Александр Поляк-Брагинский

Сеть своими руками

Санкт-Петербург

«БХВ-Петербург»

2002

УДК 681.3.06
ББК 32.973.202
П54Б

Поляк-Брагинский А. В.

П54Б Сеть своими руками. — СПб.: БХВ-Петербург, 2002. — 320 с.: ил.

ISBN 5-94157-144-5

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. Рассмотрены примеры построения конкретных сетей. Представлено обстоятельное описание программ WinRoute, Radmin, Courier Mail Server и других, позволяющих создать полнофункциональную сеть. Даны многочисленные ссылки на соответствующие ресурсы в Internet.

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	*Анна Кузьмина*
Редактор	*Владислав Борисов*
Компьютерная верстка	*Татьяны Олоновой*
Корректор	*Татьяна Звертановская*
Дизайн обложки	*Игоря Цырульникова*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 25.04.02.
Формат $70\times100^{1}/_{16}$. Печать офсетная. Усл. печ. л. 25,8.
Тираж 4000 экз. Заказ №
"БХВ-Петербург", 198005, Санкт-Петербург, Измайловский пр., 29.

Гигиеническое заключение на продукцию, товар № 77.99.02.953.Д.001537.03.02
от 13.03.2002 г. выдано Департаментом ГСЭН Минздрава России.

Отпечатано с готовых диапозитивов
в Академической типографии "Наука" РАН
199034, Санкт-Петербург, 9 линия, 12.

ISBN 5-94157-144-5

Содержание

Введение

Ваша первая сеть

На дворе уже двадцать первый век. Вся наша жизнь подчинилась компьютерным технологиям, хотим мы того или нет. Все чаще возникает необходимость в оперативной связи между компьютерами, будь то наш дом или офис, где мы работаем. Компьютеры теперь есть практически у каждого (во всяком случае, из тех, кто читает эту книгу), но объединение компьютеров в сеть считается до сих пор задачей весьма сложной, требующей специальной подготовки, и невыполнимой рядовым пользователем самостоятельно. Эта книга поможет вам создать свою сеть. Вам необходимо лишь решиться на этот шаг, согласовать вопросы строительства сети с друзьями или сотрудниками, возможно с владельцем здания или помещения, где вы хотите организовать сеть. Определившись с потребностями, приобрести недостающие детали и оборудование.

Назначение сети может быть самым разнообразным. Независимо от конкретных задач, общие принципы построения сети одинаковы. В необходимых случаях мы обратим внимание на особенности именно вашей сети, предназначенной для выполнения конкретной задачи, но большинство рекомендаций подойдут для всех.

Постепенно 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 — средство экономии некоторой суммы, которую надо 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 в выигрыше. Уже имея даже минимальный опыт общения с сетью, вы никогда не позволите "запудрить себе мозги" заумными фразами.

В основе большинства примеров будет работа в среде операционных систем Windows 9*x*, как самых распространенных среди пользователей ПК. Существующие специализированные сетевые операционные системы требуют отдельного рассмотрения и в книге представлены лишь описания некоторых из них. Применение таких систем оправдано при построении сетей

с особыми характеристиками и требованиями к ним, а сложность их требует более серьезной подготовки для поддержки и администрирования.

В качестве базовой операционной системы будет рассматриваться Windows 98, как наиболее распространенная в настоящее время. В случаях, когда возможностей этой операционной системы окажется недостаточно, обратимся к Windows 2000. Операционная система — продукт дорогой, и модернизация, а тем более замена оборудования требуют немалых вложений. Используя существующие парк оборудования и комплект программного обеспечения, необходимо взять от них все возможное, и только после этого делать новые приобретения.

Конечно, совсем ничего не приобретая, не удастся реализовать и наши недорогие проекты. Придется купить кое-что из оборудования и программного обеспечения, но затраты будут минимальными. Конкретный уровень затрат прогнозировать сложно, все зависит от того, что у вас уже есть и какие требования к своей сети вы выдвигаете.

Требования к компьютерам нашей сети не выше, чем требования со стороны операционной системы.

Таким образом, книга поможет практически войти в мир локальных сетей. Если вы почувствуете необходимость в получении дополнительной информации и знаний о сетях, то необходимая база для этого у вас уже будет, а созданная вами первая ваша сеть будет работать на вас.

Благодарности

Перед тем как перейти к первой главе, считаю необходимым поблагодарить тех, без чьего содействия написание этой книги стало бы невозможным. Все перечисленные ниже господа, в той или иной степени причастны к написанию этой книги, иногда сами того не подозревая.

Огромную благодарность выражаю Павлову Александру Робертовичу, Китросеру Михаилу Борисовичу, Яковлеву Вячеславу Максимовичу.

Глава 1

Построение локальных вычислительных сетей

На сегодняшний день в мире существует более двухсот миллионов компьютеров, большинство из которых объединены в различные информационно-вычислительные сети. Зачем компьютеры объединяются 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) в условиях организации или у вас дома? Ответы на эти и другие теоретические и практические вопросы построения ЛВС вы можете найти в данной главе.

Для чего нужна сеть

Использование сети предоставляет пользователям следующие дополнительные возможности:

- оперативного обмена информацией между пользователями;
- получения и передачи сообщений в виде 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 более детально основные преимущества, которые предоставляет пользователям объединение компьютеров в сеть:

1. Разделение ресурсов, что предполагает совместное использование периферийных устройств, таких как принтеры, а также дискового пространства удаленных компьютеров, что позволяет более рационально использовать имеющуюся дисковую память и принтеры.

2. Разделение данных — предоставление доступа и возможности управления базами данных с удаленных рабочих мест, имеющих в этом необходимость.
3. Совместное применение программных средств.
4. Использование вычислительной мощности удаленного процессора, что позволяет существенно снизить затраты на модернизацию оборудования, обновление парка компьютеров, поскольку появляется возможность получить терминальный доступ, когда компьютер с небольшими возможностями подключается к более мощному компьютеру и используется как удаленный терминал — клавиатура с дисплеем и средство связи с удаленной рабочей станцией.
5. Возможность многопользовательского режима работы с программами и документами.

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

Варианты использования сети

Пользователи могут использовать предоставляемые сетью дополнительные возможности полностью или частично, постоянно или временно. Это зависит от конкретной задачи, ради которой применяется данная сеть, т. е. от ее назначения. Рассмотрим несколько вариантов применения сети для различных целей.

Сеть для работы

Здесь имеется в виду работа, связанная с обработкой текстовых и графических материалов, вычислениями, обращением к базе данных, т. е. та работа, которая выполняется коллективно, но распределена в пространстве и времени таким образом, что только связь между компьютерами позволяет оперативно использовать результаты работы коллеги 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 прав доступа, получать информацию или использовать ресурсы другого компьютера.

Возможно, что один компьютер выделен особо. Его ресурсы могут использоваться всеми пользователями и в его памяти сохраняются результаты труда всей группы, поскольку надежность хранения информации в этой выделенной машине может быть выше, чем в остальных. Такой компьютер называется файл-сервер. Повышенная надежность может быть обеспечена особым устройством дисковой подсистемы компьютера, что, несомненно, отразится на его цене. 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, чем, собственно, и занимаются вышеупомянутые дорогостоящие дисковые

подсистемы, но в автоматическом режиме. Следует отметить, что при написании этой книги использовалась примерно такая сеть, поскольку 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, причем с выделенного компьютера должен быть доступ к каждому компьютеру класса с возможностью вмешательства в его работу и работу учащегося. Обратный доступ от учащегося к преподавателю может быть 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 распределенным по территории организации для обучения сотрудников на рабочих местах. В этом случае повышенные требования предъявляются к компьютеру преподавателя, а остальные компьютеры могут быть самыми обычными. Само собой разумеется, что такая организация сети может применяться и совершенно в иных целях. Возможно, 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

Сеть, отвечающую такому расплывчатому требованию, конкретно определить трудно, поскольку и два предшествующих варианта могут быть вариантами бизнеса. Но все же некоторые особенности такой сети можно выделить. Несколько компьютеров данной сети могут иметь специализированное назначение, при этом доступ к каждому из них ограничен для большинства пользователей. Свободный доступ предусмотрен только к части информации, которую могут использовать специалисты. Так, возможно деление сотрудников на кадровую службу, бухгалтерию, отдел продаж и другие отделы. Вы, как руководитель и сетевой администратор, получаете доступ ко всем ресурсам для возможности 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, пожалуй, применяются максимальные требования к ресурсам компьютеров (память, быстродействие), а также к оснащенности наиболее новыми версиями программ поддержки игр и устройствами, обеспечивающими

работу этих программ. Но эти требования не связаны непосредственно с характеристиками сети. Вызваны они лишь особенностями программного обеспечения, применяемого на компьютерах. Не только игры могут вызвать повышенные требования к компьютерам сети, но и работа с графикой, аудио- и видеомонтаж. Для коллективной игры должна быть обеспечена возможность подключения одного пользователя к нескольким другим.

Рассмотренные варианты сети имеют много отличий, но с точки зрения технологии построения сети они мало отличаются. Сеть универсальна и ее качество зависит в большей степени от настроек сетевого программного обеспечения отдельных компьютеров и применяемого сетевого оборудования.

Предпосылки для организации сети

Предпосылками для организации сети могут быть следующие условия:

- некоторое количество отдельно работающих 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 требуемой оперативностью доступа;
- накопленное программное и информационное обеспечение, не используемое в полном объеме и не имеющее общего стандарта хранения;
- возможность подключения к глобальной вычислительной сети (например, Internet) ограничена подключением отдельных пользователей, не имеющих связи с другими компьютерами, что снижает эффективность данного подключения и требует дополнительных расходов для расширения доступа к глобальной сети в виде организации дополнительных подключений.

Вас такое положение не устраивает, и изменить ситуацию может только организация вычислительной сети в соответствующих вашим условиям масштабах, объединяющей весь парк компьютеров (всех пользователей) в единое информационное пространство (ЕИП), обладающее следующими свойствами:

- система хранения и обработки данных, созданных в разное время и разными пользователями, доступна всем пользователям сети в любой момент времени, что позволяет повысить оперативность и эффективность решения многих задач за счет коллективного использования данных и результатов работы каждого. При этом возможен оперативный контроль над ходом работы, согласование и объединение ее результатов с целью получения максимально эффективного готового решения;
- достоверность и надежность хранения информации повышены за счет высокой помехоустойчивости и отказоустойчивости системы, обеспечи-

ваемой благодаря эффективному резервированию и организации архивного хранения данных;

- упрощенный поиск необходимой информации за счет использования объединенного архива;
- стандартизация документооборота в соответствии с общими требованиями;
- обеспечение доступа к информации авторизованному пользователю в соответствии с данными ему правами доступа и привилегиями.

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. Но вот наступил момент, когда организация сети 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 бесплатно раздают редко. 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 территориально 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, при условии, что это Windows. Итак, с чего начать построение сети?

Решение возможных нетехнических проблем

При организации сети вы можете столкнуться не только с техническими трудностями. Например, когда сеть должна расположиться на значительной площади, занимая несколько помещений или даже выходя за рамки одного здания. В этом случае придется согласовывать свои действия с владельцем или владельцами помещения, если оно не ваше, с местной администрацией, если кабель должен каким-то образом пересечь часть территории населенного пункта. Кроме неизбежных материальных проблем, могут возникнуть проблемы психологического 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 (не обязательно материальную). Если вы действительно заинтересованы в организации сети, то у вас все получится.

Компьютер1 + Компьютер2

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, а также телефонная сеть, к которой компьютеры подключены посредством модемов.

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

Основные сведения о ЛВС

Под локальной вычислительной сетью понимают совместное подключение нескольких отдельных компьютерных рабочих мест (рабочих станций) к единому каналу передачи данных, при котором пользователи получают возможность одновременного использования программ и баз данных, находясь на своих рабочих местах.

В современной технической литературе часто применяется другое сокращение для этого понятия — англоязычное LAN (Local Area Network).

Посредством ЛВС пользователи персональных компьютеров, расположенных на удаленных рабочих местах, могут совместно использовать оборудование, программное обеспечение и информацию. Ликвидируются ограничения, наложенные географическим, пространственным разделением рабочих мест.

Многоуровневая модель сети

Для обеспечения единообразного представления данных при передаче информации в линиях связи была сформирована Международная организация по стандартизации (ISO — International Standards Organization). Эта организация предназначена для разработки модели международного коммуникационного протокола, в рамках которой должны создаваться международные стандарты систем передачи данных.

ISO разработала базовую модель взаимодействия открытых систем (OSI — Open Systems Interconnection). Эта модель стала международным стандартом для разработки 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 вышестоящими и нижестоящими уровнями называются *протоколом*.

Процесс взаимодействия пользователя с сетевой средой заключается в последовательном преобразовании передаваемых пользовательских данных на передающей стороне от седьмого уровня до первого с последующим обратным преобразованием 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 MKKTT (CCITT), EIA RS232, X.21 и другие. Все большее значение для функции передачи данных приобретает

стандарт ISDN (Integrated Services Digital Network, Цифровой сети с интеграцией услуг). 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 функциям 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 обеспечиваются благодаря возможности обнаружения и исправления ошибок и аппаратно-независимой реализации сервиса транспортировки.
- Сеансовый уровень обеспечивает управление диалогом, то есть 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 дополнительно содержит функции управления паролями, подсчета оплаты за использование ресурсов сети, синхронизации и отмены связи в сеансе передачи после сбоя вследствие ошибок в нижерасположенных 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 информации по коммуникационным линиям она преобразуется в цепочку следующих друг за другом битов (двоичное кодирование с помощью двух состояний: "0" и "1").

Передаваемые алфавитно-цифровые знаки представляются с помощью 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. Четырехбитовый 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.

Среда передачи данных

В любой сети информация от одного компьютера до другого передается через некоторую среду передачи данных. Предметом нашего рассмотрения станут кабельные сети. В таких сетях информация в форме электрического сигнала передается по кабелю. На сегодняшний день для построения сетей применяются три вида кабелей:

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

Последний вариант не нашел своего освещения в данной книге вследствие его относительной дороговизны. Не исключено, конечно, что, получив необходимый опыт работы в сетях, у вас появится желание усовершенствовать вашу сеть и перейти на волоконно-оптический кабель и соответствующее ему оборудование, поскольку 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).

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 провод-

ник 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.

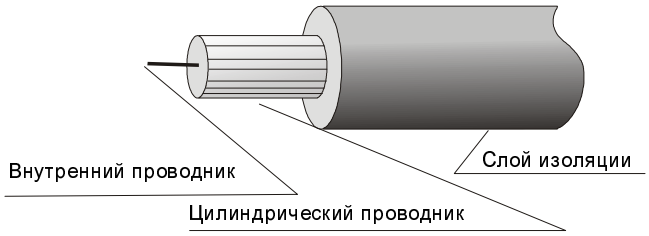

Рис. 1.1. Устройство коаксиального кабеля

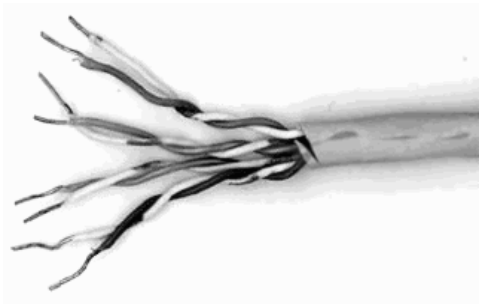

Рис. 1.2. Кабель на основе витой пары

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 скорость до 4 Мбит/с включительно
3	Используется для передачи данных со скорость до 10 Мбит/с включительно. Применяется в сетях
4	Используется для передачи данных со скорость 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 различающимися типами компьютеров применяют различные коды. Для правильной и, следовательно, полной и безошибочной передачи данных необходимо придерживаться согласованных и установленных правил. Все эти правила оговорены в *протоколе* передачи данных.

- Протокол передачи данных описывает составляющие и свойства процесса передачи данных.
- Синхронизация — механизм распознавания начала блока данных и его конца.
- Инициализация — установление соединения между взаимодействующими партнерами.
- Блокирование — разбиение передаваемой информации на блоки данных строго определенной максимальной длины (включая опознавательные знаки начала блока и его конца).
- Адресация — обеспечение идентификации различного используемого оборудования, которое обменивается друг с другом информацией во время взаимодействия.
- 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 не хватает места в буфере устройства или данные недостаточно быстро обрабатываются в периферийных устройствах (например, принтерах), 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 к данным вменяются в обязанность пункта разрешения 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, позволяющим осуществлять неискаженную передачу информации от одного компьютера сети к другому, а также добиться

совместимости компьютеров и 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/Internet-протокол). Задуманы эти протоколы для работы в сети Internet, 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 рассылает 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 четырехбайтную 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	10.0.0.0 127.0.0.0
B	255.255.0.0	128.0.0.0 — 191.255.0.0	169.254.X.X С 172.16.0.0 по 172.31.0.0
C	255.255.255.0	192—222	С 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 Internet (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. Адрес 198.168.55.1 в двоичном коде выглядит так: 11000110.10101000.110111.1. По таблице можно определить, что это адрес сети класса "С", 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.

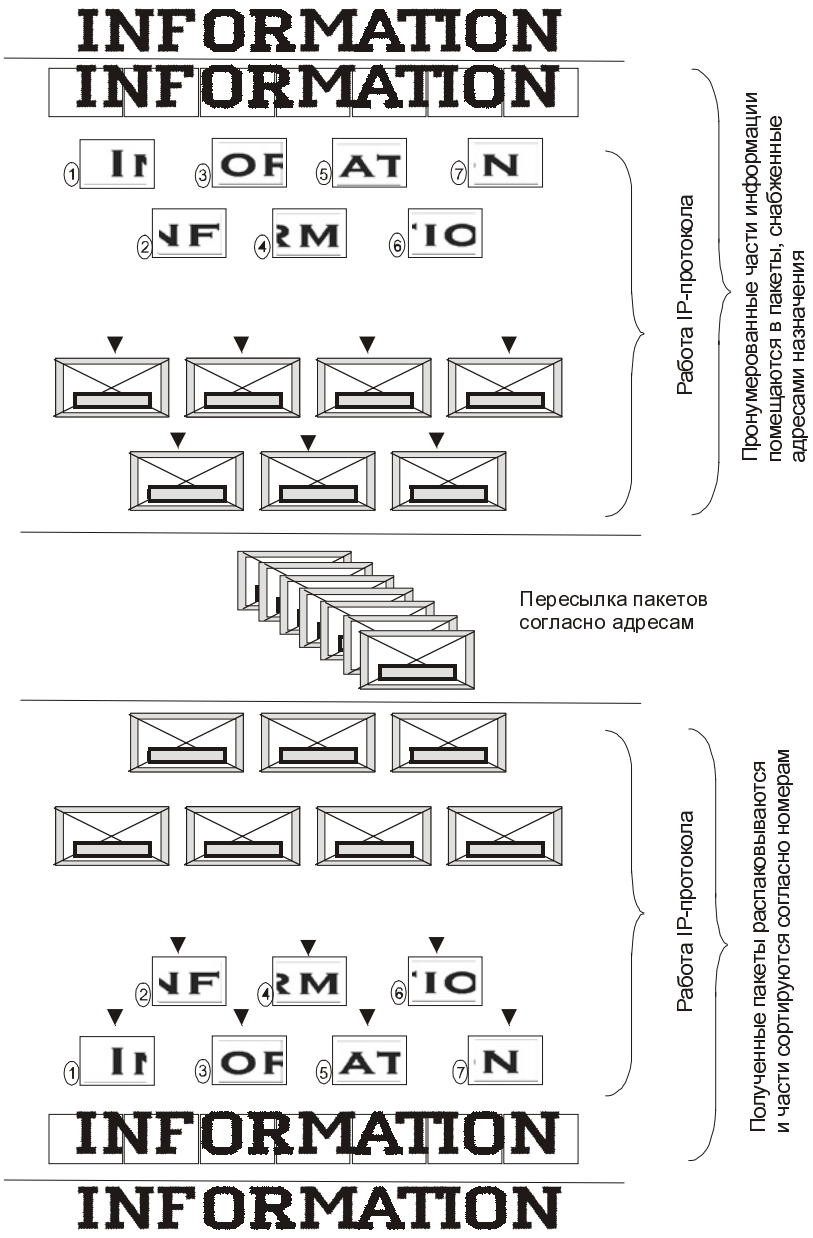

Рис. 1.3. Передача информации по IP-протоколу

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. NETBIOS (Network Basic Input/Output System, сетевая базовая система ввода-вывода) — это протокол, дополняющий спецификацию интерфейса NetBIOS, используемую сетевой операционной системой. NetBEUI формализует кадр транспортного уровня, не стандартизованный в NetBIOS. Данный интерфейс соответствует не какому-то конкретному уровню модели OSI, а охватывает транспортный уровень, сетевой уровень и подуровень LLC канального уровня. NetBEUI взаимодействует напрямую с NDIS уровня MAC. Таким образом, это не маршрутизируемый 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.

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 использовать преимущественно стандарт Ethernet, широко используемый в России и подходящий для работы с распространенными операционными системами и сетевым оборудованием. 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 более чем в пяти миллионах сетей, в которых задействовано свыше пятидесяти 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" эту сеть, а точнее 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 компь-

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

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

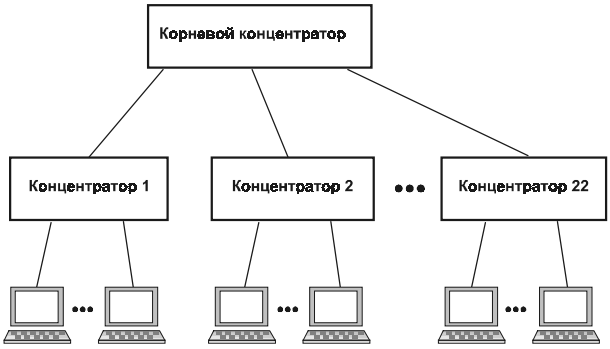

Рис. 1.4. Возможный вариант построения сети

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 такой вариант, как изображенный 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.

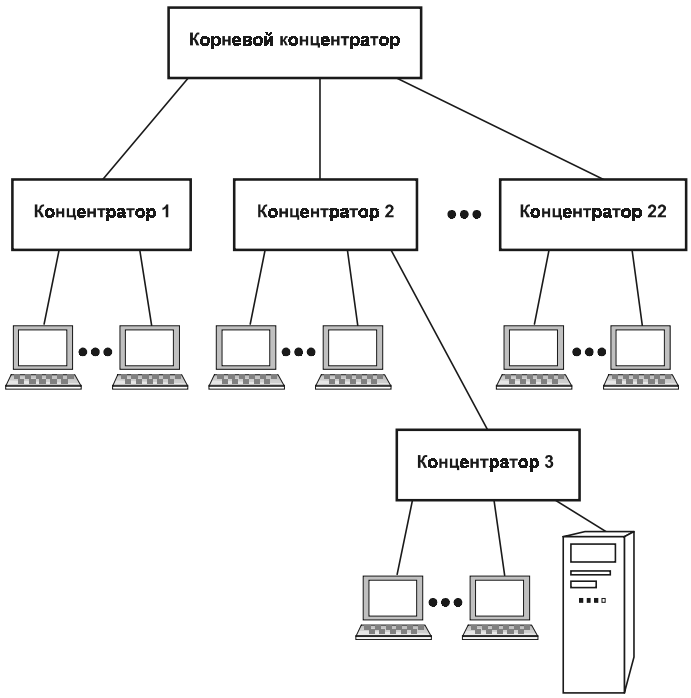

Рис. 1.5. Еще один вариант построения сети

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

Таблица 1.3 *(окончание)*

Характеристика	10Base-5	10Base-2	10Base-T	10Base-F
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.

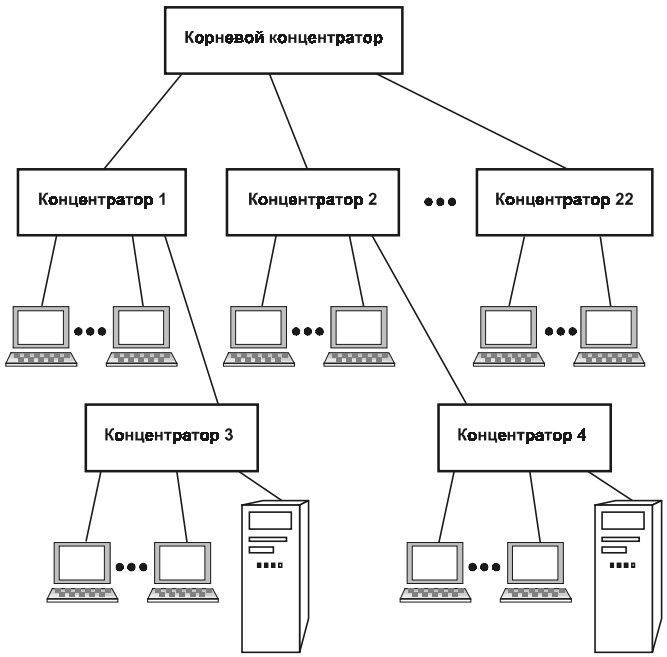

Рис. 1.6. Неправильный вариант построения сети

Если, например, мы хотим организовать сеть, расположенную на нескольких этажах или даже в разных зданиях, то вполне оправдано 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 устройств, достигает пятисот метров (для толстого кабеля), что позволит соединить между собой достаточно удаленные друг от друга помещения.

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

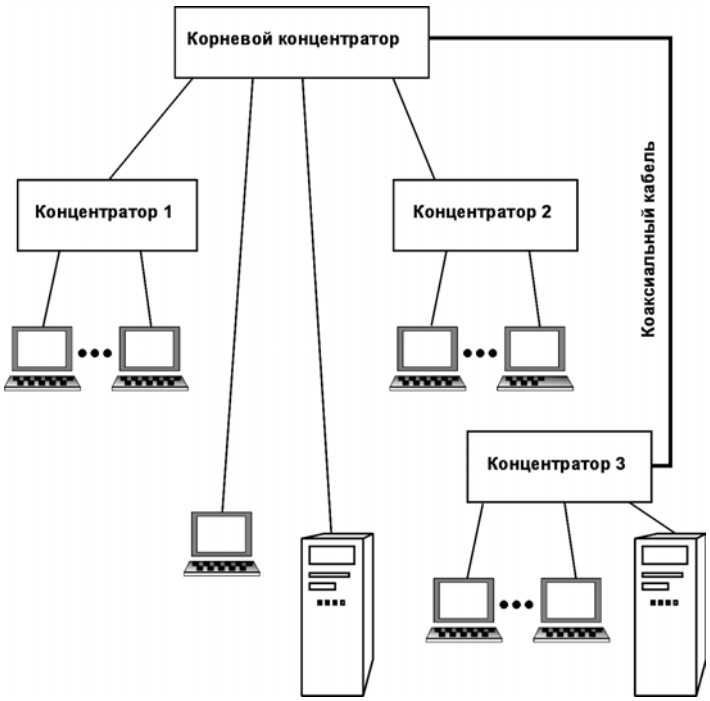

Рис. 1.7. Вариант построения сети с применением коаксиального кабеля (некоторые подробности опущены)

Существуют и другие протоколы и стандарты для построения сетей.

В 1980 году в IEEE был организован комитет 802 по стандартизации локальных сетей. Результаты работы этого комитета легли в основу комплекса международных стандартов ISO 8802-1...5. Эти стандарты 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 уход со сцены, по крайней мере, в течение нескольких лет.

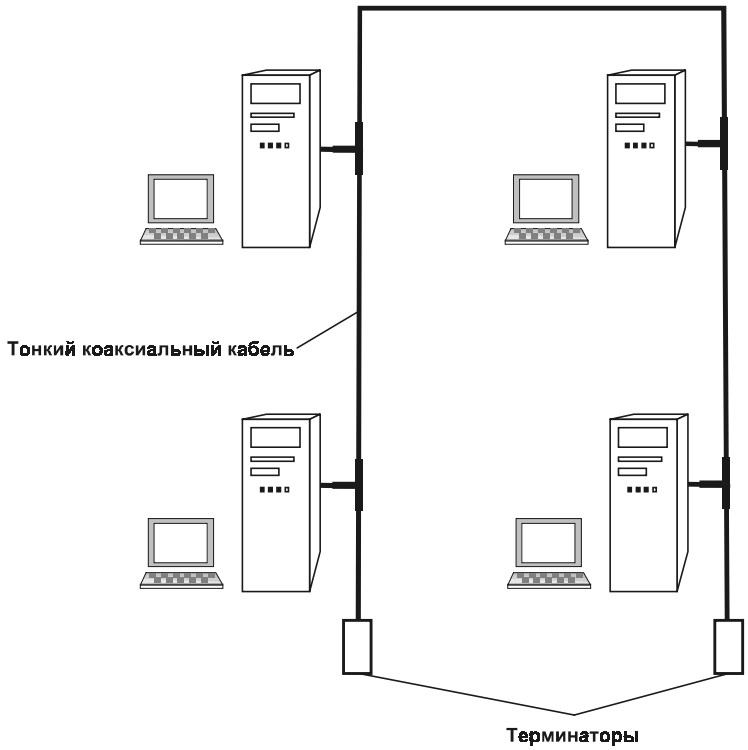

Рис. 1.8. Сеть 10Base-2

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 компьютера находятся в неравном положении. Один посылает некоторый запрос, другой должен определенным образом отреагировать на этот запрос. Проситель выступает в роли клиента, а просимый — в роли сер-

вера. В ряде случаев компьютеры могут меняться ролями в процессе общения, но в каждый момент времени один клиент, другой сервер. 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 Internet, сервер печати, обеспечивающий клиентов доступом к принтерам сети. Словом, если требуется оказать услугу, то сервер окажет ее клиенту. 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 важно в больших сетях, где сервер работает с большой нагрузкой и требуется высокая стабильность его работы. Существуют операционные системы, специально 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 множество приложений рассчитано для работы в режиме клиент-сервер. Это позволяет нескольким пользователям обращаться к одним и тем же файлам без риска разрушить или испортить информацию. Распространенный во всем мире комплект MS Office 97/2000 как раз поддерживает работу в таком режиме, что может быть особенно полезно для приложений Excel и Access, позволяющих создавать удобные специализированные приложения как для организаций, так и для личного применения и работать с базами данных. Возможно применение нескольких операционных систем в одной сети и нескольких серверов. Это позволяет 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 само по себе понятие сервера и клиента совсем необязательно неразрывно связано 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.

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. Это позволяет реализовать все наши потребности в плане сете-

вого сервиса на основе распространенных Windows 95/98. Эти операционные системы обладают множеством положительных качеств, но 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 менее подвержена различного рода сбоям. Следовательно, на сервере она должна работать более устойчиво. Для выделенного сервера обычно выделяется отдельное помещение.

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 которому они все должны быть подключены. Все рабочие станции могут непосредственно вступать в контакт с любой рабочей станцией, имеющейся в сети.

Рабочие станции в любое время, без прерывания работы всей вычислительной сети, могут быть подключены к ней или отключены. 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. Выключение и особенно подключение к такой сети требуют разрыва шины, что вызывает нарушение циркулирующего потока информации и зависание системы.

Существуют пассивные штепсельные коробки, через которые можно отключать и/или включать 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 может существовать только одна передающая информацию станция. Для предотвращения коллизий (столкновений данных) в большинстве случаев применяется временной метод разделения, согласно которому 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 снижаются, например, при вводе новых рабочих станций. 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. Пересылаемые данные модулируются на соответствующих несущих частотах, т. е. между средой передачи информации и рабочими станциями находятся, соответственно, модемы для модуляции и демодуляции. Техника широкополосных сообщений позволяет одновременно транспортировать в коммуникационной среде довольно большой объем информации. Для дальнейшего развития дискретной транспортировки данных не играет роли, какая первоначальная информация подана в модем (аналоговая или цифровая), так как в дальнейшем она все равно будет преобразована.

Топология типа звезда

Концепция топологии сети в виде звезды пришла из области больших ЭВМ, в которой головной компьютер получает и обрабатывает все данные с периферийных устройств как активный узел обработки данных. Этот принцип применяется в системах передачи данных, например, в электронной почте RELCOM. Вся информация между двумя периферийными рабочими местами проходит через центральный узел вычислительной сети. Пропускная способность сети определяется вычислительной мощностью 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 географически расположен не в центре топологии. При расширении вычислительных сетей нельзя использовать ранее выполненные кабельные связи: к новому рабочему месту необходимо прокладывать отдельный кабель из центра сети.

Топология в виде звезды является наиболее быстродействующей из всех топологий вычислительных сетей, поскольку передача данных между рабочими станциями проходит через центральный узел по отдельным линиям, используемым только этими рабочими станциями. 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 3 с рабочей станцией 4 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 географически рабочие станции расположены далеко от кольца (например, в линию).

Сообщения циркулируют регулярно по кругу. Рабочая станция посылает по определенному конечному адресу информацию, предварительно получив из кольца запрос. Пересылка сообщений является очень эффективной, 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 пропорционально количеству рабочих станций, входящих в вычислительную сеть.

Основная проблема при кольцевой топологии заключается в том, что каждая рабочая станция должна активно участвовать в пересылке информации, и в случае выхода из строя хотя бы одной из них вся сеть парализуется. Неисправности в кабельных соединениях локализуются легко.

Подключение новой рабочей станции требует краткосрочного выключения сети, так как во время установки кольцо должно быть разомкнуто. Ограничения на протяженность вычислительной сети не существует, так как оно, в конечном счете, определяется исключительно расстоянием 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 (англ. *Hub* — концентратор), которые по-русски также иногда называют "хаб". В зависимости от числа рабочих станций и длины кабеля между рабочими станциями, применяют активные или пассивные концентраторы. Активные концентраторы дополнительно содержат усилитель для подключения от 4 до 32 рабочих станций. Пассивный концентратор выполняет исключительно функции разветвителя (максимум на 3 рабочие станции). Управление отдельной рабочей станцией в логической кольцевой сети происходит так же, как и в обычной кольцевой сети. Каждой рабочей станции присваивается соответствующий ей адрес, по которому передается управление (от старшего к младшему и от самого младшего к самому старшему). Разрыв соединения происходит только для нижерасположен-

ного (ближайшего) узла вычислительной сети, так что лишь в редких случаях может нарушаться работа всей сети.

Смешанные топологии

Наряду с известными топологиями вычислительных сетей кольцо, звезда и шина, на практике применяется и комбинированная, например, древовидная структура. Она образуется в основном в виде комбинаций вышеназванных топологий вычислительных сетей. Основание дерева вычислительной сети располагается в точке (корень), в которой собираются коммуникационные линии информации (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. Коммутатор, обладающий одновременно и функциями усилителя, называют *активным концентратором*.

На практике применяют их разновидности, обеспечивающие подключение от 8 или 32 линий.

Устройство, к которому можно присоединить максимум три станции, называют *пассивным концентратором*. Пассивный концентратор обычно используют как разветвитель. Он не нуждается в усилителе. Предпосылкой для подключения пассивного концентратора является то, что максимально возможное расстояние до рабочей станции не должно превышать нескольких десятков метров.

Локальная сеть Ethernet

Спецификацию Ethernet в конце семидесятых годов 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 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. В качестве метода 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). С его помощью выполняется передача данных или команд управления работой сети;
- маркер (Token). Станция может начать передачу данных только после получения такого пакета. В одном кольце может быть только один маркер и, соответственно, только одна станция с правом передачи данных;
- пакет сброса (Abort). Посылка такого пакета вызывает прекращение любых передач.

Локальная сеть Arknet

Arknet (Attached Resource Computer NETWork) — простая, недорогая, надежная и достаточно гибкая архитектура локальной сети. Разработана корпорацией Datapoint в 1977 году. Впоследствии лицензию на Arknet приобрела корпорация SMC (Standard Microsistem Corporation), которая стала основным разработчиком и производителем оборудования для сетей. В качестве передающей среды используются 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 Arknet применяют топологии шина и звезда. Метод управления доступом станций к передающей среде — маркерная шина (Token Bus). Этот метод предусматривает следующие правила:

- 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.

Основные принципы работы таковы.

Передача каждого байта в Arknet 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), который состоит из шести служебных битов. Начальный разделитель выполняет функции преамбулы пакета.

В Arknet определены 5 типов пакетов.

- Пакет ITT (Information To Transmit) — приглашение к передаче. Эта посылка передает управление от одного узла сети другому. Станция, принявшая этот пакет, получает право на передачу данных.
- Пакет FBE (Free Buffer Enquiries) — запрос о готовности к приему данных. Этим пакетом проверяется готовность узла к приему данных.
- Пакет данных. С помощью этой посылки производится передача данных.
- Пакет ACK (ACKnowledgments) — подтверждение приема. Подтверждение готовности к приему данных или подтверждение приема пакета данных без ошибок, т. е. в ответ на FBE и пакет данных.
- Пакет NAK (Negative AcKnowledgments) — неготовность к приему. Неготовность узла к приему данных (ответ на FBE) или принят пакет с ошибкой.

Выбор оптимальной среды передачи данных

В качестве среды передачи наиболее часто используются 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, наивысшая скорость передачи данных ограничена максимально возможным расстоянием передачи данных, при котором еще обеспечивается требуемый уровень их защиты. Простота наращивания и расширения кабельной системы влияют на ее стоимость.

Витая пара (twisted pair) 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. Преимуществами являются низкая цена и отсутствие проблем при монтаже. Для повышения помехо-

защищенности 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 — хорошо помехозащищен 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 применения.
В зависимости от диаметра кабеля, предусмотренного определенным стандартом, различают "толстый" и "тонкий", коаксиальный кабель.

Оптоволоконные линии наиболее дороги. Скорость распространения информации по ним достигает нескольких Гбит в секунду. Допустимое удаление — более 50 км. Внешнее воздействие помех практически отсутствует. На данный момент это наиболее дорогостоящее соединение для ЛВС. 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 концентратора. Расстояние между концентратором 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 явля-

ется сокращением от словосочетания “топологическое пространство”, что означает — 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 приведенных ниже типовых топологий существует ряд ограничений, приводящих к следующим возможным вариантам:

- **шина (bus)** — компьютеры подключены вдоль одного кабеля (сегмента) (рис. 1.9, *а*);
- **звезда (star)** — компьютеры подключены к сегментам кабеля, исходящим из одной точки, или концентратора (hub) (рис. 1.9, *б*);
- **кольцо (ring)** — компьютеры подключены к кабелю, замкнутому в кольцо (рис. 1.9, *в*).

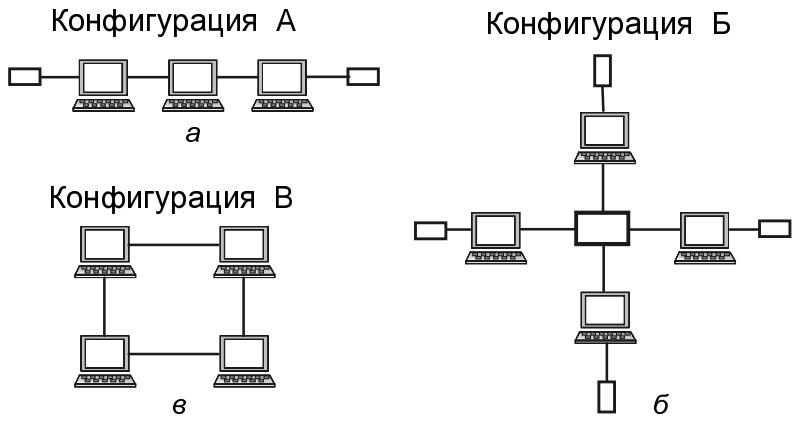

Рис. 1.9. Варианты топологии сети

Первое ограничение состоит в том, что конфигурация "В" не применяется в сетях Ethernet. Для конфигурации "А" ограничено число компьютеров, которые можно подключить к сегменту сети (на рисунке показан именно сегмент сети), оно не может превышать 30 единиц, а длина сегмента не должна превышать 185 м. Применяя репитеры (повторители), которыми можно соединять сегменты сети, можно увеличить ее протяженность до 925 м. Количество сегментов при этом не должно быть больше 5, количество репитеров

между любыми двумя компьютерами не более 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. В конфигурации "Б" также действуют ограничения, которые будут рассмотрены несколько позже. На самом деле в чистом виде такие схемы применяются редко. Чаще сеть имеет комбинированную топологию. 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 использовать возможности только первых двух вариантов 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	Ограниченны
Защищенность от прослушивания	Хорошая	Хорошая	Незначительная
Стоимость подключения	Незначительная	Незначительная	Высокая
Поведение системы при высоких нагрузках	Хорошее	Удовлетворительное	Плохое
Возможность работы в реальном режиме времени	Очень хорошая	Хорошая	Плохая
Разводка кабеля	Хорошая	Удовлетворительная	Хорошая
Обслуживание	Очень хорошее	Среднее	Среднее

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 вытекающих требований к ее возможностям. Если режим и безопасность доступа, хранения и обмена информацией по сети не требуют выделения для этих целей 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 рассмотрения этой 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. Установленную в компьютер сетевую карту можно визуально определить по задней панели, на которой находятся разъемы и индикаторы контроля состояния.

Далее приводится короткое 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-битном режиме, благодаря чему скорость передачи данных становится гораздо выше по сравнению с ISA-картами. Функция Plug and Play 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 также поддерживает полнодуплексный режим и возможность автоматического отключения. Функция отключения питания позволит Вам немного сэкономить потребление электроэнергии, а функция полного дуплекса позволяет, при наличии полнодуплексного хаба, увеличить скорость передачи с 10 до 20 Мбит/с.

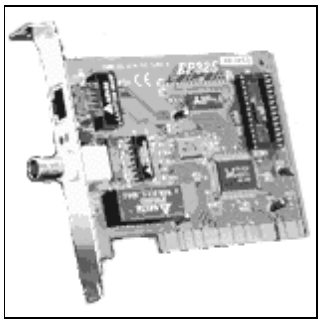

Рис. 2.1. Типичная сетевая карта (Realtec RTL8029 Ethernet Adapter)

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, зарекомендовавших себя в домашних сетях (табл. 2.1). Данные взяты на сайте **http://homenetworks.ru**.

