



НАСТРАИВАЕМ СЕТЬ

СВОИМИ руками

- сетевое оборудование
- утилиты диагностики
- настройка сетевых соединений
- защита от вторжений из сети
- общение в реальном режиме

С.В. Глушаков, Т.С. Хачиров

НАСТРАИВАЕМ СЕТЬ своими руками

аст
ИЗДАТЕЛЬСТВО
МОСКВА
Фолио
Харьков

Введение

В настоящее время практически в каждом доме можно увидеть компьютер – он стал неотъемлемой частью нашей жизни. Компьютер используется для решения задач различного рода – помогает школьникам и студентам в учебе, используется родителями как рабочий инструмент. Кроме этого, компьютер в доме чаще всего является центром развлечений, поскольку, по желанию пользователя, может выступать в роли игровой приставки, музыкального центра или DVD-проигрывателя.

Но даже самый производительный компьютер будет не интересен, если на нем не будет установлено необходимое программное обеспечение (например, игры или офисный пакет), не будут храниться музыкальные произведения и видеофильмы. Конечно, можно каждую неделю (день, месяц – на выбор) покупать новые компакт и DVD-диски, однако это может существенно сказаться на бюджете. Другим вариантом является взятие дисков во временное пользование, но и эта процедура не очень удобна.

Компьютерная сеть, то есть соединение нескольких компьютеров между собой при помощи сетевых кабелей, позволяет передавать информацию от одного компьютера к другому с очень большой скоростью и без необходимости использования каких-либо носителей информации.

Кроме того, уже сейчас нередка ситуация, когда жители одного дома объединяют свои компьютеры в локальную сеть, а затем подключают ее к глобальной сети Internet. Это дает большие преимущества, так как пользователи могут обмениваться друг с другом различными файлами, общаться в реальном режиме времени, играть и т.д.

В первой главе данной книги дается описание наиболее популярной и распространенной технологии Fast Ethernet – от общей теории (без которой, к сожалению, не обойтись) до чисто практических вопросов, связанных с оборудованием.

Вторая и третья главы посвящены теоретическим аспектам, а также вопросам, связанным с настройкой сетевого обо-

рудования, установкой драйверов и конфигурированием протокола TCP/IP.

Четвертая глава рассказывает о роли файловых серверов в сети. Описываются процессы предоставления общего доступа к файлам и папкам, настройки прав доступа и мониторинга подключений.

В пятой главе описываются программы, применяющиеся для общения в локальной сети, – Network Assistant и Courier Mail Server.

Данная книга создана на основе учебного курса, разработанного преподавателями Харьковского института информационных технологий. Мы будем рады вашим отзывам и приглашаем вас к сотрудничеству в области обучения.

Контактные телефоны: (057) 732-28-72, (057) 771-45-18

Адрес: г. Харьков, 61050, переулок Фейербаха, 1/3

E-mail: info@xiit.kharkov.ua

ХАРЬКОВСКИЙ ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ



Предлагает платное **ДИСТАНЦИОННОЕ ОБУЧЕНИЕ** специализированным курсам в области информационных технологий по следующим сериям:

для ПОЛЬЗОВАТЕЛЯ	для СПЕЦИАЛИСТА	для ПРОГРАММИСТА
Windows 2000	Photoshop 6	Delphi 6
Word 2000	CorelDRAW 10	Visual Basic 6
Excel 2000	PageMaker 6.52	Visual C++ 6
Access 2000	MathCAD 2000	Java 2
Visio 2000	AutoCAD 2000	C++

За более подробной информацией следует обращаться:

Телефоны: (057) 732-28-72, (057) 771-45-18

E-mail: info@xiit.kharkov.ua

www.EDDI.ru

Глава 1

Как объединить компьютеры в сеть

Для начала – немного теории, поскольку без нее вам трудно будет понять ту практическую часть, которая описана в книге.

Сетевой технологией называется согласованный набор стандартных протоколов (правил передачи данных) и реализующих их программно-аппаратных средств (таких как сетевые адаптеры, драйверы, кабели и др.), достаточный для построения вычислительной сети.

На заре развития компьютерных сетей, в том числе и локальных, существовало довольно большое количество технологий, позволяющих объединить компьютеры между собой. Каждая из них разрабатывалась под конкретные задачи, например обеспечение взаимодействия группы ученых или передача потокового аудио- и видеосигнала на большие расстояния. Однако из-за своей специфики стоимость разворачивания сети была очень высокой. Единственной технологией, которая могла конкурировать с остальными, была *Ethernet*, которая благодаря своей дешевизне, простоте в монтаже и настройке к настоящему времени вытеснила все остальные технологии. Сейчас применяются две модификации *Ethernet* – *Fast Ethernet* и *Gigabit Ethernet*.

Топологии сетей

Перед знакомством с принципами работы технологии *Ethernet* давайте разберемся со способами соединения компьютеров. Схема физического соединения компьютеров называется *топологией сети*. Существуют следующие основные типы сетевой топологии – *общая шина*, *звезда* и *кольцо*.

ЗВЕЗДА

Наиболее функциональной и стабильной на сегодняшний день является локальная вычислительная сеть (ЛВС, LAN – Local Area Network), имеющая топологию «Звезда» (см. рис. 1), при использовании которой каждый компьютер сети подключается к особому устройству, называемому *концентратором* (*hub*) или *коммутатором* (*switch*). Преимуществом этой топологии является ее устойчивость к повреждениям кабеля – при

Глава 1

Как объединить компьютеры в сеть

Для начала – немного теории, поскольку без нее вам трудно будет понять ту практическую часть, которая описана в книге.

Сетевой технологией называется согласованный набор стандартных протоколов (правил передачи данных) и реализующих их программно-аппаратных средств (таких как сетевые адаптеры, драйверы, кабели и др.), достаточный для построения вычислительной сети.

На заре развития компьютерных сетей, в том числе и локальных, существовало довольно большое количество технологий, позволяющих объединить компьютеры между собой. Каждая из них разрабатывалась под конкретные задачи, например обеспечение взаимодействия группы ученых или передача потокового аудио- и видеосигнала на большие расстояния. Однако из-за своей специфики стоимость разворачивания сети была очень высокой. Единственной технологией, которая могла конкурировать с остальными, была *Ethernet*, которая благодаря своей дешевизне, простоте в монтаже и настройке к настоящему времени вытеснила все остальные технологии. Сейчас применяются две модификации Ethernet – *Fast Ethernet* и *Gigabit Ethernet*.

Топологии сетей

Перед знакомством с принципами работы технологии Ethernet давайте разберемся со способами соединения компьютеров. Схема физического соединения компьютеров называется *топологией сети*. Существуют следующие основные типы сетевой топологии – *общая шина*, *звезда* и *кольцо*.

ЗВЕЗДА

Наиболее функциональной и стабильной на сегодняшний день является локальная вычислительная сеть (ЛВС, LAN – Local Area Network), имеющая топологию «Звезда» (см. рис. 1), при использовании которой каждый компьютер сети подключается к особому устройству, называемому *концентратором (hub)* или *коммутатором (switch)*. Преимуществом этой топологии является ее устойчивость к повреждениям кабеля – при

обрыве одного соединяющего кабеля (сегмента сети) перестанет работать только один из элементов сети и поиск повреждения значительно упрощается. Кроме этого, данная топология позволяет производить расширение сети, при котором не затрагивается текущая структура. Например, для добавления или соединения двух сетей достаточно соединить одним кабелем коммутаторы (при этом используется метод каскадирования, см. ниже).

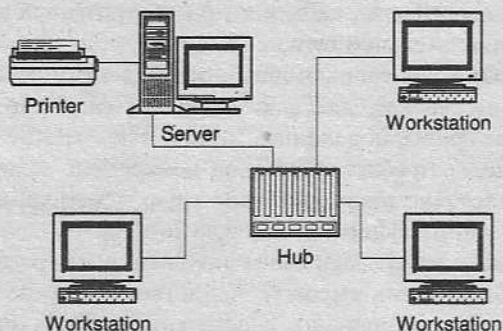


Рис. 1. ЛВС с топологией «Звезда»

ОБЩАЯ ШИНА

При использовании топологии с общей шиной (см. рис. 2) компьютеры соединяются в одну линию, по концам которой устанавливаются терминаторы – специальные сопротивления.

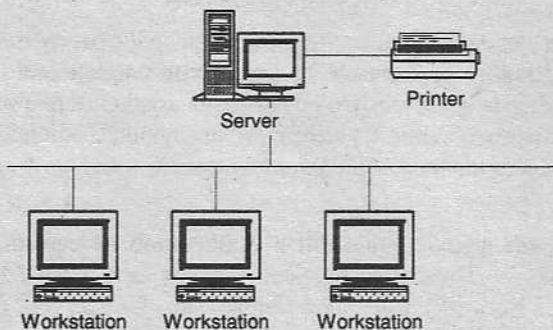


Рис. 2. ЛВС с топологией «Общая шина»

Преимущества такого построения ЛВС заключаются в простоте организации сети. Недостатком является низкая устойчи-

вость к повреждениям – при любом повреждении кабеля вся сеть перестает работать, а поиск неисправности представляется затруднительным.

КОЛЬЦО

При такой топологии узлы сети образуют кольцо, т.е. концы кабеля соединены друг с другом (см. рис. 3). Каждый узел сети соединен с двумя соседними. Преимуществом кольцевой топологии является ее достаточно высокая надежность, получаемая за счет избыточности сети. Однако стоимость такой ЛВС высока за счет расходов на адаптеры, кабели и дополнительные приспособления, обеспечивающие работу сети.

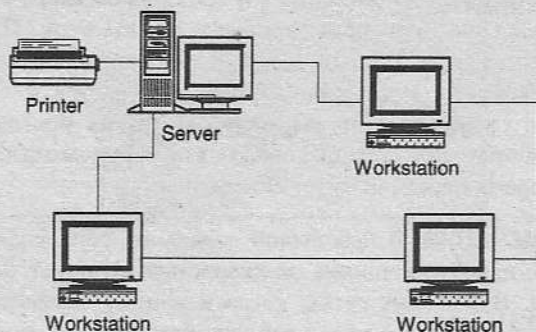


Рис. 3. ЛВС с топологией «Кольцо»

В настоящее время для построения локальных сетей, в том числе и домашних, используется топология «Звезда», поскольку она заложена в основу технологии *Fast Ethernet*, которая обеспечивает высокую надежность и быстрый обмен информацией. Две другие топологии используются или в очень старых сетях, или в каких-либо исключительных ситуациях.

Скорость передачи данных в сети

Для измерения быстродействия сети в технике введена специальная величина – *бит в секунду*. Так как один байт информации состоит из восьми бит, то для того, чтобы определить, сколько байт в секунду теоретически способна пропустить ЛВС, необходимо величину быстродействия сети разделить на восемь. Например, обычное быстродействие сети *Fast*

Ethernet равно 100 Мбит/с, тогда путем деления скорости 100 Мбит/с на 8 определяем, что сеть способна передать 12.5 МБайт данных за 1 секунду.

Однако на практике максимальное быстродействие сети никогда не реализуется. Это связано, например, с тем, что фактически ЛВС не может работать быстрее, чем самая медленная ее составляющая. Например, если осуществляется передача данных от дискового накопителя одного компьютера к другому, то затраченное время будет включать в себя не только собственно время на передачу данных. Сюда войдет и время чтения этих данных с диска компьютера, время на оперирование данными в компьютере и время на обработку данных и их запись на диск принимающего компьютера. При этом скорость передачи данных дискового накопителя будет определять скорость, с которой данные передаются к сетевому адаптеру. С другой стороны, запросы других пользователей ЛВС, работающих параллельно, будут чередоваться, и суммарное время передачи будет еще больше.

► **ПРИМЕЧАНИЕ.** В небольшой локальной сети, содержащей до 30 компьютеров, погоня за скоростью не имеет большого значения. В больших сетях, когда к одному магистральному кабелю присоединено много рабочих станций, быстродействие и пропускная способность становятся важными факторами.

В свою очередь, быстродействие зависит и от протокола передачи данных. Каждая сеть должна строиться по определенным правилам – протоколам – при передаче данных от одного компьютера к другому. *Протокол* определяет способ доступа узла сети (т.е. компьютера) к передающей среде (кабелю) и способ передачи информации от одного узла к другому. Наконец, скорость и качество работы сети зависит от оборудования, на котором она построена.

Что вам потребуется

СЕТЕВЫЕ КАРТЫ

Сетевая карта, или сетевой адаптер (см. рис. 4), предназначена для непосредственного соединения сетевого кабеля с компьютером. Очевидно, что сетевые адаптеры и кабели являются аппаратной основой организации локальной сети и их

нормальная работа жизненно важна для сети. Функцией сетевого адаптера является передача и прием сигналов из кабеля. При передаче адаптер воспринимает команды и данные от операционной системы, преобразует эту информацию в один из стандартных форматов и передает ее в сеть через подключенный к адаптеру кабель. При приеме происходят аналогичные действия, только в обратном порядке.

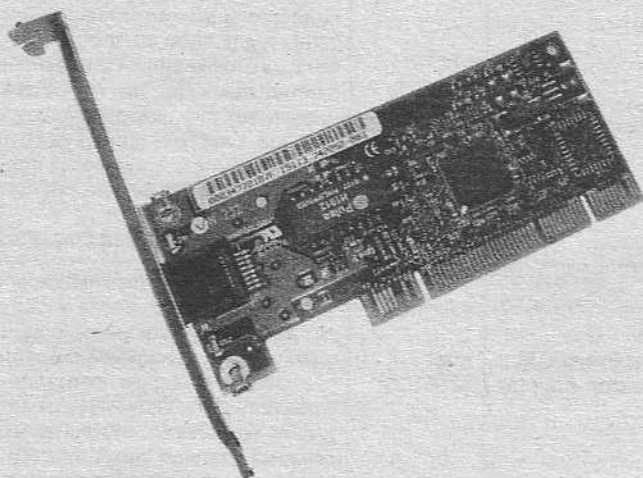


Рис. 4. Внешний вид сетевого адаптера Intel InBusiness PRO/100+

► **ПРИМЕЧАНИЕ.** В каждом компьютере, который является частью ЛВС, должен быть установлен сетевой адаптер, обеспечивающий подключение к выбранному типу кабеля.

В качестве примера приведем характеристики распространенных и хорошо себя зарекомендовавших сетевых адаптеров (см. табл. 1).

Таблица 1
Характеристики некоторых сетевых адаптеров

Наименование	Чип	Комментарий
D-Link DFE-528TX	D-Link DL10038C	Максимальная длина рабочей линии (сегмента) 400 м, P'n'P, прекрасно работает на длинных сегментах

Наименование	Чип	Комментарий
D-Link DFE-550TX	D-Link DL10050B	Хорошо выполненный чип, но без механизма адаптации к условиям конкретного кабельного окружения. Поддержка Full-duplex и очень низкая загрузка CPU
3Com 3C905CX-TX-M	3Com 920-ST06	На данной плате расположен чип, поддерживающий технологии адаптации к условиям конкретного кабельного окружения. По сравнению с остальными картами имеет самую низкую загрузку центрального процессора. Скорость передачи 10 или 100 Мбит/с, поддерживается полнодуплексная связь, есть светодиодные индикаторы для 10/100 Мбит/с, Plug and Play (P'n'P)
Intel Pro/100 M Desktop Adapter	Intel 82551QM	Автоматическая настройка скорости 10 или 100 Мбит/с обеспечивает автоматическое соединение на максимально возможной скорости, что повышает общую производительность сети. Применяется адаптивная технология, неустойчивая связь на длинных сегментах, P'n'P
InBusiness PRO/100+	Intel GD82559	Наиболее подходящая сетевая карта для рабочей станции начального уровня. Отличная поддержка режима Full-duplex и невысокая загрузка CPU. Низкая стоимость
LG LNIC-10/100Aw Planet ENW-9504 Surecom EP-320X-R	Realtek RTL8139D	Карты, построенные на этом чипсете, принадлежат бюджетному сегменту рынка и стоят очень дешево. Конечно, этот факт сказывается на их работе. Нестабильная работа в полнодуплексном режиме и большая загрузка центрального процессора не позволяют получить хорошие скоростные показатели
CompuShack Fastline II PCI UTP DEC-Chip Lantech Fast-Link/TX	Intel (DEC) 21143-PD	Старый чипсет. Высокая загрузка процессора, отсутствие поддержки режима Full Duplex. В сетях на основе концентраторов карты могут применяться, в противном случае их лучше не использовать

Конечно же, при выборе адаптера большое значение имеет тип используемого кабеля. Кроме того, каждый адаптер, устанавливаемый в компьютер, должен нормально работать с остальными устройствами компьютера, например с материнской платой.

СЕТЕВОЙ КАБЕЛЬ

Основой любой ЛВС является сетевой кабель, который обеспечивает канал связи компьютера с остальными компьютерами сети. В настоящее время в основном используются типы кабеля *витая пара* и *оптоволокно*, однако до сих пор встречаются сети, построенные с использованием *коаксиального кабеля*.

Кабель витая пара (см. рис. 5) содержит четыре пары проводов, скрученных один с другим по всей длине кабеля. Скручивание позволяет повысить помехоустойчивость кабеля и снизить влияние каждой пары на все остальные. Кроме этого, для повышения помехозащищенности был разработан *экранированный кабель*, проводники которого кроме внешней изоляции также заключены в оболочку из фольги, которая отражает магнитные помехи.

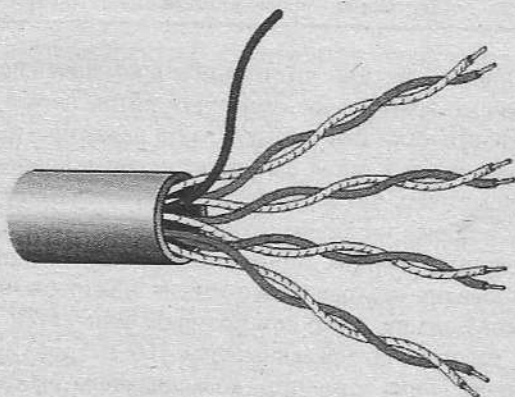


Рис. 5. Сечение кабеля витая пара

Следует иметь в виду, что из четырех скрученных пар в сетях, удовлетворяющих спецификациям 10BASE-T и 100Base-TX (см. ниже), используются только 4 проводника (т.е. 2 пары), а максимальная длина сегмента не может превышать 100 метров. Кабель разделен на классы, причем наиболее качественной

считается витая пара 5 класса (категории). Для соединения кабеля с компьютером или концентратором используется разъем типа *RJ-45*, внешний вид которого показан на рис. 6.

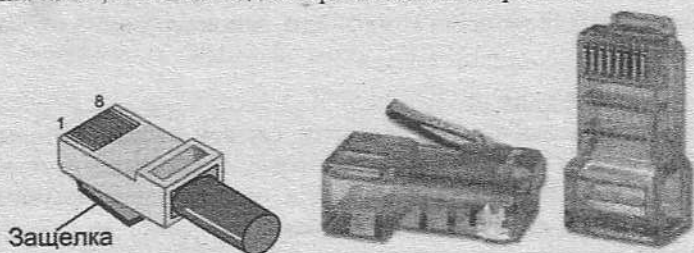


Рис. 6. Коннектор RJ-45

Таблица 2

Характеристики кабеля витая пара

Наименование	Стандарт разъема	Длина сегмента	Число витых пар
100Base-TX	RJ-45	100 м	2
100Base-T4	RJ-45	100 м	4

Необходимо отметить, что стоимость коаксиального кабеля в настоящее время выше стоимости витой пары (да и купить его практически невозможно), а по надежности и скорости передачи данных витая пара выигрывает у коаксиального кабеля. Кроме того, витая пара позволяет сделать сеть более надежной, а обрыв на линии легко локализуется и не влияет на работу других рабочих станций. Единственным оправданием использования коаксиального кабеля может быть необходимость соединения двух компьютеров или сетей, находящихся на расстоянии, превышающем 100 метров, поскольку максимальная длина «тонкого» коаксиального кабеля достигает 180 метров, а «толстого» – 500 метров. И все же оборудование для использования коаксиального кабеля купить сейчас практически невозможно.

КОНЦЕНТРАТОР

Концентратор (hub), или *репитер (repeater)* (см. рис. 7), представляет собой устройство, предназначенное для соеди-

нения компьютеров при использовании топологии «Звезда». Концентратор является узловой точкой сети, к которой подключаются компьютеры и периферийные устройства с сетевым интерфейсом. Кроме этого, при передаче данных он усиливает сигнал, что позволяет увеличить длину сегмента.

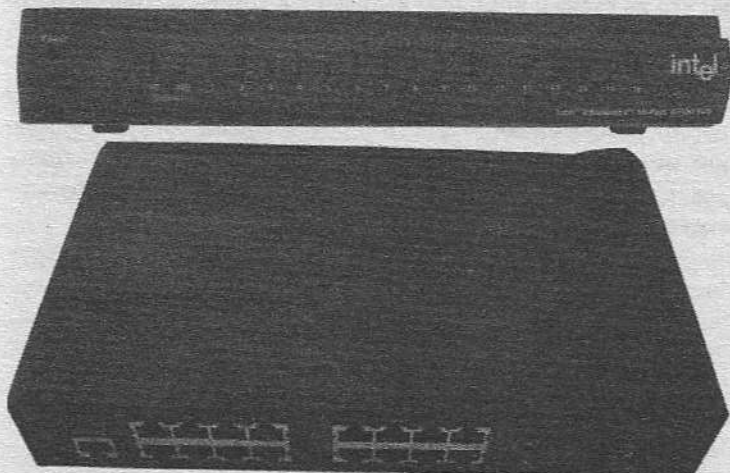


Рис. 7. Внешний вид сетевого концентратора Intel

При построении сетей важными факторами в выборе концентратора являются его стоимость, длина рабочего сегмента, надежность и универсальность. Концентраторы соединяют сегменты, использующие одинаковые или разные типы носителя; восстанавливают сигнал, увеличивая дальность передачи; передают данные в обоих направлениях. Таким образом, концентраторы – самый дешевый способ расширить сеть, построенную с использованием коаксиального кабеля или витой пары. Концентраторы расширяют возможности сети, разделяя ее на сегменты, уменьшая тем самым количество компьютеров на один сегмент. У этих устройств состояние активности сети легко наблюдать с помощью световых индикаторов, которыми, как правило, снабжен каждый порт. Кроме того, часто присутствуют индикаторы для отображения информации о передаче *неверных пакетов (jabber)* и о возникновении в сети *коллизии (collision)* (см. ниже).

