

Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

ИНФОРМАЦИОННЫЕ СЕТИ И ПЕРЕДАЧА ИНФОРМАЦИИ В ИСУЛХ

**Методические указания по одноименной дисциплине
для проведения лабораторных работ
для студентов специальности 1-75 01 01 «Лесное хозяйство»
специализации 1-75 01 01 04 «Информационные системы
в лесном хозяйстве»**

Минск 2010

УДК 630*6:004.78(075.8)

ББК 43.9:32.97я73

И74

Рассмотрены и рекомендованы к изданию редакционно-издательским советом университета

Составитель *Н. Я. Сидельник*

Научный редактор *И. В. Толкач*

Рецензент

кандидат сельскохозяйственных наук,
доцент кафедры лесных культур и почвоведения *А. П. Волкович*

По тематическому плану изданий учебно-методической литературы университета на 2010 год. Поз. 11.

Предназначены для студентов специальности 1-75 01 01 «Лесное хозяйство» специализации 1-75 01 01 04 «Информационные системы в лесном хозяйстве».

© УО «Белорусский государственный
технологический университет», 2010

ПРЕДИСЛОВИЕ

Внедрение в практику лесного хозяйства и лесоустройства современных технологий и информационных систем значительно повышает требования к специалистам отрасли. Современный инженер лесного хозяйства должен не только в совершенстве знать лесные дисциплины, но и разбираться в коммуникационных средствах, аппаратном и программном обеспечении информационных систем.

На лесохозяйственных предприятиях Республики Беларусь создана отраслевая информационная сеть, внедрены «Информационная система управления лесным хозяйством» и геоинформационная система «Лесные ресурсы», позволяющие автоматизировать задачи планирования и управления деятельностью отрасли лесного хозяйства. Подготовка специалистов, владеющих современной техникой и информационными технологиями, является важным этапом в функционировании данных систем.

Методические указания призваны помочь студентам лесохозяйственного факультета в обучении теоретическим основам функционирования глобальных и локальных информационных сетей, приобретении практических навыков работы с сетевым оборудованием и программным обеспечением, ознакомлении со структурой, аппаратными и программными средствами отраслевой информационной сети Министерства лесного хозяйства.

В результате изучения дисциплины студент должен уметь устанавливать и настраивать сетевое оборудование; управлять бюджетами пользователей и групп; знать общие принципы построения вычислительных сетей, основные модели сети, основы структуризации сетей, базовые технологии локальных сетей, принципы адресации в IP-сетях, структуру информационной сети отрасли лесного хозяйства; организовывать отдельный доступ к периферийным устройствам, локальную сеть с делением на сегменты (подсети), удаленный доступ к сети, рабочие группы, домен; подключать рабочие станции к домену; создавать пользовательские бюджеты и группы пользователей; устанавливать их права и допуски.

Настоящая работа ставит своей целью оказать методическую помощь студентам очной формы обучения специализации 1-75 01 01 04 «Информационные системы в лесном хозяйстве» при выполнении лабораторных работ по дисциплине.

Лабораторная работа № 1

ВНУТРЕННЕЕ УСТРОЙСТВО КОМПЬЮТЕРА, УСТАНОВКА СЕТЕВОГО АДАПТЕРА И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: ознакомиться с внутренним устройством компьютера; научиться устанавливать сетевой адаптер и программное обеспечение к нему.

Теоретические сведения

В зависимости от назначения и конструкции персональные компьютеры бывают: настольные (desktop); переносные, портативные (notebook); карманные (pocket).

Внутреннее устройство компьютера. Настольный персональный компьютер состоит из стандартных устройств-блоков: системного блока, дисплея (монитора), клавиатуры, манипулятора «мышь» и периферийных устройств.

Системный блок содержит основные электронные компоненты компьютера, крепления и отсеки для основных устройств. Системный блок может быть вертикальным (tower) и горизонтальным (desktop). На лицевой панели системного блока располагаются кнопки включения питания (power), кнопка перезагрузки (reset), индикаторные лампочки. На задней панели системного блока имеются разъемы (slot) для подключения других устройств.

Системная (материнская) плата – это сложная многослойная печатная плата, на которой устанавливаются основные компоненты персонального компьютера (рис. 1.1).

К числу основных компонент, установленных на материнской плате (см. рис. 1.2 на с. 6), относятся:

– *центральный процессор* (ЦПУ (CPU)) – устройство, выполняющее все основные операции по обработке информации;

– *набор системной логики* (chipset) – набор микросхем, обеспечивающих подключение ЦПУ к оперативному запоминающему устройству (ОЗУ) и контроллерам периферийных устройств. Современные наборы системной логики строятся на базе двух интегральных микросхем: северного и южного мостов;