Таблица 2.1. *Характеристики сетевых адаптеров*

Характеристики	Сетевые адаптеры					
	3COM509	OvisLink LE8009	D-Link 220C	SureCom EP329	LongShine LCS-8734	NoName UM9008F
Интерфейс	ISA	ISA	ISA	PCI	PCI	ISA
Проверенный рабочий сегмент, м	600	400	400	400	300	200

Таблица 2.1 *(окончание)*

Характеристики	Сетевые адаптеры					
	3COM509	**OvisLink LE8009**	**D-Link 220C**	**SureCom EP329**	**LongShine LCS-8734**	**NoName UM9008F**
Интерфейс	ISA	ISA	ISA	PCI	PCI	ISA
Примерная цена нового/бывшего в употреблении, $	45/25	20/10	20/10	13/8	15/8	11/5

К приведенным характеристикам сетевых адаптеров можно добавить следующие комментарии:

- 3COM509 — лучший по дальности действия сетевой адаптер при использовании кабеля с низким коэффициентом затухания;
- OvisLink LE8009 — отличный сетевой адаптер с режимами jumperless и PnP, используется при длине сегментов кабеля до 305 м, но на практике работает и на большие расстояния;
- D-Link 220C — надежен и прост в настройке, имеет режим jumpless;
- SureCom EP329 — выполнен на чипе RTL8029, отлично себя зарекомендовал (установлен у 30% отечественных пользователей), работает при длинных сегментах кабеля;
- LongShine LCS-8734 — обычный адаптер.

Управление работой любого устройства (в частности, сетевой карты) осуществляется операционной системой при помощи драйвера. После установки сетевой карты в ваш компьютер необходимо также установить на жесткий диск ее драйвер или подключить его из списка драйверов, предлагаемых операционной системой. Обычно драйвер содержится на прилагаемой 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) необходимо 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 необходимо 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 на нем 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 Windows 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 платы, только для ее выполнения компьютер запросит диск, с которого проводилась установка Windows, а он может потребоваться и при установке сетевой карты.

Если у вас старый компьютер или сама сетевая карта, то установке сетевого адаптера, возможно, 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 применялись в более старых компьютерах и уже не применяются с Pentium III, вторые, соответственно, — в более новых. Иногда есть возможность использовать оба варианта шины, для этого на материнской плате 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 (Interrupt ReQuest, IRQ, запрос прерывания) и адрес ввода-вывода (In/Out Address, I/O). 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 для пользователя 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 для обращения 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 использовать сеанс DOS из Windows. При отсутствии дискеты с программой настройки платы, можно использовать программу от однотипной платы, найдя ее в Internet на сайтах производителей плат или на сайтах архивов программного обеспечения и драйверов.

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

После установки сетевой платы у нас появляется возможность подключения компьютера к существующей сети. Если сети нет, займемся ее организаци-

ей. 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 вам необходимо. В самом простом случае, можно соединить кабелем два компьютера, снабженные сетевыми платами, и настроить их для работы в этой миниатюрной сети. Мы примем за основу немного более сложный вариант, изображенный на рис. 2.2. Настройки, которые мы будем описывать для этого варианта, подойдут и для более простых, и для более сложных сетей. В приведенном варианте применены 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.

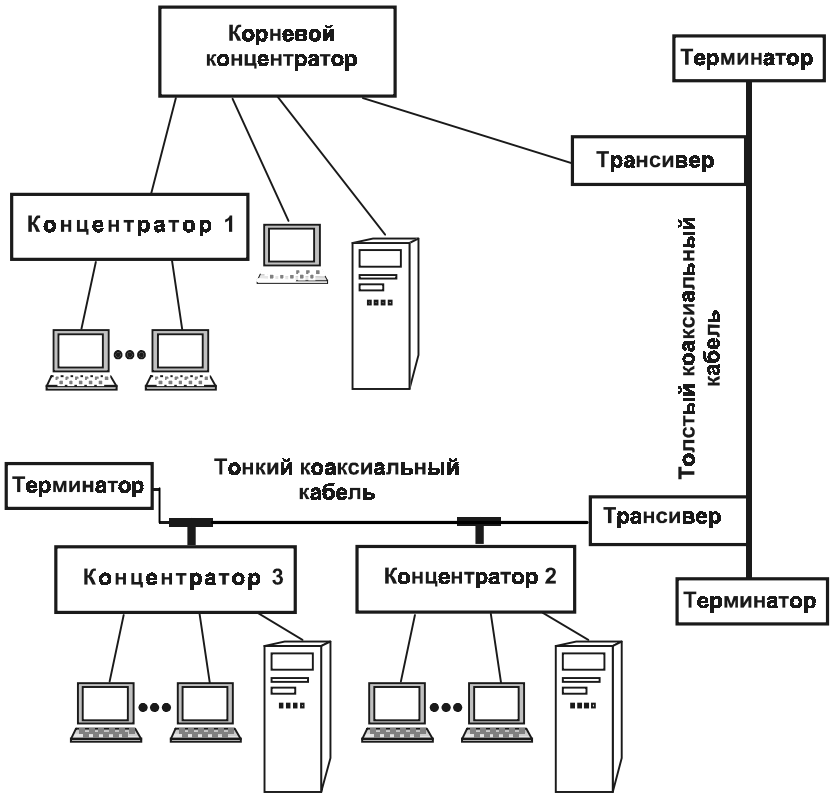

Рис. 2.2. Возможный вариант нашей сети

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.

Концентратор (хаб) 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 у вас 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.

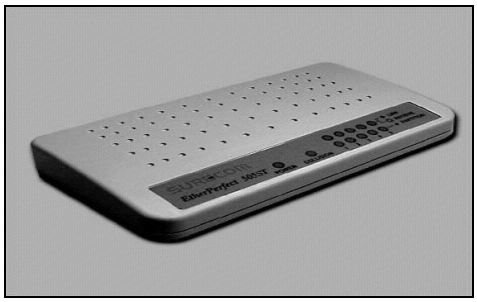

Рис. 2.3. Внешний вид концентратора EP-505ST

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.

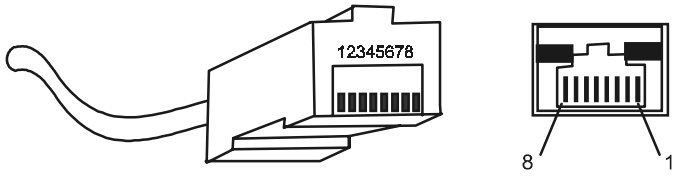

Рис. 2.4. Разъем RJ-45

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

1. Нормальный режим — это подключение к сетевому адаптеру.
2. 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)
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 типа, поэтому эти устройства лучше приобретать одновременно. Это уменьшит вероятность ошибки и несовместимости устройств.

Трансивер подключается 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 — 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**.

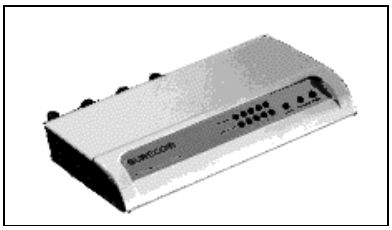

Рис. 2.6. Репитер

Репитер — это устройство, позволяющее увеличить длину коаксиального сегмента, разбив его на несколько независимых сегментов. В случае обрыва или

короткого замыкания, репитер также позволяет заблокировать этот порт с проблемным сегментом, т. е. кроме увеличения длины коаксиального сегмента, который по стандарту не должен превышать 925 м, репитер повышает надежность сети. Тогда 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 4 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 EP505C**	**Surecom EP502C**
Порты	4 BNC, 2UTP, 1AUI	2 BNC, 2AUI	4 BNC, 1AUI	2 BNC, 2AUI
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 советского 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 EP505C — простой, дешевый репитер, имеет очень качественные блоки питания (однажды мы нечаянно подключили к нему 2 фазы, так он в таком состоянии "умудрился" целый месяц проработать!).
- Surecom EP502C — дешево и сердито.

Все соединения между элементами сети осуществляются коннекторами (разъемами).

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

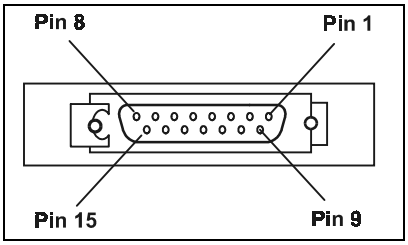

Рис. 2.7. Разъем AUI

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).

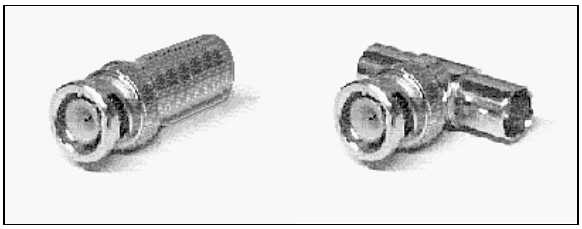

Рис. 2.8. Терминатор и тройник BNC

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:

1. 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.
2. Средства предоставления собственных ресурсов и услуг в общее пользование — серверная часть ОС (сервер):
   - блокировка файлов и записей, что необходимо для их совместного использования;
   - ведение справочников имен сетевых ресурсов;
   - обработка запросов удаленного доступа к собственной файловой системе и базе данных;
   - управление очередями запросов удаленных пользователей к своим периферийным устройствам.
3. Средства запроса доступа к удаленным ресурсам и услугам и их использования — клиентская часть ОС (редиректор):
   - распознавание и перенаправление в сеть запросов к удаленным ресурсам от приложений и пользователей (при этом запрос от приложения поступает в локальной форме, а передается в сеть в другой форме, соответствующей требованиям сервера);
   - прием ответов от серверов и преобразование их в локальный формат, так что для приложения выполнение локальных и удаленных запросов неразличимо.

4. 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 части.

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 сетевой формат 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 локальную ОС встраивался минимум сетевых функций, необходимых для работы сетевой оболочки, которая выполняла основные сетевые функции. Примером такого подхода является использование на каждой рабочей станции сети операционной системы MS-DOS (начиная с третьей версии этой ОС у нее 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 используется и в современных ОС, например, в 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 система Windows NT/2000 фирмы Microsoft, которая за счет встроенности сетевых средств обеспечивает более высокие показатели производительности и защищенности информации по сравнению с сетевой ОС LAN Manager той же фирмы (совместная разработка с IBM), являющейся надстройкой над локальной операционной системой OS/2.

В современных Сетевых Операционных Системах (Network Operation System, NOS) вычислительные операции производятся преимущественно на рабочих

станциях, на их основе 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, 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.

Первый подход — это Таблицы 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 пользователях, 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 и контролировать только одну информационную базу. 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 ресурсы сети, 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.

Второй подход — структура доменов (Domain) используется в таких сетевых ОС, как LANServer и LANMahager. 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, при этом ресурсы серверов являются 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 с использованием этого подхода также возникают проблемы при построении информационной системы с большим количеством пользователей, серверов и, соответственно, доменов. Например, сети для предприятия или большой разветвленной организации. Здесь эти проблемы уже связаны с организацией взаимодействия и управления несколькими доменами, хотя по содержанию они такие же, как и в первом случае.

Третий подход — служба доменных имен (Domain Name System, DNS) лишен этих недостатков. Все ресурсы сети: сетевая печать, хранение данных, пользователи, серверы и т. п. рассматриваются как отдельные ветви или ди-

ректории информационной системы. Таблицы, определяющие DNS, находятся на каждом сервере. Во-первых, это повышает надежность и живучесть системы, а во-вторых, — упрощает обращение пользователя к ресурсам сети. Зарегистрировавшись на одном сервере, пользователь получает доступ ко всем ресурсам сети. Управление такой системой также проще, чем при использовании доменов, так как здесь все ресурсы сети определяются при помощи одной таблицы, в то время как при доменной организации необходимо определять ресурсы, список пользователей и их права доступа для каждого домена отдельно.

Рассмотрим возможности некоторых сетевых операционных систем и требования, которые они предъявляют к программному и аппаратному обеспечению устройств сети.

Сетевые ОС фирмы Novell

Рассмотрим семейство сетевых ОС фирмы 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 (РС) клиента: 640 Кбайт.
- Операционная система: собственная разработка Novell.
- Протоколы: IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange, межсетевой пакетный обмен/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 bindery на сервере.

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

NetWare 4

Отличительная черта этой операционной системы — применение специализированной системы управления ресурсами сети (NDS, Novell Directory Services — служба каталогов Novell), что 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 NetWare 3).

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

1. 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 2 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.
2. 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.
3. 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 данной ОС предусмотрена Встроенная 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 к другому языку достаточно поменять этот модуль или добавить новый. Возможно одновременное использование нескольких языков: один пользователь при работе с утилитами использует английский язык, а другой в это же время — немецкий. Утилиты управления поддерживают DOS, Windows и OS/2-интерфейс.

По основным характеристикам и требованиям к аппаратному обеспечению эта версия сетевой ОС фирмы 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 PC 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, Mac (5), OS/2, UNIX (доп.), Windows NT.

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

NetWare 5.1

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 Internet, такие как Web-сервер, FTP (File Transfer Protocol, протокол передачи файлов), Поисковые, Мультимедийные, ASP-сервер (Active Server Pages, активные серверные страницы) и другие. В Novell Netware 5.1 предусмотрена поддержка клиентов Windows различных версий, что позволяет использовать компьютеры на базе этих операционных систем в ЛВС Novell.

В этой операционной системе имеют место очень четкие права доступа и ограничения, причем на уровне загрузки. Все версии ОС Netware поддерживают большое количество 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 фирмы 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, File Transfer Protocol, 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 фирмы 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 фирмы 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 и 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 или более сетевые карты;
- накопитель CD-ROM, поддерживающий диски в формате ISO 9660;
- мышь, подключенная к последовательному порту или PS/2-порту.

LAN Server, IBM Corporation

Отличительные черты:

- использование доменной организации сети, что упрощает управление и доступ к ресурсам сети;
- поддержка полного взаимодействия с иерархическими системами, например, с архитектурой SNA (Systems Network Architecture, сетевая архитектура систем);
- целостность операционной системы и широкий набор услуг. Работает на базе OS/2, поэтому сервер может быть невыделенным (nondedicated). Обеспечивает взаимодействие с иерархическими системами, поддерживает межсетевое взаимодействие.

Существуют две версии LAN Server: Entry (Первоначальная) и Advanced (Усовершенствованная). Advanced в отличие от Entry поддерживает высокопроизводительную файловую систему (High Perfomance File System, HPFS). 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. При использовании на рабочей станции операционной системы 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 (Remote Interface Procedure Load, RIPL) для DOS, OS/2 и Windows.

К недостаткам этой сетевой ОС можно отнести сложность процедуры 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 Мбайт — 16 Мбайт.
- Минимальный объем ОП PC 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: домены.
- 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, Mac, OS/2, UNIX, Windows NT.

VINES 5.52, Banyan System Inc

Отличительные черты:

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

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

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

Поддержка протокола X.29 позволяет удаленной рабочей станции DOS подключиться к локальной сети через сети, поддерживающие 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 Мбайт — 256 Мбайт.
- Минимальный объем ОП PC клиента: 640 Кбайт.
- Операционная система: UNIX.
- Протоколы: VINES IP, AFP, NetBIOS, TCP/IP, IPX/SPX.
- Мультипроцессорность: есть — SMP (Symmetrical MultiProcesing, симметричная многопроцессорная обработка).
- Количество пользователей: не ограничено.
- Максимальный размер файла: 2 Гбайт.
- Шифрование данных: нет.
- Монитор UPS: есть.
- TTS: нет.
- Управление распределенными ресурсами сети: StreetTalk.
- Система отказоустойчивости: резервное копирование таблиц StreetTalk и данных.
- Компрессирование данных: есть.
- Фрагментация блоков (Block suballocation): нет.
- Файловая система клиентов: DOS, Windows, Mac (доп.), OS/2, UNIX (доп.), Windows NT (доп.).

Сетевые ОС фирмы Microsoft

В данном обзоре сетевых ОС фирмы Microsoft мы подробно остановимся на рассмотрении двух версий: Windows NT и Windows 2000, хотя необходимо учитывать, что в промежутке между появлением этих двух версий были соз-

даны еще несколько, наибольшее распространение из которых получили следующие:

- Windows 95.
- Windows 98.
- Windows 98 SE.

Причем последняя из упомянутых сетевых ОС имеет ряд преимуществ при выборе операционной системы для нашей будущей сети, о чем будет сказано более подробно в *разд. "Выбор операционной системы для нашей сети" главы 2.*

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 эта операционная система 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. Обеспечивается защищенность подсистем 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 PC 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 С-2.

- Монитор UPS: есть.
- TTS: есть.
- Управление распределенными ресурсами сети: домены.
- 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, Mac, OS/2, UNIX, Windows NT.

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, применявшейся в Windows NT. По сравнению со своей предшественницей, имеет множество усовершенствований, в частности, эффективные средства доступа в Internet 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 вычислительные 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.

Выбор операционной системы для нашей сети

Несмотря на то, что Windows 9*x* является сегодня самой универсальной и распространенной операционной системой, у данной ОС есть очень существенный недостаток — нестабильность. Эта неустойчивость частично вызвана универсальностью и совместимостью с устаревшими приложениями. Но почему же мы сейчас не можем отказаться от Windows 9*x*, переходя в лучшем случае на почти ничем от нее не отличающийся, но чуть более стойкий "Миллениум"? Конечно, если на машину планируется установить только Internet-сервер, то Windows действительно не нужна. Но большинство программ, которые мы используем, работают под Windows 9*x*.

Но есть ведь выход! Большинство программ, созданных для Windows 9*x* (и для MS-DOS, Windows NT 4 и даже некоторые программы OS/2), прекрасно работают под Windows 2000 Professional! Раньше Windows NT устанавливали на домашний компьютер лишь те, кто использовал ее в качестве дорогой печатной машинки, работая с MS Office и парой-тройкой аналогичных прикладных программ. Теперь в Microsoft решили наконец-то повернуть эту, гораздо более надежную в сравнении с Windows 9*x*, операционную систему лицом к рядовым пользователям, которые за компьютером не только работают, но и учатся или развлекаются.

В Windows 2000 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 фирмы 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, больше привыкшему к Windows 9*x* и пугающемуся пока еще аббревиатуры "NT".

Система эта имеет много преимуществ не только по сравнению с Windows 9*x* или другими, не столь распространенными ОС, но и в сравнении 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 — на порядки выше, чем у Windows 9*x*.

Устойчивость работы Windows 2000 объясняется тем, что в ней, в отличие от Windows 9*x*, применена так называемая вытесняющая многозадачность, как в UNIX-подобных системах. При таком способе реализации многозадачности ни один самый "глючный" процесс не сможет полностью завладеть цен-

тральным процессором, а получит в свое распоряжение лишь небольшой кусочек времени работы ЦП, 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 после истечения отведенного ей на работу времени. При появлении сбоя достаточно снять повисшую задачу, что никак не отражается на деятельности всей системы и других программ, так как они никак не влияют друг на друга. Да и еще одного источника проблем — VxD-драйверов (виртуальный драйвер устройства, управляющий единственным ресурсом от имени всех выполняемых процессов), свободно хозяйничающих во всех областях оперативной памяти, — в Windows 2000 нет.

Перейдя на Windows 2000, 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, новая операционная система не только значительно облагорожена 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 без проблем 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, 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, наконец-то появилась операционная система, которая хоть как-то может заменить Windows 9*x*, позволив при этом не расстаться с любимыми программами. В большинстве случаев программы под Windows 2000 работают даже быстрее, чем под Windows 9*x*!

Тем не менее, не спешите переустанавливать систему. До сих пор речь шла лишь о достоинствах Windows 2000, в то время как минусов у нее тоже хватает. Поэтому, 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, из которых мы будем рассматривать только версию Windows 2000 Professional для домашних компьютеров.

Главный недостаток Windows 2000 Professional — непомерная требовательность к аппаратной конфигурации персонального компьютера, значительно превышающая запросы Windows 9*x*. И хотя Microsoft и заявляет, что минимум для нее — процессор класса Pentium 133, ОП емкостью 32 Мбайт, жесткий диск емкостью 2 Гбайт, на деле же — это характеристики компьютера, на который реально установить Windows 2000 Professional, но не работать с ней. В жизни же, даже с рекомендуемыми 64 Мбайт оперативной памяти, система будет "безбожно тормозить", ибо ей требуется как минимум 96 Мбайт, при которых уже можно более-менее комфортно работать. Если же вы хотите, чтобы своппинг (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 выше. 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 ставить в другие разделы. Но и в этом случае диск будет быстро заполняться файлами системы. Так что разбейте жесткий диск так, чтобы под раздел с ОС было отведено минимум 2—4 Гбайт, в зависимости от того, куда вы будете инсталлировать прикладные программы.

Если вы еще не передумали устанавливать Windows 2000, то составьте полный список имеющегося оборудования. Хотя под эту 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 определить такой контроллер и просит дискету с драйвером. Постоянно обновляемый список совместимых с Windows 2000 аппаратных средств находится на сайте **www.microsoft.com/hcl**. С несколько устаревшей его версией можно ознакомиться и на самом компакт-диске с дистрибутивом. Есть и другой способ проверить систему на готовность к переходу на Windows 2000 — тестовая программа Windows 2000 Readiness Analizer, кото-

рая проведет ряд тестов, аналогичных тем, которые проводятся при установке ОС, и выявит все устройства, драйвера которых придется искать самостоятельно в Internet, а также проверит совместимость BIOS (Basic Input/Output System, базовая система ввода/вывода) материнской платы с Windows 2000. Эту программу можно найти на сайте **www.microsoft.com/Windows 2000/downloads/deployment/readiness/default.as.** Бывает, что совместимость BIOS со стандартом ACPI является непременным условием успешной установки Windows 2000 на ваш компьютер, тогда придется сначала позаботиться о перепрограммировании (перепрошивке) BIOS.

Помимо этого, утилита выдаст вам список уже установленных у вас программ под Windows 9*x*, которые не заработают в Windows 2000 после обновления ОС. База данных по совместимости программ под Windows с этой ОС находится по адресу — **www.microsoft.com/Windows 2000/upgrade/compat/search**. В основном, в Windows 2000 не работают многие игрушки, программы, обращающиеся напрямую к "железу", не запустятся и приложения, использующие VxD-драйвера, применяемые в Windows 9*x*. В общем, поищите в Internet информацию о том, работоспособен ли важный для вас "софт" в Windows 2000. В крайнем случае, никто не мешает именно для них поставить на компьютер еще и Windows 9*x*.

Несмотря на все "прелести" Windows 2000 (Win2K), мы будем ориентироваться в основном на Windows 98. Операционная система Microsoft Windows 98 SE позволяет обеспечить простой доступ в Internet и высокую производительность системы. Эта ОС представляет собой обновление популярной операционной системы Windows 98, в которой используются самые современные технологии Internet, имеются средства для создания домашних сетей, поддерживается новейшее оборудование.

Во втором издании Windows 98 предлагается целый ряд новых возможностей для работы с Internet и обеспечивается дополнительная поддержка аппаратных средств.

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

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

Преимущества Microsoft Windows 98 SE перечислены ниже.

- Простота использования и доступа в Internet:
  - динамическая справочная система на основе Web-технологии и 15 программ-мастеров упрощают использование компьютера;

- Web-совместимый интерфейс пользователя Windows 98 облегчает поиск, унифицируя представление информации в компьютере, локальной сети и в WWW (World Wide Web, Всемирная паутина);
- второе издание Windows 98 обеспечивает возможность одновременного доступа в Internet 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.

Все это стало возможным благодаря новшествам, превращающим Windows 98 в мощную и надежную операционную систему.

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 NetWare от Novell, 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 поводам. 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, фирма 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, необходимо обеспечить 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 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. Но мы рассматриваем возможности Windows. Причем пытаемся использовать то, что установлено на наших компьютерах. Учитывая, что у начинающего бизнесмена, а так же у начинающего любое большое дело человека лишних финансов нет, будем считать самым выгодным для нас вариантом установку Windows 95/98. Почему не Windows 2000? Просто потому, что не известно еще, будет ли работать ваш модем или принтер под управлением этой системы. Прежде следует изучить вопрос совместимости вашего оборудования с операционной системой. В качестве примера приведу случай из собственной практики. Прекрасно работающий под Windows 98 компьютер было решено перевести на Windows 2000. Предварительно был добавлен второй винчестер и увеличена оперативная память, поскольку требования у новой операционной системы не слишком скромные. Инсталляция прошла прекрасно, сохранена предыдущая Windows 98, и меню позволяет выбрать необходимый вариант загрузки. Но радость была омрачена, когда модем, для которого был драйвер, работавший в Windows 98, работать "наотрез отказался", а принтер верой и правдой прослуживший три года, печатая цветные изображения, "решил", что он монохромный. После неоднократных попыток подобрать драйвер для модема, которые так и не привели к положительному результату (позже выяснилось, что для этого модема драйвер под Windows 2000 не существует), Windows 2000 "завис", да так, что кратчайшим путем к его восстановлению оказалась переустановка. Конечно, это не говорит об ущербности новой операционной системы, но лишь наводит на мысль, что переход на нее должен быть заранее продуман и подготовлен. Не лишним будет, на мой взгляд, посмотреть и на цены, взятые на **www.ntshop.ru.**

- Windows 2000 Server Russian (Серверная операционная система от Microsoft. Русская версия на 5 клиентов). Цена: $1 060.
- Windows 2000 Professional Russian CD (Новейшая операционная система от Microsoft. Русская версия для рабочей станции). Цена: $239.
- Windows 98 Russian CD Second Edition (Windows 98. Второе издание. Русская версия на компакт-диске). Цена: $157.
- Windows 95 Russian DocKit (Windows 95. Русская версия. Комплект инструментов документирования). Цена: $27.

И еще одно замечание: перейти с Windows 95/98 на Windows 2000 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

оправдано, если на рабочих станциях вашей сети установлен компонент Windows 2000 Professional.

Процедура установки Windows 2000

Выбор способа установки

Итак, если ваша система в принципе готова принять новую ОС, вы нашли драйвера ко всему оборудованию и готовы ради душевного спокойствия пожертвовать парой-тройкой привычных программ и чуть большим 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. "Чистая" 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. Upgrade (обновление версии) 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. Впрочем, если вы заранее поинтересовались о готовности вашей системы к обновлению версии, запустив на ней Windows 2000 Readiness Analizer, то этот список вы уже изучили. 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 (жесткий диск), 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 (ПК) две операционные системы —

и Win2K, и Windows 9*x*. Такой вариант наиболее 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 Internet — 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, конечно, 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 загрузочное 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 — она чрезвычайно надежна, работает в ряде случаев быстрее, чем FAT и гораздо более функциональна. При этом не нужно заботиться о какой-то 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 во время установки ОС.

Единственная проблема, которая возникнет при переходе на NTFS, заключается в том, что тома NTFS не видны из 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. Конечно, на сайте **www.sysinternals.com** имеются программы, позволяющие читать разделы NTFS из Windows 9*x* и из MS-DOS, но их демо-версии не дают возможность записывать на эти разделы — чтобы получить полный доступ к диску, необходимо приобрести платный

вариант этих программ. Преобразовать же FAT в NTFS очень легко и после установки системы — достаточно набрать в командной строке следующую команду: `convert <буква_диска>: /fs:ntfs`. Да, если размер оперативной памяти мал, а процессор — не из самых последних, то FAT32 окажется немного побыстрее из-за своей простоты, поскольку в этом случае специфические службы NTFS не 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, зарезервировать все важные данные (при столь глубоких изменениях файловой системы)!

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 ПК необходимо выполнить с дискеты Windows 9*x*, поскольку Windows 2000 "не умеет" делать такие большие разделы, но работает с уже готовыми 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.

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 C (вы будете выбирать ОС в загрузочном меню). Поэтому, при таком варианте необходимо делать диск C: стандарта FAT32, размещать на нем заодно и Windows 9*x*, которая NTFS изначально не поддерживает, а раздел с Windows 2000 (уже по вашему усмотрению) — либо 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 Boot Magic, System Commander — изучите хорошенько их инструкции, может, они покажутся 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 разрешить 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, кроме 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, нужно 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 все 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/удаление программ). Чтобы включить их отображение, уберите слова "HIDE" в файле C:\WINNT\INF\sysoc.inf везде, где они встретятся.

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. Microsoft рекомендует такой порядок установки ОС при создании системы с многовари-

антной загрузкой: 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, т. к. он будет уничтожен.

Монтаж сети

Познакомившись в общих чертах с составляющими деталями нашей сети, попробуем собрать ее простейший вариант. Рассмотрим два варианта — коаксиальный кабель и витая пара. Каждый из них имеет право на жизнь, и только вы сами сможете решить с чего начать, но вполне возможно, что вам потребуются оба варианта. 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 ниже разделах помещено описание инструментов, применяемых при монтаже сетей. Не все инструменты понадобятся вам для работы с вашей 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

Так как при создании "домашней" сети вам в любом случае придется тянуть кабель с дома на дом/из подъезда в подъезд через чердак/крышу/подвал (по улице это делать нецелесообразно — инициативные любители ножниц могут постараться), которые обычно закрыты на ключ, который, в свою очередь, обычно 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 — еще 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 вот что: пойти в РЭУ, узнать адрес вышестоящей инстанции жилищного хозяйства, и уже у них просить ключи, 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, бывают исключения, но

редко. Соответственно, 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, но еще 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. через крышу. Принимая за основу описанный выше метод построения сети, нам необходимо перекинуть магистраль с крыши одного дома на крышу другого. Как это 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. Потом, получив разрешение на подъем, человек на крыше первого дома начинает вытягивать нить на себя, поднимая, таким образом, вместе с нитью и сам кабель. Здесь существует проблема: кабель

может запутаться в кроне деревьев (или зацепиться за строения, фонарные столбы и т. п.), чем доставит немало хлопот. Поэтому перед тем, как начать перекидывание, необходимо максимально очистить будущий путь кабеля. 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 "тарзанки" не очень легко, но отнюдь не невозможно. Другие препятствия обходятся 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 по 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 типа вертолет. 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, это может быть и 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 следует закрепить на растянутом тросе, надежно закрепленном на обеих крышах. Крепить следует при помощи полиэтиленовых стяжек (продаются в хозяйственном магазине), которые можно достаточно легко купить в неограниченном количестве. 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 пожелание — правильное крепление кабелей, чтобы они не болтались и сильно 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 следует 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 дядюшек 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 через 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, крыша протекла и т. п.) и хорошо вентилируемы. Такие комнаты в дальнейшем могут использоваться в качестве компьютерных комнат, где будут стоять отдельные сервера.

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: они заблуждаются. 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 необходимые соединительные шнуры, разъемы и кабели, можно 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 расширен-

ного 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 отмаркированы 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 поставляются с защитным колпачком или в футляре 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, конечно, 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.

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 креп-

ления 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 конкретных ситуаций и потребностей настолько широко, 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.

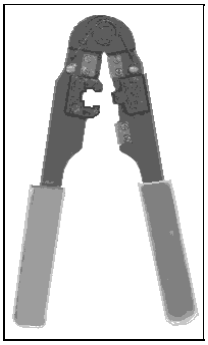

Рис. 2.9. Специализированный инструмент для обработки UTP-кабеля типа витая пара и обжима разъемов RJ-45

Монтаж сети с использованием тонкого коаксиального кабеля

Это вариант сети по стандарту 10Base-2, варианту Ethernet (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 на-

шего 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 чего 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 достаточно 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, если необходимо, обрежьте их до нужной длины. Надвиньте на разъем металлическую муфту.
   - Аккуратно обожмите муфту специальным инструментом (или плоскогубцами) до обеспечения надежного контакта оплетки с разъемом. Не обжимайте слишком сильно — можно повредить разъем или пережать изоляцию центрального проводника, что может привести к не-

устойчивой работе всей сети. Но и обжимать слишком слабо 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 драйвера у себя). Вставляем по требованию компьютера диск с дистрибутивом Windows, перезагружаем компьютер и пока 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. Тоже 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 цветности жил кабеля (табл. 2.5). Необходимо учесть, что в таком варианте разделки кабеля мы получим "Cross-Over"-кабель, 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 кабелем 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).

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

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 драйвера у себя). Вставляем по требованию компьютера диск с дистрибутивом Windows, перезагружаем компьютер и пока 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.

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 большого смысла. В небольшом коллективе, совместно использующим несколько рабочих станций, люди могут пользоваться взаимным доверием, достаточным для того, чтобы 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 Internet 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).

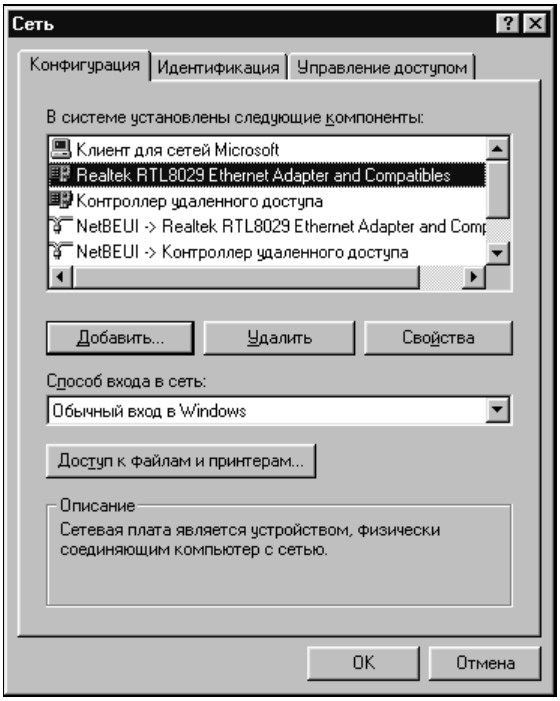

Рис. 2.10. Диалоговое окно **Сеть**

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 так же контроллер удаленного доступа. При этом протоколы для контроллера добавятся автоматически. Лишние протоколы и службы, если они установлены, следует удалить. 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).

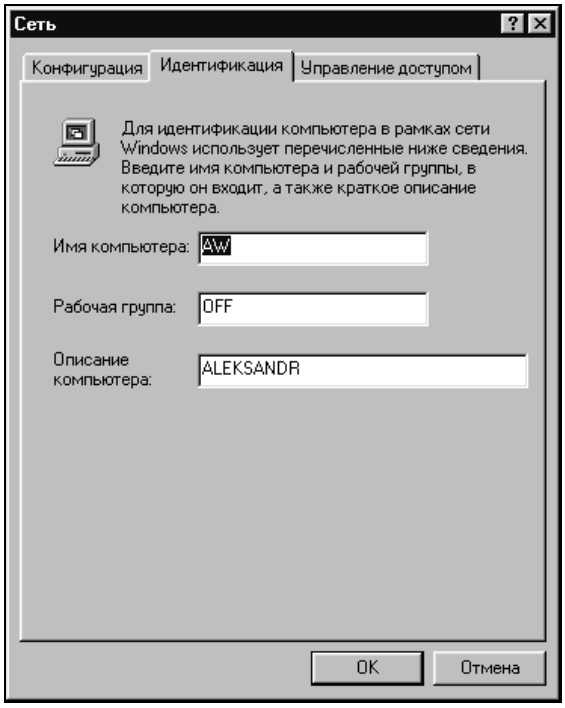

Рис. 2.11. Диалоговое окно **Сеть**, вкладка **Идентификация**

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 подробнее оба варианта. Уровень пользователей предполагает, что для каждого пользователя установлены права доступа к определенным ресурсам. Это имеет смысл, когда имеется много требующей строго индивидуального подхода 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 впереди, 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 попро-

сит первый раз ввести его, не вводите, нажмите кнопку **OK**, а при необходимости подтвердить пароль, опять не вводите и нажмите кнопку **OK**. 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 нажатий на кнопки **Применить** и **OK**, 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).

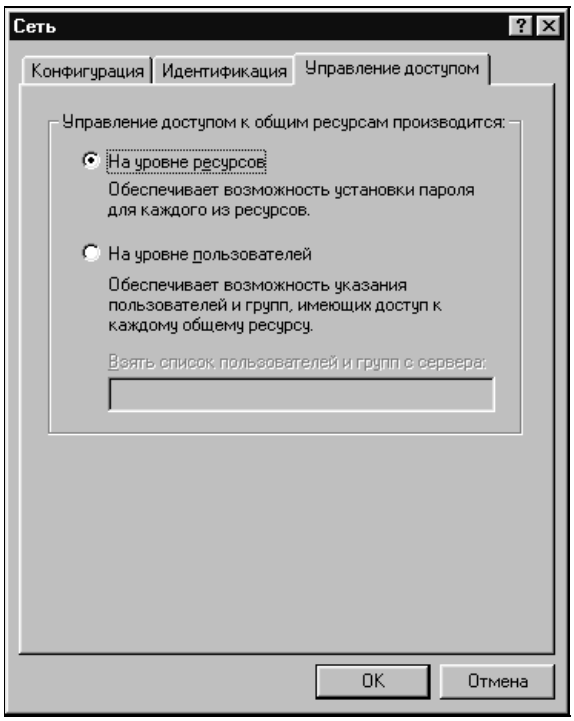

Рис. 2.12. Диалоговое окно **Сеть**, вкладка **Управление доступом**

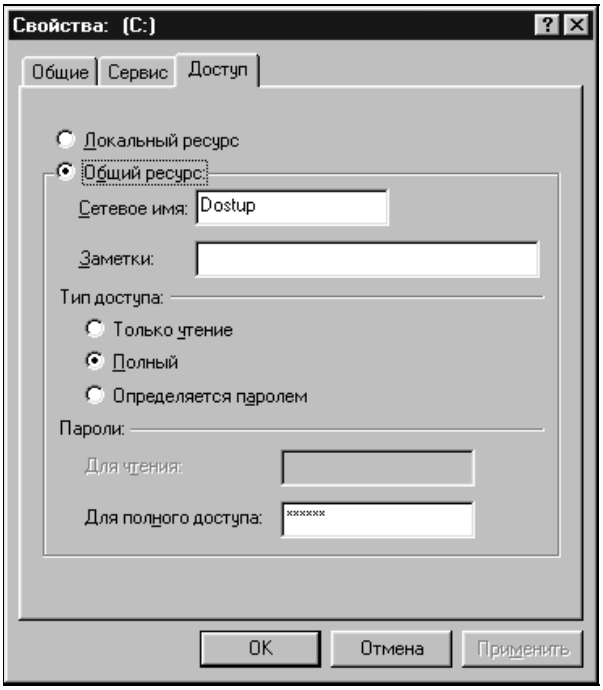

Рис. 2.13. Диалоговое окно свойств диска, вкладка **Доступ**

На этой вкладке установите переключатель **Общий ресурс**. Затем устанавливаем 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 так же сетевое имя диска или папки. С этим именем они будут отображаться на других компьютерах сети. 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 это следует сделать 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 совпадать или отличаться — по вашему желанию.

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

зоваться первыми плодами своего труда и провести пробный сеанс связи между ними. На рабочем столе того компьютера, который мы только что настроили, находим значок **Сетевое окружение**, щелкаем на нем правой кнопкой мыши и из появившегося 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**, как на 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 увидеть 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.

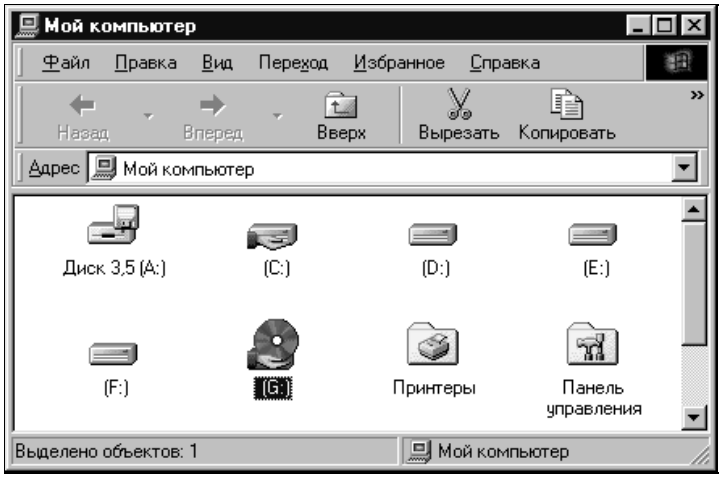

Рис. 2.14. Изображения дисков с установленным общим доступом отмечены поддерживающей рукой

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 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**. Сетевой путь вводится несколько иначе, чем обычный путь к файлу на локаль-

ном компьютере. В начале пути ставится две, а между уровнями пути — одна прямая черта, в отличие от обратной 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 использовать возможность автоматического подключения сетевых дисков.

Теперь оба компьютера могут обоюдно использовать свои ресурсы.

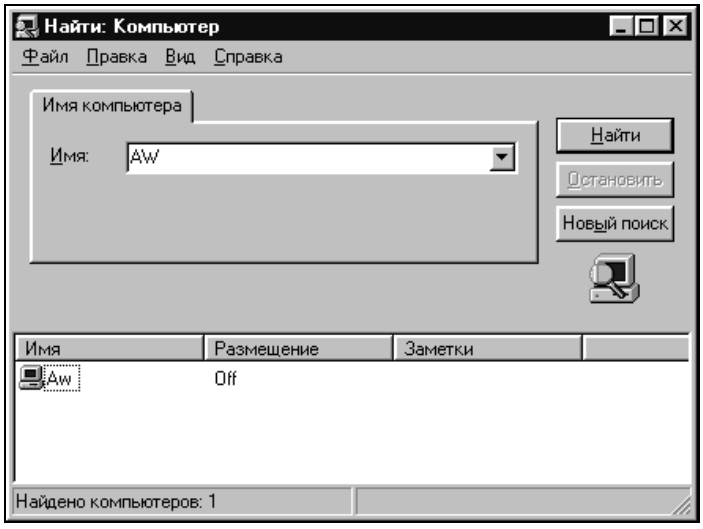

Рис. 2.15. Окно поиска компьютера в сети

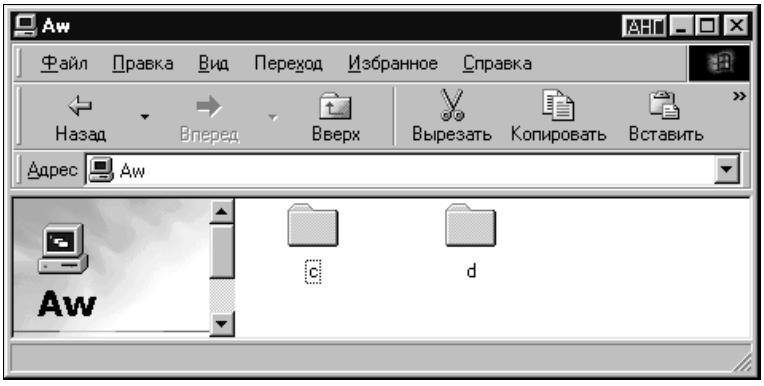

Рис. 2.16. Папки с разрешенным доступом

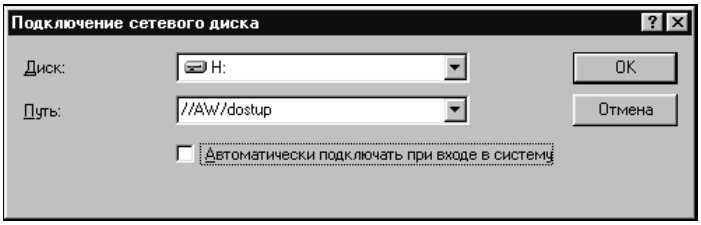

Рис. 2.17. Окно подключения сетевого диска

Подключение дополнительных рабочих станций

После настройки простейшего варианта, подключим еще один, третий компьютер. Для варианта с коаксиальным кабелем 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 той же схеме. Но простота такого пути скрывает подводные камни, обнаруживаемые при эксплуатации этой сети. Если в вашей сети уже, предположим, десять рабочих станций, а на пятой, находящейся где-то посередине всей цепочки, рабочей станции 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. Теперь 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).

