис. 5.38).

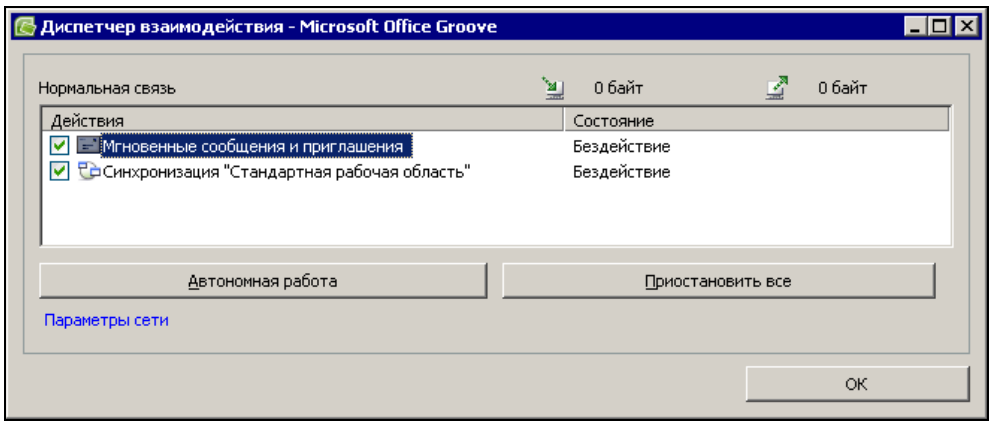


Рис. 5.38. Окно **Диспетчер взаимодействия — Microsoft Office Groove**

Вот и все. Никаких шпионских программ.

И снова NETSTAT

Программа NETSTAT с параметром `-b` должна отобразить не только адреса, но и файлы, которые принимают участие в подключениях. Но если вы попытаетесь выполнить такую команду, то увидите результат, показанный на рис. 5.39.

Что за повышение требует эта операция? Все просто. Операция требует повышенных прав пользователя. Обычные программы выдают запрос на повышение прав при необходимости выполнить критичную для системы операцию. Командная строка запросы не выдает, но предупреждает, что требуются повышенные права.

Как их повысить, если мы и так работаем с правами администратора? Все просто. Выключите контроль учетных записей, пройдя по следующему пути: **Панель управления | Учетные записи пользователей | Включение или отключение контроля учетных записей (UAC)**. После выключения контроля учетных записей перезагрузите компьютер.

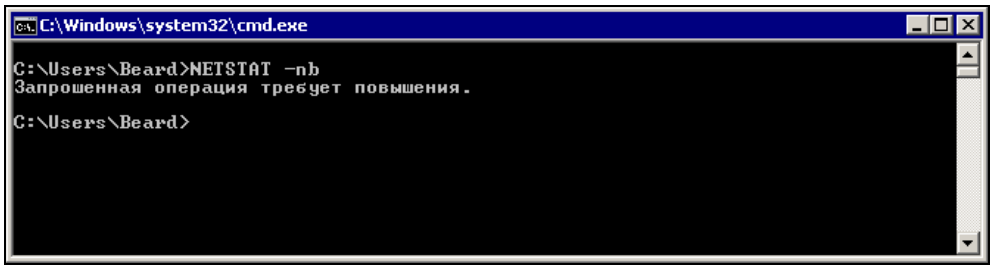


Рис. 5.39. Результат выполнения команды `NETSTAT -nb`

> ***ПРИМЕЧАНИЕ***
>
> После завершения работ, требующих повышенных прав, снова включите контроль учетных записей. Безопасность компьютера — момент очень важный.

Теперь можно снова выполнить `NETSTAT -nb`.

```
  TCP    192.168.1.150:2492     65.55.239.99:2492      ESTABLISHED
[GROOVE.EXE]
  TCP    192.168.1.150:49164    192.168.1.140:3389     ESTABLISHED
[mstsc.exe]
  TCP    192.168.1.150:49170    69.5.81.70:8110        ESTABLISHED
[wmplayer.exe]
```

В строках, выведенных на экран программой NETSTAT, теперь можно прочитать имена файлов, которые установили подключения:

- wmplayer.exe — Проигрыватель Windows Media, через который прослушивается интернет-радио;
- mstsc.exe — Клиент терминального доступа, через который выполнено подключение к ноутбуку;
- GROOVE.EXE — программа, которую мы искали.

Мы завершили анализ сетевой активности нашего компьютера, применив средства командной строки.

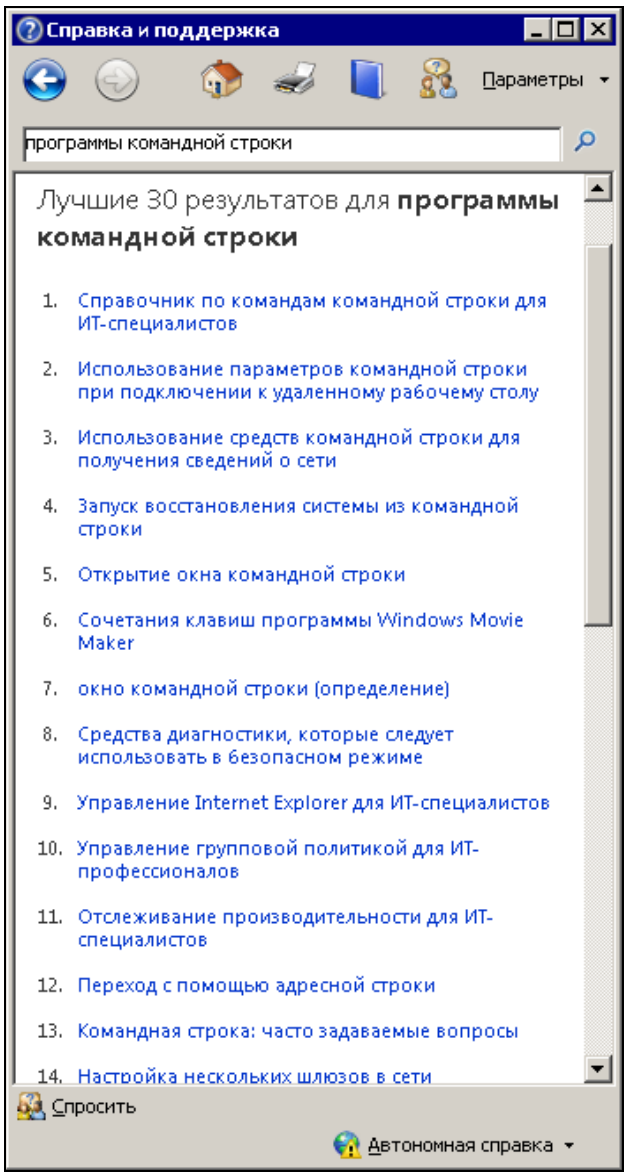


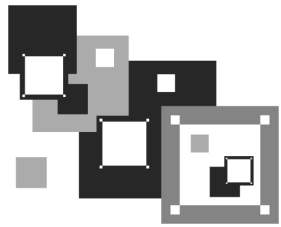
Рис. 5.40. Окно **Справка и поддержка**

Существуют специализированные программы, имеющие графический интерфейс, с помощью которых можно провести подобный анализ. Но помните рекламу "Зачем платить больше?".

И дело не только в деньгах. Хорошее знание операционной системы не требует применения дополнительных программ, которые создают дополнительную нагрузку на систему, могут вызвать проблемы несовместимости с другими программами, но сами практически используют сведения, которые дает им система. Мы и сами можем увидеть эти сведения.

Введите в окне справочной системы Windows три слова: `программы командной строки`. Вы получите несколько десятков ссылок (рис. 5.40). Прочитав доступную по ссылкам информацию, вы узнаете почти все о возможностях командной строки и программах, которые можно выполнять в ней.

ГЛАВА 6



Виртуальные технологии

Что это такое и зачем оно нам? Давайте рассмотрим возможности, которые могут нам дать эти технологии. Дело в том, что современные компьютеры обладают зачастую такими запасами быстродействия и оперативной памяти, что их мощности могло бы хватить на несколько одновременно работающих компьютеров. Виртуальные технологии позволяют запустить в одном физическом компьютере несколько виртуальных, которые по своим свойствам практически не отличаются от реальных. Это могут быть как рабочие станции, так и серверы.

Представляет интерес и то, что сами сети могут быть виртуальными. Но давайте обо всем по порядку.

Устанавливаем виртуальный сервер

Попробуем перечислить преимущества, которые можно получить, используя виртуальную машину для сервера.

1. Возможность моментального восстановления сервера в рабочее состояние после вирусной атаки, атаки хакеров; другой причины, приведшей к серьезным проблемам на сервере. Эта возможность достигается всего лишь копированием рабочего файла диска виртуальной машины и заменой испорченного на исправную копию при необходимости.
2. Возможность размещения на одном физическом сервере более одного виртуального сервера. Это могут быть Web-сервер и пара серверов, принадлежащих разным подсетям. Серверы, несмотря на размещение на одной машине, совершенно независимы друг от друга. Единственное ограничение — число виртуальных серверов. Это ограничение обусловлено ресурсами хост-

машины. Реальный компьютер должен обладать ресурсами, достаточными для обеспечения одновременной работы виртуальных машин.

3. Возможность быстрой замены сервера на другую версию. Это может быть полезно при обучении пользователей, когда в течение одного занятия необходимо рассмотреть работу и настройки двух-трех вариантов сервера. При этом учащиеся могут совершенно безбоязненно самостоятельно проводить настройки сервера. Даже самые грубые ошибки не приведут к серьезным проблемам, ведь заменить сервер очень просто!
4. Упрощение настроек базового физического сервера (хост-машины), что в свою очередь ускоряет и упрощает восстановление работоспособности сервера при серьезной аварии. Повышение надежности базового сервера. Вызывающие нестабильность в работе системы установки и переустановки программ выполняются только на виртуальных машинах.
5. Возможность дистанционного восстановления работоспособности серверов. Достаточно иметь удаленный доступ к базовой машине. К счастью, в наше время вариантов такого доступа может быть несколько, а один из весьма надежных — терминальный доступ средствами Windows.
6. Возможность размещения на одной физической машине одновременно работающих серверов под принципиально различными операционными системами — Windows и Linux могут работать на одном компьютере одновременно.
7. Возможность совершенно без риска для работы сервера испытывать различные программы, пригодность которых для ваших условий точно не установлена. Если в результате опыта выяснилась непригодность программы, то замена файла сервера позволяет полностью уничтожить следы установки программы, сохранив систему в максимально чистом виде.
8. …

Нет, хватит. Надо и вам дать возможность найти свои доводы в пользу виртуального сервера. Если кому-то покажется, что уже все сказано, то это может значить только то, что вы еще не вошли во вкус. Еще не опробовали работу с виртуальным сервером в полной мере. Если вы системный администратор или собираетесь им стать, то сможете найти у виртуального сервера еще с десяток плюсов. В каждой конкретной ситуации эти плюсы могут быть разными, но они есть всегда.

Понимание полезности виртуального сервера есть. Остается понять, как же установить этот сервер? Для этого существуют специальные программы. Среди них наиболее известны программы корпораций Microsoft и VMware.

Что можно установить?

Для кого-то покажется удивительным, но Microsoft предлагает нам виртуальный сервер Microsoft Virtual Server совершенно бесплатно! Требуется только регистрация перед загрузкой файлов. Получить этот сервер можно по адресу **http://www.microsoft.com/windowsserversystem/virtualserver/software/default.mspx**.

Предварительно можно почитать описание этого сервера на странице

http://zeus.sai.msu.ru:7000/operating_systems/virtserver/.

Также бесплатно можно скачать и VMware Server, который аналогично продукту Microsoft предназначен для создания виртуального сервера и управления им локально или удаленно через Web-интерфейс.

VMware также предлагает VMware Player, с помощью которого можно "проигрывать" виртуальные машины, созданные с помощью программ различных производителей (VMware, GSX Server, ESX Server, Microsoft Virtual PC и образы Symantec LiveState Recovery). То есть создав виртуальную машину в любой доступной вам программе, вы можете перенести ее на любой другой компьютер, где установлен VMware Player. Если виртуальная машина была создана не средствами VMware, например MS Virtual PC, то плеер автоматически импортирует файлы, преобразуя в свой формат. Подобно Adobe Acrobat Reader, который предназначен для чтения популярных PDF-файлов, VMware Player может "читать" созданные кем-либо виртуальные машины. Вы можете сами создавать виртуальные системы с помощью VMware Workstation или бесплатных виртуальных серверов Microsoft или VMware, распространяя их среди других пользователей ПК. Новому пользователю виртуальной системы даже не придется искать драйверы. После запуска в плеере драйверы устанавливаются автоматически. У автора не возникло проблем при переносе виртуальной машины, созданной на самостоятельно собранном персональном компьютере, на ноутбук HPCompaq.

Познакомиться с другими продуктами VMware можно на странице **http://www.vmware.com**. Фирма предлагает не только программы для создания и запуска виртуальных систем, но и сами системы. После установки VMware Player можно скачать множество примеров виртуальных машин, одна из которых содержит в себе ОС Linux Ubuntu и браузер Firefox. Предназначена эта виртуальная машина для безопасного просмотра интернет-страниц. Как и любая другая виртуальная машина, Browser Appliance замкнута в себе. Никакие

вирусы и опасные программы не смогут проникнуть в базовую или другую виртуальную систему. Эту виртуальную машину можно найти на странице **http://www.vmware.com/vmtn/appliances/directory/browserapp.html**.

Установка Microsoft Virtual Server 2005 R2

Выбор этого сервера обусловлен относительной простотой его настройки. Опыт других пользователей говорит о том, что на этот сервер можно установить не только Windows XP и серверные версии Windows, но и Linux. Интерфейс сервера не очень удобен для работы в виртуальной системе, хотя и позволяет это делать, но зато системой можно управлять дистанционно через Web-интерфейс с любого компьютера сети или даже… через Интернет! Корпорация Microsoft предлагает также инструментальный набор Virtual Server Migration Toolkit (VSMT) в качестве бесплатного дополнения для Virtual Server. Набор можно загрузить по адресу **http://www.microsoft.com/widowsserversystem/virtualserver/evaluation/vsmt.mspx**. С помощью VSMT можно преобразовать физические машины в VM, а виртуальные машины VMware VM — в совместимые с Virtual Server (компания VMware предлагает аналогичный продукт VMware P2V Assistant, но его нужно приобретать отдельно). Все это говорит в пользу Microsoft Virtual Server 2005 R2 при выборе виртуального сервера. Большинство пользователей Windows смогут без значительных проблем установить и освоить этот продукт.

Перед установкой виртуального сервера следует проверить, установлен ли у вас в системе компонент Internet Information Services Manager из состава Internet Information Services (IIS). Если компонент не установлен, то установите его. В системе Windows 2003 Server этот компонент находится в составе Сервера приложений. На клиентском компьютере, где будет установлен Virtual Machine Remote Control (Клиент удаленного контроля), никаких дополнительных компонентов не требуется.

Установка сервера не отличается от установки большинства обычных программ под Windows. Достаточно запустить на выполнение скачанный файл Setup.exe и для первой установки ничего не изменять в параметрах установки по умолчанию. На физическом сервере, где будет установлен виртуальный сервер, следует выполнить полную установку. Дополнительно можно установить компонент Virtual Machine Remote Control (Клиент удаленного контроля) на рабочую станцию, сняв отметки с остальных компонентов сервера во время установки.

После установки виртуального сервера в окне браузера откроется страница с информацией о результатах установки (рис. 6.1).

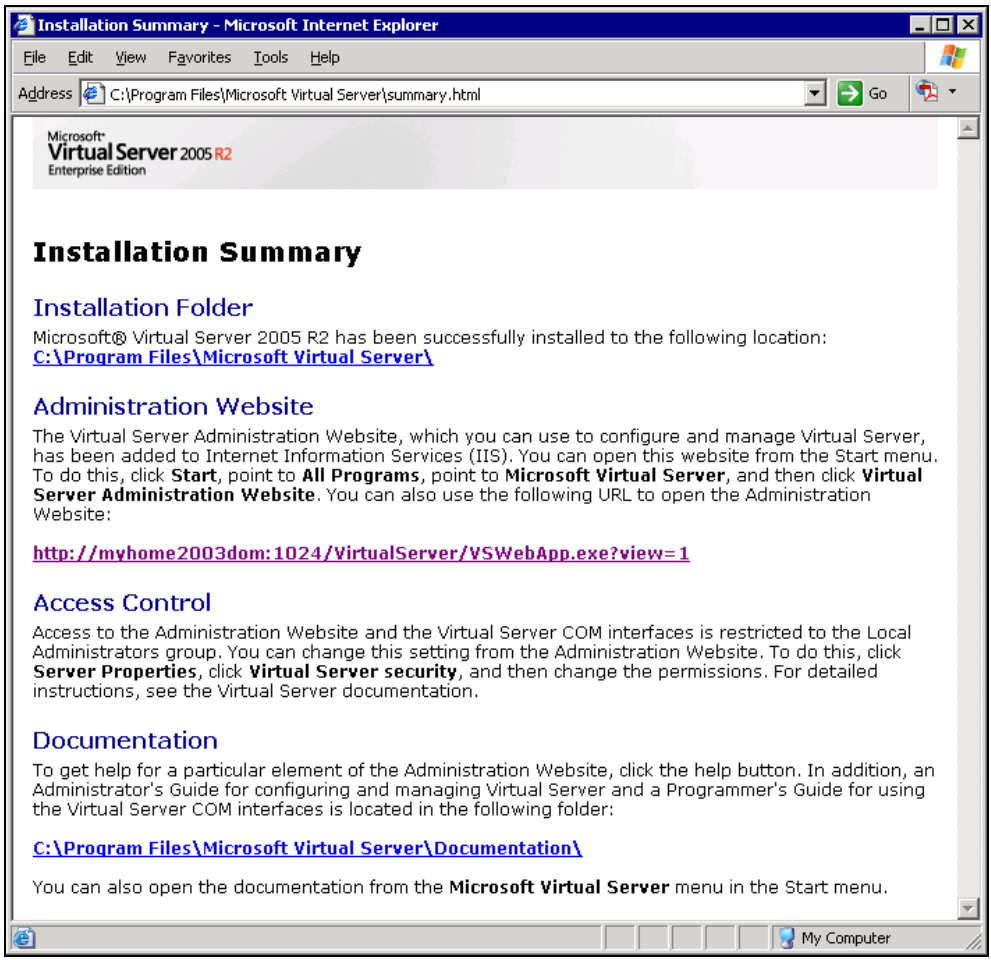


Рис. 6.1. Окно браузера **Installation Summary**
(Результат установки)

В этом окне указаны пути, куда установлены компоненты программы, а также ссылка на Web-интерфейс администратора. Выбрав в меню страницы пункт **Virtual Machines | Create** (Виртуальные машины | Новая), вы попадете в интерфейс создания новой виртуальной машины (рис. 6.2).

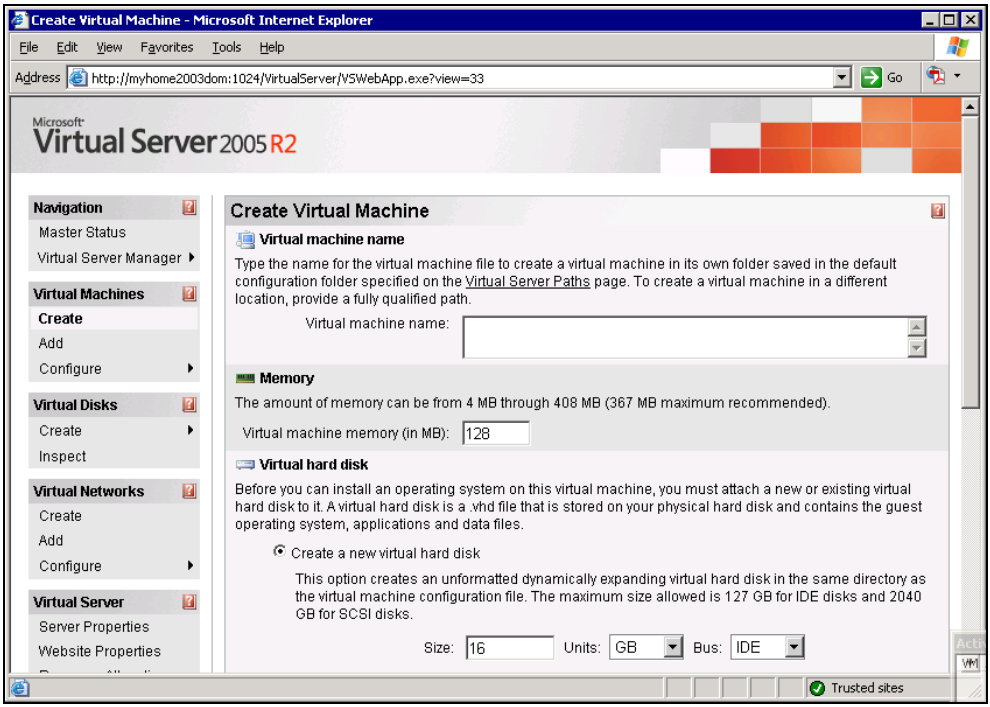


Рис. 6.2. Окно браузера **Create Virtual Machine** (Создание виртуальной машины)

Задав имя виртуальной машины, указав размер оперативной памяти для нее, размер и тип виртуального жесткого диска, а также указав, что должен использоваться физический сетевой адаптер, установленный на вашем компьютере, можно нажимать кнопку **OK**. В процессе создания виртуальной машины программа предложит отключить автозапуск CD-ROM. Автозапуск будет мешать подключению дисковода к виртуальной машине.

После создания виртуальной машины перейдите в меню **Master Status** (Страница состояния сервера) (рис. 6.3).

Из этого окна, воспользовавшись выпадающим меню у имени виртуальной машины, вы можете включить ваш виртуальный компьютер, а если в дисковод компакт-дисков вставлен дистрибутив Windows XP или Windows Server 2003, то можно сразу начать установку системы на виртуальный сервер.

Для того чтобы получить удобное окно управления виртуальной системой, можно кликнуть по маленькому изображению этого окна в интерфейсе

Virtual Machine Status. Или через меню **Пуск** запустить Virtual Machine Remote Control (рис. 6.4).

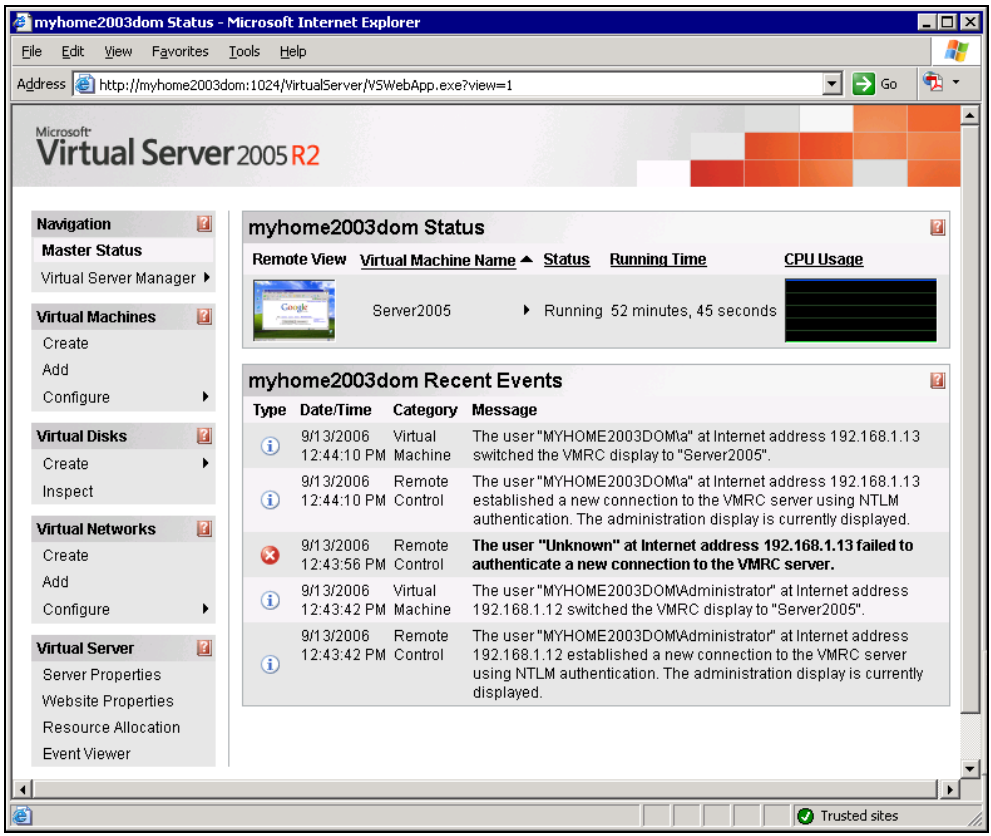


Рис. 6.3. Окно браузера **Virtual Machine Status**
(Статус виртуальной машины)

Пользуясь этим окном, вы сможете провести установку системы, а в дальнейшем просто работать в системе, производя необходимые настройки сервера (рис. 6.5).

Учитывая виртуальность сервера, вы можете создавать любое мыслимое число виртуальных машин, сохранять удачные, уничтожать не понравившиеся вам и запускать несколько виртуальных машин одновременно. При этом Virtual Machine Remote Control позволит переключаться между созданными машинами.

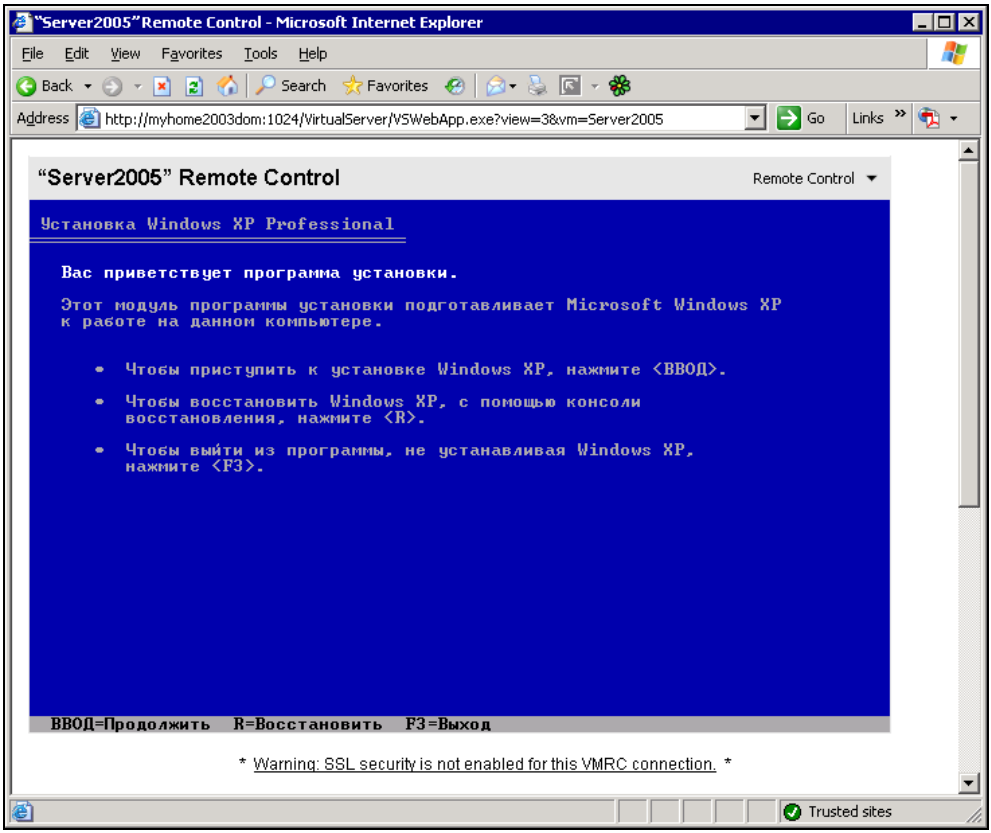


Рис. 6.4. Окно браузера **Virtual Machine Remote Control** (Клиент удаленного управления), раздел **Установка системы**

Создав более одного виртуального сервера, вы сможете подключаться с клиентского компьютера к любому из них. Установив на виртуальный сервер серверную версию операционной системы, вы можете осваивать варианты настройки сервера, применив впоследствии полученный опыт.