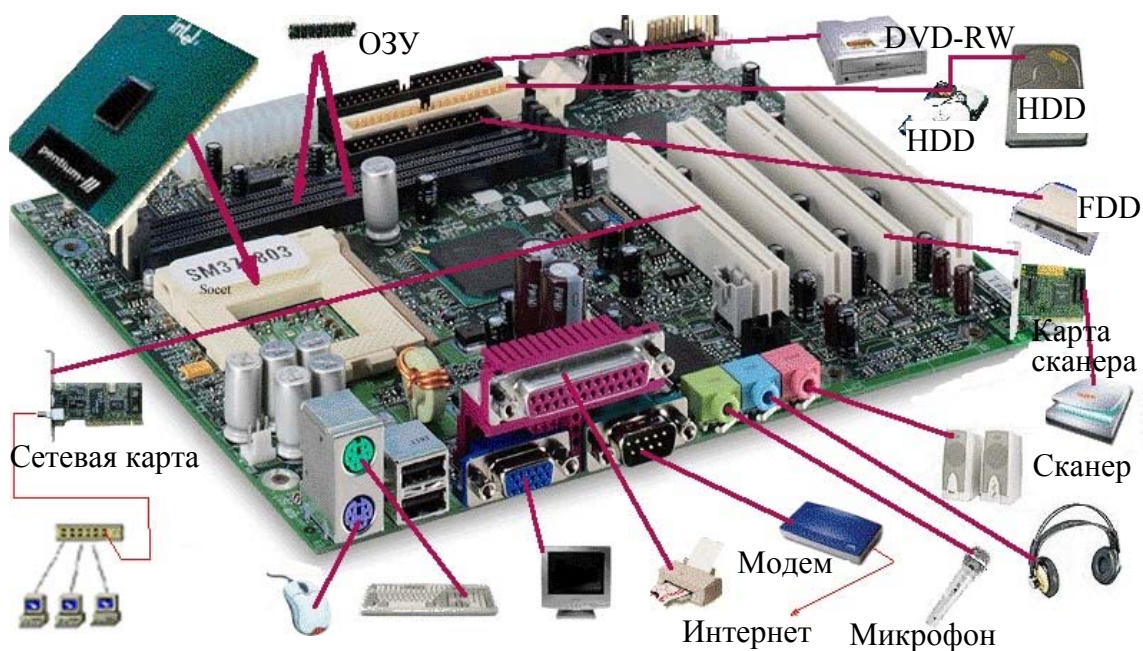


Рис. 1.1. Разъемы и компоненты материнской платы

– *северный мост* (northbridge), МСН (Memory Controller Hub), *системный контроллер* – устройство, которое обеспечивает подключение ЦПУ к узлам, использующим высокопроизводительные шины: ОЗУ, графический контроллер. В качестве шины для подключения графического контроллера на современных материнских платах применяется PCI-Express;

– *южный мост* (southbridge), ИСН (I/O Controller Hub), *периферийный контроллер* – устройство, которое содержит контроллеры периферийных устройств (жесткого диска, Ethernet, аудио), контроллеры шин для подключения периферийных устройств (шины PCI, PCI-Express и USB (Universal Serial Bus)), а также контроллеры шин, к которым подключаются устройства, не требующие высокой пропускной способности, – последовательного и параллельного интерфейсов, контроллера клавиатуры и мыши;

– *микросхема BIOS* – базовая система ввода-вывода (Basic Input Output System), состоящая из набора программ ввода-вывода, благодаря которым операционная система и прикладные программы могут взаимодействовать с различными устройствами как самого компьютера, так и подключенных к нему;

– *встроенные (интегрированные) дополнительные устройства.*

Оперативное запоминающее устройство (ОЗУ или RAM (Random Access Memory)) предназначено для временного хранения данных и команд, необходимых процессору для выполнения операций.

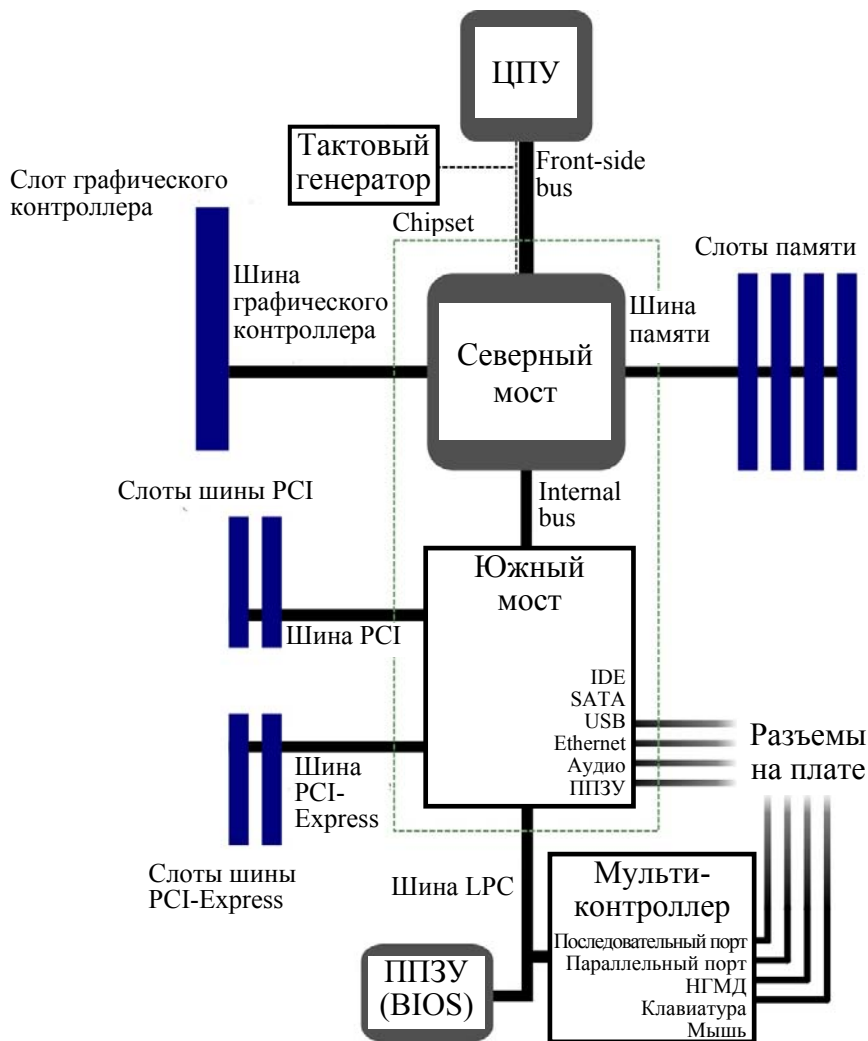


Рис. 1.2. Устройство материнской платы

Оперативная память передает процессору данные непосредственно, либо через кэш-память (промежуточный буфер с быстрым доступом). Наибольшее распространение имеют два вида ОЗУ:

- SRAM (Static RAM) – статическая память. Достоинство этого вида памяти – скорость, недостатки – стоимость и размер;
- DRAM (Dynamic RAM) – динамическая память, так как разряды в ней хранятся не статически, а «стекают» динамически во времени (более экономичный вид памяти, но более медленный).

В настоящее время используются модули DDR2 (Double-Data-Rate 2) и DDR3, которые в результате некоторых изменений в архитектуре позволяют получить большую пропускную способность подсистемы памяти.

Постоянное запоминающее устройство (ПЗУ или ROM (Read Only Memory)) предназначено для не изменяющихся в процессе экс-

плуатации программ, например, тестирования и первоначальной загрузки компьютера. Иными словами, это устройство хранения программ и данных, определяющих работу ПЭВМ после включения питания. В роли ПЗУ используется **жесткий магнитный диск** (HDD (Hard Disk Drive), винчестер), предназначенный для хранения постоянно используемой при работе с компьютером информации. Жесткие диски отличаются назначением, размером, скоростью вращения, интерфейсом подключения.

Видеоадаптер (видеокарта) обеспечивает формирование картинки на мониторе. Наиболее популярны видеокарты компании NVIDIA, ATI и SIS.

Звуковая карта (встроенная или внешняя) и акустические системы (колонки) служат для воспроизведения звука.

Сетевая карта (сетевой адаптер) – это плата расширения (встроенная или внешняя), предназначенная для объединения компьютеров в локальную сеть. Существуют сетевые адаптеры стандарта PCMCIA для ноутбуков и подключаемые к USB-порту компьютера. Использование встроенной в материнскую плату сетевой карты не гарантирует работу компьютера в локальной сети на максимально возможной скорости [1].

Блок питания преобразует высокое переменное напряжение в низкое постоянное, необходимое для работы электроники.

Модем – устройство, дающее возможность подключить компьютер к телефонной линии связи. Он может быть встроенным в системный блок в виде платы, а также в виде отдельного устройства. Это устройство, которое осуществляет модуляцию, т. е. преобразование цифровой информации, поступающей из компьютера, в аналоговую форму, необходимую для телефонной линии, и демодуляцию (обратное преобразование). Модем дает возможность пользователю выйти в глобальные сети (Интернет).

Монитор (дисплей) служит для отображения вводимой и выводимой текстовой или графической информации. В зависимости от строения монитора бывают: ЭЛТ – монитор на основе электронно-лучевой трубки; ЖК – жидкокристаллический монитор; плазменный – на основе плазменной панели; проекционный – проектор и экран, размещенные отдельно или в одном корпусе; OLED-монитор – на основе технологии OLED (Organic Light-Emitting Diode).

Клавиатура предназначена для ввода в компьютер алфавитно-цифровых и псевдографических символов.

Манипулятор «мышь» служит для перемещения курсора на экране дисплея и выполнения определенных положением курсора

действий. Существуют опτικο-механические, оптические, инфракрасные беспроводные мыши.

Принтер предназначен для вывода цифровой, символьной и графической информации на бумагу. Существуют матричные, струйные и лазерные принтеры.

Блок бесперебойного питания служит для минимизации потерь при кратковременном отключении от сети.

Сменные накопители предназначены для хранения постоянно неиспользуемой информации, архивации содержимого жесткого магнитного диска и переноса программ с одного компьютера на другой:

1) флорпи-диски емкостью 1,44 Мб;

2) CD-диски (Compact Disc) объемом до 800 Мб;

3) DVD-диски (Digital Video Disc), имеющие емкость от 4,7 Гб. Запись и считывание информации с таких дисков производится с помощью оптических приводов (внутренних или внешних), дающих возможность однократной (на дисках DVD-R (Read)) и многократной записи (DVD-RW (Disc ReWritable));

4) USB-накопители (Flash Drive) с объемом флэш-памяти от 1 Гб и более.

Порядок выполнения работы

1. Используя теоретические сведения, ознакомиться с внутренним устройством компьютера.

2. Установка сетевой карты. Открыть системный блок, вставить сетевую карту в PCI-разъем на материнской плате.