При выборе места для установки концентратора в целях уменьшения длин сегментов сети целесообразно расположить

его вблизи геометрического центра сети. Такое расположение позволит минимизировать расход кабеля, причем длина кабеля от концентратора до любого из подключаемых к сети компьютеров или периферийных устройств не должна превышать 100 метров. Чаще всего концентратор ставят на стол или закрепляют его на стене с помощью входящих в комплект концентратора скоб. При планировании сети не забудьте о возможности наращивания (каскадирования) концентраторов путем соединения их в одном месте по несколько устройств с использованием портов расширения (см. рис. 8). В этом случае обратите внимание на возможность подвода электропитания для концентраторов, а также на тот факт, что расстояние между каскадируемыми концентраторами не должно превышать 5 метров.

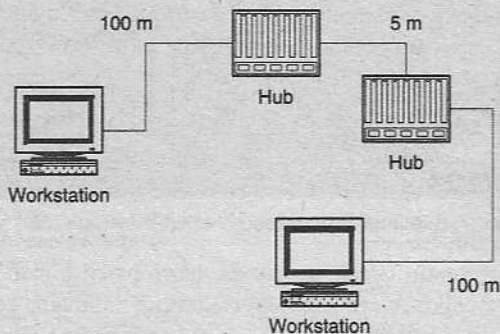


Рис. 8. Правила каскадирования сетевых концентраторов

Концентраторы позволяют использовать для объединения компьютеров в сеть стандартный кабель на основе скрученных пар медных проводников – так называемой витой пары (см. выше). Для таких соединений предусмотрен стандарт 10BaseT, обеспечивающий полную совместимость с сетевым оборудованием разных фирм и позволяющий организовать сеть на базе недорогих и простых в установке кабелей и разъемов. Для подключения устройств к сети используются модульные разъемы типа RJ-45.

КОММУТАТОР

Коммутатор (switch) является технически более сложным устройством, чем концентратор.

Основным недостатком концентратора является тот факт, что при получении сигнала от какого-либо компьютера он усиливает его и передает на все остальные порты, тем самым создавая лишний трафик (поток информации), поскольку чаще всего передаваемый сигнал предназначен только для одного компьютера.

Коммутаторы позволяют направить поступивший в них сигнал только в тот порт, к которому подключен требуемый компьютер. Другими словами, коммутатор выполняет целенаправленную пересылку пакетов между двумя портами на основе физического (MAC) адреса получателя (см. рис. 9). Это возможно благодаря тому, что коммутатор обладает встроенным процессором и памятью и хранит таблицу соответствий MAC-адресов компьютеров и портов, к которым они подключены. Это свойство коммутаторов позволяет существенно уменьшить сетевой трафик и тем самым повысить производительность сети.

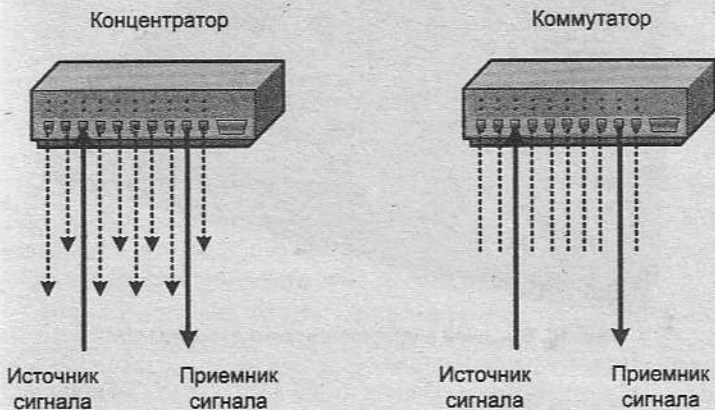


Рис. 9. Отличие концентратора от коммутатора

MAC-адрес – это идентификатор, который назначается сетевому устройству его производителем. Каждая сетевая карта имеет свой MAC-адрес, который состоит из шести шестнадцатеричных чисел, разделенных дефисом, например 00-02-B3-A6-52-CC. Чтобы увидеть MAC-адрес своей сетевой карты, вам необходимо в командной строке Windows XP, вызываемой через меню *Пуск | Все программы | Стандартные | Командная строка*, выполнить команду **ipconfig /all**.

► **ПРИМЕЧАНИЕ.** Также необходимо отметить, что при использовании коммутатора (и правильной его настройке) практически исключается возможность перехвата третьей стороной с помощью sniffеров передаваемой/принимаемой информации (например, паролей, электронных писем и т.д.).

Снифферы (sniffers) – это программы, которые перехватывают информацию, передающуюся по локальной сети, т.е. осуществляют перехват сетевых пакетов. Также они могут расшифровывать пакеты стандартных протоколов связи.

Подробнее о защите вашей сети вы можете прочитать в книге Глушаков С.В., Хачиров Т.С., Соболев Р.О. «Секреты хакера: защита и атака» издательства «Фолио».

Вид коммутатора показан на рис. 10, а основные характеристики некоторых коммутаторов сведены в табл. 3.

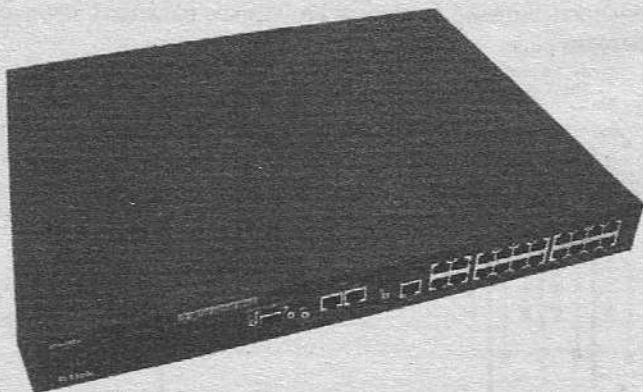


Рис. 10. Внешний вид сетевого коммутатора D-link

Таблица 3

Характеристики некоторых коммутаторов

Наименование	Порты	Комментарий
Planet FSD-803	8xRJ45	Скорость передачи до 100 Мбит/с. Возможность монтажа в стойку. Полнодуплексный режим. Память до 2000 MAC-адресов на порт
3COM 3C16751	16xRJ45	Скорость передачи до 100 Мбит/с

Наименование	Порты	Комментарий
Focus 16-port 10/100BaseTX (065-9131i)	16xRJ45	Скорость передачи 10 или 100 Мбит/с с автоматическим ее определением для каждого порта
Planet FSD-1603	16xRJ45	Скорость передачи 10 или 100 Мбит/с с автоматическим ее определением для каждого порта
D-link DES 3624i	24xRJ45	Скорость передачи 10 или 100 Мбит/с с автоматическим ее определением для каждого порта. Возможность ручной настройки каждого порта

► **ПРИМЕЧАНИЕ.** В настоящее время практически все производители сетевого оборудования прекратили выпуск концентраторов, сосредоточив все усилия на коммутаторах. Благодаря этому была существенно снижена цена последних.

Технология Ethernet

Существует большое количество технологий, позволяющих соединить компьютеры в сеть. Каждая из них была разработана в разное время и предназначена для решения определенной задачи.

В настоящее время для построения локальных сетей используют технологию *Fast Ethernet*, которая является новой реализацией технологии *Ethernet*.

ЧТО ТАКОЕ ETHERNET

Эта технология была разработана в 1970 г. исследовательским центром в Пало-Альто, который принадлежит корпорации Хейгох, а в 1980 г. на ее основе была принята спецификация IEEE 802.3.

Основной принцип работы, используемый в данной технологии, заключается в следующем. Для того чтобы начать передачу данных в сети, сетевой адаптер компьютера «прослушивает» сеть на наличие какого-либо сигнала. Если его нет, то адаптер начинает передачу данных, если же сигнал есть, то

передача откладывается на определенный интервал времени. Время монопольного использования разделяемой среды одним узлом ограничивается временем передачи одного кадра.

Кадр – это единица данных, которыми обмениваются компьютеры в сети Ethernet. Кадр имеет фиксированный формат и наряду с полем данных содержит различную служебную информацию, например адрес получателя и адрес отправителя. После того как адаптер отправителя поместил кадр в сеть, его начинают принимать все сетевые адаптеры. Каждый адаптер проводит анализ кадра, и если адрес совпадает с их собственным адресом устройства (MAC-адрес), кадр помещается во внутренний буфер сетевого адаптера, если же не совпадает, то он игнорируется.

В том случае, если два или более адаптера, «прослушав» сеть, начинают передавать данные, возникает *коллизия* (*collision*). Адаптеры, обнаружив коллизию, прекращают передачу данных, а затем, повторно «прослушав» сеть, повторяют передачу данных через разные промежутки времени.

► **ПРИМЕЧАНИЕ.** Чтобы получить пакет данных, который предназначен для конкретного адаптера, он должен принимать все пакеты, которые появляются в сети.

Такой метод доступа к среде передачи данных получил название *CSMA/CD* (*carrier-sense multiple access/collision detection*) – множественный доступ с обнаружением несущей.

Как следует из вышесказанного, при большом числе компьютеров в сети и при интенсивном обмене информацией очень быстро растет число коллизий, и, как следствие, пропускная способность сети падает. Не исключен случай, когда пропускная способность может упасть до нуля. Но даже в сети, где средняя нагрузка не превышает рекомендованную (30–40% от общей полосы пропускания), скорость передачи составляет 70–80% от номинальной.

Однако в настоящее время данная проблема практически решена, поскольку разработаны устройства, способные разделять потоки данных между теми компьютерами, для которых эти данные предназначаются. Другими словами, трафик между портами, подключенными к передающему и принимающему сетевым адаптерам, изолируется от других портов и адаптеров. Такие устройства называются *коммутаторами* (*switch*).

Существуют различные реализации данной технологии – Ethernet, Fast Ethernet, Gigabit Ethernet, которые могут обеспечивать скорость передачи данных 10, 100 и 1000 Мбит/с соответственно.

Стандарт IEEE 802.3 содержит несколько спецификаций, отличающихся топологией и типом используемого кабеля. Например, 10 BASE-5 использует толстый коаксиальный кабель, 10 BASE-2 – тонкий, а 10 BASE-F, 10 BASE-FB, 10 BASE-FL и FOIRL используют оптический кабель. Наиболее популярна спецификация IEEE 802.3 100BASE-TX, в которой для организации сети используется кабель на основе неэкранированных витых пар с разъемами RJ-45.

Таблица 4

Реализации сети Ethernet

Параметр	Ethernet	Fast Ethernet	Gigabit Ethernet
Номинальная скорость передачи информации, Мбит/с	10	100	1000
Среда передачи	Витая пара, коаксиальный кабель, оптоволокно	Витая пара, оптоволокно	Витая пара, оптоволокно
Варианты реализации	10 Base-2, 10 Base-T, 10 Base-5, 1 Base-5, 10 Broad-36	100 Base-TX, 100 Base-FX, 100 Base-T4	1000Base-X 1000Base-LX 1000Base-SX 1000Base-CX 1000Base-T
Топология	Общая шина, звезда	Звезда	Звезда

Перечисленные выше спецификации Ethernet можно описать следующим образом. Первое число в имени спецификации указывает максимальную скорость передачи данных, например «10» обозначает скорость передачи сигнала 10 Мбит/с. «Base» означает использование в стандарте Baseband-технологии

(*baseband* – это узкополосная передача). При таком способе передачи данных по кабелю каждый бит данных кодируется отдельным электрическим или световым импульсом, при этом весь кабель используется в качестве одного канала связи, т.е. одновременная передача двух сигналов невозможна.

Первоначально последняя секция в названии спецификации предназначалась для отображения максимальной длины кабельного сегмента (без концентраторов и коммутаторов) в сотнях метров. Однако для удобства и более полного определения сути стандарта в его названии цифры были заменены буквами T и F, где T обозначает *twisted pair* – витую пару, а F обозначает *fiber* – волокно.

Таким образом, в настоящее время можно встретить сети, основанные на следующих спецификациях:

- 10Base-2 – 10 МГц Ethernet на коаксиальном кабеле с сопротивлением 50 Ом, *baseband*. 10Base-2 известен как «тонкий Ethernet»;
- 10Base-5 – 10MHz Ethernet на стандартном (толстом) коаксиальном кабеле с сопротивлением 50 Ом, *baseband*;
- 10Base-T – 10MHz Ethernet по кабелю витая пара;
- 100 Base-TX – 100MHz Ethernet по кабелю витая пара.

Весьма существенным преимуществом различных вариантов Ethernet является обоюдная совместимость, которая позволяет использовать их совместно в одной сети, в ряде случаев даже не изменяя существующую кабельную систему.

ПОЛНОДУПЛЕКСНЫЙ РЕЖИМ

Стандарт технологии Fast Ethernet также включает в себя рекомендации относительно обеспечения возможности *полнодуплексной работы (full-duplex mode)* при подключении сетевого адаптера к коммутатору или же при непосредственном соединении коммутаторов между собой.

Суть полнодуплексного режима заключается в возможности одновременной передачи и приема данных по каналам Tx (канал от передатчика к приемнику) и Rx (канал от приемника к передатчику), при этом скорость передачи возрастает вдвое и достигает 200 Мбит/с. На данный момент практически все производители сетевого оборудования заявляют, что их устройства обеспечивают работу в полнодуплексном режиме, однако из-за разного толкования стандарта, в частности способов

управления потоком кадров, не всегда удается добиться корректной работы этих устройств и хороших скоростных показателей.

Соединяем компьютеры

В этом разделе вы ознакомитесь с монтажом сети и приемами работы с различными средами передачи данных. Установка кабельной системы – достаточно сложный процесс, поскольку правильный монтаж элементов сети очень важен, особенно если речь идет о кабеле на основе витой пары.

Для построения сети для трех и более компьютеров вам понадобятся:

- *сетевой адаптер* – по одному устройству в каждый компьютер;
- *коммутатор (switch)* – одно устройство с необходимым количеством портов. Лучше, когда количество портов на треть больше, чем требуется. Например, если необходимо объединить пять компьютеров, то лучше приобрести 8-портовый коммутатор. Это даст вам возможность подключить к сети еще несколько компьютеров, не устанавливая при этом дополнительного коммутатора. Не забудьте, что его желательно разместить в геометрическом центре, чтобы экономить кабель;
- *кабель* – перед его приобретением следует продумать, как он будет проложен, где находится коммутатор, и измерить все расстояния. По наблюдениям авторов, только для разводки по квартире требуется около 30 метров кабеля, а в подъезде дома – еще больше;
- *коннекторы* – каждый конец кабеля должен быть обжат специальным образом с использованием коннекторов.

Рассмотрим подробнее этапы монтажа сети.

КАК УСТАНОВИТЬ СЕТЕВУЮ КАРТУ

Большинство современных бюджетных сетевых карт построены на чипсете Realtek RTL8139D, который корректно определяется операционной системой Windows XP. Это значит, что при установке карты вы сможете сразу же начать работу в сети, не устанавливая дополнительных драйверов.

Но для начала карту следует физически установить в компьютер. Для этого необходимо выполнить такие действия.

- ① Отключите компьютер от электросети. Простого выключения недостаточно, так как современные блоки питания все равно подают напряжение на материнскую плату. Необходимо или выключить фильтр питания, или отсоединить кабель от блока питания компьютера.
- ② Снимите стенку корпуса. Обратите внимание: обычно на материнской плате есть световой индикатор, показывающий наличие напряжения на ее элементах, – он не должен светиться.
- ③ Найдите на материнской плате любой свободный слот PCI (белый слот, их должно быть несколько). Посмотрите, есть ли на задней стороне корпуса прямоугольное отверстие рядом с этим слотом.
- ④ Если отверстия нет, очень аккуратно удалите заглушку рядом со слотом. Ее придется выломать, но будьте предельно осторожны!
- ⑤ Выньте сетевую карту из упаковки и вставьте ее в слот PCI. При установке карты не нажимайте на нее очень сильно, а после установки закрепите ее одним болтом.
- ⑥ Закройте стенку корпуса и подключите кабель питания.
- ⑦ Включите компьютер. При загрузке операционной системы будет обнаружено новое оборудование, и если в системе уже имеются драйверы данной сетевой карты, они будут установлены, и карта готова к работе.
- ⑧ Если операционная система не обнаружила драйверов, она попросит установить дискету или компакт-диск в соответствующее устройство, произведет поиск драйверов и установит их.

В том случае, если автоматический поиск драйверов не удался, их следует установить вручную. Каждый производитель сетевого оборудования вместе с устройствами поставляет и драйверы (на различных носителях). Однако у дешевых сетевых карт драйверы обычно записаны на дискетах и не имеют программы установки. Поэтому вам потребуются дополнительные сведения: нужно точно знать, как называется ваша сетевая карта, и желательно знать, на каком чипсете она собрана.

ОБЖИМ КАБЕЛЯ

Витая пара (UTP/STP, unshielded/shielded twisted pair, см. рис. 5) в настоящее время является наиболее распространенной средой передачи сигналов в локальных сетях. Кабели этого типа различаются по категориям (в зависимости от полосы пропускания) и типа проводников. В кабеле 5-й категории находится восемь проводников, перевитых попарно (то есть четыре пары).

Структурированная кабельная система, построенная на основе витой пары 5-й категории, имеет очень большую гибкость в использовании. Грамотное построение сети на ее основе должно базироваться на следующих принципах.

Для витой пары применяют коннектор RJ-45 – восьмиконтактный разъем, использующийся обычно для подключения кабеля к сетевым платам Ethernet.

Для монтажа коннекторов RJ-45 используются специальные обжимные приспособления, оснащенные лезвиями для снятия защитной оболочки и восемью ножами для фиксации разреза (см. рис. 11). Для обжима кабеля вам необходимо выполнить нижеуказанные действия.

- ① Аккуратно обрезать конец кабеля. Обратите внимание на то, чтобы торец кабеля был ровным.
- ② Используя обжимной инструмент (см. рис. 11), необходимо снять с кабеля внешнюю изоляцию на длину примерно 20 мм и обрезать нить, вмонтированную в кабель. Она предназначена для удобства снятия изоляции с кабеля на большую длину. Обратите внимание, что любые повреждения изоляции проводников недопустимы – именно поэтому желательно использовать специальный инструмент, лезвие резака которого выступает на толщину внешней изоляции.
- ③ Далее следует надеть на кабель защитный колпачок, который предназначен для защиты коннектора от повреждения и попадания пыли.
- ④ Затем следует аккуратно расплести и выровнять проводники в один ряд, при этом их следует расположить в следующей последовательности (естественно, слева направо):
 - первый – бело-оранжевый;
 - второй – оранжевый;
 - третий – бело-зеленый;
 - четвертый – синий;
 - пятый – бело-синий;

- шестой – зеленый;
- седьмой – бело-коричневый;
- восьмой – коричневый.

Проводники должны располагаться строго в один ряд, без нахлестов друг на друга. Затем их обрезают так, чтобы они выступали над внешней обмоткой на 8–10 мм.

- 5) Далее, удерживая разъем защелкой от себя (вы не должны видеть защелку, см. рис. 6), вставьте в коннектор кабель. Каждый проводник должен попасть на свое место в разьеме и упереться во фронтальную стенку коннектора. Прежде чем обжимать коннектор, стоит убедиться, что в расположении проводников нет ошибок (провода часто путаются, когда их вставляют в коннектор).
- 6) Теперь вы должны вставить коннектор в гнездо на обжимных клещах и сжать его до упора-ограничителя на клещах. В результате фиксатор на коннекторе встанет на свое место, удерживая кабель в разьеме неподвижным. Контактные ножи разьема врежутся каждый в свой проводник, обеспечивая надежный контакт.
- 7) Далее следует надеть колпачок на коннектор, – и кабель готов.

► **ПРИМЕЧАНИЕ.** Коннектор можно использовать только один раз. При обжиме происходит его необратимая трансформация, и в случае ошибки вам придется срезать коннектор и повторить операцию.

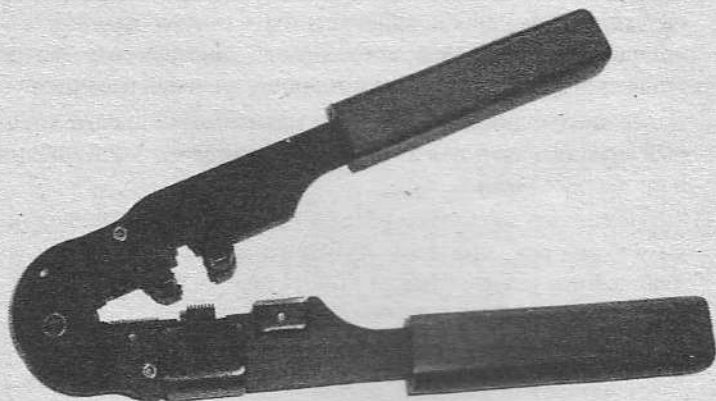


Рис. 11. Обжимной инструмент

УСТАНОВКА КОММУТАТОРА И ПРОКЛАДКА КАБЕЛЯ

Данная процедура является очень простой. Обычно коммутаторы имеют специальные отверстия в корпусе, предназначенные для крепления на стену. Для крепления необходимо просверлить в стене два отверстия на требуемом расстоянии друг от друга, забить в них деревянные или пластмассовые дюбели и вкрутить шурупы. Помните, что коммутатор лучше всего установить в геометрическом центре будущей сети.