Возможно, что вам будет интересно прочитать некоторые подробности о виртуальном сервере. Это можно сделать на страницах **http://soft.mail.ru/article_page.php?id=91** и **http://www.osp.ru/text/302/177505/**.

Вполне возможно, что вам не требуется интерфейс управления виртуальным сервером. Можно просто установить виртуальную машину и использовать ее как обычный физический сервер. В этом случае для удаленного управления

виртуальной машиной можно использовать средства удаленного доступа к физическому серверу. Для управления самой виртуальной машиной можно организовать удаленный доступ прямо к ней. В этом случае можно заранее создать необходимые виртуальные машины, перенести их на физические машины, где они должны работать, а запускать их можно с помощью VMware Player.

Рис. 6.5. Окно браузера **Virtual Machine Remote Control** (Клиент удаленного управления). Система установлена

Используем VMware Player

Установка этой программы настолько проста, что описывать ее нет смысла. Единственное, на что можно обратить внимание, — если у вас уже установлена программа VMware Workstation версии ниже 5.0, то программа установ-

ки потребует ее удалить. Плеер входит в состав VMware Workstation 5.*x*, а бесплатные обновления для продуктов VMware возможны только в пределах основного номера версии программы. Но сам плеер бесплатный, а устанавливать его лучше на компьютер, где не установлена VMware Workstation.

После установки плеера и переноса на компьютер, где он установлен, файлов виртуальной машины можно запустить плеер. Программа попросит указать конфигурационный файл виртуальной машины, которую необходимо запустить (рис. 6.6).

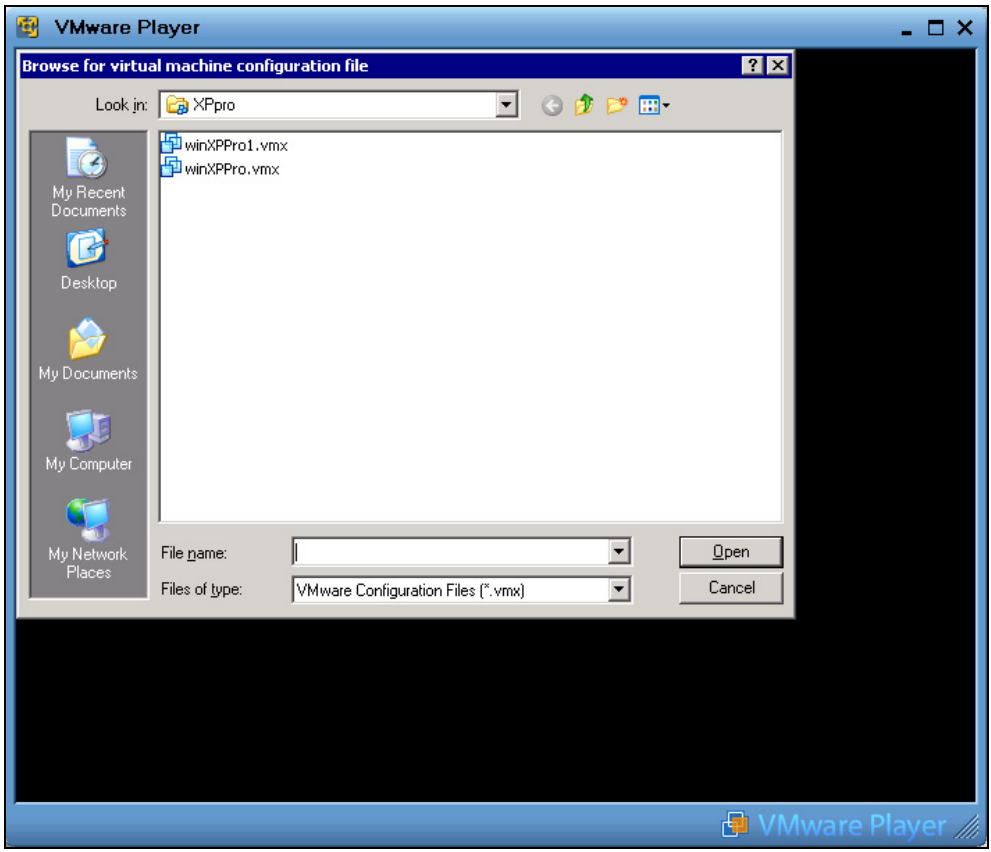


Рис. 6.6. Окно **VMware Player** (поиск файла конфигурации)

Если ваша виртуальная машина создана средствами Microsoft, то укажите соответствующий тип файла в поле **Files of type** и выберите необходимый

файл. Плеер преобразует виртуальную машину в формат VMware и запустит ее (рис. 6.7).

Рис. 6.7. Окно **VMware Player**
(запуск виртуальной машины)

Управление плеером ограничено возможностью отключения и подключения дисководов, сетевой карты и аудиосистемы. Все свойства виртуального компьютера определяются во время его создания. Тем не менее вам ничто не мешает устанавливать и переустанавливать операционную систему виртуального компьютера, выполнять в ней любые настройки. Соответственно, установив серверную операционную систему, вы можете настроить полноценный сервер.

Можно установить на один физический компьютер более одного виртуального сервера. Особенно интересен вариант, когда каждый из виртуальных серверов выполняет свою определенную задачу. В этом случае, вы можете совершенно ничем не рискуя, заменить, например, почтовый сервер, оставив без изменения файловый и Web-сервер. Если не понравилась работа нового сервера — просто запустите старый файл сервера!

Соблюдаем лицензии

Может возникнуть вопрос: не потребуется ли для виртуальных машин покупать отдельные лицензии на операционные системы? Ведь в правилах лицензирования ОС сказано:

"Персональные операционные системы лицензируются по следующему принципу — одна лицензия на один компьютер. Не имеет значения, сколько физических лиц использует компьютер".

Но на странице **http://www.toms-hardware.ru/business/200512091/index.html** есть указание на то, что в новых правилах лицензирования допускается использовать Windows XP Professional на одной физической и на одной виртуальной машине.

Лицензия на Windows Server 2003 R2 Enterprise допускает одновременное использование системы не более чем на одном физическом сервере и не более чем на четырех виртуальных серверах. Это значит, что на одном физическом сервере под Windows Server 2003 R2 можно установить еще четыре виртуальных сервера с той же ОС. При этом не запущенные копии системы могут храниться в любом количестве. Ограничения есть только на одновременно работающие копии системы.

По адресу

http://download.microsoft.com/download/4/7/4/47415510-647d-4847-a554-b5bb33bd44af/Licensing_with_Microsoft_Virtual_Server_R2.doc

можно получить документ, подтверждающий ваши права на использование операционной системы на виртуальной машине.

Но в отдельных случаях вам может не хватить разрешенного числа работающих копий. В этом случае вы можете использовать другие операционные системы на виртуальных машинах. Обычно это операционные системы се-

мейства Linux. Но как установить и настроить систему, если у вас нет опыта работы в этих системах?

И здесь есть выход. VMware предлагает на своем сайте несколько десятков готовых виртуальных машин различного назначения!

Virtual Appliances

Загляните на страницу **http://www.vmware.com/vmtn/appliances/**. На ней можно найти ссылки на готовые виртуальные машины. Virtual Appliances (Виртуальные приборы) — это уже установленные и сконфигурированные под определенные задачи системы.

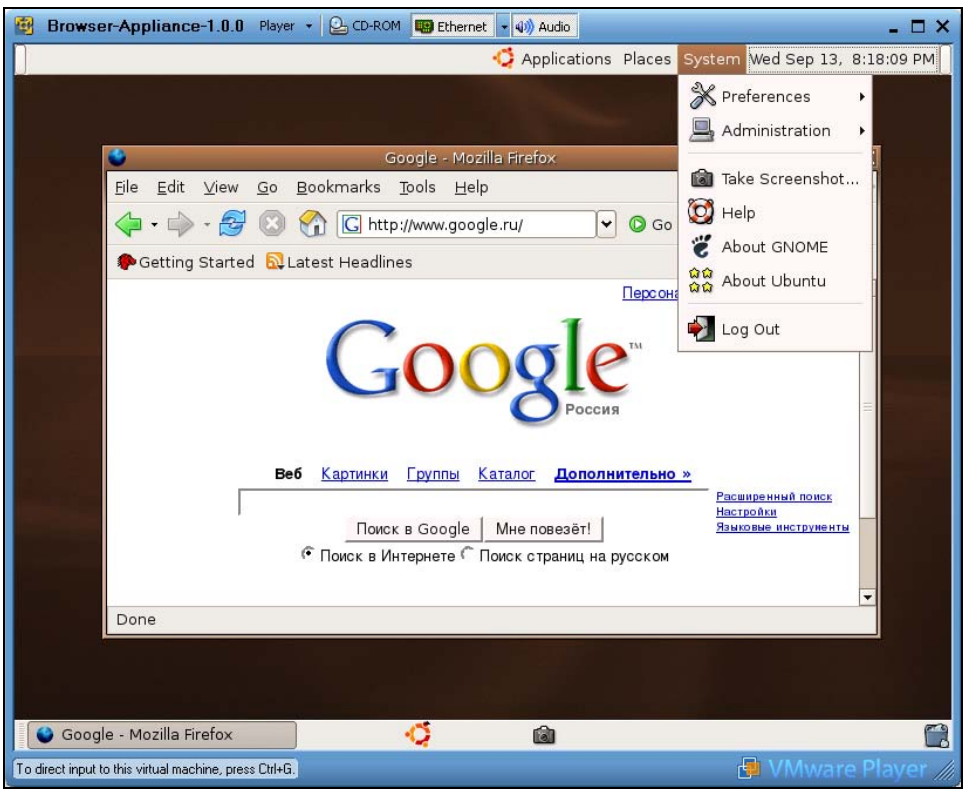


Рис. 6.8. Окно **VMware Player**
с запущеным Browser Appliance и открытым системным меню

Browser Appliance (Виртуальный браузер) уже упоминался в начале главы. Автор скачал и запустил этот инструмент с помощью VMware Player. Результаты просто ошеломляющие (рис. 6.8)! Без особого труда удалось подстроить систему под часовой пояс и использование русской раскладки клавиатуры. Были установлены дополнительные программы: текстовый редактор и Macromedia Flash Player. Теперь, запуская эту виртуальную машину, можно совершенно безопасно посещать самые рискованные участки Всемирной паутины, не опасаясь при этом проблем на базовой машине. Подключенная флэшка опозналась моментально. Любые недостающие компоненты при настройке сети или установке программ моментально скачиваются из Интернета и устанавливаются.

Есть Virtual Appliances с почтовым сервером и фильтрами спама, MySQL-сервер, Apache-сервер, маршрутизаторы, специальный Appliance для обеспечения общего подключения к Интернету, прокси-серверы, просто установленные Linux различных версий… всего не перечислишь. Это надо видеть!

К сожалению, многие инструменты имеют довольно большой объем, но современный Интернет позволяет скачивать такие объемы.

Теперь, имея достаточно мощный компьютер, вы можете установить на него несколько серверов или вспомогательных систем. Можно просто своими руками "потрогать" уже настроенные системы. И все это без нарушения лицензий, если вы имеете одну официально приобретенную ОС Windows.

Что ж, пожалуй, теперь вы имеете достаточно информации о виртуальных машинах и виртуальных серверах. Нет необходимости приобретать еще один компьютер, когда требуется установить дополнительный сервер, выполняющий какую-либо специальную задачу. А опробовать идею, изучить настройки системы можно на виртуальной машине, предварительно сохранив ее копию.

Только не забудьте, что виртуальный компьютер, как и обычный, выключать надо правильно, начиная с кнопки **Пуск**…

Устанавливаем виртуальный компьютер

Виртуальный компьютер, установленный на базовой реальной машине, расширяет возможности пользователя и даже приносит существенную финансовую экономию, а также экономию времени. Например, чтобы организовать защиту от неблагоприятного воздействия на вашу систему из Интернета, обычно требуется установка и настройка специализированного программного

обеспечения. Причем это программное обеспечение будет выполнять только ту функцию, которую вы для него определили. Виртуальный компьютер может работать, не взаимодействуя с базовой системой на уровне обмена информацией. Это значит, что установив виртуальный компьютер с ОС Linux и посещая с него страницы Интернета, вы на 100% защитите свою базовую систему. А в случае краха виртуальной системы (маловероятного) вы можете ее восстановить за несколько секунд.

Виртуальные серверы и рабочие станции не требуют приобретения реального оборудования для отладки каких-либо сетевых или программных решений.

Две корпорации Microsoft и VMware предлагают как виртуальные серверы, так и виртуальные рабочие станции. В *главе 2* мы познакомились с виртуальной машиной VMware, а в этой главе — с Microsoft Virtual Server и VMware Player. Теперь рассмотрим подробнее работу с виртуальными машинами.

VMware специализируется на программном обеспечении для виртуальных компьютеров и серверов. Поэтому, в отличие от Virtual PC производства Microsoft, VMware Workstation предлагает значительно больше возможностей для настройки виртуального ПК, позволяя пользователю не только создавать простой компьютер общего пользования, но и подключать к нему USB-, SCSI-устройства, создавать сложные, разветвленные сети как внутри базового компьютера, так и сети, объединенные с реальными. Есть возможность сделать "снимок" внутренней операционной системы, к которому можно вернуться в любой момент. Это делает виртуальную ОС практически вечной — в случае краха системы можно вернуть ее в изначальное состояние одним щелчком мыши.

Существующие операционные системы поддерживаются VMware практически все. У вас не возникнет проблем при установке любой операционной системы Microsoft и большинства систем Linux. Более того, можно вместо скачивания дистрибутива Linux скачать с сайта **http://www.vmware.com/vmtn/appliances/directory/** уже готовый виртуальный компьютер с установленной операционной системой. Если в плеере VMware Player можно эти готовые виртуальные компьютеры использовать по их прямому назначению, то VMware Workstation позволит модифицировать их по вашему усмотрению.

Виртуальный компьютер, конечно, требует определенных ресурсов для своей работы. Но оперативная память используется виртуальными машинами VMware очень рационально. Если виртуальный компьютер запущен на базовом и не выполняет ресурсоемких вычислений, то на базовом компьютере вы практически не заметите потерь в производительности. Поэтому вполне воз-

можен запуск на одном базовом двух или трех виртуальных компьютеров одновременно.

Серверная операционная система может быть установлена в обычной виртуальной машине. Это не позволит управлять виртуальной машиной через Web-интерфейс, но сервер будет работать нисколько не хуже. Во всяком случае, в моей домашней сети виртуальный сервер Windows 2000 Server, содержащий Active Directory, работает на физическом сервере, выполняющем другие функции. Они не мешают друг другу, работают в одном системном блоке, не имеют клавиатуры, мыши и монитора. Стоят себе в уголочке, к которому пришлось подвести кабель питания и витую пару. Связь с серверами осуществляется через терминальный доступ. В виртуальной машине, установленной на базовом компьютере, работают еще два виртуальных компьютера, которые обычно выключены. Но при необходимости они включаются и выполняют свои задачи, не вмешиваясь в работу серверов. Один системный блок с виртуальной машиной заменяет несколько компьютеров!

Думаю, что вы уже прониклись идеей полезности виртуальной машины для вас лично.

http://www.vmware.com/products/ws/ — это страница VMware Workstation. Здесь можно купить или скачать пробную версию программы. В любом случае необходимо зарегистрироваться на этом сайте. Если вы скачаете пробную версию, вам будет выслан серийный номер программы, который действует ограниченное время, а если вам не хватит отведенного времени, вы сможете получить еще один серийный номер.

Итак, вы скачали и установили программу. Для выполнения большинства операций по созданию виртуальных машин предусмотрены мастера. Если в процессе создания виртуальной машины мастер задает вопрос, на который вы не можете пока ответить, соглашайтесь на все, что предлагает мастер по умолчанию. Позднее вы можете изменить все, что потребуется. Настройки сети вынесены в отдельную утилиту Virtual Network Editor (Редактор виртуальной сети), где можно настроить виртуальные сетевые адаптеры и маршрутизаторы. Виртуальная машина, созданная в VMware Workstation, может использовать любой из созданных сетевых адаптеров.

Если не говорить о создании виртуальной сети в вашем компьютере, то из всех возможных сетевых адаптеров вам пригодится чаще всего VMnet0 , который может быть связан с реальным сетевым адаптером, но иметь самостоятельный IP-адрес и работать независимо. Для всех компьютеров, находящихся в сети, компьютер с этим сетевым адаптером будет виден, как самостоятельная машина.

Есть еще один большой плюс у виртуальной машины, ради которого каждый системный администратор захочет ее иметь на своем компьютере.

Известно много средств резервирования и восстановления системы. Но два из них, а точнее симбиоз двух таких средств заслуживает особого внимания. BartPE Builder и Acronis True Image — вот эти средства. Первое из них позволяет создать самостоятельно загрузочный диск с Windows-подобной операционной системой, а вторая, предназначенная для создания образов дисков и последующего их восстановления, может быть встроена в эту систему. Но делать диск придется своими руками. Приближаясь к идеальному, по вашему мнению, варианту загрузочного диска, вы переведете множество болванок CD-R.

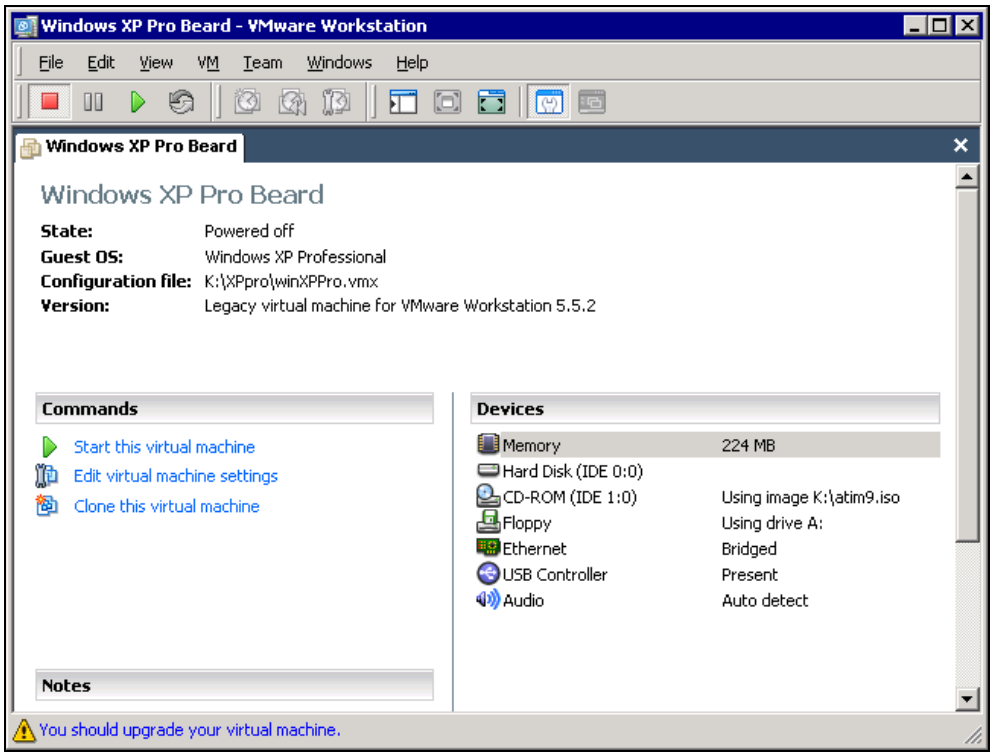


Рис. 6.9. Окно виртуальной машины VMware Workstation

В то же время, виртуальная машина может использовать вместо реальных дисков их образы. Подключив образ диска к виртуальной машине, постепен-

но доводя этот образ до желаемого состояния, вы можете здесь же и проверять результат своей работы, загружая виртуальную машину с образа диска. И только завершив пробы, устранив все ошибки, вы можете записать образ на реальный диск.

Интересно, что на таком загрузочном диске можно поместить даже интернет-браузер. На дисках автора работает Mobile Firefox (**http://mobilefirefox.com/**). Вот теперь самые ревнивые блюстители сетевой безопасности могут быть спокойны. До тех пор, пока вы сами не сохраните результаты поиска в Интернете на какой-либо носитель, ничто не сможет проникнуть в вашу реальную систему из Интернета!

Давайте посмотрим настройки на работу виртуальной машины.

На рис. 6.9 показано окно виртуальной машины, в которой уже создан виртуальный компьютер с ОС Windows XP.

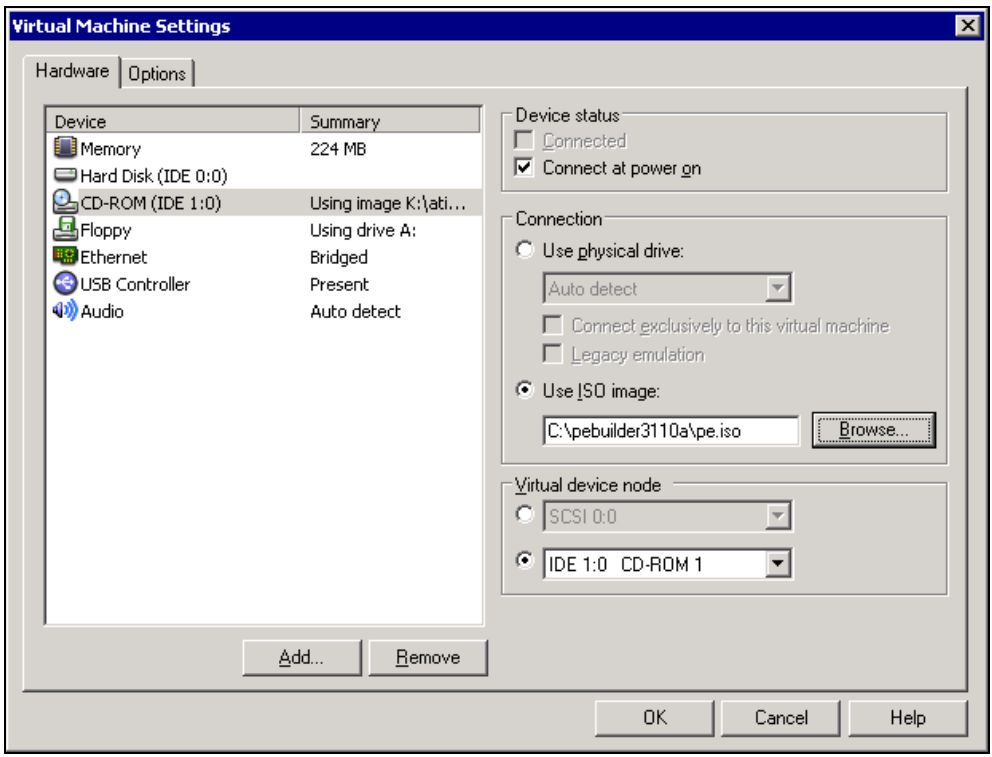


Рис. 6.10. Окно **Virtual Machine Settings**

С помощью меню **Edit Virtual Machine Settings** (Редактор настроек виртуальной машины) можно подключать и отключать устройства, менять некоторые параметры системы, например размер оперативной памяти (рис. 6.10). Там же можно подключить образ CD-ROM-диска вместо реального дисковода.

Запускаем виртуальную машину, предварительно в BIOS виртуальной машины установив загрузку с CD-ROM (рис. 6.11).

После выхода из настроек BIOS Setup начинается загрузка системы (рис. 6.12).

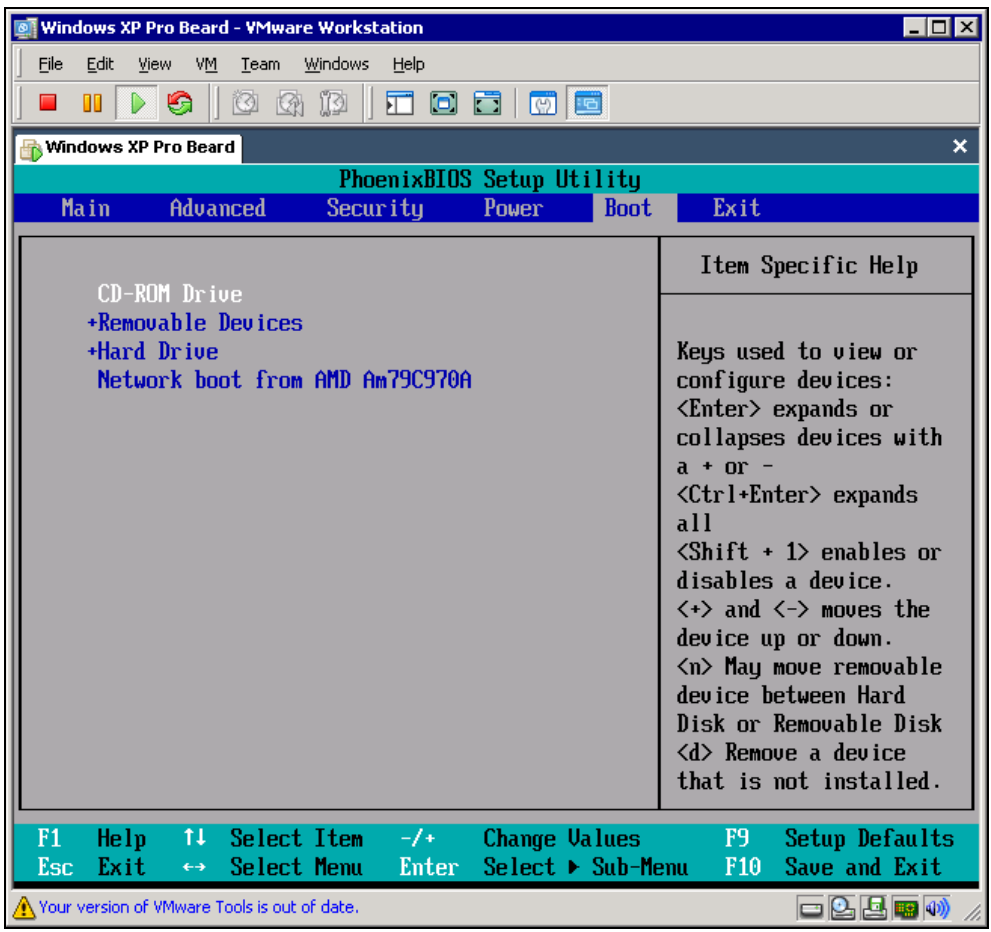


Рис. 6.11. Окно виртуальной машины VMware Workstation. Настраиваем BIOS Setup

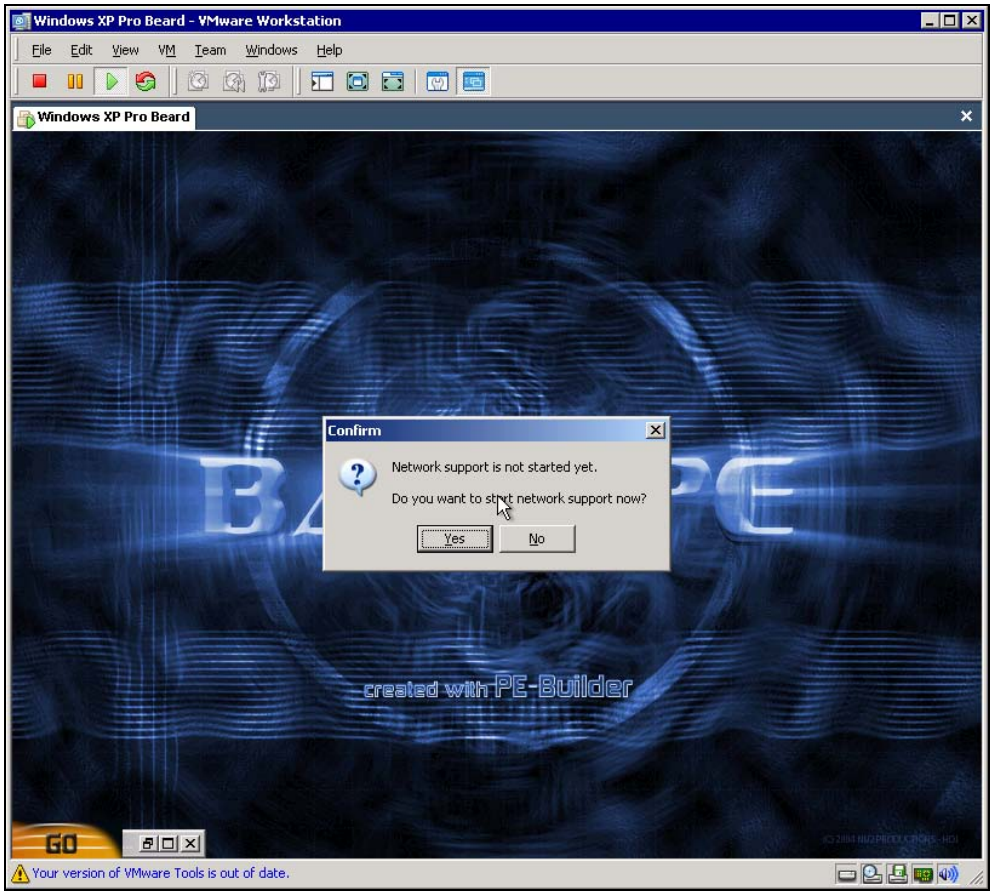


Рис. 6.12. Окно виртуальной машины VMware Workstation. Вход в BartPE и предложение настроить сеть

В самом начале загрузки система предложит настроить сетевые параметры. Они настраиваются, как и обычно, в соответствии с требованиями вашей сети. В сети, где делался этот пример, все необходимые настройки компьютерам передает DHCP-сервер. Чтобы получить к нему доступ, необходимо было ввести имя рабочей группы и домена, а также имя и пароль администратора сервера.