3. После физической установки сетевой платы в компьютер ее следует настроить, т. е. установить для нее программное обеспечение (драйвер):

– нажать кнопку **Пуск** и выбрать в меню **Настройка** команду **Панель управления** (рис. 1.3);

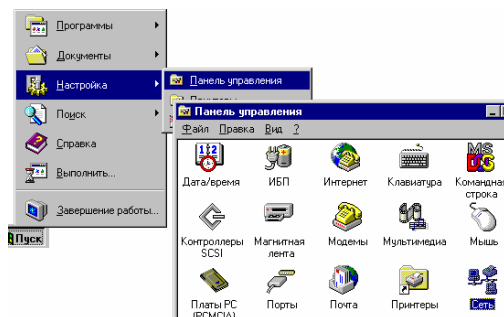


Рис. 1.3. Панель управления

– дважды щелкнуть значок **Сеть**. На экране появится диалоговое окно **Сеть** с набором вкладок, позволяющих внести необходимые изменения;

– выбрать вкладку **Адаптеры** (рис. 1.4) и нажать кнопку **Добавить**. В появившемся окне **Выбор: Сетевая плата** нажать **Установить с диска...** (рис. 1.4);

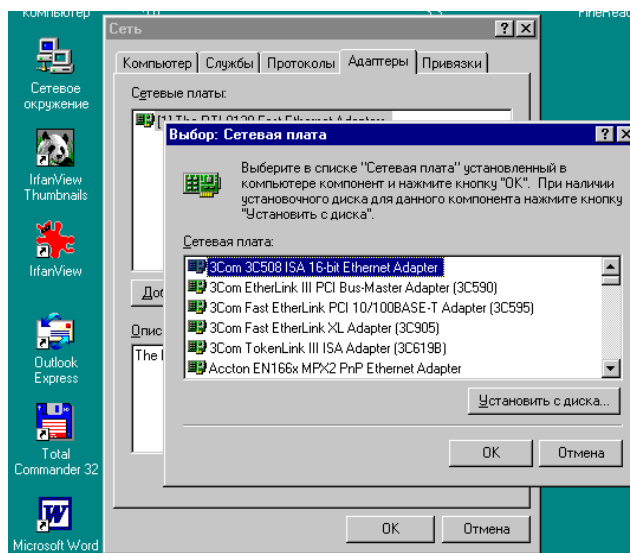


Рис. 1.4. Окна «Сеть» и «Выбор: Сетевая плата»

– указать путь на CD-R диске (рис. 1.5), который прилагается к устанавливаемому сетевому адаптеру, где находится программное обеспечение (драйвера) сетевой карты;

– выбрать сетевой адаптер (рис. 1.6) и нажать **ОК**;

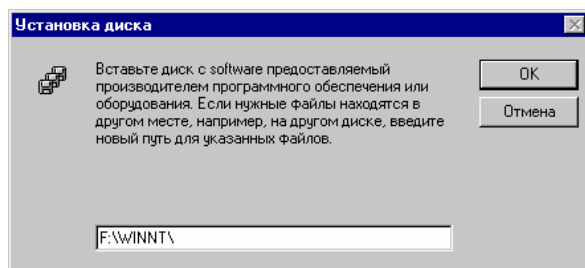


Рис. 1.5. Установка диска

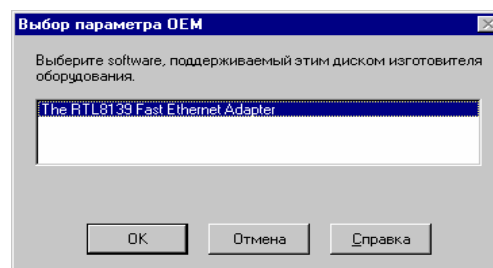


Рис. 1.6. Выбор параметра

– в появившемся окне **Свойства: Microsoft TCP/IP** выбрать **Указать адрес IP явным образом** и ввести IP-адрес, который приведен на системном блоке компьютера, например 192.168.14.11, маску подсети 255.255.255.0, основной шлюз 192.168.14.10 (рис. 1.7).

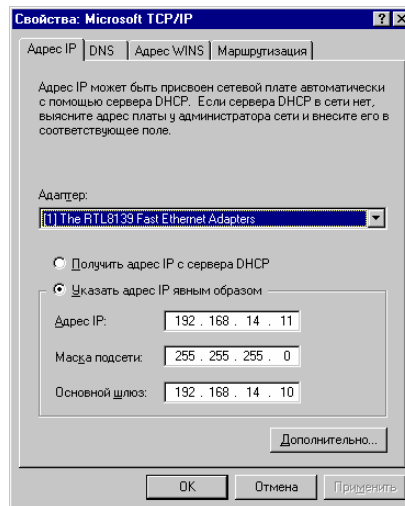


Рис. 1.7. Окно «Свойства:
Microsoft TCP/IP»

Таким образом, сетевой адаптер и его программное обеспечение установлены.

Лабораторная работа № 2

ПЛАНИРОВАНИЕ СЕТИ И ВЫБОР СЕТЕВОГО ОБОРУДОВАНИЯ, ПОДКЛЮЧЕНИЕ КАБЕЛЕЙ

Цель работы: изучить основные топологии сетей; научиться обжимать и подключать сетевые кабели.

Теоретические сведения

Компьютерная сеть – это совокупность компьютеров и различных устройств, обеспечивающих информационный обмен между компьютерами в сети без использования каких-либо промежуточных носителей информации.

Компьютерные сети можно классифицировать по группе следующих признаков: территориальная распространенность, ведомственная принадлежность, скорость передачи информации, тип среды передачи.

В зависимости от территориальной распространенности сети могут быть локальными, региональными и глобальными. Локальные сети (LAN (Local Area Network)) – это сети, перекрывающие небольшую территорию, региональные – расположенные на территории города или области, глобальные (WAN (Wide Area Network)) – на территории государства или группы государств (Интернет) [1].

Сетевая технология – согласованный набор стандартных протоколов (документы, в деталях описывающие, как должна работать сеть) и реализующих их программно-аппаратных средств (технологии Ethernet и Token Ring).

Ethernet – самый распространенный стандарт локальных сетей. Для построения сети необходим один адаптер для каждого компьютера и малое количество кабеля. Технология Token Ring требует наличия дополнительного устройства – концентратора.