Также необходимо избегать установки коммутатора и прокладки кабеля рядом с силовой (электрической) проводкой, поскольку она будет вносить значительные помехи в сигнал, передаваемый по витой паре.

Если же вы решили проложить кабель в шахтах, где находится электрическая проводка дома, следует использовать экранированную витую пару (*Shield twisted pair, STP*). От неэкранированной витой пары она отличается тем, что проводники заключены в оболочку из фольги, которая отражает магнитные помехи.

КАК СОЕДИНИТЬ ДВА КОМПЬЮТЕРА

Для соединения только двух компьютеров вам не обязательно использовать коммутатор, или switch. Вместо него требуется специально обжатый кабель – так называемый «crossover» (скрученный) кабель (см. табл. 5).

Таблица 5

Crossover-кабель

Номер проводника	Первый коннектор	Второй коннектор
Первый	бело-оранжевый	бело-зеленый
Второй	оранжевый	зеленый
Третий	бело-зеленый	бело-оранжевый
Четвертый	синий	бело-коричневый
Пятый	бело-синий	коричневый
Шестой	зеленый	оранжевый
Седьмой	бело-коричневый	синий
Восьмой	коричневый	бело-синий

После изготовления данного кабеля вы должны вставить его концы в сетевые платы двух компьютеров, при этом вы получите полнофункциональное соединение на скорости, зависящей только от сетевых карт. Если это качественные карты от известных производителей, которые поддерживают полнодуплексный режим, то вы получите соединение на скорости, близкой к 200 Мбит в секунду.

Таким образом, нами рассмотрены основные аппаратные составляющие ЛВС, однако для того, чтобы сеть нормально функционировала, необходимо разобраться в принципах передачи данных внутри самой сети.

Глава 2

Как общаются компьютеры

После прокладки проводов, подключения их к коммутатору и установки сетевых карт операционная система Windows XP создает соединение, которое называется *Local Area Connection* (*Соединение по локальной сети*). Однако в большинстве случаев без определенной настройки его использование невозможно или ограничено. Для полноценной работы сети вам потребуется сконфигурировать параметры протокола TCP/IP. Этому посвящена данная глава.

Протоколы семейства TCP/IP

В свое время создатели ЛВС пришли к осознанию важности использования межсетевых технологий для передачи данных. Результатом стали исследования и создание набора сетевых стандартов, которые детально описывают процесс взаимодействия компьютеров, а также содержат ряд соглашений при взаимодействии сетей и маршрутизации данных.

Принципы построения сетей и организации процессов, которые в них происходят, во многом связаны со стандартами, которые называют *протоколами*. Протоколы реализуют способы передачи сообщений, описывают детали форматов сообщений и указывают, как обрабатывать ошибки. Однако важным является то, что они позволяют рассматривать стандарты взаимодействия вне зависимости от типа оборудования, на котором они реализованы. Другими словами, коммуникационный протокол позволяет описать или понять процесс передачи данных, не привязываясь к какому-либо конкретному оборудованию, использованному для выполнения этого процесса.

Официально названный *Transmission Control Protocol/Internet Protocol* (TCP/IP) стал промышленным стандартом протоколов, разработанных для глобальных сетей. Он может использоваться для взаимодействия компьютеров с помощью неограниченного числа сетей. Например, можно использовать TCP/IP для связи отдельных сетей внутри организации или жилого дома, даже если связь с внешними сетями отсутствует.

Технология TCP/IP хороша благодаря своей высокой жизнеспособности, поэтому она стала базовой технологией для большого количества ЛВС.

Сам протокол TCP/IP состоит из нескольких уровней реализации. На нижнем уровне он поддерживает все популярные стандарты физического (канального) уровня реализации: для локальных сетей это, например, Ethernet, Token Ring, Fast Ethernet, а для глобальных сетей это могут быть протоколы соединений SLIP и PPP.

На более высоком уровне обеспечивается межсетевое взаимодействие – здесь происходит передача пакетов данных с использованием различных транспортных технологий локальных сетей, территориальных сетей или линий специальной связи.

ПРОТОКОЛЫ TCP/IP МЕЖСЕТЕВОГО УРОВНЯ

Протокол *Internet Protocol* (IP) выступает в качестве базового протокола сетевого уровня в технологии TCP/IP. Последний изначально был спроектирован как протокол передачи пакетов в составных сетях, состоящих из большого количества ЛВС, объединенных как локальными, так и глобальными связями. Именно по этой причине IP-протокол хорошо работает в сетях со сложной структурой, рационально используя аппаратную часть и экономно расходуя пропускную способность низкоскоростных линий связи.

IP-протокол относится к такому типу протоколов, которые не гарантируют доставку пакетов до узла назначения (подтверждение доставки может отсутствовать), но стараются это сделать. К рассматриваемому уровню межсетевого взаимодействия относится и протокол межсетевых управляющих сообщений *ICMP* (*Internet Control Message Protocol*). Он имеет широкое распространение и предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом – источником пакета. С помощью специальных пакетов ICMP сообщается о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и другая служебная информация. Например, этот протокол использует утилита **ping**, предназначенная для проверки наличия соединения между двумя узлами.

ПРОТОКОЛЫ ТСП/ІР ТРАНСПОРТНОГО УРОВНЯ

Транспортный уровень ТСП/ІР является базовым и обеспечивает функционирование протокола управления передачей ТСП (*Transmission Control Protocol*) и протокола датаграмм пользователя UDP (*User Datagram Protocol*).

Протокол ТСП обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования виртуальных соединений. Протокол UDP обеспечивает передачу пакетов данных, однако он не гарантирует доставку данных от одного компьютера к другому, а поэтому используется для передачи небольших объемов информации. ТСП и UDP выполняют функции связующего звена между межсетевым протоколом и многочисленными прикладными процессами, которые работают на вашем компьютере (например, программы общения или передачи файлов).

ПРОТОКОЛЫ ТСП/ІР ПРИКЛАДНОГО УРОВНЯ

Для обеспечения взаимодействия программ клиентов и серверов предназначен прикладной уровень ТСП/ІР. На этом уровне существует большое количество протоколов и сервисов. К ним относятся такие широко используемые протоколы, как протокол копирования файлов *FTP (File Transfer Protocol)*; протокол эмуляции терминала *Telnet*; почтовый протокол *SMTP (Simple Mail Transfer Protocol)*, используемый в электронной почте сети Internet; гипертекстовые сервисы доступа к удаленной информации, такие как *WWW* и многие другие.

Таким образом, скрытие в технологии ТСП/ІР низкоуровневых деталей взаимодействия помогает улучшить производительность сети. По этой причине при создании и использовании программного обеспечения пользователям и администраторам не нужно знать или помнить множество деталей о конкретных параметрах оборудования. Такие программы, разработанные с учетом самого высокого уровня ТСП/ІР, не ограничены архитектурой конкретного ПК или конкретного сетевого оборудования, их не надо изменять при замене компьютера или изменении конфигурации. Наконец, так как прикладные программы не зависимы от используемого оборудования, они могут обеспечивать прямое взаимодействие различных элементов ЛВС. Другими словами, необходимость в специальных версиях прикладных программ передачи данных для всех возможных соединений между компьютерами в сети отпадает.

Взаимодействие между разнородными сетями

В том случае, если вам необходимо подключить свою локальную сеть к уже существующей, придется решить несколько проблем, связанных, во-первых, с физическим объединением, а во-вторых, возможно, с проблемой маршрутизации (перенаправления) пакетов из одной подсети в другую.

При решении проблемы построения составных сетей необходимо иметь в виду, что физически две сети могут соединяться только с помощью устройства, присоединенного к каждой из них. Однако непосредственное соединение не гарантирует, что компьютер сможет взаимодействовать с компьютером, находящимся в другой подсети. Для обеспечения надежной связи необходимо, чтобы компьютеры умели передавать пакеты данных из одной сети в другую. Компьютеры, соединяющие две сети и передающие пакеты из одной в другую, называются *межсетевыми шлюзами (gateway)*, или *межсетевыми маршрутизаторами (router)*.

Рассмотрим функционирование шлюза на простейшем соединении двух сетей (см. рис. 12). Компьютер, выполняющий функции шлюза, присоединен как к сети А, так и к сети В. Работа компьютера в качестве шлюза подразумевает, что он должен принимать из сети А пакеты данных, предназначенные компьютерам сети В, и передавать их адресату. Аналогично, шлюз должен принимать из сети В пакеты, которые предназначены компьютерам в сети А, и передавать их в эту сеть.

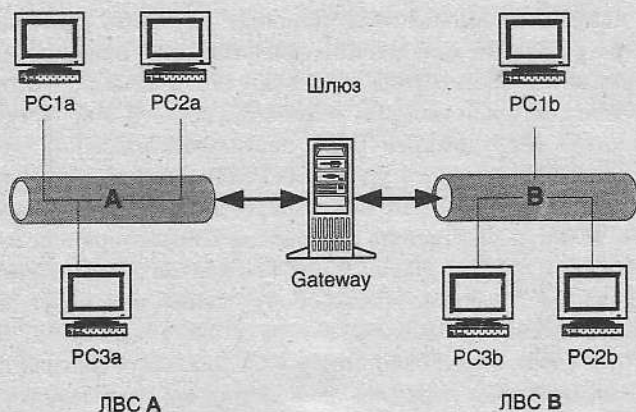


Рис. 12. Функционирование шлюза между двумя сетями

Например, если пакет данных отправлен с компьютера PC1a, а предназначен компьютеру PC3b, то данные от PC1a передаются на шлюз, а далее шлюз адресует их на PC3b.

Идея шлюза не является сложной, однако важна по той причине, что она обеспечивает способ взаимного соединения сетей, а не отдельных компьютеров.

Адресация в IP-сетях

Коммуникационная система, которую вы создаете, должна обеспечивать универсальное средство взаимодействия, т.е. осуществлять связь между любыми компьютерами, независимо от их аппаратной конфигурации и операционной системы. Чтобы сделать коммуникационную систему универсальной, нужно определить приемлемый для всех пользователей сети метод идентификации компьютеров, которые к ней присоединены.

Традиционно идентификаторы в сети состоят из:

- *идентификатора хоста* – имени, указывающего на конечный объект;
- *идентификатора сети* – адреса, идентифицирующего физическое местоположение объекта;
- маршрута, определяющего, как добраться до объекта.

В реальных сетях имена, адреса и маршруты определяются на разных уровнях представления TCP/IP-идентификаторов, причем имена – на самом верхнем, а маршруты – на самом нижнем. Пользователю удобнее применять для идентификации произносимые имена, в то время как программное обеспечение лучше работает с более компактным числовым представлением идентификаторов. В TCP/IP-технологиях было принято решение стандартизовать компактные двоичные адреса, которые делают такие вычисления, как выбор маршрута, более эффективными.

Разработчики TCP/IP выбрали схему адресации, в которой каждому компьютеру в сети назначается адрес в виде четырех целых чисел, называемый *межсетевым адресом*, или *IP-адресом*. При этом значения IP-адреса выбираются особым образом, чтобы сделать маршрутизацию эффективной. Иначе говоря, IP-адрес кодирует идентификацию сети, к которой присоединен компьютер, а также идентификацию самого

компьютера в этой сети. Поэтому каждому компьютеру в TCP/IP сети назначен уникальный 32-битовый межсетевой адрес, который используется при взаимодействии.

Для удобства пользователей в технических документах или прикладных программах IP-адреса записываются как четыре десятичных числа, разделенных десятичными точками, и каждое из этих чисел представляет значение группы из восьми символов двоичного IP-адреса. Поэтому 32-битовый IP-адрес

11000000 10101000 01101111 00000001

обычно записывается как

192.168.111.1

Очевидно, что такая запись гораздо удобнее для использования, чем двоичная форма.

Принципиально, каждый адрес является парой «идентификатор сети – идентификатор компьютера в этой сети». На практике каждый IP-адрес должен иметь одну из трех форм, или классов: А, В или С, которые можно различить по первым двум битам адреса.

В табл. 6 приведены диапазоны номеров, соответствующие каждому классу сетей.

Таблица 6

Диапазон номеров сетей разного класса

Класс	Наименьший адрес	Наибольший адрес
A	1.0.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.0.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	254.255.255.255

Адреса класса А используются для сетей, имеющих в своем составе не более чем 16 777 214 компьютеров, однако таких сетей может быть не более 126. В этих адресах выделяется под идентификатор сети 8 бит, а под идентификатор компьютера – 24 бита.

Адреса класса В используются для сетей меньшего размера, включающих до 65 534 компьютеров. В этих адресах выделяется 16 бит под идентификатор сети и 16 бит – под идентификатор компьютера.

Сети класса С должны состоять менее чем из 254 компьютеров, причем в адресе выделяется 24 бит под идентификатор сети и 8 бит – под идентификатор компьютера.

Номер сети (т.е. номер сети внутри ЛВС, иначе говоря – номер подсети) в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла гибкое, и граница между этими полями может устанавливаться достаточно произвольно при помощи маски подсети. Идентификаторы сетей и идентификаторы узлов в IP-адресе различаются с помощью *маски подсети*. Каждая маска подсети представляет собой 32-битное число, состоящее из последовательной группы единичных битов для выделения из IP-адреса идентификатора сети и последовательной группы нулевых битов для выделения идентификатора узла.

Ниже приведена маска подсети, которая обычно используется с IP-адресом 192.168.1.1:

```
11111111 11111111 11111111 00000000
```

Данная маска подсети состоит из 24 единичных бит, за которыми следуют 8 нулевых бит. Это означает, что часть IP-адреса, соответствующая идентификатору сети, состоит из трех октетов, а часть, соответствующая идентификатору узла, имеет длину 8 бит. В точно-десятичной нотации эта маска будет иметь следующий вид: 255.255.255.0.

Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Следует иметь в виду, что адресация в IP-сетях основана на следующих типах адресов: *сетевом* (IP-адрес, рассмотрен выше), *физическом* (MAC-адрес) и *символьном* (DNS-имя).

Физический адрес узла сети определяется технологией, с помощью которой построена эта сеть. Для узлов, входящих в ЛВС, это MAC-адрес сетевого адаптера или порта маршрутизатора (MAC – Media Access Control, контроль доступа к среде передачи данных). Данные адреса назначаются производителем.

лями оборудования и являются уникальными адресами, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC-адрес имеет 6 байт, из которых: старшие 3 байта – идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.

Символьный идентификатор – имя, например xiit.kharkov.ua, которое назначается администратором и состоит из нескольких частей, например имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, используется на прикладном уровне, например в протоколах FTP или Telnet. Отображением символьных адресов и учетом соответствия IP-адреса его DNS-имени занимается служба *DNS (Domain Name System)*.

Для операционных систем Windows компания Microsoft разработала собственную систему имен, которая называется *Windows Internet Naming System (WINS)*. В небольшой сети развернуть службу DNS достаточно тяжело, поскольку для нее необходимо выделить отдельный компьютер или, по крайней мере, компьютер, который будет выполнять еще ряд задач, но будет работать круглосуточно. Именно об использовании и настройке WINS мы расскажем ниже.

Выбор IP-адресов

Для локальных сетей, которые не имеют выхода в сеть Internet или используют для этого шлюз, вы должны использовать один из диапазонов IP-адресов (см. табл 7), которые зарезервированы организацией IANA (Internet Assigned Numbers Authority) и не используются в Internet.

Таблица 7

Внутренние IP-адреса

Идентификатор сети	Маска подсети	Диапазон IP-адресов
10.0.0.0	255.0.0.0	10.0.0.1 – 10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1 – 172.31.255.254
192.168.0.0	255.255.255.0	192.168.0.1 – 192.168.255.254

Например, для сети из пяти компьютеров можно использовать конфигурацию, которая приведена на рис. 13.

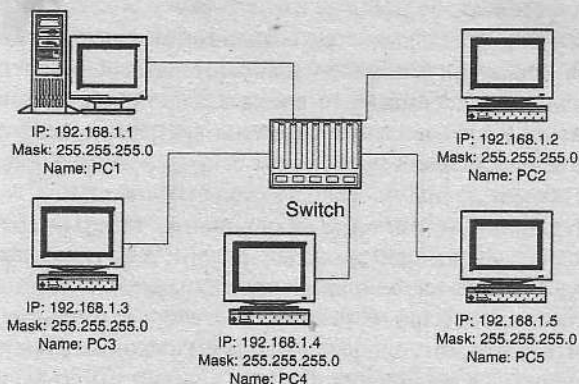


Рис. 13. Возможная конфигурация сети

В такой конфигурации каждый компьютер получает IP-адрес из диапазона С и маску подсети 255.255.255.0, а это значит, что максимальное число компьютеров в данной сети не может превышать 254.

Кроме этого, использование IP-адресов из таблицы 7 позволит избежать конфликтов, если вы подключите такую сеть к Internet, поскольку указанные в таблице адреса не маршрутизируются, т.е. не передаются провайдером Internet из вашей сети в Internet.

Порты

Существуют два типа межкомпьютерного обмена данными – *датаграммы* и *сеансы*. *Датаграмма* – это сообщение, которое не требует подтверждения о приеме от принимающей стороны, а если такое подтверждение необходимо, то адресат должен сам послать специальное сообщение. Для осуществления обмена данными таким способом принимающая и передающая стороны должны строго придерживаться определенного протокола во избежание потери информации. Каждая датаграмма является самостоятельным сообщением, и при наличии нескольких датаграмм в ЛВС их доставка адресату, вообще говоря, не гарантируется. При этом датаграмма обыч-

но является частью какого-либо сообщения, и в большинстве ЛВС скорость передачи датаграмм гораздо выше, чем сообщений в сеансах.

В *сеансе* предполагается создание логической связи для обмена сообщениями между компьютерами и гарантируется получение сообщений. В то время как датаграммы могут передаваться в произвольные моменты времени, в сеансе перед передачей сообщения происходит открытие сеанса, а по окончании обмена данными сеанс должен быть закрыт.

Операционные системы большинства компьютеров поддерживают мультипрограммный режим, т.е. несколько программ выполняются одновременно (параллельно выполняется несколько процессов). С некоторой степенью точности можно говорить о том, что процесс – это и есть окончательное место назначения для сообщения. Однако в силу того, что процессы создаются и завершаются динамически, отправитель редко имеет информацию, достаточную для идентификации процесса на другом компьютере. Поэтому возникает необходимость в определении места назначения данных на основе выполняемых процессами функций, ничего не зная о тех процессах, которые реализуются этими функциями.

На практике вместо того, чтобы считать процесс конечным местом назначения, полагают, что каждый компьютер имеет набор некоторых точек назначения, называемых протокольными портами. Каждый порт идентифицируют целым положительным числом (от 0 до 65535). В этом случае операционная система обеспечивает механизм взаимодействия, используемый процессами для указания порта, на котором они работают, или порта, к которому нужен доступ. Обычно порты являются буферизированными, и данные, приходящие в конкретный порт до того, как процесс готов их получить, не будут потеряны: они будут помещены в очередь до тех пор, пока процесс не извлечет их.

Чтобы лучше понять технологию портов, представьте, что вы пришли в банк, чтобы сделать вклад. Для этого вам необходимо подойти к определенному окошку, где оператор оформит документы и вы откроете счет. В этом примере банк представляет собой компьютер, а операторы банка – программы, которые выполняют определенную работу. А вот окошки – это и есть порты, при этом каждое окошко в банке часто нумеруется (1, 2, 3 ...). То же самое относится и к портам.

Следовательно, чтобы связаться с портом на другом компьютере, отправитель должен знать как IP-адрес компьютера-получателя, так и номер порта в компьютере. Каждое сообщение содержит как номер порта компьютера, которому адресовано сообщение, так и номер порта-источника компьютера, которому должен прийти ответ. Таким образом реализуется возможность ответить отправителю для каждого процесса.

Порты с номерами от 0 до 1023 являются привилегированными и используются сетевыми службами, которые, в свою очередь, запущены с привилегиями администратора (суперпользователя). Например, служба доступа к файлам и папкам Windows использует порт 139, однако если она не запущена на компьютере, то при попытке обратиться к данной службе (т.е. к данному порту) будет получено сообщение об ошибке.

Порты с 1023 до 65535 являются непривилегированными и используются программами-клиентами для получения ответов от серверов. Например, web-браузер пользователя, обращаясь к web-серверу, использует порт 44587 своего компьютера, но обращается к 80 порту web-сервера. Получив запрос, web-сервер отправляет ответ на порт 44587, который используется web-браузером.

Глава 3

Настройка соединений

Из этой главы вы узнаете, как настроить операционные системы Microsoft Windows XP и Windows 98 для работы в сети на основе TCP/IP.

При инсталляции операционной системы на компьютер и при подключении его к сети требуется указание (или изменение) его имени, имени рабочей группы или других сетевых параметров (например, настройка протокола TCP/IP). Чаще всего такая ситуация встречается при подключении компьютера к сети, когда требуется настроить компьютер для взаимодействия с другими ПК, входящими в сеть.

Как изменить имя компьютера

WINDOWS XP

Для изменения сетевой идентификации компьютера (т.е. его имени) необходимо выполнить следующие действия.

- ① Открыть Панель управления и выбрать пункт *Система*.
- ② Перейти на вкладку *Имя компьютера* и нажать на кнопку *Изменить*.
- ③ В появившемся окне *Изменение имени компьютера* (см. рис. 14) требуется ввести новое имя компьютера, а также, если необходимо, можно изменить его принадлежность к рабочей группе или домену (группа переключателей *Является членом*).
- ④ Нажать кнопку *ОК*.
- ⑤ Перезагрузить компьютер, если он не выполнил эту процедуру самостоятельно.

► **ПРИМЕЧАНИЕ.** Изменения, касающиеся имени компьютера и его принадлежности к группе, вступают в силу только после перезагрузки.

При создании небольшой сети, скорее всего, вы должны будете создать рабочую группу, поскольку для создания домена потребуется установка на один из компьютеров серверной операционной системы, например Windows Server 2003.