После завершения загрузки можно запускать приложения, которые вы предусмотрели при изготовлении загрузочного диска. Очень удобно иметь на этом диске привычный многим файловый менеджер FAR (рис. 6.13). Он позволяет входить не только в локальные, но и в сетевые каталоги. При запуске FAR

необходимо нажать комбинацию клавиш <Alt>+<F9>, чтобы перевести его в видеорежим. В обычном текстовом режиме окно менеджера оказывается слишком длинным и не поддается настройке. Если во время работы с восстанавливаемой системой вам потребовался Интернет, то он тоже к вашим услугам прямо из BartPE (рис. 6.14).

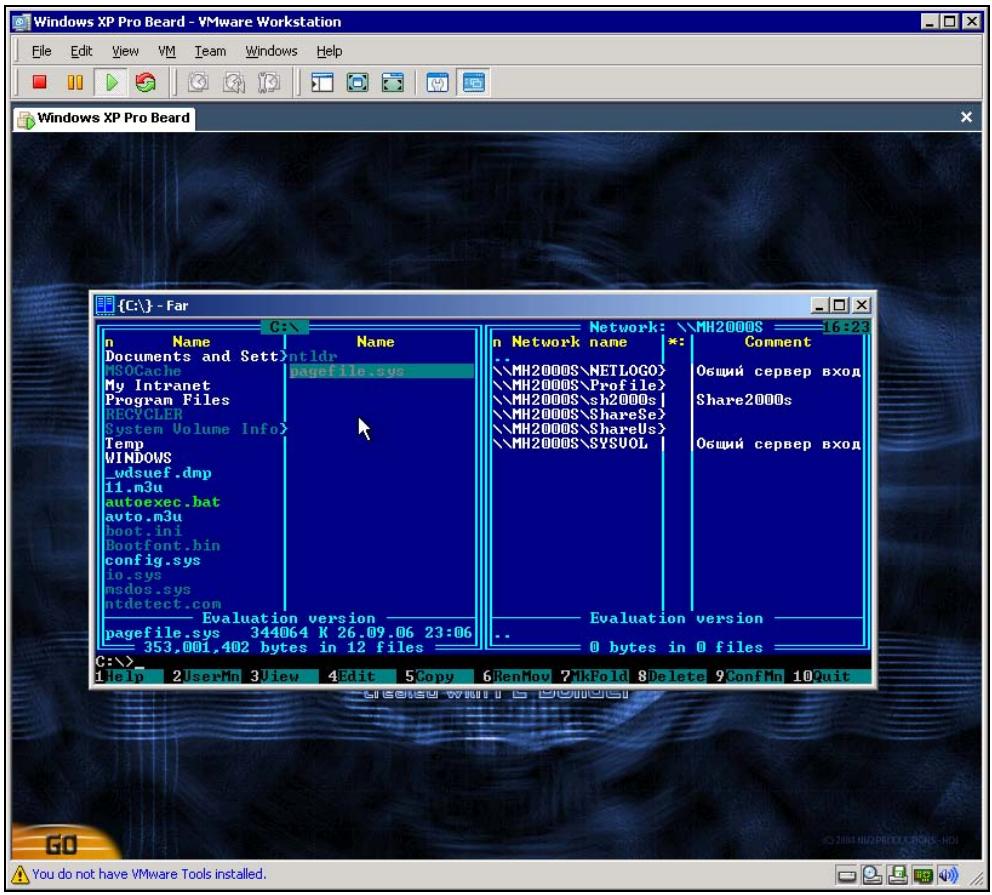


Рис. 6.13. Окно виртуальной машины VMware Workstation и привычный FAR

И, конечно, Acronis True Image тоже можно запустить в окне BartPE (рис. 6.15). Возможность включения Acronis True Image в BartPE предусмотрена самой фирмой Acronis, которая с последними версиями программы поставляет и специальный плагин для BartPE.

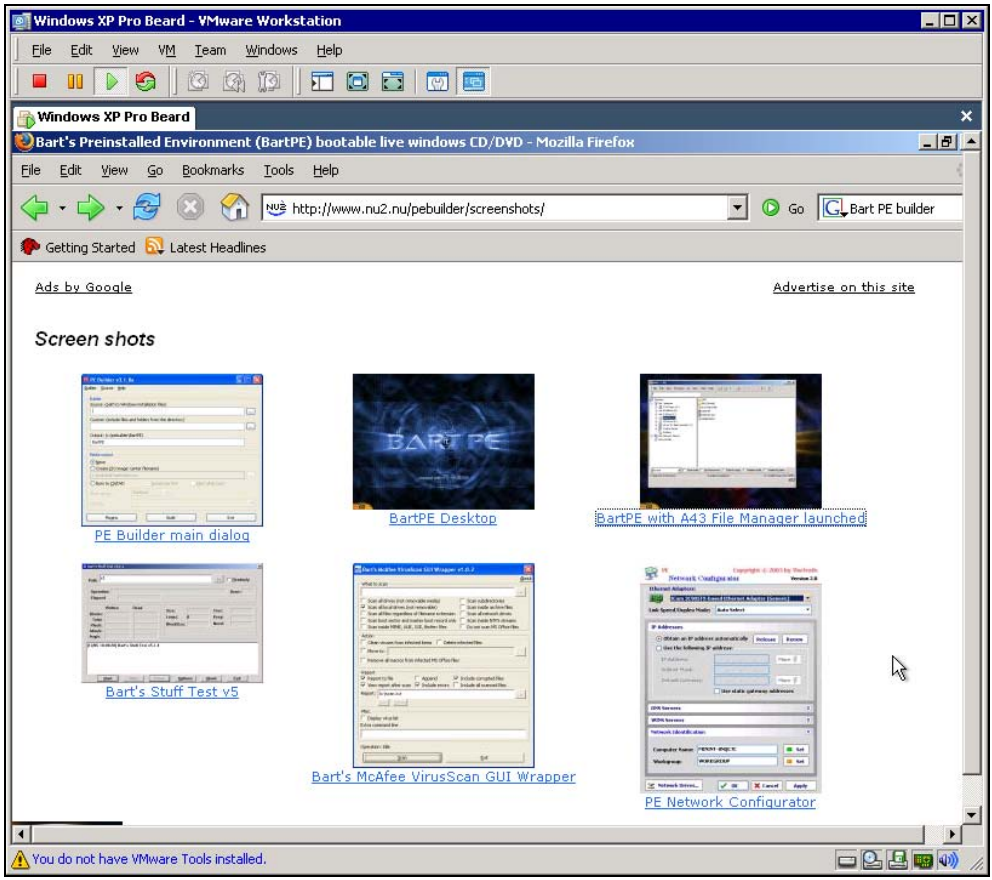


Рис. 6.14. Окно виртуальной машины VMware Workstation и браузер Mobile Firefox

Работа с обычными операционными системами практически не отличается от работы с ними на реальных компьютерах. Просто надо установить их на виртуальный диск.

Теперь вы можете иметь постоянно под рукой несколько компьютеров с различными ОС и различного назначения. Никакие материальные затруднения не могут помешать провести эксперимент во временно созданной сети, проверить работу программы. Можно даже смотреть на реальную работу вирусов, сохранив предварительно файл виртуального диска. А создание загрузочных CD-дисков теперь станет увлекательным занятием, не требующим расхода болванок.

Рис. 6.15. Окно виртуальной машины VMware Workstation и программа Acronis True Image

Ссылки на страницы о Bart PE Builder и работе с программой:

- **http://www.izcity.com/lib/18012005/Bart_PE_Builder_3_1_3.htm**;
- **http://www.nu2.nu/pebuilder/download/**.

Ссылки на страницы о Acronis True Image:

- **http://www.acronis.ru/homecomputing/products/trueimage/**.

Ссылки на страницы о виртуальных машинах:

- **http://gazette.linux.ru.net/lg86/ward.html**;
- **http://citforum.ru/operating_systems/seven/**;

- **http://www.openproj.ru/index.php?t=412**;
- **http://onix.opennet.ru/content/view/12/26/**.

Виртуальная сеть

Как вы понимаете, виртуальные компьютеры настраиваются так же, как и реальные, подключать к локальной сети или объединять в отдельную сеть. Этим удобно воспользоваться для моделирования локальной сети в безопасных условиях. Достаточно иметь мощную машину, на которой установлено три-четыре виртуальных компьютера, чтобы создать сеть на вашем рабочем столе. Но для реальной сети может быть полезнее организация виртуальной сети между реальными компьютерами, экспериментальную модель которой вполне можно создать на базе виртуальных компьютеров.

VPN

Виртуальная частная сеть (Virtual Private Network, VPN) для большинства обычных пользователей и начинающих администраторов — область мало известная. Даже когда услуга по организации виртуальной частной сети предоставляется какой-либо фирмой (провайдером), то на стороне пользователя обычно производятся настройки клиентской части VPN, что не вызывает затруднений (учитывая рекомендации провайдера). Windows позволяет настраивать подключения к сетям VPN, организовывать каналы VPN между локальными сетями через Интернет. Но в практике администратора локальной сети чаще может возникнуть задача обеспечения связи одной удаленной рабочей станции с локальной сетью. Организация такого доступа к локальной сети позволяет решить задачу доступа пользователя к своим файлам и принтерам. При этом, в отличие от терминального доступа или доступа через программы удаленного администрирования, на экране компьютера, с которого осуществлен доступ, не будет рабочего стола удаленной машины. Но в сетевом окружении будут необходимые папки, а для печати документов можно использовать принтер, находящийся в локальной сети и подключенный к компьютеру, к которому осуществлен доступ через VPN. Задержки передачи информации между компьютером удаленного пользователя и сетью не повлияют на скорость обычной работы с документами. В зависимости от скорости передачи информации через применяемое подключение к Интернету, будут более или менее значительными время копирования файлов и время

печати документа. Само по себе соединение устанавливается достаточно быстро даже при использовании выхода в Интернет через обычный модем. У автора соединение устанавливается в течение 40 секунд, в то время как локальная сеть находится на расстоянии более 50 км от места подключения. Единственное условие, которое должно быть соблюдено, — это наличие у рабочей станции, с которой осуществляется доступ к сети, реального (пусть даже динамически выделяемого) IP-адреса, а у компьютера, через который подключена к Интернету локальная сеть, должен быть постоянный IP-адрес, выделенный поставщиком услуг Интернета. Если не ставить условие обратного доступа из сети к удаленной рабочей станции, то подключение может быть выполнено, когда выход в Интернет удаленной рабочей станции выполняется через другую локальную сеть.

Применение VPN позволяет предоставить доступ к файлам и принтерам не только администратору, но отдельным пользователям (возможно, руководителю организации). Доступ к файлам и принтерам через VPN не нарушает работы пользователя компьютера, через который осуществляется доступ. Методы шифрования, применяемые для организации VPN, не позволят постороннему перехватить передаваемую информацию, пароли и получить доступ к сети. В отличие от доступа через сервер терминалов, в данном случае не потребуется и приобретение каких-либо дополнительных лицензий в случае предоставления доступа нескольким пользователям.

Итак, наша сеть через вспомогательный сервер (компьютер) подключена к Интернету через ADSL-модем. Нам требуется доступ к файлам и принтерам сети. Поскольку без экспериментов здесь не обойтись, начнем с описания организации тестовой VPN между двумя машинами. Ваша сеть может существенно отличаться от той, что рассматривается в данной книге. Поэтому для организации VPN мы воспользуемся свободно распространяемым программным обеспечением, которое может работать на любом компьютере сети, где нет встроенных средств для создания виртуальной сети.

Эта программа называется OpenVPN, а найти ее можно по адресу в Интернете **http://openvpn.sourceforge.net**. Программа распространяется бесплатно, имеет реализации для различных платформ, что позволяет настраивать подключения к серверам, работающим как под Windows, так и под Linux (UNIX). Для скачивания файлов дистрибутива программы лучше воспользоваться страницей **http://openvpn.sourceforge.net/beta**. Серверная и клиентская части программы ничем не отличаются, кроме нескольких строчек в файле конфигурации программы. В режиме сервера программа может быть

запущена в качестве службы. После установки программы на компьютере появляется виртуальный сетевой адаптер (рис. 6.16).

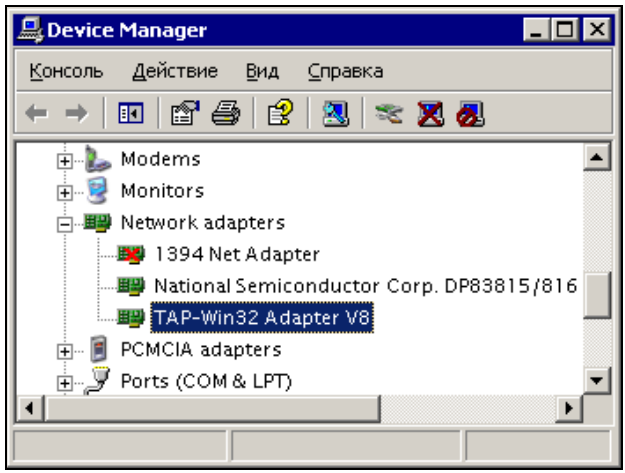


Рис. 6.16. Новый адаптер
в перечне оборудования компьютера

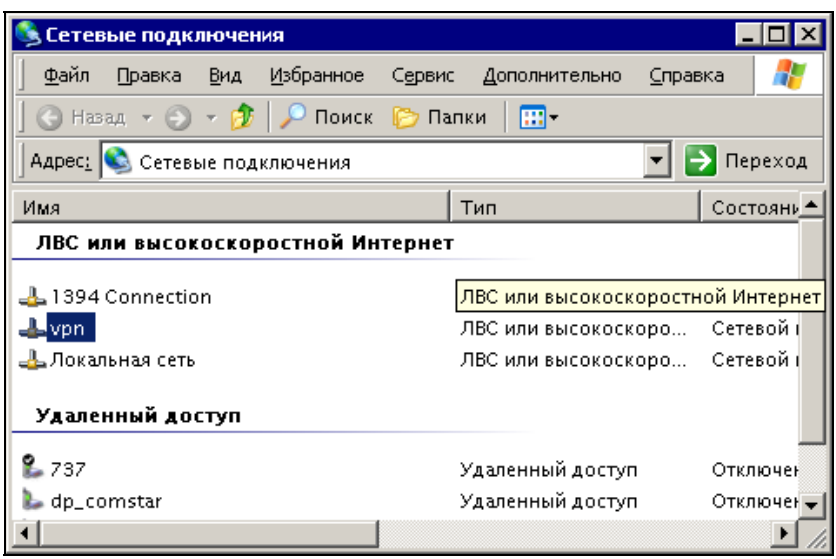


Рис. 6.17. Окно **Сетевые подключения**
с новым сетевым подключением

Для нового адаптера автоматически создается и новое подключение (рис. 6.17), которое следует сразу переименовать в короткое и понятное имя. Это необходимо, поскольку в файлах конфигурации программы OpenVPN требуется указать имя сетевого адаптера. При этом программа работает в режиме командной строки, где короткие имена предпочтительны.

Файлы конфигурации для сервера и клиента в самом простом варианте приведены в листингах 6.1 и 6.2.

Листинг 6.1. Файл конфигурации для клиента OpenVPN Local.ovpn

```
# имя компьютера, к которому осуществляем доступ
remote hp-admin
# порт, через который осуществляется связь (любой свободный)
port 35000
# указание на роль компьютера в VPN
proto tcp-client
dev tap
ifconfig 192.168.116.3 255.255.255.0
dev-node vpn
secret key.txt
ping 10
comp-lzo
verb 4
mute 10
```

Листинг 6.2. Файл конфигурации для сервера OpenVPN Server.ovpn

```
port 35000
proto tcp-server
dev tap
ifconfig 192.168.116.1 255.255.255.0
dev-node vpn
secret key.txt
ping 10
comp-lzo
verb 4
mute 10
```

В обоих файлах имя сетевого подключения (`dev-node`) — `vpn`. Сетевые подключения настройки не требуют, их параметры устанавливаются самой программой.

Так в клиентском файле есть строка:

```
ifconfig 192.168.116.3 255.255.255.0.
```

Эта строка устанавливает IP-адрес для подключения VPN равным 192.168.116.3, а маску подсети — 255.255.255.0. Файлы должны иметь расширение ovpn. При этом в контекстном меню этих файлов появится пункт **Start OpenVPN on this config file** (Запустить OpenVPN с этим файлом конфигурации).

Для организации виртуальной частной сети необходимо, чтобы со стороны удаленного компьютера можно было выполнить команду ping по адресу сервера, к которому делается попытка подключения. В локальном файле конфигурации указывается имя сервера (параметр remote), причем это должно быть только имя. Следовательно, связь имени и IP-адреса следует обеспечить установкой. Например, записать в файле C:\WINDOWS\system32\drivers\etc\hosts строку, содержащую IP-адрес и имя компьютера, разделенные пробелом. В описываемом примере строка в файле Hosts выглядит так:

```
192.168.115.136 hp-admin.
```

Адрес в файле Hosts отличается от адреса в файле конфигурации. Это связано с тем, что адрес основного сетевого адаптера не совпадает с адресом адаптера, созданного программой OpenVPN.

OpenVPN-сервер, запущенный на сервере сети, ожидает попыток подключения извне. В случае удачной попытки сетевое подключение VPN активизируется.

OpenVPN-клиент после запуска предпринимает попытки определить доступность сервера по его имени. Как только сервер обнаружен, создается канал связи через виртуальные сетевые адаптеры.

Для обеспечения защищенности этого канала применяется шифрование. Оно обеспечивается наличием файла ключа key.txt, который должен быть сформирован средствами самой программы на одном из компьютеров и передан на другой любым доступным способом. Кроме того, связь осуществляется через выбранный вами порт, номер которого указывается в файлах конфигурации (параметр `port`).

Как серверная часть, так и клиентская не имеют графического интерфейса. Работа программы видна в текстовом окне, в котором выводятся все сообще-

ния о действиях программы и ее состоянии. Примеры окон клиентской и серверной частей программы с установленным соединением показаны на рис. 6.18 и 6.19. Признаком установившегося соединения в обеих частях программы является сообщение, содержащее строку "Initialization Sequence Completed" ("Процедура инициализации завершена").

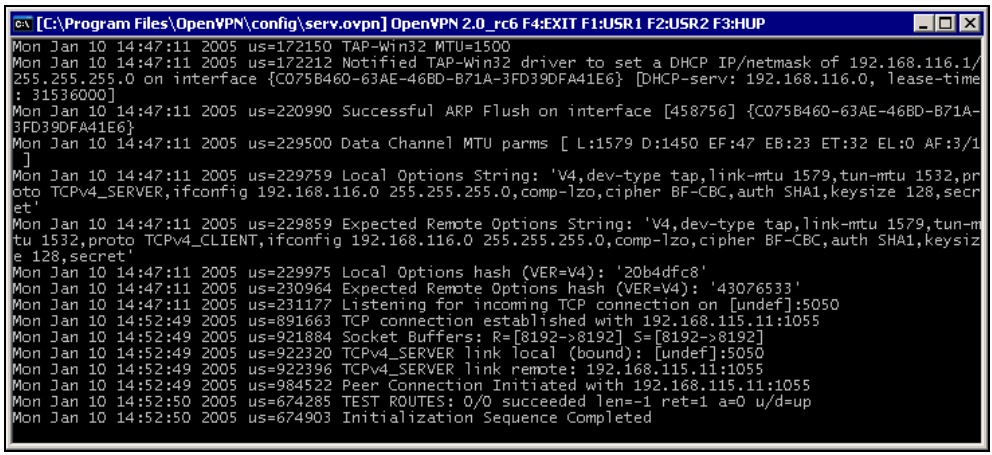


Рис. 6.18. Окно **OpenVPN** на сервере

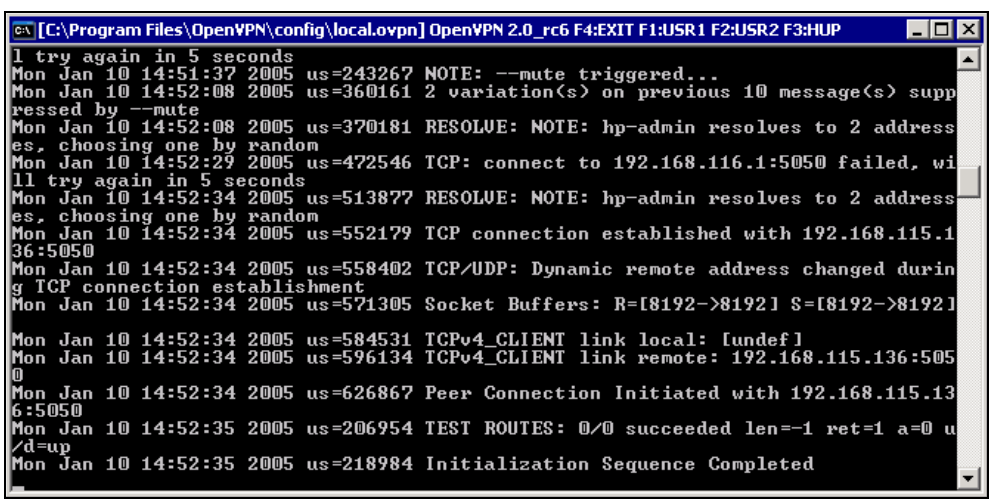


Рис. 6.19. Окно **OpenVPN** на локальной машине

Сообщение клиентской программы "mute triggered" означает, что попытки связи неудачны и программа ожидает изменений в настройках. Например, если был недоступен адрес сервера по его имени, а вы внесли верную запись в файл Hosts (не закрывая OpenVPN), программа возобновит попытки установления связи.

При установившейся связи в сетевом окружении удаленного компьютера появится сервер. Чтобы зарегистрироваться на нем, потребуется ввести имя пользователя и пароль, допустимые в сети.

Для успешного соединения следует проконтролировать выполнение еще двух условий:

- локальный IP-адрес удаленной рабочей станции и сервера должен принадлежать подсети, которой не принадлежат адреса виртуальных адаптеров, созданных OpenVPN;
- имя рабочей группы, к которой принадлежит удаленная рабочая станция, должно совпадать с именем домена или рабочей группы сервера. Компьютер может принадлежать и самому домену (ноутбук, например).

Первое из этих условий обеспечивает однозначность поиска компьютера-сервера программой клиентом. Невыполнение этого условия приведет к невозможности установления связи с удаленной сетью, а OpenVPN не предоставит вам никакой информации о причинах неудачи.

Второе условие обеспечивает появление компьютеров, находящихся в локальной сети, в сетевом окружении удаленной рабочей станции.

При достаточном качестве связи пользователь получит практически все те же возможности, что и при работе в локальной сети.

Если вход в локальную сеть защищен брандмауэром, то необходимо разрешить доступ к файлам и принтерам через виртуальный интерфейс, а основной интерфейс должен быть доступен для команды `ping`. Для этого следует включить параметр протокола ICMP (Internet Control Message Protocol, протокол управляющих сообщений в сети Интернет) **Разрешать запрос входящего эха**, что обеспечит возможность ответов компьютера на команду `ping` по его адресу. Настройки этого протокола доступны в дополнительных параметрах брандмауэра в ОС Windows XP и Windows 2003 Server.

Поскольку в каждой сети, в том числе и в вашей, настройки доступа к ней могут иметь свои особенности, без экспериментов вам не обойтись, поэтому для тонкой настройки придется обратиться к справке по OpenVPN и справочной системе Windows. Но применение OpenVPN позволит вам достаточно

быстро провести настройки подключения, если они возможны в ваших условиях. Когда подключение установлено, скорость передачи информации по этому каналу будет ниже, чем при прямом соединении. Дополнительные преобразования информации, шифрование и дешифрование — все это требует добавочного времени. Но для обычной работы в сети скорость связи вполне достаточна, особенно если рабочая станция подключена к Интернету через быстрый канал связи. Автору удалось установить такое соединение через коммутируемый доступ (dial-up). При этом работа с документом Word требовала, чтобы он был скопирован на рабочую станцию, но печать на один из принтеров сети проходила нормально. Более того, этот принтер был подключен к рабочей станции во время соединения. Для ускорения процесса подключения желательно, чтобы драйвер принтера уже был установлен на удаленной рабочей станции.

Можно обеспечить несколько подключений к серверу, запустив на нем несколько экземпляров OpenVPN-сервера. Каждый из экземпляров должен быть связан со своим виртуальным сетевым подключением. Виртуальные подключения могут создаваться средствами OpenVPN в любом необходимом количестве. Это позволяет для каждого подключения применять свой ключевой файл, что повышает защищенность сети.