Различают:

– топологию физических связей (физическую структуру сети). В этом случае конфигурация физических связей определяется соединениями компьютеров, т. е. отрезками кабеля, связывающими пары узлов. Отрезки кабеля, соединяющие два компьютера или какие-либо два других сетевых устройства, называются физическими сегментами;

– топологию логических связей (логическую структуру сети). Здесь в качестве логических связей выступают маршруты передачи данных между узлами сети [1].

Физическая структуризация сети. Все сети строятся на основе трех базовых топологий: «шина», «звезда», «кольцо». Если компьютеры подключены вдоль одного кабеля (сегмента), топология называется «шиной» (рис. 2.1). В том случае, когда компьютеры подключены к сегментам кабеля, исходящим из одной точки или концентратора, топология называется «звездой» (рис. 2.2). Если кабель, к которому подключены компьютеры, замкнут в кольцо, такая топология носит название «кольца» (рис. 2.3).

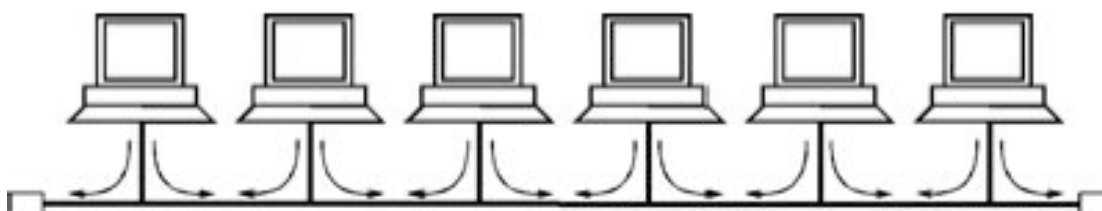


Рис. 2.1. Топология «шина»

Структура типа «шина» проще и экономичнее, так как для нее не требуется дополнительное устройство и расходуется меньше кабеля, но она очень чувствительна к неисправностям кабельной системы. Если кабель поврежден хотя бы в одном месте, то место неисправности трудно обнаружить. Поскольку данные в сеть передаются лишь одним компьютером, ее производительность зависит от количества компьютеров, которые подключены к «шине» (чем больше компьютеров, ожидающих передачи данных, тем медленнее сеть).

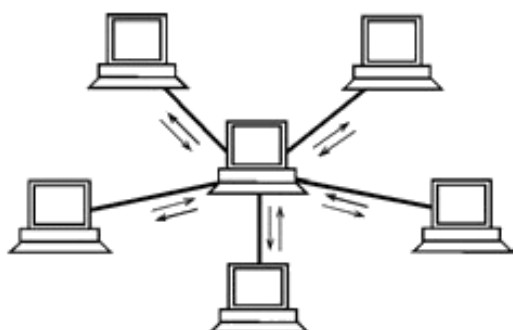


Рис. 2.2. Топология «звезда»

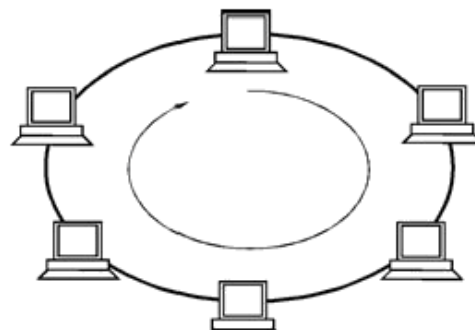


Рис. 2.3. Топология «кольцо»

При топологии «звезда» все компьютеры с помощью сегментов кабеля подключаются к центральному компоненту (концентратору). Сигналы от передающего компьютера поступают через концентратор ко всем остальным. Топология возникла, когда компьютеры были подключены к центральному, главному, компьютеру.

В сетях с топологией «звезда» подключение кабеля и управление конфигурацией сети централизованы. Недостаток – значительно увеличивается расход кабеля, так как все компьютеры подключены к центральной точке. Если центральный компонент выйдет из строя, нарушится работа всей сети. Если выйдет из строя один компьютер (или кабель, соединяющий его с концентратором), то только этот компьютер не сможет передавать или принимать данные по сети. На остальные компьютеры в сети это не повлияет.

Во многих случаях физическая и логическая топологии сети совпадают. Например, сеть, представленная на рис. 2.4, имеет физическую топологию «кольцо».

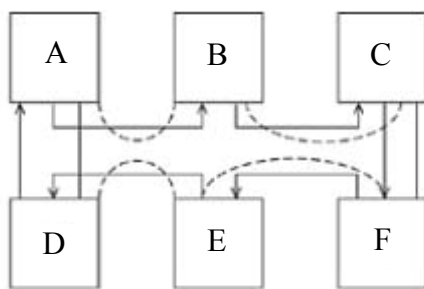


Рис. 2.4. Совпадение логической и физической структуры сети

Физическая и логическая топологии сети могут не совпадать (рис. 2.5). Физически компьютеры соединены по топологии общая «шина». Доступ к «шине» происходит не по алгоритму случайного доступа, применяемому в технологии Ethernet, а в кольцевом порядке. При этом физическая структура сети не изменяется.