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

Таблица 2.6 *(окончание)*

Одна сторона	Цвет провода	Другая сторона
Кабель на четыре пары		
1	Бело-зеленый	1
2	Зеленый	2
3	Оранжевый	3
4	Синий	4
5	Бело-синий	5
6	Оранжево-белый	6
7	Бело-коричневый	7
8	Коричневый	8

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, или подключение вышестоящего хаба, когда используется их каскадирование, или подключение выхода трансивера, подключенного к толстому коаксиальному кабелю.

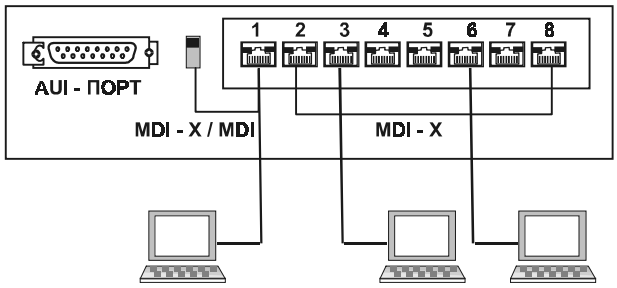

Рис. 2.18. Концентратор 10Base-T — соединение с компьютерами

Нами уже были настроены для соединения в 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 возможность количественно развивать нашу сеть практически неограниченно. Можно соединить компьютеры (см. рис. 2.2), применяя толстый и тонкий коаксиальный кабель (см. рис. 2.19), применяя тонкий коаксиальный кабель или используя только каскадное подключение хабов и не применяя коаксиальный кабель, словом, простор для творчества широчайший.

Необходимо лишь при приобретении оборудования учитывать вариант возможного подключения рабочих станций. Так, терминаторы и трансиверы, например, существенно отличаются, если они выполнены для соединения с тонким, или с толстым коаксиальным кабелем. В некоторых случаях, при использовании тонкого кабеля, трансивер может не понадобится 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 дальнейшее развитие.

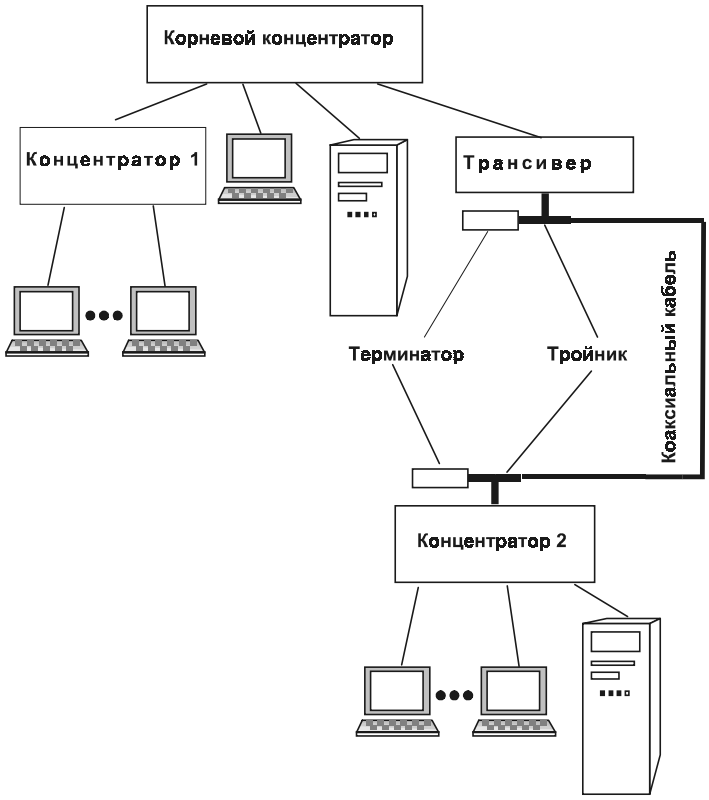

Рис. 2.19. Вариант комбинированного построения сети

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** в свойствах сети протокол TCP/IP для сетевого адаптера, 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.

Обратите внимание на то, что эти изменения следует производить только для сетевого адаптера. Протокол TCP/IP, используемый контроллером удаленного доступа, который используется для соединения с Internet, 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.exe (см. рис. 2.21), находящаяся в каталоге Windows.

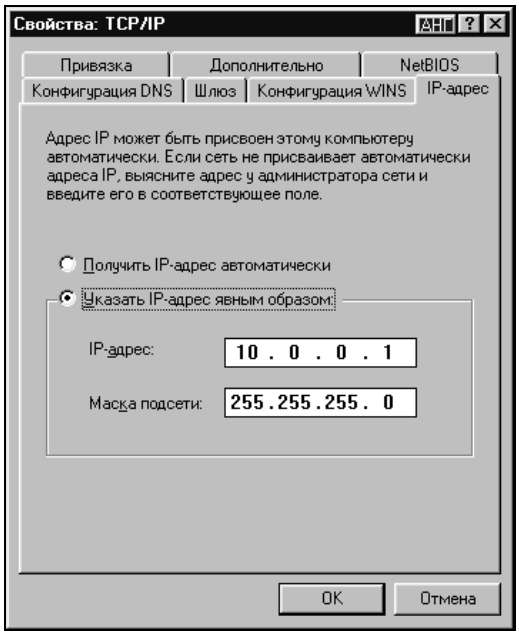

Рис. 2.20. Окно свойств TCP-IP — установка адреса

Если ярлык программы поместить в папку **Автозагрузка**, то при включении компьютеров она будет готова к приему и передаче сообщений между входящими в состав сети компьютерами. 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 установке опе-

рационной системы, в этом случае ее следует добавить, воспользовавшись опцией **Установка и удаление программ** в меню **Панель управления**.

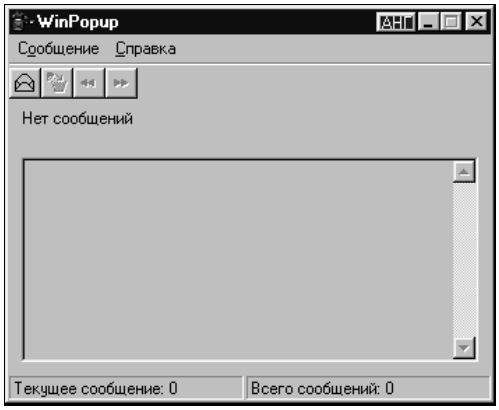

Рис. 2.21. "Выскочка" — программа для передачи сообщений по локальной сети

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, по вашему мнению, количестве пользователей, можно условно распределить их по рабочим группам. При этом мы получим возможность обращаться сразу к группе пользователей. По какому принципу происходит 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 соседние по рабочей группе компьютеры (рис. 2.22), а остальные можно будет найти, дважды щелкнув по значку **Вся сеть** (рис. 2.23) и открыв нужную рабочую группу.

Доступ к файлам и папкам мы получим, конечно, только после установки доступа в свойствах папок 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 директории. 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 директории, где находится программа.

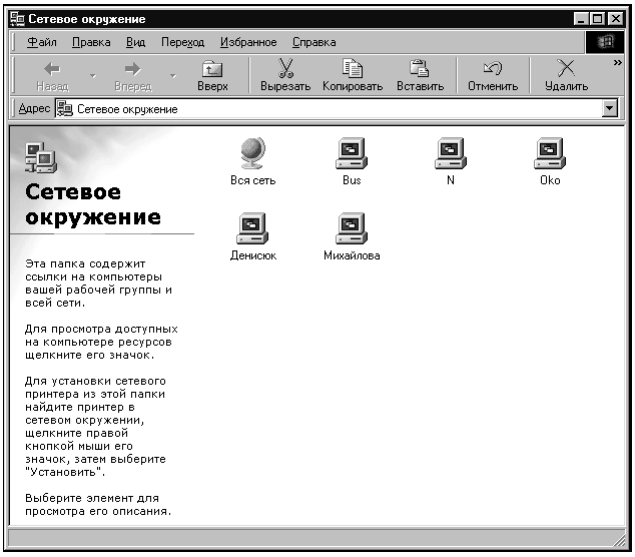

Рис. 2.22. В окне **Сетевое окружение** видны компьютеры вашей рабочей группы

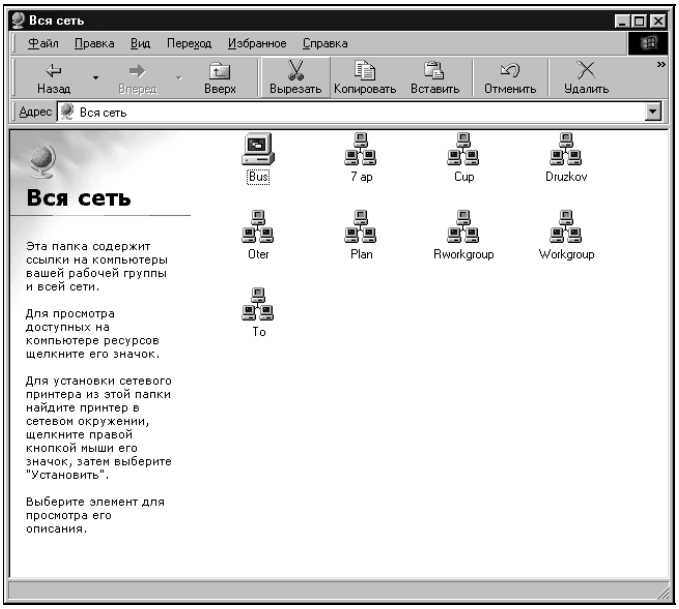

Рис. 2.23. Окно **Вся сеть** показывает все рабочие группы сети

Работа в сети

Некоторые особенности работы в сети

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, видно в сетевом окружении и не сразу. Несколько больше можно увидеть, обратившись к значку **Вся сеть**, но и там не все появляется моментально. Иногда требуется довольно значительное время, чтобы увидеть и получить доступ к компьютеру, который, возможно, вы видите невдалеке от вас. Из этой ситуации существует довольно простой выход. Когда все, или, по крайней мере, часть соединений видны, можно создать к ним ярлыки и поместить в отдельную папку. При следующем включении, несмотря на то, что еще не все компьютеры видны в сетевом окружении, 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.

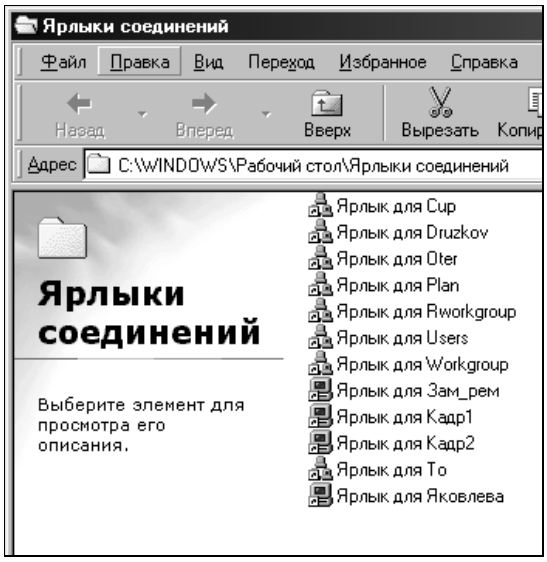

Рис. 2.24. Ярлыки соединений могут ускорить доступ к компьютерам сети

В Windows возможности командных файлов дополнены возможностями их ярлыков, или т. н. PIF-файлов, 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. Конечно, простые команды можно быстро научиться вводить напрямую, но когда требуется выполнить сложную серию команд, которые, например, архивируют, переименовывают, перемещают или копируют группы файлов (если операция стандартно выполняется периодически, а ее запись выглядит громоздко), то и опытный пользователь обратится к помощи BAT-файла. Windows позволяет сделать операции с файлами более наглядными, безликие BAT-файлы могут приобрести выразительные ярлыки.

Если в вашей сети много компьютеров, может возникнуть необходимость произвести какие-либо изменения на всех. Например, изменить свойства ярлыка к общедоступной программе, которая установлена 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 к этому командному файлу 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 свойствах 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 использовать 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. Так вот, в эту директорию можно поместить не саму функцию, а ярлык к ней, который будет ссылаться на файл на сетевом диске или удаленном каталоге. При этом в свойствах файла функции необходимо установить возможность общего доступа без возможности изменения. Теперь каждый раз при старте MS Excel будет подключаться эта функция, становясь доступной 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 содержит цифры, удобные для восприятия компьютером, но неудобные для применения пользователями сети. Это значит, что при выходе за пределы локальной сети трудно будет, не применяя каких-либо иных средств, кроме уже рассмотренных, использовать понятные и удобные для применения имена компьютеров и адреса Internet. По сложившейся практике в больших сетях используют доменную систему имен DNS. Домен — организационная единица безопасности в сети. Рабочая станция является доменом. Домен может охватывать несколько физических точек. В каждом домене своя политика безопасности и 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 идет 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 содержит систему цифровых адресов, которые в специальных конфигурационных файлах DNS поставлены в соответствие с именами символьными. Файлы эти находятся на серверах доменов, что позволяет компьютеру определить действительный IP-адрес по его символьной записи. Так, если мы имеем соединение с компьютером (сервером) провайдера, который обеспечивает нам доступ в Internet, адрес этого компьютера в цифровом виде записан в конфигурации соединения. Далее, адреса, вводимые нами в поле адреса в используемом браузере, ставятся в соответствие цифровым адресам, исходя из имеющейся на сервере информации. Если вводимому нами символьному адресу не сопоставлен цифровой адрес на сервере, то никакого соединения не произойдет. Компьютер, имеющий соединение с провайдером, имеет цифровой адрес, который временно выделен для этой рабочей станции. Компьютер также

имеет имя. При этом с другого компьютера, который через того же провайдера в данный момент подключен к Internet, мы не сможем соединиться с первым компьютером, набрав его символьный адрес. Но, зная его цифровой адрес, мы можем, в принципе, такое соединение осуществить. Для обеспечения возможности соединения нашей сети с другими сетями, наша сеть должна иметь выделенный сервер — особый компьютер, который не используется для обычной работы. Установленные на нем сервисы должны обеспечивать 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 повторятся. 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 серьезны последствия совпадения MAC-адресов (Media Access Control, управление доступом к среде), адресов сетевого оборудования, которые заданы производителем и "вшиты" в это оборудование. Совпадение таких адресов практически невозможно, так как в состав такого адреса входит много сведений, которые не могут совпасть. При совпадении IP-адресов необходимо перезапустить компьютеры с совпавшими адресами, изменив адрес на первом 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 Internet. В этом случае возможны неустранимые конфликты адресов. Поэтому, планируя организацию сети, следует заранее запланировать и соответствующие стандартам диапазоны адресов компьютеров и подсетей.

Доступ к ресурсам в Windows 2000

В отличие от 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.

Если не отменен общий доступ (рис. 2.26) к папке, то можно задать предельное число пользователей, которые могут пользоваться этой папкой одновременно, а также разрешения, где для каждого пользователя (которого можно добавлять и удалять) устанавливаются параметры доступа (рис. 2.27).

Ресурс будет недоступен пользователю, не включенному в список имеющих доступ к этому ресурсу.

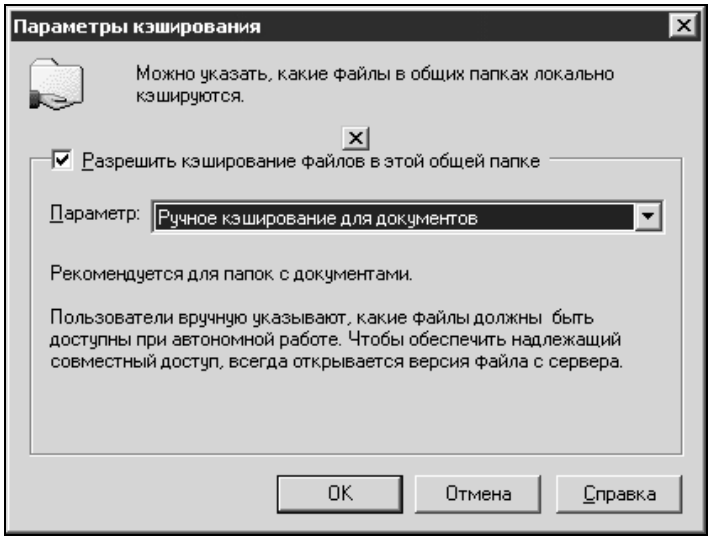

Рис. 2.25. Настройка кэширования папок с документами

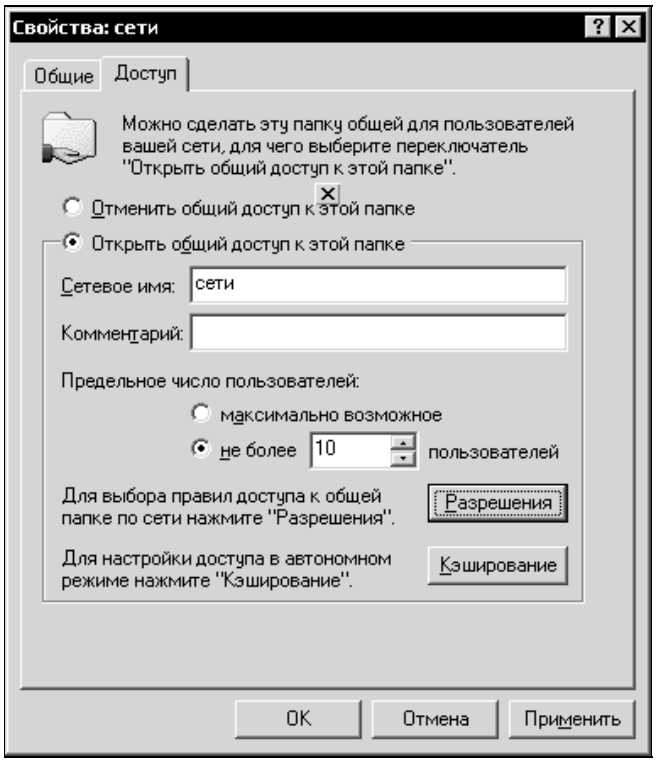

Рис. 2.26. Окно настройки сетевого доступа к папкам

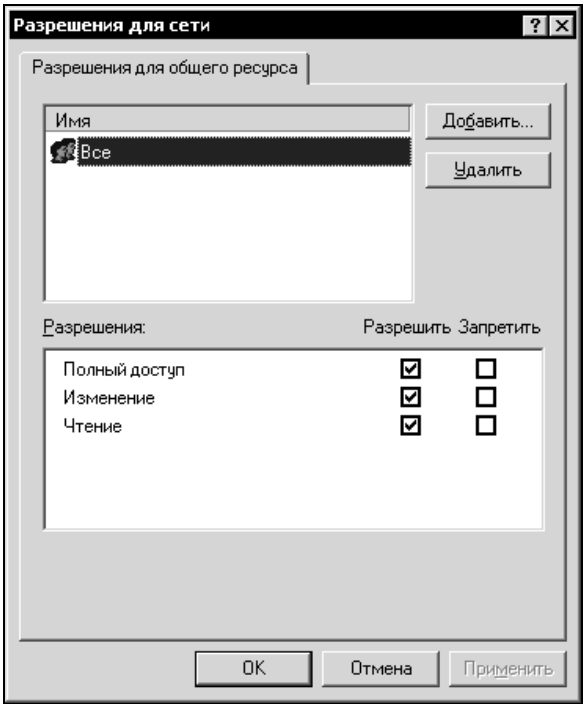

Рис. 2.27. Установка разрешений

Общение в одноранговой сети

Для передачи простых сообщений в одноранговой односегментной сети существуют стандартные средства (WinPopup). Более широкие возможности для общения предоставляют программы, обеспечивающие режим чата. Это режим текстовых переговоров, широко распространенный в Internet, 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. Возможны как общий, так и приватный режим общения, имеется доска объявлений, возможна установка фильтров на принимаемые сообщения.

Интерфейс программы простой, а помощь, которая может быть оперативно вызвана во время работы при возникновении затруднений, в лаконичном виде дает советы. Программа работает под управлением Windows 95/98/NT. Проблемы, которые могут возникнуть при установке и настройке, подробно описаны в документации. Даже начинающий пользователь сети сможет вос-

пользоваться 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.

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 сообщение будет дополнительно отображаться в отдельном всплывающем окне.

- **Фильтровать сообщения**

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

- **Состояние чата**

  - Никаких ограничений. Обычный режим (принимаются все сообщения).
  - "Не беспокоить" на массовые личные сообщения.
  - "Не беспокоить" на личные сообщения, отправленные нескольким пользователям сразу, а не конкретно вам.
  - "Не беспокоить" на все сообщения.
  - "Не беспокоить" на все сообщения.
  - Меня нет.

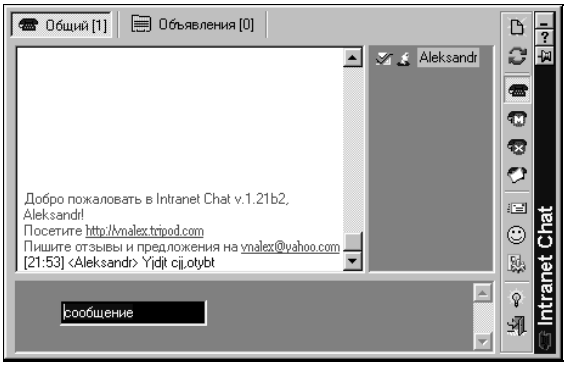

Рис. 2.28. Окно **Intranet Chat**

- "Меня нет за компьютером".
- Показать в отдельном плавающем окне.

Состояние чата будет дополнительно отображено в отдельном плавающем окне (аналог того, как это сделано в ICQ (Система интерактивного общения в Internet). Его можно переместить в самое удобное для вас место. 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 описываемое меню.

❒ **Показать**

- **Список пользователей**

  Показать/спрятать список пользователей.

- **Панель инструментов**

  Показать/спрятать панель инструментов.

- **Доску объявлений**

  Показать/спрятать доску объявлений.

- **Пользователи**

  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.

Ниже приведены основные возможности программы.

❒ Не требует выделенного сервера. В этом случае для передачи сообщений чат использует Windows MailSlots (Слоты электронной почты в Windows). Для их работы достаточно одного из установленных протоколов в систе-

ме 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 многосегментых сетях и даже в Internet. 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. При этом можно выбрать действие, которое при этом будет произведено:
  - появится чат и сообщит о том, что пользователь появился в чате;
  - набранное при задании предупредительное сообщение будет отправлено появившемуся пользователю;
  - набранное предупредительное сообщение будет оправлено 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 отправлены 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.

Программа Intranet Chat поддерживает двадцать 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 про-

грамм, 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 с нетривиальным решением. 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, где будет удобно расположить его территориально.
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 с необходимыми настройками.
4. Переходим к компьютеру, с которого предполагается печать на сетевом принтере.
5. Устанавливаем драйвер принтера, так, как бы мы его устанавливали для локальной установки, но на предложение напечатать пробную страницу отвечаем отказом.
6. Открыв 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. Возможно это, конечно, 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).

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 при внимательном просмотре свойств принтера всегда можно принять решение по их выбору. При необходимости можно поэкспериментировать для выбора наиболее подходящего варианта настроек.

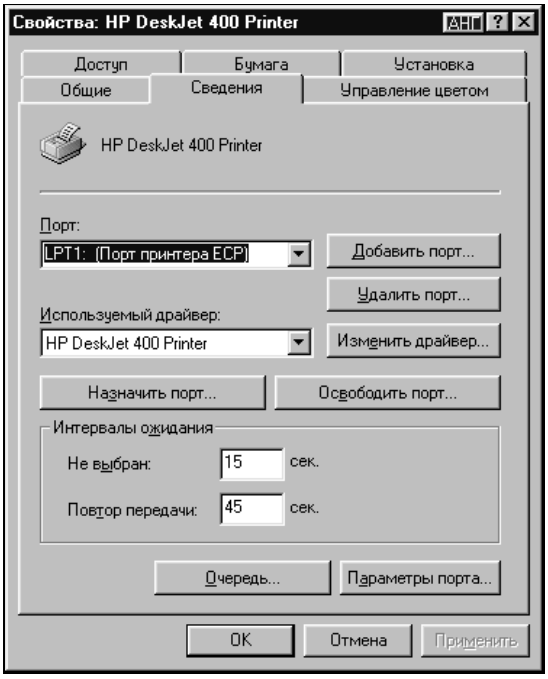

Рис. 2.29. Настройка сетевого принтера

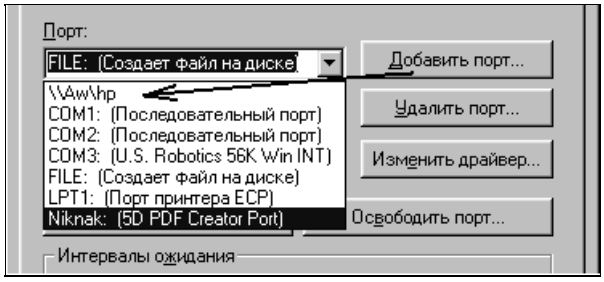

Рис. 2.30. Выбор порта принтера

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. Необходимо поставить галочку напротив флажка очереди заданий печати из DOS.

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, же-

лая 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.

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, представляя 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 де-

[1] Хаб — *Прим. ред.*

лать 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 лестницы 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 "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, используя его как сервер 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 часть Windows 2000 (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 реорганизацию и модернизацию сети. 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 Internet, 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 Internet.

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 доступа к Internet 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 Internet, станет почтовым отделением внутри локальной сети, свяжет каждого пользователя сети с его собственным почтовым ящи-

ком 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 добавить новое, добавить память? 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 организация этой сетей не вышла за рамки одноранговой уровня с операционной системой Windows 9*x*. Потребности этой организации удовлетворены тем, что они имеют, а поддержка такой сети в рабочем состоянии не требует больших затрат. В других организациях 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 получения необходимых результатов простыми средствами, вы сможете принять верное решение, когда

встанет проблема выбора пути дальнейшего 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 Hiper Terminal — 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 Windows. Их работа поддерживается программой, работающей под управлением этой операционной системы. 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 необходима 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 явный 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. Возможно еще несколько вариантов применения выделенных серверов. Они могут выполнять функции маршрутизаторов, т. е. управлять направлением передачи информации при соединении двух или нескольких подсетей, хранить таблицы имен и обеспечивать связь одной или нескольких небольших локальных сетей с глобальными сетями типа Internet. Эти возможности будут рассмотрены в следующих главах.

Глава 3

Иерархическая сеть

Завершив настройку одноранговой сети, вы в скором времени можете почувствовать необходимость дальнейшего развития вашего предприятия. 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 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 в данный момент информацию или передать сообщение. А если вы решите организовать выход в Internet через одного из участников сети, для более рационального использования самого быстрого подключения, то кому из соседей отдадите предпочтение? Есть, конечно, сети даже не домашние, а весьма известные и серьезные, в которых приходится мириться с режимом жизни пользователей. Это, например, FIDO. Сеть использует коммутируемые соединения, а 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 придется выбрать наиболее подходящего претендента из существующих в вашей сети компьютеров, или приобрести дополнительную машину. Поскольку параметры сервера зависят от наших требований и размеров сети, следует провести хотя бы приблизительный ее расчет. Большим подспорьем в расчетах может быть 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 Internet, может получить проект будущей сети буквально за считанные минуты. Такую воз-

можность предоставляет компания "Тауэр-Сети и Технологии" с помощью своей новой 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*. Наиболее сложные проекты, также *бесплатно*, получают экспертную оценку у специалистов в Presales Center 3Com. 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 структурную схему, спецификацию и техзадание. Конечно, проект поддерживается определенными фирмами и рекомендует использовать оборудование этих фирм. Но, даже если у вас уже есть большая часть оборудования, вы вполне можете дополнить его, руководствуясь спецификацией. Некоторые элементы навязываются системой, не спрашивая вас, но вы можете, подойдя рассудительно к проекту, 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 в этой системе проект поможет сориентироваться в ценах и ваших возможностях. Предположим, что будущая сеть состоит из шести рабочих мест, расположена компактно на одном этаже, расстояние между машинами и хабом около десяти метров. Операционная система Windows 98. До сих пор мы не рассматривали вариант сети с выделенным сервером, но автоматический проектировщик самостоятельно предлагает включить в состав сети сервер и указывает конкретный тип и характеристики машины. Даже если вы не собираетесь пока устанавливать сервер, вы можете ознакомиться с характеристиками и ценой такой машины, чтобы в будущем сознательно принять решение на основании точных знаний. Но рассмотрим результаты расчета по порядку.

Прежде всего, приводятся характеристики сети **www.netwizard.ru**. Количество коммуникационных центров в данном случае соответствует всего лишь количеству хабов или коммутаторов в нашем варианте сети. Все компьютеры подключены к одному устройству, позволяющему им связываться друг с другом и с сервером. Каждый ПК подключен к сети через свой порт. В проекте указано поэтому, что количество активных портов — 6. Каналы для рабочих станций выделенные. Это значит, что каждая станция имеет свой адрес и может быть связана с сервером параллельно с другими станциями.

Далее идет описание Главного коммутационного центра. В нашем случае — это вся наша компактно расположенная сеть. В больших сетях с несколькими серверами могут применяться несколько коммутационных центров. Среди них есть главный и коммутационные центры более низких уровней, 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. Но источник бесперебойного питания предложен проектировщиком без нашей просьбы, иначе сеть не будет иметь достаточной, по мнению программы, надежности. Указано общее количество портов — 12. Это говорит лишь о том, что допускается возможность развития сети, что весьма разумно и полезно. Никто не может сказать, что произойдет завтра, и какие резервы придется использовать. Но, когда резервов нет, а появилась потребность развития сети, проблем у вас возникнет достаточно. Указаны некоторые конструктивные особенности сети.

Следующий раздел — Серверы коммуникационного центра. Он описывает единственный сервер сети, которого может и не быть. Точнее выделенного сервера в сети может и не быть, но программа считает, что это необходимо. Сервер — это и вид программного обеспечения, позволяющего обеспечивать рабочие станции некоторыми сервисными возможностями. Мы предполагали, что в нашей сети потребуется электронная почта для всех станций и файловый сервис, позволяющий всем машинам использовать дисковое пространство сервера. Все станции на равных правах могут пользоваться сервером электронной почты и файловым сервером, физически находящимися в одной машине, характеристики которой предлагаются далее. А предлагается — сервер 1-го уровня Аквариус: AquaServer E200.

Эта модель относится к серверам начального уровня, рекомендованного изготовителем для использования в качестве файлового и принт-сервера в рабочих группах или сервера электронной почты. В базовой конфигурации он поставляется с одним процессором Intel Pentium III 500, ОЗУ 128 Мбайт ECC SDRAM, Ultra Wide SCSI-винчестером емкостью 9,1 Гбайт, накопителем CD с 40-кратной скоростью и сетевым адаптером Fast Etherlink III 3C905B-TX. Легко наращиваемый, неприхотливый и простой в обслуживании, сервер прослужит вам долгие годы. Повышенная надежность в работе и разумная цена — вот основные отличительные особенности AquaServer E200. По желанию заказчика серверы могут комплектоваться и другим оборудованием.

Ниже приведены базовые конфигурации моделей серии AquaServer E.

- AquaServer E200.
- Процессор Intel Pentium III 500 МГц/512 Кбайт кэш-памяти.
- Системная плата Soyo SY-D6IBA(-2)/MicroStar MS-6120.
- Системная шина 100 МГц.
- Оперативная память 128 Мбайт ECC SDRAM.
- Жесткие диски 9,1 Гбайт UWSCSI.
- Порты ввода-вывода 4 PCI, 3 ISA, 1 порт AGP2x, 2 Ultra2 Wide SCSI, 2 UDMA.

- Сетевой адаптер 3C905B-TX/IntelPro100/B.
- Видеоконтроллер SVGA, 2 Мбайт AGP.
- CD-ROM 40x.
- Стандартный дисковод для гибких дисков 1,44 Мбайт, 3,5 дюйма.
- Корпус Big Tower.
- Внутренние отсеки для жестких дисков 3×5,25", 3×3,5".
- Отсеки для съемных накопителей 3×5,25", 4×3,5".
- Источник питания 300 Вт.
- Поддерживаемые операционные системы MS Windows 2000/NT 4.0 Server, UNIX, Novell Netware 5.1, RedHatLinux 6.2.

В этом сервере можно установить до двух процессоров Intel Pentium II/III. Он содержит 4 разъема PCI, 3 ISA, 1 порт AGP и два интерфейса Ultra Wide SCSI. В корпусе Big Tower может разместиться до четырех 3,5-дюймовых и до трех 5,25-дюймовых устройств. Системные платы SY-D6IBA (-2) с набором микросхем i440BX поддерживают процессоры до Pentium III 600 МГц; максимальный объем оперативной памяти — 1 Гбайт. Дисковая подсистема рассчитана на 4 жестких диска Ultra Wide или Ultra2 SCSI (на системной плате SY-D6IBA-2).

В разделе "Сервер № 1", в графе "Тип операционной системы сервера" стоит "NO". Дело в том, что свойства сети, которые мы хотим получить, поддерживаются сервером с Windows 2000 Server, а мы пока рассчитываем обойтись Windows 98. И завершает описание параметров сети раздел "Персональные компьютеры главного коммуникационного центра". Предложено использовать Aquarius Standard. Ниже приводятся характеристики базовой модели этого компьютера.

- Оперативная память наращивается до 512 Мбайт; возможна установка до 4 дисков IDE.
- Ultra-DMA. Слоты расширения (4 PCI) позволяют разместить необходимое количество устройств.
- Три 5,25-дюймовых отсека предназначены для внешних устройств. Дают возможность устанавки нужных накопителей. Компьютеры этой серии оборудованы двумя портами универсальной последовательной шины (USB) для подключения периферийных устройств новейших стандартов.
- Процессор Intel Celeron с тактовой частотой 466—600 МГц.
- Системная шина 66/100 МГц.
- Кэш-память второго уровня 128 Кбайт.
- Набор микросхем базовой логики Intel 810/440ZX.
- ОЗУ минимум 32 Мбайт с возможностью расширения до 512/768 Мбайт, 2—3 разъема для модулей DIMM.

- Жесткий диск от 4,3 Гбайт до 20 Гбайт Ultra DMA; поддерживаются до 4-х жестких дисков.
- Флэш BIOS, 4 Мбит флэш-памяти для системной BIOS, SCSI и видео BIOS.
- Слоты расширения 3—4 PCI/0-2 ISA.
- Каналы ввода/вывода, последовательный и параллельный порт, 2 порта USB, порт IrDA, разъемы PS/2 для клавиатуры и мыши.
- Внутренние отсеки для жестких дисков. Два 3,5-дюймовых отсека для съемных накопителей.
- Источник питания 250 Вт.
- Стандартный дисковод для гибких дисков 1,44 Мбайт, 3,5 дюйма.
- CD-ROM40X.
- Видеоконтроллер Video i810/AGP видеоплата.
- Видеопамять. Динамическое выделение памяти из ОЗУ (i810)/4—32 Мбайт.
- Поддерживаемые операционные системы MS-DOS, MS Windows 9*x*/NT/2000, RedHat Linux 6.2.
- Корпус MiddleTower (ATX)/MiniTower (microATX).
- Габариты корпуса MiddleTower (высота x ширина x глубина) 400×210×420 мм, MiniTower 365×185×400 мм.
- Сертификат соответствия системы качества производства стандарту РИ-СО 9002, сертификат соответствия РОСС RU ME06.B00193.
- Гигиенический сертификат № 12РЦ-128. Сертификат надежности № RINC.RU.E003.C00002. Сертификат на совместимость с ОС Windows 98 и Windows NT.

Структурная схема компьютерной сети

Структурная схема сети показана в следующих таблицах (табл. 3.1—3.6)[1].

Таблица 3.1. *Параметры сети*

Параметр	Величина или свойство
Количество коммуникационных центров	1
Количество активных портов	6
Каналы для рабочих станций	Выделенные

[1] Данный отчет построен при помощи системы NETWIZARD.

Таблица 3.2. *Главный коммуникационный центр*

Параметр	Величина или свойство
Количество активных портов	6
Управляемость активным оборудованием	Нет
Резервирование источников питания активного сетевого оборудования	Нет
Резервирование центрального сетевого устройста	Нет
Резервирование управления	Нет
Средняя длина кабельных каналов, м	10
Способ прокладки кабеля	Короб
Крепление розеток СКС	На плоскую поверхность
Количество портов UTP	12
Нужны источники бесперебойного питания для активного сетевого оборудования	Да

Таблица 3.3. *Серверы коммуникационного центра*

Серверы уровня 1	Распределение пользователей по серверам	
	Сервер эл. почты (кол-во клиентов)	Файловый и принт-сервер (кол-во клиентов)
Сервер 1	6	6

Таблица 3.4. *Сервер № 1*

Параметр	Величина или свойство
Процессор	Обычный
Объем ОЗУ (Мбайт)	384
Объем дискового пространства (Гбайт)	18
Желаемый тип корпуса сервера	Rack
Отказоустойчивость	Нет
Наличие устройства для резервного копирования данных (стримера)	Нет
Тип операционной системы сервера	Нет
Источник бесперебойного питания	Требуется
Количество связей	1
Технология связи	10Base-T

Таблиа 3.4 *(окончание)*

Параметр	Величина или свойство
Скорость передачи	10 Мбайт/с
Среда передачи	Twisted Pair
Характеристика связи	UTP

Таблица 3.5. *Персональные компьютеры главного коммуникационного центра*

Параметр	Величина или свойство
Количество	6
Станции стандартной конфигурации	Да
Тип процессора	Celeron
Частота процессора, МГц	600
Объем ОЗУ, Мбайт	64
Объем видео ОЗУ, Мбайт	4
Объем жесткого диска, Гбайт	10
Диагональ монитора, дюймов	15
Наличие мультимедиа	Нет
Наличие источников бесперебойного питания	Да
Операционная система	Windows 98
Количество лицензий ОС	6
Офисное ПО	MS Office 2000 Standard
Количество лицензий офисного ПО	6

Таблица 3.6. *Связи персональных компьютеров*

Параметр	Величина или свойство
Количество	6
Тип связи	Коммутируемая
Технология	10Base-T
Скорость передачи	10 Мбайт/с
Среда передачи	Twisted Pair
Характеристика	UTP

После описания общих характеристик сети предлагается спецификация, в которой вы найдете ответы на все — "Что?", "Сколько?" и "Почем?". В разделе Активное сетевое оборудование предлагается использовать двенадцатипортовый коммутатор SuperStack 3 Baseline 10/100 Switch 12 port 10/100Base-TX и сетевую плату Fast EtherLink XL PCI 10/100 TX M.

Коммутаторы SuperStack II Baseline 10/100 применяются в любой сети, где требуется высокая производительность, но нет необходимости в управлении. Они могут, во-первых, использоваться как агрегирующие устройства при подключении других коммутаторов и концентраторов, во-вторых, предоставлять эффективное по стоимости, быстродействующее решение для соединения с рабочими станциями пользователей. Коммутаторы 3Com SuperStack II Baseline не имеют функций управления, они готовы к работе сразу же после включения.

Ключевые особенности устройств:

- автоматическое определение скорости передачи и возможность установки полудуплексного или дуплексного режимов для каждого порта удваивает скорость соединения до 200 Мбит/с;
- таблицы MAC-адресов дают возможность поддерживать до 4000 устройств локальной вычислительной сети;
- функция управления потоком IEEE 802.3x (Flow Control) гарантирует отсутствие потери пакетов в высокоскоростных дуплексных соединениях во время пиков трафика;
- размер устройства обеспечивает легкость установки в стойку с помощью поставляемого комплекта для монтажа. Оно может также использоваться автономно;
- диагностические индикаторы (LED) показывают состояние сети и статус каждого порта, облегчая поиск ошибок и проверку статуса индивидуального порта;
- возможность подключения резервной системы питания Advanced Redundant Power System обеспечивает надежную защиту от простоев сети.

Если у вас есть хаб и сетевые платы иного, чем здесь описано, типа, — вы можете использовать их. Но в последнее время вместо хабов все чаще применяют коммутаторы, отличающиеся тем, что передают сигнал не на все компьютеры сразу, а только в тот сегмент, где находится этот компьютер. Это позволяет делать более сложные (топологически) сети. Источники бесперебойного питания, безусловно, вещь нужная и полезная, но если сумма $1607,92 в восторг не приводит, и у вас электрическая сеть работает стабильно, напряжение не меняется более чем на 10% и не выключается в неподходящий момент, то какое-то время можно обойтись без них.

Спецификация

Спецификация для проекта приведена в табл. 3.7[1].

Таблица 3.7. *Спецификация*

Артикул	Наименование товара	Ед. изм.	Кол-во	Цена, $	Сумма, $
Активное сетевое оборудование					778,44
3C16464B	SuperStack 3 Baseline 10/100 Switch 12 port 10/100Base-TX	шт.	1	424,24	424,24
3C905C-TX-M	Fast EtherLink XL PCI 10/100 TX M	шт.	7	50,60	354,20
Источники бесперебойного питания					1 607,93
SU1000INET	Smart-UPS 1000	шт.	1	452,90	452,90
BK650MI	Back-UPS 650MI	шт.	6	192,50	1 155,02
Кабельные каналы					87,10
NCT1050	Короб 100×50	м	6	9,88	59,28
NCI1050	Соединитель 100×50	шт.	1	1,69	1,69
NJC1050	Заглушка на шов 100×50	шт.	1	1,69	1,69
NAF1050	Плоский угол 100×50	шт.	2	5,68	11,36
NWP1050	Заглушка внутренняя 100×50	шт.	3	2,86	8,58
PVH_GOFR_20_P	Труба ПВХ гофрированная 20 мм с протяжкой	м	18	0,25	4,50
Серверы и рабочие станции					6 136,00
QEV-1G6670131091NINN	Aquarius Server E100 133	шт.	1	1 351,00	1 351,00
DIMM 256 Мбайт	SDRAM ECC 100 MHz	шт.	1	315,00	315,00
Monitor15	Monitor 15 LITE-ON TCO95	шт.	7	198,00	1 386,00
QSI-C600064100-FNNS2	Aquarius Std MC600 (C600/64/VINT/H10/KM-SB)	шт.	6	514,00	3 084,00
Программное обеспечение					1 738,64
730-01011	Windows 98 Russian Disk Kit CD /Upg Second Edtn	шт.	1	20,08	20,08

[1] Данный отчет построен при помощи системы NETWIZARD. **(www.netwizard.ru)** © 2000. Компания Тауэр.