Описанный ранее пример подключения предназначен только для первого опыта. В нем предполагается прямое соединение двух компьютеров перекрестным кабелем или через концентратор (хаб, коммутатор). Реальное соединение, которое далее будет описано, лучше организовывать после удачного завершения первого эксперимента по установке связи между двумя компьютерами. Для реальной связи через Интернет с локальной сетью потребуется более кропотливая работа. Приведем пример реально работающей пары компьютеров, связанных через VPN. Само собой разумеется, что на оба компьютера необходимо установить OpenVPN. Имя виртуальному сетевому адаптеру следует присвоить короткое латинскими буквами. Можно использовать имя программы OpenVPN.

В этом примере описаны настройки для двух компьютеров. Один из них — ноутбук, который работает и в локальной сети, и вне ее. Другой — вспомогательный сервер под управлением Windows Server 2003, через который локальная сеть имеет выход в Интернет. Подключение к Интернету осуществлено через ADSL-модем. При этом сеть имеет единственный внешний адрес 81.195.117.138. Внутренние адреса ЛВС принадлежат подсети 192.168.115.0. Постоянный адрес ноутбука в данном случае значения не имеет, поскольку при подключении к Интернету через обычный модем он

получает динамически выделяемый адрес. Конкретное значение этого адреса тоже не имеет значения и в настройках соединения не применяется. В файлах конфигурации OpenVPN виртуальным сетевым адаптерам присваиваются адреса: 192.168.116.1 — для сервера и 192.168.116.2 — для ноутбука (удаленной рабочей станции). На рис. 6.20 схематично показана организация подключения к локальной сети через Интернет с использованием виртуальной частной сети.

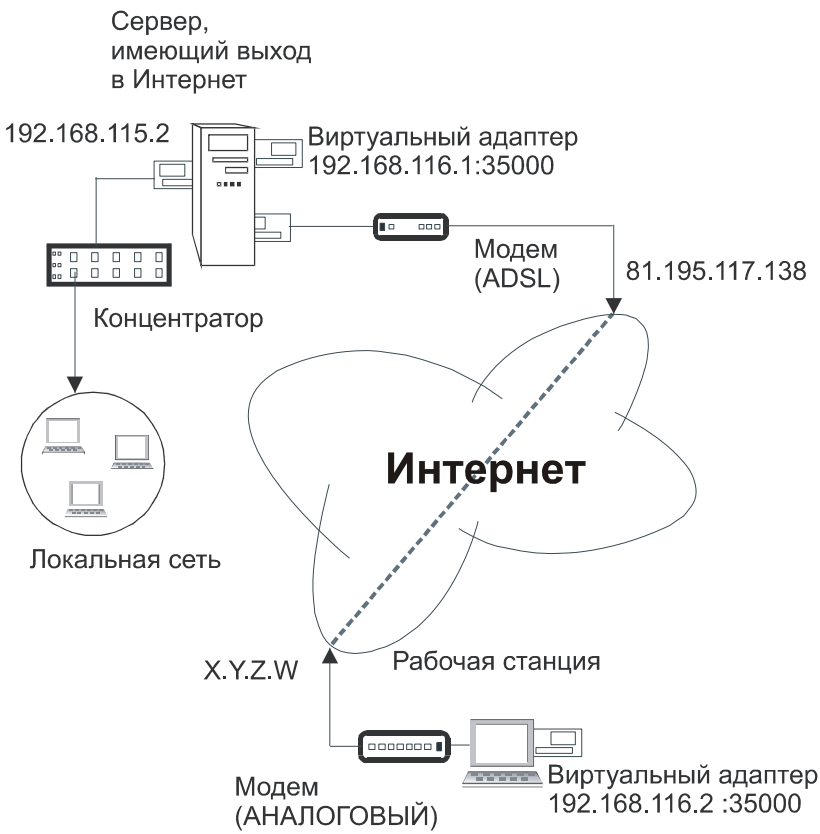


Рис. 6.20. Схема подключения к ЛВС через Интернет с применением VPN

Прежде всего необходимо обеспечить возможность ответа сервера на команду `ping`. Иногда администраторы намеренно запрещают эту возможность, пытаясь максимально обезопасить сеть от проникновения в нее извне. Но в нашем случае именно такое проникновение и готовится. При этом защищен-

ность сети не ухудшается, если не считать возможности простого обнаружения вашего компьютера (сервера) из Интернета. Ответ компьютера на команду `ping` запрещается, если включен брандмауэр и выключен параметр протокола ICMP (Internet Control Message Protocol) **Запрос входящего эха** (рис. 6.21).

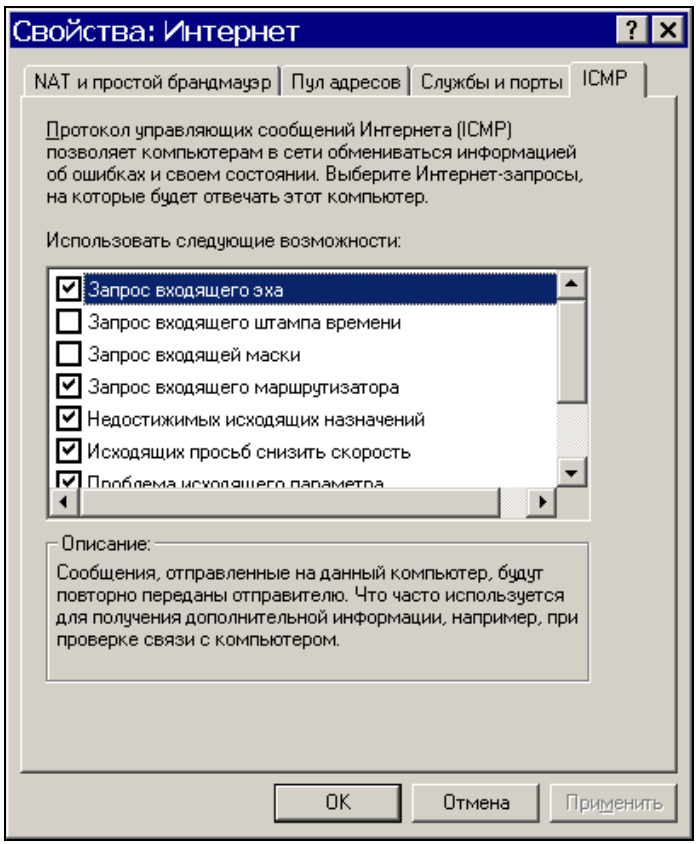


Рис. 6.21. Свойства интерфейса "Интернет", вкладка **ICMP**, параметр **Запрос входящего эха**

Компьютер, имеющий несколько сетевых подключений (соответственно, и несколько сетевых адаптеров), может иметь различные настройки брандмауэра для каждого из них. Тем более это относится к компьютеру, на котором настроено преобразование сетевых адресов (NAT). Поэтому, настраивая параметры сетевых подключений, будьте внимательны. Случайная ошибка при

установке параметров подключений к катастрофе не приведет, но заставит помучиться в поисках причин неудачи.

Когда вы убедились, что команда `ping` до сервера проходит нормально, время ответа не превышает 300 мс, а разброс значений этого времени невелик (не более 50%), можно продолжать настройки. Если время ответа больше, работа с удаленной рабочей станции с ресурсами локальной сети будет очень медленной. Но иногда достаточно даже медленной связи для выполнения необходимых процедур администрирования. Связь будет очень неустойчивой, если ответы на команду `ping` будут нерегулярными. В случае появления среди строчек ответов на экране сообщения "Превышено время ожидания" следует искать причины нарушения качества связи или выбрать другое время для подключения.

Защищенный канал связи, создаваемый в Интернете, работает через порт, который мы зададим в файлах конфигурации OpenVPN. Это значит, что на всем протяжении этого канала (рабочая станция — сервер провайдера 1 — Интернет — сервер провайдера 2 — сервер локальной сети) данный порт должен быть открыт.

В примере показано применение порта 35 000, но можно выбрать любое значение, не используемое на вашем сервере. Если есть сомнения в том, что выбранный вами порт открыт на каком-либо участке предполагаемого канала, его можно изменить. Если на сервере ЛВС не применяется какой-нибудь из известных сервисов, например POP3, то можно использовать стандартный для этого сервиса порт 110. Скорее всего, он будет открыт на всем протяжении канала VPN. Для того чтобы открыть этот порт на вашем сервере, следует настроить свойства интерфейса, подключенного к Интернету в оснастке **Маршрутизация и удаленный доступ**. На рис. 6.22 показано окно **Свойства: Интернет** с перечнем служб, доступных из Интернета. На рис. 6.23 показано окно изменения свойств службы с указанием на номер входящего и исходящего порта. Можно выбрать эти значения разными. В этом случае соответствующие значения должны быть указаны в файлах конфигурации на удаленной рабочей станции (значение для входящего порта) и на сервере (значение для исходящего порта).

Открыв используемый порт, необходимо настроить маршрутизацию IP-пакетов, передаваемых через Интернет. Это также делается в оснастке **Маршрутизация и удаленный доступ**, где необходимо указать статические маршруты (рис. 6.24). Один маршрут уже был указан, когда настраивался доступ к Интернету для пользователей сети. Теперь следует добавить еще два (один для основного, другой для виртуального сетевого адаптера).

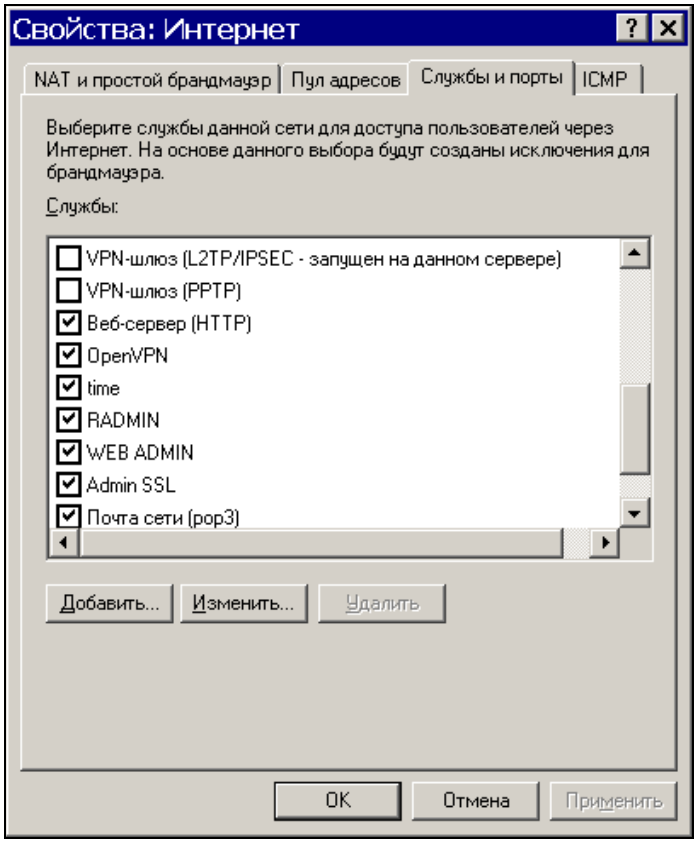


Рис. 6.22. Окно **Свойства: Интернет**
с перечнем служб, доступных из Интернета

В дальнейшем может понадобиться подключение других пользователей через VPN. Для этого потребуется создать несколько виртуальных адаптеров по числу создаваемых каналов и присвоить им имена с различными суффиксами. Причем для каждого канала следует запускать свой экземпляр OpenVPN-сервера, а в файле конфигурации каждого экземпляра указать соответствующее имя адаптера. Выбранный вариант маршрутов изменять не потребуется.

Создадим файлы конфигурации, подобные тем, что приведены ранее (см. листинги 6.1 и 6.2), но содержащие новые значения IP-адресов и портов, которые вы будете использовать.

Создадим файл секретного ключа с помощью пункта меню программы OpenVPN **Generate a static OpenVPN key** (Создать статический ключ) и по-

местим одну копию на OpenVPN-сервере, а другую — на OpenVPN-клиенте в папке с файлами конфигурации программы. Можно использовать и те файлы, что применялись на локальных машинах. Важно, чтобы на обеих машинах были копии одного и того же файла.

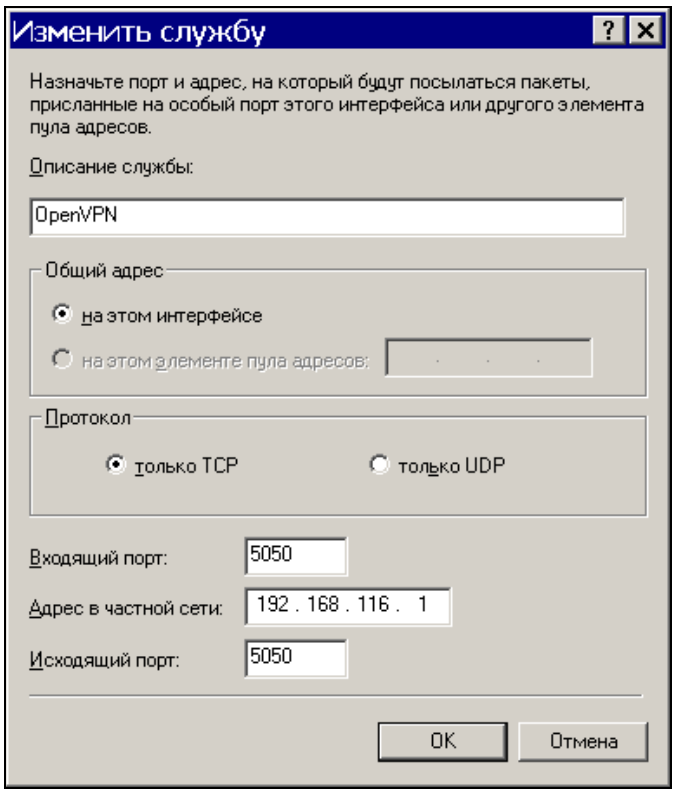


Рис. 6.23. Окно изменения свойств службы

На рабочей станции обычно специальных настроек не требуется. Должна быть установлена программа OpenVPN, а в папку с конфигурационными файлами программы помещены файл конфигурации клиента и секретный ключ.

Теперь можно запустить OpenVPN-сервер и попытаться установить соединение с рабочей станцией, подключенной к Интернету. Хорошо, если для проведения пробного подключения есть второй телефон. К сожалению, соединение dial-up по той же линии, к которой подключен ADSL-модем, не всегда

бывает достаточно хорошего качества, но, возможно, вам повезет, и вы сможете для эксперимента использовать одну телефонную линию.

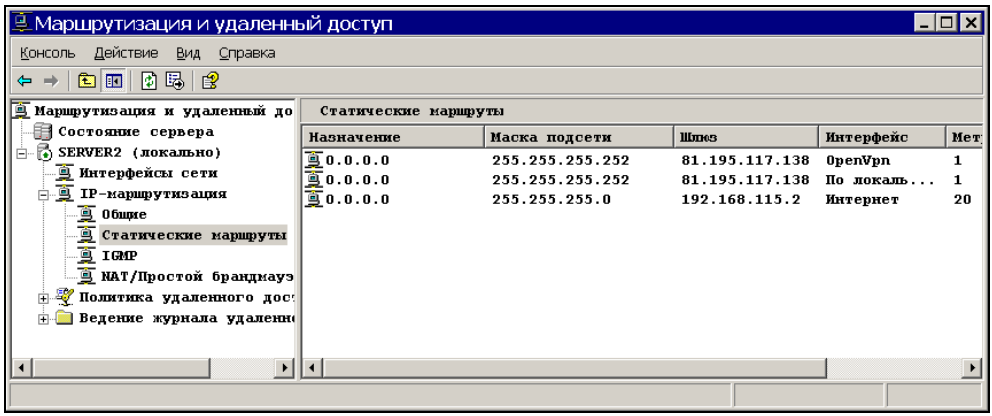


Рис. 6.24. Окно **Маршрутизация и удаленный доступ**, раздел **Статические маршруты**

На рабочей станции устанавливаем соединение с Интернетом через обычный модем и запускаем OpenVPN с использованием локального (клиентского) файла конфигурации. Программа делает несколько попыток соединения и, если все настроено верно, соединение устанавливается. Вы можете определить момент установки соединения по сообщению "Initialization Sequence Completed". В противном случае следует проверить настройки и качество соединения.

После установления соединения VPN откройте сетевое окружение на рабочей станции. Вы должны увидеть компьютер, к которому производилось подключение. Попытка открыть этот компьютер и получить доступ к ресурсам может оказаться неудачной, если для доступа к компьютеру требуется сертификат, а на рабочей станции его нет. Установите для входящего подключения на сервере проверку подлинности по имени пользователя и паролю. Это можно сделать на вкладке **Проверка подлинности** в окне свойств подключения. При работе в локальной сети может быть включен режим проверки подлинности по смарт-карте или сертификату, но при наличии доступа к сведениям о компьютере проверяется подлинность самого компьютера. В нашем случае связь оказывается односторонней. Удаленная рабочая станция не имеет постоянного IP-адреса, OpenVPN установила связь и идентифицировала клиента по своему секретному ключу, а сервер теперь хочет прове-

рить подлинность пользователя или компьютера при попытке доступа к его ресурсам. В этом случае можно установить проверку подлинности по имени пользователя и паролю (MD5-Challenge).

Можно, конечно, установить и настроить центр сертификации на сервере Windows Server 2003. Но это тема отдельного разговора.

Подключение к рабочим станциям сети

Если вам удалось подключиться к серверу сети или к компьютеру, имеющему непосредственное подключение к Интернету, то можно начинать настройку доступа к любой рабочей станции сети (рис. 6.25). Эта возможность позволяет любому пользователю (если вы настроили для него доступ) подключиться из дома к своему рабочему компьютеру. В нашей сети второй сервер, непосредственно подключенный к Интернету, имеет реальный IP-адрес в Интернете. У других компьютеров сети только внутренние адреса. Тем не менее есть возможность обеспечить доступ к этим компьютерам через VPN. Это возможно, потому что обращение к компьютерам происходит не только по IP-адресу, но и с использованием определенного порта. Если на стороне OpenVPN-клиента в файле конфигурации указать порт, отличающийся от того, который был применен для связи с сервером, а на сервере, подключенном к Интернету, создать маршрут к рабочей станции в локальной сети, OpenVPN-сервер на которой имеет этот же номер порта, то связь OpenVPN-клиента осуществится именно с этой рабочей станцией. Если применяется брандмауэр, то необходимо разрешить доступ из Интернета по этому номеру порта.

Настройте доступ по выбранному порту к рабочей станции, создав еще одну запись о службе OpenVPN подобно тому, как показано на рис. 6.10, но с именем, отличным от существующего (например, OpenVPN1), адресовав ее на соответствующий рабочей станции IP-адрес и указав выбранный для работы порт. Следует указать также статические маршруты (рис. 6.24) к рабочим станциям. Указывать их надо для интерфейса, подключенного к Интернету. Шлюз — адаптер, смотрящий в локальную сеть, назначение — IP-адрес рабочей станции в сети, маска подсети — 255.255.255.255.

Можно заранее настроить возможность доступа к нескольким рабочим станциям, выбрав для них различные номера портов. Если при организации удаленного доступа пользователя к своей рабочей станции подготовить отдельный ключевой файл, то кроме этого пользователя никто не сможет подключиться к его рабочей станции. Аналогично этот пользователь не сможет подключиться к другим рабочим станциям и серверам.

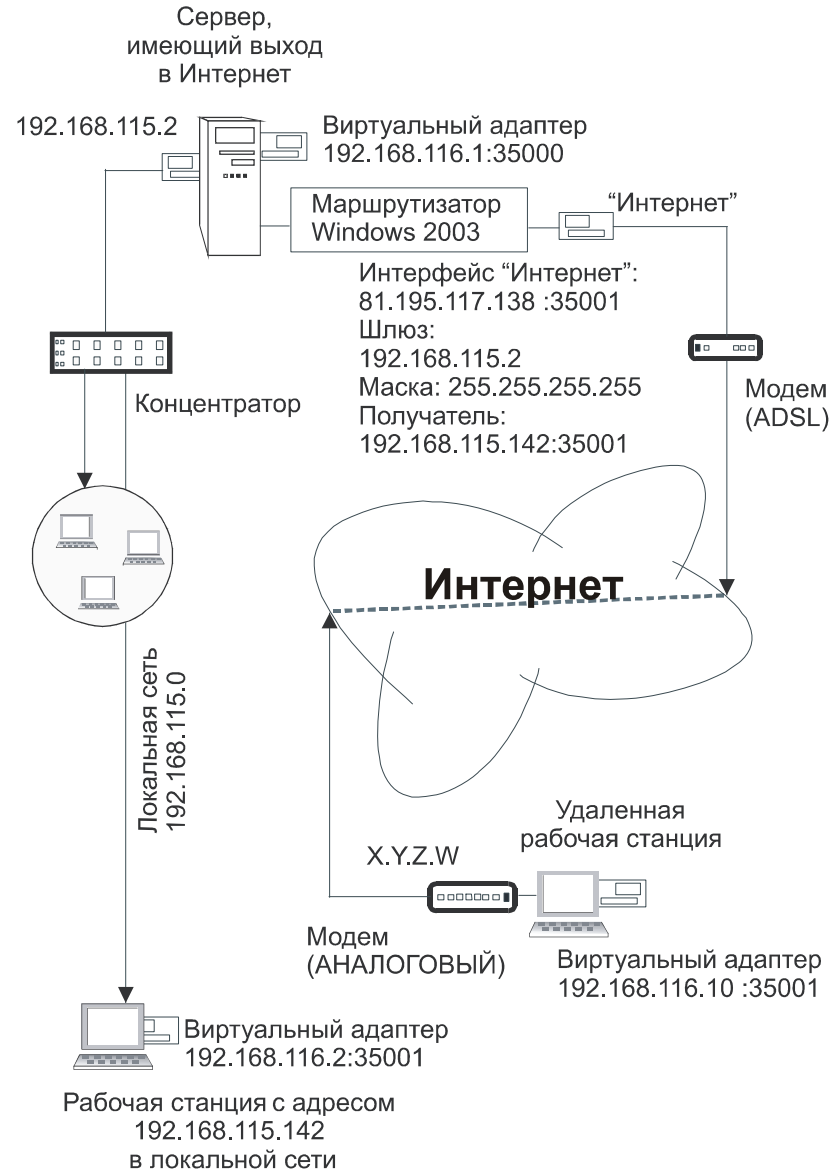


Рис. 6.25. Схема подключения к рабочей станции

При подготовке нескольких подключений следует дать понятные имена ключевым файлам, самим подключениям и файлам конфигурации, чтобы избежать путаницы.

Если ваш компьютер (рабочая станция) поддерживает работу с несколькими сетевыми адаптерами, то можно одновременно подключиться к рабочей станции в локальной сети и к серверу. Несмотря на то что в файлах конфигурации клиентов будет указано одно и то же имя удаленного компьютера, соответствующее IP-адресу сервера, подключение будет происходить к соответствующим рабочим станциям. При этом в сетевом окружении они будут появляться под своими именами. Таким образом, ваша работа на удаленной рабочей станции почти не будет отличаться от работы в локальной сети. Работу с несколькими виртуальными сетевыми адаптерами необходимо обязательно проверить в условиях, когда с одним адаптером все работает устойчиво. Если вместо сообщения "Initialization Sequence Completed" на экране будет появляться "Initialization Sequence Completed with Errors", когда установлено более одного виртуального адаптера, работа с сетевыми ресурсами может быть затруднена или невозможна.

В файлах конфигурации могут быть предусмотрены параметры, позволяющие улучшить надежность VPN-соединения и уменьшить время его восстановления при сбоях. Подробное описание всех возможных параметров приведено на сайте разработчиков OpenVPN, а здесь приведем еще раз содержимое файлов конфигурации сервера и клиента с некоторыми изменениями (листинги 6.3 и 6.4).

Листинг 6.3. Файл конфигурации для клиента OpenVPN Local.ovpn

```
remote server2 # необходимо в файле HOSTS указать IP-адрес
proto tcp-client
dev tap2
ifconfig 192.168.116.12 255.255.255.0
mssfix
dev-node den
secret den.txt
ping-restart 60
ping-timer-rem
persist-key
resolv-retry 86400

ping 10
comp-lzo
verb 4
mute 10
```

Листинг 6.4. Файл конфигурации для сервера OpenVPN Server.ovpn

```
port 35001
proto tcp-server
dev tap
ifconfig 192.168.116.142 255.255.255.0
dev-node <Имя подключения>
secret den.txt
ping 10
comp-lzo
verb 4
mute 10
```

В обоих файлах (один клиентский, другой — серверный) упоминается один и тот же файл ключа (копия). При этом имя ключевого файла можно изменять.

Если вам все удалось и вы довольны результатом — не торопитесь считать работу завершенной. Возможно, что вы не заметили "подводных камней".

О возможных проблемах и реальных перспективах

Несмотря на удобство доступа к компьютерам сети через VPN и защищенность канала связи, после удачно организованного доступа к сети не спешите вводить этот метод удаленной работы в "промышленную эксплуатацию". Это относится в равной мере ко всем новшествам, применяемым в вашей сети. Вполне может случиться, что новая программа или устройство, в том числе и виртуальное, станет конфликтовать с другими компонентами системы. Если обнаружится, что OpenVPN не уживается с какой-либо программой или службой, следует попытаться найти причины конфликта. Если это не удается, то можно попытаться разделить во времени конфликтующие процессы. Такие конфликты особенно вероятны, когда процессы запускаются на сервере. В нашей сети, например, при запуске OpenVPN на сервере пропадает удаленный доступ к одной из баз данных, обслуживаемых разработчиками только в режиме удаленного доступа. Возможны некоторые нарушения в работе локальной сети. Но все эти проблемы могут быть успешно решены. Важно внимательно отнестись к анализу работоспособности сети, попытаться в короткое время получить максимум сведений о состоянии системы. Если не

замечено никаких проблем, связанных с применением VPN, то начинайте использовать эту возможность в повседневной работе. Тем не менее, если вы решили получать доступ к рабочей станции, нет смысла оставлять работающей OpenVPN, когда вы находитесь непосредственно около этого компьютера. Для сервера можно рассмотреть возможность запуска программы только при необходимости с помощью средств удаленного администрирования или через планировщик задач. Если конфликтов не обнаружено, то OpenVPN может быть запущена постоянно. Ресурсы, которые требуются программе, для современных компьютеров незначительны.

Обычно конфликтов не наблюдается, когда осуществляется доступ пользователя к своей рабочей станции, и при этом никто более не работает за этим компьютером.

Следует учитывать, что проект OpenVPN активно развивается. Уже сейчас OpenVPN позволяет организовать связь с компьютерами, работающими в разных сетях, имеющих выход в Интернет, причем в одной из них может не быть компьютеров с реальными IP-адресами, как при подключении dial-up, например. Во многих домашних (городских, районных) сетях доступ в Интернет организован через VPN. Это тоже не помеха для OpenVPN. До момента, когда каждый компьютер сможет иметь свой IP-адрес, а это произойдет после повсеместного внедрения протокола IPv6, OpenVPN будет помогать компенсировать отсутствие реального IP-адреса у вашего компьютера благодаря технологиям, примененным при разработке этой программы.