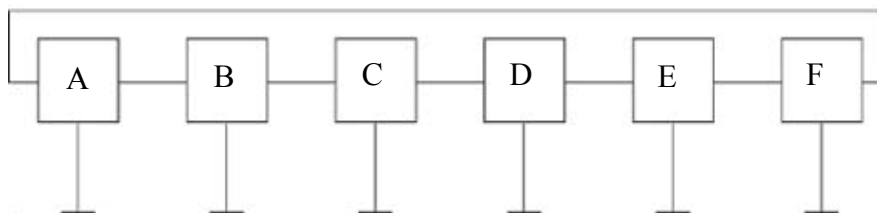


Рис. 2.5. Физическая общая «шина», но логическое «кольцо»

Другой пример несовпадения физической и логической топологий сети. Концентратор Ethernet поддерживает в сети физическую топологию общая «шина». Однако логическая топология сети осталась без изменений – это «звезда» (рис. 2.6). Физическая структуризация сети с помощью концентраторов полезна как для увеличения расстояния между узлами сети, так и для повышения ее надежности.

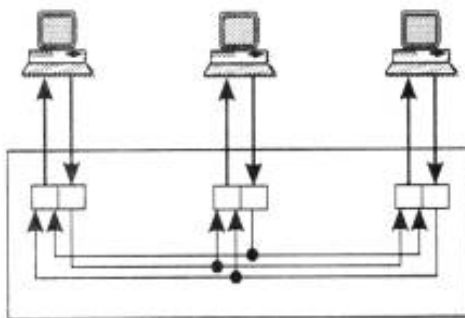


Рис. 2.6. Концентратор Ethernet (физическая общая «шина», логическая «звезда»)

Логическая структуризация сети. Физическая структуризация сети полезна во многих отношениях, кроме сетей большого размера, где без логической структуризации сети обойтись невозможно. Сеть с типовой топологией («шина», «кольцо», «звезда»), в которой все физические сегменты рассматриваются в качестве одной разделяемой среды, приводит к увеличению времени для ожидающих доступа в сеть компьютеров.

Для решения проблемы нужно отказаться от идеи единой однородной разделяемой среды (рис. 2.7).

Для логической структуризации сети могут быть использованы мосты, коммутаторы и маршрутизаторы [2].

Мост (bridge) делит разделяемую среду передачи сети на части (часто называемые логическими сегментами), передавая информацию из одного сегмента в другой только в том случае, если такая передача действительно необходима, т. е. если адрес компьютера назначения принадлежит другой подсети. Мост запоминает, через какой порт на него поступил кадр данных от каждого компьютера сети, и в дальнейшем передает кадры, предназначенные для данного компьютера, на этот порт.

Коммутатор (switch), в отличие от моста, является своего рода коммуникационным мультипроцессором, так как каждый его порт оснащен специализированной микросхемой, которая обрабатывает данные по алгоритму моста независимо от микросхем других портов.

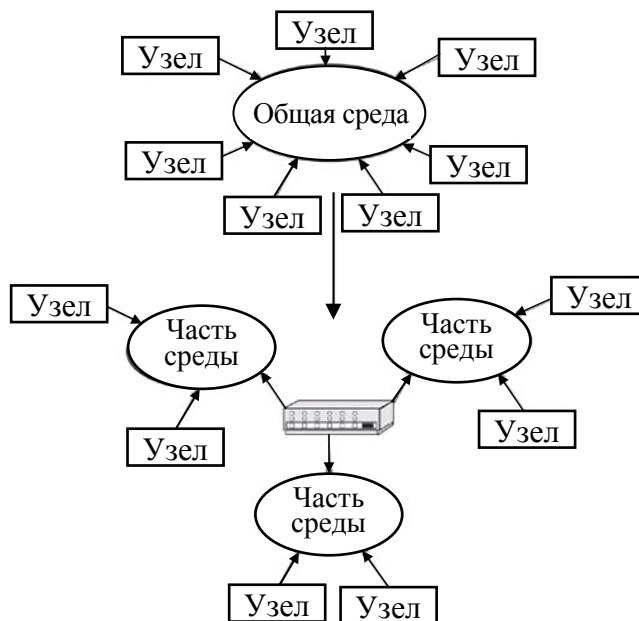


Рис. 2.7. Отказ от единой разделяемой среды

Маршрутизаторы (router) образуют логические сегменты посредством явной адресации, поскольку используют не плоские аппаратные, а составные числовые адреса (рис. 2.8).

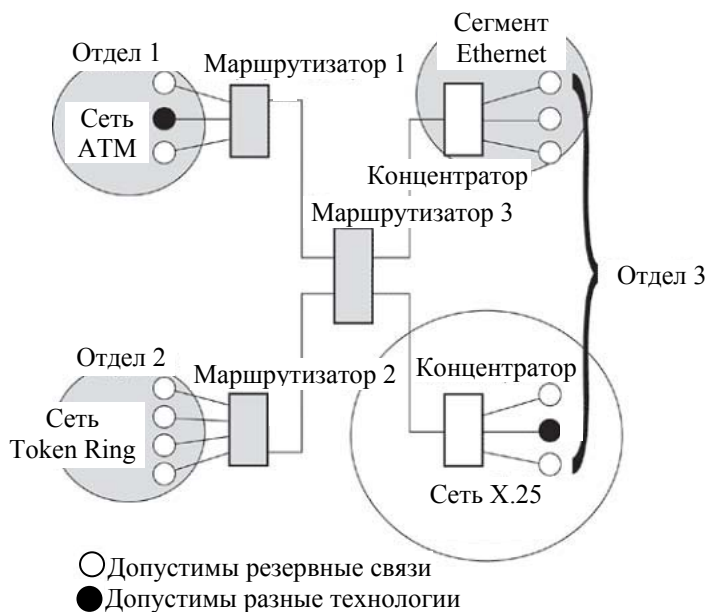


Рис. 2.8. Логическая структуризация сети с помощью маршрутизаторов

Если в сети участвует больше двух компьютеров, то нужно устройство, которое объединяет всю систему, т. е. к нему сходятся все сетевые кабели. При топологии «кольцо» компьютеры подключаются

к кабелю, замкнутому в кольцо. Поэтому у кабеля просто не может быть свободного конца, к которому надо подключать терминатор. Сигналы передаются по кольцу в одном направлении и проходят через каждый компьютер. В отличие от пассивной топологии «шина», здесь каждый компьютер выступает в роли репитера, усиливая сигналы и передавая их следующему компьютеру. Поэтому при выходе из строя одного компьютера прекращает функционировать вся сеть.