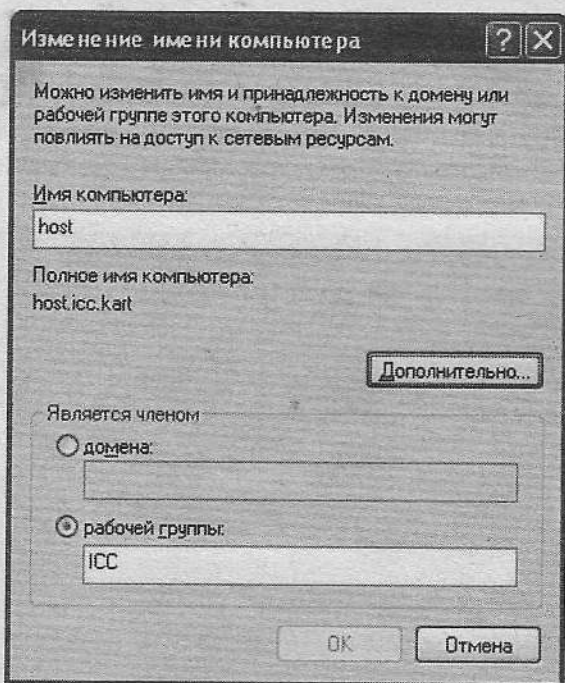


Рис. 14. Изменение имени компьютера в Windows XP

Запомните, что при указании названия рабочей группы вы должны следовать определенным правилам:

- имя рабочей группы не должно совпадать с именем компьютера;
- имя рабочей группы может содержать до 15 символов;
- запрещается использование следующих символов: ; : " < > * + = \ | ? , .

WINDOWS 98

Для изменения имени компьютера в операционной системе Windows 98 вы должны выполнить нижеперечисленные действия.

- ① Открыть Панель управления и выбрать пункт *Сеть*.
- ② Перейти на вкладку *Идентификация* (см. рис. 15).
- ③ В поле *Имя компьютера* указать NetBIOS-имя, которое можно будет использовать для обращения к компьютеру.

- ④ В поле *Рабочая группа* следует указать имя рабочей группы, к которой принадлежит компьютер.
- ⑤ В поле *Описание компьютера* можно указать небольшой комментарий о назначении или владельце этого компьютера.
- ⑥ После заполнения полей следует нажать кнопку *ОК* и перезагрузить компьютер.

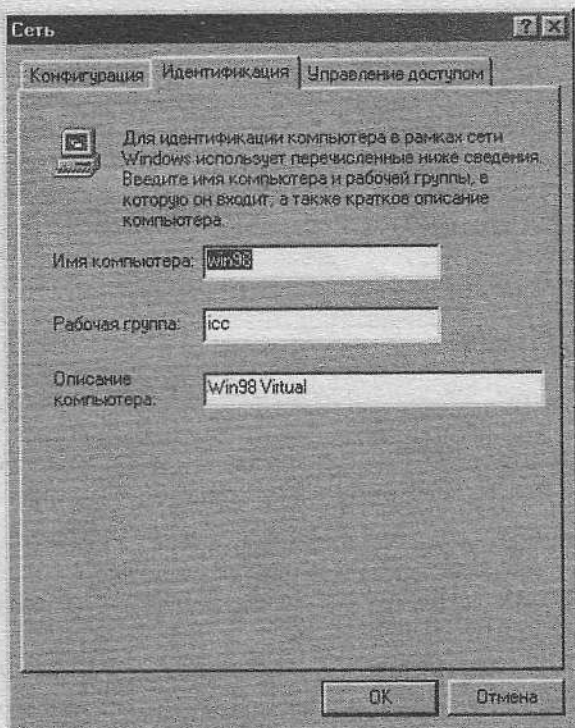


Рис. 15. Изменение имени компьютера в Windows 98

Как добавить сетевые компоненты

Сетевые компоненты обеспечивают наличие тех или иных возможностей при работе компьютера в сети. Например, компонент *Client for Microsoft Networks* (*Клиент для семей Microsoft*) позволяет компьютеру получать доступ к ресурсам в сети Microsoft, а компонент *File and Printer Sharing for Microsoft*


Networks (Служба доступа к файлам и принтерам сетей *Microsoft*) позволяет другим компьютерам получать доступ к ресурсам данного ПК.

WINDOWS XP

Для добавления необходимого компонента (службы или протокола) необходимо отобразить окно свойств сетевого подключения. Для этого следует выполнить следующие действия.

- 1 Открыть Панель управления и выбрать пункт *Сетевые подключения*.
- 2 Выделить требуемое подключение, например *Local Area Connection* (*Подключение по локальной сети*).

- 3 Выбрать команду *Свойства*.

В появившемся окне *Local Area Connection – свойства* (см. рис. 16) отображается наименование сетевого адаптера, который обеспечивает физическое подключение к сети (*Подключение через*); список компонентов, которые установлены для этого адаптера (*Компоненты, используемые этим подключением*); кнопки добавления (*Установить*), удаления (*Удалить*) и настройки (*Свойства*) компонентов. Также в данном окне присутствует флажок *При подключении вывести значок в области уведомлений*, при установке которого в области уведомлений появляется иконка , свидетельствующая о том, что компьютер подключен к сети. Данная иконка может использоваться для быстрого доступа к свойствам сетевого подключения, а также она мигает, когда имеет место передача пакетов. Настоятельно рекомендуется устанавливать данный флажок, поскольку администратор всегда может отслеживать сетевую активность.

Для добавления требуемого компонента выполняем перечисленные ниже действия.

- 1 Нажимаем в окне *Local Area Connection – свойства* (см. рис. 16) кнопку *Установить*.
- 2 В появившемся окне выбираем необходимую службу, протокол или клиента.
- 3 Нажимаем кнопку *Добавить*, после чего будет открыто окно с перечнем доступных компонентов.
- 4 Выбрав необходимый компонент, нажимаем кнопку *ОК*, после чего он будет установлен.

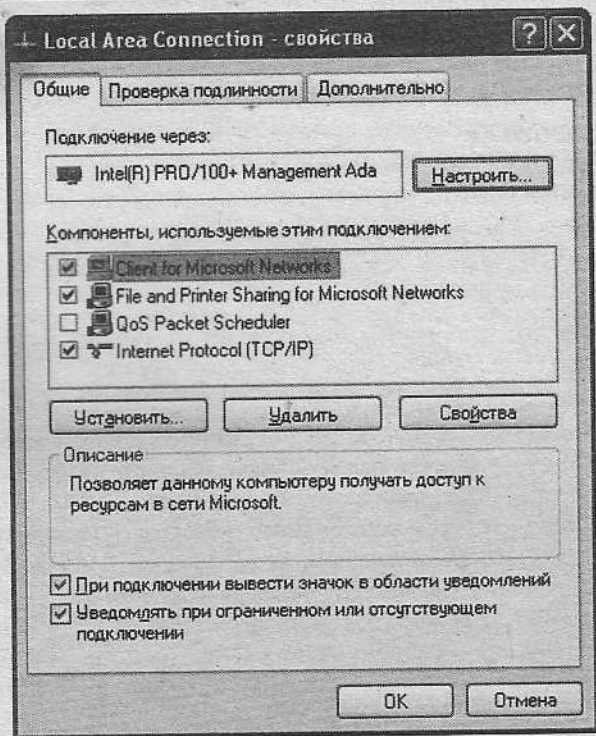


Рис. 16. Свойства подключения по локальной сети

При обнаружении системой сетевого адаптера Windows XP автоматически создается новое подключение и устанавливаются следующие сетевые компоненты:

- Client for Microsoft Networks;
- QoS Packet Scheduler;
- File and Printer Sharing for Microsoft Networks;
- Internet Protocol (TCP/IP).

Как настроить TCP/IP

Протокол TCP/IP является основным протоколом, который используется в сетях Microsoft и в большинстве других сетей. Данный протокол используется для доступа в сеть Internet, а также подходит для построения сетей в организациях и на предприятиях любого масштаба.

Для изменения параметров протокола TCP/IP следует в диалоговом окне *Local Area Connection – свойства* (см. рис. 16) выбрать компонент *Internet Protocol (TCP/IP)* и нажать кнопку *Свойства*. В том случае, если данный компонент не установлен, его следует установить так, как описано выше.

В появившемся окне *Свойства: Internet Protocol (TCP/IP)* (см. рис. 17) пользователь может определить способ назначения IP-адреса компьютера. При установке переключателя в положение *Получить IP-адрес автоматически* компьютер будет арендовать IP-адрес у DHCP-сервера (см. ниже). Иными словами, во время загрузки операционной системы она будет отправлять в сеть широковещательный запрос, при помощи которого будет искать любой DHCP-сервер в сети. В том случае, если DHCP-сервер в сети присутствует, он предлагает компьютеру IP-адрес из своей области.

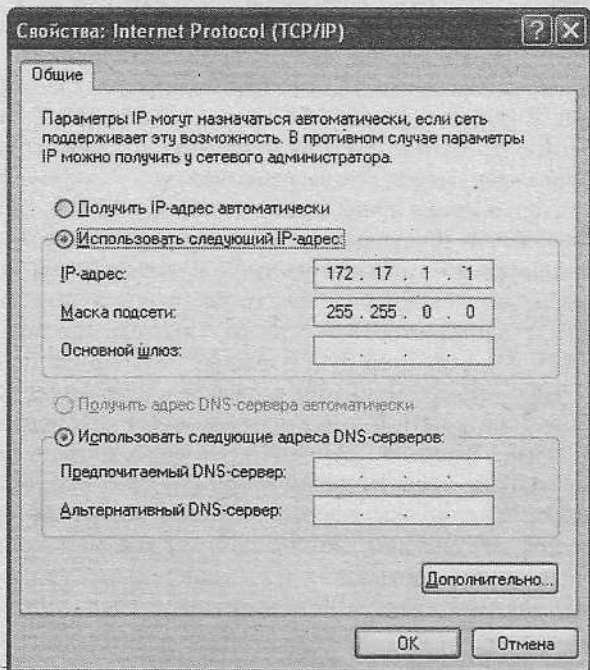


Рис. 17. Свойства протокола TCP/IP

Но вряд ли в вашей сети существует DHCP-сервер, поэтому вам следует вручную настроить IP-адрес компьютера.

Для назначения статического IP-адреса следует установить переключатель в положение *Использовать следующий IP-адрес* и такие следующие параметры:

- *IP-адрес* – IP-адрес компьютера (обязательный параметр);
- *Маска подсети* – маска подсети (обязательный параметр);
- *Основной шлюз* – шлюз, используемый по умолчанию.

Альтернативная и Автоматическая частная IP-адресации (APIPA)

В операционной системе Windows XP, по сравнению с Windows 9x, появилась очень полезная функция, которая позволяет компьютеру использовать (правда, ограниченно) ресурсы локальной сети. Суть функции заключается в следующем: после физического соединения компьютеров с использованием технологии Ethernet и корректной установкой драйвера сетевого адаптера операционная система пытается автоматически сконфигурировать параметры TCP/IP. Она использует специальный диапазон IP-адресов от 169.254.0.1 до 169.254.255.254 (*Automatic private IP-Address*, APIPA) и, обладая адресом из указанного диапазона, может взаимодействовать с системами, IP-адреса которых также принадлежат диапазону APIPA. Системы с «нормальными» IP-адресами компьютер «видеть» не будет.

Функция автоматической частной IP-адресации изначально разрабатывалась для случаев, когда компьютер не сможет получить IP-адреса от DHCP-сервера. Поэтому при использовании APIPA компьютер будет каждые пять минут пытаться найти DHCP-сервер, чем будет порождать ненужную передачу информации в сети и уменьшать пропускную способность канала связи. Конечно, в небольшой сети на основе *Fast Ethernet* падение пропускной способности невелико, однако в большой сети возможны задержки пакетов. Кроме этого, каждый раз при загрузке компьютера он будет получать новый IP-адрес, а это не совсем удобно.

Итак, для настройки APIPA выполняем следующие инструкции:

- ① Открываем окно *Свойства: Internet Protocol (TCP/IP)*.
- ② Устанавливаем переключатель в положение *Получить IP-адрес автоматически*, при этом появится вкладка *Альтернативная конфигурация* (см. рис. 18).

- ③ На вкладке *Альтернативная конфигурация* устанавливаем переключатель в положение *Автоматический частный IP-адрес*.
- ④ Нажимаем кнопку *OK*.

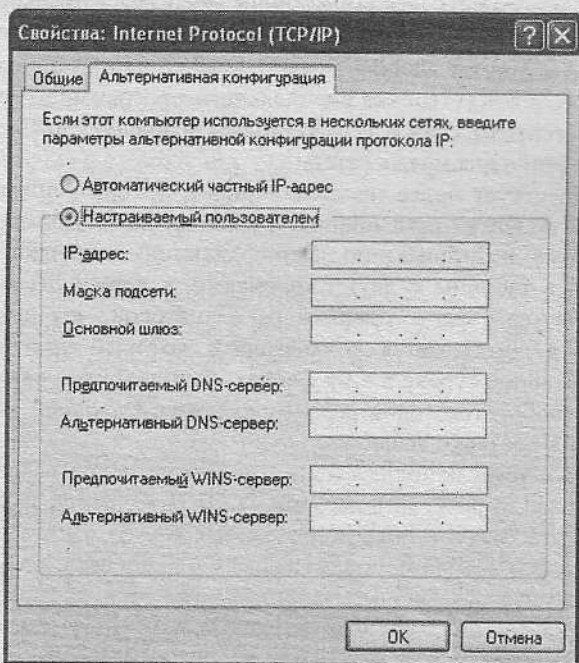


Рис. 18. Настройка альтернативных параметров TCP/IP

Кроме указания использования APIPA, на вкладке *Альтернативная конфигурация* вы можете вручную настроить параметры TCP/IP так же, как это делается при статической IP-адресации, однако эти настройки будут использоваться только тогда, когда в сети не будет присутствовать DHCP-сервер.

Например, для сети из пяти компьютеров вы можете использовать конфигурацию, которая приведена на рис. 13.

Имена компьютеров

Кроме IP-адреса, у каждого компьютера есть символьное имя, используя которое вы можете обращаться к требуемому компьютеру. Естественно, гораздо удобнее использование

имен, чем IP-адресов, поскольку имена легче в запоминании и они отражают владельца, местоположение или назначение компьютера.

Но возникает вопрос: как преобразовывать имена в IP-адреса и обратно? Для выполнения этого преобразования были созданы две системы – DNS (*Domain Name System*) и WINS (*Windows Internet Naming System*). Однако для их использования требуется установка специального программного обеспечения (серверы DNS и WINS), но это довольно сложная задача, особенно для малых сетей.

Существует более простой вариант, который применялся на заре развития сети Internet, а именно: использование файлов **hosts** и **lmhosts.sam**. Эти файлы представляют собой обычные таблицы с двумя колонками, в первой из которых указывается IP-адрес компьютера, а во второй – его имя. Символом # обозначается комментарий, который принадлежит определенной строке в этих файлах. Файлы можно редактировать в любом текстовом редакторе, даже в *Блокноте*, который входит в поставку Windows.

Файл **hosts** используется компьютерами для разрешения DNS-имен, а файл **lmhosts.sam** – для разрешения имен Net-BIOS (для этого сейчас используется WINS). Для использования имен компьютеров, входящих в вашу сеть, потребуются изменить эти файлы. Например, для сети, которая представлена на рис. 13, эти файлы будут иметь следующее содержимое:

127.0.0.1	localhost	#PRE	
192.168.1.1	PC1	#PRE	#Компьютер 1
192.168.1.2	PC2	#PRE	#Компьютер 2
192.168.1.3	PC3	#PRE	#Компьютер 3
192.168.1.4	PC4	#PRE	#Компьютер 4
192.168.1.5	PC5	#PRE	#Компьютер 5

Здесь расширение #PRE означает, что данная запись будет загружена в буфер имен при запуске системы, и при обращении к какому либо компьютеру по имени будет происходить разрешение с использованием буфера, а не широковещательной рассылки запросов. Также каждый IP-адрес должен быть отделен от имени компьютера по крайней мере одним пробелом, однако для удобства можно использовать или несколько пробелов, или символ табуляции.

Для того чтобы все компьютеры могли «общаться» используя имена, необходимо, чтобы эти файлы (естественно, с требуемым содержимым) присутствовали на каждом компьютере. Именно это и делает неудобным применение такого подхода в разрешении имен. При добавлении нового компьютера в сеть вам придется вносить изменения в файлы **hosts** и **lmhosts.sam** на всех компьютерах, что является довольно трудоемкой задачей. Однако если компьютеры в сеть добавляются редко, то использование и поддержка этих файлов является более простой задачей, чем настройка и управление серверами DNS и WINS (см. главу 4).

Итак, для добавления нового сопоставления имени и IP-адреса компьютера вы должны выполнить следующие действия.

- ① Найти на диске компьютера файл **lmhosts.sam**. Для Windows 98 он находится в папке **C:\Windows**, а для Windows 2000 или Windows XP – в папке **C:\Windows\system32\drivers\etc**.
- ② Затем открыть файл двойным щелчком.
- ③ При вопросе системы, какую программу использовать для открытия файла, вы должны указать *Блокнот*.
- ④ В последней строке файла требуется указать IP-адрес нового компьютера, нажать клавишу **Пробел** или **Tab** и ввести имя.
- ⑤ При необходимости можно указать комментарий к строке, отделив его от имени с помощью знака **#**.
- ⑥ После внесения изменений следует сохранить файл и закрыть *Блокнот*.

Как проверить наличие связи

После настройки всех компьютеров, входящих в вашу сеть, нужно проверить наличие связи между ними и правильность настройки сетевых протоколов. При создании сети возможен ряд ошибок, которые приводят к тому, что компьютеры не могут взаимодействовать. К таким ошибкам относятся:

- некорректная установка драйверов сетевой карты;
- неправильная работа сетевых протоколов или их некорректная настройка;
- назначение ошибочного IP-адреса или маски подсети;
- физическое повреждение кабеля.

ПРОВЕРКА СЕТЕВОЙ КАРТЫ

– Первое, что вы должны сделать, – это проверить правильность установки и настройки драйверов сетевой карты. Если вы используете Windows XP или Windows 2000, то нужно выполнить следующие действия.

- ① Открыть Панель управления и выбрать пункт *Система*.
- ② В открывшемся окне *Свойства системы* перейти на вкладку *Оборудование*.
- ③ Нажать кнопку *Диспетчер устройств*, при этом будет открыто одноименное окно.
- ④ В окне *Диспетчера устройств* требуется раскрыть пункт *Сетевые платы (Networks adapters)* и убедиться, что около вашей платы не стоит значок с желтым восклицательным знаком.
- ⑤ Если значок с желтым восклицательным знаком присутствует, следует переустановить драйвер. Наиболее правильным является загрузка свежего драйвера с сайта производителя (это можно сделать в Internet-кафе или любом доступном для вас компьютере, подключенном к Internet).
- ⑥ Заменить сетевой адаптер, если переустановка драйвера не помогла избавиться от ошибки.

В том случае, если вы используете Windows 98, для вызова *Диспетчера задач* необходимо открыть окно свойств системы и просто перейти на вкладку *Устройства*. Остальные действия выполняются аналогично Windows XP.

ПРОВЕРКА НАСТРОЙКИ TCP/IP

Для проверки настройки протокола TCP/IP требуется выполнить следующие действия.

- ① Нажать на кнопку *Пуск* и выбрать команду *Выполнить*.
- ② В появившемся окне *Запуск программы* ввести команду **cmd** для Windows XP или **command** – для Windows 98. При этом будет отображено окно консоли.
- ③ Ввести команду **ipconfig /all** и нажать **Enter**. При выполнении команды вам будут показаны параметры текущей конфигурации TCP/IP (см. рис. 19).
- ④ Убедиться в правильности конфигурирования протокола TCP/IP путем сверки планируемых настроек с реальными.

- ⑤ Если настройки не совпадают, изменить их и выполнить процедуру проверки еще раз.

```

Microsoft Windows [XP] Версия 5.1.2600.1
(c) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Kl in>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : host
Основной DNS-сервис . . . . . : test.kart
Тип шлюза . . . . . : неизвестный
IP-адресация включена . . . . . : нет
DNS-прокси включен . . . . . : нет

Local Area Connection - Ethernet adapter:

DNS-сервис этого подключения . . . . . :
Описание . . . . . : Intel(R) PRO/100 Management Adapter
Физический адрес . . . . . : 00-02-83-06-52-00
Включен . . . . . : нет
IP-адрес . . . . . : 172.17.1.1
Маска подсети . . . . . : 255.255.0.0
Основной шлюз . . . . . :
ID-адрес DHCP . . . . . : N/A
  
```

Рис. 19. Использование утилиты Ipconfig

ПРОВЕРКА НАЛИЧИЯ ФИЗИЧЕСКОЙ СВЯЗИ

После проверки сетевых настроек вашего и остальных компьютеров, входящих в сеть, необходимо проверить, корректно ли работают коммутаторы и кабели. Основной ошибкой при работе с кабелем является его неправильное обжатие, которое ведет к невозможности передачи данных, или размещение рядом с источником сильных электромагнитных помех (например, силовым кабелем), которое вносит значительные искажения в сигнал, передаваемый по кабелю.

Для выполнения этой проверки следует использовать утилиту **ping**, которая проверяет правильность настройки TCP/IP и тестирует соединения с другими узлами. Ее принцип работы заключается в отправке небольших пакетов данных по указанному адресу. Существующие стандарты предполагают, что получив такой пакет, любое сетевое устройство должно отправить ответ на адрес источника. Если ответ не пришел в течение определенного времени, считается, что между двумя устройствами отсутствует линия связи.

Для использования утилиты **ping** вы должны выполнить следующие инструкции.

- ① Включить все компьютеры или хотя бы те, с которыми хотите проверить связь.
- ② Нажать кнопку *Пуск* и выбрать команду *Выполнить*.