Таблица 3.7 *(продолжение)*

Артикул	Наименование товара	Ед. изм.	Кол-во	Цена, $	Сумма, $
730-01196	Windows 98 Russian DocKit Second Edtn	шт.	1	16,05	16,05
730-01629	Windows 98 Russian VUP OLP NL	шт.	6	67,62	405,72
021-02771	Office 2000 Win32 Russian Disk Kit CD	шт.	1	20,08	20,08
021-02770	Office 2000 Win32 Russian DocKit	шт.	1	16,05	16,05
021-03881	Office 2000 Win32 Russian OLP NL	шт.	6	210,11	1 260,66
	Пассивное сетевое оборудование				760,83
27.1B.241.A005G	19" Patch Panel, 24xRJ45 KATT with cover, 568B, UTP, Power Cat, 1U, Graphite	шт.	1	169,89	169,89
25.A017G	19" Ring Run (Jumper) Panel, 1U, Graphite	шт.	2	23,49	46,98
45.0B.011.D022E	Patch Cord RJ45, 568B-N, UTP stranded, PowerCat, 1m, Grey	шт.	6	5,09	30,54
45.0B.011.D024E	Patch Cord RJ45, 568B-N, UTP stranded, PowerCat, 3m, Grey	шт.	6	7,64	45,84
39-504-PS	UTP PVC Cable PowerCat 4-pair	м	120	0,42	50,10
17.1B.011.A0042	Euromod 1xRJ45, M1 Straight, 568B, UTP, PoweCat, White	шт.	12	5,14	61,68
42-501-32	Розеточная коробка для установки на плоскую поверхность Surface Box UK 1G 32mm	шт.	6	1,94	11,64
17-0111-02	Лицевая панель розетки Labelled Single Gang Wallplate, United Kindom, 86×86×10 mm, White	шт.	6	2,84	17,04
DR3016604	CageNuts/Washers/6mm Screws. (50)	шт.	1	16,09	16,09

Таблица 3.7 *(окончание)*

Артикул	Наименование товара	Ед. изм.	Кол-во	Цена, $	Сумма, $
DR3006106	W/M Cab. Acrylic Door. 600w×400d×6U	шт.	1	311,03	311,03
	Работы по монтажу сети				582,50
MUTP5	Прокладка кабеля UTP	м	120	0,30	36,00
MKOROB	Монтаж короба	м	28	2,00	56,00
MKOROBB	Монтаж короба на бетонной стене	м	3	2,50	7,50
MROZ1	Установка розетки RJ-45	шт.	11	10,00	110,00
MROZ1B	Установка розетки RJ-45 на бетонной стене	шт.	1	15,00	15,00
MRACK	Установка шкафа	шт.	1	150,00	150,00
MPATCH	Монтаж патч-панели, 1 порт	шт.	12	4,00	48,00
TUTP	Тестирование UTP/STP порта	шт.	12	5,00	60,00
MDOC	Подготовка документации на СКС	шт.	1	100,00	100,00
	ИТОГО				11 691,44

В спецификации перечислены почти все "мелочи", о которых недосуг задуматься, когда мечтаешь об организации сети и представляешь ее работу. Кабели должны быть аккуратно уложены и защищены от случайного смещения половой тряпкой, от повреждения передвигаемой мебелью и 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 концентратору, напрямую, без использования промежуточных панелей, а также управляя питанием от сети переменного тока, используя выключатели на сетевых фильтрах, использование которых при отсутствии источников бесперебойного питания очень желательно. И, наконец, в специфика-

ции 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.

Последний важный документ, который нам позволяет получить автоматический проектировщик, это Техническое задание. Ни один серьезный проект не воплощается без предварительного составления технического задания. В нем отражены все особенности и требования к сети. По сути, это не последний, а первый документ, на основе которого проект может детализироваться и рассчитываться. По техническому заданию, составленному автоматическим проектировщиком, вы можете оценить, соответствует ли проект вашим представлениям о предполагаемой сети. Если обнаружены какие-либо неточности, несоответствия с вашим замыслом, то проект можно пересчитать за несколько минут, введя необходимые коррективы при вводе первичной информации. Изменения могут повлиять и на состав оборудования, и на общие затраты по монтажу сети.

Техническое задание на разработку проекта компьютерной сети

Название проекта: "Проект сети на шесть пользователей".

Дата создания: 16.10.2001 19:56:42.

Общие положения

Данное техническое задание составлено на основе анализа ответов на вопросы, заданных системой NetWizard в интерактивном диалоге через сеть Internet. Многие параметры проектируемой сети установлены в соответствии с экспертной оценкой системы, часть из них по причине имеющихся ограничений.

Описание задачи

1. Основные параметры[1].

   Компьютерная сеть проектируется для 1-го этажа здания, в котором необходимо обеспечить взаимодействие 6 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 — 6 штук.

[1] Техническое задание составлено при помощи системы NETWIZARD. **(www.netwizard.ru)** © 2000. Компания Тауэр.

3. Активное сетевое оборудование.

   Программой предлагается активное сетевое оборудование фирмы 3Com, но каждый вправе выбирать.

4. Параметры производительности.
   - Полоса пропускания канала связи с рабочими станциями должна составлять не менее 10 Мбит/с.
   - Необходимо выделять эту полосу пропускания для каждой рабочей станции (коммутируемая сеть).
   - Магистраль должна обеспечивать пропускную способность не менее 33% от максимального трафика коммуникационного центра.

5. Управление трафиком.

   Средства эффективного управления трафиком в сети не требуются.

   Параметры межузловых каналов связи проектируемой сети (табл. 3.8).

Таблица 3.8. *Параметры межузловых каналов*

Назначение канала	Скорость канала, Мбит/с	Кол-во каналов	Объединять каналы
Связи с ЛВС другого здания	100	1	–

6. Структурированная кабельная система.
   - Для связи с серверами необходимо использовать кабель типа неэкранированная витая пара.
   - Для связи с рабочими местами необходимо использовать кабель типа неэкранированная витая пара.
   - Для связи с ЛВС другого здания необходимо использовать кабель типа неэкранированная витая пара.
   - На каждом рабочем месте необходимо установить порты кабельной системы в количестве, равном 2.

7. Параметры кабельной системы главного коммуникационного центра.
   - Среднее расстояние от коммуникационного центра до рабочего места составляет 10 м.
   - Среднее расстояние между главным и этажным коммуникационными центрами 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 фирмы Microsoft.

   В качестве операционной системы персональных компьютеров необходимо применять программный продукт — Windows 98, при этом предпочитаемый язык интерфейса операционной системы — русский.

   В качестве офисных приложений для персональных компьютеров должен использоваться программный продукт — MS Office 2000 Standard, при этом предпочитаемый язык интерфейса приложения — русский.

9. Центральные серверы и персональные компьютеры.

   Для центральных серверов проекта должно быть выбрано оборудование группы Aquarius.

   - Количество центральных серверов должно равняться 1.
   - Распределение приложений и пользователей по серверам (табл. 3.9).

Таблица 3.9. *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	6	6

10. Необходимая конфигурация сервера № 1.
    - Тип процессора: обычный.
    - Количество процессоров в сервере: 1.
    - Объем оперативной памяти (ОЗУ) сервера 384 Мбайт.
    - Необходимый объем дискового пространства 18 Гбайт.
    - Желаемый тип корпуса: монтируемый в стойку (RackMount).
    - Количество линий связи сервера должно равняться 1.
    - Скорость передачи линии связи должна составлять 10 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 Internet. Расчет, подобный приведенному выше, длится около 5 мин. Более сложные задания, возможно, потребуют большего времени. Использование такого помощника в процессе разработки сети избавит вас от большого количества ошибок. А обнаруженные незначительные несоответствия вашему замыслу, в плане применяемого оборудования, применения каких-либо недокументированных особенностей операционной системы, иных версий программ, по сравнению с предлагаемыми, могут быть разрешены вами самостоятельно.

Выбираем сервер

Какими особыми свойствами должна обладать машина, претендующая на роль сервера в нашей сети? Многое зависит и от наших требований и от размеров 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 128 Мбайт оперативной памяти и винчестерна 20 Гбайт, да для игрушек графический ускоритель. 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 его 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 раздача ее по первому требованию клиента, имеющего право ее получить. Другие задачи, возложенные на него, могут занимать небольшую часть ресурсов сервера и не вызовут проблем.

Очень часто в качестве файлового сервера применяют обычный персональный компьютер. Если альтернативное решение не возможно, то можно пойти и на

такой вариант. Ориентируясь на него, мы и будем позже рассматривать 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. Возможно, 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, и трагедии не случилось. Возможна и другая причина порчи файлов — может быть, возникла 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, да еще с зеркально отраженными дисками, информация на которых повторяется один к одному, но 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 аппаратно. 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, конечно, 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) массивов. RAID — это избыточный массив недорогих дисков, который может быть выполнен как аппаратно в виде отдельного устройства, так и программно средствами операционной системы

(NetWare, Windows NT/2000), 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 механике, которая не связана напрямую с вычислительными процессами, но при неисправности механизмов процессы эти 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 даже при остановившемся вентиляторе. Процессоры последних серий, рабочая частота которых достигает 1 ГГц и выше, не протянут без принудительного охлаждения и часа. Для некоторых из них предлагаются системы с водяным охлаждением. Если есть возможность применить программное средство поддержания оптимального температурного режима процессора, то не следует пренебрегать ею.

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

При больших размерах вашей сети, возможно, следует выбрать операционную систему, специально предназначенную для работы на сервере. Так, например, ОС Novell NetWare разных версий позволяет очень эффективно управлять процессом доступа к информации. Права пользователей в этой ОС могут настраиваться очень тонко, и предназначена она специально для работы на файловом сервере. Огромным потенциалом обладают и Windows NT/2000. Но и привычная Windows 98 имеет массу возможностей, которые могут с успехом применяться на сервере сети. При этом отсутствуют материальные затраты для приобретения новой операционной системы, и нет затрат времени на освоение этой системы. Novell NetWare 4.11, например, отличается от Windows настолько, что освоение этой ОС со всеми ее особенностями установки и эксплуатации может занять весьма продолжительное время. При этом реально надежность системы на обычных машинах обеспечивается применением зеркальных дисков и своей файловой системы NFS, которая не позволит использовать сервер в каких-либо других целях, кроме непосредственного своего назначения. Более новые версии системы — NetWare 5.1, например, имеют существенно расширенные возможности, но требования к ресурсам растут тоже существенно. Для обычной работы файлового сервера рекомендуется иметь 16 Мбайт оперативной памяти на каждый Гбайт используемого дискового пространства. При этом условии вполне реально обеспечение работы пятидесяти пользователей сети, работающих с сервером одновременно. Физические ограничения на доступ

к дискам сервера могут наступать в связи с недостаточной пропускной способностью канала связи (сетевая карта — кабель — концентратор — кабель — сетевая карта), и, при интенсивной работе сети, частым возникновением коллизий. Для повышения пропускной способности сети можно рекомендовать вместо концентраторов 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.

Подключение

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 потребностям 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 клиента 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. 3.1), и в случае ошибок в действиях пользователей, выдаются сообщения с информацией о них (рис. 3.2).

Рис. 3.1. Вид окна сетевого соединения DOS-клиента

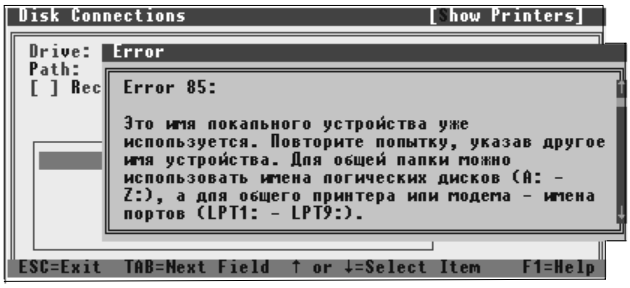

Рис. 3.2. Сообщение об ошибке DOS-клиента

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 с сервера **www.microsoft.com**. Клиент раздается бесплатно.

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;
- ❒ tp-клиент;
- ❒ telnet;
- ❒ dial-up.

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.

Инсталляция проводится в следующей последовательности:

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 ресурами**;
   - **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 115200, 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.
5. 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 директории сервера, в которой содержатся файлы для печати на сетевом принтере (Network Printer Queue). Этот ресурс называется SPOOLDIR.
6. 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 запус-

кать программу NET.EXE. Для удобства работы можно дополнить START-NET.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 в PTS-DOS во многом похожи на стандартные MS-DOS, а в случае затруднений доступна команда `help`, выводящая 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.

Недавно вышла новая версия этой системы — PTS-DOS 32, она 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 отлично 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 небольшие сети, организованные как самостоятельные локальные сети. Один (или более) из имеющихся компьютеров в этом случае 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 для маршрутизации в различных условиях. Мы рассмотрим подробно следующие вопросы:

- маршрутизируемая сеть в небольшом офисе;
- домашняя сеть.

Маршрутизируемая сеть в небольшом офисе

Сеть небольшого офиса обладает следующими характеристиками:

- несколькими сегментами ЛВС (например, отдельные сегменты на каждом этаже или в каждом крыле здания);
- только одним сетевым протоколом (IP или IPX) в каждом сегменте;
- закрытостью, т. е. отсутствием 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. 3.10.

Таблица 3.10. *Адреса сегментов*

Сегмент	Сеть	IP	Маска
Сеть А	200.1	.1.0	255.255.255.0
Сеть Б	200.1	.2.0	
Сеть В	200.1	.3.0	

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. 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. 3.11.

Таблица 3.11. *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. 3.12.

Таблица 3.12. *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 или DNS (в зависимости от того, что вы используете).

Рассмотрим теперь небольшую домашнюю сеть, подключенную к Internet. Характерные черты такой сети:

- один сегмент;
- протокол IP;
- подключение к поставщику услуг Internet по коммутируемому или выделенному каналу с дозвоном по необходимости.

На маршрутизаторе необходимо сконфигурировать сетевой адаптер и установить модем или иное устройство для подключения к ISP. ISP, 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 необходимо сконфигурировать для использования DNS ISP, почтовых серверов, серверов новостей и т. д. Кроме того, следует установить фильтры для внешнего интерфейса, чтобы исключить просмотр содержимого вашего компьютера из Internet.

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 к сети Internet своего компьютера через сеть. Для этого следует организовать переход из вашей маленькой сети в глобальную сеть Internet. Используя операционные системы Windows 95/98, это можно осуществить описанным ниже способом. Для Windows 95, на компьютере с модемом, придется установить дополнительно сервер удаленного доступа из комплекта Microsoft Plus! и провести обновление до Winsock 2.0, если оно еще не сделано.

Существуют и другие решения поставленной задачи, но преимущество предлагаемого варианта — возможность организации удаленного доступа при миминимальных изменениях в данной одноранговой сети 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 (DUN, Dial-Up Networking — система удаленного доступа) сервера:

- **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 клиент/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 бывают разными.

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 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, — должен стоять флажок **IP Routing Enabled**. 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`, при этом TRACERT должен показывать путь между подсетями, где первым адресом должен быть адрес шлюза, вторым — запрашиваемый компьютер. Если вместо IP-адресов выдается `Timeout`, значит ошибка в настройках IP.

Если с какого-либо из компьютеров устанавливается соединение с Internet, то для того чтобы при этом удаленные компьютеры маршрутизировались правильно (а не через Internet, как "захочет" Windows 95/98), нужно вручную на этом компьютере прописать маршрутизацию на них 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 Internet прокси-сервер, а на остальные — по модему, можно поиграть в Internet-провайдера.

При наличии достаточных материальных, аппаратных, программных, интеллектуальных и/или прочих ресурсов существуют и 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 от Microsoft

Один из простых вариантов предложен самой корпорацией Microsoft. Возможность управлять домашней сетью, имеющей выход в Internet, заложена в один из вариантов Windows 98/Windows 98 SE.

Компонент **Общий доступ к подключению Интернета** предоставляет удобный способ организации и настройки домашней сети. Только сервер должен иметь непосредственное подключение к Internet, для остальных компьютеров IP-адреса назначаются сервером. Таким образом, остальные компьютеры сети получают возможность доступа к Internet через сервер, используя преобразование личных IP-адресов.

Когда компьютер сети отправляет запрос в Internet, его личный IP-адрес передается серверу, который выполняет преобразование этого адреса в свой IP-адрес, а затем отправляет запрос в Internet. Получив результаты запроса, сервер выполняет обратное преобразование IP-адреса и направляет полученные результаты соответствующему компьютеру сети. Единственным компьютером сети, видимым другим пользователям Internet, является сер-

вер, и применение специальных средств для скрытия компьютеров пользователей сети от постороннего доступа со стороны глобальной сети Internet не требуется.

Для подключения к Internet необходимо выбрать компьютер, который будет использоваться в качестве компьютера общего доступа, и подключить его к Internet удобным вам способом. После проверки работоспособности подключения к Internet выполните установку компонента операционной системы **Общий доступ к подключению Интернета**. Настройкой общего доступа к Internet (рис. 3.3) 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) для динамического назначения личных IP-адресов всем компьютерам домашней сети. Кроме того, существует возможность 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 Internet.

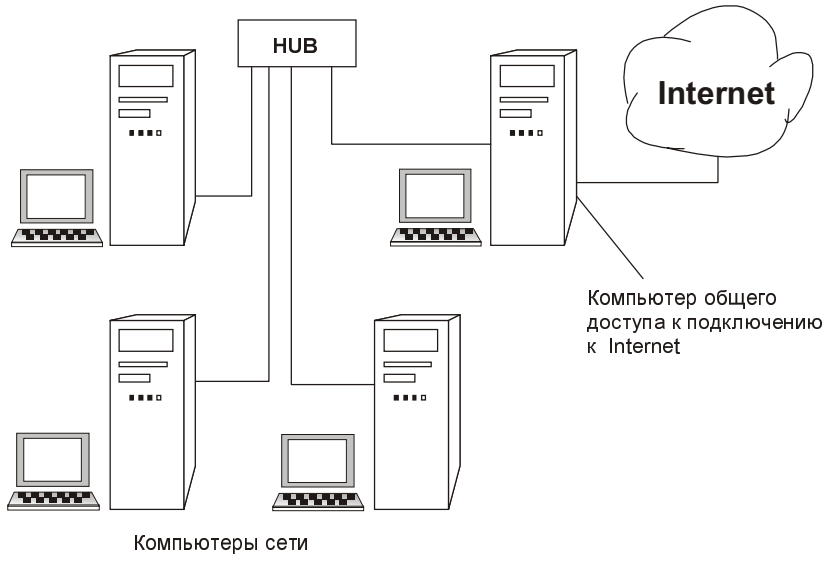

Рис. 3.3. Общий доступ к подключению к Internet

Настройка домашней сети с общим доступом в Internet

Если у вас еще не установлен общий доступ к подключению Internet, 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**.
2. Выберите команду **Средства Internet** и нажмите кнопку **Состав**.

   Поставьте 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 Internet.

   Откройте вкладку **Подключение** в диалоговом окне **Свойства обозревателя**.

   Для этого нажмите кнопку **Пуск**, выберите команды **Настройка** и **Панель управления**, дважды щелкните значок **Свойства обозревателя**, выберите вкладку **Подключение** и нажмите кнопку **Доступ** в группе **Настройка локальной сети** (рис. 3.4).

   Если кнопка **Доступ** отсутствует в группе **Настройка локальной сети**, необходимо запустить мастер общего доступа к подключению Internet. 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 (рис. 3.5) введите параметры, указанные в табл. 3.13.

Таблица 3.13. *Параметры настройки общего доступа к подключению к Internet*

Параметр	Описание
Выводить значок на панель задач	Добавление значка общего доступа к подключению Internet на панель задач. Значок показывает число подключенных в данное время компьютеров и включает контекстное меню, содержащее параметры общего доступа к подключению Internet
Выберите подключение, используемое для доступа к Интернету	Выберите нужный параметр
Разрешить общий доступ к подключению Интернета	Включение или отключение общего доступа к подключению Internet
Выберите сетевой адаптер, используемый для доступа к домашней сети	Выберите нужный параметр

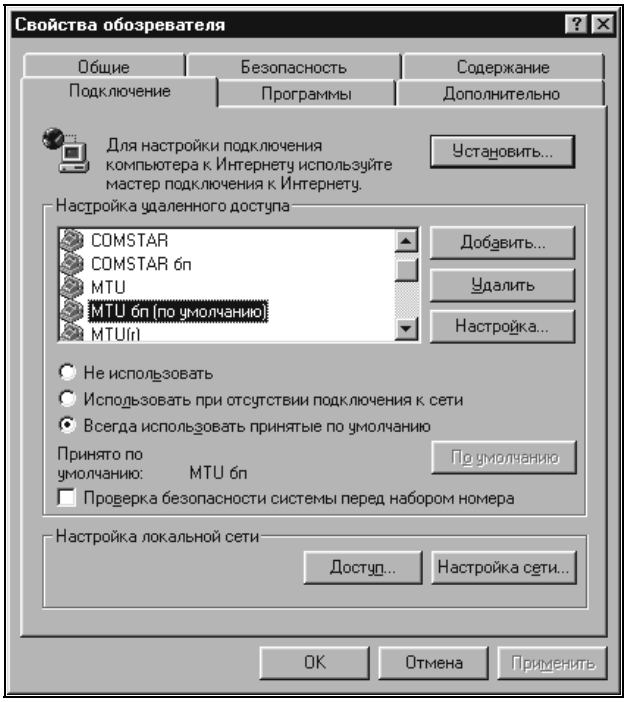

Рис. 3.4. Окно **Свойства обозревателя**

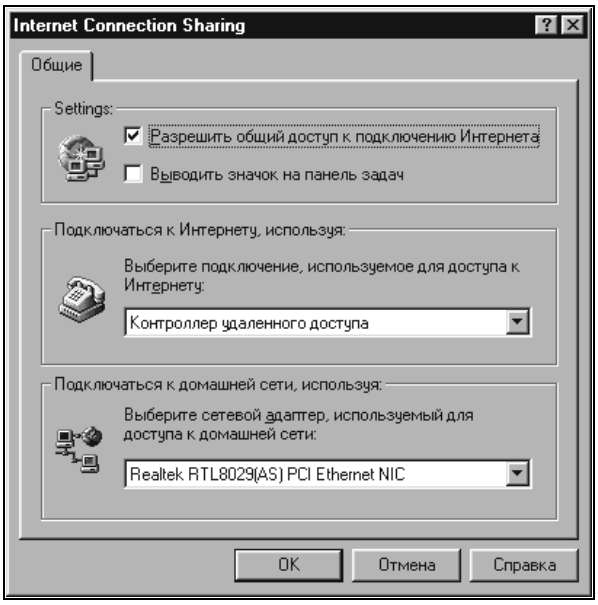

Рис. 3.5. Окно **Internet Connection Sharing**

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. 3.6).

3. Нажмите кнопку **Свойства**, появится окно, изображенное на рис. 3.7:

   - чтобы автоматически назначить IP-адрес, выберите 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;
   - чтобы назначить статический IP-адрес, отметьте 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 Internet используют адреса в диапазоне 192.168.0.xxx.

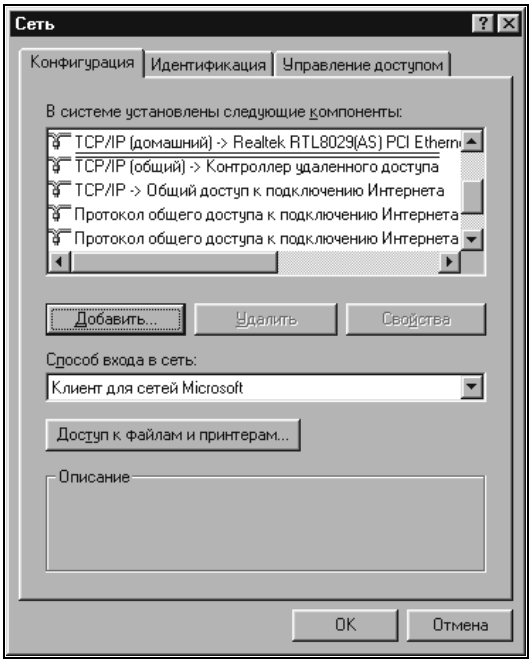

Рис. 3.6. Окно **Сеть**

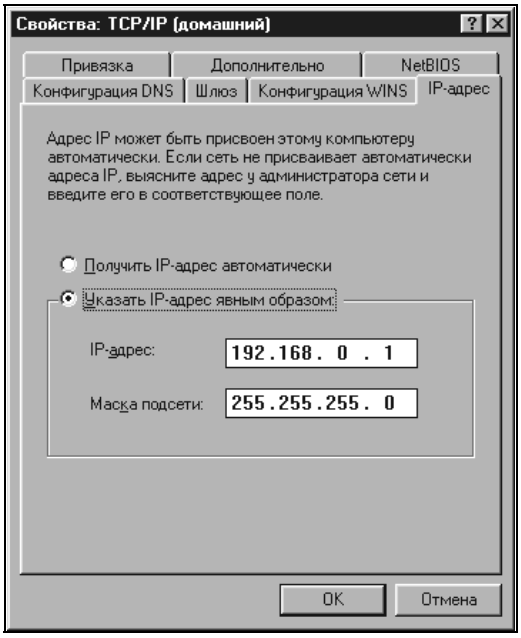

Рис. 3.7. Указание IP-адреса

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, есть возможность 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 не действительны для узлов, которые являются видимыми в Internet. Они не применимы для компьютеров, объединенных в сеть с общим доступом к подключению Internet. После назначения сетевого IP-адреса LINKLOCAL сетевому адаптеру компьютер получает возможность связываться с помощью 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 име-

ет 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 Internet или действующей службы DHCP. Статическая IP-адресация позволяет 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.

Программа настройки IP (WINIPCFG)

Windows 95/98 имеет в своем составе полезную служебную программу WINIPCFG.EXE (рис. 3.8). 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 кнопки **Освободить** или **Обновить**. Если требуется обновить или осво-

бодить 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.

Вообще говоря, маршрутизацию можно обеспечить и на Windows 95/98, правда некоторые дополнительные программки придется привлечь. Нужно будет обновить Windows 95, 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 (см. рис. 3.8), если стоит флажок рядом с надписью **Маршрутизация IP** (ip Routing enabled) все прописанные таблицы роутинга начинают работать. По умолчанию в Windows 95/98 этот флажок не выставлен.

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.

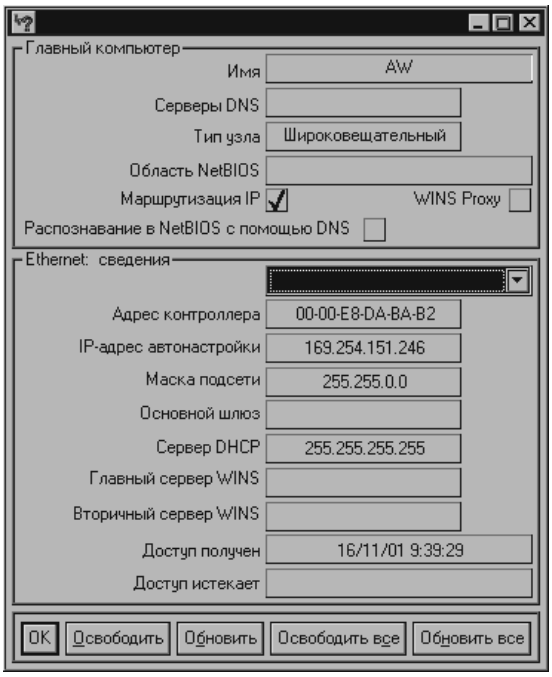

Рис. 3.8. Окно программы WINIPCFG.EXE

Ниже 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, установив которые на компьютер, вы превращаете его в шлюз между сетями.

Программа, описание которой приведено далее, позволяет установить маршрутизацию как между локальными подсетями, так и между локальной сетью и Internet. Программа эта называется WinRoute, разработана Tiny Software Inc. Различные версии программы обладают некоторыми особенностями и разнятся в списке дополнительных возможностей, как-то защита сети различных уровней, но основные функции программы доступны во всех версиях. В Internet можно найти версии от WinRoute Lit 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:

1. 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.

2. 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 Internet по модему) нет необходимости модифицировать таблицу роутинга 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. 3.9 показана сеть с двумя сегментами, один из которых подключен через маршрутизатор.

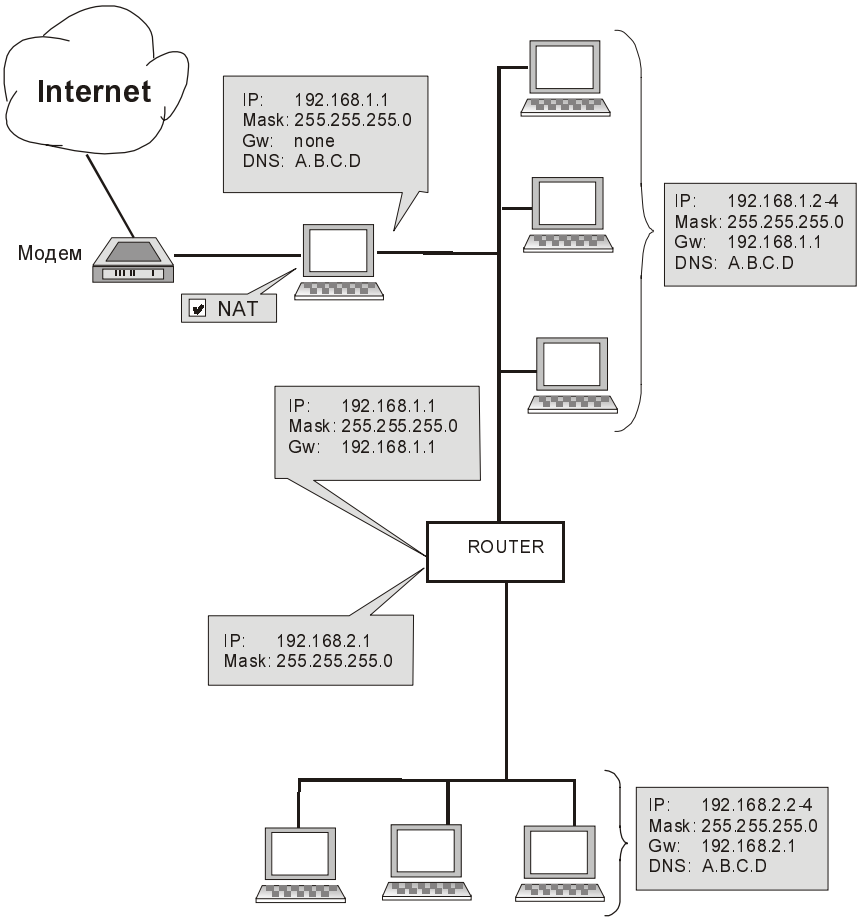

Рис. 3.9. Сеть с двумя сегментами, подключенными через маршрутизатор

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.

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, по какому интерфейсу будет пересылаться пакет. Основные пункты таблицы маршрутизации:

- network/network mask (сеть/сетевая маска);
- metric (метрика);
- interface (интерфейс);
- gateway (шлюз).

После принятия решения, каким интерфейсом будет отослан пакет, применяется следующий алгоритм:

1. Просматривается таблица маршрутизации для обнаружения записи, в которой поле **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 записей, 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 на категории записи в таблице маршрутизации в соответствии с их источниками.

- Direct (Прямые).

  Прямые маршруты добавлены в таблицу, используя IP-адрес и маску, назначенные 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 (Internet).

Таблица может быть модифицирована пользователем или протоколом маршрутизации (например, RIP), если таковой используется. Если вы создаете модемное соединение, Windows добавляет маршрут по умолчанию (в соответствии с настройками соответствующего модемного соединения). Если таблица маршрутизации уже содержит маршрут по умолчанию, его метрика увеличивается и таким образом модемное соединение получает более высокий приоритет. При закрытии модемного соединения маршрут удаляется.

Примеры работы с портами

Приведенные ниже 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 Internet к некоторым службам вашей сети. Используйте фильтрацию пакетов, если хотите разрешить доступ к порту только с нужных адресов в Internet.

Предположим, у вас в ЛВС работает Web-сервер (адрес 192.168.1.10) и вы хотите открыть к нему доступ из Internet. Вам необходимо создать порт:

1. Protocol: TCP;
2. Listen IP: <неопределен>;
3. Listen Port: `80`;
4. Destination IP: введите IP-адрес Web-сервера (в нашем случае `192.168.1.10`);
5. Destination Port: `80`.

SMTP

Если у вас в ЛВС работает почтовый сервер и вы хотите получать почту из Internet по протоколу SMTP, добавьте следующие записи в таблицу портов:

1. Protocol: TCP;
2. Listen IP: <неопределен>;
3. Listen Port: `25`;

4. Destination IP: введите IP-адрес вашего почтового сервера;
5. 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.

1. Для управляющего соединения:
   - Protocol: TCP;
   - Listen IP: <неопределен>;
   - Listen Port: 1723;
   - Destination IP: IP-адрес вашего сервера PPTP;
   - Destination Port: 1723.
2. Для пакетов GRE (PPTP):
   - Protocol: PPTP;
   - Listen IP: <неопределен>;
   - 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:

1. Protocol: UDP;
2. Listen IP: <неопределен>;
3. Listen Port: 7648;
4. Destination IP: IP-адрес компьютера, на котором запущен клиент CU-SeeMe;
5. Destination Port: 7648;
6. Protocol: UDP;
7. Listen IP: <неопределен>;
8. Listen Port: 7649;
9. Destination IP: IP-адрес компьютера, на котором запущен клиент CU-SeeMe;
10. 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:

1. Protocol: TCP;
2. Listen IP: <неопределен>;
3. Listen Port: `5000–5011`;
4. Destination IP: IP-адрес машины, на которой запущен клиент ICQ;
5. 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 Internet), **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 клентов ICQ (и эти клиенты хотят получать вызовы из Internet), 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 Internet быстрые соединения, такие как в системе DirecPC, осуществляющей связь через спутник.

Уверенный прием сигнала со спутника Eutelsat IIF3 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. Со спутника HotBird 3 зоной уверенного приема является вся европейская часть России. 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 телевизинную приемную спутниковую антенну с конвертором соответствующего диапазона и купить DirecPC ISA или PCI-карту. 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 приоб-

рести сетевую версию программного обеспечения DirecPC или, в качестве более дешевого решения, при наличии у вас dial-up-соединения с Internet, 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 Internet, 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 Internet пакеты:

- отсылаются программным обеспечением DirecPC (DirecPC Navigator);
- 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 **Use default gateway of remote network** (Использовать стандартный шлюз для удаленной сети).

На рис. 3.10 и 3.11 показана конфигурация сети с использованием первого метода (пакеты отсылаются в Internet с использованием DirecPC Navigator).

На рис. 3.12 и 3.13 показана конфигурация с использованием второго метода. Пакеты отсылаются через интерфейс RAS (модем или адаптер ISDN). В настройках TCP/IP для RAS **Use default gateway of remote network** (Использовать стандартный шлюз для удаленной сети) не должен быть отмечен, иначе весь трафик пойдет через RAS, и DirecPC не будет использоваться.

На рис. 3.14 и 3.15 показана конфигурация сети с использованием второго метода; исходящие пакеты отсылаются через интерфейс Ethernet.

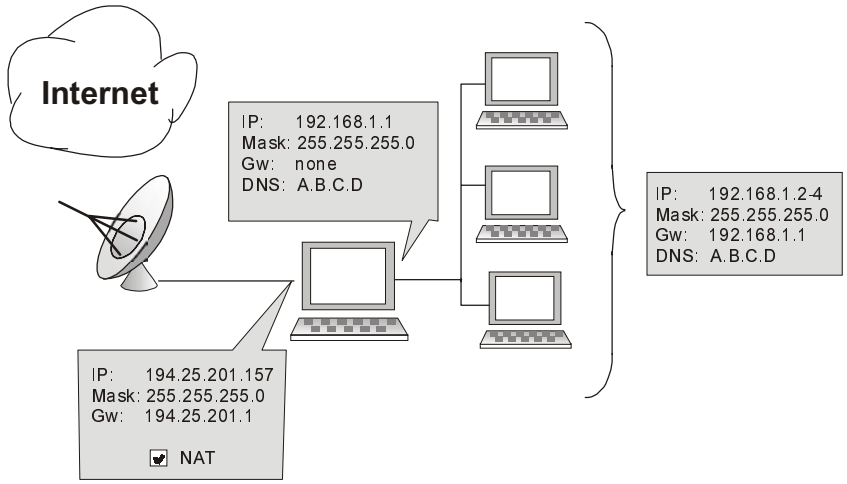

Рис. 3.10. Настройка с использованием DirecPC Navigator

Чтобы получить наилучшую пропускную способность при подключении к Internet 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.

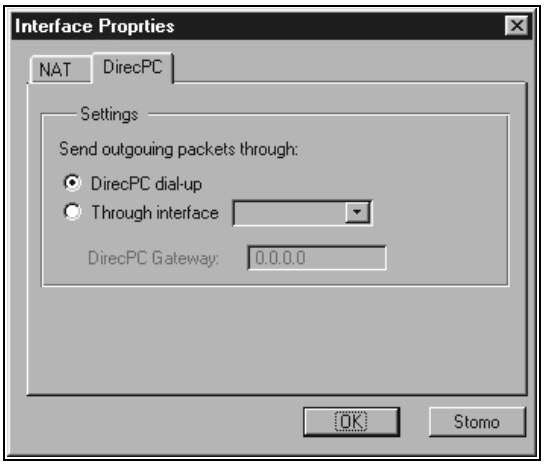

Рис. 3.11. Окно **Interface Properties**

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".

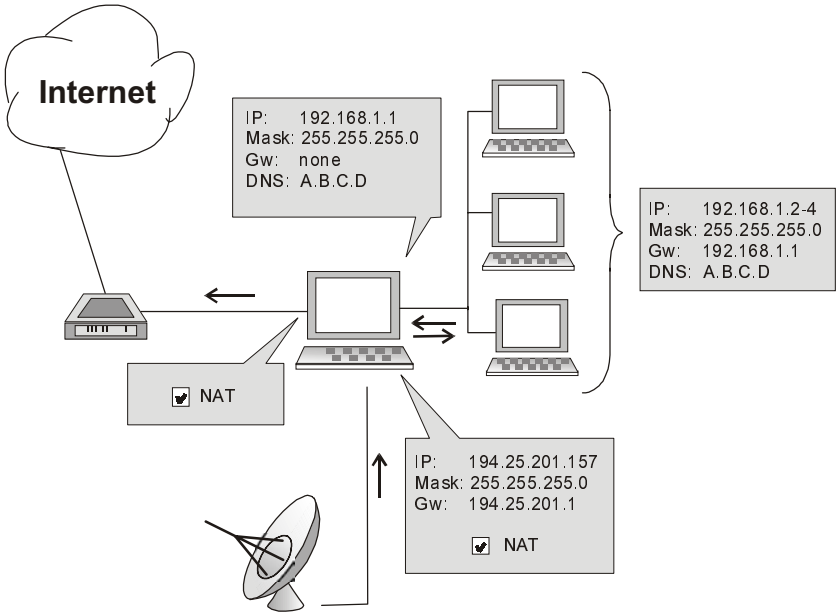

Рис. 3.12. Настройка сети с использованием RAS

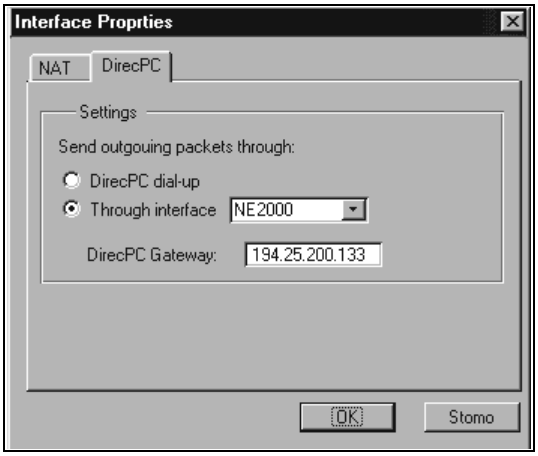

Рис. 3.13. Окно **Interface Properties**

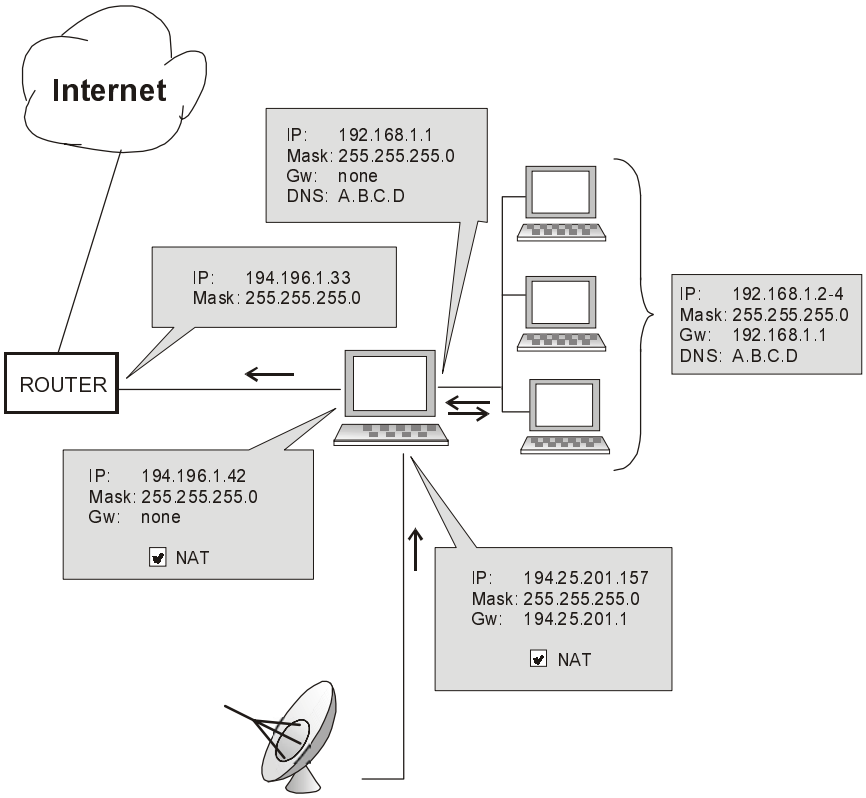

Рис. 3.14. Использование интерфейса Ethernet

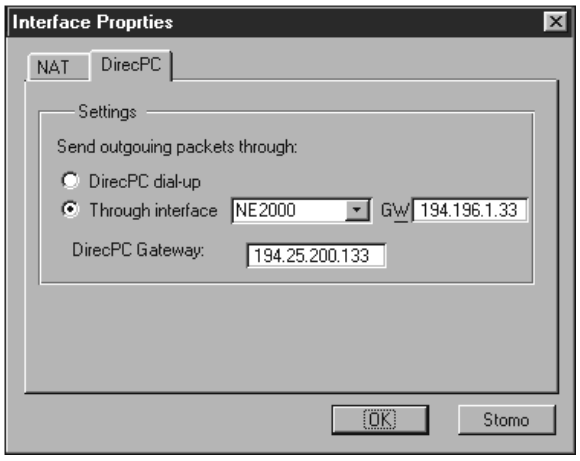

Рис. 3.15. Окно **Interface Properties**
(пакеты отсылаются через интерфейс Ethenet)

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 Internet через маршрутизатор с использованием зарегистрированного IP-адреса (рис. 3.16). 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. 3.17);
- с NAT — сеть разделена на два сегмента. Один из них открыт (public) и использует зарегистрированные IP-адреса, другой использует адрес вне приватного блока. Для доступа в Internet из приватного сегмента используется NAT. Компьютер, на котором работает WinRoute, использует две сетевые карты и подключен к обоим сегментам (рис. 3.18).