Виртуальные технологии существенно расширяют возможности администратора сети независимо от ее сложности. Имея один-два достаточно мощных компьютера, можно моделировать довольно сложные участки реальных сетей, испытывать программные продукты, которые на реально работающем сервере или рабочей станции вы не решились бы запустить. Бывает, что для решения каких-либо задач необходим сервер с настройками, в корне отличающимися от настроек вашего рабочего сервера. Вы можете создать и сохранить несколько конфигураций компьютеров, которые будете запускать по мере необходимости. Освоив виртуальные технологии, вы во многих случаях сможете сэкономить материальные и временные ресурсы.

Ну, вот и все

Организация сети в любом из возможных вариантов требует как от руководителя, так и от исполнителя творческого подхода. Надеюсь, что эта книга

помогла вам сориентироваться в информационных просторах и найти для своей сети оптимальное решение как с точки зрения конструктивного исполнения, так и с точки зрения идеологии. Не следует усложнять проблему, когда решение лежит на поверхности. Зачем удорожать систему включением в нее выделенного сервера, когда требуется связь с соседом сверху? Две сетевые карты и кабель решат все проблемы. Позже сеть может развиваться и совершенствоваться по мере подключения новых пользователей и выдвижения новых требований. Но следует помнить и о том, что невозможно угодить всем. Определенные ограничения всегда будут существовать — "нельзя объять необъятное". И все же при творческом подходе бóльшую часть проблем вам удастся решить. Не пренебрегайте помощью и советами бывалых. Они прошли огонь и воду, и их опыт бесценен. Много информации можно обнаружить в Интернете и других сетях. Ссылки на адреса в Интернете, приведенные в книге, были действующими на момент сдачи рукописи. Возможно, что теперь что-то изменилось (Интернет быстро меняется). Большую помощь вам окажет поисковая система **www.google.ru**, которая по мнению автора является, пожалуй, лучшей русскоязычной поисковой системой.

В заключение приведем статью, найденную в Интернете (**http://www.telecoms.ru/document_228195.html**). Опубликована она была в марте 2000 года, но ценность ее сохраняется (статья приводится с незначительными изменениями).

Советы бывалого

История создания домашних компьютерных сетей в большинстве случаев практически одинакова. Различны варианты развития.

Что касается нашей сети Интерлан, то начиналось все просто: возникла идея соединить два компьютера. Сказано — сделано. А дальше произошел ряд случайных событий, которые и подвигли к созданию сети.

В одном из журналов появилась статья о домашней сети на улице Удальцова. Тогда впервые появилась мысль, а почему бы и нет? Затем была еще телепередача, а вслед за ней пришло осознание необходимости и незаменимости домашней сети.

Но этот этап для всех является лишь чем-то вроде небольшого испытания, хотя на самом деле препятствия еще впереди, и не для всех они легко преодолимы. Но вот окончательное решение о создании сети принято, и что дальше? Главная задержка возникает, когда создатели пытаются понять, на кого все это будет рассчитано, кто же все-таки станет потребителем услуг этой сети. Почти любая домашняя сеть начинается с организации "площадки" для игр и обмена различными ресурсами, но, как показывает

практика, сеть с такой ориентацией лишена будущего и в дальнейшем не приносит своим создателям ничего, кроме головной боли.

Следовательно, для ее успешного развития требуется обеспечить доступ в Интернет. И здесь мы снова возвращаемся к потребителю: я знаю сети, которые давно вышли из младенческого возраста и доросли до приличных размеров, но из-за своей ориентации на развлекающуюся молодежь до сих пор только мечтают о канале в Интернет. Поэтому в дальнейшем прекращаем рассматривать сеть как площадку для игр. Возникает резонный вопрос: так что же все-таки нужно делать?

Совет 1

Если вы решили организовать сеть с выходом в Интернет по высокоскоростному каналу, организуйте собрание жильцов, составьте списки, выявите желающих и объясните людям преимущества работы в сети. Самое главное — необходимо запомнить, что в этом случае вы уже не обойдетесь только благими намерениями и горячим желанием. Пытайтесь учиться на чужих ошибках и прислушивайтесь к советам тех, кто через все это уже прошел.

Но вот уже собрание позади, желающих хоть отбавляй. Пора переходить от разговоров непосредственно к воплощению, т. е. к созданию сети.

Совет 2

Не растягивайте два первых, важных этапа во времени, иначе люди могут передумать, расценят задержку как ваше желание пропасть, и вы окажетесь вновь только со своею мечтой.

Совет 3

Не стоит начинать организацию сети, если вы не нашли хотя бы 20 человек, желающих воспользоваться этой услугой, в противном случае вам придется оплачивать все самостоятельно. Поэтому все цифры приведены из расчета на 20 человек.

Совет 4

И, самое главное, не забывайте, что вам большей частью придется общаться не с компьютерами, кабелями и прочими привычными для вас вещами, а с людьми.

Сперва вам придется рассчитать начальные вложения, которые потребуются для организации сети и непосредственно самого канала в Интернет.

Для этого необходимо определиться с топологией вашей будущей сети (стандартно используется топология "шина — звезда", но не будем уходить далеко от нашей темы и вдаваться в терминологию — для этого есть уйма книг; в конце концов можно обратиться к тем, кто это воплотил) и с прокладкой магистралей между домовыми ЛВС. С учетом нынешних цен ваши затраты составят ориентировочно $1700.

Что касается самого канала, на практике большинство домашних сетей используют радиоканалы, так как этот вид относительно дешев, да и при современных технологиях скорость доступа по радиоканалу составляет от 2 до 11 Мбит/с. Вместе с платой за подключение непосредственно к сети провайдера канал вам обойдется еще около $1500. Значит, всего ваш вклад в сеть составит $3200.

Бег с препятствиями

Вроде со всем определились, все закупили, даже оборудование настроили. Пора, собственно, заниматься подключением квартир и протяжкой магистралей — на самом деле вы как раз и подошли к самому трудному этапу, где вам предстоит преодолеть множество препятствий.

Итак, самое первое препятствие, с которым вы столкнетесь, — протяжка магистрали, даже не столько она сама, сколько то, что ей предшествует. Правда, если вы решили сделать сеть только в своем доме, то никаких проблем, скорее всего, не будет, достаточно заручиться поддержкой жильцов и председателя вашего жилищного кооператива — в таком случае вас можно поздравить, ибо практически все проблемы у вас позади и вы можете полностью отдаться делу создания сети.

Но сеть в одном доме неперспективна, и поэтому проблемы возникнут, как только ресурсы вашего дома иссякнут, и появится необходимость в расширении сети.

Можно, конечно, продолжить успешное начинание и договариваться в дальнейшем с председателями остальных домов, но очень часто на деле оказывается, что для большинства людей, с которыми вам предстоит общаться, ваш успех — это далеко не главный и решающий фактор.

Итак, что же нужно в дальнейшем?

Получить разрешение в органах самоуправления. И это есть самая сложная задача, так как эта сеть нужна вам и еще раз вам. Никто помогать вам в этом не будет.

А самым трудным будет, как вы догадываетесь, получить первое разрешение.

Хотите знать, зачем оно вам нужно?

Для того чтобы вы смогли попадать в технические помещения и просто на этажи.

При получении этого разрешения наблюдается следующая закономерность: чем ниже ранг начальника, тем он больше требует бумаг, лицензий и прочих документов, которых у вас, конечно, нет, как нет возможностей и денег их получить, да это и не входит в ваши планы. Ну, например, зачем вам нужна строительная лицензия, которую непременно потребуют от вас в РЭУ? Очевидно, что этап получения бумаг, хоть как-то легализующих ваше положение, потребует массу сил и энергии. Получение этой маленькой бумажечки отняло у нас около полутора месяцев драгоценного времени, которое вместо полезной плодотворной деятельности было потрачено на обивание порогов в кабинетах различных начальников из РЭУ и привело к тому, что в боях с бюрократией потерялось большое количество желающих.

Не хотелось бы запугивать, так как и из правил бывают исключения, наше первое разрешение далось очень тяжело и то только тогда, когда вопрос был поставлен на таком высоком уровне, что дальше, как говорится, только Кремль.

Совет 5

Для того чтобы все-таки получить долгожданное и необходимое разрешение, обращайтесь напрямую в более высокие инстанции, чем РЭУ, РУ и им подобные.

Составьте проект вашей сети (это потребуется обязательно, причем некоторые из прошедших через это не обошлись одними только распечатками карт местности с отметками карандашиком, где должен быть провод, — им пришлось добывать чертежи домов в разрезах и в масштабе, но это тоже, скорее, исключение), приложите туда образцы кабелей, коннекторы и прочие сетевые атрибуты для наглядности, подготовьте материалы, на которые вы сможете сослаться в ходе вашей беседы, статьи в прессе о сетях и Интернете в целом и, самое главное, сразу говорите, что вы являетесь инициативной группой жильцов дома, которым препятствуют в исполнении благородного дела, — "интернетизации" жилого массива.

И вот вам выдали бумажку с гербовой печатью (не забудьте отметить это с соратниками) от дирекции единого заказчика, а теперь смело бегите в РЭУ и заключайте с их начальником договор об использовании кровли, технических помещений и электростояков для прокладки вашего кабеля и, конечно же, на выдачу ключей под вашу ответственность. После этого бегите к председателям и заключайте договоры с ними (обычно соглашаются и проблем не возникает).

Но бывают и тут нестандартные ситуации — вас просят оказать различную посильную помощь (чердак прибрать, мусор вывезти, коего очень много, а убирать некому, помещение правления отремонтировать, да мало ли чем помочь нужно), но это все решаемо: если не хотите помогать, есть два варианта: либо пожертвуйте деньги на благоустройство дома (очень часто помогает, но встречаются и такие председатели, которые хотят благоустраиваться постоянно и не за счет основных средств), либо просто уходите, если есть куда уйти.

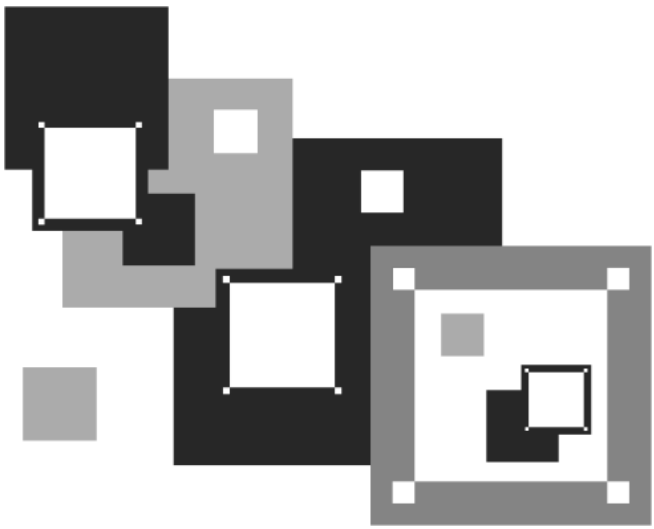
Вот и все: нужные и ненужные бумаги у вас на руках, времени на это вы потратили не много, желающие еще не разбежались, и можно приступать.

Протянуть магистраль, создать серверную, настроить оборудование, вдохнуть в него жизнь, а точнее, Интернет... и вперед.

Дальше, конечно, тоже ждут некоторые неожиданности и сложности, например у нас поначалу возникали казусы с количеством используемого кабеля, которого, к нашему удивлению, на подключение одного пользователя уходило подчас больше, чем на протяжку одного из сегментов нашей магистрали, но это уже совершенно другая история.

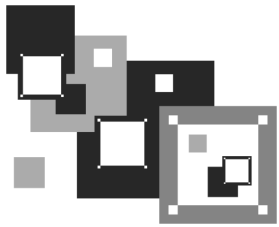
Михаил Данилевич

"Контакт. Связь в жизни"/TELECOM.RU



Приложения

Приложение 1



Настройка рабочих станций с различными операционными системами для работы с выделенным сервером

Описываемые здесь настройки можно применять (с небольшими корректировками) и для работы с невыделенным сервером, даже в одноранговой сети. Важно "научить" компьютеры видеть друг друга в сети и обмениваться информацией. Работа с выделенным сервером требует применения наибольшего числа параметров настройки рабочих станций, поэтому мы и будем рассматривать этот вариант работы сети.

Настройка рабочих станций с операционной системой DOS

Начнем с рабочих станций под управлением DOS. Несмотря на бурный прогресс в области вычислительной техники и прекращение поддержки MS-DOS, в нашей стране еще работают компьютеры под управлением различных версий этой операционной системы, причем количество их весьма велико. Для доступности и универсальности подхода мы рассмотрим MS-DOS 7.1, которая входит в состав Windows 98. Несложно, выполнив команду `Sys C:`, перенести эту систему с загрузочной дискеты Windows 98 на винчестер. Вы можете применить и другие DOS, под управлением которых работают ваши компьютеры. Различные версии DOS требуют разной конфигурации памяти. Некоторые версии этой операционной системы могут работать в нашей сети не совсем так,

как MS-DOS 7.1. Но если нет необходимости применять какую-либо особенную версию DOS, то почему бы не использовать MS-DOS 7.1, которая поддерживает файловую систему FAT32 и достаточно просто настраивается.

Установка операционной системы MS-DOS 7.1

Для установки и настройки этой операционной системы необходимо перенести системные файлы с загрузочной дискеты Windows 98 и дописать самостоятельно файлы конфигурации. Все файлы нужно готовить в текстовом редакторе под управлением DOS. Можно использовать встроенный в Windows 9*x* редактор Edit.com.

Условимся, что каталог, в который устанавливается DOS, называется DOS7. В него будут помещены все необходимые файлы для работы системы, кроме основных системных файлов. В корневом каталоге диска C: должны находиться файлы, содержание которых приведено далее (листинги П1.1—П1.4).

Листинг П1.1. Файл Msdos.sys

```
[Paths]
WinDir=c:\dos7\
WinBootDir=c:\
HostWinBootDrv=c:\

[Options]
BootMulti=0;Отключает возможность множественной загрузки
BootGUI=0  ;Отключает загрузку графического интерфейса
Network=1  ;Включает возможность работы с сетью
logo=1     ;Позволяет показывать заставку (файл Logo.sys) при загрузке
```

Этот файл уже существует на диске после переноса системных файлов и его необходимо исправить в соответствии с приведенным текстом. Заставку вы можете изготовить самостоятельно, создав в корневом каталоге файл Logo.sys из растрового рисунка с разрешением 320×400 точек.

Листинг П1.2. Файл Config.sys

```
[menu]
menuitem=D, Use Net ;В этом разделе создается меню для
menuitem=C, No net ;выбора вариантов загрузки
```

```
menudefault=D,10
menucolor=14,1
[D]
device=c:\dos7\himem.sys
dos=high,umb noauto
devicehigh=emm386.exe noems
devicehigh c:\net\ifshlp.sys
[C]
device=c:\dos7\himem.sys
dos=high,umb noauto
devicehigh=emm386.exe noems
[COMMON]
fileshigh=80
buffershigh=20
stackshigh=9,256
lastdrivehigh=z
INSTALLHIGH=C:\DOS7\RKM.COM  ;Загрузка русификатора, который можно
                             ;найти по ссылке:
                             ;http://win95.nm.ru/switch.htm
shell=c:\command.com /E:512 /P
FCBSHIGH=1
```

Вы можете самостоятельно изменить некоторые строки. Например, русификатор может быть любым другим, но будет лучше, если вы повторите пример полностью. Файлы emm386.exe, ifshlp.sys, choice.exe и himem.sys можно скопировать из Windows.

Листинг П1.3. Файл Autoexec.bat (вариант для начальной установки системы)

```
@echo off
set temp=c:\temp
path c:\;C:\NC;c:\dos7
lh c:\dos7\mouse

@echo "ПРИЯТНОЙ РАБОТЫ!"
```

Необходимо самостоятельно создать каталог TEMP, установить Norton Commander или другой файловый менеджер, скопировать в каталог DOS7 драйвер мыши (можно из Windows).

Листинг П1.4. Файл Autoexec.bat (окончательный вариант)

```
@echo off
set temp=c:\temp
path c:\;C:\NET;C:\NC;c:\dos7
lh c:\dos7\mouse
choice /c:SNLA /t:L,20 "Share-S сеть- N локально- L  АРАХНА- A  "
;Команда choice соответствует choice.exe из Windows.
if errorlevel 4 goto p
if errorlevel 3 goto l
if errorlevel 2 goto n
C:\NET\net initialize
C:\NET\netbind.com
C:\NET\umb.com
C:\NET\tcptsr.exe
C:\NET\tinyrfc.exe
C:\NET\nmtsr.exe
C:\NET\emsbfr.exe

C:\NET\net start
C:\NET\net start server
C:\NET\net share
cls
@echo "Сеть с доступом загружена Ctrl+Alt+N подкл.диск"
@echo "netshare — обеспечить доступ"
net
c:\net\netshare.exe
goto l

:n
C:\NET\net initialize

C:\NET\netbind.com
C:\NET\umb.com
C:\NET\tcptsr.exe
C:\NET\tinyrfc.exe
C:\NET\nmtsr.exe
C:\NET\emsbfr.exe
```

```
C:\NET\net start
cls
@echo "Сеть загружена"
net

goto l
:p  ;этот раздел файла необходим, если применяется браузер "Арахна"
c:\drv\pktdrv\hppclanp 0x60 ;пакетный драйвер сетевой платы должен быть
                            ;свой
cd\
cd arachne
arachne
:l
@echo "ПРИЯТНОЙ РАБОТЫ!"
```

Этот вариант файла пока не устанавливайте, а сохраните до заключительных действий по настройке сетевых возможностей рабочей станции DOS. В процессе установки сетевого программного обеспечения файл будет изменяться автоматически, но его окончательный вид должен быть таким, как в листинге П1.4. Кроме приведенных файлов вам могут понадобиться и другие. В табл. П1.1—П1.3 дан примерный перечень файлов, которые можно скопировать с загрузочной дискеты и из \Windows\Command в соответствии с их размещением на диске, полученном командой `DIR`.

Таблица П1.1. *Содержимое диска C:*

Название файла или папки	**Размер файла, байт**	**Описание**
COMMAND.COM	95 202	Командный процессор
NC <ПАПКА>		Norton Commander
NET <ПАПКА>		Каталог установки клиента
DISTRIB <ПАПКА>		Дистрибутивы
EMM386.EXE	125 975	EMM386
ARACHNE <ПАПКА>		Браузер ARACHNE
TEMP <ПАПКА>		Папка для временных файлов

Таблица П1.1 *(окончание)*

Название файла или папки	Размер файла, байт	Описание
DRV <ПАПКА>		Хранилище драйверов
DOS7 <ПАПКА>		Системный каталог
MSDOS.SYS	116	Файл MS-DOS
CONFIG.SYS	432	Файл MS-DOS
LOGO.SYS	129 078	Заставка
AUTOEXEC.BAT	869	Файл MS-DOS

Таблица П1.2. *Содержимое папки C:\DISTRIB*

Название файла или папки	Размер файла, байт	Описание
ARCHN170.EXE	1 012 717	Браузер ARACHNE
CYRILLIC.APM	279 421	Пакет русификации для ARACHNE
DSK-1 <ПАПКА>		Клиент
DSK-2 <ПАПКА>		Клиент
DSK3-1.EXE	864 723	Клиент
DSK3-2.EXE	288 142	Клиент

Таблица П1.3. *Содержимое папки C:\DOS7*

Название файла или папки	Размер файла, байт	Описание
COMMAND.COM	95 192	Командный процессор
COUNTRY.SYS	30 742	Файл MS-DOS
DEBUG.EXE	20 874	Файл MS-DOS

Таблица П1.3 *(окончание)*

Название файла или папки	Размер файла, байт	Описание
DISPLAY.SYS	17 239	Файл MS-DOS
EDIT. COM	70 318	Текстовый редактор
EGA3.CPI	58 753	Файл MS-DOS
EMM386.EXE	25 975	Файл MS-DOS
FDISK.EXE	64 588	Файл MS-DOS
FORMAT.COM	50 071	Файл MS-DOS
HIMEM. SYS	33 191	Файл MS-DOS
IFSHLP.SYS	3708	Файл MS-DOS
KEYB.COM	20 135	Файл MS-DOS
KEYBRD3.SYS	31 633	Файл MS-DOS
MEM. EXE	32 338	Файл MS-DOS
MODE.COM	29 911	Файл MS-DOS
MOUSE.COM	34 747	Драйвер мыши
RKM.COM	41 000	Русификатор
SCANDISK.BAT	152	Файл MS-DOS
SCANDISK.EXE	50 977	Файл MS-DOS
XCOPY.EXE	3910	Файл MS-DOS
MSDOS.SYS	108	Файл MS-DOS
TEMP <ПАПКА>		Папка для временных файлов
CHOICE.COM	1610	Файл MS-DOS
DISPLAY.CPI	88 045	Файл MS-DOS
UTIL <ПАПКА>		Папка с утилитами

Вы можете самостоятельно корректировать состав необходимых вам файлов.

Теперь, если система загружается, можно начать установку сетевого программного обеспечения. Для начала скопируйте файлы dsk3-1.exe, dsk3-2.exe, nnet.exe и netshar.exe, пользуясь следующими ссылками:

- **ftp://ftp.microsoft.com/Softlib/MSLFILES/netshar.exe**;
- **ftp://ftp.microsoft.com/softlib/mslfiles/nnet.exe**;
- **ftp://ftp.microsoft.com/bussys/Clients/MSCLIENT/dsk3-1.exe**;
- **ftp://ftp.microsoft.com/bussys/Clients/MSCLIENT/dsk3-2.exe**.

dsk3-1.exe, dsk3-2.exe — это дистрибутив MS Client для DOS, nnet.exe и netshar.exe — обновления для клиента. Создайте на диске C: директорию \DISTRIB и поместите туда полученные файлы. Эти файлы позволят включить рабочие станции под управлением DOS в сеть.

Установка Microsoft Network Client Version 3.0 for MS-DOS

Перед началом установки выполните следующее:

1. Создайте каталоги: \DISTRIB\DISK1 и \DISTRIB \DISK2.
2. Скопируйте в них dsk3-1.exe и dsk3-2.exe.
3. Распакуйте файлы, запустив их на выполнение.
4. Перейдите в каталог DISTRIB\DISK1 и запустите setup.exe.
5. На экране появится окно программы установки клиента. Нажмите клавишу <Enter>.
6. В окне выбора каталога установки, ничего не меняя, нажмите клавишу <Enter>. Клиент будет установлен в каталог C:\NET.
7. На экране появится окно проверки системы. Дождитесь окончания проверки. Если компьютер долго не подает признаков жизни, перезагрузите его.
8. В окне выбора сетевого адаптера выберите тип вашей сетевой карты, перемещаясь по строкам клавишами со стрелками. Если ваш адаптер в списке отсутствует, выберите пункт ***Network adapter not shown on list below** (Сетевой адаптер отсутствует в списке). При этом надо указать путь к драйверу вашей сетевой карты, введя его с клавиатуры. Можно использовать драйвер с дискеты, прилагаемой к устройству, или найти его в Интернете.

9. Следующим появится окно **Set Network Buffers** (Оптимизация памяти). Если вы используете описанные ранее системные файлы, то нажмите клавишу <Enter>.

10. В появившемся окне введите имя пользователя. Вы можете выбрать любое имя длиной не более 20 символов. В нашем примере используется имя компьютера serdos и имя пользователя Admin. Имя компьютера можно будет ввести на следующем этапе, при корректировке настроек.

11. Далее потребуется скорректировать сетевую конфигурацию компьютера. Клавишами со стрелками выберите **Change Network Configuration** и нажмите клавишу <Enter>.

12. На следующем экране (рис. П1.1) можно перемещаться между окнами клавишей <Tab>, а внутри каждого окна — клавишами со стрелками. Установив курсор на пункт в верхнем окне, перейдите с помощью клавиши <Tab> в нижнее для выбора необходимого действия.

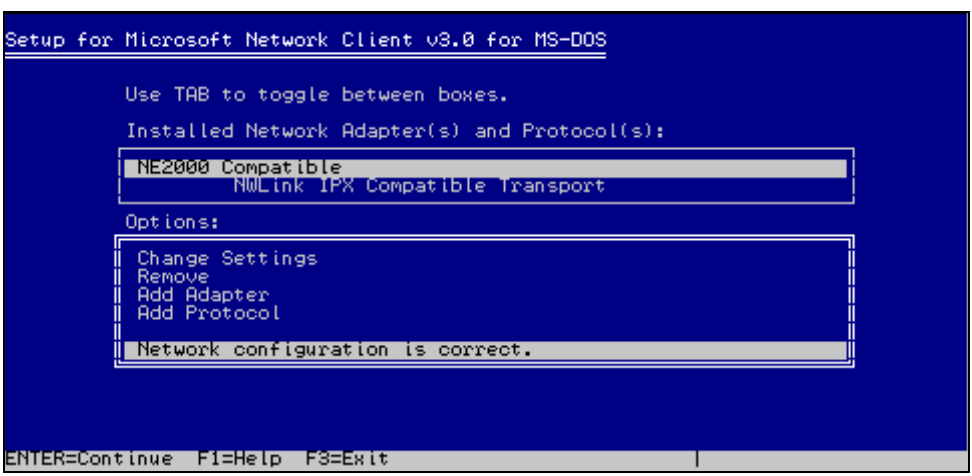


Рис. П1.1. Один из экранов
Setup for Microsoft Network Client v3.0 for MS-DOS

13. Если сетевой адаптер установлен верно, то, скорее всего, его настройки менять не надо, но необходимо установить сетевые протоколы, которые используются в нашей сети. Для этого следует установить курсор на имя сетевого протокола, перейти в нижнее окно с помощью клавиши <Tab> и выбрать **Add Protocol**. Нам потребуется добавить Microsoft TCP/IP и

Microsoft NetBEUI. Протокол, который предлагался по умолчанию, следует удалить (**Remove**).

14. Теперь необходимо настроить протокол Microsoft TCP/IP. Установив курсор на имя протокола, в нижнем меню выберите **Change Settings** (Изменить настройки).

    Если в вашей сети есть DHCP-сервер, то можно ничего не трогать и пропустить настройку TCP/IP, но лучше установить IP-адрес из зоны зарезервированных адресов, т. е. адресов, которые не изменяются DHCP-сервером. Это позволит работать в любой сети, минимально изменив настройки. На сервере WINS при этом желательно создать статическое сопоставление адреса и имени. Как изменить настройки сервера, будет показано после описания установки клиента. В нашем примере используется адрес 192.168.0.126. Маска подсети — 255.255.255.0. Вместо точек вводятся пробелы.

    ВНИМАНИЕ!

    Если адрес ввести с точками вместо пробелов, то во время загрузки сети будет выведено на экран множество сообщений об ошибках и невозможности загрузить тот или иной драйвер.

15. Если все введено правильно, выберите **The listed options are correct** (Список настроек верен).

Аналогично можно изменить и настройки сети — имя компьютера, имя пользователя, имя рабочей группы и имя домена. Два последних имени в нашем случае должны совпадать. Проверить правильность настроек и подправить их можно позже, изменяя настройки напрямую в файлах конфигурации, которые будут созданы в процессе установки. После нажатия **The listed options are correct** начнется процесс копирования файлов, по завершении которого компьютер выдаст запрос на перезагрузку. Если в дисководе была дискета, выньте ее и нажмите клавишу <Enter>.