- ③ В появившемся окне *Запуск программы* ввести команду **cmd** для Windows XP или **command** для Windows 98, после чего появится окно консоли.
- ④ Ввести команду **ping 127.0.0.1**, которая позволит протестировать корректность работы самой утилиты. Вы должны получить результаты, похожие на те, которые показаны на рис. 20.
- ⑤ Изменить адрес в команде на адрес компьютера, за которым сейчас находитесь, например **ping 192.168.1.1**. Этим вы еще раз проверите, насколько корректно работает сетевая карта.
- ⑥ Выполнить проверку целевого компьютера, например **ping 192.168.1.2**. Если вы получаете ответ, то все в порядке, если же получен ответ в виде *Превышен интервал ожидания для запроса*, то это говорит о неисправности кабеля или коммутатора.
- ⑦ Протестировать связь других компьютеров. Если связь существует, значит коммутатор работает, и причину отсутствия связи между вашим компьютером и другими следует искать в вашем кабеле.

```

C:\Documents and Settings\Kcin>ping 127.0.0.1
Обмен пакетами с 127.0.0.1 по 32 байт:
Ответ от 127.0.0.1: число байт=32 время(ТTL)=128
Ответ от 127.0.0.1: число байт=32 время(ТTL)=128
Ответ от 127.0.0.1: число байт=32 время(ТTL)=128
Ответ от 127.0.0.1: число байт=32 время(ТTL)=128

Статистика Ping для 127.0.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
    Приблизительное время приема-передачи в мс:
        Минимальное = 0 мсек, Максимальное = 0 мсек, Среднее = 0 мсек
C:\Documents and Settings\Kcin>
  
```

Рис. 20. Использование утилиты Ping

При использовании утилиты **ping** можно применять ключ **-t** (отделяется пробелом от команды **ping**), который позволяет отправлять в сеть неограниченное количество пакетов. Например, при выполнении команды **ping -t 192.168.1.2** будет происходить постоянная отправка пакетов, и вы можете обнаружить ситуацию, при которой появляется (или пропадает) связь.

Глава 4

Как использовать общие ресурсы

Из этой главы вы узнаете, как можно использовать дисковое пространство компьютеров, которые включены в локальную сеть.

Что такое сервер

Сервер (server) представляет из себя компьютер, разделяющий свои ресурсы с другими компьютерами сети, в первую очередь с рабочими станциями. *Рабочая станция (workstation)*, или *клиент*, использует ресурсы сервера. Рабочие станции имеют доступ к сетевым ресурсам, но своих ресурсов в общее пользование, как правило, не предоставляют.

В большинстве случаев сервер – это обычный компьютер, на котором установлено специальное программное обеспечение, в первую очередь серверная операционная система, например Windows Server 2003. Однако для построения небольшой сети (5–20 компьютеров) вам вполне хватит или Windows 2000 Professional, или Windows XP Professional. Эти системы полностью могут справиться с ролями файлового и принт-серверов.

РОЛИ СЕРВЕРА

В вашей сети будут существовать серверы, выполняющие различные роли. Ниже мы рассмотрим основные роли, которые назначаются серверам в большинстве сетей:

- *File server (Файловый сервер)* – предоставляет общий доступ к файлам и папкам системы, на которой активизирована данная роль;
- *Print server (Сервер печати)* – позволяет клиентам подключаться к принтеру, физически подключенному к компьютеру, которому назначена эта роль;
- *Application server (Сервер приложений)* – используется для хранения web-страниц, а также web-ориентированных приложений;
- *Mail server (Почтовый сервер)* – хранит электронные почтовые ящики пользователей и управляет корреспонденцией;

- *DNS server (DNS-сервер)* – разрешает DNS-имена компьютеров. Здесь под разрешением понимается процесс преобразования имени компьютера в IP-адрес;
- *Wins server (WINS-сервер)* – разрешает NetBIOS-имена компьютеров;
- *DHCP server (DHCP-сервер)* – распределяет IP-адреса из заранее выделенной области;
- *Streaming media server (Сервер потоков мультимедиа)* – направляет потоки аудио- и видеоданных клиентам через Internet или локальную сеть.

Естественно, существуют и другие роли, такие как *Terminal server (Сервер терминалов)*, *Remote access/VPN server (Сервер удаленного доступа и ВЧС)*, *Domain controller (Контроллер домена)*, однако в домашней локальной сети они используются редко.

Учетные записи пользователей

Как вы уже знаете, любой компьютер может быть как клиентом, так и сервером. Но всегда возникает вопрос, как может клиент получить доступ к серверу и какими правами клиент при этом будет обладать. Например, кто имеет право изменять файлы, которые находятся на другом компьютере, а кто может только просматривать их содержимое. Все привилегии и запреты назначаются для пользователей, которые представлены в системе в виде учетных записей.

Учетная запись представляет собой набор некоторых атрибутов, таких как имя и пароль, права доступа и разрешения, а также настройки системы. Кроме этого, система позволяет сохранить настройку цветовой схемы, специальных возможностей, другие пользовательские параметры, привязав их к учетной записи пользователя и храня их в профиле пользователя. *Профиль пользователя* представляет набор каталогов, в которых хранятся его документы и настройки.

Когда при входе в систему пользователь сообщает свое имя, Windows настраивает компьютер в соответствии с заданными им параметрами. Кроме этого, система позволяет настроить разрешения для каждого пользователя. Это означает, что пользователи, которые принадлежат к группе административной,

торов, будут иметь полный контроль над компьютером, а остальные будут ограничены в правах.

Кроме этого, имя пользователя и пароль, которые однозначно идентифицируют пользователя и его учетную запись, используются для доступа к различным ресурсам как отдельного компьютера, так и сетевых ресурсов.

Теперь перейдем к рассмотрению типов учетных записей. В Windows XP, так же как и в Windows 2000, существует несколько типов учетных записей, которые отличаются набором привилегий, однако наиболее часто используются два типа учетных записей: учетные записи администраторов компьютера и учетные записи с ограниченными правами. Также существуют две учетные записи, которые создаются при установке системы на диск компьютера и которые невозможно удалить из списка учетных записей компьютера. Это учетные записи *Администратор* (*Administrator*) и *Гость* (*Guest*). Пользователь, который регистрируется в системе под учетной записью *Администратор*, является хозяином компьютера и имеет неограниченные права при работе с системой. Учетная запись *Гость* предназначена для пользователей, не имеющих собственных учетных записей на компьютере.

УЧЕТНАЯ ЗАПИСЬ АДМИНИСТРАТОРА

Учетная запись администратора компьютера предназначена для тех, кто должен иметь право вносить изменения на уровне системы, устанавливать программы и иметь доступ ко всем файлам на компьютере. Пользователь с учетной записью администратора имеет полный доступ к другим учетным записям пользователей на компьютере. Также пользователь с учетной записью администратора:

- может создавать и удалять учетные записи пользователей на компьютере;
- может создавать пароли для других пользователей компьютера;
- может изменять в учетных записях полные имена пользователей, рисунки, пароли и типы учетных записей;
- не может изменить тип своей учетной записи на ограниченную в случае, когда на компьютере больше нет пользователей с учетной записью администратора компьютера. Таким образом обеспечивается наличие на компьютере по крайней мере одного пользователя с учетной записью администратора.

Учетная запись *Администратор* создается автоматически в процессе установки Windows 2000/XP. Эта учетная запись с полномочиями администратора компьютера использует пароль, который был задан во время установки. Если в системе существует еще хотя бы один пользователь с правами администратора, в окне приветствия отсутствует кнопка, позволяющая зарегистрироваться используя учетную запись *Администратор*, однако для того чтобы получить к ней доступ, необходимо дважды нажать комбинацию клавиш **Ctrl+Alt+Del**. При этом появится диалоговое окно, в котором следует в строке «Имя пользователя» указать слово «Администратор», а в строке «Пароль» – пароль доступа к учетной записи *Администратор*, который был задан при установке системы.

УЧЕТНАЯ ЗАПИСЬ С ОГРАНИЧЕННЫМИ ПРАВАМИ

Учетная запись с ограниченными правами предназначена для пользователей, которым должно быть запрещено изменение большинства настроек компьютера и удаление важных файлов. Пользователь с учетной записью с ограниченными правами:

- не может устанавливать программы и оборудование, но имеет доступ к уже установленным на компьютере программам;
- может изменять собственный рисунок, назначенный учетной записи, а также создавать, изменять или удалять собственный пароль;
- не может изменять имя или тип собственной учетной записи. Такие изменения должны выполняться пользователем с привилегиями администратора компьютера.

Некоторые программы могут работать неправильно для пользователей с ограниченными правами. В таком случае следует временно или навсегда изменить тип учетной записи на администратора компьютера.

УЧЕТНАЯ ЗАПИСЬ ГОСТЯ

В том случае, если пользователь не имеет учетной записи на компьютере, он может работать на нем, используя учетную запись гостя. Данная учетная запись позволяет быстро войти в систему для проверки электронной почты или просмотра ресурсов Internet. Пользователь, вошедший с учетной записью гостя:

- не может устанавливать программы и оборудование, но имеет доступ к уже установленным на компьютере программам;
- не может изменить тип учетной записи гостя;
- может изменить рисунок учетной записи гостя.

► **ПРИМЕЧАНИЕ.** Вы должны помнить, что для подключения к другому компьютеру (серверу), на котором находятся интересующие вас файлы, необходимо обладать учетной записью на удаленном компьютере. При попытке подключения клиент, т.е. ваш компьютер, отправляет на сервер имя вашей учетной записи и пароль. Если такая учетная запись на сервере существует, то клиент получает доступ к нему (при этом, естественно, обладая какими-то правами и привилегиями). Если же на сервере нет указанной учетной записи, сервер предлагает ввести другое имя пользователя и пароль. Если вы его не знаете, то не сможете подключиться к серверу.

Таким образом, если вы хотите иметь доступ ко всем компьютерам в вашей сети, вы должны создать свою учетную запись на каждом компьютере.

СОЗДАНИЕ УЧЕТНОЙ ЗАПИСИ

Для создания новой учетной записи в Windows XP выполняем следующие действия.

- ① Открываем Панель управления и выбираем пункт *Учетные записи пользователей*. В появившемся окне (см рис. 21) вы можете видеть набор команд (заданий) и кнопки для перехода к администрированию уже существующих учетных записей.
- ② Выбираем команду *Создание учетной записи*.
- ③ В появившемся окне указываем имя создаваемой учетной записи (см. рис. 22), и нажимаем кнопку *Далее*.
- ④ В следующем окне указываем тип учетной записи (см. рис. 23). Затем нажимаем кнопку *Создать учетную запись*, в результате чего в локальной базе безопасности будет сделана соответствующая запись.

В дальнейшем при загрузке операционной системы в окне приветствия будет присутствовать пункт с именем созданной учетной записи.

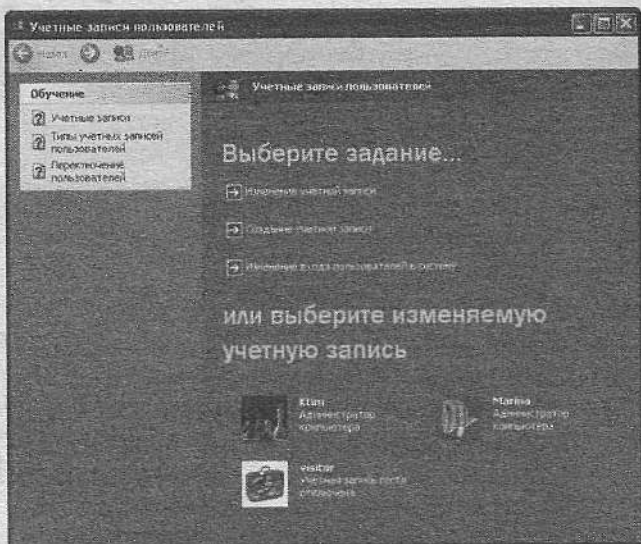


Рис. 21. Диалоговое окно управления учетными записями

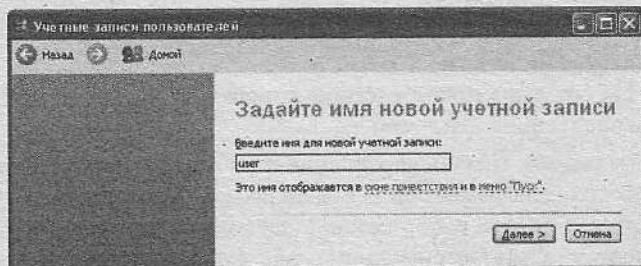


Рис. 22. Создание учетной записи. Ввод имени

Параметры созданной учетной записи можно изменять. Для этого вы должны выбрать учетную запись в окне *Учетные записи пользователей* (см. рис. 21), в результате чего будет открыто окно, показанное на рис. 24.

Команда *Изменение имени* открывает диалоговое окно, аналогичное окну, представленному на рис. 22, в котором можно указать новое имя учетной записи, а точнее – имя, которое будет использоваться в меню *Пуск* и на Экране приветствия. На самом же деле имя, которое было введено при создании учетной записи, изменено не будет.

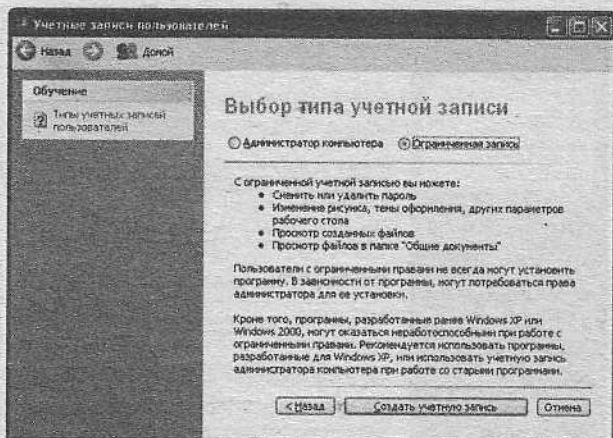


Рис. 23. Создание учетной записи. Выбор типа учетной записи

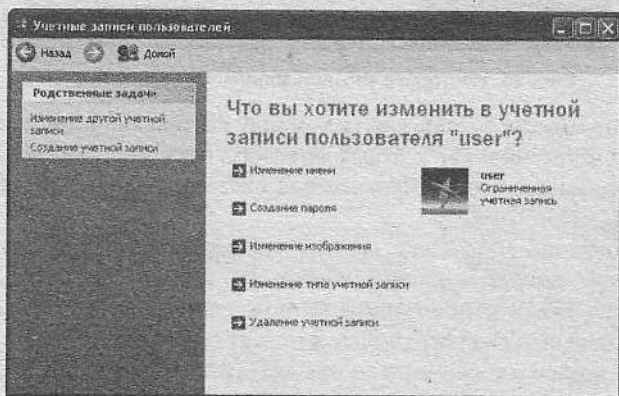


Рис. 24. Настройка учетной записи

Команда *Создание пароля* позволяет вам защитить учетную запись и не допустить входа в систему или подключения к компьютеру неавторизованным пользователям. Пароль является очень важным атрибутом любой учетной записи и должен обязательно присутствовать в ней. Другими словами, вы должны обязательно устанавливать пароль. При вызове команды открывается диалоговое окно, показанное на рис. 25, в котором необходимо дважды ввести пароль для исключения опечатки, а также указать слово или фразу-подсказку, которая напомнит пароль в том случае, если вы его забудете.

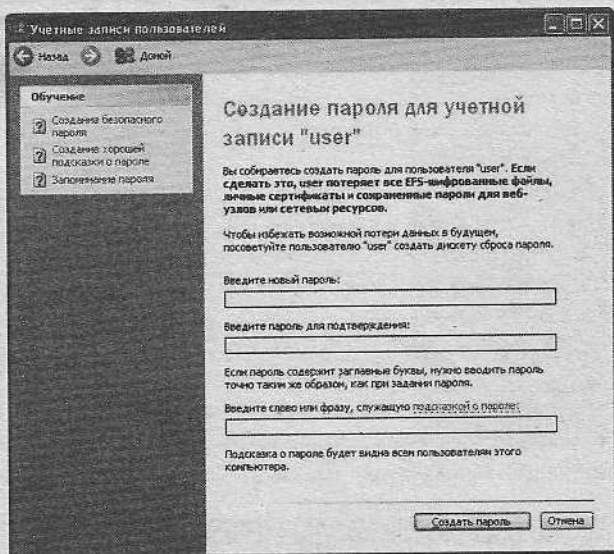


Рис. 25. Настройка учетной записи. Создание пароля

Вы можете использовать команду *Изменение изображения* для смены иконки, которая соответствует учетной записи и отображается в окне приветствия системы, а также в верхней части меню *Пуск*.

Команда *Изменение типа учетной записи* позволяет вам открыть диалоговое окно, показанное на рис. 23, и переопределить тип учетной записи. В том случае, если изначально пользователь был ограничен в правах, изменить тип его учетной записи может только пользователь с учетной записью администратора.

Используя команду *Удаление учетной записи*, вы можете удалить запись пользователя. При этом можно сохранить все файлы, с которыми работал пользователь.

Что такое группа пользователей

Группа является объединением учетных записей пользователей. Она упрощает управление пользователями, поскольку позволяет назначить права и разрешения нескольким пользователям одновременно. В противном случае назначение прав надо выполнять индивидуально для каждого пользователя.

Например, если вам необходимо предоставить доступ к сетевому ресурсу нескольким пользователям, то гораздо удобнее объединить этих пользователей в группу, а потом назначить ей право доступа, чем определять право доступа для каждого пользователя.

Разрешения и права определяют, какие действия пользователь может выполнить с объектом (например, с файлом, папкой или принтером). Когда назначаются разрешения, тем самым определяются права доступа к объекту и их тип. Например, если нескольким пользователям необходимо считывать какой-либо файл, можно объединить их учетные записи в группу и назначить группе разрешения на чтение файлов.

Права позволяют пользователям выполнять различные системные операции, такие как изменение времени в системе или архивировании данных.

В Windows XP существуют встроенные группы, которые используются для назначения прав пользователям (см. табл. 8).

Таблица 8

Встроенные локальные группы и их права

Локальные группы	Описание
Администраторы (Administrators)	Могут выполнять любые административные задачи. По умолчанию в группу входит учетная запись Администратор (Administrator)
Операторы Архива (Backup Operators)	Члены этой группы могут использовать Windows Backup для архивирования и восстановления данных
Гости (Guests)	Могут выполнять только те задачи, которые разрешены администратором. Имеют доступ только к тем ресурсам, для которых установлены соответствующие разрешения. По умолчанию в группу включена учетная запись Гость (Guest)
Опытные пользователи (Power Users)	Могут создавать и изменять учетные записи, а также открывать ресурсы
Пользователи (Users)	Могут выполнять только те задачи, для которых явно заданы разрешения. Имеют доступ только к тем ресурсам, для

Локальные группы	Описание
	<p>которых установлены соответствующие разрешения. По умолчанию при создании учетной записи пользователя она помещается в эту группу</p>
Репликатор (Replicator)	Выполняют операции реплицирования в домене

ВСТРОЕННЫЕ СИСТЕМНЫЕ ГРУППЫ

Встроенные системные группы существуют на всех компьютерах, работающих под управлением Windows XP. Они не имеют специфических пользователей, но могут содержать различные учетные записи в различное время, в зависимости от того, каким образом пользователь получает доступ к ресурсам компьютера. Например, группа *Все (Everyone)* является встроенной группой Windows XP.

Настройка каталога для общего использования

Основным назначением локальной сети является обеспечение информационного обмена между пользователями, а как известно, вся информация представлена в файлах. В связи с этим необходимо научиться предоставлять доступ к файлам, которые нужны пользователям, и разделять права доступа.

Например, вам требуется создать каталог, в котором пользователи других компьютеров могли бы хранить свои файлы. Для этого, во-первых, необходимо настроить Проводник с целью обеспечения более комфортной работы (только в том случае, если вы используете Windows XP). Настройка заключается в снятии всего одного флажка путем выполнения перечисленных ниже действий:

- ① Запускаем Проводник.
- ② В меню *Сервис* выбираем команду *Свойства папки*.
- ③ Переходим на вкладку *Вид* (см. рис. 26).
- ④ Снимаем флажок *Использовать простой общий доступ к файлам*.
- ⑤ Нажимаем *ОК*.

Теперь можно приступить к созданию папки и предоставлению общего доступа к ней.

Для этого выполняем следующие действия.

- 1) Запускаем Проводник и находим папку, к которой будем предоставлять доступ другим пользователям сети. Если такой папки нет, вы можете ее создать.
- 2) Щелкаем правой кнопкой мыши на папке и в появившемся контекстном меню выбираем команду *Свойства*.
- 3) Переходим на вкладку *Доступ* (см. рис. 27).
- 4) Устанавливаем переключатель в положение *Открыть общий доступ к этой папке*.
- 5) Указываем максимальное число подключений к данному каталогу, используя переключатель *Предельное число пользователей*. Заметим, что для не серверных систем максимальное число ограничено десятью подключениями, т.е. одновременно к ресурсу могут быть подключены не более десяти пользователей, даже если переключатель установлен в положение *максимально возможное*.
- 6) Нажимаем кнопку *ОК*.