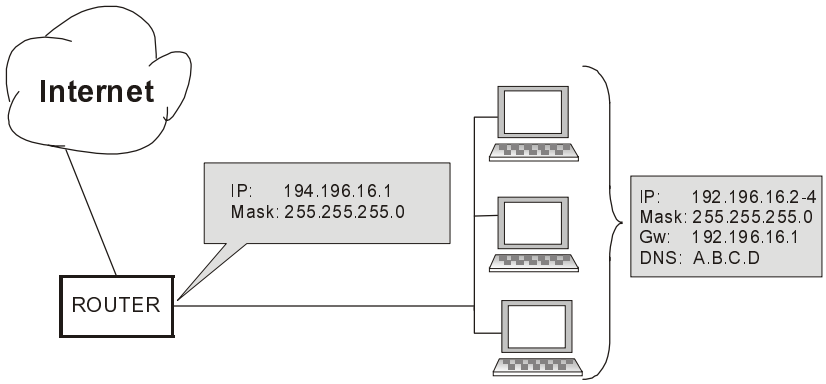

Рис. 3.16. Подключение через маршрутизатор (Router)

"Горячие" клавиши в WinRoute

- <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.

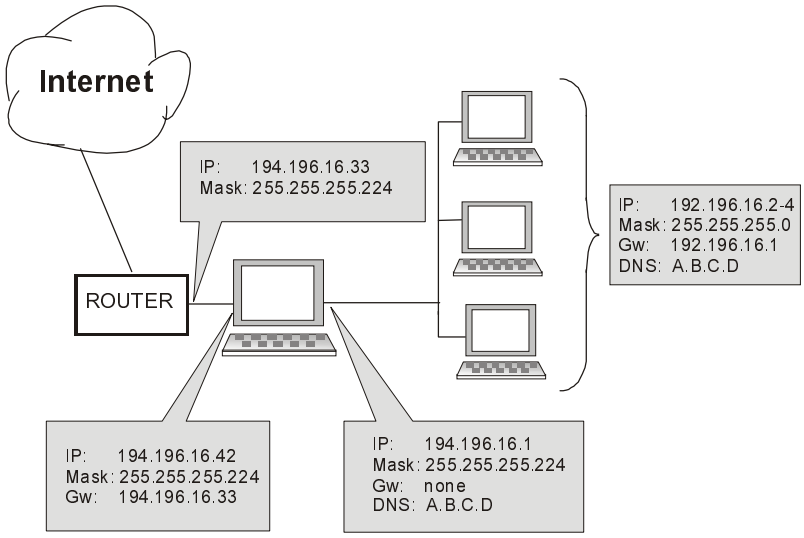

Рис. 3.17. К маршрутизатору подключены два сегмента сети

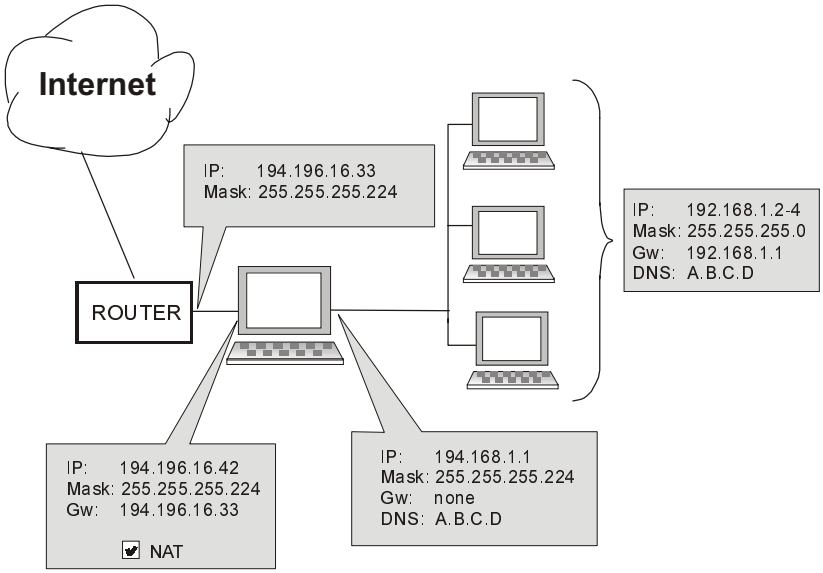

Рис. 3.18. Использование NAT для доступа к Internet из приватного сегмента

С помощью NAT (Network Address Translation) WinRoute преобразовывает вышеупомянутые адреса в "удобоваримые" для Internet.

Кроме того, WinRoute выполняет следующие полезные функции:

- NAT, Firewall;
- DNS-сервер;
- DHCP-сервер;
- Proxy-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 Internet. Winroute работает быстрее многих других proxy-серверов, т. к. весь обмен пакетами реализован на низком уровне.

Пример подключения локальной сети к Internet показан на рис. 3.19.

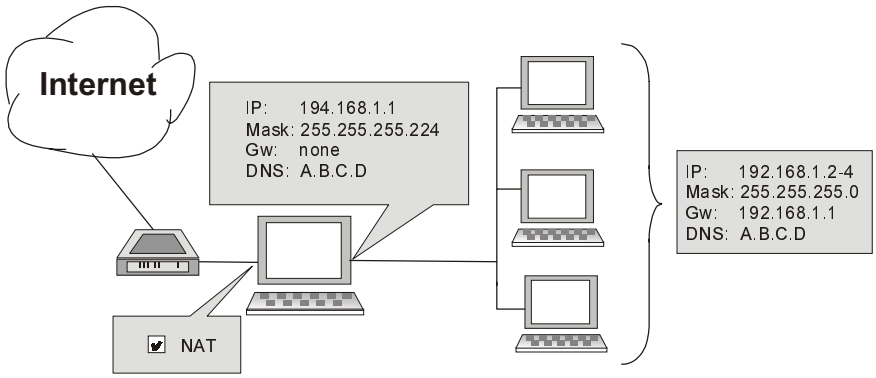

Рис. 3.19. Пример подключения локальной сети к Internet

Краткий обзор возможностей программы WinRoute Pro 4.1 RU

WinRoute Pro представляет собой уникальный по своим возможностям программный Internet-маршрутизатор и межсетевой экран, позволяющий практически без каких-либо усилий подключить к Internet 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, представляет собой решение по обеспечению безопасности, возможности которого сравнимы 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, тем самым, обеспечивая 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 и управления сетевой конфигурации. 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 Internet.

Кэширование HTTP

В архитектуре WinRoute применен не имеющий аналогов механизм кэширования. В отличие от прокси-серверов, обладающих возможностью кэширования, 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 применении 16-разрядной таблицы размещения файлов (FAT16), характерной для большинства версий ОС Windows 95.

Поддержка Internet-протоколов

Программа WinRoute поддерживает все стандартные Internet-протоколы, в том числе: IPSEC, H.323, NetMeeting, Net2Phone, WebPhone, UnixTalk, RealAudio, RealVideo, ICA Winframe, IRC, FTP, HTTP, Telnet, PPTP,

Traceroute, Ping, Year 2000 Aol, chargen, cuseeme, daytime, discard, dns, echo, finger, gopher, https, imap3, imap4, ipr, IPX overIP, netstat, nntp, ntp, ping, pop3, radius, wais, rcp, rlogin, rsh, smtp, snmp, ssl, ssh, systat, tacacs, uucpover 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 Internet-протокола, применяемый с тем, 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. Тем самым, не обладая сведениями о закрытом адресном пространстве внутреннего интерфейса, защищенного межсетевым экраном WinRoute, становится практически невозможным 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 Internet или другие сети на базе IP-протокола, а также в обратном направлении.

- Исходящие пакеты.

  Претерпевая преобразование адресов по пути из ЛВС, пакеты видоизменяются или преобразуются таким образом, чтобы они выглядели как отправленные компьютером, оснащенным технологией NAT (имеется в виду компьютер, напрямую подключенный к Internet). Конкретно речь идет о замене IP-адреса отправителя в головной метке пакета (общедоступным) IP-адресом "NAT-компьютера" (рис. 3.20). Одновременно механизм преобразования адресов создает таблицу протоколирования каждого пакета, направляемого в Internet.

- Входящие пакеты.

  Попадая в ЛВС, пакеты подвергаются "досмотру" согласно записям, хранимым механизмом NAT. При этом IP-адрес "адресата" снова заменяет-

ся (на основании упомянутых записей) на закрытый IP-адрес конкретного компьютера, подключенного к ЛВС. Следует помнить, что входящий пакет 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. 3.21).

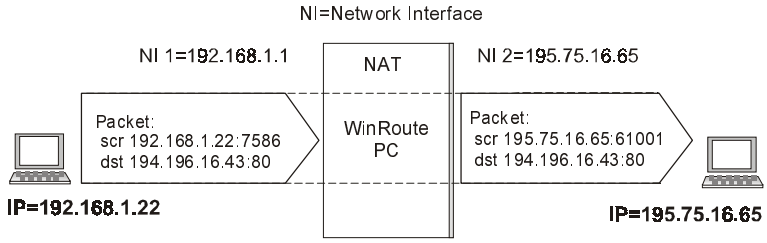

Рис. 3.20. Преобразование исходящих пакетов

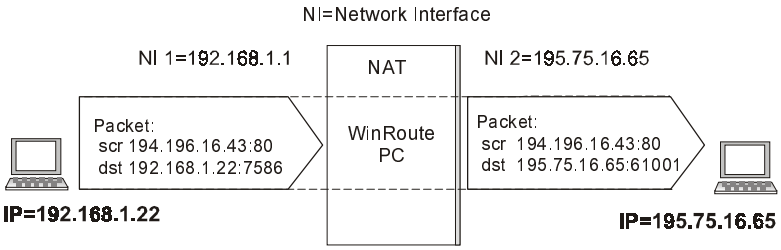

Рис. 3.21. Преобразование входящих пакетов

Архитектура WinRoute

Для освоения расширенных возможностей работы с Internet 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 ваш компьютер.

Благодаря столь совершенной архитектуре система безопасности WinRoute становится практически *неуязвимой.*

Полная поддержка протоколов

Будучи программным маршрутизатором, WinRoute работает практически с любыми Internet-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 Internet в *локальную сеть*. Если имеющееся у вас решение по организации коллективного доступа в Internet не позволяет эксплуатировать внутри частной сети серверы и приложения, к которым необходимо обеспечить доступ из Internet, тогда установка системы WinRoute в этой конкретной конфигурации может стать единственно верным решением.

Вот некоторые сетевые сервисы, к которым вам может понадобиться доступ из Internet:

- сервер telnet (например, AS400);
- Web-сервер;
- почтовый сервер;
- PC Anywhere;
- 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. 3.14.

Таблица 3.14. *Отличия в настройках WinRoute для случая нейтрального маршрутизатора*

Набор функций	Рекомендуемая настройка	В данном сценарии
NAT в интерфейсе Internet	ВКЛ.	ВКЛ.
NAT во внутреннем (ЛВС) интерфейсе	ВЫКЛ.	ВКЛ.
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 Internet без изменения сетевой конфигурации.

Примечание

Установка NAT в обоих интерфейсах не позволяет использовать WinRoute как средство коллективного доступа в Internet!

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 (telnet-сервер), 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 Internet, а второй (внутренний) — к имеющейся у вас сети.
2. Назначьте внешнему интерфейсу IP-адрес, который будет использоваться для подключения к службам/серверам, доступным из Internet.
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 Internet 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, т. е. преобразование адресов портов) может блокировать доступ из Internet к таким общедоступным сервисам внутри вашей частной сети, как, например, Web-сервер, FTP-сервер и т. д.

Как действует механизм распределения портов

На рис. 3.22 наглядно показан механизм распределения портов. Все пакеты, поступающие извне (в том числе из Internet), проверяются на предмет соответствия их атрибутов (т. е. протокола, порта и IP-адреса адресата) соответствующим 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 Internet доступ к Web-серверу, работающему по внутреннему IP-адресу 192.168.1.3. На компьютер, работающий под управлением программы WinRoute, поступают запросы пользователей из Internet 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.

Настройка механизма распределения портов

Чтобы настроить механизм распределения портов, войдите в меню **Setting | Advansed | Port Mapping** (Настройки | Дополнительно | Распределение портов) (рис. 3.23) 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, ассоциированный с вашим Internet-интерфейсом.

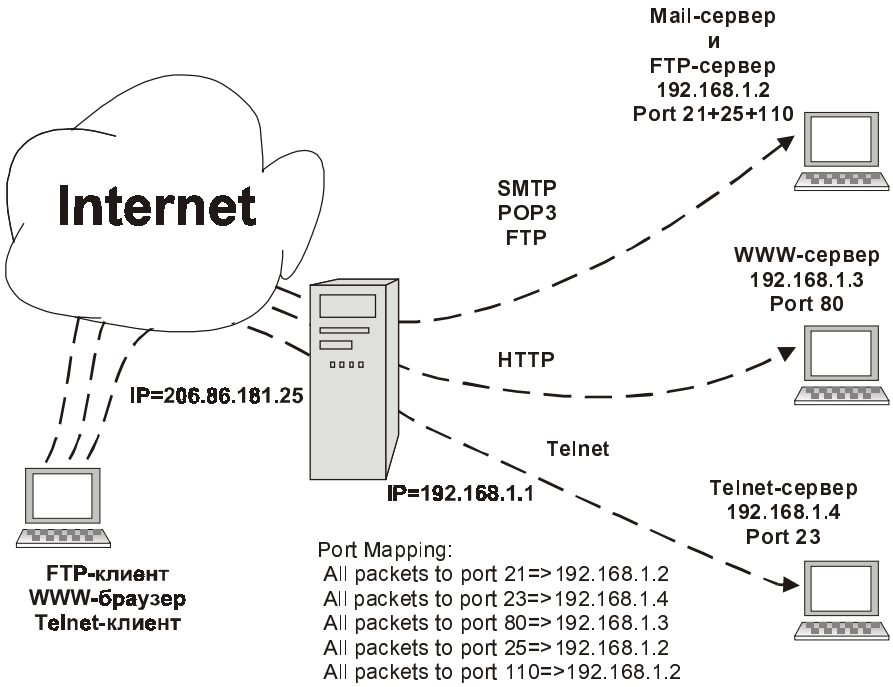

Рис. 3.22. Распределение портов

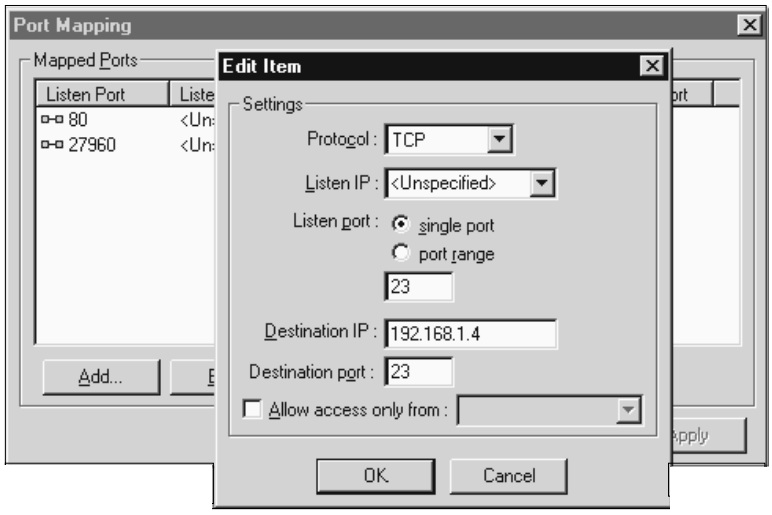

Рис. 3.23. Настройка распределения портов

Замечание

С этим интерфейсом может быть ассоциировано несколько IP-адресов (например, если у вас несколько Web-серверов).

- **Listen IP** (Прослушивание порта).

  Имеется в виду порт, на который поступают пакеты.

- **Distination 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.).

- **Distination 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 onli 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, PC Anywhere и т. п. Можно указать и группу IP-адресов, для чего ее нужно сначала создать с помощью диалогового окна окна **Addres 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. 3.24).

  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 сети WAN подразделения корпоративной структуры, обладающие закрытым адресным пространством, при этом требуется обеспечить им единый доступ в Internet;
  - 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.

Внимание

Необходимо согласовать с вашим Internet-провайдером маршрутизацию таких IP-адресов через ваш основной адрес.

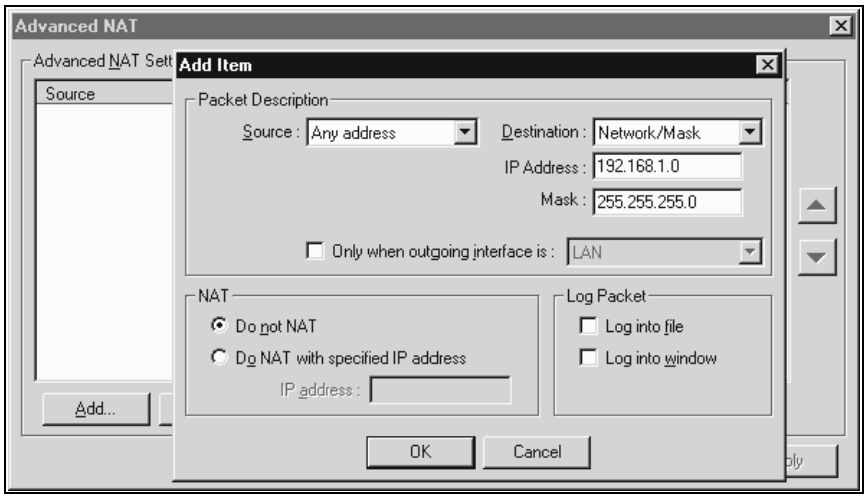

Рис. 3.24. Дополнительные настройки NAT

- **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 | Addres Groups Setting** (Настройки | Дополнительно | Группы адресов).

- **Do not NAT** (Не преобразовывать).

  Если эта опция отмечена, то в пакеты, проходящие через Internet-интерфейс, изменения не вносятся.

- **Do NAT with specified IP addres** (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 интерфеса (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), предложенный Комитетом по инженерным проблемам Internet (IETF), и Point-to-Point Tunneling protocol, завоевавший 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, а именно, 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, будучи пригодным, в особенности для высокопроизводительных Internet-узлов, которые, помимо всего прочего, выигрывают и в быстродействии.

Архитектура

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 полный свой контроль сетевые интерфейсы. Вот в этом критическом 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 получает уникальную возможность взять под контроль 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 принятия 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 Internet-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 любых 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. Будучи оснащенными средствами антиспуфинга, такие крупнейшие Web-узлы, как Yahoo и Buy.com, не подверглись бы нашумевшим в феврале 2000 года атакам с применением технологии распределенного отказа в обслуживании. Пользователи WinRoute могут быть уверенными в том, что их сети никогда не станут источником таких атак, если у них активизированы упомянутые средства антиспуфинга.

Для чего нужен прокси-сервер?

Главным предназначением прокси-сервера является экономия пропускной способности канала подключения к Internet. Когда пользователи подключаются к Internet 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 Internet и одновременно значительно ускоряя повторную загрузку файлов, в особенности графических.

При этом следует 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 Internet, поскольку эти функции берет на себя NAT-маршрутизатор, встроенный в WinRoute, а технология NAT обеспечивает коллективное подключение к Internet 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** (**Setting** (Настройки | Настройки прокси | Общие настройки) — рис. 3.25. Проверьте, активизирован ли параметр **Proxy Server Enabled** (Включить прокси-сервер). Номер порта (3128) оставьте без изменений.

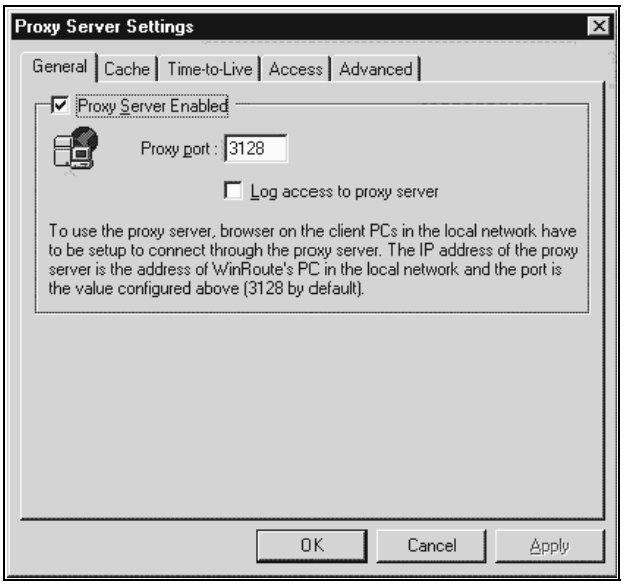

Рис. 3.25. Общие настройка прокси-сервера

2. Откройте в вашем Internet-браузере MS Internrt (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*

- **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 Internet

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 Internet, 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. 3.26) меню настроек 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. С

Access

Здесь перечисляются пользователи и/или группы пользователей, которым предоставлен доступ к тому или иному URL.

Avial. 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.

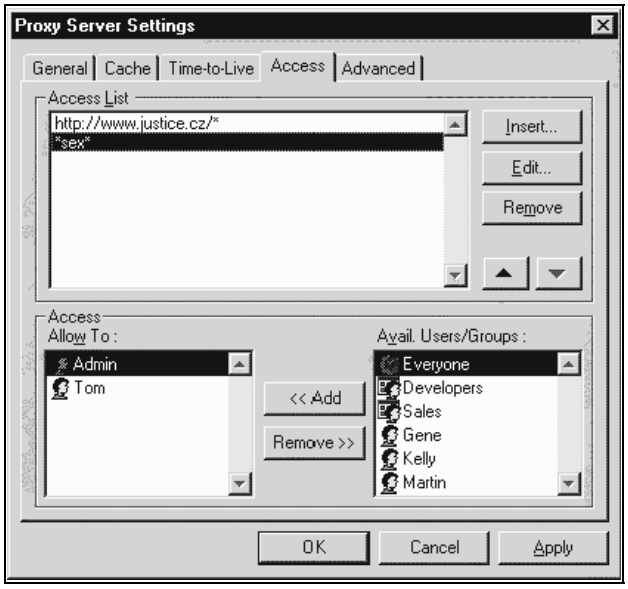

Рис. 3.26. Добавление пользователей в настройках прокси-сервера

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 Internet-сеанса им следует удалять свои опознавательные данные из памяти компьютера путем закрытия браузера.

Дополнительные возможности

На вкладке **Advanced** (Дополнительно) окна настроек прокси-сервера можно настроить программный комплекс WinRoute на использование исходного прокси-сервера (рис. 3.27).

Иногда необходимо получить доступ к прокси-серверу, обладающему значительно большей емкостью кэш-памяти или подключенному к Internet по быстрому каналу. При этом ваш собственный канал связи с этим сервером также будет сравнительно быстр, 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 присходит кэширование

В прокси-сервере программного комплекса WinRoute применяется чрезвычайно экономичный способ хранения данных: все кэшируемые объекты записываются 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 компоненты Web-страниц имеют в своей массе небольшой размер. Как правило, 50% таких объектов не превышают 6 Кбайт, тогда как размер каждого блока размещения объемных дисков — 32 Кбайт (при использовании файловой системы FAT).

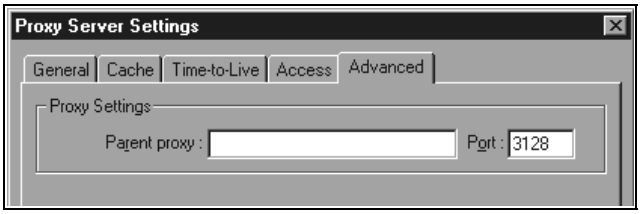

Рис. 3.27. Установка порта прокси-сервера

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 эффективную технологию индексации и, соответственно, значительно ускорить процесс кэширования в программном комплексе WinRoute.

Настройка кэширования

Кэширование можно настроить, открыв вкладку **Cache** (Кэширование) (рис. 3.28).

- **Cache Enabled** (Включить кэширование).

  Включение и отключение кэширования. При отключенном кэшировании Web-страницы всегда загружаются непосредственно из Internet.

- **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 отменит запрос (т. е. если пользователь нажмет на кнопку **Остановить** или перейдет по ссылке на другую страницу, не дожидаясь завершения загрузки текущей страницы). Это значительно ускорит повторную загрузку той же страницы в дальнейшем.

- **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.

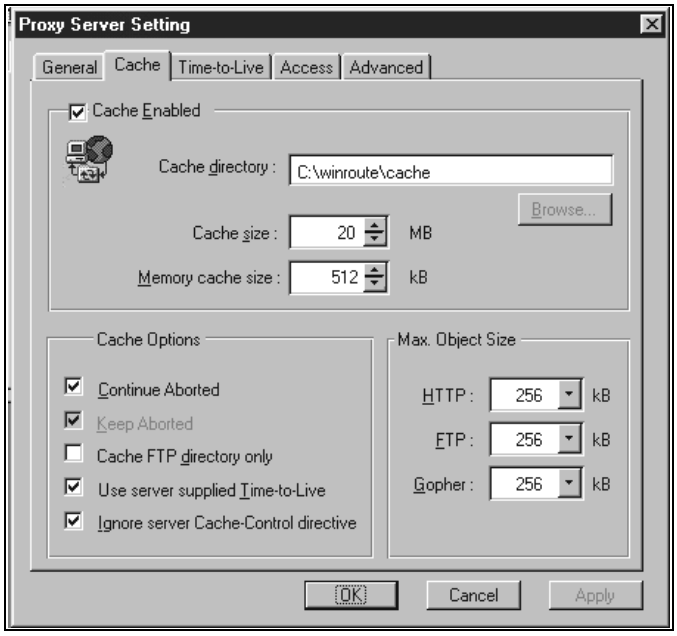

Рис. 3.28. Установка режимов кэширования

- **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, загружае-

мые 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-cControl 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.

- **Time-to-Live** (Время жизни).

  Значение времени жизни (Time-to-Live, TTL) по умолчанию следует вводить (рис. 3.29), 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 Setting** (Особые настройки по протоколам).

  Здесь можно указать время существования в днях по умолчанию для протоколов HTTP, FTP и Gopher.

- **URL Specific Setting** (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 словами, можно ввести просто `ftp` для обозначения всех серверов, в именах

которых присутствует "ftp". (В предыдущих версиях WinRoute такая возможность отсутствовала).

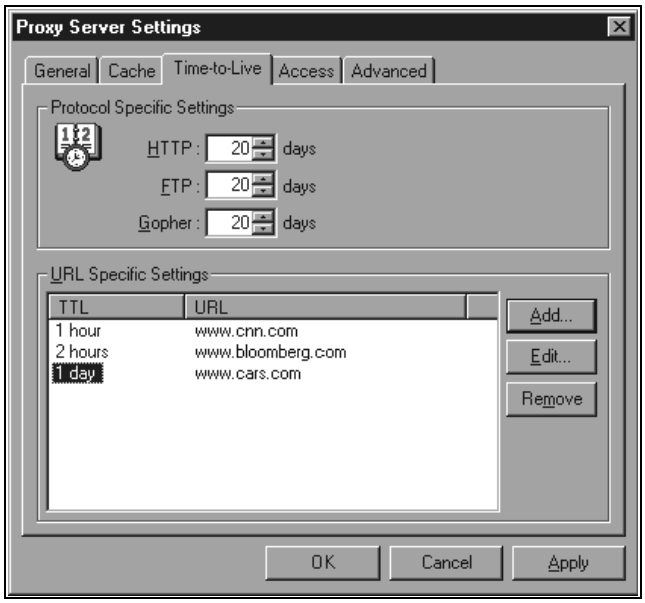

Рис. 3.29. Настройка времени жизни

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 **URL Specific Setting** (Особыми настройками 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 Internet-провайдера. Почтовый сервер WinRoute позволяет отправлять корреспонденцию как через Internet, 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 про-

вайдера 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 Internet необходимо через NAT, и кроме этого, настройте ваше почтовое программное обеспечение на прямой выход в Internet. Если вам не удается наладить обмен почтой, значит, конфигурация NAT настроена неправильно. Чтобы настроить ее надлежащим образом, см. далее *"Контрольный перечень параметров"*.

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. 3.30), 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.
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;
- **No access to administration** — контроль линий с вызовом по номеру.

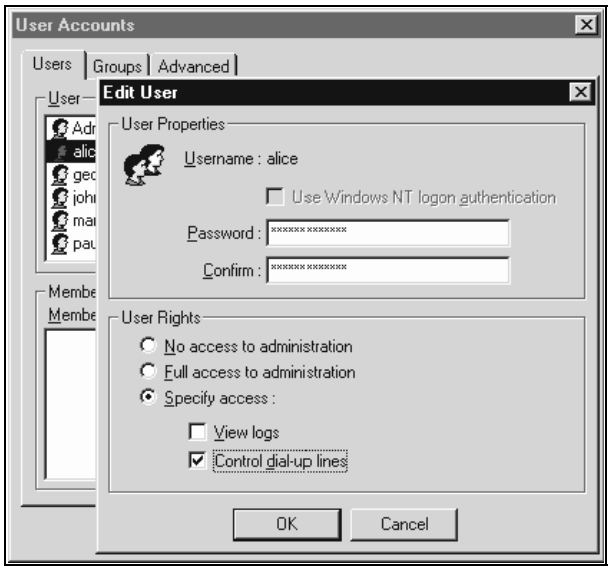

Рис. 3.30. Регистрация пользователя

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.

Контроль линий с вызовом по номеру — данный пользователь вправе подключаться к программе управления WinRoute с целью установки/разрыва связи с Internet. 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 выделяются те или иные полномочия.

Замечание

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;
- **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 Internet. Пользователи не обладают правом доступа к другим настройкам для внесения в них изменений.

Удаленное администрирование

Программный комплекс WinRoute Pro предоставляет пользователям широкие возможности удаленного администрирования. Пользователь, чьи настройки выполнены надлежащим образом и которому выделены соответствующие полномочия, может 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.

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.

- **WinRoute Engine Monitor** (Монитор).

  Является диспетчерским приложением (рис. 3.31), непрерывно отслеживающим состояние механизма WinRoute. Программа отображается в правом нижнем углу рабочего стола в виде маленького голубого значка.

- **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 главах данного раздела.

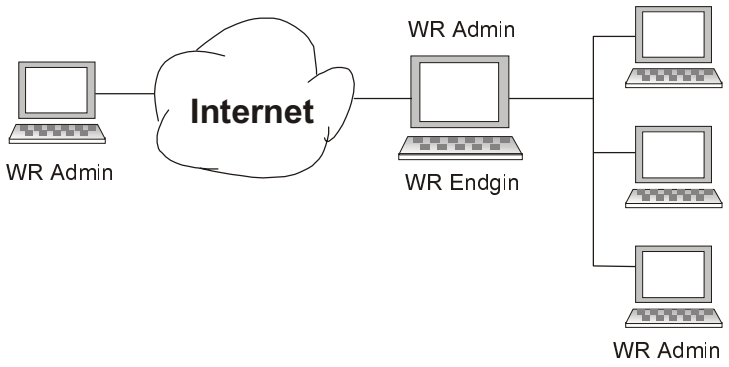

Рис. 3.31. WR Admin и WR Endgine обеспечивают настройку и контроль в WinRoute

Временные интервалы

Временные интервалы (рис. 3.32) вводятся для выполнения по расписанию следующих действий:

- фильтрация пакетов;
- обмен электронной почтой (отправка и прием сообщений);
- подключение к Internet;
- 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.

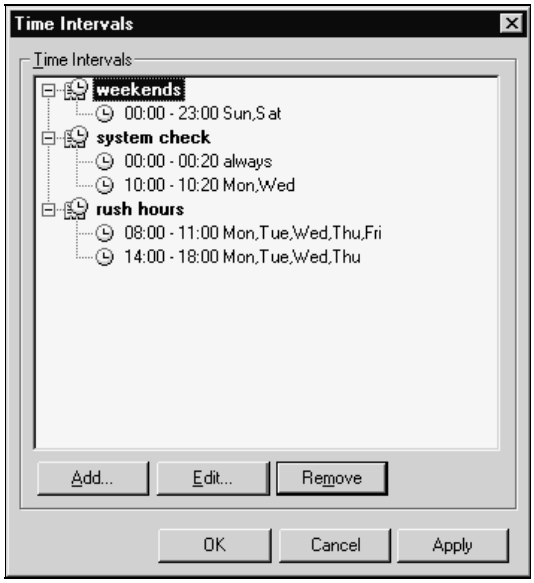

Рис. 3.32. Установка временных интервалов (расписание)

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, соблюдение которого обеспечит

успешное подключение вашей сети к Internet — разумеется, при наличии работоспособного канала для такого подключения.

Если вы намерены воспользоваться всеми преимуществами коллективного подключения к Internet с использованием технологии преобразования сетевых адресов (Network Address Translation, NAT), необходимо 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 ваши браузеры 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

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 Internet, 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 Internet (через Ethernet или RAS, либо по схеме коммутируемого доступа), а другой или другие (Ethernet, Ttoken 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 Internet-интерфейсе головного ПК комплекса WinRoute!** ВКЛЮЧИТЕ параметр преобразования сетевых адресов для интерфейса, обслуживающего подключение к Internet (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 из поля **Включить преобразование сетевых адресов** в интерфейсах, обеспечивающих подключение к внутренним сетям. В чрезвычайно 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 се-

ти, шлюз по умолчанию *не установлен*. И конечно же, шлюз по умолчанию интерфейса подключения к Internet 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 будуте 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 коплекс WinRoute используется только как межсетевой экран или почтовый сервер (т. е. без организации коллективного подключения к Internet), 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 Internet, проблем не возникает. Однако, если у вас три интерфейса (2 локальных и один для Internet), 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 возможности и настройки этой программы. Существующие варианты и версии WinRoute позволяют выбрать и подходящую по цене, и удовлетворяющую функционально программу.

Но, несмотря на множество достоинств у WinRoute, эта программа — продукт коммерческий. Версии, обладающие большими возможностями, стоят больших денег.

Internet, тем не менее, предлагает нам и бесплатные программы, которые мы рассмотрим ниже.

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 Internet 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, является нарушением общепринятых правил.

Данная программа может использоваться любым лицом или организацией для любых целей, не противоречащих закону, в том числе коммерческих, без какой-либо оплаты авторам. Ни сейчас, ни когда-либо в будущем, никто не имеет права требовать, какой бы то ни было оплаты за использование данной программы. Допускается лишь получение платы за оказание консультаций, проведение работ по установке, настройке и сопровождению данного сервера.

При создании данного сервера авторы прилагали все возможные усилия по устранению обнаруженных ошибок, но, в то же время, полное отсутствие недоработок не гарантируется. Авторы не принимают 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 Internet-серверов, к которым разработчики пришли в результате многолетних усилий в данном направлении.

Основными моментами, которым уделялось внимание, являются скорость, стабильность и надежность работы сервера. Разработчики пришли к заключению, что единственным способом добиться этой цели 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. Ниже 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** — номер порта, который принимает запросы от клиентов;
- **Threads** — количество рабочих потоков, выполняющих запросы клиентов;
- **Idle Thread Time** — время (в миллисекундах), на которое каждый поток освобождает процессор в отсутствие запросов от клиентов;
- **Master** — 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 миллисекундам. 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 на 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 миллисекунды.

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 выше, 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 освобождении 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**, имеющая два параметра:

- **Page Count** — количество используемых страниц памяти;
- **Page Size** — размер используемых страниц памяти.

По умолчанию программа устанавливает 4 096 страниц по 1 024 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, предназначенного для освобождения записи таблицы, с адресами, с которых давно не поступало никаких запросов (что 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**, имеющая четыре параметра:

- **Enable** — включение (1) или выключение (0) этого модуля;
- **Count** — наибольшее количество клиентов, которые могут одновременно работать с сервером;
- **Idle Thread Time** — время (в миллисекундах), на которое поток отслеживания клиентов освобождает процессор в промежутках между своей работой;
- **Time To Live** — 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 удлинит 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 часов, 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** и **Status Log**. 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**, 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 не обязательно) определить имена созданных групп.

Команда описания группы `GD` имеет три параметра: номер группы (от 1 до 64), адрес группы, маска. 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 более 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 бит — чем их больше, тем приоритет выше. В частности, маска `255.255.255.255`, определяющая один уникальный хост, имеет наивысший возможный приоритет (установлены все 32 бита). Другой крайний случай — маска `0.0.0.0` (при любом адресе) определяет все множество возможных адресов Internet. 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 приоритет, 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 Internet.

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 Internet.

Если для одной и той же группы имеется несколько сходных записей, то приоритет 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 (символизирует, как это уже указывалось выше, любую страницу Internet), имеет низший приоритет, который перекрывается любой записью с не пустым адресом.

Если описана некоторая группа хостов, но для этой группы нет ни одной записи типа `PA` или `PD`, то для этой группы считается открытым доступ к любой странице Internet.