Подключите компьютер к сети. Если все настройки выполнены верно, то после перезагрузки компьютера появится надпись: **Type your user name, or press ENTER if it is USER** (Напечатайте ваше имя или нажмите ENTER, если оно, в данном случае, Admin). Если это ваше имя, то нажмите клавишу <Enter>. Или наберите другое имя и тоже нажмите <Enter>.

Появится строка **Type your password:** (Напечатайте ваш пароль). Введите пароль. Вместо букв будут выводиться звездочки, затем нажмите <Enter>.

На экран будут выводиться следующие сообщения, выделенные в тексте жирным шрифтом.

There is no password-list file for USER. Do you want to create one? (Y/N) [N]: (Отсутствует запись паролей для Admin. Хотите создать?)

Нажмите клавишу <Y>, потом — <Enter>.

Please confirm your password so that a password list may be created: (Пожалуйста, подтвердите пароль для создания записи паролей).

Еще раз введите пароль.

The command completed successful (Команда выполнена полностью).

Теперь ваш компьютер в сети. Но если все произошло иначе и нет входа в сеть, не отчаивайтесь. Сначала продолжим установку клиента (она еще не завершена), а затем проверим все настройки по содержимому файлов конфигурации.

Установите обновления для клиента. Для этого перезагрузите компьютер. При загрузке выберите пункт меню **No net** (Без сети). Это позволит освободить память для процесса установки. Файлы nnet.exe и netshar.exe скопируйте в каталог C:\NET и распакуйте их, запустив на выполнение. Теперь замените файл Autoexec.bat на заранее подготовленный. Проверьте содержание файлов конфигурации клиента. Это два файла в каталоге C:\NET — Protocol.ini и System.ini. Содержание файлов с комментариями приведено в листингах П1.5 и П1.6, но оно может несколько отличаться в зависимости от применяемого сетевого адаптера. Тем не менее основные настройки, которые не связаны с типом сетевого адаптера, должны быть такими же.

Листинг П1.5. Файл Protocol.ini

```
[network.setup]
version=0x3110
netcard=hwp$27247b,1,HWP$27247B,1
transport=tcpip,TCPIP
transport=ms$ndishlp,MS$NDISHLP
transport=ms$netbeui,MS$NETBEUI
lana0=hwp$27247b,1,tcpip
lana1=hwp$27247b,1,ms$netbeui
lana2=hwp$27247b,1,ms$ndishlp
;В этом разделе сведения о драйвере сетевого адаптера и установленных
;протоколах.
```

```
[TCPIP]
NBSessions=6
;Замените в следующих строках адреса сервера и компьютера на свои
WINS_SERVER0=192 168 0 15     ;адрес сервера
DefaultGateway0=192 168 0 15  ;адрес сервера
SubNetMask0=255 255 255 0     ;маска подсети
IPAddress0=192 168 0 126      ;адрес компьютера
DisableDHCP=0
DriverName=TCPIP$
BINDINGS=HWP$27247B
LANABASE=0

[protman]
DriverName=PROTMAN$
PRIORITY=MS$NDISHLP


[HWP$27247B]
DriverName=HPLANP$

[MS$NDISHLP]
DriverName=ndishlp$
BINDINGS=HWP$27247B


[MS$NETBEUI]
DriverName=netbeui$
SESSIONS=10
NCBS=12
BINDINGS=HWP$27247B
LANABASE=1
```

Листинг П1.6. Файл Sistem.ini

```
[network]
filesharing=yes
printsharing=yes
```

```
;два предыдущих значения становятся равными "NO" при запуске настройки
;параметров командой Setup, поэтому после изменения свойств сетевого
;адаптера или его смене восстановите "YES", иначе не будет доступа
;к компьютеру из сети.
autologon=no
;autologon=yes
computername=SERDOS ;Замените на имя вашего компьютера
lanroot=C:\NET
username=ADMIN ;Замените на ваше сетевое имя
workgroup=AP15 ;Замените на имя вашей рабочей группы (имя домена)
reconnect=yes
dospophotkey=N
lmlogon=1
logondomain=AP15 ;Замените на имя вашей рабочей группы (имя домена)
preferredredir=full
autostart=full,popup
maxconnections=8

[network drivers]
netcard=hplanp.dos
transport=tcpdrv.dos,nemm.dos,ndishlp.sys,*netbeui
devdir=C:\NET
LoadRMDrivers=yes

[386enh]
TimerCriticalSection=5000
UniqueDosPSP=TRUE
PSPIncrement=2

[Password Lists]
*Shares=C:\NET\Share000.PWL
ADMIN=C:\NET\ADMIN.PWL ;Изменяется при регистрации пароля на локальном
                       ;компьютере
NET=C:\NET\NET.PWL
```

После корректировки файлов сохраните их резервные копии. При изменении этих файлов самой системой, например после запуска Setup.exe для корректировки настроек, проверяйте содержание файлов конфигурации с помощью текстового редактора.

Если все настройки верны, то при загрузке сети (пункт загрузочного меню **Use Net**), система предложит указать сетевой диск для подключения, далее для выбора компьютера и доступных ресурсов запустится специальный браузер. После выбора сетевых ресурсов система предложит предоставить сети свои ресурсы. Осталось настроить сервер для работы с нашей рабочей станцией.

Настройки DHSP и WINS на сервере Windows 2000 Server

Протокол TCP/IP, который используется рабочей станцией DOS, несколько отличается от того, который применяется сервером Windows 2000. В связи с этим настройка сервера для общения с Microsoft Network Client Version 3.0 for MS-DOS имеет некоторые особенности. IP-адрес, который мы назначили рабочей станции, может быть изменен сервером при первом удачном входе в сеть. Для того чтобы в дальнейшем быть уверенным, что связь с компьютером будет надежной как со стороны сервера, так и со стороны других рабочих станций, выполните следующее:

1. Войдите на сервер в качестве администратора домена и создайте, если еще не создан, пользователя с именем Admin или другим именем, которое вы применили для пользователя рабочей станции DOS.
2. Нажмите кнопку **Пуск**.
3. Выберите **Программы | Администрирование | DHCP**. Откроется окно **DHCP** (рис. П1.2).
4. Раскройте папку **Область**, соответствующую адресам вашей сети, выделите папку **Арендованные адреса** и в списке справа найдите адрес рабочей станции DOS (в нашем случае — 192.168.0.126), ориентируясь по имени компьютера (serdos). Если адрес отличается от того, что был установлен в параметрах рабочей станции, отредактируйте файлы конфигурации рабочей станции DOS в соответствии с новым значением адреса и перезагрузите ее.
5. Выделите папку **Резервирование**, щелкните правой кнопкой мыши и выберите пункт **Создать резервирование**.
6. В открывшемся окне введите имя рабочей станции, ее IP-адрес и при необходимости комментарий.
7. Нажмите кнопку **Добавить**.

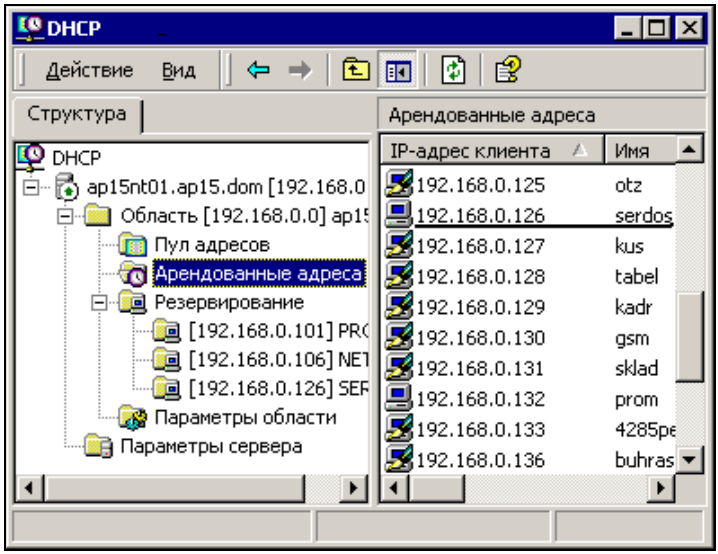


Рис. П1.2. Окно **DHCP**

8. Закройте окно **DHCP**.
9. Нажмите кнопку **Пуск**.
10. Выберите **Программы | Администрирование | WINS**. Откроется окно **WINS** (рис. П1.3).
11. Выделите папку **Активные регистрации**.
12. Щелкните правой кнопкой мыши и выберите **Статическое сопоставление**.
13. В открывшемся окне введите имя рабочей станции, MAC-адрес сетевого адаптера и его IP-адрес. Для того чтобы узнать MAC-адрес адаптера на рабочей станции DOS, достаточно внимательно посмотреть на строки, появляющиеся на экране в процессе загрузки с установленным Microsoft Network Client v3.0 for MS-DOS.
14. Нажмите кнопку **OK**.

Теперь IP-адрес рабочей станции DOS не будет изменяться по воле сервера и при установке программного обеспечения, которое требует указания адреса компьютера, вы будете уверены, что вводите действительный адрес. Компьютеры сети, не использующие сервис, предоставляемый сервером, также смогут подключаться к рабочей станции DOS и предоставлять ей свои ресурсы.

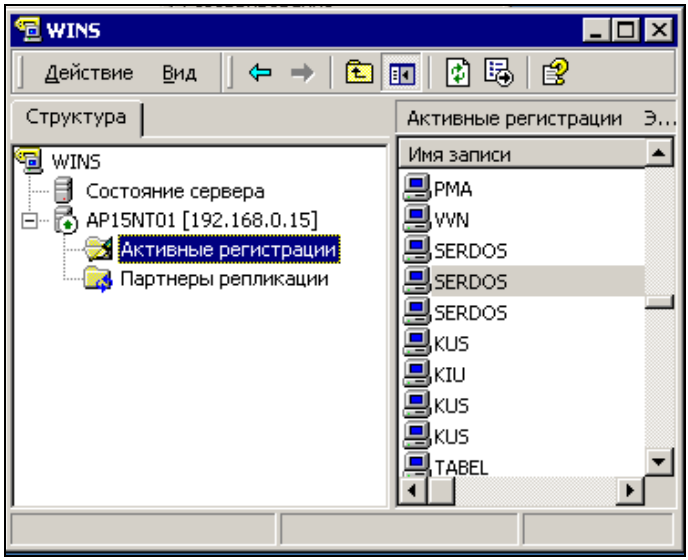


Рис. П1.3. Окно **WINS**

Применение настроек рабочей станции DOS при обслуживании компьютеров сети

Если вам удалось настроить рабочую станцию DOS для работы в вашей сети, то у вас в руках оказался очень полезный инструмент, который можно применять для настройки и установки программного обеспечения на новых компьютерах сети.

Для этого понадобится приобрести небольшую деталь — Flash Drive. Эти миниатюрные устройства теперь достаточно широко распространены. Замечательная особенность Flash Drive состоит в том, что он может быть загрузочным. Практически все современные компьютеры имеют в BIOS Setup режим загрузки компьютера с устройства USB-ZIP. Создав загрузочный Flash Drive и установив на него Microsoft Network Client v3.0 for MS-DOS, вы получите возможность загружать новый компьютер (без установленной операционной системы), устанавливать по сети или копировать установочные файлы программ. В случае необходимости полного форматирования диска, вы можете не носить с собой дистрибутивы, а записать их на доступный по сети диск и подключаться к ним даже с "пустой" машины. Если учесть, что в организациях иногда экономят на приводах CD-ROM, а современные компью-

теры все чаще предлагаются без floppy-дисковода, то загрузка с Flash Drive может оказаться единственным вариантом загрузки компьютера, не требующим его вскрытия.

Установка Microsoft Network Client v3.0 for MS-DOS на Flash Drive не сложнее, чем на обычный диск. Следует лишь учесть, что диск будет обозначаться буквой "A". Все пути должны соответствовать букве диска. Современные сетевые платы обычно имеют в составе дистрибутивной дискеты необходимые драйверы. У распространенного сетевого адаптера ReadyLINK Express RE 100ATX/WOL есть подходящий драйвер, расположенный в папке Ndis2. Некоторые сетевые адаптеры снабжены специальными драйверами для Microsoft Network Client v3.0 for MS-DOS.

Универсальность описываемого инструмента может пострадать, если с каждым новым компьютером вы получаете новый тип сетевого адаптера. В этом случае можно всегда иметь при себе адаптер для временной замены штатного или приобретать компьютеры с одинаковыми сетевыми платами.

Перед установкой Microsoft Network Client v3.0 for MS-DOS на Flash Drive все дистрибутивы можно записать туда же. Когда программа установки будет запрашивать загрузочную дискету или дискету с дистрибутивом, — потребуется только нажимать клавишу <Enter>. Для указания местонахождения драйвера сетевой платы придется вводить путь вручную. При этом средства, подобные файловому менеджеру, отсутствуют.

Загрузочный диск, полученный средствами Windows и с помощью инструментов, прилагаемых к Flash Drive, может быть легко дополнен необходимыми компонентами для загрузки сети. При этом вы не ограничены размером дискеты. Полный текст файлов Autoexec.bat и Config.sys, откорректированный для нашего случая, приведен в листингах П1.7 и П1.8.

Листинг П1.7. Файл Autoexec.bat для Flash Drive

```
@ECHO OFF
IF "%config%"=="SUPERDISK" GOTO SUPER ;добавлено
if "%config%"=="SUPERDISK1" GOTO SUPER ;добавлено

set EXPAND=YES
SET DIRCMD=/O:N
set LglDrv=27 * 26 Z 25 Y 24 X 23 W 22 V 21 U 20 T 19 S 18 R 17 Q 16 P 15
set LglDrv=%LglDrv% O 14 N 13 M 12 L 11 K 10 J 9 I 8 H 7 G 6 F 5 E 4 D 3 C
cls
```

```
call setramd.bat %LglDrv%
set temp=c:\
set tmp=c:\
path=%RAMD%:\;a:\;%CDROM%:\
copy command.com %RAMD%:\ > NUL
set comspec=%RAMD%:\command.com
copy extract.exe %RAMD%:\ > NUL
copy readme.txt %RAMD%:\ > NUL

:ERROR
IF EXIST ebd.cab GOTO EXT
echo Вставьте загрузочный диск 2 для Windows 98
echo.
pause
GOTO ERROR

:EXT
%RAMD%:\extract /y /e /l %RAMD%: ebd.cab > NUL
echo Средства диагностики находятся на диске %RAMD%.
echo.

IF "%config%"=="NOCD" GOTO QUIT
IF "%config%"=="HELP" GOTO HELP
LH %ramd%:\MSCDEX.EXE /D:mscd001 /L:%CDROM%
echo.
GOTO QUIT

:HELP
cls
call help.bat
echo После перезагрузки будет выведено загрузочное меню.
echo.
echo.
echo.
echo.
echo.
echo.
echo.
```

```
echo.
echo.
echo.
restart.com
GOTO QUIT

:QUIT

echo Для получения справки наберите HELP и нажмите клавишу ввода.
echo.
rem clean up environment variables
set CDROM=
set LglDrv=

goto ex ;далее добавлены строки

:SUPER
echo mem +
set temp=c:\TEMP
set tmp=c:\TEMP
path=a:\;a:\NET

choice /c:SNLA /t:L,20 "Share-S сеть-N локально-L"
if errorlevel 3 goto l
if errorlevel 2 goto n
a:\NET\net initialize
a:\NET\netbind.com
a:\NET\umb.com
a:\NET\tcptsr.exe
a:\NET\tinyrfc.exe
a:\NET\nmtsr.exe
a:\NET\emsbfr.exe
a:\NET\net start
a:\NET\net start server
a:\NET\net share
cls
@echo "Сеть с доступом загружена Ctrl+Alt+N подкл.диск"
@echo "netshare — обеспечить доступ"
```

```
net
a:\net\netshare.exe
goto l

:n
a:\NET\net initialize
a:\NET\netbind.com

a:\NET\umb.com
a:\NET\tcptsr.exe
a:\NET\tinyrfc.exe
a:\NET\nmtsr.exe
a:\NET\emsbfr.exe
a:\NET\net start
cls
@echo "Сеть загружена"
net
goto l
:l
@echo "ПРИЯТНОЙ РАБОТЫ!"
:ex
```

Листинг П1.8. Файл Config.sys для Flash Drive

```
[menu]
menuitem=CD, Start computer with CD-ROM support.
menuitem=NOCD, Start computer without CD-ROM support.
menuitem=HELP, View the Help file.
menuitem=SUPERDISK, NET.;Можно выбирать загрузку с доступом к сети
menuitem=SUPERDISK1, Mouse and RKM.
menudefault=CD,30
menucolor=14,1

[CD]
dos=high,umb
device=himem.sys /testmem:off
device=oakcdrom.sys /D:mscd001
device=btdosm.sys
```

```
device=flashpt.sys
device=btcdrom.sys /D:mscd001
device=aspi2dos.sys
device=aspi8dos.sys
device=aspi4dos.sys
device=aspi8u2.sys
device=aspicd.sys /D:mscd001
devicehigh=ramdrive.sys /E 2048
lastdrive=z
device=display.sys con=(ega,,1)
country=007,866,country.sys
install=mode.com con cp prepare=((866) ega3.cpi)
install=mode.com con cp select=866
install=keyb.com ru,,keybrd3.sys

[NOCD]
dos=high,umb
device=himem.sys /testmem:off
devicehigh=ramdrive.sys /E 2048
lastdrive=z
device=display.sys con=(ega,,1)
country=007,866,country.sys
install=mode.com con cp prepare=((866) ega3.cpi)
install=mode.com con cp select=866
install=keyb.com ru,,keybrd3.sys

[HELP]
dos=high,umb
device=himem.sys /testmem:off

[SUPERDISK]
dos=high,umb,noauto
device=himem.sys /testmem:off
device=emm386.exe noems
devicehigh=A:\display.sys con=(ega,,1)
country=007,866,country.sys
install=mode.com con cp prepare=((866) ega3.cpi)
install=mode.com con cp select=866
```

```
installhigh=keyb.com ru,,keybrd3.sys
devicehigh a:\net\ifshlp.sys


[SUPERDISK1]
dos=high,umb
device=himem.sys/testmem:off
devicehigh=emm386.exe noems
installhigh=rkm.com
installhigh=mouse.com

[COMMON]
dos=high,umb
fileshigh=80
buffershigh=20
stackshigh=9,256
lastdrivehigh=z
FCBSHIGH=1
shell=a:\command.com /E:512 /P
```

Просмотрите внимательно тексты файлов. Возможно, вы что-либо измените в них, добавите запуск утилит или программ. Но следует иметь в виду, что Flash Drive не слишком быстрый диск. Если программа требует высокой скорости операций (например, видео), то файлы необходимо копировать на жесткий или виртуальный диск. Однако для целей, которые были обозначены ранее, быстродействия Flash Drive вполне достаточно. Flash Drive, построенный на основе файлов обычной загрузочной дискеты с добавлением Microsoft Network Client v3.0 for MS-DOS и его обновлений, сохраняет возможности загрузочной дискеты, но имеет режим загрузки сети. Как и в случае с рабочей станцией DOS, при установке Microsoft Network Client v3.0 for MS-DOS откажитесь от автоматического изменения этих файлов и используйте заранее подготовленные образцы. При необходимости, позже вы их сможете откорректировать в соответствии с вашими потребностями.

Примечание

Применяя загрузочный Flash Drive с доступом к сети, не забывайте изменять имя компьютера в файле \NET\System.ini, а если в сети используется DHCP-сервер, то не указывайте IP-адрес компьютера: DHCP-сервер выдаст

адрес самостоятельно. В одноранговой сети и сети без DHCP указывать адрес обязательно, но необходимо следить за его уникальностью в пределах сети.

Настройка рабочих станций с операционной системой Windows 9*x*

Если операционная система установлена корректно, то настройка рабочих станций под управлением Windows 9*x* проще, чем для рабочих станций DOS. Тем не менее при настройке требуются аккуратность и внимание. Если вам придется переводить всю сеть на работу под Windows, то устранение допущенных ошибок при массовой настройке рабочих станций отнимет у вас очень много времени.

Чтобы компьютер с операционной системой Windows 9*x* смог работать в сети с сервером Windows 2000 Server, этот компьютер необходимо подключить к сети и выполнить следующее:

1. Нажать кнопку **Пуск**.
2. В открывшемся меню выбрать **Настройка | Панель управления**.
3. В открывшемся окне найти значок **Сеть** и двойным щелчком по нему открыть одноименное окно (рис. П1.4).
4. Если еще не добавлены компоненты: **Клиент для сетей Microsoft**, **TCP/IP**, сетевой адаптер, **Служба доступа к файлам и принтерам сетей Microsoft**, то добавить их.

Для добавления компонентов нажмите кнопку **Добавить**. Откроется окно **Выбор типа компонента**. В этом окне выберите тип компонента, например **Клиент**, **Протокол** или **Служба** в соответствии с типом устанавливаемого компонента. После выбора типа компонента станет доступной кнопка **Добавить**. Нажав ее, вы сможете выбрать необходимый компонент.

Вполне возможно, что вы уже использовали ваш компьютер для подключения к Интернету. В этом случае у вас будет установлено два протокола TCP/IP, но с различной привязкой. Один будет работать с сетевым адаптером, а другой с контроллером удаленного доступа, который уже установлен. Это необходимо учесть, когда будем настраивать работу сети. Протокол, работающий с контроллером удаленного доступа, настраивать не следует, чтобы не испортить свойства подключения к Интернету.

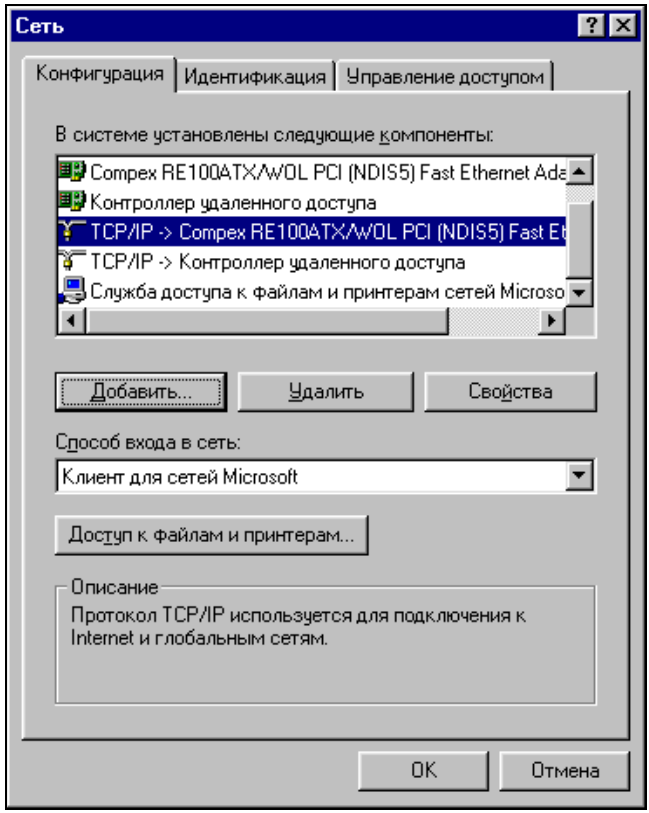


Рис. П1.4. Окно **Сеть**

Выбирать следует компоненты, разработанные корпорацией Microsoft.

1. В окне **Сеть** на вкладке **Конфигурация** (см. рис. П1.4) выделите протокол **TCP/IP**.
2. Нажмите кнопку **Свойства**.
3. В открывшемся окне **Свойства: TCP/IP** на вкладке **IP-адрес** установите переключатель в положение **Получить IP-адрес автоматически**, если было установлено иное.
4. Если используется сервер DNS, откройте вкладку **Конфигурация DNS** (рис. П1.5). Если DNS не используется, переходите к пункту 12.
5. Отметьте переключатель **Включить DNS**.
6. Введите имя компьютера и имя домена в соответствующие поля ввода.

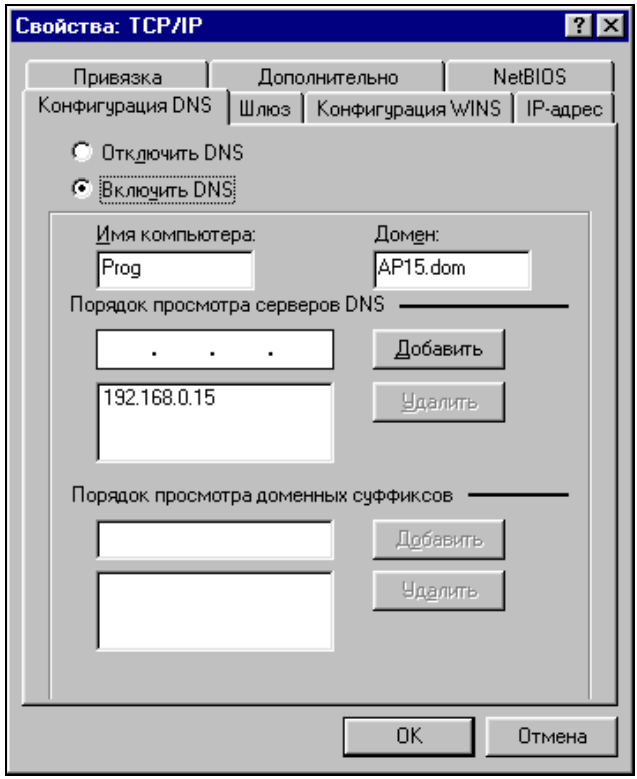


Рис. П1.5. Окно **Свойства: TCP/IP**, вкладка **Конфигурация DNS**

7. В разделе **Порядок просмотра серверов DNS** введите IP-адрес вашего сервера и нажмите кнопку **Добавить**.
8. Если применяется WINS-сервер без сервера DNS, то откройте вкладку **Конфигурация WINS**.
9. Установите переключатель в положение **Включить распознавание WINS** (рис. П1.6).
10. Введите IP-адрес вашего сервера и нажмите кнопку **Добавить** (При наличии сервера DHCP отмечается только переключатель **Использовать DHCP для распознавания WINS**.)
11. Нажмите кнопку **OK**.
12. Откройте вкладку **Идентификация** окна **Сеть**.

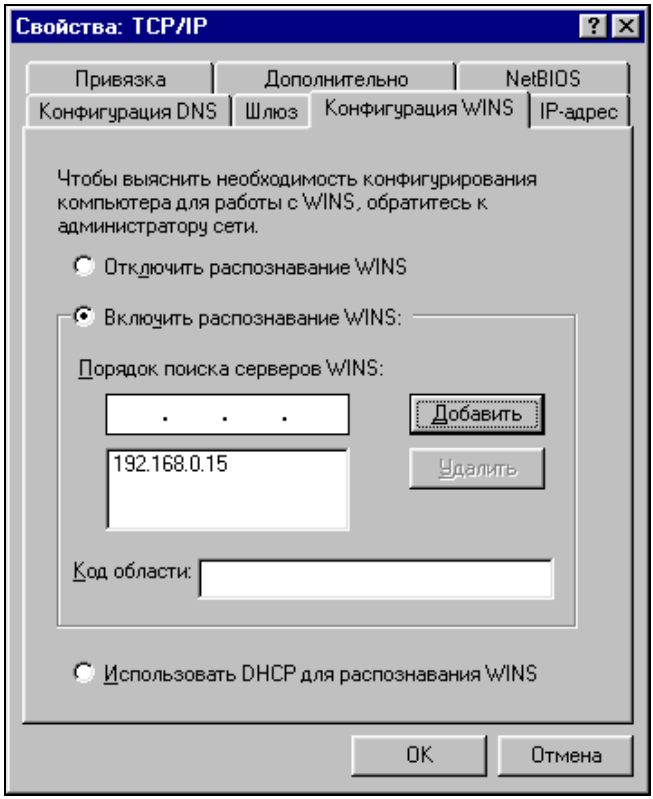


Рис. П1.6. Окно **Свойства: TCP/IP**, вкладка **Конфигурация WINS**

13. Введите имя компьютера, имя рабочей группы и описание компьютера. Имя рабочей группы должно совпадать с именем домена без суффикса (рис. П1.7).
14. На вкладке **Конфигурация** установите **Способ входа в сеть**, выбрав пункт **Клиент для сетей Microsoft**.
15. При необходимости нажмите кнопку **Доступ к файлам и принтерам** и в открывшемся окне отметьте флажки, разрешающие доступ к компьютеру. Нажмите кнопку **OK**.
16. Выделите пункт **Клиент для сетей Microsoft**.
17. Нажмите кнопку **Свойства**.