В настоящее время часто используются топологии, которые комбинируют компоновку сети по принципу «шины», «звезды» и «кольца», например «звезда-шина», «звезда-кольцо».

В зависимости от типа среды передачи сети бывают на витой паре, коаксиальные, оптоволоконные (рис. 2.9), с передачей информации по радиоканалам или в инфракрасном диапазоне (беспроводное соединение, Wi-Fi).

Витая пара (Twisted Pair) – в настоящее время это наиболее распространенный сетевой проводник. По структуре он напоминает многожильный телефонный кабель, имеет восемь медных проводников, перевитых друг с другом, и хорошую плотную изоляцию из поливинилхлорида. Обеспечивает высокую скорость соединения – до 100 Мбит/с. Существует неэкранированная и экранированная (есть защитный экран, по структуре и свойствам напоминающий фольгу) витая пара. Обычная витая пара не предназначена для проводки сети на улице.

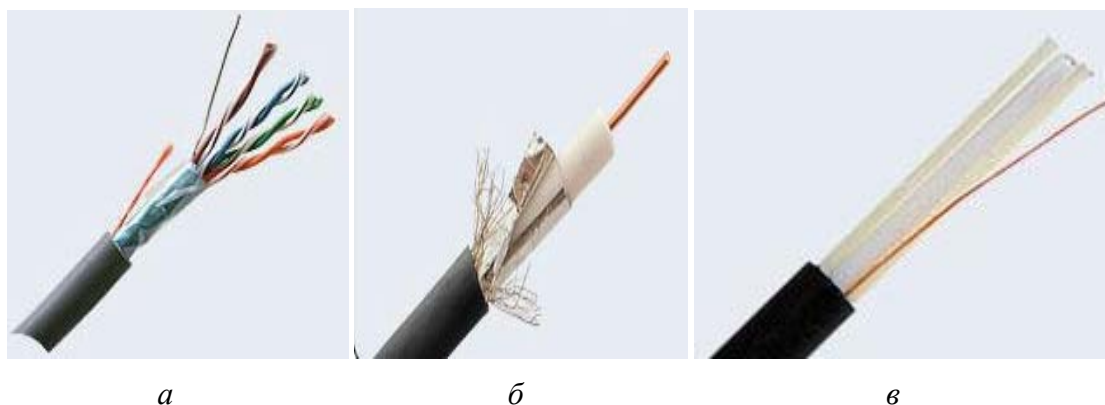


Рис. 2.9. Типы сетевых кабелей:

а – витая пара; *б* – коаксиальный кабель; *в* – оптоволоконный кабель

Коаксиальный кабель (Coaxial) – это один из первых проводников, использовавшихся для создания сетей. Содержит в себе центральный проводник, слой изолятора в медной или алюминиевой оплетке и внешнюю ПВХ изоляцию. Максимальная скорость передачи

данных – 10 Мбит/с. Кабель достаточно сильно подвержен электромагнитным наводкам. В настоящее время коаксиальный кабель в основном применяется в качестве проводника сигнала спутниковых тарелок и прочих антенн.

Оптоволоконный кабель (Optic Fiber) – кабель, который содержит несколько световодов, хорошо защищенных пластиковой изоляцией. Он обладает сверхвысокой скоростью передачи данных (до 2 Гбит/с) и абсолютно не подвержен помехам. Расстояние между системами, соединенными оптоволоконном, может достигать 100 км (высокая стоимость), но для работы требуются специальные сетевые карты, коммутаторы и т. д.

Подключение кабелей. Для этого нужен кабель пятой категории (витая пара) с легко распознаваемой цветной кодировкой внутренних жил кабеля. Различают плотный прямой кабель и мягкий крученный кабель. Жесткий прямой кабель показывает, что каждая из восьми жил состоит из сплава меди. Данный тип кабеля используется для прокладки в стены и почти не гнется. Это предполагает, что местоположение кабеля будет постоянно. Он имеет лучшую проводимость, чем мягкий крученный кабель, что позволяет его прокладывать на более длинные дистанции.

Второй тип кабеля также состоит из восьми многожильных проводов. Этот кабель очень легко гнется, его используют для небольших участков сети, где важна мобильность.

В качестве соединителей применяются модульные разъемы (коннекторы) RJ-45 (рис 2.10), имеющие восемь контактов. Для обжима сетевого кабеля используется специальный обжимной инструмент. Хорошая модель имеет пару ножниц для резки кабеля, лезвия для снятия изоляции и паз для обжима коннекторов RJ-45 (рис 2.11).



Рис. 2.10. Коннекторы



Рис. 2.11. Инструмент для обжима сетевых кабелей

Существует два вида сетевого кабеля, обычно применяемых в компьютерных сетях, – Cross-over («нуль хабный») и Straight-through (прямо проходящий, использующий хаб).