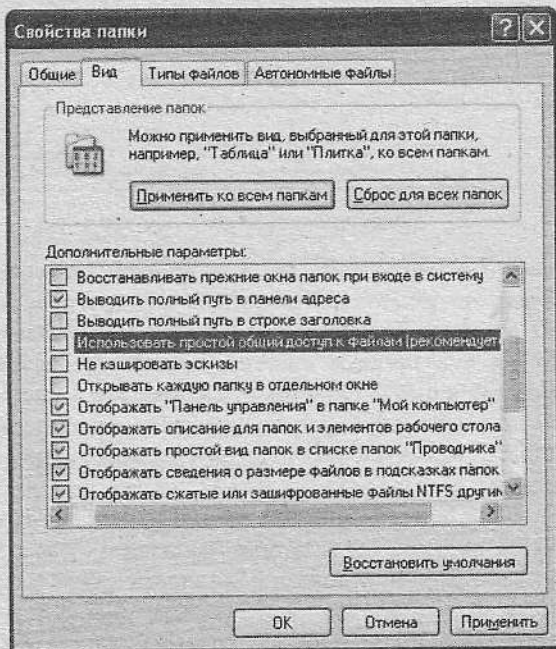


Рис. 26. Настройка Проводника

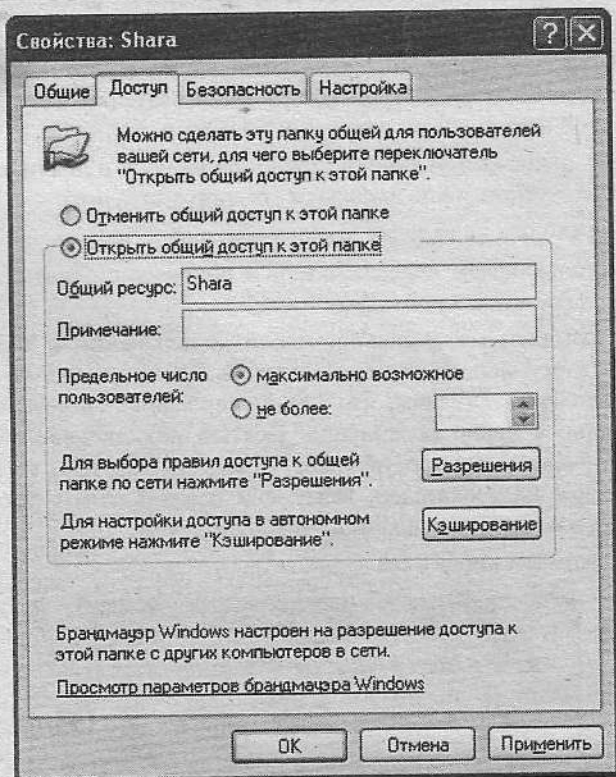


Рис. 27. Предоставление общего доступа к папке

Однако и после предоставления общего доступа данный каталог все еще не может использоваться другими пользователями. Связано это с тем, что мы не определили права доступа. Поэтому и возникают ошибки, показанные на рис. 28 и рис. 29, когда клиент пытается подключиться к папке, находящейся на компьютере, работающем под управлением Windows 2000/XP. Следует заметить, что в первом случае (Windows XP) пользователь все же может указать имя пользователя и пароль и получить доступ к каталогу. А вот пользователь Windows 98 не имеет даже этой возможности, поскольку его имя, пересылаемое при попытке установки связи с сервером, отвергается и клиентская система немедленно возвращает пользователю ошибку, не давая возможности указать другое имя.

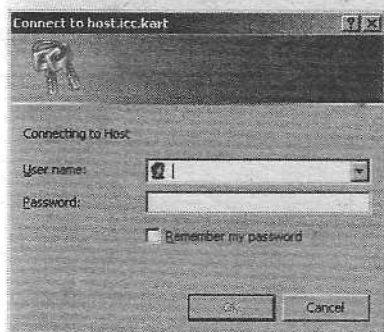


Рис. 28. Попытка доступа к папке из Windows XP

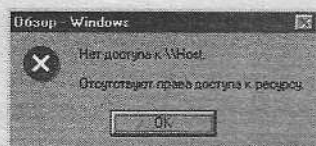


Рис. 29. Попытка доступа к папке из Windows 98

Как настроить разрешения для файлов

Решение указанной выше проблемы заключается в создании учетных записей для пользователей и групп, которые желают подключаться к вашей системе (см. выше) и назначении им соответствующих разрешений.

Применяются следующие типы разрешений доступа к общим папкам или дискам:

Чтение (Read) – назначается группе *Все (Everyone)* по умолчанию и позволяет:

- просматривать имена файлов и подкаталогов;
- просматривать данные в файлах;
- выполнять программные файлы;

Изменение (Change) – никогда не назначается группам по умолчанию. Включает все функции разрешения *Чтение*, а также позволяет:

- добавлять файлы и подпапки;
- изменять данные в файлах;
- удалять подпапки и файлы;

Полный доступ (Full Control) – по умолчанию назначается группе *Администраторы* на локальном компьютере. Разрешение *Полный доступ* включает разрешения *Изменение* и *Чтение*, а также позволяет изменять разрешения (только для файлов и папок, которые находятся на диске, имеющем файловую систему NTFS) и назначать владельцев папок и файлов.

Для настройки разрешений необходимо выполнить сле-

дующие операции.

- ① Открыть окно свойств папки.
- ② Перейти к вкладке *Доступ* (см. рис. 27).
- ③ Нажать кнопку *Разрешения*, после чего будет отображено окно, показанное на рис. 30.

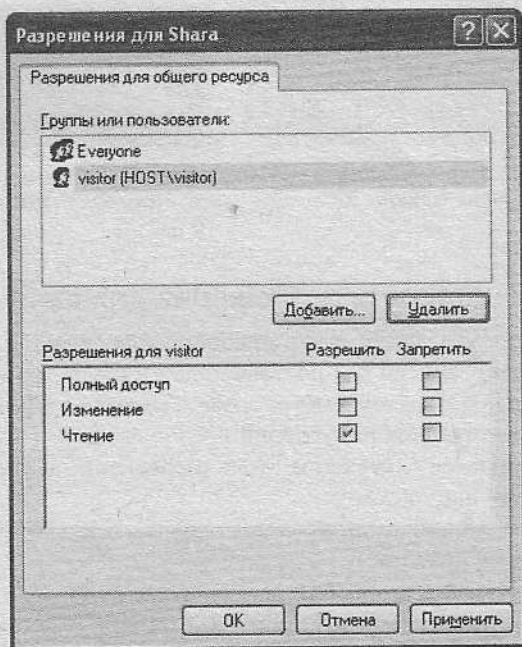


Рис. 30. Разрешения общего доступа для выбранного каталога

В данном окне отображается информация о пользователях и группах, которые имеют право подключаться к данному ресурсу, а также о тех правах, которыми они обладают.

Для добавления нового пользователя и назначения ему определенных разрешений вы должны выполнить следующие действия.

- ① Создать учетную запись для данного пользователя, как это описывалось выше.
- ② В окне *Разрешения для папки* нажать кнопку *Добавить*.
- ③ В появившемся окне (см. рис. 31) ввести имя пользователя, которому вы хотите предоставить доступ, и нажать кнопку

Проверить имена. Если ошибки в имени нет, система допишет к имени пользователя имя компьютера (как показано на рис. 31).

④ Нажать *ОК*.

После выполнения данной процедуры в окне *Разрешения для папки* появится имя пользователя. Выделив его, вы сможете назначить этому пользователю разрешения доступа к каталогу.

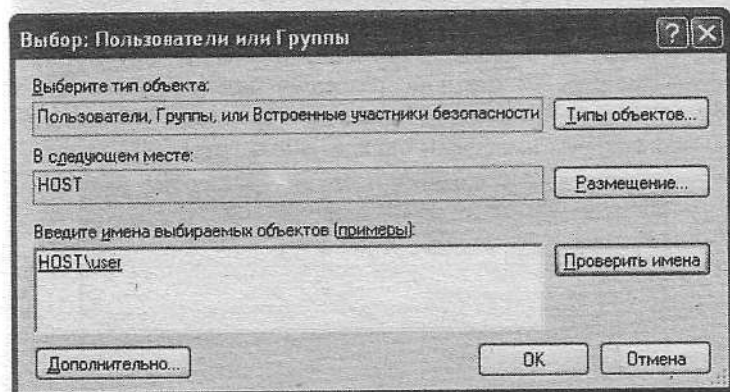


Рис. 31. Выбор пользователя

Безопасность папок

Кроме разрешений для общих ресурсов, вы можете столкнуться с еще одной проблемой, которая выглядит следующим образом: вы создали общий ресурс, назначили права общего доступа для определенного пользователя (например, *Полный доступ*), однако пользователь сообщает вам, что при попытке изменения файла, созданного другим пользователем, система возвращает отказ в виде *Невозможно создать файл (Cannot create a file)* или *Доступ запрещен (Access denied)*.

Связано это с тем, что логический диск, на котором находится общий ресурс, скорее всего, использует файловую систему NTFS, которая обеспечивает повышенный уровень безопасности для файлов и папок. NTFS имеет собственные разрешения, которые позволяют обеспечить безопасность данных на уровне диска. Иначе говоря, контроль за доступом к данным

осуществляется на основе *Списков контроля доступа (Access Control List)*, которые присутствуют в каждом каталоге и опираются на учетные записи пользователей. Эти списки контроля доступа являются частью логического диска и не принадлежат операционной системе, хотя могут изменяться пользователем посредством операционной системы.

Существует возможность назначать NTFS-разрешения для папок и файлов, в то время как разрешения для общих ресурсов можно назначить только для папок.

Чтобы увидеть NTFS-разрешения, вы должны открыть диалоговое окно свойств папки и перейти на вкладку *Безопасность* (см. рис. 32). Как и для разрешений общего ресурса (см. рис. 30), здесь представлены различные пользователи и группы, для которых назначены определенные разрешения.

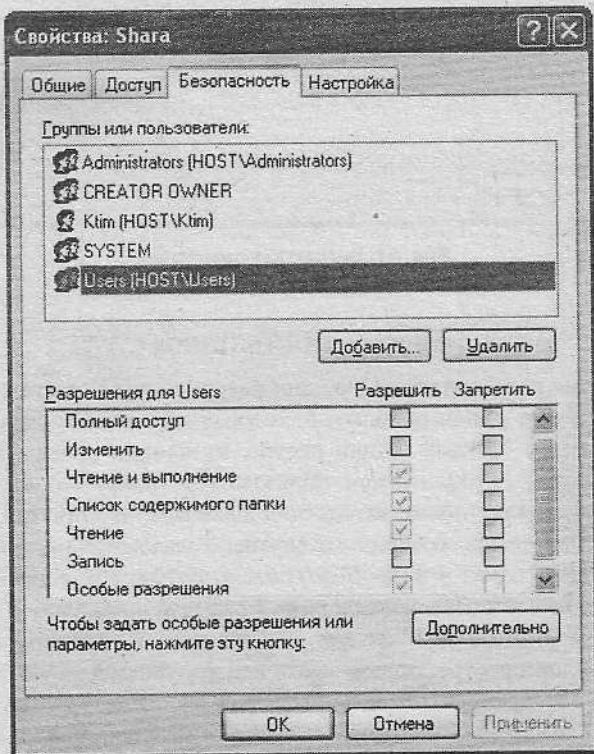


Рис. 32. NTFS-разрешения для папки

Например, из рис. 32 вы можете видеть, что группа пользователей *Users (Пользователи)* обладает правами на чтение файлов, а также особыми разрешениями. Если с правами на чтение все понятно, то что же такое особые разрешения? Они позволяют выполнять особые действия в данном каталоге. В нашем примере группа *Users (Пользователи)* имеет право чтения всех файлов, находящихся в каталоге, однако благодаря особым разрешениям члены этой группы могут создавать в этом каталоге новые файлы и папки и изменять их. Но изменять чужие папки и файлы, владельцами которых они не являются, членами группы *Users (Пользователи)* не могут. Владелец, то есть пользователь, который создал папку или файл, может выполнять с ними любые действия, вплоть до удаления объекта.

Чтобы просмотреть особые разрешения, вы должны на вкладке *Безопасность* окна *Свойства папки* нажать кнопку *Дополнительно*. При этом будет отображено окно *Дополнительные параметры безопасности для папки* (см. рис. 33).

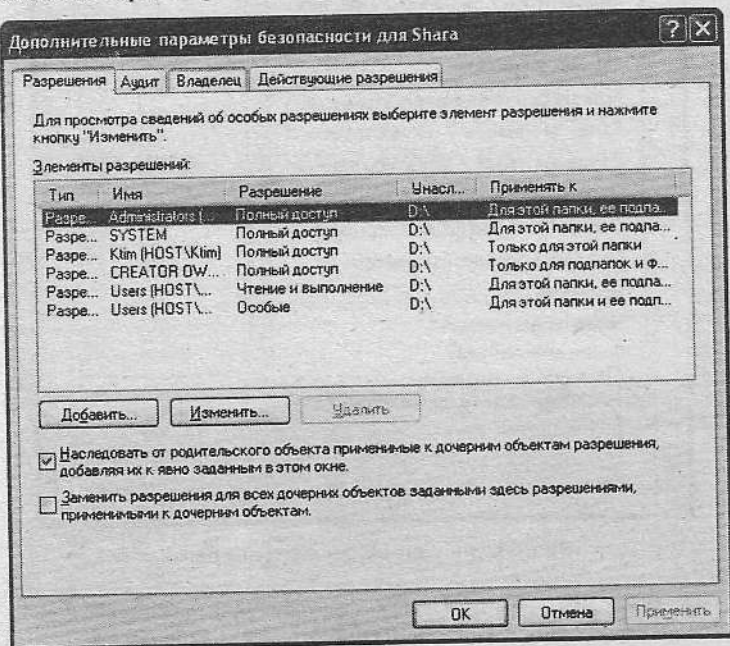


Рис. 33. Дополнительные NTFS-разрешения для папки

В данном окне отображаются элементы разрешений для папки, при этом вы можете добавлять новые разрешения, удалять старые, а также изменять существующие. Например, при выделении для группы *Users* (*Пользователи*) элемента разрешения *Особые* и его изменении было открыто окно (см. рис. 34), в котором указано, что пользователи данной группы могут создавать файлы и папки, а также изменять их.

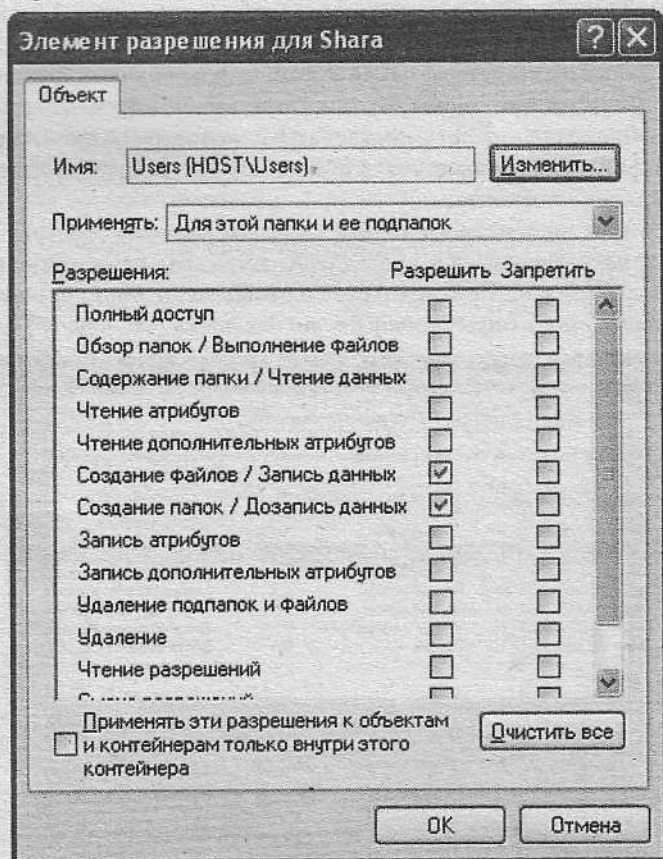


Рис. 34. Элемент разрешения для папки

Разрешения, которые вы можете назначать файлам и папкам, перечислены в табл. 9 и табл. 10. Эти разрешения можно назначать на вкладке *Безопасность* окна свойств файла или папки.

Таблица 9

NTFS-разрешения для папок

Разрешения	Описание
Чтение (Read)	Позволяет просматривать файлы и папки внутри каталога, а также сведения о владельце, разрешения и атрибуты (например, Read-Only, Hidden, Archive и System)
Запись (Write)	Позволяет создавать новые файлы и папки в каталоге, изменять атрибуты, а также просматривать сведения о владельце и разрешения
Список содержимого папки (List Folder Contents)	Разрешает просматривать имена файлов и папок, находящихся в каталоге
Чтение и выполнение (Read & Execute)	Объединяет разрешения Read (Чтение) и List Folder Contents (Список содержимого папки), а также позволяет «проходить» через папку и получать доступ к другим папкам и файлам, даже если явно не указаны права доступа к этим папкам
Изменение (Modify)	Объединяет разрешения Write (Запись) и Read & Execute (Чтение и выполнение), а также позволяет удалять папку
Полный доступ (Full Control)	Позволяет изменять разрешения, назначать владельца, удалять папки и файлы и выполнять операции, допустимые всеми остальными разрешениями

Таблица 10

NTFS-разрешения для файлов

Разрешения	Описание
Чтение (Read)	Позволяет просматривать файл, а также сведения о владельце, разрешения и атрибуты (например, Read-Only, Hidden, Archive и System)
Запись (Write)	Позволяет изменять файлы, изменять атрибуты, а также просматривать сведения о владельце и разрешения
Чтение и выполнение (Read & Execute)	Позволяет запускать приложения, просматривать файл, сведения о владельце, разрешения и атрибуты (например, Read-Only, Hidden, Archive и System)

Разрешения	Описание
Изменение (Modify)	Объединяет разрешения Write (Запись) и Read & Execute (Чтение и выполнение), а также позволяет удалять файл
Полный доступ (Full Control)	Позволяет изменять разрешения, назначать владельца, удалять файлы и выполнять операции, допустимые всеми остальными разрешениями

В том случае, если вы хотите удалить какое-либо разрешение, вы должны снять флажок в соответствующем пункте диалогового окна свойств папки или файла, однако и здесь существует «подводный камень».

По умолчанию разрешения, которые определены для родительского каталога, наследуются всеми объектами, которые находятся в нем. Следовательно, если для диска (или папки) заданы разрешения только на чтение файлов, то и все папки, которые находятся на этом диске, также будут иметь эти разрешения. Это значит, что вы не сможете просто изменить параметры доступа к файлам и папкам, — сначала необходимо отменить наследование разрешений. При отмене наследования папки становятся новыми родительскими папками и вложенные папки будут теперь наследовать другие разрешения.

Для отмены наследования необходимо снять флажок *Наследовать от родительского объекта* в окне *Дополнительные параметры безопасности для папки* (см. рис. 33). При снятии флажка вы можете или скопировать существующие разрешения, а потом отредактировать их, или удалить существующие и назначить новые. В том случае, если вы удалите разрешения для файла или папки и не назначите новые, никто не сможет получить доступ к данному объекту, даже вы. Единственным выходом из этой ситуации является назначение разрешений.

Алгоритм ваших действий

Итак, для обеспечения возможности подключения пользователя к сетевым ресурсам необходимо выполнить изложенные ниже инструкции.

- ① Узнать имя учетной записи и пароль, который использует (или хочет использовать) человек, желающий подключиться

к вашему компьютеру. В случае с Windows 98 необходимо, чтобы это имя пользователя и пароль полностью совпадали с теми, которые применяются пользователем на своем компьютере.

- ② Создать на вашем компьютере учетную запись с теми именем и паролем, которые вы получили.
- ③ Создать ресурс, который будет предназначен для общего использования, и настроить разрешения для пользователей.
- ④ Настроить безопасность папок, с тем чтобы пользователи вашей сети даже случайно не смогли удалить или изменить файлы в общих папках.

В большинстве случаев вы должны устанавливать доступ к объектам только для чтения данных.

Глава 5

Общение в локальной сети

Из этой главы вы узнаете, какие программы можно использовать для онлайн-общения, а также научитесь устанавливать сервер электронной почты, который позволит вам обмениваться электронной корреспонденцией.

Network Assistant

Одной из самых удобных, функционально богатых и поэтому популярных является программа Network Assistant компании Gracebyte Software (<http://www.gracebyte.com>). Эта программа специально разрабатывалась для малых домашних или офисных сетей, а поэтому она не использует выделенного сервера, что является очень большим преимуществом.

Демо-версию программы можно загрузить с официального сайта компании, однако без регистрации программа работает только 30 дней.


Для загрузки и установки программы вам необходимо выполнить следующие действия.

- ① Обратиться по адресу в сети Internet <http://www.gracebyte.com/nassi/files/nassi.zip>.
- ② Сохранить на диске файл **nassi.zip**.
- ③ Используя архиватор WinZip или WinRAR, распаковать архив в папку.
- ④ После распаковки запустить файл **nassi.exe**.
- ⑤ Следовать инструкциям программы.

После установки программы вы сможете запустить ее, используя главное меню кнопки *Пуск*.

ИНТЕРФЕЙС ПРОГРАММЫ

Первое, что желательно сделать при первом запуске программы, это выбрать русский язык (*Russian*) в меню *Language* (*Язык*) и перезапустить программу. Теперь для вывода всех меню, подписей кнопок и т.д. программа использует русский язык.

Интерфейс программы показан на рис. 35. Также программа представлена иконкой в области уведомлений Windows .

которую удобно использовать для выполнения наиболее часто вызываемых действий.

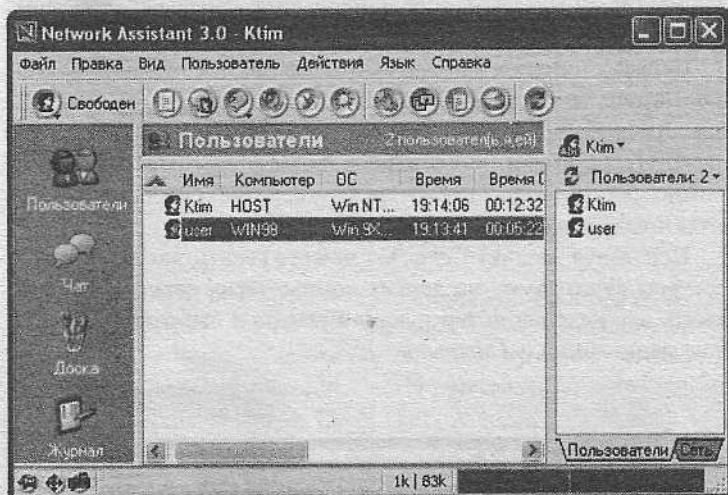


Рис. 35. Главное окно Network Assistant

Слева в окне расположена *Панель режимов*, где вы можете выбрать один из режимов работы:

- *Пользователи* – в данном режиме вы можете пригласить пользователя поучаствовать с вами в беседе (чате), оповестить пользователей о своем появлении звуковым сигналом, который передается на другие компьютеры. Также можно просмотреть список программ, которые запущены на компьютере пользователя, или увидеть его Рабочий стол;
- *Чат* – данный режим используется непосредственно для общения пользователей;
- *Доска* – в этом режиме любой пользователь программы может нарисовать на виртуальной доске любой рисунок, и он будет сразу же отображен на экранах других пользователей программы;
- *Журнал* – в журнал записываются системные события программы, такие как время старта программы, используемая технология связи и другие технические сведения.