Формат команды запрещенных слов `BW` включает номер группы и запрещенный в URL фрагмент. Например, команда

```
BW : 0 : photo : Комментарий
```

предотвращает доступ клиентов 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 больший 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 не обязательно)

```
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 67 584 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 3.15 от 27 сентября 2001 года по адресу **http://ln.com.ua/~vendor/progs/price.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**.

Программа позволяет настроить практически все необходимые сетевые службы (рис. 3.33).

Рис. 3.33. Фрагмент панели GateKeeper — средства настройки Wingate

Может исполнять роль прокси-сервера, сервера DNS и DHCP, выполняет маршрутизацию за пределы локальной сети, обеспечивая доступ нескольких компьютеров к Internet, осуществляет надежную защиту сети 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 приведем здесь.

Упрощенная инструкция по установке WinGate в Windows 95/98

Эту инструкцию следует использовать, если у вас имеются модем и dial-up-доступ к Internet.

Для установки WinGate необходимо выполнить шаги, описанные далее. Приведены варианты установки программы для ПК, подключенного к Internet, и компьютеров, подключаемых к Internet через WinGate.

WinGate Server Computer (WG Server) — компьютер, подключенный к Internet:

1. Установить соединение с Internet 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 Internet 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 Internet с WG Server согласно инструкциям вашего провайдера. Однако в процессе установки программного обеспечения WinGate необязательно должен быть подключенным к Internet.
4. На следующем шаге 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 из Internet или вашим провайдером. Также он никак не повлияет на настройки Internet-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 выпадающее меню;

     Замечание

     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** (Контроллера удаленного доступа) или другого сетевого адаптера, в зависимости от типа подключения к Internet;
   - 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 выпадающем меню пункт **Properties** (Свойства). Найдите протокол TCP/IP, привязанный к внутреннему сетевому адаптеру (который вы добавили на шаге 2). 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). Если у вас нет ключа регистрации, вы можете получить 30-дневный ключ по следующему адресу **http://wingate.deerfield.com/trialkey.htm**.
7. Если на ПК с WG-клиент установлена Windows 98, продолжите с п. 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 пункту 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 Client с использованием **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 **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 следующему пункту.

Настройка WG-клиент 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 мышкой 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 **Specify an IP Address** (Указать IP-адрес явным образом).
7. В поле IP-адреса введите `192.168.0.2`.
8. В поле **Subnet Mask** (Маска подсети) введите `255.255.255.0`.
9. Выберите вкладку **Gateway** (Шлюз).

10. Введите IP-адрес WinGate в поле **Gateway** (Шлюз) `192.168.0.1`.
11. Нажмите кнопку **Add** (Добавить).
12. Выберите вкладку **DNS**.
13. Выберите опцию **Enable DNS** (Включить DNS).
14. Введите уникальное имя компьютера в сети в поле **Host** (Имя компьютера).
15. Оставьте *пустым* поле **Domain** (Домен).
16. В поле **DNS server search order** (Порядок просмотра серверов DNS) введите IP-адрес WinGate `192.168.0.1`.
17. Нажмите кнопку **Add** (Добавить).
18. Оставьте пустым поле **Domain Suffix Search Order** (Порядок просмотра доменных суффиксов).
19. Нажмите кнопку **OK**, перезагрузите компьютер и переходите к п. 20.
20. Установите WinGate Internet Client. Инсталляция осуществляется с помощью того же файла, что и для WG-сервера. Выберите Client-инсталляцию. После чего, перезагрузите компьютер.

Замечание

Рекомендуется скопировать этот файл на клиентский компьютер, а не запускать его из сети.

Установка WinGate завершена. Internet-приложения на WG-клиент нужно настроить на подключение к Internet, 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 возможность выхода нашей сети в Internet. Эта возможность 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 доступ к сети извне по телефонной линии, и даже выход через нее в Internet, вполне возможно организовать. Эти и некоторые другие возможности будут рассмотрены в следующей главе.

Глава 4

Изоляции — нет!

Создав сеть с выходом в Internet, вы получили "государство", из которого можно посмотреть на окружающий мир, но из этого мира попасть к вам можно (хотя и ограниченно) только из Internet, если ваше соединение в данный момент активно. В то же время, практически везде, где бы вы ни находились, вас окружают телефоны. Возможность входа в вашу сеть по телефонной линии это:

- во-первых, бесплатный вход с удаленного компьютера, в отличие от входа через Internet;
- во-вторых, возможность доступа к вашим данным из любой точки, где есть телефон;
- в-третьих, 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. Можно проходить сквозь эти сети, получая доступ к Internet, например, используя компьютер, не имеющий к глобальной сети самостоятельного доступа, или к другой подсети, через телефонную линию, подключенную ко второму компьютеру подсети, с которой установлено соединение (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 имя нового соединения и телефон (рис. 4.2).
2. На вкладке **Тип сервера** установите опцию **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.

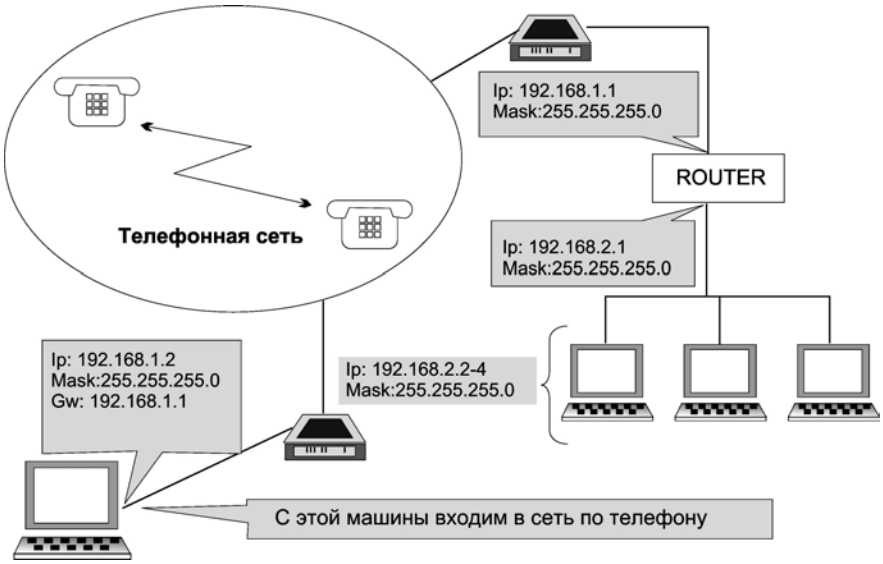

Рис. 4.1. Доступ по телефонной линии к одной из подсетей

Настройка компьютера, с которым должно производиться соединение:

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**.
6. Нажмите кнопку **ОК**, 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.

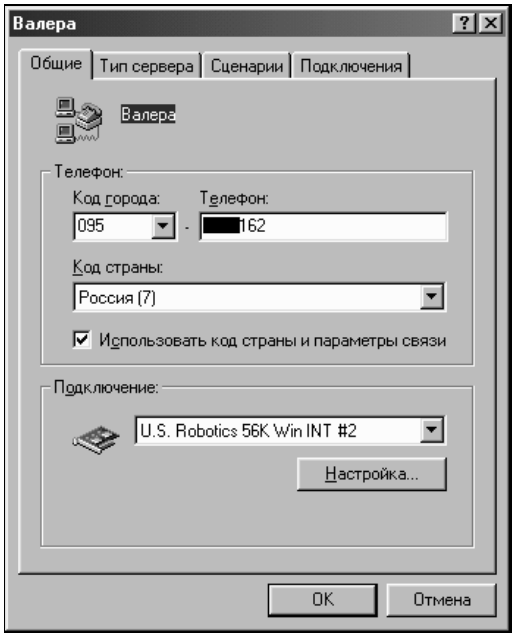

Рис. 4.2. Свойства соединения

8. Если не соглашаться с автоматическим присвоением IP-адреса для контроллера удаленного доступа, то необходимо установить 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 **Клиента для сетей Microsoft** установите — **Быстрый вход в сеть**. Остальные параметры можно оставить по умолчанию.
11. Нажмите кнопку **Доступ к файлам и принтерам** и разрешите доступ к файлам и принтерам, поставив соответствующие флажки.
12. На вкладке **Управление доступом** установите 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**. Выбрав из меню **Соединения**, обратите внимание на пункт **Сервер удаленного доступа**. Открыв этот пункт, вы можете разрешить или запре-

тить 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, т. к. 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 иконке требуемого диска, выбирете пункт **Доступ**, включите 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 программку ServerOK с сайта **http://serverok.newmail.ru** и заставить планировщик заданий, встроенный в Windows, включать разрешение на доступ в определенное время. Автор программы предлагает ее бесплатно. Рекомендации по применению находятся там же. 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 папку **Мой компьютер** и **Удаленный доступ к сети,** выбирать вкладку **Соединения**, открывать окно **Сервер удаленного доступа** и выбирать вариант — **Разрешить/Запретить удаленные подключения**, включая 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 осуществляются доступ к Internet 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.

Модем

Прочитав этот материал, возможно, вы более сознательно подойдете к выбору оборудования, от которого во многом зависит качество связи по телефонной линии, а также качество работы в Internet. Учитывая, что предполагается коллективный доступ к Internet, а также доступ к сети извне по телефонной линии модем становится одним из важнейших элементов вашей 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 связи 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, необходимо чтобы они использовали одинаковые способы преобразования цифровых данных в аналоговые и обратно, 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. Данные передаются последовательно бит за битом. Скорость, с которой происходит этот обмен, измеряется в битах за 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 определяется числом изменений сигнала, передаваемого модемом по телефонной линии, произошедших за одну секунду.

Для модуляции сигнала обычно используются следующие методы.

- 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 уже всей полосы канала. Отсюда вытекает область применения FSK — низкоскоростные, но высоконадежные стандарты, позволяющие 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 бит выше 3 (8 позиций поворота фазы) приводит к резкому снижению помехоустойчивости. 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 бит. В настоящее время используются модуляции, в которых количество кодируемых на одном "бодовом" интервале информационных бит 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, т. н. 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 бит 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 бит.

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—20000 байт, в зависимости от качества связи. Каждый блок снабжается заголовком, в котором 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 он автоматически переходит в режим передачи данных;
- 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 следующие 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 обычному модему. 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. Режим используется, когда заранее неизвестно, поддерживает ли удаленный модем протокол MNP, CCITT V.32, CCITT V.32bis и другие. В начале сеанса связи, после определения режима удаленного модема, устанавливается один из трех выше описанных 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).

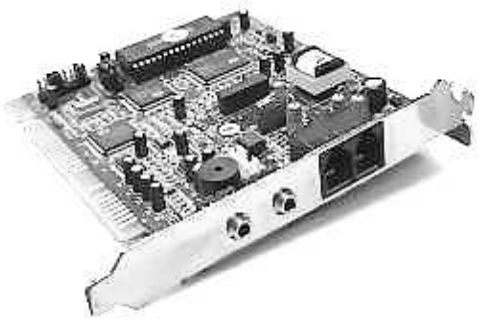

Рис. 4.3. Внутренний модем

Рис. 4.4. Внешний модем

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;

- 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 тоже 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 фирмы US Robotics — 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" — 1 180 Гц. На верхнем канале (передает отвечающий) "1" передается частотой 1 650 Гц, а "0" — 1 850 Гц. Модуляционная и информационная скорости равны — 300 бод, 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) — 1 200 Гц, верхнего (передает отвечающий) — 2 400 Гц. Модуляционная скорость — 600 бод. Имеет режимы двухпозиционной (кодируется бит) и четырехпозиционной (дибит) фазоразностной модуляции с фазовым расстоянием между точками, соответственно, в 180° и 90°. Соответственно,

информационная скорость может быть 600 или 1 200 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) — 1 200 Гц, верхнего — 2 400 Гц. Модуляционная скорость — 600 бод. Имеет режимы четырехпозиционной (кодируется дибит) и шестнадцатипозиционной (кодируется квадробит) квадратурной амплитудной модуляции. Соответственно, информационная скорость может быть 1 200 или 2 400 бит/с. Режим 1 200 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 — 1 800 Гц, модуляционная скорость — 2 400 бод. Таким образом, используется спектр шириной от 600 до 3 000 Гц. Имеет режимы двухпозиционной (бит), четырехпозиционной (дибит) и шестнадцатипозиционной (квадробит) QAM. Соответственно, информационная скорость может быть 2 400, 4 800 и 9 600 бит/с. Кроме того, для скорости 9 600 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 — 1 800 Гц, и модуляционная скорость — 2 400 бод. Имеет режимы 16-TCM, 32-TCM, 64-TCM и 128-TCM. Соответственно, информационная скорость может быть 7 200, 9 600, 12 000 и 14 400 бит/с. Режим 32-TCM полностью совместим с соответствующим режимом V.32. Протокол V.32bis является стандартом де-факто для всех скоростных модемов.

- **V.23**

  Это полудуплексный протокол с частотной модуляцией FSK. В нем имеются два скоростных режима: 600 бит/с и 1 200 бит/с. Модуляционная

и информационная скорости равны соответственно, 600 и 1 200 бод. В обоих режимах "1" передается частотой 1 300 Гц. В режиме 600 бит/с "0" передается частотой 1 700 Гц, а в режиме 1 200 бит/с — частотой 2 100 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 — 1 800 Гц и модуляционная скорость — 1 200 бод. Разница между ними заключается в возможности 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 2 400 бит/с посредством четырехпозиционной (дибит) DPSK. V.26bis и V.26ter, кроме того, имеют режим двухпозиционной (бит) DPSK, обеспечивая скорость 1 200 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 1 800 Гц и модуляционную скорость 2 400 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 1 800 Гц. Могут использоваться два режима с разными

информационными скоростями: 2 400 и 4 800 бит/с. Информационная скорость 2400 бит/с достигается модуляционной скоростью 1200 бод и кодированием дибита (4-позиционный DPSK), а 4800 бит/с — скоростью 1 600 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 — 1 700 Гц, модуляционная скорость — 2 400 бод. Имеет режимы 8-позиционной (трибит) и 16-позиционной (квадрбит) QAM. Соответственно, информационная скорость может быть 7 200 и 9 600 бит/с.

- **V.17**

  Этот протокол по своим параметрам очень напоминает V.32bis. В нем используется модуляция с решетчатым кодированием. Частота несущего сигнала — 1 800 Гц и модуляционная скорость — 2 400 бод. Имеет режимы 16-TCM, 32-TCM, 64-TCM и 128-TCM. Соответственно, информационная скорость может быть 7 200, 9 600, 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 фирмы U.S.Robotics. Протокол фактически является механическим развитием технологии V.32bis: дуплекс с эхо-подавлением, модуляция с решетчатым кодированием, модуляционная скорость — 2 400 бод, несущая — 1 800 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 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 1 800 Гц. Модуляционная же скорость 2 400 бод сохраняется лишь для 16 800 бит/с. Скорость 19 200 бит/с обеспечивается повышением модуляционной скорости до 2 743 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 сказы-

ваться при больших искажениях амплитудно-частотной характеристики канала.

- **HST**

  Протокол HST (High Speed Technology) разработан фирмой U.S.Robotics и реализован в модемах фирмы серии Courier. Это асимметричный дуплексный протокол с частотным разделением каналов. Обратный канал имеет режимы 300 и 450 бит/с. Основной канал — 4 800, 7 200, 9 600, 12 000, 14 400 и 16 800 бит/с. Применяется модуляция с решетчатым кодированием и модуляционной скоростью 2 400 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). В этих протоколах 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 бит из общего потока информации. Такого рода протоколы называют многоканальными, или параллельными, или протоколами с множеством несущих (multicarrier). В протоколе 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. Имеется 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 бит, может достигать скорости 23 000 бит/с. Кроме того, в протоколе TurboPEP применяется модуляция с треллис-кодированием, что увеличивает помехоустойчивость протокола.

- **V34**

  Отличается от протокола V32 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.

- **V90**

  По этому протоколу данные от модема к модему передаются с использованием разного вида преобразований. Информация от пользователя передается по протоколу V32 или V34, 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.

Управление модемом

После выпуска американской фирмой Hayes модемов серии Smartmodem система команд, использованная в ней, стала стандартом, которого стали придерживаться 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: `ATSr` и `ATSr=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 Hyper Terminal.

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 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

Таблица 4.1 *(продолжение)*

Команда	Значение
D	Набор номера и соединение с удаленным модемом. Формат команды D*xxxxxxx*, где *x* — цифры номера
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 "говорит" 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
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)

Таблица 4.1 *(окончание)*

Команда	Значение
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 Hyper Terminal 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 программы требуют ввода строки инициализации, которая включает последовательность AT-команд, необходимых для начала работы модема.

Модемы и доступ к Internet

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 DirectPC.

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 Internet по обычным медным кабелям.

ADSL обеспечивает обмен 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 провайдера Internet.

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 PnP и работающий в стандарте V.34. Другой пример, на выставке Comdex Fall"97 компания Boca Reseach представила двухканальный модем, работающий по технологии 56K и обеспечивающий соединение со скоростью до 112 Кбит/с.

Технология ISDN

Описанные выше 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 Service Digital Network). Интеграция услуг предполагает, что данная технология позволяет передавать по цифровым телефонным линиям не только сетевой трафик, но и другие дан-

ные, 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 Internet не претерпевает ни одного преобразования, а следовательно и не искажается. При этом пользователь имеет возможность выбирать между скоростью 128 Кбит/с 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 Internet, 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).

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 сер-

веру. При этом разрешение на доступ удобнее включать автоматически с помощью ServerOK.

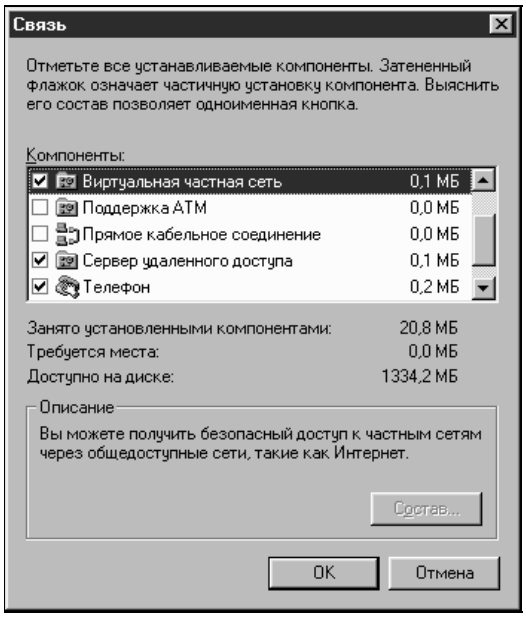

Рис. 4.5. Добавление поддержки виртуальной частной сети через установку Windows

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).

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

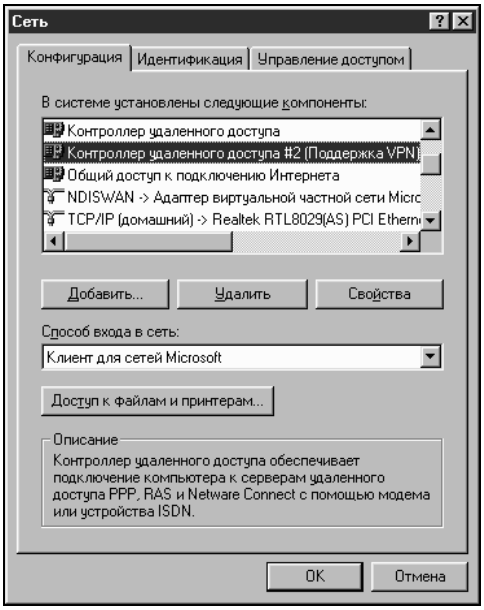

Рис. 4.6. В свойствах сети должен появиться контроллер удаленного доступа № 2

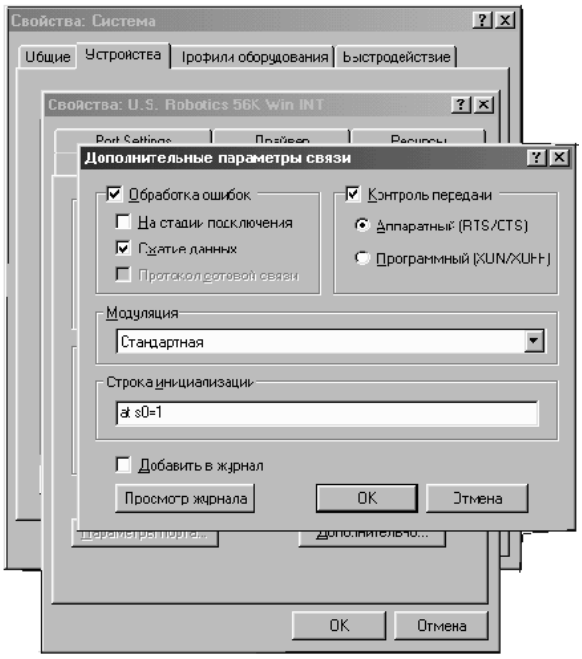

Рис. 4.7. Строка инициализации модема

Ниже приводится расшифровка строк маршрутизации.

- Сетевой адрес:
  - 0.0.0.0 — routing по умолчанию;
  - 127.0.0.0 — loopback-адрес;
  - 157.57.11.169 — адрес сетевой карты;
  - 157.57.255.255 — подсетевой "широковещательный" адрес;
  - 224.0.0.0 — multicast-адрес;
  - 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.

При включенной маршрутизации (изменение в реестре, рассмотренное в третьей главе) можно добавить необходимое число маршрутов, для обеспечения комфортной работы с сетью. Тогда не придется для обнаружения необходимого 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

Получив доступ к любой машине вашей сети (или сетей), было бы разумно получить возможность управления компьютерами сети с удаленной машины. Такая возможность позволяет:

1. Управлять сервером, не подходя к нему, даже находясь на значительном удалении от него.
2. Получать доступ к приложениям, установленным на удаленных компьютерах.
3. Совместно работать над одним документом, в одном приложении, в одно время, находясь на расстоянии от коллеги.

4. Организовывать систему помощи пользователям сети, непосредственно включаясь в их работу и корректируя их действия.
5. 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.
6. Устанавливить 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.

В настоящее время существует много таких программ, разработанных зарубежными и отечественными программистами. Среди них можно выделить три продукта:

1. RA (Remote-Anything). Разработчик: компания TWD Industries. Размер файлов 520 Кбайт, плюс PDF — руководство 780 Кбайт (**http://twd-industries.com**).
2. PcAnywhere. Разработчик: компания Symantec. Размер файла 34,7 Мбайт.
3. 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 ($25);
- ❒ ее пробная версия полнофункциональна и ограничена лишь временем использования;
- ❒ есть русскоязычная версия;
- ❒ в использовании чрезвычайно проста и понятна;
- ❒ работает в Windows 95/98/2000;
- ❒ компанией оговорены условия бесплатного получения программы.

Radmin

Это программа дистанционного управления, которая позволит вам работать на удаленном компьютере с вашего рабочего места. При этом вы видите экран удаленного компьютера в окне на своем рабочем столе или можете развернуть его на весь экран. А ваша мышь и клавиатура подменяют мышь и клавиатуру на удаленном компьютере, если управление осуществляется в полноэкранном режиме или окно удаленного экрана активно (рис. 4.8). Но можно и просто наблюдать за происходящим. Программа поддерживает LAN, WAN, а также соединение через dial-up, т. к. не требует высокоскоростного соединения. При подключении через модем, вы можете получить приемлемую частоту обновления экрана (около 5—10 обновлений в секунду). При работе внутри локальной сети, экран обновляется в реальном времени (около 100—500 обновлений в секунду). Иногда, используя Radmin в полноэкранном режиме, вы можете даже забыть, что работаете на удаленном компьютере (рис. 4.9). Radmin состоит из двух частей:

- серверная часть, которая генерирует изображение экрана;
- клиентская часть (программа просмотра), которая постоянно отображает экран удаленного компьютера на вашем экране.

Для старта Radmin вы должны запустить сервер, а также установить соединение с помощью клиентской части (программы просмотра).

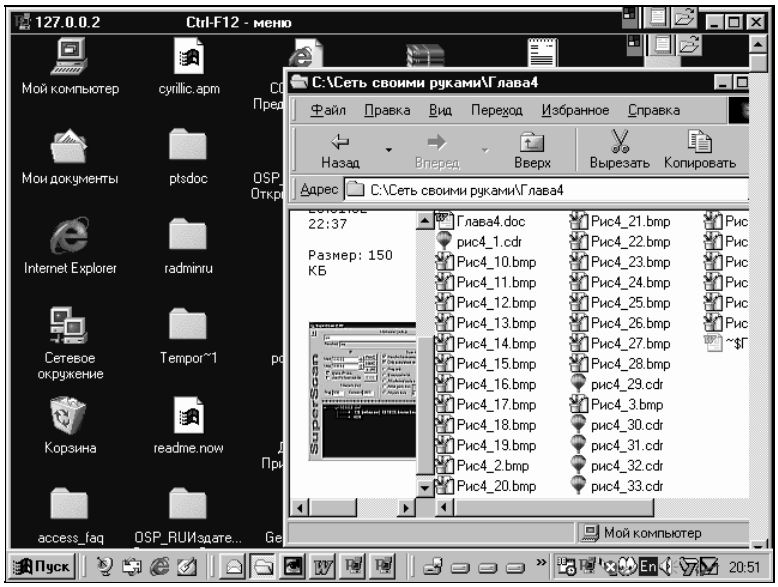

Рис. 4.8. Экран удаленного компьютера на экране вашей машины

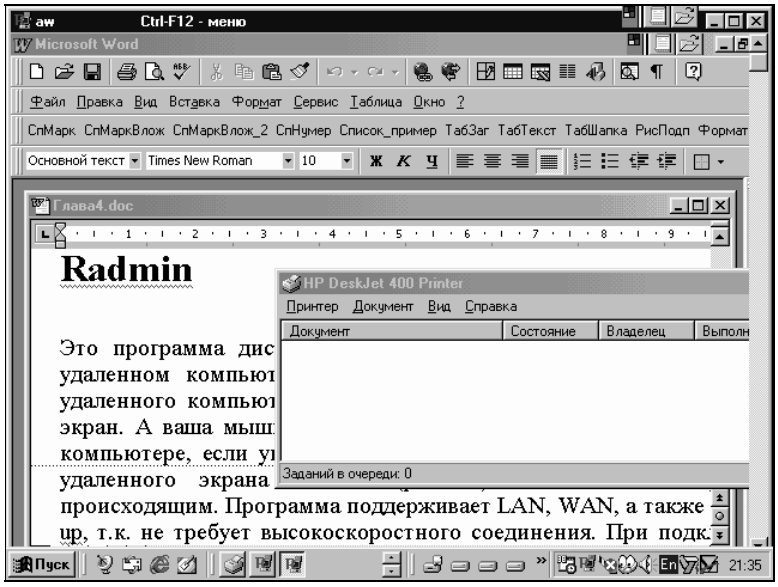

Рис. 4.9. Экран удаленного компьютера, включенного в сеть и использующего сетевой принтер

Программа существует как в русской, так и в английской версии. Далее приводится описание последней русской версии (v. 2.1).

Возможности

Radmin-сервер может работать как сервис Windows NT, Widows 2000 и Windows 9*x*/ME, что позволяет вам делать установку программы и перезагрузку удаленного компьютера дистанционно, поддерживать одновременно несколько сессий дистанционного управления и просмотра на одном рабочем месте. Полноэкранный режим позволяет вам видеть экран удаленного компьютера на всей поверхности своего дисплея. Масштабируемый режим дает возможность изменять размер экрана удаленного компьютера в своем окне.

Radmin использует драйвер видеозахвата под Windows NT для получения изменений экрана. Это позволяет вам работать на удаленном компьютере в реальном времени с потрясающей скоростью (сотни обновлений экрана в секунду и обмениваться файлами с удаленным компьютером. Дает возможность выключить компьютер дистанционно без необходимости соединения в режим просмотра (соединение в режим просмотра требует дополнительного времени, а команда **выключить** подается нажатием одной кнопки). Radmin-сервер предоставляет Telnet-доступ к удаленному компьютеру, если этот сервер работает под Windows NT. Вы можете предоставить права на удаленное управление, просмотр, обмен файлами, а также Telnet-доступ оп-

ределенным пользователям или группам пользователей. Если пользователь принадлежит к домену Windows NT, то Radmin будет использовать текущие регистрационные данные для предоставления доступа к Radmin-серверу. Если система безопасности Windows NT выключена, то доступ контролируется паролем. Radmin определяет пользователя методом "запрос — ответ", основанном на 128-битном шифровании. Для всех передаваемых данных используется 128-битное шифрование. Начиная с версии 2.1, шифрование невозможно отключить. IP-фильтр предоставляет доступ к Radmin-серверу только определенных IP-адресов и подсетей. Максимальное разрешение экрана, поддерживаемое Radmin до 2048×2048 при 32-битном цвете.

Текущая версия Radmin требует TCP/IP соединение между серверной и клиентской частями.

Минимальные требования к аппаратной части: программа работает даже на P386 с 8 Мбайт RAM под Windows 95. Может работать без дисплея, мыши или клавиатуры. Для всех операционных систем (Windows 9*x*/ME/NT/2000) необходим установленный протокол TCP/IP.

Установка

Для работы с Radmin вам необходимы два компьютера, соединенные через сеть. Установите TCP/IP-протокол на оба компьютера, а также Remote Administrator на каждый компьютер. Перед инсталляцией на ПК пользователей деинсталлируйте предыдущие версии Radmin, если таковые присутствуют.

Для пользователей Windows NT 4.0:

- для установки сервиса или драйвера вы должны иметь права администратора;
- если вы желаете использовать Radmin-сервер с драйвером видео-захвата, то должны деинсталлировать все другие программы удаленного доступа, использующие технологию видеозахвата;
- выполнение нескольких программ, использующих один драйвер видеозахвата, может привести к разрушению системы во время загрузки.

Примерами таких приложений могут быть: NetMeeting 3.0+, SMS, Timbuktu. Если имеют место проблемы с загрузкой Radmin-драйвера, то необходимо нажать клавишу "1" пять раз в течение 1 с пока идет загрузка, и Radmin-драйвер загружен не будет.

Для пользователей Windows 2000:

- для установки сервиса Remote Administrator вы должны иметь права администратора;
- распакуйте установочные файлы;

- запустите radmin21.exe;
- следуйте инструкциям программы установки.

После установки программы вы можете запустить серверную или клиентскую часть программы из меню **Пуск**. Также можно запустить из меню **Настройка сервера Remote Administrator**, и настроить Radmin-сервер для автоматической загрузки при старте Windows, изменить пароль для сетевого доступа и произвести другие настройки.

Для Windows NT 4.0 требуется Service pack 4 или более поздний.

Установка соединения

Для установки соединения необходимо выполнить следующие действия:

1. Запустите Radmin-сервер на удаленном компьютере. При этом должен появиться значок Radmin-сервера в панели Windows.
2. Подведите мышь к значку, появится IP-адрес компьютера, двойной щелчок по значку показывает список текущих соединений.
3. Значок может быть отключен в настройках Radmin-сервера.
4. На локальном компьютере запустите Radmin-viewer, выберите из меню **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 использования соединения модем — модем вы должны настроить режим удаленного доступа на стороне клиента и сервере. TCP/IP-протокол должен быть установлен на обоих компьютерах. На серверной стороне вы должны установить сервер Dial-Up (это стандартный компонент для Windows 98 и компонент из MS Plus! для Windows 95), если используется Windows 9*x*, или же RAS, если вы используете Windows NT/2000. Также необходимо настроить сервер на работу с использованием TCP/IP-протокола. На клиентской стороне вы также должны установить Dial-Up networking и настроить его на использование протокола TCP/IP. Далее требуется сделать звонок, используя Dial-Up. Затем необходимо сделать звонок, используя Dial-Up. После подключения можно найти IP-адрес удаленного сервера в **Свойствах подключения** или в **Мониторе подключения**, находящемся в **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.

Подключение через Internet

Установить соединение через Internet так же просто, как сетевое соединение. 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 Internet 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 Internet.
4. Любым образом получите информацию об IP-адресе компьютера, к которому вы желаете подключиться.
5. Подключите ваш компьютер к Internet.
6. Запустите Radmin-обозреватель на локальном компьютере, нажмите на Соединение/Соединение с..., введите IP-адрес удаленного компьютера, который вам уже известен.

Соединение через прокси-сервер

Radmin использует 4899 TCP-порт по умолчанию. 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-сервер работает под Windows, вы можете установить Radmin-сервер на этом же компьютере. Далее можно подключаться, используя **Соединение через...**. Сказанное выше относится и к firewall/router.

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, для того чтобы подключиться к компьютеру во внутренней сети, необходимо указывать IP-адрес маршрутизатора.

Если используется совместное Internet-соединение, входящее в Windows 98 SE, обозреватель Radmin не найдет ваш сервер. Проблема в том, что порт должен быть открыт, чтобы обозреватель мог найти сервер. Ссылка на программу, которая позволяет это делать, находится по адресу **www.practicallynetworked.com/sharing/ics.htm**.

Пример настроек TCP/IP для сегмента локальной сети

Для установки IP-адреса одного сегмента локальной сети войдите в установки TCP/IP сетевой карты на первом компьютере и установите IP-адрес: 10.0.0.1, сетевую маску: 255.255.255.0.

На втором компьютере установите IP-адрес 10.0.0.2, сетевую маску 255.255.255.0.

Попробуйте выполнить команду `ping` со второго компьютера:

```
ping 10.0.0.1
```

Telnet-доступ

Доступ через Telnet для Windows 95/98/ME не поддерживается из-за ограничений интерпретатора командной строки command.com в Windows 95/98/ME.

Некоторые 32-разрядные приложения используют прямой доступ к консоли. Такие приложения не работают через Telnet, потому что этот режим использует стандартные потоки ввода — вывода для взаимодействия с приложениями. Вы просто не запустите такие приложения через Telnet. Но можете выполнять их в режиме просмотра удаленного экрана.

Настройка RADMIN-сервера

Log-файл

Все действия могут быть записаны в log-файл, вы можете включить запись в log-файл, находясь в окне **Options** (Опции) параметров настройки Remote Administrator.

IP-фильтр

Эти настройки позволят вам предоставлять доступ к Radmin-серверу только с определенного IP-адреса или подсети. Вы можете установить IP-фильтр, используя команду **Настройки Radmin-сервера** в меню **Настройка сервера Remote Administrator** (из меню **Пуск**).

Ниже приводится пример настройки.

- ❒ 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 соответствуют фильтру IP-адреса, то соединение установится успешно, иначе вы получите

```
Client I/O error
```

Установка и изменение пароля для Radmin-сервера

Вы можете установить или изменить пароль для Radmin-сервера непосредственно из окна **Настройка сервера Remote Administrator**. При открытии соединения для ввода пароля будет появляться отдельное окно (рис. 4.10).

Если вы пользуетесь Windows NT/2000, можно включить поддержку системы безопасности NT в настройках Radmin-сервера. После чего следует раздать соответствующие права доступа (Полный контроль, Обзор, Telnet, Перепись файлов, Выключение) к Radmin-серверу.

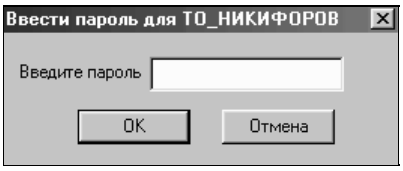

Рис. 4.10. Окно ввода пароля при открытии соединения

Установки порта

Номер и адрес порта сервера могут быть изменены из меню **Настройки Radmin-сервера** (Radmin server setup). Номер порта по умолчанию 4899.

Меню *Соединение*

Вы можете создать новое соединение, использовать уже установленное, а также выбрать вид соединения непосредственно из меню **Обозревателя Radmin**.

Окно обозревателя Radmin

Вид окна приведен на рис. 4.11.

Команды **Соединение с** или **Создать** используются для создания соединения. **Соединение с...** позволяет выбирать компьютер, через который производится подключение (опция **Соединение через**), а также устанавливать тип соединения и номер порта.

Меню режимов

Устанавливает режим контроля удаленным компьютером. Вы можете использовать **Полный контроль**, **Обзор**, **Телнет**, **Перепись файлов**, **Выключение**, режимы соединения. Если режим **Обзор** позволяет только видеть экран уда-

ленного компьютера, то использование режима **Полный контроль** позволяет управлять удаленным компьютером с помощью мыши, клавиатуры и т. д.

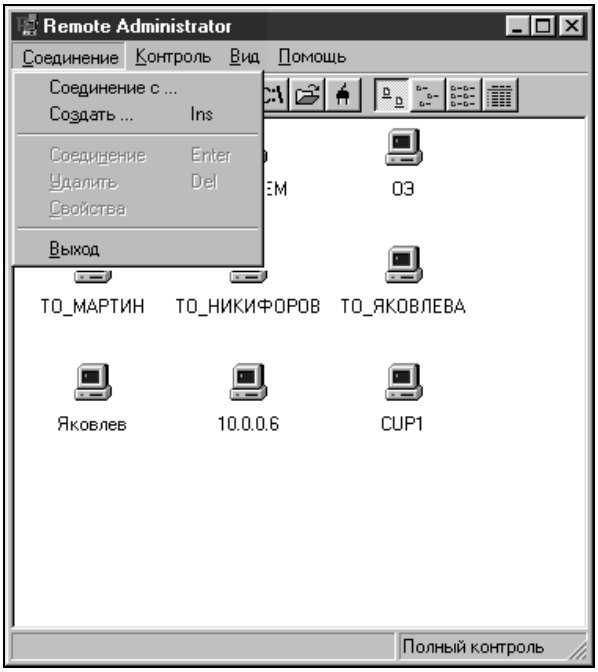

Рис. 4.11. Обозреватель Radmin

Перепись файлов

Этот режим включен в Radmin, начиная с версии 2.0. Вам необходимо выбрать **Перепись файлов** из меню **Контроль** или нажать кнопку с изображением желтой папки на панели инструментов. Интерфейс передачи файлов в Radmin похож на обозреватель Windows (рис. 4.12), однако, он работает с двумя окнами — локальным и удаленным. Вы можете выбрать вид просмотра файлов, используя кнопки на панели инструментов. Для копирования файлов можно использовать технологию drag and drop.

Также можно нажать кнопку **Копировать** на панели инструментов или щелкнуть правую клавишу мыши и выбрать **Копировать** в появившемся меню. Команда **Стоп** отменяет операцию.

Примечание

В этом режиме Radmin не поддерживает сетевые диски.

Переключение между нормальным и полноэкранным режимами

Переключение между нормальным, растянутым и полноэкранным режимами производится нажатием клавиши <F12>. Если вы хотите передать код клавиши <F12> удаленному компьютеру, используйте команду **Передать F12** из меню окна экранного просмотра (оно не имеет надписи с наименованием в заголовке, но разработчиками называется окно **RScreen**). Иногда режим нормального просмотра не подходит (например, если экран удаленного компьютера больше). Тогда можно сжать или растянуть окно **RScreen** на полный экран. Меню удаленного экрана вызывается с использованием комбинации клавиш <Ctrl>+<F12>.

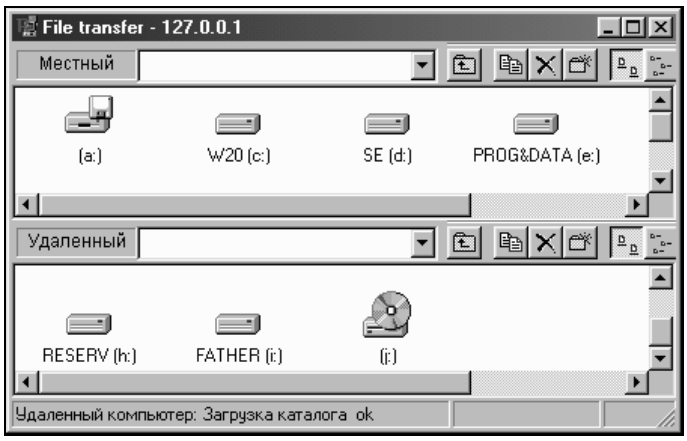

Рис. 4.12. Панели перемещения файлов

Полноэкранный текстовый режим

Radmin не регистрирует экранные изменения, если удаленный компьютер находится в полноэкранном текстовом режиме. В таком режиме GDI (Graphic Display Interface) не выполняет прорисовку экрана. Это связано с тем, что Windows работает через драйвер видеопорта недокументированно. Работа в текстовом режиме на удаленной машине возможна в оконном режиме.

Команда *Послать <Ctrl>+<Alt>+<Del>*

Если вы хотите послать код команды <Ctrl>+<Alt>+<Del> на удаленный компьютер, то можно воспользоваться пунктом меню этого окна **Послать <Ctrl>+<Alt>+<Del>**. Эта возможность существует только при подключении в режиме полного контроля и работе Radmin-сервера как системного сервиса под управлением Windows NT/2000.

Опция *Послать команду*

Вы можете использовать эту опцию для отправки на удаленный компьютер кода "горячих" клавиш типа <Ctrl>+<Esc>, <F12>, <Ctrl>+<F12>, <Alt>+<F12>, <Ctrl>+<Alt>+<F12>.

Команды *Получить буфер* и *Установить буфер*

Эти команды меню **RScreen** позволяют изменять содержимое буфера обмена.

Для того чтобы скопировать буфер обмена:

1. Выделите текст в "удаленном" окне.
2. Исполните стандартную команду "копировать" (можно просто нажать комбинацию клавиш <Ctrl>+<C>).
3. Щелчком мыши выполните команду Получить буфер (доступна в меню RScreen).
4. Выполните стандартную команду **Вставить** (<Ctrl>+<V>), предварительно переключившись для работы в "локальном" окне.

Примечание

В этом режиме Radmin не позволяет работать с файлами.

Перезагрузка

Radmin позволяет перезагрузить, выключить, завершить и возобновить сеанс пользователя на удаленном компьютере. Это можно сделать из меню окна **RScreen**.

Настройки RScreen

Если процессор на удаленном компьютере сильно загружен, установите меньшее значение максимальной скорости обновлений экрана в минуту в настройках **RScreen**. Если удаленный компьютер работает под Windows 95/98 (или Windows NT, без установленного драйвера видеозахвата) Radmin-сервер может стать причиной большой загрузки процессора при установке максимальной скорости обновлений (более 50 обновлений в минуту).

Отключение обоев приводит к увеличению скорости взаимодействия между локальным и удаленным компьютерами. Также можно установить качество цветопередачи в режим **16 цветов**. Если вы подключены через dial-up модем, то не сможете установить более 10 обновлений в секунду, потому что сигнал не способен пройти туда и обратно более чем 10 раз в секунду (ping > 100 ms).

Если вы используете Win95/98 на удаленной стороне, скорость будет зависеть от разрешения экрана удаленного компьютера. Устанавливайте невысо-

кие разрешения удаленного компьютера. Также пользуйтесь пониженными цветовыми форматами 256 цветов или 65 536 цветов. Скорость обновления экрана не зависит напрямую от количества цветов, но будьте уверены, что она не ограничена полем **Максимальная скорость обновлений в минуту** в настройках окна **Rscreen**.

Если вы пользуетесь на удаленной машине Windows NT без установленного драйвера видеозахвата, помните, что с этим драйвером Radmin работает примерно в 10 раз быстрее и намного меньше использует процессорное время.

Статистика соединения

Используйте окно **Информация о соединении,** вызываемое в меню **RScreen**, — окна для получения информации о количестве прорисовок в секунду, байт переданных в секунду и т. д.

Управление из командной строки

Radmin позволяет вводить команды управления из командной строки. Это дает возможность автоматизировать некоторые действия путем создания командных файлов, содержащих необходимую последовательность команд. Доступные через командную строку команды описаны ниже.

С помощью команды

```
radmin.exe /copyphonebook
```

создает Radmin 2.*x* телефонную книгу из телефонной книги Radmin 1.11.

Radmin-клиент может управляться из командной строки, которая позволяет создавать соединение с хостом без использования адресной книги.

Правило:

```
radmin.exe /connect:xxxxx:nnnn other_options
```

Пример:

```
radmin.exe /connect:server:1000 /fullscreen /encrypt
radmin.exe /connect:10.0.0.100:4000 /telnet
radmin.exe /connect:server /through:gate
```

Настройки:

- `/connect:xxxxx:nnnn` — указывает сервер и порт для подключения. Эта опция запрашивает соединение с сервером даже при отсутствии записи в адресной книге;
- `/through:xxxxx:nnnn` — указывает адрес и порт промежуточного сервера.

По умолчанию, режим соединения **Полный контроль** (видеть удаленный экран, управлять мышью и клавиатурой).

Для установки других режимов соединения используются следующие команды:

- /noinput — режим просмотра (видишь только экран);
- /shutdown — режим удаленного выключения компьютера;
- /file — режим пересылки файлов;
- /telnet — телнет-режим.

Следующие далее настройки работают только в режимах **Полный контроль** и **Просмотр**:

- /fullscreen — устанавливает полноэкранный режим просмотра;
- /hicolor — устанавливает формат цвета, равный 65 536, для передачи по сети;
- /locolor — устанавливает формат цвета 16, для передачи по сети;
- /updates:nn — указывает максимальное количество прорисовок для просмотра;
- /encrypt — включает шифрование всех данных при работе.

Другие настройки:

- /unregister — удаляет все уже введенные ключи для Radmin;
- /? — показывает окно помощи.

Radmin имеет некоторые дополнительные команды для управления из командной строки. Но, конечно, лучше всего, если вы все настройки будете производить, следуя за указаниями программы установки или используя **Radmin server setup** (Установка сервера Radmin). После чего вам не понадобится пользоваться настройками из командной строки.

Эта возможность предоставлена системным администраторам, которые могут вручную инсталлировать и деинсталлировать Radmin-сервер, а также изменять его настройки (номер порта, пароль и т. д.)

Правило: r_server.exe <switches>

/setup — показывает диалог (запускает мастера), который поможет установить сервис и драйвер, а также указать пароль и номер порта для Radmin-сервера.

Пример:

```
r_server.exe /setup [/port:xxxx] [/pass:xxxx]
```

Если не имеется никаких других определенных переключателей, за исключением /port и /pass, r_server выполняется как Radmin-сервер.

Пример запуска r_server без параметров, при этом удаленный ПК будет доступен без пароля и через стандартный порт (4899):

```
r_server.exe
```

Пример запуска с включением доступа по паролю:

```
r_server.exe /pass:mypass
```

Пример запуска с включением доступа через нестандартный порт:

```
r_server.exe /port:5505
```

Пример запуска `r_server` с изменением и сохранением измененного пароля и номера порта в реестре:

```
r_server.exe /port:3333 /pass:qwerty/save [/port:xxxx] [/pass:xxxxx
```

Пример:

```
r_server.exe /port:5505 /pass:qwerty /save
```

Эта команда позволяет сохранить номер порта и пароль в реестре.

Пример:

```
r_server.exe /save
```

Эта команда сохранит в реестре номер порта по умолчанию и пустой пароль.

`/install` — установка Radmin — как сервиса для Windows 95/98/NT или драйвера — для Windows NT.

Для установки драйвера, файл raddrv.dll должен быть переписан в папку System32, находящуюся внутри системного каталога Windows (обычно, c:\Windows или c:\Winnt).

Пример:

```
r_server.exe /install
```

`/uninstall` — деинсталляция программы.

Пример:

```
r_server.exe /uninstall
```

`/installservice` — установка только сервиса (Windows 95/98 или Windows NT).

Пример:

```
r_server.exe /installservice
```

`/uninstallservice` — деинсталляция сервиса.

Ошибочное выполнение данной команды приводит к сообщению, что сервис не установлен.

Пример:

```
r_server.exe /uninstallservice
```

`/installdrv` — только для установки драйвера (работает только под Windows NT).

Пример:

```
r_server.exe /installdrv
```

/`uninstalldrv` — деинсталляция только драйвера.

Ошибочное выполнение данной команды вызывает сообщение, что сервис не установлен.

Пример:

```
r_server.exe /uninstalldrv
```

`/silence` — не показывать `error-` или `ok`-сообщения, в командах `/install`, `/uninstall` или `/save`.

`/stop` — останавливает Radmin-сервер. Эта команда останавливает сервис и завершает приложение. Для остановки сервиса под Windows 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 хранится в адресной книге. Ваша адресная книга хранится в системном реестре (registry). Все операции с ней можно делать, используя regedit.exe. Экспортируйте все ключи, находящиеся

```
HKEY_CURRENT_USER\Software\RAdmin\v2.0\Clients
```

в файл. Далее вы можете импортировать этот файл (собственно, адресную книгу) в реестр на другом компьютере. Если вы желаете воспользоваться старой (из прошлой версии программы) адресной книгой, то используйте следующую команду:

```
radmin.exe /copyphonebook
```

которая создает Radmin2.*x* адресную книгу из Radmin1.11.

Поддержка

Radmin имеет прекрасно поставленную систему поддержки. На любой вопрос, возникший у вас в процессе эксплуатации программы, вы получите обстоятельный ответ. Любая проблема будет оперативно рассмотрена и разрешена. Если для исправления обнаруженного вами дефекта потребуется

обновленная версия какого-либо файла, вам его пришлют с ответом на вопрос, не заставляя посещать сайт разработчиков программы. А последняя версия программы, скорее всего, не заставит вас обращаться в службу поддержки, поскольку продумана и отработана очень тщательно.

Еще немного об удаленном администрировании

Для серверов на базе Unix и Linux возможно удаленное администрирование с помощью штатного средства Windows — Telnet.exe, для вызова которого достаточно в меню **Пуск** выбрать пункт **Выполнить** и набрать `Telnet`. Для серверов на базе Windows 95/98 это средство не подходит, но Windows 2000 совместима с Telnet.

Удаленное администрирование Windows 2000 Professional с помощью встроенного сервера Telnet

У Windows 2000 Professional есть одна ценная особенность — встроенный Telnet-сервер. Если у вас под рукой Telnet-клиент, а у сервера имеется 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 изменить режим запуска с Manual на Automatic (это делается в окне **My Computer**) — необходимо открыть **Control Panel** | **Manage** | **Services and Applications** | **Services** (Панель управления | Администрирование | Службы и приложения | Службы). После запуска сервера ваш компьютер готов обслуживать клиентские запросы на TCP-порт 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 **Display** | **Change Registry settings** (Вывод на экран | Изменение установок аутентификации), а в следующем меню — пункт **NTLM**. По умолчанию значение этого ключа 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, выведет запрос ввода имени пользователя и пароля. Значение 0 отменяет попытку аутентификации клиента по NTLM.

Теперь, когда процесс конфигурации сервера завершен, он доступен отовсюду, хоть из-под UNIX. Стоит только набрать команду:

```
telnet <имя или IP — адрес сервера>.
```

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://tucows.aaanet.ru/preview/195094.html**.

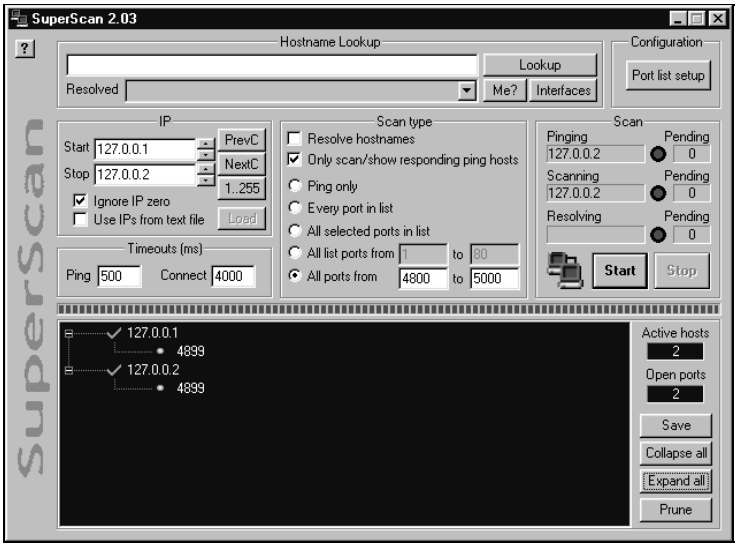

Рис. 4.13. SuperScan 2.03

Эта утилита позволяет определить активные в данный момент компьютеры в 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 Internet.

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 специально разработана для учебного класса. Возможно, конечно 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 учеб-

ного 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.

Для учебного класса актуальным является вопрос защиты программы и сети от несанкционированных действий учащихся. В LANSCHOOL этот вопрос решен достаточно хорошо. Кроме возможности установки защиты, создатели программы предположили, что особенно "продвинутые" учащиеся смогут обойти защиту. Но в этом случае действия нарушителя будут зафиксированы в *реестре* компьютера студента. Преподаватель имеет возможность 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 SP-4 или более новый, или Windows 2000;
- 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 Мбайта 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 после окончания 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

Настроенная иерархическая сеть позволяет организовать общение между пользователями более гибко, чем одноранговая. Каналом связи может служить как сама сеть, через сетевые карты, так и Internet, или телефонная ли-

ния. В некоторых случаях возможно использование всех этих каналов одновременно. Собственно 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://thunder.nht.ru**). 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 как по Internet, так и по локальной сети, и даже напрямую по модему между компьютерами. Позволяет разговаривать голосом (реализована возможность полнодуплексного разговора), передавать/получать сообщения, файлы, вести диалоговое взаимодействие. Своего рода Internet-телефон с расширенными возможностями. Также возможно предоставить определенные ресурсы (каталог, диск) для удаленного использования. Вся передаваемая информация шифруется.

Если вы желаете использовать программу в сети Internet, 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 Internet, необходим сервер-координатор. Для того чтобы сервер вас обслуживал, необходимо зарегистрироваться на нем. Регистрация производится из меню программы Координатор — **Регистрация нового пользователя**. После заполнения формы регистрации у вас будет регистрация сети "Transmitter" и пароль, которые вы сами выберите. 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 Internet, 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 не совместима с другими программными продуктами подобного рода, только с серией Transmitter.

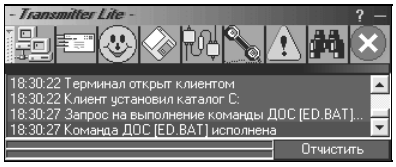

Рис. 4.14. Вид главной панели программы

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 на кнопку **Соединение**, затем введите нужные данные и нажмите кнопку **OK**. 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 Координатора указанный для связи порт игнорируется, т. к. 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 установится в 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 сервером при запуске сразу устанавливается в 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 (см. подробнее данный пункт).

В зависимости от вышеуказанных установок, Transmitter, чтобы впустить клиента, или спросит разрешения у вас, или проверит пароль, или просто допустит клиента на сервер.

Если требуется ваше разрешение, то будет мерцать кнопка **Соединение** и иконка на системной панели. Так же вы услышите звук (схожий со звуком телефона). Нажмите на кнопку, появится окно с данными клиента, его имя и адрес IP. Затем сделайте выбор: принять или игнорировать. Если вы выберите второе, то Transmitter закроет соединение и установится в режим ожи-

дания. 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 установится в 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 соответственно.

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 **Allow caller access** (Разрешить удаленные подключения). Теперь можно установить связь с этим компьютером по протоколу TCP/IP (как в Internet). В большинстве случаев после соединения у сервера будет адрес IP 192.168.55.1, а у клиента IP 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 на кнопку **Сообщение**, и в появившемся окне (рис. 4.15) введите сообщение и нажмите кнопку **Послать**. Сообщение может быть размером не более 32 Кбайт. Пустое сообщение не отсылается.

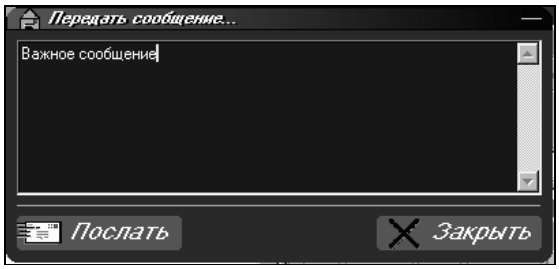

Рис. 4.15. Панель передачи сообщений

При получении сообщений от противоположной стороны, будет изменяться фон кнопки **Сообщение**, мерцать значок на системной панели. Для того чтобы прочитать полученное сообщение, нажмите на 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.

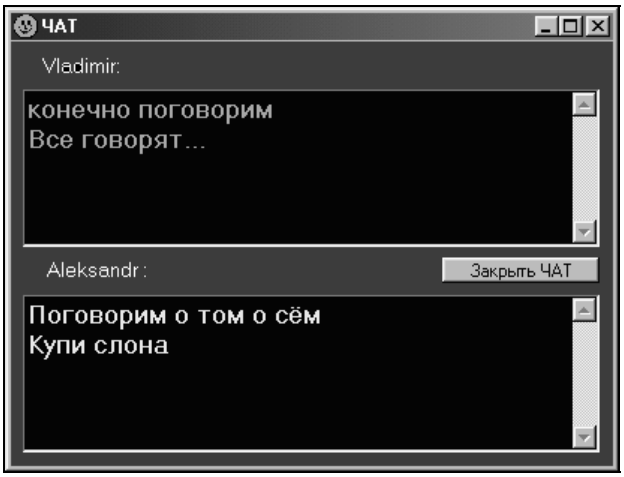

Рис. 4.16. Чат

Удаленный терминал

Один из полезных режимов работы программы — **Удаленный терминал** (рис. 4.17).

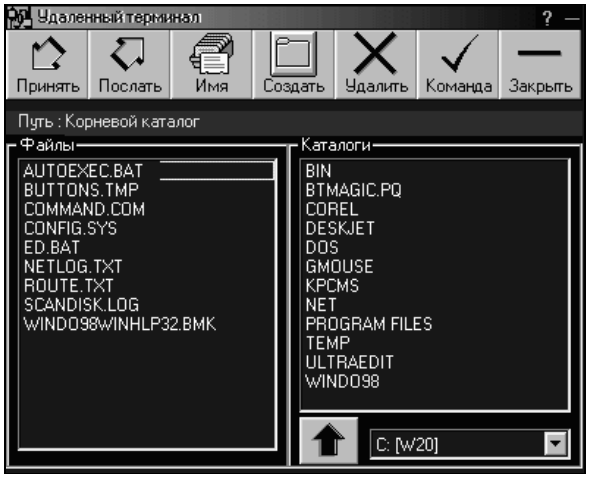

Рис. 4.17. Удаленный терминал

В этом режиме возможен 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.

Голосовая связь

Возможна при нажатии на кнопку 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. Выбрав правой кнопкой мыши значок программы в системном лотке и указав на пункт меню **Оставить сообщение**, вы получите возможность ввести в открывшемся окне текст сообщения, которое будет передано при соединении. Можно также автоматически отключиться от установившего соединение пользователя сразу после передачи сообщения.

Если у вас локальная сеть и для доступа в Internet 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, т. к. Transmitter отошлет Координатору свой текущий порт и адрес прокси-сервера.

Пример. Если программа установлена в локальной сети на компьютере с адресом 192.168.0.3, порт 20000, то вам надо создать связь на прокси: порт ожидания (Listen port, accept port) такой же, как у программы — 20000, связь на адрес 192.168.0.3, порт 20000.

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, т. к. для каждого пользователя будет своя TCP-связь.

Данная TCP-связь служит для приема звонков, а для связи с другими пользователями в Internet 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 (Internet).

Для настройки на сервис SOCKS4 откройте панель настроек **Параметры связи**, нажмите на изображение пары компьютеров и введите в соответст-

вующих полях адрес прокси-сервера и порт, на котором установлен сервис SOCKS4.

Также в данном окне можно изменить адрес сервера Координатора, если вдруг тот перенесен на другой. Не рекомендуется изменять данные Координатора без сопровождения службы технической поддержки программы.

Примечание

На момент написания этой главы я попытался соединиться с сервером автора для проверки обновлений. Увы, сервер был недоступен. Поэтому программа помещена на сайт **www.okobox.narod.ru**, где ее можно получить. Авторский сервер регистрации был доступен. На указанном выше сайте можно будет найти информацию об адресе страницы поддержки программы Transmitter, как только она будет доступна.

Такие программы, как RADMIN, SuperScan и Transmitter, могут применяться и совместно. Каждая из них обладает возможностями, дополняющими друг друга. Комплекс таких программ может обеспечить надежную и оперативную связь между компьютерами, обладающую свойствами, которые удовлетворят самого требовательного пользователя.

ICQ (I Seec You)

Следующая рассматриваемая программа предназначена исключительно для работы в Internet. Часто ее называют "Аська" (рис. 4.18). Для этой программы существуют как англоязычные, так и русскоязычные версии. Программа обладает широчайшими возможностями. После регистрации и получения регистрационного номера пользователи Internet и ICQ смогут найти вас и подключиться для разговора или передачи файлов. Если запущен NetDetect Agent — программка, обнаруживающая наличие соединения с Internet, то ICQ может стартовать автоматически, при обнаружении соединения с Internet. Работая в фоновом режиме, программа занимает мало ресурсов, и не мешает работе других приложений. При обнаружении соединения программа "объявит" о вашем присутствии в Internet 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.

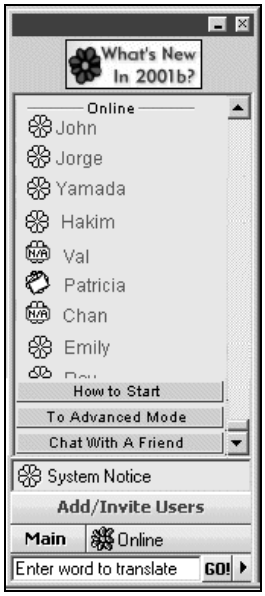

Рис. 4.18. ICQ в развернутом виде

Кроме того, программа позволяет вести наблюдение за состоянием активности пользователей, причем, как уже зарегистрированных, так и предполагаемых. Если вы знаете, что какой-либо ваш знакомый собирается установить и зарегистрировать ICQ, вы можете внести его в список пользователей, и когда он действительно зарегистрируется и подключится к Internet, 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.

Замечание

Попытка послать сообщение из Outlook Express привела к приему сообщения, которое не могло быть понято ICQ. Невозможно было посмотреть текст сообщения.

Замечание

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

Следующая программа, рассматриваемая нами (рис. 4.19), это почтовый сервер, который может работать под управлением операционной системы Windows 95/98/ME/NT/2000 (**http://courierms.narod.ru**).

Он позволит компьютерам вашей локальной сети обмениваться электронной почтой друг с другом или с любым компьютером, подключенным к Internet.

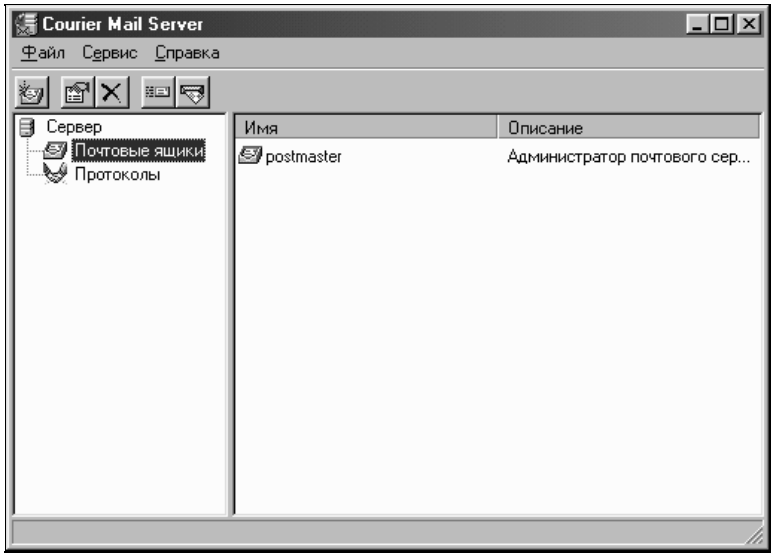

Рис. 4.19. Внешний вид окна сервера

Достоинства Courier Mail Server.

- Бесплатный
- Не требует инсталляции
- Компактен
- Легок в установке, администрировании и использовании
- Малое потребление системных ресурсов
- Многопоточность
- Удобная графическая оболочка
- Русскоязычный интерфейс и документация

Основные возможности программы:

- Courier Mail Server позволяет получить доступ к электронной почте с любого рабочего места вашей локальной сети;
- одновременно могут обслуживаться несколько клиентов;

- прием и отправка почты сервером ведется по протоколу SMTP;
- доступ клиентов к их почтовым ящикам осуществляется по протоколу POP3;
- администрирование сервера может проводиться без нарушения его работы;
- количество создаваемых почтовых ящиков неограниченно.

Courier Mail Server включает в себя следующие основные компоненты:

- SMTP-сервер;
- POP3-сервер;
- SMTP-клиент для отправки в Internet исходящих сообщений;
- POP3-клиент для получения почты из внешних почтовых ящиков.

Принципы работы

После запуска почтовый сервер ожидает подключения клиентов по протоколам SMTP и POP3. Протокол SMTP используется для отправки почты на сервер, протокол POP3 — для доступа к почтовому ящику (прием почты).

Пользователи, используя специальную программу — почтовый клиент, могут создавать сообщения, отправлять их на сервер и забирать почту из своих почтовых ящиков. Когда сервер получает от клиента сообщение, он помещает его в очередь входящих сообщений. Специальный компонент сервера — роутер — занимается просмотром очереди сообщений. Для каждого сообщения роутер просматривает список получателей. Если получатель локальный (т. е. его почтовый ящик находится на данном сервере), роутер помещает сообщение в его почтовый ящик. Если имеются получатели за пределами сервера, сообщение помещается в очередь исходящих, откуда SMTP-клиент отправляет его в Internet.

В случае, когда другой почтовый сервер отправляет почту на данный сервер, он выступает в роли клиента, и процесс передачи идет таким же образом.

Если клиент хочет получить свою почту, он подключается к почтовому серверу с помощью почтового клиента, который принимает почту с сервера и сохраняет на локальном диске для дальнейшего просмотра.

Системные требования

Для нормального функционирования Courier Mail Server, компьютер, на котором он будет установлен, должен отвечать следующим требованиям:

- операционная система Windows 95/98/ME/NT/2000;
- свободное место на жестком диске достаточное для программы — 1 Мбайт. Для поддержки пользовательских почтовых ящиков (зависит от количества ящиков и объема сообщений в них) — по крайней мере, несколько Мбайт;

❒ установленный протокол TCP/IP.

Если предполагается обмен электронной почтой с Internet, то необходимо непосредственное соединение компьютера с Internet через сетевую плату (выделенная линия) или через модем.

При наличии локальной сети, на всех компьютерах, работающих с электронной почтой, должен быть установлен протокол TCP/IP и клиентские программы, способные работать с серверами POP3/SMTP (Outlook Express, The Bat! или аналогичные).

Установка и запуск сервера

Сервер поставляется в виде архива zip, содержащего исполняемый файл и документацию. Для установки сервера необходимо создать каталог, в котором он будет функционировать, разархивировать его в этот каталог и запустить исполняемый файл.

При первом запуске сервер автоматически создаст необходимые ему для работы подкаталоги и файлы. За пределами своего каталога сервер не производит никаких изменений.

После запуска сервера в системном лотке (System Tray) рядом с часами появится его значок. При двойном щелчке мышью на иконке откроется главное окно почтового сервера.

Описание главного окна

Окно делится на несколько частей. В левой части представлена иерархическая структура компонентов (дерево компонентов) почтового сервера — **Сервер**, **Почтовые ящики** и **Протоколы**. В правой части (списке элементов) отображается содержимое того компонента сервера, который выделен в дереве компонентов.

При выборе компонента **Сервер** — в списке элементов отображаются текущие подключения клиентов. При выборе компонента **Почтовые ящики** — в списке элементов отображаются все имеющиеся на сервере почтовые ящики. При выборе компонента **Протоколы** — в списке элементов отображаются протоколы SMTP и POP3, с которыми работает сервер.

В верхней части главного окна находятся строка меню и панель инструментов. Меню содержит различные команды управления сервером. Панель инструментов содержит наиболее часто применяемые команды меню и служит для быстрого их вызова.

Настройка сервера

Выберите в дереве компонентов **Сервер** и откройте его свойства (команда **Свойства** в меню).

Вкладка *Общие*

- **Локальный домен**

  Введите имя домена, который вы хотите использовать как локальный. Например, **mycompany.ru**. Теперь, если сервер получит сообщение, адресованное, например, **user@mycompany.ru**, то он будет считать данного получателя локальным и поместит данное сообщение в почтовый ящик user. Если адрес получателя будет — **user@yourcompany.ru**, то письмо будет отправлено в Internet, так как домен **yourcompany.ru** не является локальным для этого сервера.

  Получатель, у которого не указан домен, считается локальным. Если сервер принял сообщение с адресом получателя user, он поместит сообщение в локальный почтовый ящик user, так же, как если бы был указан адрес **user@mycompany.ru**.

- **Администратор**

  Выберите из списка почтовый ящик администратора. Согласно стандарту Internet 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**, оно будет доставлено в тот почтовый ящик, который вы выбрали в списке.

- **Автоматически разрывать соединения при останове**

  Если флажок отмечен, то при останове сервера, он разорвет клиентские соединения автоматически, без подтверждения администратора.

- **Описание**

  Здесь можно указать любой текстовый комментарий.

Вкладка *Отправка*

- **SMTP-сервер**

  Укажите имя SMTP-сервера, через который будет отправляться почта в Internet. Обычно здесь указывается сервер провайдера. Если провайдер имеет домен **provider.ru**, то SMTP-сервер чаще всего называется либо **smtp.provider.ru**, либо **mail.provider.ru**.

- **Порт**

  Для протокола SMTP стандартным является порт 25. Менять его необходимо только в том случае, когда SMTP-сервер, через который вы предполагаете отправлять почту в Internet, работает через нестандартный порт.

- **Заменять локальные адреса на**

  Укажите здесь адрес e-mail, который будет определяться в качестве адреса отправителя в сообщениях, направляемых в Internet. Если поле пусто,

то замена не производится. Функция замены необходима в том случае, если локальный домен официально не зарегистрирован в службе доменных имен Internet (DNS). Предположим, что локальный домен называется **mycompany.ru**. Этот домен не зарегистрирован. Локальный пользователь с адресом **user@mycompany.ru** отправил сообщение на адрес в Internet. Имеется два варианта.

- SMTP-сервер, через который производится отправка, откажется принимать такое сообщение, поскольку домен **mycompany.ru** ему неизвестен.
- Сообщение будет отправлено и доставлено получателю, но при ответе на это сообщение адрес получателя будет **user@mycompany.ru**. Такое сообщение не сможет быть доставлено, поскольку домен не зарегистрирован и, соответственно, неизвестен почтовым серверам Internet. Таким образом, в данной ситуации необходимо использовать замену адреса. Если в поле ввести реально существующий адрес e-mail (например почтовый ящик, размещенный у провайдера), то сервер, принимающий сообщение, будет считать, что оно отправлено с этого адреса. Ответ на сообщение будет доставлен на данный адрес.

Вкладка *Внешние ящики*

В списке содержатся параметры подключения к почтовым ящикам, расположенным на других почтовых серверах. Записи с установленным флажком — активные. Когда серверу будет дана команда **Принять почту**, он подключится к активным почтовым ящикам и заберет с них почту. После успешного приема почты, сообщения удаляются из почтовых ящиков. Кнопки **Добавить**, **Изменить**, **Удалить** позволяют редактировать список. При добавлении или изменении элемента, необходимо заполнять следующие поля:

❒ **POP3-сервер**

Имя POP3-сервера, на котором расположен почтовый ящик. Если e-mail имеет вид **user@provider.ru**, то POP3-сервер, обычно, имеет имя **pop.provider.ru** или **mail.provider.ru**.

❒ **Порт**

Для протокола POP3 стандартным является порт 110. Менять его необходимо только в том случае, когда POP3-сервер, на котором находится данный почтовый ящик, работает через нестандартный порт.

❒ **Пользователь**

Имя пользователя, используемое для подключения. Если e-mail имеет вид **user@provider.ru**, то, обычно, имя пользователя — **user**.

❒ **Пароль**

Пароль почтового ящика.

- **Получатель**

  Выберите из списка локальный почтовый ящик, в который будут помещаться принятые сообщения. Если выбрано **Входящие**, то сообщения будут помещаться в очередь входящих. Можно не выбирать значение из списка, а ввести вручную любой адрес e-mail. Сообщения будут отправлены на этот адрес.

- **Использовать авторизацию APOP/MD5**

  Поставьте флажок, если вы хотите использовать шифрование пароля при передаче его на сервер. Некоторые POP3-сервера могут не поддерживать этот метод авторизации.

Вкладка *Очереди*

Используя переключатель **Имя очереди**, можно выбрать либо **Входящие сообщения** — для просмотра сообщений, которые только что получены сервером и еще не обработаны, либо **Исходящие сообщения** — для просмотра сообщений, которые будут отправлены в Internet при очередном сеансе связи.

Список сообщений имеет следующие поля:

- **От** — отправитель сообщения;
- **Кому** — получатель сообщения;
- **Время отправки** — время, когда сообщение было поставлено в очередь;
- Кнопка **Обновить** служит для обновления на экране содержимого очереди.

Вкладка *Журнал*

В списке перечислены основные компоненты сервера. Для каждого компонента показан уровень подробности, использующийся при записи событий сервера в журнал работы.

При низком уровне, в журнал записываются только наиболее важные сообщения и сообщения об ошибках.

При среднем уровне к протоколируемым событиям добавляются все основные события компонента в кратком виде.

При высоком — записываются также данные почтовых протоколов и прочая детальная информация.

Для изменения уровня выделите компонент и укажите нужный уровень, нажав соответствующий переключатель.

Настройка протокола SMTP

Выберите в дереве компонентов **Протоколы**, в списке элементов **SMTP** и откройте его свойства.

- **Разрешить протокол** — если флажок отмечен, то сервер будет принимать подключения клиентов по данному протоколу, если флажок снят — протокол будет отключен.
- **Порт** — для протокола SMTP стандартным является порт 25. Если вы укажете нестандартный порт, то будет необходимо указать этот же порт и в клиентских программах, которые будут подключаться к этому серверу.
- **Тайм-аут бездействия** — бездействием считается ситуация, когда клиент, подключенный к серверу, перестал отправлять серверу команды. Поскольку это отнимает ресурсы сервера, можно ограничить время ожидания сервером команды от клиента.
- **Не закрывать бездействующие соединения** — сервер будет бесконечно долго ожидать команд от клиента. Данная установка не рекомендуется, потому что сервер будет впустую расходовать ресурсы системы.
- **Закрывать бездействующие соединения** — если за указанное время от клиента не поступило ни одной команды, сервер принудительно отключает клиента и закрывает соединение.
- **Тайм-аут (минут)** — время ожидания в минутах. Согласно стандартам Internet — не менее 10 мин, но для локальной сети можно указать и меньшее значение.
- **Описание** — здесь можно указать любой текстовый комментарий.

Настройка протокола POP3

Выберите в дереве компонентов **Протоколы**, в списке элементов **POP3** и откройте его свойства.

Вкладка *Общие*

Параметры на этой вкладке имеют то же значение, что и в протоколе SMTP. Стандартным для протокола POP3 является порт 110.

Вкладка *Авторизация*

Отметьте флажками те способы авторизации, которые разрешено использовать клиентам при подключении к серверу. При базовой авторизации USER/PASS, клиент передает пароль серверу в открытом виде. При авторизации методом APOP/MD5, пароль шифруется алгоритмом MD5 и в таком виде передается на сервер. Для защиты от перехвата пароля рекомендуется использовать метод APOP/MD5 и отключать базовую авторизацию. При этом в клиентских программах необходимо включить использование этого метода.

Создание почтовых ящиков

Выберите в дереве компонентов **Почтовые ящики**. В списке элементов появятся имеющиеся на сервере почтовые ящики. Для создания нового ящика выполните команду меню **Создать почтовый ящик**. Появится окно со свойствами нового ящика, которые необходимо заполнить (рис. 4.20).

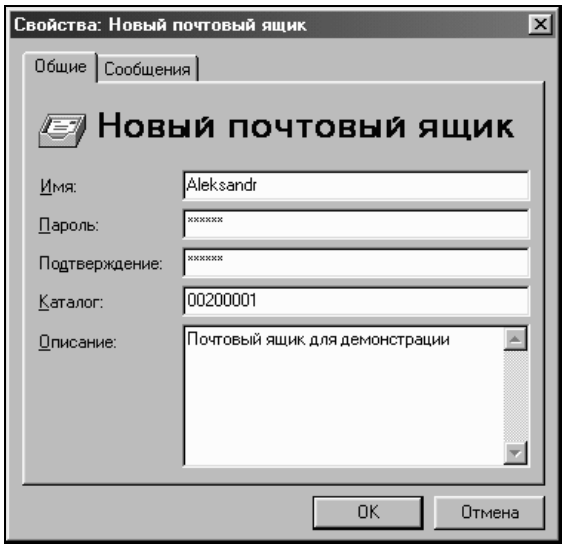

Рис. 4.20. Добавление нового ящика

Вкладка *Общие*

- **Имя** — имя почтового ящика. Желательно не использовать русские и специальные символы — некоторые программы работают с ними некорректно.
- **Пароль** — пароль для подключения к почтовому ящику.
- **Подтверждение** — повторите пароль.
- **Каталог** — имя каталога, в котором будут храниться письма данного ящика. По умолчанию предлагается уникальное имя из восьми символов. Вы можете заменить его на более осмысленное.
- **Описание** — здесь можно указать любой текстовый комментарий.

Вкладка *Сообщения*

Список содержит заголовки сообщений, которые находятся в данном почтовом ящике. Внизу указано количество сообщений в ящике.

- **Редактирование и удаление почтовых ящиков** — выберите нужный ящик в списке элементов компонента **Почтовые ящики**. Для редактирования

свойств выполните команду меню **Свойства**. Для удаления ящика выполните команду меню **Удалить**. При удалении ящика удаляется также каталог, содержащий сообщения.

Эксплуатация сервера

Чтобы сервер запускался автоматически при запуске Windows, поместите его ярлык в папку **Автозагрузка** (Startup). Правильно настроенный сервер не требует внимания и работает в автоматическом режиме. Для остановки сервера используйте команду меню **Файл | Остановить**.

Текущие подключения к серверу можно увидеть в списке элементов компонента **Сервер**. В списке показываются:

- IP-адрес подключившегося компьютера (**Хост**);
- внутренний идентификатор подключения (**ID**);
- имя пользователя (поле, которое показывается только при подключении по протоколу POP3, и только после авторизации клиента сервером);
- протокол, по которому произошло подключение (**Протокол**);
- время, когда произошло подключение (**Время подключения**).

Очередь входящих и исходящих сообщений можно посмотреть в свойствах сервера (см. п. "Настройка сервера").

Заголовки писем, находящихся в почтовом ящике, можно посмотреть в свойствах ящика.

В случае возникновения проблем, для определения их источника, можно воспользоваться журналом работы. Файлы журнала находятся в подкаталоге Log\ каталога сервера. В них записываются события, происходящие на сервере. Файлы журнала имеют названия вида: ГГГГММДД.log (год, месяц, день). Журнал каждого дня работы сервера записывается в отдельный файл.

Настройка почтовых клиентов

Для того чтобы почтовый клиент мог отправлять и принимать почту, в его настройках нужно указать адреса серверов для входящей и исходящей почты, а также параметры подключения к почтовому ящику. Настройки в разных почтовых клиентах называются по-разному, но, обычно, имеются следующие настройки:

- **SMTP-сервер**, **POP3-сервер**, **Пользователь** (Учетная запись), **Пароль**.

  В поля **SMTP-сервер** и **POP3-сервер** нужно ввести адрес компьютера, на котором запущен почтовый сервер. Желательно вводить IP-адрес, а не сетевое имя. IP-адрес компьютера можно узнать, запустив на нем программу winipcfg.exe из каталога Windows и выбрав в ней из списка сете-

вую плату. В поля **Пользователь** и **Пароль** нужно ввести имя и пароль почтового ящика, которые были использованы на сервере при создании этого ящика. Если сервер использует нестандартные номера портов, то в клиентской программе нужно указать соответствующие значения (обычно, есть поле **Порт**). Тип подключения к серверу — с помощью локальной сети.

Проверка работоспособности почтовой системы

После настройки сервера и клиентских программ попробуйте отправить сообщение от одного локального пользователя другому. В почтовом клиенте создайте новое сообщение. В поле **Кому** (To) введите почтовый адрес другого пользователя, почтовый ящик которого уже создан на сервере. Можно указать просто имя ящика, например, Пользователь или полный адрес — `user@mydomain.ru`, где `mydomain.ru` — ваш локальный домен (*см. разд. "Настройка сервера" ранее в этой главе*). Тему и содержание письма напишите любые. Отправьте письмо. Оно должно без ошибок отправиться на сервер. Теперь примите почту на компьютере адресата. Должно прийти ваше тестовое письмо.

Ответьте на письмо. Примите почту на исходном компьютере. Если ответ получен, можно считать почтовую систему работоспособной в локальной сети.

Если возникают проблемы с отправкой или получением почты, запустите на клиентском компьютере программу telnet.exe из каталога Windows. Выберите в меню **Подключить** команду **Удаленная система**. В поле **Имя узла** введите IP-адрес или имя компьютера с почтовым сервером. В поле **порт** введите `110`. Нажмите кнопку **Подключить**. Если в окне появилась строка, начинающаяся с символов `+OK`, то почтовый сервер доступен по протоколу POP3. Выполните команду меню **Отключить** и повторите описанные действия для порта 25. В окне должна появиться строка, начинающаяся с символов `220`. Если это так, то почтовый сервер доступен по протоколу SMTP.

Если сервер доступен, а почта не принимается или не отправляется, то дело в настройке почтового клиента.

Если сервер недоступен из программы telnet, то причина либо в настройке сервера (или он не запущен), либо в проблемах сети.

Пример настройки и тестирования сервера на одном компьютере

Предполагается, что вы ознакомились со всеми предыдущими разделами, поэтому изложение будет вестись в краткой форме.

- В свойствах сервера укажите локальный домен — `mydomain.ru`.

- ❒ В свойствах SMTP и POP3 проверьте, что протоколы разрешены и указаны порты `25` и `110`, соответственно.
- ❒ Создайте два почтовых ящика **user1** с паролем `123` и **user2** с паролем `234`.
- ❒ Запустите клиентскую почтовую программу (например, The Bat!).
- ❒ Создайте два почтовых ящика. В качестве адреса SMTP и POP3 сервера укажите `127.0.0.1` (или `localhost`, что то же самое), порты стандартные: `25` и `110`. Имена пользователей и пароли — такие же, как на сервере.
- ❒ Создайте сообщение от **user1** к **user2@mydomain.ru**. Отправьте его.
- ❒ Примите почту **user2** (возможно, нужно будет подождать несколько секунд, пока сообщение попадет в его почтовый ящик и станет доступно). Должно прийти ваше сообщение.
- ❒ Ответьте на него и отправьте ответ.
- ❒ Примите почту для **user1**. В случае возникновения проблем, проверьте все настройки, просмотрите файл журнала (см. п. "Эксплуатация сервера"). Возможно, потребуется повысить уровень подробности журнала для отдельных компонентов, чтобы детально разобраться в проблеме.

В текущей версии не все необязательные команды протокола POP3 поддерживаются сервером, что будет исправлено в будущих версиях. При использовании сервера, проверяйте соответствие вашей версии той, что предлагается на сайте разработчика.

Автор программы предлагает техническую поддержку по Email.

FTP-сервер

Значительный интерес для использования в сети может представлять FTP-сервер. Для тех, кто часто ищет файлы в Internet и перекачивает их, этот FTP-протокол не является "тайной за семью печатями". Множество FTP-клиентов можно найти как в Internet, 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. 4.21), который можно найти на сайте **www.jgaa.com**, или на сайтах, поддерживающих тему создания домашних сетей, например, на сайте **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.

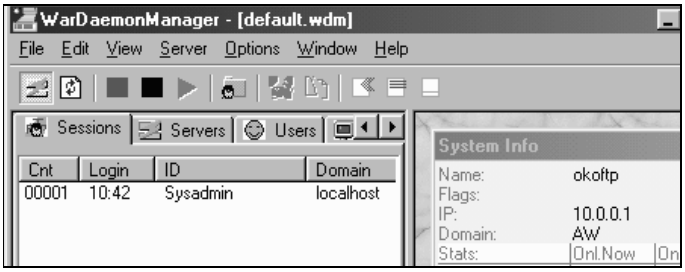

Рис. 4.21. Окно **WarDaemonManager**

Устанавливается сервер достаточно легко и может быть запущен как приложение, или как сервис. При этом он будет запускаться вместе 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.

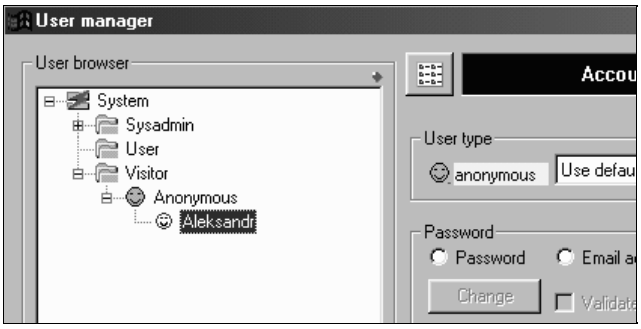

Рис. 4.22. Окно **User manager**

User manager (рис. 4.22) позволяет 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 актуаль-

но использование формата MDB (Microsoft Access входит в состав Microsoft Office Professional). Заготовка такой базы данных содержится в папке с установленной программой.

На просторах Internet можно найти и другие программы такого же назначения.

Например, ST FTP Service v1.5. Это простой FTP-сервер (рис. 4.23).

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).

Рис. 4.23. Диалоговое окно простого FTP-сервера

Сеть без кабеля

Наверняка многие знают или слышали о BBS — 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 Internet, 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 имеет возможность перекачать на свою машину (в пределах отведенного ему на это времени), а также забрать адресованную ему почту. Неоспоримое преимущество таких сетей перед Internet, это бесплатность, не считая платы за телефонное время, если она взимается. Конечно, в этом случае невозможна организация каких-либо выделенных каналов, online multimedia и игр по сети.

Но информацией можно обмениваться, "soft" 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 Internet, но в этом случае необходимо подключение к глобальной сети всех пользователей, участвующих в обмене информацией. Это возможно не всегда. В тоже время телефон на просторах нашей страны — явление более доступное, чем Internet.

Попробуем организовать регулярную связь между пользователями, имеющими телефон и модем, но не подключенными к Internet.

Программное обеспечение

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 нетрудно установить, имея дистрибутив Windows той версии, которая находится на компьютере.

Для этого надо открыть папку **Панель управления**, выбрать значок **Установка удаление программ**, перейти на вкладку **Установка Windows**, выбрать компонент **Связь**, нажать кнопку **Состав** и отметить флажок **HyperTerminal** (рис. 4.24).

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. 4.25.

Каждое подключение может быть сохранено со своей картинкой, выбор которой предоставлен при сохранении самой программой (рис. 4.26).

В рабочем окне (рис. 4.27) 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.

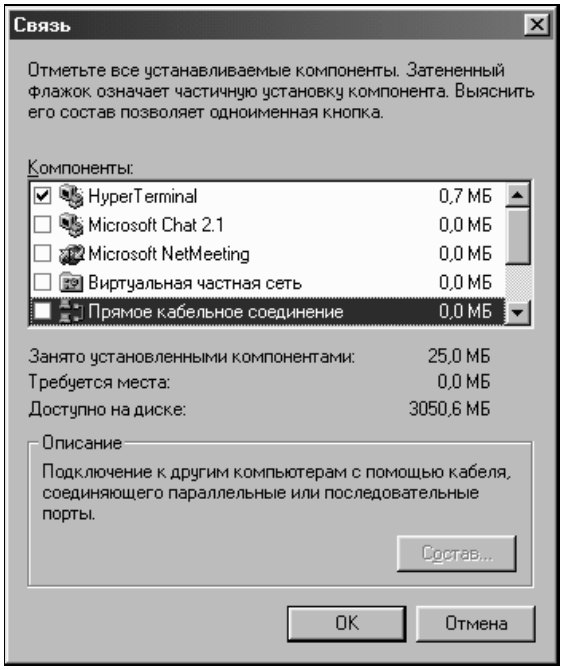

Рис. 4.24. Установка программы HyperTerminal

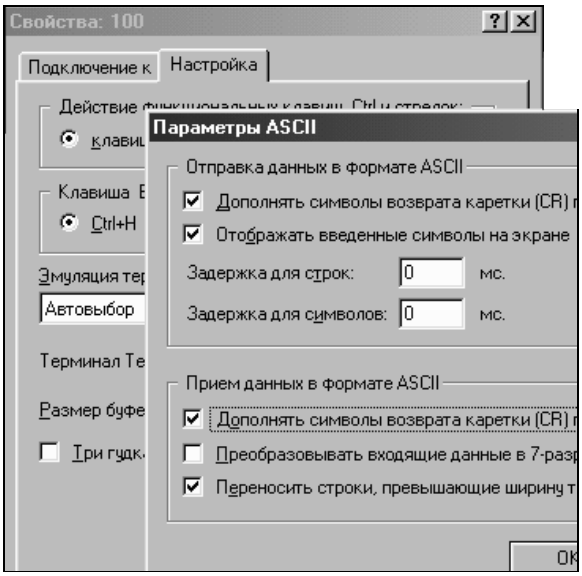

Рис. 4.25. Некоторые настройки программы HyperTerminal

Рис. 4.26. Внешний вид папки с программой и сохраненными подключениями

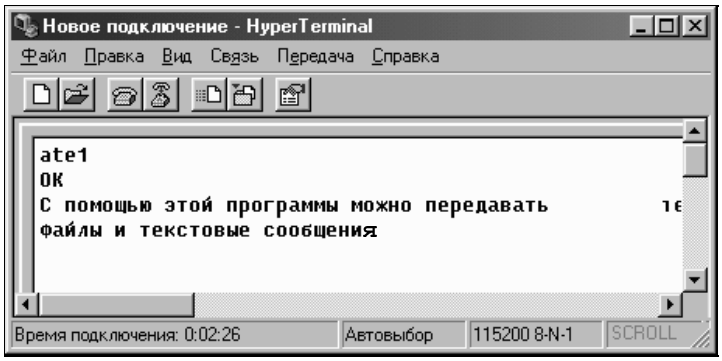

Рис. 4.27. Рабочее окно терминала

Во время запуска программы появляется заставка, приглашающая обновить текущую версию на более новую. Версия 6.3, которую можно получить бесплатно, позволяет использовать макросы (рис. 4.28), дающие возможность во время сеанса связи нажатием на одну-две клавиши вводить заранее заготовленные строки большой длины.

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 не вводятся команды модему. Возможно, что более удобным будет написание текста транслитерацией.

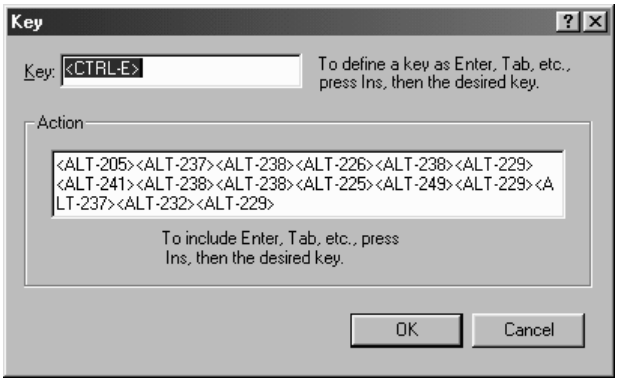

Рис. 4.28. Панель создания — модификации макроса в новой версии HyperTerminal

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 Internet), 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.

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 были 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** или **longsoft.raid.ru**. Второй адрес — персональная страница, автор которой готов рассмотреть ваши пожелания и скорректировать существующие или разработать новые программы в соответствии с вашими требованиями. Естественно, могут выполняться лишь разумные требования. Готовый АОН распространяется не бесплатно, хотя и не дорого.

Если нет хаба

Этот материал предназначен для случаев, 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. 4.29).

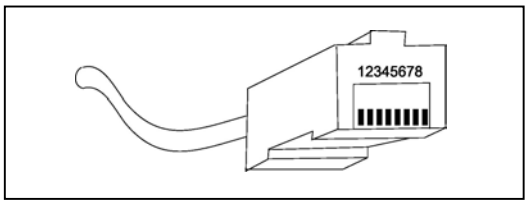

Рис. 4.29. Нумерация контактов

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 (монотонный небелый 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 его нет.

Полудуплексный режим функционирует так: когда карта передает информацию, пришедший на вход сигнал дает ей понять, что какая-то еще карта

решила передать информацию одновременно с нашей — возникла коллизия. В этом случае передача останавливается, и повторяется через некоторый случайный промежуток времени. Поскольку с большой вероятностью адаптеры начнут вторую попытку передачи в разное время, то запоздавшая с передачей сетевая карта "увидит", что началась передача другим адаптером, и будет принимать информацию, отложив передаваемую в свой буфер для 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 резисторный 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.

Теперь рассмотрим хаб на N компьютеров. В общем случае это такая схема, которая с точки зрения каждого из интерфейсов (входа и выхода для конкретной 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. 4.30).

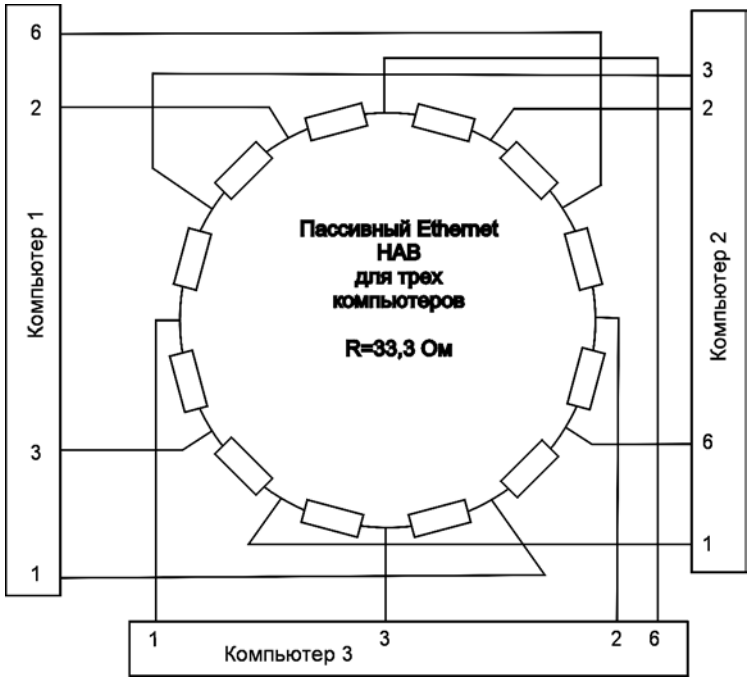

Рис. 4.30. Пассивный хаб для витой пары

Если нет сетевой карты

Решение было предложено еще в 1991 году Малым Научно-производственным предприятием "Интеллектуальные компьютерные системы" из г. Алма-Ата (автор С. Е. Заубекеров). Проект назывался "Локальная вычислительная сеть "ВИТАЯ ПАРА". Описываемая система требует MS-DOS 6.22.

Кто-то скажет, что это анахронизм, и теперь не серьезно использовать подобные технологии, но всякое бывает, да и не лишним будет узнать нестандартный вариант решения задачи, может, когда и пригодится.

Описание такой сети, основанное на оригинальном документе, приведено ниже.

Локальная вычислительная сеть "Витая пара" работает по обычной двухпроводной линии. В качестве линии может быть использована витая пара проводников, а также экранированный двухпроводный кабель или любая другая пара проводников. При этом компьютеры в сети подключаются по схеме "общая шина". Конфигурация сети может быть аналогичной той, которая приведена на рис. 4.31.

Рис. 4.31. Схема сети

Количество подключаемых компьютеров устанавливается при генерации и не может быть больше 26. Подключение осуществляется к последовательному порту через специальный разъем. Скорость приема/передачи выбирается при установке и может принимать значения: 600, 1200, 2400, 4800, 9600, 19 200, 38 400, 57 600 и 115 200 бит/с.

В сети нет выделенного компьютера, осуществляющего функции файл-сервера, все компьютеры равноправны и возможен обмен между любыми компьютерами сети. Сервис, предоставляемый пользователю, — это логические диски, связанные с диском конкретного компьютера. Количество логических дисков — пять. Исходное назначение логических дисков задается при запуске компьютера в файле config.sys, и в процессе работы они могут быть переназначены на любой другой диск любого компьютера. Пользователь может прочитать файл с любого диска любого компьютера сети (как флоппи-диска, так и с винчестера или виртуального диска), записать файл на любой компьютер или запустить на своем ПК задачу, хранящуюся на чужом компьютере. В сети могут работать всевозможные прикладные задачи (системы управления базами данных, электронные таблицы, редакторы и т. д.) безо всякой перенастройки. При этом пользователь сети в своих программах использует стандартные вызовы и функции операционной системы MS-DOS и может для разработки своих программ применять любые доступные языки программирования. Помимо стандартных вызовов в распоряжение пользователя предоставляется дополнительно сетевой интерфейс пользователя, дающий возможность использовать операции, специфичные для сети.

Установка сети

Для установки сети необходимо следующее:

- разъемы — по количеству компьютеров;
- файл TWP.BIN — для каждого компьютера сети свой;
- файл TWPINI.COM — для всех компьютеров сети один и тот же.

Разъемы должны быть выполнены конструктивно в одном корпусе с адаптерами по прилагаемой схеме (рис. 4.32).

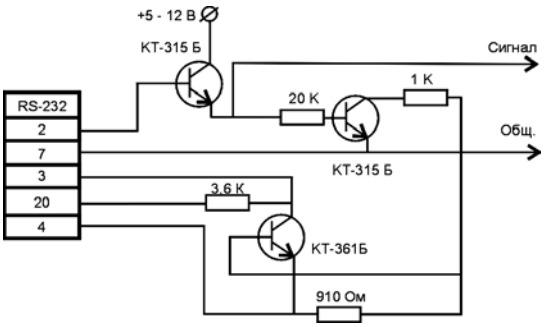

Рис. 4.32. Принципиальная схема адаптера

После монтажа кабеля и подключения разъемов на каждом компьютере сети необходимо проделать шаги, описанные ниже.

В файле config.sys необходимо добавить строку