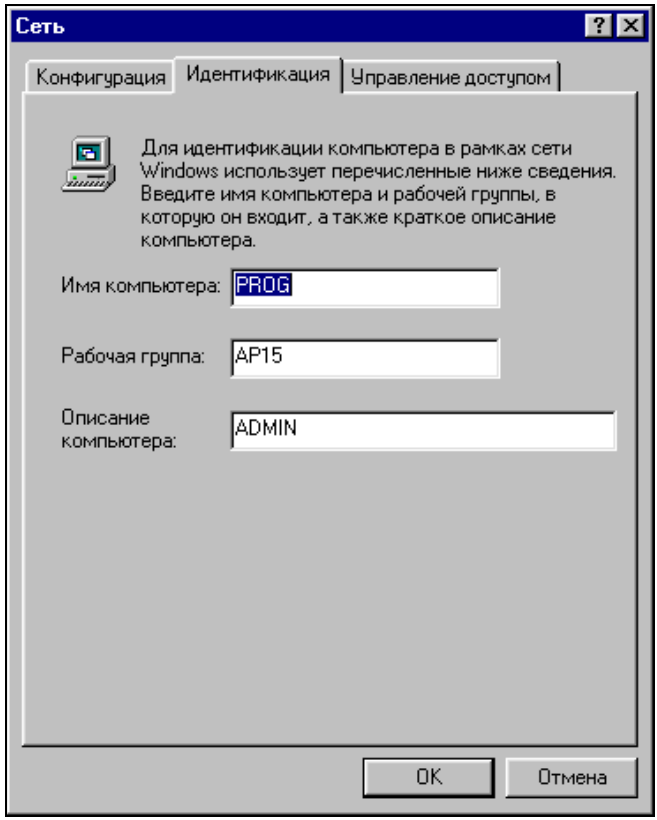


Рис. П1.7. Окно **Сеть**, вкладка **Идентификация**

18. В открывшемся окне **Свойства: Клиент для сетей Microsoft** (рис. П1.8) установите флажок **Входить в домен Windows NT** и внесите имя домена (опять без суффикса).
19. В разделе **Параметры входа в сеть** выберите подходящий вам вариант.
20. Нажмите кнопку **OK**.
21. На вкладке **Управление доступом** установите желаемый вариант доступа к компьютеру. Доступ на уровне ресурсов даст возможность подключаться к компьютеру с рабочих станций, не зарегистрированных на сервере (не входящих в домен), доступ на уровне пользователей позволяет подключаться к компьютеру только зарегистрированным пользователям. Для второго варианта необходимо заполнить поле **Взять список пользователей с сервера**, но указать необходимо имя домена без суффикса.

22. Нажмите кнопку **OK** и перезагрузите компьютер.
23. После перезагрузки, если не удастся войти в сеть, проверьте еще раз все настройки и исправьте ошибки.

На этом настройка рабочей станции под управлением Windows 9*x* завершена.

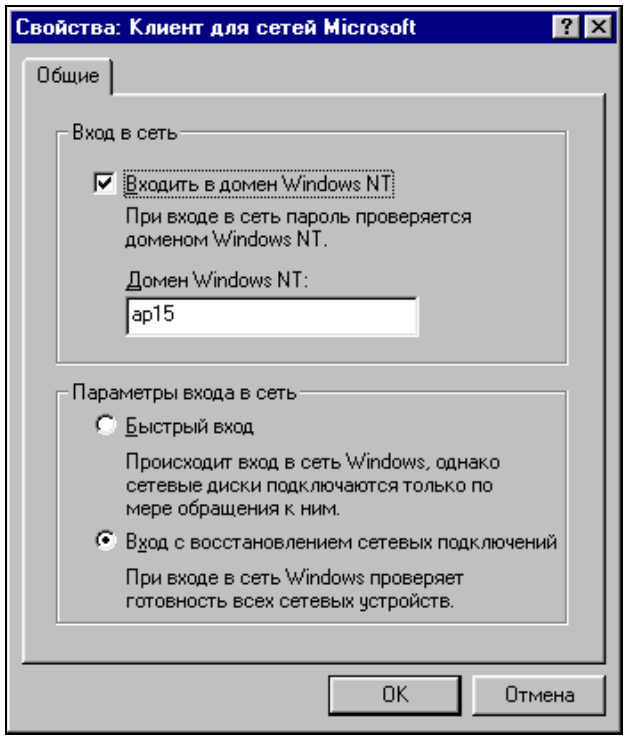


Рис. П1.8. Окно **Свойства: Клиент для сетей Microsoft**

Настройка рабочих станций с операционной системой Windows 2000/XP

Настройка рабочих станций под управлением Windows 2000/XP мало отличается от описанной ранее. В большинстве случаев все отличия заключаются в расположении и виде окон.

Для обеспечения работы компьютера в сети необходимо проделать следующее:

1. Подключите компьютер к сети.
2. Нажмите кнопку **Пуск**.
3. Выберите **Панель управления**.
4. Найдите значок **Система** и откройте окно **Свойства системы** двойным щелчком мыши по значку.
5. На вкладке **Имя компьютера** этого окна введите описание компьютера и нажмите кнопку **Изменить**.
6. Откроется окно **Изменение имени компьютера** (рис. П1.9), в котором надо указать имя компьютера и домен или рабочую группу. Имя домена должно быть указано с суффиксом.
7. Нажмите кнопку **OK** в каждом открытом окне.

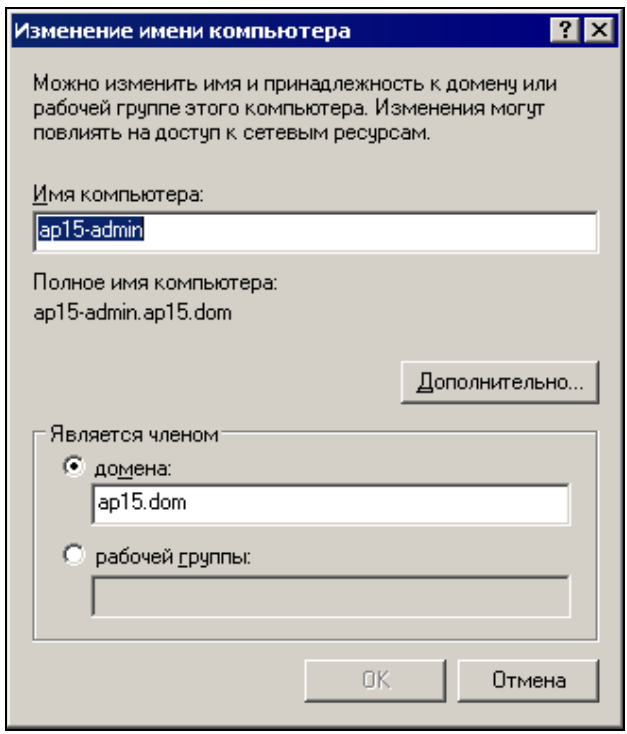


Рис. П1.9. Окно **Изменение имени компьютера**

8. На Панели управления откройте окно **Сетевые подключения** двойным щелчком мыши на одноименном значке.
9. Правой кнопкой мыши щелкните на значке **Подключение по локальной сети** и выберите **Свойства**.
10. Установите следующие свойства протокола Интернета (TCP/IP): **Получить IP-адрес автоматически** и **Получить адрес DNS-сервера автоматически**.
11. В строке каждого используемого протокола должен быть отмечен флажок.

При необходимости вы можете скорректировать эти настройки, но в большинстве случаев этого не требуется, и компьютер можно считать настроенным после перезагрузки.

Операционная система Windows 2000/XP многие настройки сети может определять самостоятельно, и вам придется изменять их лишь в особых случаях.

Автоматизация настройки сетевых параметров

Иногда может потребоваться перенастройка сетевых параметров компьютера, причем не разовая, а регулярная. Например, если у вас есть ноутбук, который приходится подключать к разным сетям, придется в каждой сети корректировать настройки портативной машины. Эти операции можно существенно упростить, создав необходимое число пакетных файлов, которые будут содержать команды для настройки сетевых параметров. Windows XP и Windows Vista позволяют выполнять из командной строки множество настроек системы, в том числе и сетевых.

Приведем пример файлов (листинги П1.9 и П1.10), которые позволяют перенастраивать компьютер в зависимости от параметров сети, к которой он подключается. Сети имеют различную систему IP-адресов. Обе сети подключены к Интернету посредством ADSL-модемов. В первой строке каждого файла выполняется смена текущего каталога на корневой. Если этого не сделать, то команды могут не выполниться из-за слишком длинного пути к файлу. Далее выполняются инструкции набора команд `netsh interface ip`. Вы можете ознакомиться подробно с возможностями команд `netsh` для интерфейса IP в справочной системе Windows. В последней строке — инструкция, останавливающая работу командного файла, чтобы можно было увидеть вывод результатов команд и сообщения о возможных ошибках. Подставив вместо указанных свои значения IP-адресов, вы получите аналогичные файлы для своих сетей.

Листинг П1.9. Файл Net1.bat

```
cd c:\
netsh interface ip delete dns name="Local Area Connection" addr=all
netsh interface ip set address name="Local Area Connection" static
addr=192.168.1.123 mask=255.255.255.0 gateway=192.168.1.1 gwmetric=1
netsh interface ip set dns name="Local Area Connection" static
addr=195.34.32.116 register=Both
netsh interface ip add dns name="Local Area Connection" addr=192.168.1.1
index=2
pause
```

Листинг П1.10. Файл Net2.bat

```
cd c:\
netsh interface ip delete dns name="Local Area Connection" addr=all
netsh interface ip set address name="Local Area Connection" static
addr=10.15.0.6 mask=255.255.255.0 gateway=10.15.0.198 gwmetric=1
netsh interface ip set dns name="Local Area Connection" static
addr=10.15.0.199 register=Both
netsh interface ip add dns name="Local Area Connection"
addr=195.34.32.116 index=2
pause
```

Настройка рабочих станций с операционной системой Linux

Версий Linux больше, чем версий Windows. Каждая из них обладает определенными преимуществами или недостатками по сравнению с другими. Каждый пользователь может выбрать наиболее подходящую для него версию, установить ее в необходимой конфигурации. Если Windows в серверной редакции и в редакции для рабочей станции это разные дистрибутивы, то в Linux это может быть один дистрибутив, а как вы его будете устанавливать — ваше дело. Вот и ASPLinux можно устанавливать в необходимом вам объеме. Установив систему как рабочую станцию, необходимо будет указать параметры сети, в которой эта рабочая станция будет работать.

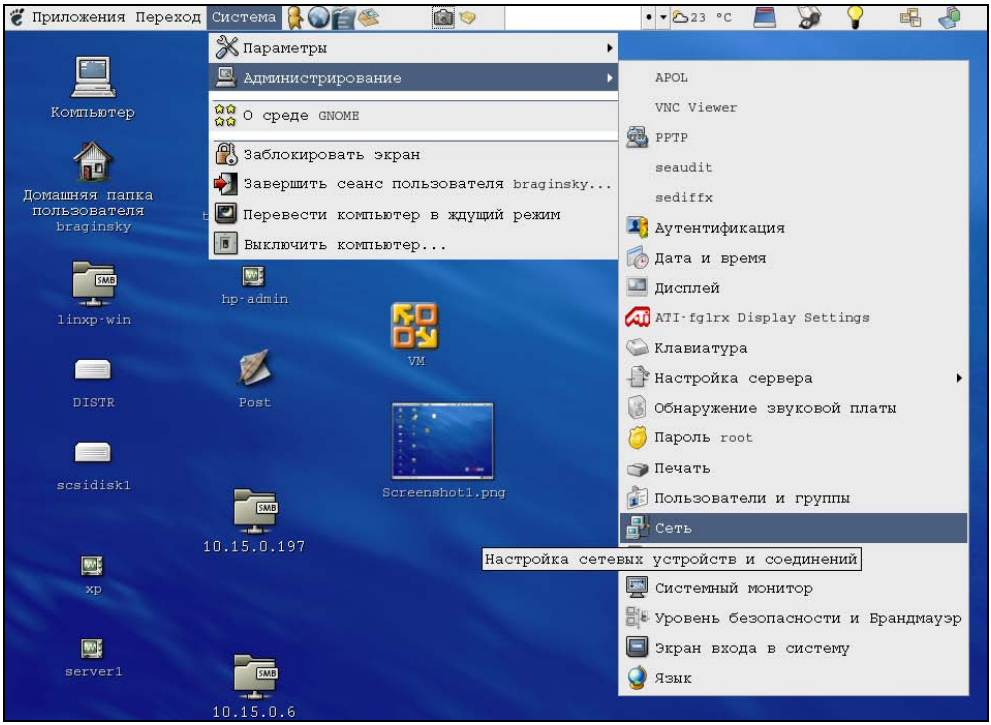


Рис. П1.10. Рабочий стол ASPLinux 11.2 (фрагмент).
Выбор меню **Сеть**

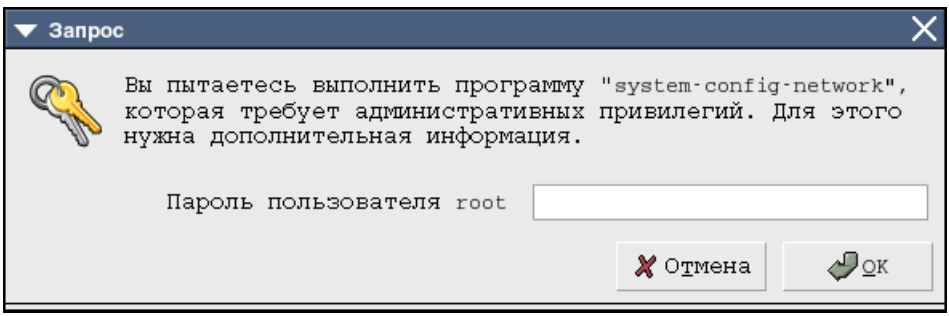


Рис. П1.11. Окно **Запрос**.
Ввод пароля администратора

Практически все возможные настройки системы Linux доступны из командной строки, но пользователям Windows привычнее работать с графическим

интерфейсом, в котором и рассмотрим настройку рабочей станции Linux для работы в сети Windows. На рабочей станции установлена ОС ASPLinux 11.2, имеющая весьма широкое распространение у российских пользователей.

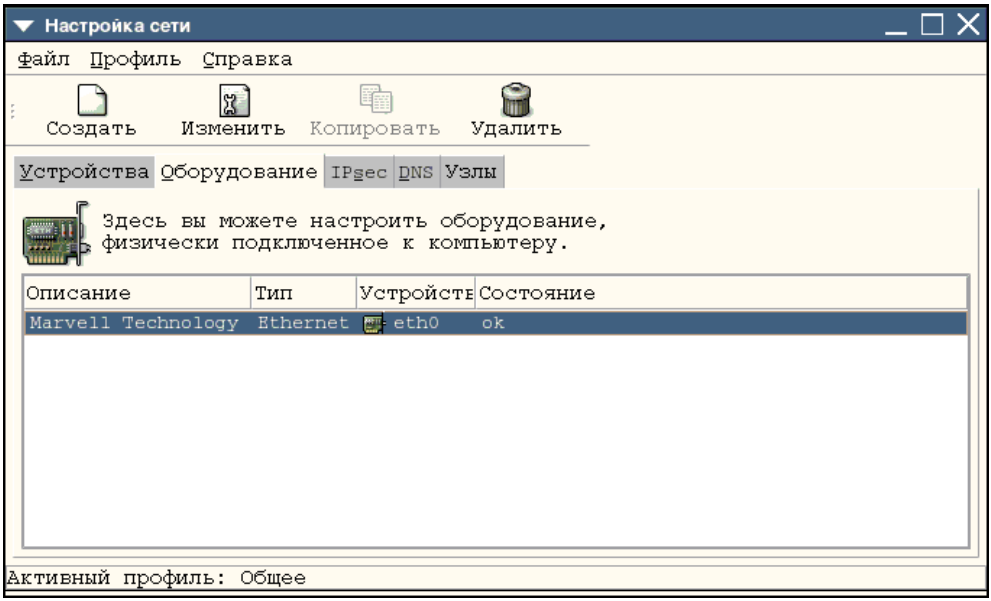


Рис. П1.12. Окно **Настройка сети**

Процедура настройки сети не сложна и заключается в следующем:

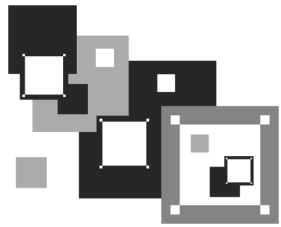
1. Подключите компьютер к сети.
2. Нажмите кнопку **Система** (рис. П1.10).
3. Выберите **Администрирование | Сеть**.
4. В открывшемся окне **Запрос** (рис. П1.11) введите пароль администратора системы. Откроется окно **Настройка сети** (рис. П1.12).
5. На вкладке **Оборудование** этого окна вы должны увидеть ваш сетевой адаптер, который определился во время установки системы.
6. На вкладке **Устройства** этого окна с помощью кнопки **Создать** создайте новое устройство (аналог подключения в Windows), которое далее в окнах для ввода параметров будет именоваться как **Новое соединение**. В них выберите тип соединения **Ethernet** и имя вашей сетевой карты.

7. Теперь в окне **Настройка сети** на вкладках **DNS** и **Узлы** укажите необходимые IP-адреса.
8. В свойствах подключения (кнопка **Изменить**) укажите IP-адрес рабочей станции, маску подсети и адрес основного шлюза, если это необходимо. Или оставьте вариант **Автоматически получить адрес IP при помощи DHCP**.
9. Согласитесь с предложением системы сохранить настройки.

Вы можете создать несколько соединений с различными параметрами для разных сетей. Это может быть полезно для ноутбуков. Аналогично Ethernet-соединению вы можете настроить и модемное соединение. Если модем внешний, то не потребуются драйверы для него, но устройство необходимо создать, указав имя `/dev/ttyS0`, где `S0` соответствует порту COM1.

Для подключения к сетевым каталогам достаточно в меню **Файл** любого локального каталога выбрать пункт **Соединиться с сервером** и указать в окне **Соединение с сервером** тип сервиса — **Ресурс ОС Windows**, сетевое имя или IP-адрес компьютера. На рабочем столе будет создан значок сетевого каталога. В процессе создания сетевого каталога потребуется авторизация на удаленном компьютере.

Приложение 2



Вопрос — ответ

Любое обучение предполагает, что в конце урока или после выполнения задания у учащихся появляются вопросы, на которые они хотят получить ответ. Вероятно, часть вопросов, которые приведены в данном приложении, совпадут с вашими.

● Вопрос:

Какие настройки сети и программы требуются для организации сети на двух компьютерах и выхода обоих в Интернет через один модем, установленный на первом компьютере?

Ответ:

Windows начиная с версии Windows 98 SE позволяет осуществить это без применения дополнительного программного обеспечения. Необходимо установить для сетевого адаптера протоколы TCP/IP и NetBEUI. В параметрах протокола TCP/IP установить переключатель **IP-адрес получать автоматически**. На одном компьютере, том, на котором установлен модем, настроить соединение и общий доступ к подключению Интернета.

● Вопрос:

В моем офисе компьютер подключен к Интернету. Могу ли я использовать это подключение к Интернету из дома?

Ответ:

При наличии второй телефонной линии можно установить два модема на офисный компьютер, контроллер удаленного доступа, адаптер виртуальной

частной сети. Адаптер виртуальной частной сети — это компонент Windows. Контроллеров удаленного доступа должно получиться два (по одному на модем).

После этих дополнений компьютер сможет одновременно использовать два модема. При недостатке внешних портов для подключения модемов один из них или оба могут быть внутренними.

Может случиться так, что после установки двух модемов вызываемый модем не будет отвечать на звонки. В этом случае необходимо в строку инициализации модема вписать: `ATS0=1`. Для этого надо открыть **Панель управления | Система | Устройства | Модемы | *<Ваш модем>* | Свойства | Дополнительно**.

Настройки сервера удаленного доступа остаются по умолчанию. IP-адрес назначается автоматически (192.168.55.2 на стороне клиента и 192.168.55.1 на стороне сервера), но на всякий случай установите пароль для доступа к серверу.

Следует иметь в виду, что скорость соединения будет существенно зависеть от качества связи с офисным компьютером. При отсутствии второй телефонной линии дешевле подключить к Интернету домашний компьютер.

● Вопрос:

Можно ли использовать программу Telnet для удаленного администрирования Windows 2000?

Ответ:

Да, можно. Windows 2000 Professional, как и Windows 2000 Server, имеет встроенный Telnet-сервер. Если у вас под рукой Telnet-клиент, а у сервера есть постоянный IP-адрес, вы можете открыть окно командной строки на сервере откуда угодно, из любой точки земного шара. По умолчанию запуск Telnet-сервера отключен из-за очевидной угрозы безопасности. Чтобы запустить эту службу, воспользуйтесь следующей командой:

```
Net start telnet
```

Если нужно, чтобы сервер стартовал автоматически при запуске системы, следует установить режим запуска **Авто**, для этого необходимо открыть **Панель управления | Администрирование | Службы | Telnet**. После запуска сервера ваш компьютер готов обслуживать клиентские запросы к TCP-порту 23. По умолчанию сервер пытается аутентифицировать клиента по схеме NT

LAN Manager (NTLM), что позволяет регистрироваться автоматически. Для удаленного доступа из-за пределов локальной сети это неудобно; чтобы сменить режим аутентификации, сначала нужно запустить утилиту администрирования сервера Telnet-командой `tlntadmn`.

В появившемся меню выберите пункт **Отобразить/изменить параметры реестра**, а в следующем меню — пункт **NTLM**. По умолчанию значение этого параметра реестра равно 2, что соответствует аутентификации средствами NTLM. Если изменить это значение на 1, сервер сначала попробует аутентифицировать клиента по NTLM, а если не получится, запросит имя пользователя и пароль. Значение 0 отменяет попытку аутентификации клиента с помощью NTLM.

Теперь, когда процесс конфигурации сервера завершен, он доступен отовсюду, даже с компьютера под управлением UNIX. Стоит только набрать команду:

```
telnet <имя или IP-адрес сервера
```

и все!

> ***ПРИМЕЧАНИЕ***
>
> Если установка Windows 2000 проводилась как обновление Windows 98, то служба Telnet может функционировать неправильно. Надо также иметь в виду, что доступ к компьютеру может получить и злоумышленник (даже через Интернет, если компьютер подключен к нему), поскольку системы Windows не имеют средств ограничения доступа по данному протоколу.

● Вопрос:

Компьютер под управлением Windows XP не видит в сети рабочие станции с Windows 95 и DOS. Как это исправить?

Ответ:

Протокол TCP/IP совершенствуется, некоторые функции новых редакций этого протокола не поддерживаются старыми операционными системами. В сложившейся ситуации может помочь старый протокол NetBEUI. Достаточно установить на все компьютеры протокол NetBEUI (для Windows XP устанавливается отдельно с дистрибутивного диска). Применение только протокола TCP/IP не позволит компьютеру с Windows XP использовать файлы и принтеры рабочих станций DOS. Но рабочие станции DOS смогут использовать ресурсы компьютеров с Windows XP и Windows 2000.

● **Вопрос:**

До перехода с NetWare на Windows 2000 Server не возникало проблем при печати из прикладных программ на принтере, подключенном к рабочей станции DOS. Теперь эта печать идет чрезвычайно медленно. Что делать?

Ответ:

Если нет возможности установить более новый компьютер или подключить принтер к серверу, увеличьте оперативную память одной из рабочих станций DOS до 8 Мбайт. Затем установите на нее Windows 95. Прикладные DOS-программы будут работать не хуже, а печать будет идти быстро с любых компьютеров.

● **Вопрос:**

Почему не виден принтер в сетевом окружении?

Ответ:

Причин может быть несколько:

1. Для принтера не установлен общий доступ.
2. Общий доступ установлен, но пользователь, под именем которого вы вошли в сеть, не имеет прав доступа к принтеру.
3. Принтер не поддерживает сетевое использование (встречается редко).
4. Неправильно установлен принтер.
5. При установке принтера использовался неподходящий драйвер.
6. Не включен компьютер, к которому подключен принтер.
7. Не исправен или не подсоединен сетевой кабель компьютера, к которому подключен принтер.

● **Вопрос:**

Почему не все компьютеры сети видны в сетевом окружении?

Ответ:

Причин может быть несколько:

1. Не все компьютеры включены.

2. Не на всех компьютерах есть ресурсы с общим доступом.
3. Не на всех компьютерах выполнен вход в сеть.
4. Возможно, что следует подождать несколько минут, если компьютеры только что подключились к сети.
5. Не все компьютеры используют одни и те же сетевые протоколы.
6. Не у всех компьютеров исправен сетевой кабель.

● Вопрос:

Почему на некоторых компьютерах операции выполняются очень медленно?

Ответ:

Причин может быть несколько:

1. Возможно, применяется сетевой кабель слишком низкой категории, следует заменить кабель.
2. Слишком длинный кабель от хаба до компьютера (более 100 м). Можно разрезать кабель в удобном для этого месте и установить в разрыв дополнительный хаб.
3. Если вы перешли с хабов 10 Мбит на коммутаторы 10/100 Мбит, а кабели оставили старые, настройте коммутаторы на работу с пониженной скоростью.
4. Проверьте обжим сетевых разъемов и подключение кабелей к розеткам. Плохой контакт может вызвать нарушения в работе сети и даже потерю данных (при работе с базами данных).
5. Если дефект зависит от времени суток, возможно, что сервер работает с перегрузкой.

● Вопрос:

Не удается зарегистрироваться в сети, но имя пользователя и пароль верны.

Ответ:

Причин может быть несколько:

1. Потеряна связь с сервером (нарушения в кабельной системе).
2. Включена клавиша <Caps Lock>.

3. Пароль изменен пользователем, имеющим права администратора.
4. Если на сервере установлено более одной сетевой карты, то исключите протокол NetBEUI с проблемных компьютеров или отключите лишние сетевые адаптеры на сервере.

● Вопрос:

Почему после замены сетевой карты компьютер не входит в сеть и даже "зависает"?

Ответ:

Следует после включения компьютера подождать несколько минут, а иногда около часа. Регистрационные данные компьютера на сервере привязаны к MAC-адресу сетевой платы, а он изменился. Вход в сеть может быть произведен, когда прекратятся попытки сервера найти в сети старую сетевую карту, зарегистрированную сервером вместе с именем компьютера.

● Вопрос:

Как проверить качество связи компьютера с сервером?