Центральная часть окна программы зависит от выбранного режима. Здесь отображается или список пользователей (ре-

жим *Пользователи*), или поля полученных и отправленных сообщений (режим *Чат*), или полотно, на котором можно рисовать (режим *Доска*), или список системных событий программы (режим *Журнал*).

Справа отображается панель *Контакты*, в которой присутствуют имена пользователей (вкладка *Пользователи*) (см. рис. 36), или перечень компьютеров (вкладка *Сеть*) (см. рис. 37). Если щелкнуть на имени пользователя, будет открыто окно, которое можно использовать для отправки коротких сообщений, при этом новый канал создаваться не будет.

Используя вкладку *Сеть*, вы можете узнать, какие открытые ресурсы существуют на других компьютерах сети, а также открыть их, выделив интересующий ресурс и выбрав в контекстном меню команду *Открыть*.



Рис. 36. Панель *Контакты*.
Вкладка *Пользователи*

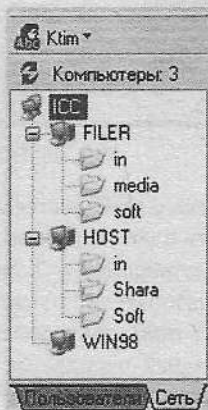



Рис. 37. Панель *Контакты*.
Вкладка *Сеть*

Кнопка  позволяет обновить списки пользователей и компьютеров с целью обнаружения подключившихся пользователей.



РЕЖИМ ПОЛЬЗОВАТЕЛИ

Этот режим показывает, какие пользователи находятся сейчас в сети; их имена; имена компьютеров, за которыми они работают, а также используется для отображения другой информации. Практически все действия, которые вы можете выполнить по отношению к другому пользователю, вынесены на панель инструментов *Пользователи* (см. табл. 11).

Таблица 11

Кнопки панели инструментов Пользователи

Кнопка	Название	Описание
 Свободен	Статус	Используется для изменения статуса. Можно выбрать режим <i>Играю</i> , <i>Работаю</i> или другой, соответствующий вашему текущему занятию. В зависимости от выбранного режима меняются способы оповещения пользователя о событиях в программе
	Сообщение	Используется для отправки короткого сообщения адресатам
	Секретный чат	Позволяет пригласить выбранного пользователя в приватный чат, который будет доступен только вам двоим
	Подключиться к каналу чата	Позволяет подключиться к уже существующему каналу чата
	Сигнал	Отправляет звуковое сообщение выбранному пользователю. Этим сообщением вы можете оповестить пользователя о своем возвращении в чат. Естественно, у вашего собеседника должна быть включена акустическая система
	Отправить файл	Открывает окно передачи файла выбранному пользователю
	Сигнализаторы	Позволяет настроить оповещения при возникновении различных событий
	Просмотр процессов	Отображает окно с перечнем процессов (программ), которые запущены на компьютере выбранного пользователя
	Просмотр копии экрана	Отображает окно с содержимым экрана выделенного пользователя

Кнопка	Название	Описание
	Просмотр буфера обмена	Отображает окно с содержимым буфера обмена выбранного пользователя
	Просмотр статистики	Показывает статистику по выделенному пользователю: сколько времени работает пользователь за компьютером, какой объем информации он передал и получил, какова его сетевая активность и др.
	Обновить	Позволяет обновить список пользователей

РАБОТА В ЧАТЕ

Основное назначение программы – обеспечение интерактивного общения пользователей.

Network Assistant базируется на концепции каналов. *Канал* представляет собой виртуальную комнату, где встречаются и беседуют пользователи. Каждый пользователь может видеть те сообщения, которые отправляются другими пользователями в канал. Каналы позволяют разбить пользователей по интересам, другими словами – разделить разговоры пользователей по темам.

Существует четыре типа каналов:

- *Обычный* – канал, открытый для любого пользователя, который знает имя канала. Указав это имя в окне *Присоединиться к каналу* (см. рис. 40), любой пользователь может войти в выбранную комнату;
- *Общий для всех* – канал может использоваться вами для оповещения всех пользователей программы Network Assistant. Другими словами, каждый пользователь, у которого запущен Network Assistant, видит те сообщения, которые приходят по этому каналу. Каждый пользователь автоматически подключается к данному каналу при запуске программы;
- *Защищенный паролем* – канал, по функциональности схожий с обычным, однако для подключения пользователя требуется указать не только имя канала, но и пароль. Создатель канала может подключать к нему пользователей, для этого в контекстном меню пользователя он должен

выбрать команду *Подключить к каналу чата* и указать канал. При этом подключаемый пользователь не обязательно должен знать пароль;

- *Приватный* – канал используется для бесед наедине. При создании вами приватного канала он создается как на вашем компьютере, так и на компьютере человека, с которым вы желаете побеседовать, поэтому нет необходимости подключать собеседника к каналу или просить его сделать это.

Network Assistant содержит семь стандартных общих каналов: *#Main*, *#New*, *#Business*, *#Problems*, *#Office Talks*, *#Miscellaneous* и *#Announcements*. Кроме этого, вы можете создавать собственные каналы или присоединяться к тем, которые уже созданы. Канал *#Main* является основным каналом. К нему автоматически подключаются все пользователи Network Assistant, и его невозможно покинуть.

Для начала общения вам и вашему собеседнику необходимо просто запустить программу. Она автоматически находит пользователей, которые уже запустили программу на своих компьютерах, и добавляет их в список пользователей. Также при запуске программы создается канал (чат) *#Main*, к которому присоединяются все пользователи. Это значит, что сообщения, которые вы отправите в этот канал, будут доступны для чтения всем пользователям (см. рис. 38).

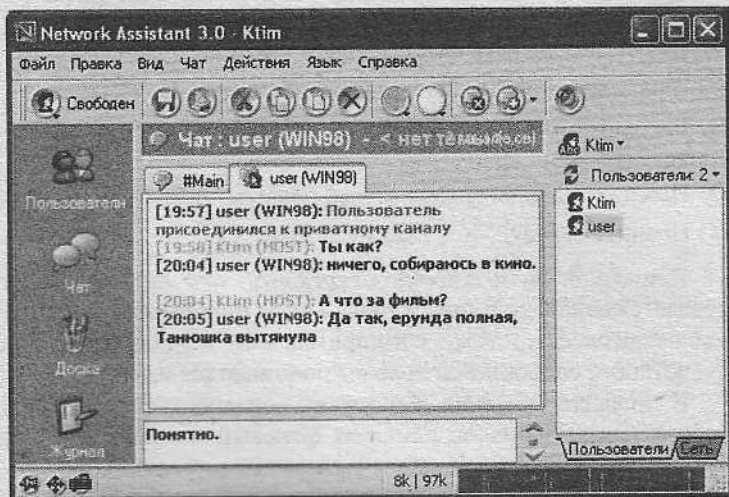


Рис. 38. Режим Чат

Для отправки сообщения всем пользователям необходимо выполнить следующие действия:

- ① Запустить программу *Network Assistant*.
- ② Перейти в режим *Чат* (см. рис. 38).
- ③ В нижней части окна набрать текст сообщения.
- ④ Нажать клавишу **Enter** для отправки сообщения пользователям.

При получении сообщения программа оповестит пользователя звуковым сигналом, на короткое время отобразит текст сообщения и изменит иконку в области уведомлений (см. рис. 39).



Рис. 39. Входящее сообщение

В том случае, если вы хотите побеседовать с человеком «один на один», вам необходимо создать секретный (приватный) чат с помощью одноименной кнопки режима *Пользователи*. Для этого следуйте нижеперечисленным инструкциям:

- ① Перейдите в режим *Пользователи* (см. рис. 35).
- ② Выделите имя пользователя, с которым вы хотите побеседовать.
- ③ Нажмите на кнопку *Секретный чат* (см. табл. 11).
- ④ Начните беседу.

При нажатии на кнопку *Секретный чат* автоматически создается канал, доступный только двум пользователям (тому, кто начал беседу, и тому, кого пригласили), и для обеспечения секретности собеседники должны пользоваться именно им.

В процессе общения вам может понадобится сохранить или распечатать диалог, изменить фоновый цвет чата или покинуть его. Все эти операции вы можете выполнить при помощи кнопок, которые находятся на панели инструментов *Чат* (см. табл. 12).

Таблица 12

Кнопки панели инструментов Чат

Кнопка	Название	Описание
	Сохранить	Позволяет сохранить текст сообщений, которые отображаются в окне <i>Чат</i> , в текстовом файле
	Печать	Используется для печати текста сообщений, которые отображаются в окне <i>Чат</i>
	Отрезать	Позволяет переместить выделенный текст в буфер обмена. Можно использовать комбинацию клавиш Ctrl+X
	Копировать	Выполняет копирование выделенного текста в буфер обмена. Можно использовать комбинацию клавиш Ctrl+C
	Вставить	Используется для вставки текста из буфера обмена. Можно использовать комбинацию клавиш Ctrl+V
	Очистить	Позволяет очистить окно чата. Окно очищается только у вас, у остальных пользователей история сообщений останется
	Цвет в чате	Позволяет выбрать цвет, которым будет отображаться ваше имя в чате
	Фоновый цвет окна чата	Используется для настройки фонового цвета окна чата
	Покинуть канал	Применяется для выхода из канала, при этом теряется вся история сообщений
	Присоединиться к каналу	Позволяет подключиться к одному из стандартных каналов или создать свой собственный канал

В небольшой сети (5–10 компьютеров) вполне можно обойтись теми стандартными чатами, которые присутствуют в

программе. Однако в сети, которая насчитывает несколько десятков компьютеров, всегда найдется три-четыре человека, которые захотят побеседовать между собой. Для этого они должны создать свой собственный чат. Для создания нового канала вы должны выполнить следующие действия.

- ① Нажать кнопку *Подключится к каналу чата* (см. табл. 11), в результате чего будет открыто окно *Присоединиться к каналу* (см. рис. 40).
- ② В окне необходимо указать:
 - имя канала – если канал с таким именем уже существует, вы присоединитесь к нему, если же нет – вы создадите новый канал;
 - тему канала – это может быть любая фраза, которая описывает предмет разговора;
 - тип канала – позволит вам ограничить доступ других пользователей к каналу.
- ③ После заполнения данных нажать кнопку *Войти*, при этом вы перейдете в режим *Чат* и будет открыто окно канала, к которому вы присоединились или который вы создали.

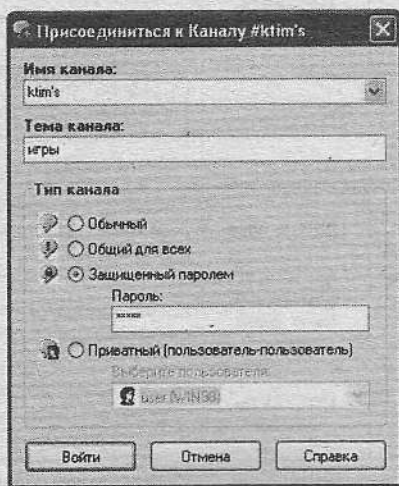


Рис. 40. Окно создания или подключения к каналу

Чтобы просмотреть имена пользователей, которые присутствуют в чате, вы должны набрать команду */here* в окне чата и нажать клавишу **Enter**.

НАСТРОЙКА БЕЗОПАСНОСТИ NETWORK ASSISTANT

Большинство настроек Network Assistant касаются настроек интерфейса и поведения программы, однако существуют настройки, касающиеся безопасности как программы, так и системы в целом. По умолчанию программа позволяет удаленным пользователям просматривать ваш Рабочий стол, получать список программ (точнее, процессов), которые работают на вашем ПК, запускать или завершать процессы на вашем компьютере. С одной стороны, это очень большая брешь в системе безопасности, с другой – очень удобный инструмент слежения за пользователями (например, за теми сотрудниками фирмы, которые любят играть в компьютерные игры на работе) и управления удаленными компьютерами.

Для изменения настроек программы вы должны перейти в режим администратора (меню *Файл*, команда *Переключиться В Режим Администратора*). Если переключение происходит впервые, программа предложит указать пароль, который в дальнейшем будет использоваться для переключения в режим администратора. Далее вам следует в меню *Файл* выбрать команду *Настройки*, при этом будет показано окно *Настройки Network Assistant* (см. рис. 41).

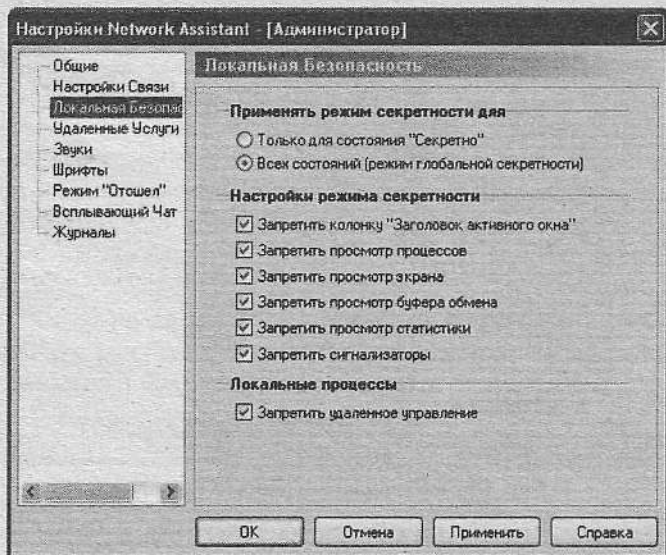


Рис. 41. Настройка безопасности Network Assistant

Пункт *Локальная Безопасность* предназначен для настройки режима секретности. Если вы хотите, чтобы удаленные пользователи не имели возможности управлять вашим компьютером, вы должны установить все флажки пункта *Локальная Безопасность*, как показано на рис. 41.

СБРОС ПАРОЛЯ NETWORK ASSISTANT

В том случае, если вы забыли пароль администратора, вы не сможете вносить изменения в настройки программы Network Assistant. Также в программе не предусмотрена возможность подсказки пароля или его сброса, однако вы можете удалить пароль путем прямой правки реестра операционной системы. Для этого вы должны выполнить следующие действия:

- ① Закрыть программу Network Assistant.
- ② В меню *Пуск* выбрать пункт *Выполнить*.
- ③ В появившемся окне ввести команду **regedit** и нажать кнопку *ОК*. Будет открыто окно программы *Regedit* (см. рис. 42).

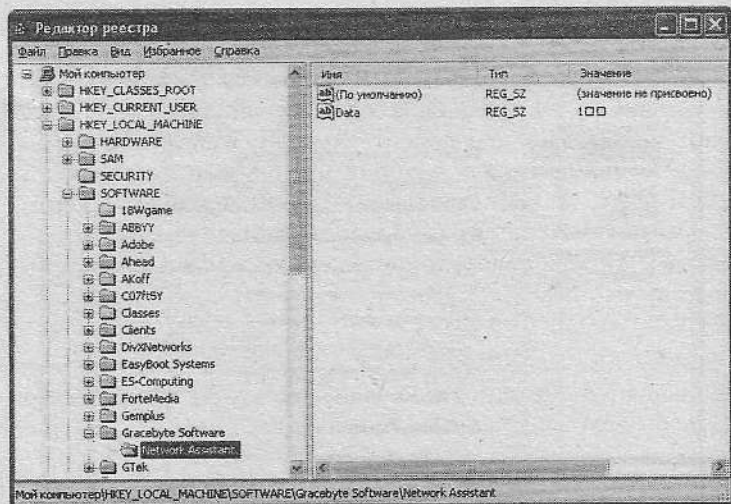


Рис. 42. Окно редактора реестра Regedit

- ④ Перейти в раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Gracabyte Software\Network Assistant`, как это показано на рис. 42. Открывать разделы можно при помощи знаков

«+», которые находятся рядом с названием раздела. Вообще, процесс навигации по разделам напоминает процесс перемещения по папкам в Проводнике Windows.

- ⑤ Обратите внимание на параметр *Data* в этом разделе. Именно он хранит пароль администратора. Вам необходимо удалить параметр, чтобы убрать пароль. В этом случае при следующей попытке переключиться в режим администратора Network Assistant попросит вас ввести новый пароль и, естественно, разрешит вам вход.
- ⑥ Для удаления параметра вы должны выделить его и в меню *Правка* выбрать команду *Удалить* или просто нажать клавишу **Delete**.
- ⑦ Программа отобразит окно подтверждения удаления параметра, в котором вы должны нажать кнопку *Да*.
- ⑧ Теперь вы можете закрыть программу *Regedit*. Изменения, которые вы сделали, будут внесены в реестр автоматически, поэтому ничего сохранять не требуется.
- ⑨ Запустите Network Assistant и переключитесь в режим администратора.

► **ПРИМЕЧАНИЕ.** Реестр операционной системы Windows представляет собой базу данных различных настроек и параметров ОС, а также настроек приложений, которые установлены на компьютере. Он является одним из важнейших компонентов операционной системы, и неосторожное обращение с ним может привести к **полной** неработоспособности компьютера. Поэтому или строго придерживайтесь вышеуказанных инструкций, или попросите более опытного пользователя выполнить их за вас.

Как вы могли убедиться, Network Assistant является мощным инструментом, способным обеспечить интерактивное общение всех пользователей вашей сети.

Courier Mail Server

Еще одним способом общения, имеющим 30-летнюю историю, является электронная почта. Именно возможность быстрой пересылки писем при помощи компьютерной сети обусловила успех, которым в настоящее время пользуется элек-

тронная почта. Теперь в письма, помимо текста, можно вставлять практически любые объекты: рисунки, аудиофайлы и т.д. Кроме того, сообщение можно создать в виде web-страницы, используя формат HTML.

Работу электронной почты обеспечивают специальные программы – серверы электронной почты, одним из которых является *Courier Mail Server*. Кроме серверов, для создания электронных писем используются почтовые клиенты – программы, позволяющие «забирать» почту с почтовых серверов, создавать (формировать) письма и отправлять их на почтовый сервер, например Outlook Express, которая входит в поставку операционной системы Windows.

Почтовый сервер Courier Mail Server (CMS) является бесплатной программой, которую можно загрузить с web-сайта <http://courierms.narod.ru/>. Являясь очень компактным (менее 1 МБайт), относительно простым в установке и настройке, он обладает большим количеством функций и возможностей. Например, если сравнивать CMS и почтовый сервер, интегрированный в Windows Server 2003, первый выигрывает по функциональности и возможностям.

УСТАНОВКА COURIER MAIL SERVER

Минимальные системные требования, предъявляемые Courier Mail Server к компьютеру, выглядят следующим образом:

- операционная система Microsoft Windows;
- 10 МБайт свободного места на жестком диске;
- сетевой протокол TCP/IP.

Courier Mail Server распространяется в виде ZIP-архива и не требует установки в обычном понимании этого слова. Архив достаточно распаковать в какую-либо папку на диске, и на этом установка закончена. Сам сервер представляет собой один исполняемый файл **CourierMS.exe**, именно он используется для запуска CMS.

При установке сервера следует иметь в виду, что для обеспечения бесперебойной работы электронной почты компьютер, на котором будет запущен CMS, должен быть постоянно включен или, во всяком случае, работать с раннего утра до позднего вечера.

БАЗОВАЯ НАСТРОЙКА СЕРВЕРА

После запуска Courier Mail Server вы увидите окно, показанное на рис. 43.

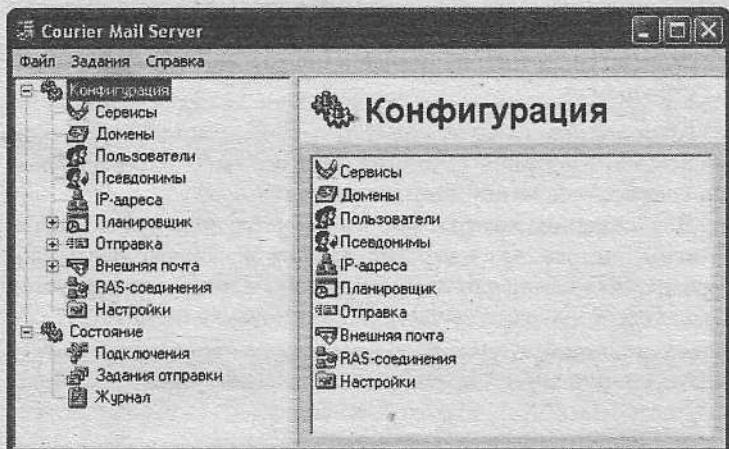


Рис. 43. Окно Courier Mail Server

Поскольку CMS разработан российскими программистами, он поддерживает русскоязычный интерфейс. Для изменения языка интерфейса необходимо в меню *File* выбрать команду *Interface*, при этом будет открыто окно, показанное на рис. 44. В этом окне вам следует в списке *Language* выбрать русский язык и нажать кнопку *OK*.

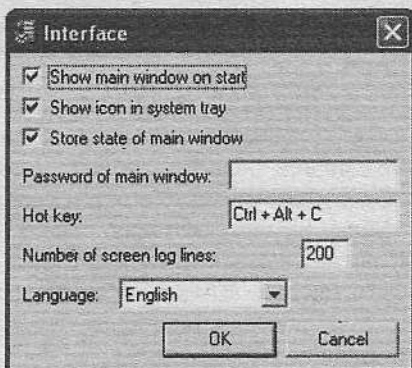


Рис. 44. Настройка интерфейса Courier Mail Server

Для обеспечения функционирования почтового сервера вы должны выполнить основные настройки:

- создать необходимые домены;
- создать почтовые ящики;

- настроить IP-адреса;
- сконфигурировать почтовые клиенты на работу с вашим сервером.