```
DEVICE=<дисковод:\путь\>TWP.BIN ключи
```

где `<дисковод:\путь\>` означают месторасположение файла TWP.BIN, а под словом "ключи" понимаются следующие ключи:

- `/N` — ключ конфигурации сети (ОБЯЗАТЕЛЬНО!!!), который задает исходное соответствие пяти логических дисков физическим. Соответствие определяется пятью парами букв, разделенных запятыми, где первая буква соответствует компьютеру, а вторая — дисководу. Например, если указано:

  ```
  /NAC,BD,CC,DC,EC
  ```

  то это означает, что первый логический диск назначен на компьютер A, дисковод C, второй — на компьютер B, дисковод D, третий, четвертый и пятый соответственно на диск C компьютеров C, D и E.

  Имена логических дисков определяются относительным положением строки `DEVICE=TWP.BIN` в файле CONFIG.SYS среди других драйверов блочных устройств, подключенных к данному компьютеру. Например, пусть на компьютере имеются два флоппи-диска и один винчестер, а строка `DEVICE=TWP.BIN` — единственная, тогда имена физических и логических дисков будут: A и B для флоппи-дисков, C — для винчестера,

D, E, F, G и H — для сетевых дисков, каждый из которых назначен на конкретные диски компьютеров сети. Если же строка `DEVICE=TWP.BIN` не единственная, а, к примеру, перед ней стоит строка:

- `DEVICE=RAMDRIVE.SYS` (драйвер виртуального диска), то имена дисков в этом случае будут: A и B — для флоппи, C — винчестер, D — виртуальный диск, а E, F, G, H, I — сетевые;
- `/P` — ключ защиты. По этому ключу защищаются диски на своем компьютере.

  Ключ защиты задается в форме:

  `DN, DN,...`

  где `D` — защищаемый диск, а `N` — код защиты *см.* табл. 4.3.

Таблица 4.3. *Коды защиты*

Код защиты	Читать	Записывать
0	Можно	Нельзя
1	Можно	Нельзя
2	Нельзя	Можно

  Если задан ключ `PA0, B2, C1`, то это означает, что на диск A можно писать и читать, на диск B — нельзя ни писать, ни читать, а на диск C нельзя писать, но разрешено читать. Если какой-либо диск пропущен, то по умолчанию для него все разрешено;
- `/C` — ключ используемого порта. Может принимать значения от 1 до 4 и по умолчанию равен 1. Если это вас устраивает, ключ можно не указывать;
- `0/I` — ключ уровня прерывания для COM-порта. Может принимать любые свободные значения. Ниже приведены значения по умолчанию:
  - COM1 — IRQ4
  - COM2 — IRQ3
  - COM3 — IRQ4
  - COM4 — IRQ3
- `/B` — ключ, определяющий скорость приема/передачи. После ключа указывается значение выбранной скорости, которая может принимать значения: 115 200, 57 600, 38 400, 19 200, 9 600, 4 800, 2 400, 1 200, 600 бит/с.

  По умолчанию устанавливается максимальная скорость — 115 200 бит/с.

Кроме перечисленных ключей в одинарных кавычках можно указать имя компьютера — строку, состоящую не более чем из 20 символов, помогающую

идентифицировать компьютер в сети. Так, например, компьютеру, установленному в бухгалтерии, можно назначить имя компьютера "Бухгалтерия".

В файле autoexec.bat в любом месте необходимо вставить команду инициализации сетевого драйвера TWPINI.

Просмотр и изменение назначения логических дисков

В процессе работы возможно вы забудете имена логических дисков и их назначение. Чтобы посмотреть их, нажмите левые клавиши <Shift> и <Alt> и вы все увидите в появившемся окне. В этом же окне можно изменить текущие назначения дисков.

Работа в сети

Если вы используете Norton Commander, то просто перейдите на необходимый логический диск. После этого можете использовать все возможности Norton Commander для копирования, редактирования, запуска, переименования файлов и т. д.

Если же вы работаете на уровне командного процессора MS-DOS, то также перейдите на необходимый логический диск и после этого используйте любые команды DOS.

Необходимые файлы можно найти на сайте **http://icenet.boom.ru/index.htm** и еще нескольких сайтах, набрав в поисковой машине RAMBLER ключевое слово `twp.bin`.

Что мы теперь можем сделать?

Рассмотренный нами материал позволяет создавать сети комбинированной структуры, исходя из потребностей 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 Internet, устанавливать сетевые соединения, причем браузер, входящий в состав системы (к сожалению, не русифицирован), позволяет организовать рабочий стол, а для файлов использовать значки.

Попробуем, используя имеющиеся у нас возможности, составить эскизный проект сети, который вам не предложит ни одна компания (рис. 4.33), 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 Internet;

- пользователи 2, 3, 7 — территориально в пределах досягаемости кабельной сети;
- пользователи 4, 5 — возможен доступ по телефонной линии;
- пользователь 6 — удаленный доступ через Internet.

Рассмотрим средства связи, установленные на компьютерах пользователей (табл. 4.4).

Таблица 4.4. *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	+	–	–	+/–	+/–	+/–	+/–
Hyper-Terminal		+	+	+	+	–	–
Система	95/98	95/98	95/98	95/98	95/98	95/98	95/98
Windows							
Скорость связи с Пользователем 1	–	Высокая	Высокая	По расписанию. Низкая	По расписанию. Низкая	По расписанию. Высокая	Определяется портом
Постоянный IP-адрес	Со стороны Ehternet	+	+	+	+	–	–
NetBEUI		+	+	+	+		

"+" — желательно

"–" — не требуется

"+/–" — по желанию

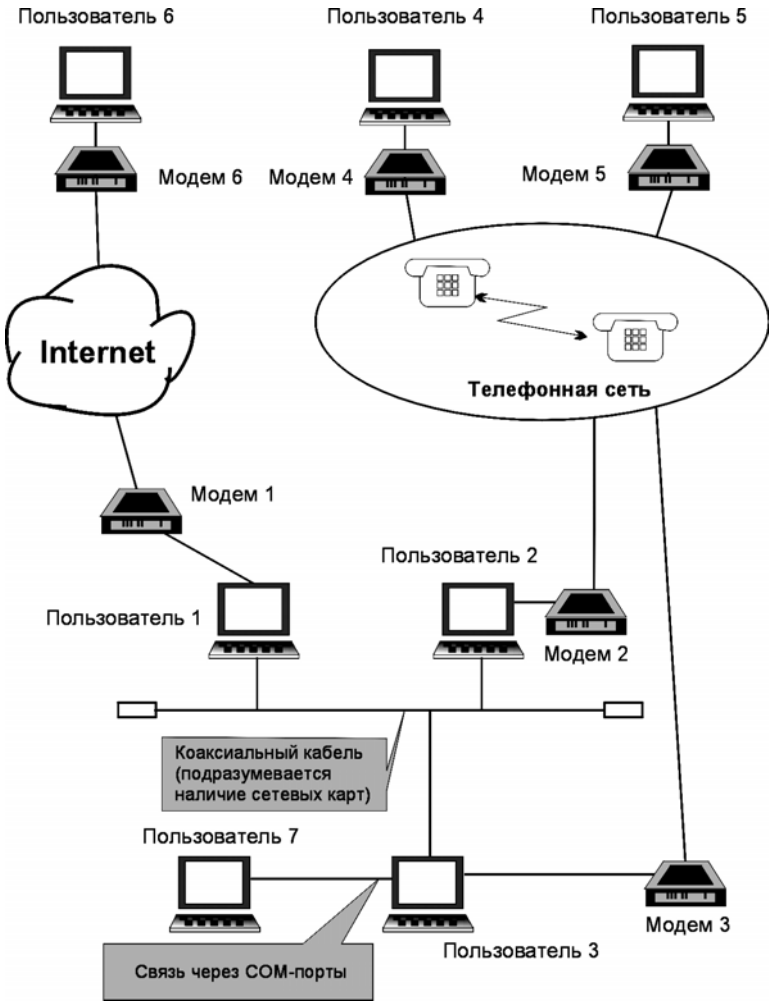

Рис. 4.33. Одна из возможных "композиций" на тему "Наша сеть"

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 Internet, 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 ресур-

сам 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 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, изображенный на рис. 4.33, выполнен на коаксиальном кабеле, но ничего не изменится с точки зрения функциональности сети, если применить витую пару. Поменяется только состав применяемого 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, могут применяться на предприятиях и в учреждениях, поскольку для этих случаев существуют определенные нормы, особенно для крупных организаций, связанные с совместимостью с другими сетями и высокой надежностью, требуют применения дорогостоящего оборудования. Но сети домашние, сети небольших офисов и предприятий, которые не входят в сети корпораций, вполне могут строиться на основе творческого подхода с применением нестандартных вариантов. Постепенная доводка сети и определение наиболее удобных и надежных решений приведут к результату, который по соотношению надежности, быстродействия и стоимости недостижим для стандартных сетей.

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 удалите файлы или соберите 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, пользуются 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 пользователей "виснут", они 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 директорий и несколько бесполезных файлов, разбросанных там и сям. Зараза уничтожила все труды пользователя, и не только его.

Я не придумал эту историю, она произошла три года 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.

Посещая время от времени архивы домашних сетей, доступ к которым возможен через Internet, я обнаруживаю и в некоторых из них зараженные файлы.

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. 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, файл(ы), который вы читали или создавали позже, и обязательно удалить шаблон Normal.dot. Шаблон будет восстановлен автоматически, а зараза будет удалена. Бывает, что недостаток памяти слабой машины пользователя 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 от лаборатории Касперского (**www.kaspersky.ru**).

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. (рис. 5.1).

Перед началом работы online-антивируса вас попросят ввести страну проживания и предупредят о том, что никакая персональная информация не будет передана с вашего компьютера, вам будут показаны результаты проверки и список обезвреженных вирусов. Само собой, сканирование и лечение может занять продолжительное время, и перед запуском online-антивируса оцените запасы времени вашего доступа к Internet.

На сайте **http://av-online.ru** предложат сканирование с помощью антивирусной программы Dr.Web.

В этом случае вы самостоятельно выбираете подозрительные файлы (рис. 5.2) для проверки.

Если у вас установлена версия антивирусной программы, которая поддерживает проверку сетевых дисков, 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 анти-

вируса, запуская его перед загрузкой Windows. Дольше происходит загрузка, но самозапускающиеся вирусы могут быть уничтожены перед началом работы.

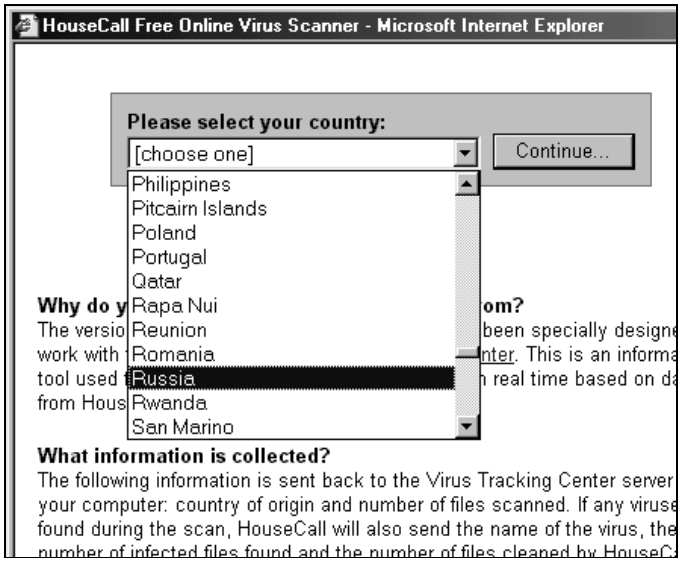

Рис. 5.1. Окно входа в программу Online-антивирусного сканера

Рис. 5.2. AV-Online проверяет выбранные вами файлы

Неплохо также использовать антивирусный монитор, который входит в большинство современных антивирусных пакетов. Такая программа-резидент будет стоять на страже и контролировать появление или обращение к зараженным файлам.

Чем чаще вы будете проверять на наличие вирусов ваш компьютер и машины пользователей сети, тем безопаснее будет ваша сетевая жизнь.

Интерфейс большинства антивирусных программ понятен, и многие программы имеют русские версии. В качестве примера приведем вид окна программы Dr.Web (рис. 5.3).

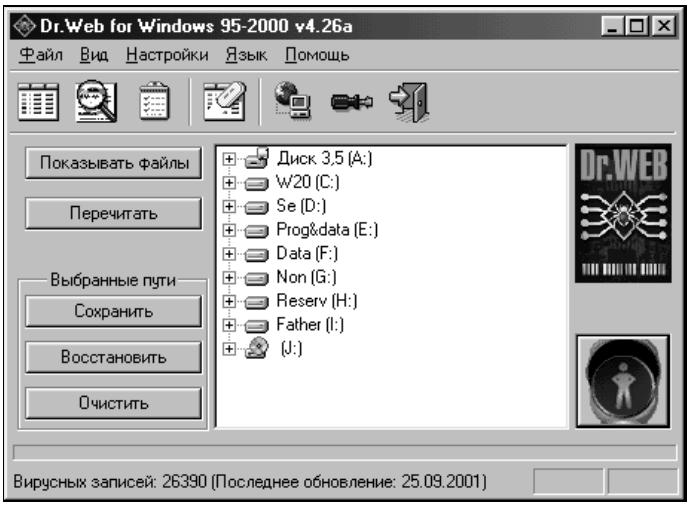

Рис. 5.3. Внешний вид окна антивирусной программы

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 Internet. 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 просто 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 вызвать ваше беспокойство и заставить провести проверку на вирусы.

Если ваш компьютер имеет непосредственный выход в Internet, то наличие на нем антивирусной программы обязательно, но не достаточно, 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 собой 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 на 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 мышки и выбрав команду **Settings** (Настройки), можно получить доступ ко всем настройкам программы (рис. 5.4).

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 **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.

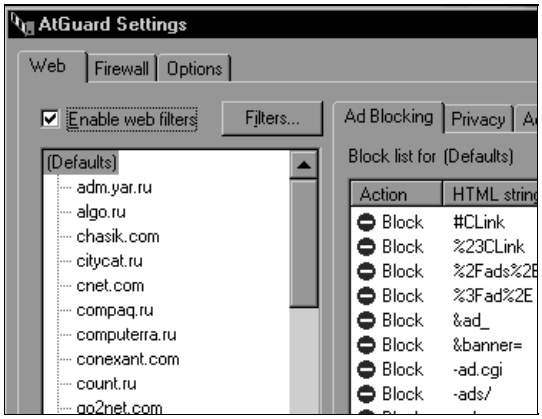

Рис. 5.4. Фрагмент окна программы AtGuard Settings 3.22

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 установите переключатель на **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** (Панель защиты). 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 настройки

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. 5.5). 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).

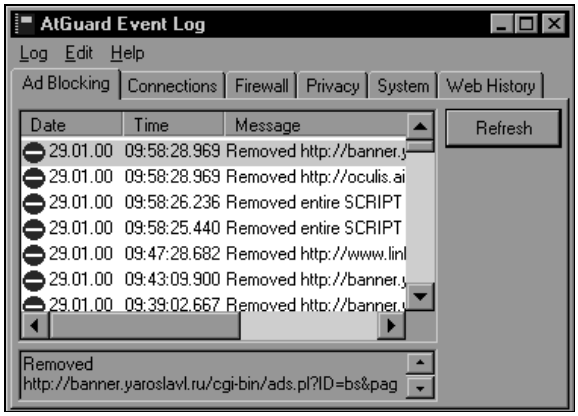

Рис. 5.5. Второй этап настройки

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. 5.6).

Точно также 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** (События).

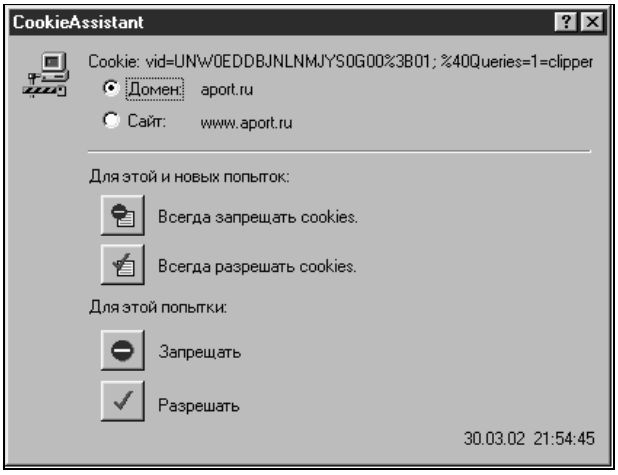

Рис. 5.6. Окно разрешения/запрещения правила соединений

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 Web-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 позволит 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.com. AtGuard — не единственная программа firewall. При желании можно найти программы других производителей, более простые, но помогающие защитить ваш компьютер от нежелательных контактов в Internet.

Для защиты от непрошеных страниц в Internet, можно использовать очень простую в использовании бесплатную программу NoAds с сайта **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 сети Internet — 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 вашего 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.

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 обеспечения более высокой степени надежности хранения информации. Суть S.M.A.R.T. заключается в том, что сам винчестер отслеживает состояние своей работоспособности и способен заранее предупредить пользователя о предаварийном состоянии. Пользователь компьютера, оснащенного S.M.A.R.T. HDD 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/стопных циклов, выполненых 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. HDD 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, верхние 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.

Для того чтобы получить расширенную информацию, дважды щелкните мышкой по значку S.M.A.R.T.-состояния. В раскрывшемся окне вы увидите таблицу представленных в системе HDD, состоящую из четырех столбцов (рис. 5.7):

1. **HDD** — место винчестера в системе: Primary/Master, Primary/Slave, Secondary/Master, Secondary/Slave.
2. **Model** — тип винчестера.
3. **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.

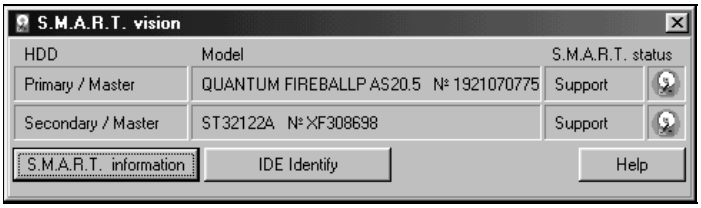

Рис. 5.7. Информация о HDD

4. **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 в 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. 5.8).

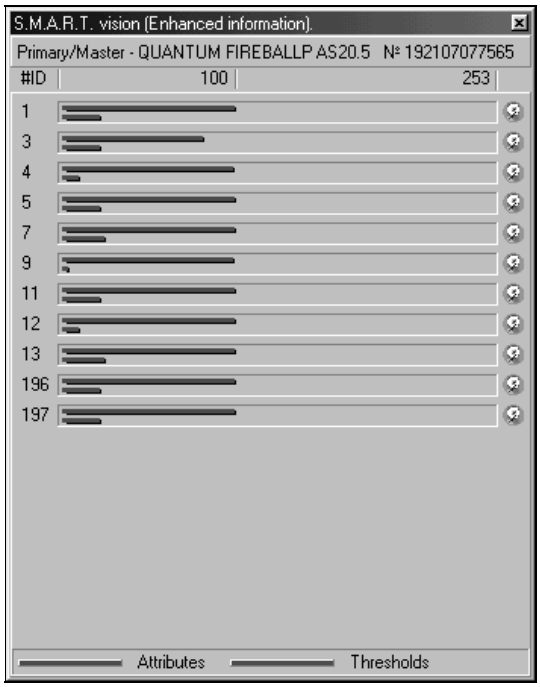

Рис. 5.8. Подробно о параметрах винчестера

На рис. 5.8 короткие индикаторные линии соответствуют пороговому значению параметров, а длинные — их действительному значению.

В настоящее время не все производители HDD предоставляют сведения о том, что характеризуют атрибуты надежности. Считается, что достаточно знать, не вышел ли какой из контролируемых атрибутов за установленные пределы.

Нажав на кнопку **IDE Identify**, можно получить подробную информацию о характеристиках HDD (паспорт диска), соответствующую спецификации ATA-4.

Для примера приведем паспорт QUANTUM FIREBALLP AS20.5 (табл. 5.2).

Таблица 5.2. *Паспорт диска*

Параметр	Значение
Интерфейс	ATA
Тип	Несъемное устройство и/или контроллер
Логических цилиндров	16383
Логических головок	16
Логических секторов в треке	63
Модель	QUANTUM FIREBALL P AS20.5
Серийный номер	192107077565
Версия микропрограммы	A1Y.1500
Количество байт, 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 (8 063 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
Multiword DMA Mode 2	Доступен, активный
Ultra DMA/33 Mode 0	Доступен
Ultra DMA/33 Mode 1	Доступен

Таблица 5.2 *(окончание)*

Параметр	Значение
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 выше адресу или на сайт **www.antivirus.ru**.

По последнему адресу находится компьютерная скорая помощь, которая восстанавливает информацию в режиме online, или выезжает на место. Консультации по восстановлению информации можно получить на сайте **http://okobox.narod.ru**.

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 продол-

жительное 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 Utilites 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 программе удалось создать. Пользователь имеет возможность сохранить на другом носителе все или часть найденных файлов. Имена директорий могут не соответствовать реальным, но файлы, содержащиеся в них, обычно восстанавливаются очень корректно.

Принцип работы программы не изменился, поэтому рассмотрим работу старой версии программы, которую часто еще можно встретить у "продвинутых" пользователей.

После запуска командой **Start Recovery**, Tiramisu довольно продолжительное время анализирует выбранный диск (рис. 5.9).

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. 5.10), 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 директорию и копируем на второй винчестер или дискету (рис. 5.11).

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 гигабайт (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. 5.9. Интерфейс программы Tiramisu

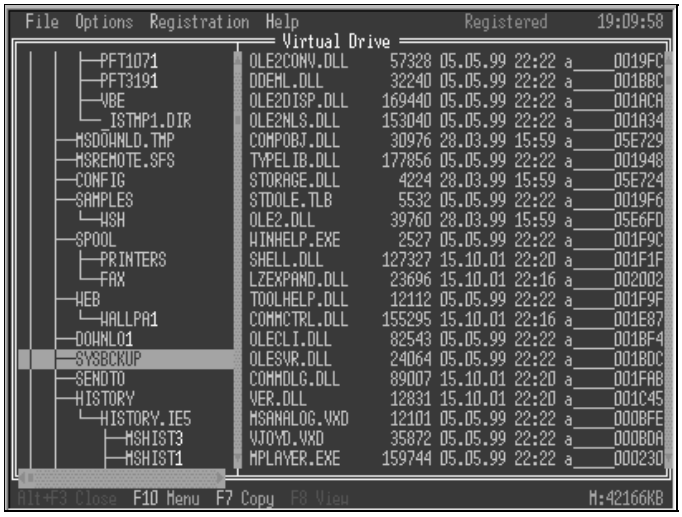

Рис. 5.10. Результат работы Tiramisu

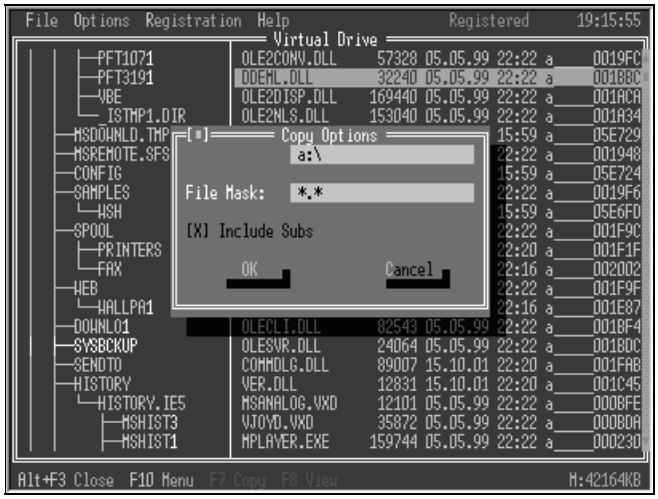

Рис. 5.11. Выбор диска — получателя копии восстановленного файла или файлов

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, когда 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 приводить его здесь. 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 к системе 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. Большая 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 широким кругом 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 расскажем немного ниже, 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 строчки, были доступны PTS-DOS 2000, с входящими в комплект командным процессором CP (рис. 5.12), поддержкой сети LOTLAN и Internet браузером Arachne. PTS-DOS 32 не комплектовалась ничем.

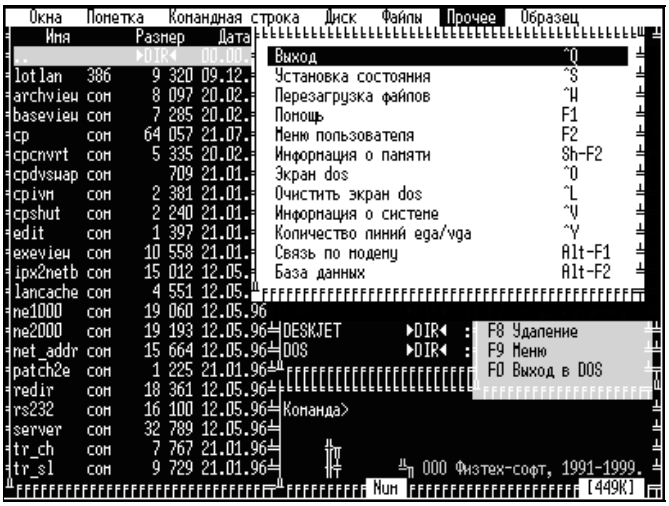

Рис. 5.12. Вид окна командного процессора в PTS-DOS

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. Он имеет в своем составе **Администратор Дисков** (в демо-версии отключен) и может заменить Diskedit из NU, PartitionMagic, 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 Internet, 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.

Возможно применение и других менее распространенных операционных систем. В Internet можно найти информацию даже о любительских разработках. 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. 5.13), которую можно скачать по адресу **www.5star-shareware.com/Homehob/Kids-Parenting/alot-nanny.html**.

После запуска программа начинает фиксировать все события, происходящие на машине, где она установлена, отмечая типы открываемых файлов, время их открытия, продолжительность процесса работы с ними. Вся информация сохраняется и может быть просмотрена в любой момент времени (рис. 5.14).

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.

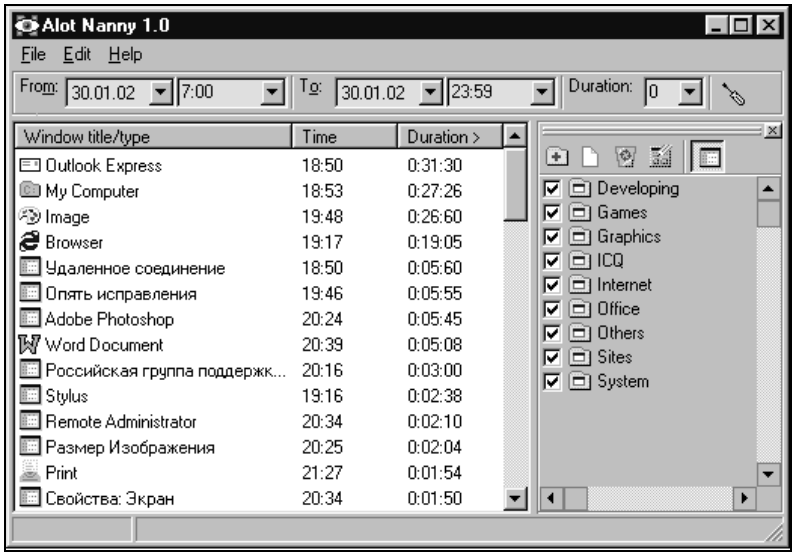

Рис. 5.13. Окно **Alot Nanny**

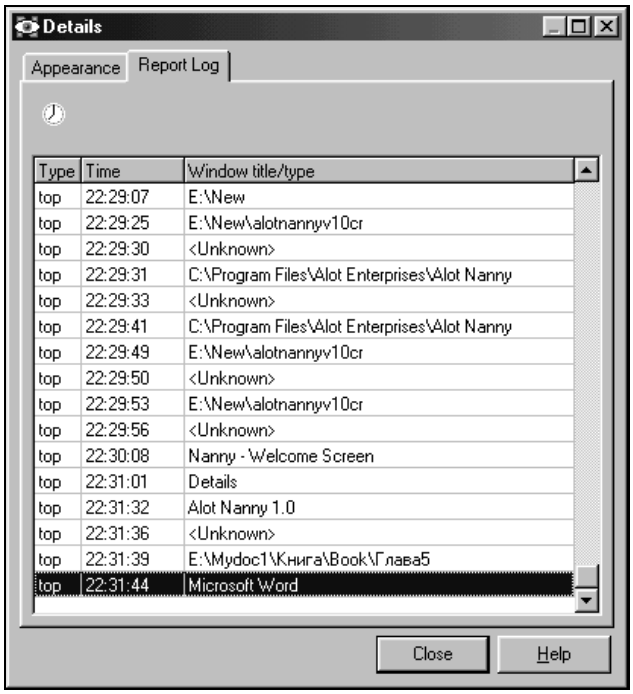

Рис. 5.14. Подробная информация о событиях в системе

Традиционные средства

Как и при работе на обычном ПК, работая в сети, необходимо быть готовым к устранению неполадок, которые возникают, как правило, неожиданно. Не обязательно неполадка приведет к разрушениям и потребует мер, рассмотренных выше. 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 обычная, предложенная Windows при установке, или созданная позже. Но можно создать и 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 ниже.

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 дисковый доктор NDD из комплекта NortonUtilites. Хорошо, если есть DOS-версии PartitionMagic v.5-7, Easy Recovery v.5 и выше, комплект архиваторов 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 соломку, хотя бы там, где можем упасть.

Как обезопасить себя от последствий некорректной работы новой программы или собственной ошибки? Такое средство есть.

Резервирование

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 готова 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 не большой, 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 Winrim.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 С 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 команд `winsec` или `winprim`, можно переходить из одной системы в другую. Такой вариант установки двух систем интересен тем, что будет использован один загрузчик, не требуется BootManager, 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, можно устанавливать программу в другую папку. Такая возможность обычно оставляется пользователю производителями 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.

Ну, вот и все

Организация сети в любом из возможных вариантов требует как от руководителя, так и от исполнителя творческого подхода. Надеюсь, что информация, приведенная в книге, поможет 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 появления новых пользователей и 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 большую 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 Internet и других сетях. Ссылки на адреса в Internet, приведенные в книге, были действующими на момент сдачи рукописи. Возможно, что теперь что-то изменилось (Internet быстро меняется). Большую помощь вам окажет поисковая система **www.google.ru,** которая на момент написания книги была, пожалуй, лучшей русскоязычной поисковой системой.

В заключение приведем статью, найденную в Internet (**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 Internet. 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 Internet. 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 Internet 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 Internet.

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 достаточное 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 Internet 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 немного, желающие еще не разбежались, и можно приступать.

Протянуть магистраль, создать серверную, настроить оборудование, вдохнуть в него жизнь, а точнее, Internet... 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

И, уж совсем на прощание...

Технологии передачи данных постоянно совершенствуются. В последнее время появляется все больше сообщений об организации передачи данных через электросеть.

"Германская компания MVV планирует запустить принципиально новый технологический проект, который позволит обеспечить жилые дома высокоскоростной связью через обычную сеть электропитаниия. Новая технология, которую MVV разрабатывает совместно с израильской Main.net, позволит передавать через электросеть как аналоговые, так и цифровые данные" — сообщает ABC News.

"Австрийская электротехническая компания EVN после завершения полевых испытаний получила разрешение на дальнейшее развитие технологии Powerline, обеспечивающей пользователям доступ в Internet через бытовую электросеть, без использования телефонных линий.. Цены на такое "электроподключение к Internet", по-видимому, будут очень низкими и постоянными, независящими от времени использования" — сообщает Yahoo!Actualites.

"РАО "ЕЭС России" хочет начать предоставлять доступ в Internet, используя свои электрические сети." О планах РАО "ЕЭС России" сообщил ресурс "Интернет и Инвестиции"

"Компания Linksys **http://www.linksys.com** объявила о выпуске устройств связи по электрическим сетям с использованием технологии HomePlug v1.0, со скоростью передачи до 14 Мбит/с. Среди объявленных устройств роутер Instant PowerLine EtherFast 10/100 Router (PLERT10), мост Instant PowerLine EtherFast 10/100 Bridge (PLEBR10) и адаптер Instant PowerLine USB Adapter (PLUSB10). Все они построены на основе чипсета, разработанного компанией **http://www.intellon.com**. Окончательная спецификация технологии HomePlug 1.0 была опубликована летом 2001 г., и сразу же после этого компания Intellon **http://www.intellon.com** объявила о выпуске чипсета, который полностью соответствует спецификации. Особенностями технологии являются скорость передачи до 14 Мбит/с и метод доступа к среде передачи по протоколу CMSA/CA (множественный случайный доступ с контролем несущей и разрешением коллизий), который используется также и в беспроводных сетях стандарта 802.11. Подробнее о технологии HomePlug можно прочитать на сайте **http://www.homeplug.org** и на сайте компании **http://www.intellon.com**."

Это выдержки из сообщений, которые появлялись в прошлом (2001) году. Иногда можно встретить и любительские разработки на эту тему. Но будьте осторожны! Любительские разработки делаются энтузиастами "под себя", они применяют свои системы на свой страх и риск. Работа с электросетью сопряжена с определенным риском как для вашего компьютера, так и для вашей жизни.

Познакомиться с информацией из области альтернативных методов подключения к компьютерным сетям можно на сайте **http://aic.eltrast.ru/index.html**.

Успехов вам!

С автором можно связаться по e-mail **braginsky@comail.ru**. На сайте **okobox.narod.ru** есть страница поддержки книги, где можно найти ответы на часто задаваемые вопросы.

Предметный указатель