Ответ:

Достаточно использовать команду `PING` из командной строки, введя в качестве параметра IP-адрес сервера. Если время ответа менее 10 мкс, то все нормально, если время ответа исчисляется десятками и сотнями микросекунд, да еще нестабильно, — ищите причины в неисправности кабельной системы или несоответствии параметров кабеля параметрам нового оборудования.

● Вопрос:

Проложены новые кабели и установлено новое сетевое оборудование, но качество связи очень низкое. Почему?

Ответ:

Вполне возможно, что на одном или нескольких участках сетевой кабель проходит вблизи кабеля высокого напряжения. Необходимо проложить сетевой кабель не ближе 50 см от силового.

● **Вопрос:**

Почему при подключении сетевого кабеля в разъем сетевой платы не загораются ее индикаторы?

Ответ:

Скорее всего, поврежден кабель. Но возможно, что второй конец кабеля не вставлен в розетку.

● **Вопрос:**

Сетевой диск подключается при входе в систему, но если нет доступа к компьютеру, на котором расположены данные, пользователи машинально отключают возможность подключения диска при следующей загрузке. Как избежать этого?

Ответ:

Очень просто. Достаточно создать BAT-файл со следующим содержимым:

```
net use Буква_диска: \\Имя_компьютера\Имя_каталога
```

Поместите ярлык этого файла в папку Автозагрузка. При каждой загрузке компьютер будет пытаться установить соединение с сетевым ресурсом.

● **Вопрос:**

Мне приходится часто подключать и отключать сетевые диски, можно ли упростить эту процедуру?

Ответ:

Как и в предыдущем случае, создайте несколько BAT-файлов со строками, содержащими команды для подключений, и используйте их для подключения необходимого набора сетевых дисков.

● **Вопрос:**

Как упростить установку и модификацию приложений в сети?

Ответ:

Проще всего на одном из компьютеров установить виртуальный CD-ROM. Программы такого назначения часто распространяются с новыми компью-

терами, но можно их найти и в Интернете. Создайте несколько виртуальных дисков и скопируйте на них дистрибутивные диски. Настройте общий доступ к виртуальным дискам. Теперь, подключая такой диск в качестве сетевого на любой рабочей станции, вы можете устанавливать и модифицировать программное обеспечение на этих рабочих станциях. Причем подключаться к такому виртуальному диску можно с нескольких рабочих станций одновременно.

● Вопрос:

Компьютеры для нашей сети в целях экономии средств приобретаются без приводов CD-ROM. Существует ли возможность подключить компьютер к сети до установки Windows для последующей установки операционной системы и программного обеспечения?

Ответ:

Существует. Проще всего это реализуется на современных компьютерах с поддержкой различных режимов работы USB-портов из BIOS. Приобретите один Flash Drive. Сделайте его загрузочным и установите на него Microsoft Network Client Version 3.0 for MS-DOS. Если вы приобретаете одинаковые сетевые адаптеры для всех компьютеров, то проблем не будет совсем, иначе вам потребуется дополнительно настраивать Microsoft Network Client Version 3.0 for MS-DOS для работы с каждым компьютером. Установка клиента описана в *приложении 1*.

● Вопрос:

Для доступа к рабочей станции Linux применяю VNC. Не удается переключать раскладку клавиатуры на удаленном компьютере. В чем может быть причина?

Ответ:

Причина проста. Настройте переключение раскладки на удаленном и на вашем компьютерах разными сочетаниями клавиш.

● **Вопрос:**

Существует ли возможность доступа к серверу терминалов с рабочей станции Linux?

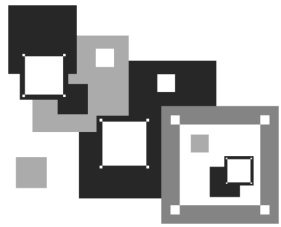
Ответ:

Да. В большинстве дистрибутивов Linux есть свой терминальный клиент rdesktop. Правда, зачастую он не имеет графического интерфейса, все настройки выполняются в командной строке. Для удобства работы можно создать значок запуска клиента, а в его свойствах (как в свойствах ярлыка Windows) описать все необходимые настройки.

Пример строки запуска для такого значка:

```
rdesktop <IP-адрес> -u <Имя_пользователя> -p <пароль> -r clipboard:CLIPBOARD -r sound:remote -k en-us -g 1024x768 -a 16.
```

Приложение 3



Краткий словарь терминов и сокращений

Беспроводная сеть

Это сеть, построенная на основе беспроводных сетевых адаптеров и концентраторов. Среди множества изделий различных фирм обращают на себя внимание концентраторы корпорации Intel. Intel PRO/Wireless 2011 LAN Access Point — точка доступа для связи удаленного компьютера с локальной сетью — может применяться и как повторитель (repeater) для увеличения максимального расстояния при подключении. Intel PRO/Wireless 2011 LAN PC Card — беспроводный сетевой адаптер для компьютеров.

Строить сеть полностью на основе таких устройств нерационально. В отдельных случаях они позволяют обеспечить доступ пользователям, не имеющим возможности подключиться к сети с помощью кабеля.

Виртуальный компьютер

Виртульный компьютер эмулирует работу отдельного физического компьютера. На одной машине может быть запущено множество виртуальных компьютеров. Помимо некоторых очевидных ограничений, каждый виртуальный компьютер предоставляет полный и независимый контроль и управление, как предоставляет его обычный компьютер. Каждый виртуальный компьютер имеет свои процессы, ресурсы, конфигурацию и отдельное администрирование. Для эмуляции обычно используются технологии виртуальных машин.

Виртуальная машина

Виртуальной машиной (англ. *virtual machine*) называют программную или аппаратную среду, исполняющую некоторый код, например машинный код реального процессора, или спецификацию такой системы.

Зачастую виртуальная машина эмулирует работу реального компьютера. На виртуальную машину, так же как и на реальный компьютер, можно инсталлировать операционную систему, у виртуальной машины также есть BIOS, оперативная память, жесткий диск (выделенное место на жестком диске реального компьютера), могут эмулироваться периферийные устройства. На одном компьютере может функционировать несколько виртуальных машин.

Виртуальная частная сеть

VPN (англ. *Virtual Private Network* — виртуальная частная сеть) — логическая сеть, создаваемая поверх другой сети, например Интернет. Несмотря на то что коммуникации осуществляются по публичным сетям с использованием небезопасных протоколов, за счет шифрования создаются закрытые от посторонних каналы обмена информацией.

Витая пара

Кабели на основе витой пары находят широкое применение в сетях передачи данных. Для кабеля на основе витых пар используются медные проводники диаметром 0,64—0,51 мм. В качестве материала изоляции обычно применяются полиэтилен, полипропилен, тефлон, вспененный полиэтилен. Неэкранированная витая пара представляет собой от 1 до 100 пар медных изолированных проводников, скрученных парами с согласованными шагами для уменьшения взаимного влияния. Наиболее распространены двух- и четырехпарные конструкции. Цветовая комбинация проводников фиксирована: один из проводников в паре имеет белый цвет с метками цвета второго одноцветного проводника этой пары — синего, оранжевого, зеленого или коричневого. Конструктивно все кабели делятся на экранированные и неэкранированные. Экранированные конструкции более защищены от помех и имеют лучшие показатели переходного затухания, но их применение требует специальных разъемов и правильной схемы заземления, поэтому в нашей стране большее распространение получили неэкранированные кабели. Наиболее распространен серый цвет кабеля, однако производятся кабели всех цветов, как правило, пастельных тонов. В случае наружной прокладки используется светостойкий полиэтилен (черного цвета). Все кабели маркируются по оболочке примерно следующим образом: фирма-производитель — марка изделия — тип изделия (4×2×0,52 — четырехпарный кабель с диаметром проводника), далее кодируются дата производства (1002 — октябрь 2002 года) и отметка метровой длины (иногда футы). Кроме того, на кабеле могут быть указаны материал оболочки, система сертификации и т. д.

Драйвер (Driver)

Небольшая компьютерная программа для работы с конкретным периферийным устройством, таким как, например, сетевая плата или принтер.

Интерфейс

См. *Interface*.

Коаксиальный кабель

Представляет собой два соосных гибких металлических цилиндра, разделенных диэлектриком. Название произошло от латинских: *co* — совместно и *axis* — ось. Применяется для передачи высокочастотных сигналов. Для организации компьютерных сетей используется ограниченно. Кабель на основе витой пары вытесняет коаксиальный кабель в области сетестроения, ввиду большего удобства применения. В отдельных случаях может быть оправдано использование толстого коаксиального кабеля для связи удаленных на расстояние 180 м и более участков сети.

Коммутатор (switch)

Как и концентратор, позволяет объединить несколько компьютеров, подключив их к одному серверу. В отличие от устаревших теперь концентраторов (hub), коммутатор позволяет пересылать пакеты между несколькими сегментами сети, не загружая остальную сеть. Он является обучающимся устройством. Коммутатор анализирует адрес назначения в заголовке пакета и, сверившись с адресной таблицей, тут же (время задержки около 30—40 мкс) направляет этот пакет в соответствующий порт. Таким образом, его заголовок уже передается через выходной порт, хотя пакет еще целиком не прошел через входной.

Компьютерная сеть

Компьютерная сеть — это компьютеры, соединенные между собой средствами передачи информации. Эти средства достаточно разнообразны и применяются для решения возникающих на практике проблем. Их, тем не менее, можно разделить на программные средства, сетевое оборудование и кабельные системы.

В простейшем случае все компьютеры подсоединяются к одному и тому же коаксиальному кабелю и, тем самым, оказываются соединенными друг с другом. Но чаще используется более совершенная технология, в которой все компьютеры подсоединяются к специальному устройству, называемому концентратором, а для подключения применяется витая пара. В этом случае на каждом рабочем месте оборудуются розетки для подключения компьютера, а в центре, где будет установлен концентратор, — коммутационная панель. Эта же самая кабельная система может использоваться для подключения телефонов к офисной АТС. Расстояние от концентратора до рабочего места ограничено. Оно не может быть больше 100 м. Если есть необходимость подключить к сети достаточно удаленные рабочие места, то используется оптоволоконный кабель. Такой кабель позволяет подключить рабочее место, удаленное на 2000 м. Но стоимость такого соединения существенно выше. Различные модификации концентраторов обычно обеспечивают объединение от 4 до 24 компьютеров. Если на ваших компьютерах установлена операционная система Windows, то все необходимые программные средства для одноранговой сети у вас уже есть, их необходимо только задействовать, изменив конфигурацию операционной системы. Для более эффективной реализации работы в сети следует использовать специализированный компьютер — сервер, который применяется только для обеспечения работы в сети. Он отличается от обычных компьютеров тем, что при его проектировании предприняты специальные меры для повышения его надежности, расширяемости и безопасности. И это понятно, так как на нем чаще всего размещается жизненно важная для компании информация и от его работоспособности может зависеть трудоспособность всей компании. На сервер устанавливаются специальные программные средства, которые в состоянии эффективно обслуживать многочисленные запросы, поступающие с остальных компьютеров сети.

Коннектор

Распространенное название электрических разъемов, применяемых для соединения кабельных коммуникаций с оборудованием. Для соединения компьютеров и сетевого оборудования кабелем "витая пара" обычно применяют коннекторы RJ-45.

Концентратор (хаб, hub)

Устройство, которое "разветвляет" сеть на витой паре. Любая информация, пришедшая на один из его портов, через небольшое время отсылается через

все остальные порты. Соответственно, все порты хаба — двунаправленные. Количество портов концентратора — от 4 до 32.

Маршрутизатор (router)

Система, выбирающая один из нескольких путей передачи сетевого трафика. Для выполнения этой задачи используются маршрутизируемые протоколы, содержащие информацию о сети и алгоритмы выбора наилучшего пути на основе нескольких критериев, называемых метрикой маршрутизации (routing metrics). В терминах OSI маршрутизатор является промежуточной системой сетевого уровня. Маршрутизатор распознает адрес получателя и перенаправляет по нему пакет. Для этих целей возможно применение отдельного компьютера с несколькими сетевыми адаптерами. Маршрутизатор можно применять для связи различных сетей. Внутри одной сети применяются коммутаторы.

Модем

Сокращение от "модулятор/демодулятор". Модем преобразует последовательные цифровые (двоичные) данные, поступающие от оконечного устройства, в форму, пригодную для передачи по аналоговой телефонной линии. Второй модем (на приемном конце) выполняет обратное преобразование аналогового сигнала в цифровые данные, принимаемые другим устройством (получателем).

Одноранговая сеть

Сеть, в которой нет выделенных серверов, а все компьютеры, подключенные к сети, делят между собой свои же ресурсы.

Пакет

Информация в локальной сети передается блоками одинаковой длины — пакетами, в заголовках которых содержатся адреса отправителя и получателя. В IP-пакетах соответственно это IP-адреса, а в IPX-пакетах это Ethernet-адреса.

Порт

В широком смысле — место связи, точка подключения, "дверь" для входа на сервер или другое устройство. Существуют как физические порты (COM —

последовательные, LPT — параллельные и др.), так и программные, определяющие диапазон памяти процессора, который используется для подключения. Так, интернет-соединения используют порты 80 (HTTP), 21 (FTP) и др. Применение того или иного номера порта обусловлено лишь стандартами и договоренностями, необходимыми для равномерного распределения нагрузки на память компьютера и позволяющими работать максимальному числу процессов в одно время.

Протокол

Правила и язык общения компьютеров сети между собой. Наиболее популярные протоколы: NetBEUI (расширенный NetBIOS), IPX/SPX, TCP/IP. NetBEUI — устаревающий протокол, пригодный для маленькой сети, которая состоит из одного сегмента.

IPX/SPX — протокол для NetWare, его поддерживают все версии NetWare. У него есть подробности в виде типа кадра Ethernet (тип фрейма). Для того чтобы компьютеры в одной IPX-сети видели друг друга, они все должны работать на одинаковом типе кадра.

TCP/IP — интернет-протокол, ему посвящены целые книги. Сложный протокол, в домашней сети его имеет смысл использовать при наличии систем UNIX, маршрутизатора и/или выхода в Интернет, а также при работе с приложениями, применяющими этот протокол.

"Расшаренный диск"

Очень распространенное жаргонное выражение, ставшее обычным на Web-страницах пользователей и администраторов сетей и означающее диск общего доступа (shared disk) или область на диске, открытые для доступа другим объектам сети. От англ. *share* — разделять. "Шарить диски" — открывать диски для сетевого доступа или подключать чужие диски, предоставленные для доступа.

Сегмент сети

Это часть сети, в которой все компьютеры "видят" друг друга напрямую. Любая сеть состоит как минимум из одного сегмента. Сеть, состоящая из нескольких сегментов, имеет в своем составе более сложное сетевое оборудование, как-то: маршрутизатор, мост, коммутатор.

Сервер

1. Главный компьютер, содержащий централизованные данные и управляющий получением этих данных другими компьютерами. Обычно такой компьютер всегда включен и за ним практически никто не работает, ему даже монитор не очень нужен. На сервере выполняется сетевая операционная система — как правило, это Novell NetWare 3.*x*, 4.*x*, 5.*x*, Windows NT/2000 Server, UNIX (Linux, FreeBSD) и др.
2. В технологии "клиент-сервер": главная программа, управляющая работой подчиненных программ-клиентов.

Сервер удаленного доступа

Программное средство, обеспечивающее доступ к компьютеру для пользователей, находящихся вне локальной сети.

Сетевая плата

См. *Сетевой адаптер*.

Сетевой адаптер (сетевая карта, сетевая плата)

Устройство внутри компьютера (может быть встроенным в материнскую плату), позволяющее соединить этот компьютер с компьютерной сетью. Обычно используются адаптеры для кабельных сетей, но могут применяться и беспроводные адаптеры. Выпускаются сетевые адаптеры многими производителями, среди них: 3Com, Intel, DEC, AMD, Cabletron и др., но самая популярная сетевая карта — так называемая NE2000. Сетевые платы выпускаются в ISA-16 и PCI-вариантах, с разъемами BNC и/или UTP (TP), а иногда и с разъемом AUI. Каждая плата имеет уникальный адрес из шести байт, например 1E:34:00:00:FF:12, который называется Ethernet-адрес или MAC-адрес. По этому адресу каждый сетевой адаптер однозначно идентифицируется сервером, что позволяет повысить безопасность сети.

Сетевой кабель

Коаксиальный кабель с волновым сопротивлением 50 Ом или кабель "витая пара". В настоящее время коаксиальный кабель применяется реже витой пары. Это связано с тем, что локальная сеть на основе витой пары имеет больше возможностей для расширения и модификации.

Трансивер

Приемопередатчик. Физическое устройство, которое соединяет интерфейс хоста с локальной сетью, такой как Ethernet. Трансиверы Ethernet содержат электронные устройства, передающие сигнал в кабель и детектирующие коллизии.

Active Directory

Термин Active Directory используется как для обозначения каталога с информацией о пользователях, компьютерах и других объектах сети, так и для обозначения службы каталога — комплекса программ, обеспечивающих доступ к этой информации. Active Directory поддерживает систему имен DNS, а имена в формате NetBIOS использует только для совместимости со старыми операционными системами. В Windows XP вообще прекращена поддержка NetBIOS (хотя и может быть еще установлена). При наличии множества связанных серверов Active Directory позволяет хранить свою базу данных в распределенном виде и осуществлять автоматическую синхронизацию данных на всех серверах, входящих в домены Active Directory. Домены могут объединяться в деревья и леса.

AUI (Access Unit Interface)

Интерфейс устройств доступа; интерфейс подключаемых устройств. N-контактный кабельный интерфейс штекерного типа, используемый в магистральных соединениях.

Auto-sensing 10/100 Mbps (Автоматическое распознавание скорости передачи данных 10/100 Мбит/с)

Средство, позволяющее коммутаторам и концентраторам автоматически распознавать и настраивать скорость передачи данных по кабелю (называемое также *автосогласованием*). Интеллектуальные средства автораспознавания способны, кроме того, определять качество канала и автоматически выбирать максимальную скорость передачи.

BNC

Кабельный интерфейс для соединения коаксиального кабеля в магистральных сетях.

Bridge (мост)

Комбинация аппаратного и программного обеспечения, соединяющая две локальных сети и позволяющая осуществлять коммуникации между их станциями. Мосты функционируют на канальном (втором) уровне эталонной модели OSI (Open Systems Interconnection — модель взаимодействия открытых систем).

Bridge/Router (мост/маршрутизатор)

Устройство, функционирующее как мост, как маршрутизатор или как оба устройства одновременно.

Broadcast (широковещательная рассылка)

Передача сообщений всем адресатам сети.

Broadcast Domain (домен широковещательной рассылки)

Совокупность всех устройств, которые будут получать кадры широковещательной рассылки с любого устройства данной группы. Домены широковещательной рассылки, как правило, ограничиваются маршрутизаторами.

Broadcast Storm ("лавина" широковещательных пакетов)

Одновременная широковещательная рассылка пакетов несколькими отправителями, обычно поглощающая значительную часть доступной полосы пропускания сети и способная вызвать тайм-ауты.

CSMA/CD

Метод доступа к среде передачи (кабелю), определенный в спецификации IEEE 802.3 для локальных сетей Ethernet. CSMA/CD требует, чтобы каждый узел, начав передачу, продолжал прослушивать сеть на предмет обнаружения попытки одновременной передачи другим устройством — коллизии. При возникновении конфликта, передача должна быть незамедлительно прервана и может быть возобновлена по истечении случайного промежутка времени. В сети Ethernet с загрузкой 35—40% коллизии возникают довольно часто и могут существенно замедлить работу. При небольшом числе станций вероятность коллизий существенно снижается.

DHCP (Dynamic Host Configuration Protocol)

Служба динамического выделения сетевых адресов. Позволяет не загружать администратора сети проблемами распределения адресов, работает автоматически.

DNS (Domain Name System)

1. Символьный идентификатор — имя типа **serv.firma.ru**. Этот адрес назначается администратором и состоит из нескольких частей: имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, используется на прикладном уровне, например в протоколах FTP или Telnet.
2. Распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Интернет. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.
3. Распределенный механизм имен/адресов, используемых в сети Интернет. Применяется для разрешения логических имен в IP-адреса. В Интернете позволяет работать с понятными и легко запоминающимися именами вместо неудобных числовых IP-адресов.

DOS ODI и DOS NDIS

Сетевые драйверы, поддерживающие большинство ОС, в том числе Novell NetWare, Microsoft 9*x*, Microsoft Windows for Workgroups, Microsoft LAN Manager, Banyan VINES, Artisoft LANtastic, IBM LAN Server, HP LAN Manager и многие другие.

Ethernet

Самый распространенный стандарт компьютерных сетей. Имеет несколько модификаций и вариантов, которые совместимы друг с другом. Конкретные реализации обозначаются как 802.10 — обычные локальные сети, 802.11b — радиосети, существуют и другие варианты.

Fast Ethernet

Широко распространенный протокол локальных вычислительных сетей, поддерживающий скорости передачи данных 10 и 100 Мбит/с.

FTP (File Transfer Protocol)

Протокол передачи данных в сети. Применяется для передачи файлов.

HTML

Язык гипертекстовой разметки. Средство создания страниц для публикации в Интернете и последующего просмотра с помощью браузера. HTML-страницы могут применяться и для обмена информацией в локальной сети, а также для хранения информации в виде HTML-файлов.

Hub (хаб)

См. *Концентратор*.

Interface

1. Физическое устройство, соединяющее две системы или два устройства.
2. Стандарт (такой как RS-232-C), специфицирующий взаимодействие систем.

ISDN (Integrated Service Digital Network)

Международный стандарт передачи голоса, видеоинформации и данных по цифровым телефонным линиям.

LAN (Local Area Network)

Локальная компьютерная (вычислительная) сеть. Русское сокращение — ЛВС.

LINKLOCAL

Диапазон сетевых адресов, применяемых в локальных компьютерных сетях и не используемых в глобальных сетях.

MAC-адрес

Аппаратный адрес сетевого устройства. Не может повторяться, обеспечивает идентификацию сетевого устройства независимо от назначаемого адреса или имени.

NetBIOS

NetBIOS (Network Basic Input/Output System) — протокол для взаимодействия программ через компьютерную сеть. NetBIOS находится на сеансовом и транспортном уровне модели OSI.

Протокол NetBIOS был разработан в 1983 году компанией Sytek для локальной сети персональных компьютеров. Интерфейс был разработан для малых сетей; он поддерживал не более 80 компьютеров одновременно. Однако благодаря тому, что стандарт был изначально опубликован в руководстве от IBM, он стал стандартом де-факто. Применяется метод работы NetBIOS поверх протокола TCP (см. *NetBEUI*).

NetBEUI

NetBEUI (NetBIOS Extended User Interface) — расширенный интерфейс датаграммной передачи NetBIOS.

Протокол, используемый как механизм передачи для NetBIOS на основе широковещательных рассылок. Этот протокол является реализацией стандарта NetBIOS. Сейчас вместо NetBEUI обычно применяется NBT (NetBIOS over TCP/IP — NetBIOS поверх TCP/IP). Как правило, NetBEUI используется в сетях, где нет возможности использовать NetBIOS, например в компьютерах с установленной MS-DOS.

Network mask

32-битовое число, показывающее диапазон IP-адресов, находящихся в одной IP-сети/подсети.

Proxy Server (Proxy-сервер)

Это система, находящаяся между исполняемыми приложениями (такими как Internet Explorer) и соединением с Интернетом. Она перехватывает запросы к серверу, пытаясь выполнить их самостоятельно. Такой способ увеличивает

быстродействие за счет отсечения повторных запросов одной и той же информации из Интернета. Proxy-сервер может кэшировать загружаемые из Интернета страницы (файлы). Если кто-то еще обращается к странице или файлу, ранее уже кем-либо запрошенным, Proxy-сервер выдает их из своего кэша. Это значительно быстрее, чем снова загружать страницу (файл) из Интернета. Proxy-серверы также могут выступать в качестве сетевого экрана, фильтруя IP-трафик по порту или IP-адресу.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Современный сетевой протокол. Подробно описан в *приложении 2*.

Telnet

Это один из старейших протоколов Интернета. Он появился в 1969 году в ARPANET (сеть государственной организации The Advanced Research Projects Agency — бюро проектов передовых исследований. Теперь организация называется *DARPA*). Имя этого протокола является сокращением от названия telecommunications network protocol (сетевой коммуникационный протокол). Его описание находится в спецификации RFC 854. Этот протокол позволяет подсоединиться к удаленному компьютеру, находящемуся в сети, и работать с ним как будто бы вы работаете непосредственно на этом удаленном компьютере, т. е. в режиме терминала. Ваши возможности ограничены уровнем доступа, который задан для вас администратором удаленной системы.

В поставку Windows входит одноименная программа, которую вы можете запустить из меню **Пуск | Выполнить**.

Throughput (производительность, пропускная способность)

Общий объем корректно переданной (или обработанной) информации в заданный период времени. Выражается в битах в секунду или в пакетах в секунду.

UTP (неэкранированная витая пара)

Это самый популярный тип кабеля, используемый для соединения настольных систем и рабочих групп. См. *Витая пара*.

Virtual LAN (VLAN, виртуальная локальная сеть)

Виртуальная локальная сеть (VLAN) состоит из связанной группы пользователей, которые могут осуществлять коммуникации непосредственно друг с другом и получать широковещательную информацию от других пользователей. При этом входящие в группу пользователи необязательно должны находиться в одном месте. В сетевой инфраструктуре, основанной на многопортовых коммутаторах и концентраторах, все рабочие станции могут взаимодействовать непосредственно друг с другом и получать друг от друга широковещательные пакеты. В такой сети виртуальные локальные сети (VLAN) применяются для управления трафиком, обеспечения защиты и для контроля широковещательной рассылки.

VPN

См. *Виртуальная частная сеть*.

WAN (Wide Area Network, территориально распределенная сеть)

Глобальная сеть. Сеть, обеспечивающая передачу информации на значительные расстояния с использованием коммутируемых и выделенных линий или специальных каналов связи. Сеть, охватывающая область, превышающую по размеру район или город.

WINS (Windows Internet Name Service)

Служба определения адресов, преобразующая имена компьютеров в сети (NetBIOS) в IP-адреса.

Если вы используете NetBIOS поверх TCP/IP, необходимо запустить WINS для определения корректных IP-адресов.

10BASE-2 (тонкий коаксиальный кабель)

Спецификация IEEE 802.3 сетей Ethernet на тонком коаксиальном кабеле.

10BASE-5 (толстый коаксиальный кабель)

Спецификация IEEE 802.3 сетей Ethernet на толстом коаксиальном кабеле.

10BASE-FL (оптоволоконный кабель 10 Мбит/с)

Часть спецификации IEEE 10BASE-F, охватывающая сети Ethernet на оптоволоконном кабеле. Она совместима со спецификацией FOIRL (Fiber Optic Inter Repeater Link — волоконно-оптическая связь между повторителями (репитерами)).

100BASE-FX (оптоволоконный кабель 100 Мбит/с)

Реализация сети Ethernet на оптоволоконном кабеле, обеспечивающая скорость передачи данных 100 Мбит/с.

10BASE-T (витая пара 10 Мбит/с)

Спецификация IEEE 802.3 сетей Ethernet на неэкранированной витой паре (UTP).

100BASE-T (Fast Ethernet)

Технология 100 Мбит/с, основанная на методе доступа Ethernet/CD и использующая кабель "витая пара".

Предметный указатель

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

А

Б

В

Д

З

И

К

Л

М

Н

О

П

P

C

T

У

Ф

Х

Ц

Ч

Ш

Я