Кроме этого, следует поместить CMS в автозагрузку или переключить в режим службы (для этого необходимо в меню *Файл* выбрать команду *Запускаться службой*).

Для создания домена вам потребуется перейти в раздел *Домены* (см. рис. 45) и отредактировать начальные настройки сервера. В качестве начального домена в сервере используется *local.domain*, однако для удобства его можно изменить.

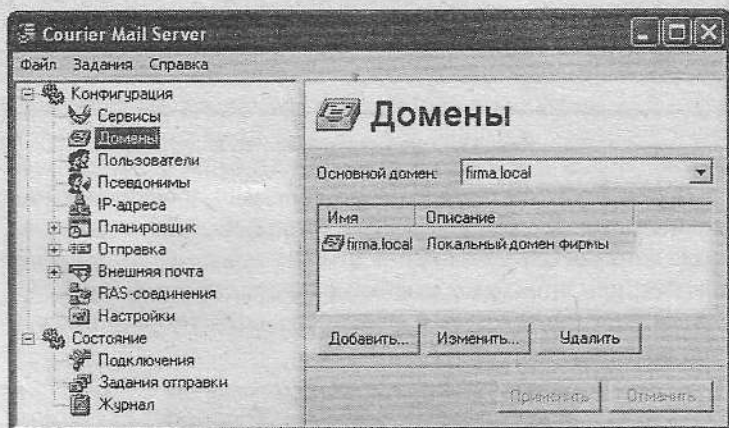


Рис. 45. Раздел *Домены* программы CMS

Домен представляет собой группу пользователей, чьи почтовые ящики объединены общими правилами обработки корреспонденции. Однако домен также является частью системы DNS (Domain Name System), которая используется в сети Internet для разрешения имен компьютеров. Если ваша сеть не подключена к сети Internet, вы можете создать любой домен, однако если сеть подключена к Internet, выбор домена должен быть согласован с вашим провайдером.

Чтобы изменить (или отредактировать) домен, необходимо выполнить следующие действия.

- ① В разделе *Домены* (см. рис. 45) нажать кнопку *Добавить* (или *Изменить*), при этом будет открыто окно *Домен* (см. рис. 46).
- ② Указать имя домена. Желательно, чтобы оно содержало и

родительский домен, пусть даже несуществующий. В будущем это облегчит подключение вашего сервера к Internet.

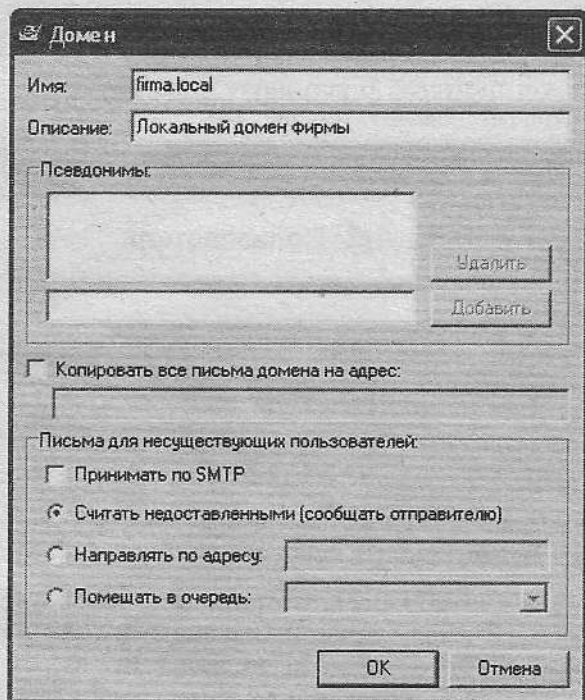


Рис. 46. Добавление (редактирование) домена

- ③ В поле *Описание* можно указать небольшой комментарий к домену.
- ④ На первом этапе настройки следует просто нажать кнопку *ОК*, поскольку остальные параметры используются для расширенной настройки домена.

На этом создание и базовая настройка домена завершены.

Для создания почтовых ящиков для пользователей вашей сети вы должны перейти в раздел *Пользователи* (см. рис. 47). В этом разделе отображаются существующие почтовые ящики, привязанные к созданным доменам. По умолчанию существует только один почтовый ящик – *admin*, который должен принадлежать администратору почтового сервера.

Чтобы добавить новый почтовый ящик или изменить параметры уже существующего, вы должны выполнить следующие действия.

- ① Перейти в раздел *Пользователи* (см. рис. 47).
- ② Нажать кнопку *Добавить* или *Изменить* в зависимости от того, что требуется. В результате будет открыто диалоговое окно *Пользователь* (см. рис. 48).

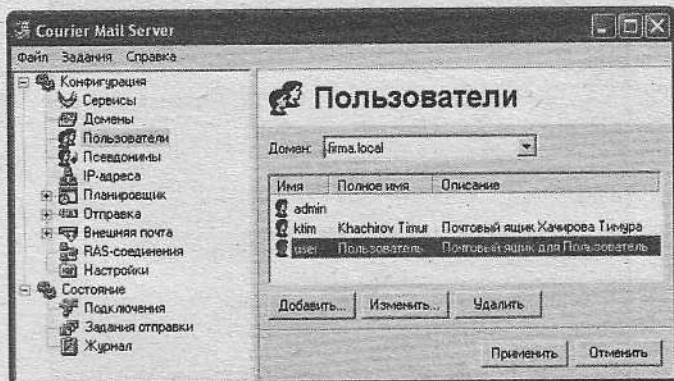


Рис. 47. Раздел *Пользователи* программы CMS

- ③ В поле *Имя* ввести имя почтового ящика, используя только латинские символы и цифры. Это имя будет фигурировать в адресе электронного почтового ящика. Как известно, сам адрес состоит из имени ящика и имени сервера, на котором он хранится (для разделения имен используется символ @). В данном примере адрес будет выглядеть как *user@firma.local*.
- ④ Указать пароль, который обеспечит защиту почтового ящика от несанкционированного получения электронной почты другими пользователями сети.
- ⑤ В поле *Полное имя* указать имя владельца почтового ящика, а в поле *Описание* – дополнительный комментарий.
- ⑥ Проследить, чтобы флажок *Разрешить доступ к почтовому ящику* был установлен, иначе пользователь не сможет подключиться к почтовому ящику.
- ⑦ Остальные параметры используются для расширенной настройки почтового ящика, поэтому их пока можно пропустить. Вам следует просто нажать на кнопку *OK*.

Далее вам необходимо настроить сервисы POP3 (Post Office Protocol 3 – служба электронной почты для получения сообщений электронной почты) и SMTP (Simple Mail Transfer Protocol – простой протокол передачи сообщений электронной почты), которые отвечают за получение клиентами писем с почтовых серверов и за передачу писем от клиентов и между серверами соответственно.

Пользователь

Имя: user

Пароль: user

Полное имя: Пользователь

Описание: Почтовый ящик для Пользователь

Внешний адрес e-mail:

Добавлять локальный адрес

Разрешить отправку внешней почты

Разрешить доступ к почтовому ящику

Собственные параметры отправки:

Макс. число получателей в письме: 100

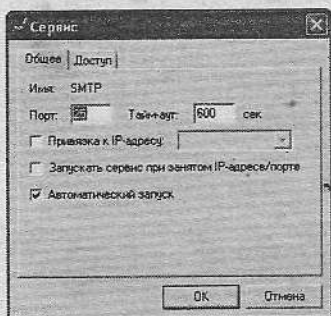
Макс. размер письма: 2048 Kб

OK Отмена

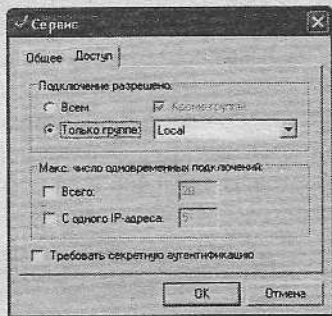
Рис. 48. Добавление (редактирование) почтового ящика

Для этого в основном окне CMS следует перейти к разделу *Сервисы*, выбрать один из настраиваемых сервисов и нажать кнопку *Изменить*. При этом будет отображено окно, показанное на рис. 49а.

Нас интересует группа *Подключение разрешено* на вкладке *Доступ* (см. рис. 49б). Эти параметры определяют, какие пользователи могут подключаться к почтовому серверу для отправки и получения почты. В данном случае подключаться могут только пользователи, входящие в группу *Local* (локальные), а это значит, что вы должны добавить в эту группу IP-адреса компьютеров, которые входят в вашу сеть.



а)



б)

Рис. 49. Настройка сервиса SMTP

Для добавления IP-адресов в группу вы должны перейти в раздел *IP-адреса* (см. рис. 50) и убедиться, что:

- диапазон IP-адресов вашей сети добавлен в сервер (нижняя часть окна);
- группа *Local* содержит диапазон IP-адресов вашей сети, поскольку именно этой группе разрешено подключаться к сервисам POP3 и SMTP. По умолчанию доступ к серверу разрешен с IP-адреса 127.0.0.1 и сети, чей идентификатор выглядит как 192.168.0.0.

Для добавления или изменения существующего диапазона IP-адресов вы должны следовать перечисленным ниже инструкциям.

- ① Нажать кнопку *Добавить* или, выделив диапазон, кнопку *Изменить*.
- ② В появившемся окне *IP-адрес* (см. рис. 51) указать тип IP-адреса – это может быть *хост* (указание IP-адреса одного компьютера), *сеть* (задание идентификатора сети) или *диапазон* (задание перечня IP-адресов). Например, если вы выбрали диапазон, нужно в поле *С* указать начальный IP-адрес диапазона, используемого в вашей сети, а в поле *По* – конечный.
- ③ При желании – задать небольшой комментарий к данному диапазону в поле *Описание*.
- ④ Установить флажок *Активен*, иначе данный диапазон не будет обслуживаться сервером.
- ⑤ Выделить группу *Local* и переместить ее в область *Входит в группы* с помощью кнопки *<*.
- ⑥ нажать кнопку *OK*.

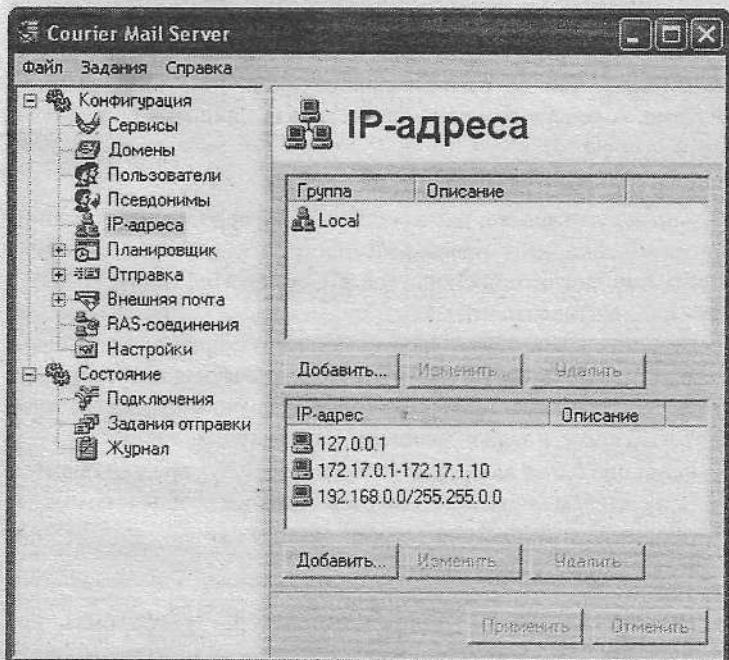


Рис. 50. Раздел IP-адреса программы CMS

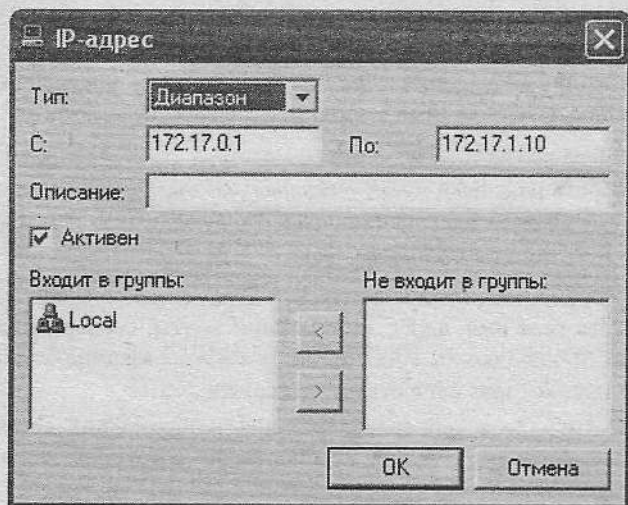


Рис. 51. Добавление (редактирование) диапазона IP-адресов

На этом базовая настройка сервера закончена. Дополнительную информацию по конфигурированию сервера вы можете найти или на сайте разработчиков, или в справочной системе. А теперь вам следует настроить клиентов на работу с вашим сервером.

КАК НАСТРОИТЬ КЛИЕНТОВ

Как вы уже знаете, для использования сервера электронной почты необходимо правильно настроить рабочие станции, чтобы они могли подключаться к Courier Mail Server и получать или отправлять письма.

Для такой настройки следует запустить программу Outlook Express и создать новую учетную запись. Учетная запись хранит сведения о почтовом сервере, который обслуживает электронный почтовый ящик, а также сведения о самом ящике, такие как:

- фамилию и имя владельца (эти данные будут предоставляться получателям почты вместе с отсылаемыми сообщениями);
- используемый адрес электронной почты;
- имя учетной записи и пароль.

► **ПРИМЕЧАНИЕ.** На одном компьютере может быть несколько пользователей, и для каждого из них можно создавать неограниченное количество учетных записей. Это также удобно, если вы используете для работы несколько адресов электронной почты.

Итак, для добавления в Outlook Express новой учетной записи для почты необходимо выполнить следующие действия:

- ① Открыть меню *Сервис*.
- ② Выбрать из списка пункт *Учетные записи*, в результате чего появится окно *Учетные записи в Интернете* (см. рис. 52).
- ③ Нажать кнопку *Добавить*, а затем – *Почта*.
- ④ В появившемся окне *Мастер подключения к Интернету* задать свое имя, адрес электронной почты, серверы входящих и исходящих сообщений, а также название учетной записи, которая существует на сервере.
- ⑤ Ввести адреса серверов входящих и исходящих сообщений, используя IP-адрес компьютера, на котором запущен Courier Mail Server (см. рис. 53).
- ⑥ Нажать кнопку *Готово*.

В результате в список учетных записей окна *Учетные записи в Интернете* добавится новый пункт с названием указанной Вами учетной записи почты.

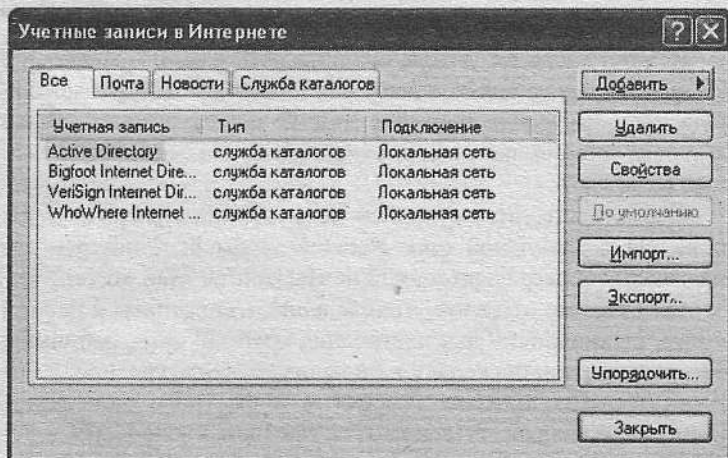


Рис. 52. Список учетных записей в Outlook Express

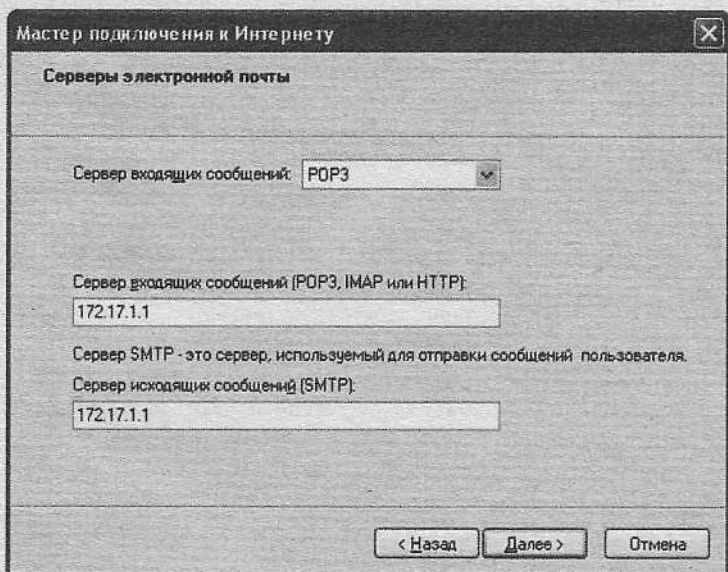


Рис. 53. Указание почтовых серверов

Заключение

Из этой книги вы узнали, как объединить свой компьютер с компьютерами соседей по дому или коллег по работе в локальную сеть, настроить протокол TCP/IP и использовать общие каталоги для обмена информацией между пользователями вашей сети.

Кроме этого, вы научились использовать программу для общения в локальной сети Network Assistant и настраивать настоящий сервер электронной почты Courier Mail Server.

Необходимо отметить, что сведений, изложенных в данной книге, недостаточно для построения крупной сети, например, на предприятии, поскольку в больших сетях встают проблемы корректного назначения IP-адресов и быстрого разрешения имен компьютеров. Решение этих проблем заключается в установке и настройке различных серверов (DHCP, DNS и WINS), которые существенно упрощают работу администратора, а также повышают качество сети.

Содержание

<i>Введение</i>	3
<i>Глава 1. Как объединить компьютеры в сеть</i>	5
Топологии сетей.....	5
Скорость передачи данных в сети.....	7
Что вам потребуется.....	8
Технология Ethernet.....	17
Соединяем компьютеры.....	21
<i>Глава 2. Как общаются компьютеры</i>	27
Протоколы семейства TCP/IP.....	27
Взаимодействие между разнородными сетями.....	30
Адресация в IP-сетях.....	31
Выбор IP-адресов.....	34
Порты.....	35
<i>Глава 3. Настройка соединений</i>	38
Как изменить имя компьютера.....	38
Как добавить сетевые компоненты.....	40
Как настроить TCP/IP.....	42
Альтернативная и Автоматическая частная IP-адресации (APIPA).....	44
Имена компьютеров.....	45
Как проверить наличие связи.....	47
<i>Глава 4. Как использовать общие ресурсы</i>	51
Что такое сервер.....	51
Учетные записи пользователей.....	52
Что такое группа пользователей.....	58
Настройка каталога для общего использования.....	60
Как настроить разрешения для файлов.....	63
Безопасность папок.....	65
Алгоритм ваших действий.....	70
<i>Глава 5. Общение в локальной сети</i>	72
Network Assistant.....	72
Courier Mail Server.....	83
<i>Заключение</i>	94

Научно-производственная литература

Глушаков С. В., Хачиров Т. С.

НАСТРАИВАЕМ СЕТЬ СВОИМИ РУКАМИ

Компьютерный дизайн Э. Э. Кунтыш

Подписано в печать 12.02.08. Формат 84x108¹/₃₂.
Усл. печ. л. 5,04. Тираж 5 000 экз. Заказ № 8119.

Общероссийский классификатор продукции
ОК-005-93, том 2; 953004 — научная и популярная литература

Санитарно-эпидемиологическое заключение
№ 77.99.60.953.Д.007027.06.07 от 20.06.2007 г.

ООО «Издательство АСТ»
141100, Россия, Московская область, г. Шелково, ул. Заречная, д. 96
Наши электронные адреса:
WWW.AST.RU E-mail: astpub@aha.ru

ООО «Издательство Фолио»
Свидетельство о внесении субъекта издательской деятельности
в Государственный реестр издателей, изготовителей
и распространителей издательской продукции
ДК № 502 от 21.06.2001 г.

ООО «Фолио»
Свидетельство о внесении субъекта издательской деятельности
в Государственный реестр издателей, изготовителей
и распространителей издательской продукции
ДК № 683 от 21.11.2001 г.
61057, Харьков, ул. Донец-Захаржевского, 6/8
Электронные адреса: www.folio.com.ua E-mail:
realization@folio.com.ua
Интернет-магазин «Книга — почтой»: www.bookpost.com.ua

ОАО «Владимирская книжная типография»
600000, г. Владимир, Октябрьский проспект, д. 7
Качество печати соответствует качеству предоставленных диапозитивов

Эта книга расскажет вам, как объединить свой компьютер с компьютерами соседей по дому или коллег по работе в локальную сеть, которая позволит вам обмениваться файлами, музыкой, видеофильмами, а также весело отдыхать вместе, играя в сетевые игры.

Если вы хотите понять, как же взаимодействуют компьютеры, какое оборудование используется для этого и как его настраивать, то эта книга для вас. Она позволит вам шаг за шагом научиться работать с сетевым оборудованием и утилитами диагностики и настройки сетевых соединений. Также вы узнаете о программах, необходимых для защиты компьютера от вторжений из сети, и программах, позволяющих общаться в реальном режиме времени.

Прочитав эту книгу, вы сможете не только создать структурированную кабельную систему, настроить операционные системы для работы в локальной сети, но и научитесь использовать программы и службы, ради которых и создавалась сеть.

ISBN 978-5-17-048458-4



9 785170 484584