Cross-over применяется для соединения двух компьютеров через сетевые карты, напрямую, т. е. не используется ни хаб, ни коммутатор. Таким образом можно подключить только два компьютера одновременно, для подключения трех и более потребуется хаб.

Straight-through – название этого вида кабеля говорит само за себя – передает сигнал напрямую из одного конца в другой, а именно с 1-го контакта на 1-й, со 2-го на 2-й, с 3-го на 3-й и т. д. Применяется для различных видов соединений (компьютер – хаб, компьютер – DSL/ISDN/кабельный модем) или соединения хаба и коммутатора между собой.

Порядок выполнения работы

Для выполнения работы нужен кабель пятой категории (витая пара), два коннектора RJ-45, обжимной инструмент.

1. Отрезать необходимый по длине кусок кабеля. Убедиться, что концы кабеля отрезаны ровно (рис. 2.12, *а*).

2. Снять оплетку примерно на 2,5 см (рис. 2.12, *б*) (обжимной инструмент (см. рис. 2.11 на с. 17) имеет специальные лезвия для снятия оплетки). Вставить кабель до упора (с другой стороны инструмента есть ограничитель) для того, чтобы зачистить необходимую длину. Нельзя задеть сами жилы кабеля, поскольку перерезание одной из восьми жил приведет к неработоспособности.

3. Расплести жилы кабеля (рис. 2.12, *в*). Кабель состоит из четырех пар разноцветных проводов, которые нужно отсортировать по цветам (голубой – бело-голубой; оранжевый – бело-оранжевый; зеленый – бело-зеленый; коричневый – бело-коричневый).

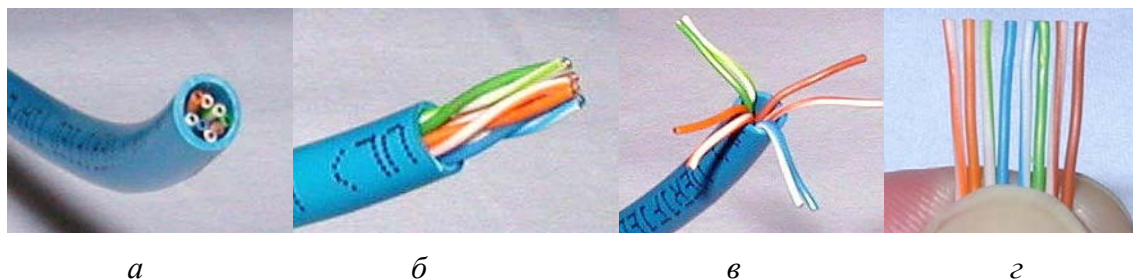


Рис. 2.12. Нарезка (*а*), зачистка (*б*), расплетка (*в*) и сортировка жил кабеля (*г*)

4. Разложить проводки (жилы) слева направо в нужной последовательности. Есть соответствующий стандарт, установленный Telecommunications Industry Association (TIA). Он называется EIA/TIA-568 Commercial Building Telecommunications Wiring Standard (бело-оранжевый, оранжевый, бело-зеленый, голубой, бело-голубой, зеленый, бело-коричневый, коричневый).

5. Отсортировать все жилы, чтобы они были прямыми и ровными (рис. 2.12, *з*). Срезать несколько миллиметров, чтобы все проводки стали одной длины и выходили за изоляцию примерно на 1,3 см. Вставить жилы в коннектор RJ-45 и проследить, чтобы оболочка не болталась на проводках. Вставлять отсортированные и выровненные жилы осторожно, как только жилы начнут попадать в пазы внутри коннектора, почувствуется сопротивление.

6. Проверить, чтобы жилы оставались в нужной последовательности (иногда при вставке кабеля в коннектор в последний момент они могут поменяться местами). Протолкнуть жилы до конца коннектора, чтобы все жилы были равной длины и касались прозрачной стенки. Если какая-то жила прошла не до конца, вынуть кабель, выровнять жилы и попробовать снова. Обратит внимание на то, что изоляционная оболочка должна проходить в коннектор и как все жилы упираться в конец коннектора (рис. 2.13).

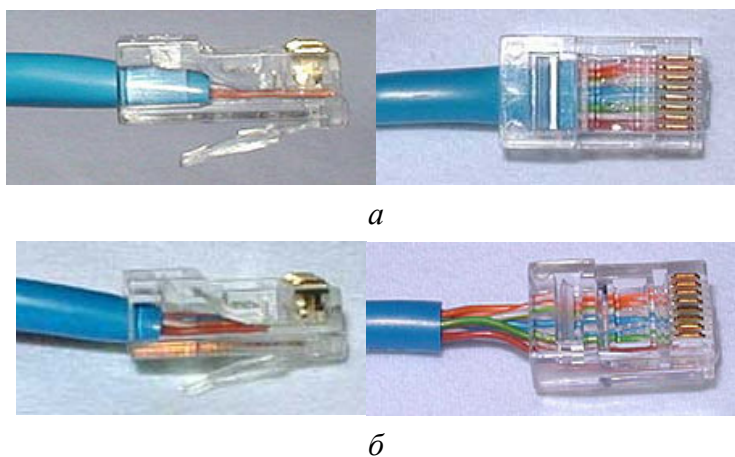


Рис. 2.13. Вставка жил кабеля в коннектор:
а – правильно; *б* – неправильно

7. Перед обжимом еще раз проверить, что все жилы выровнены и проходят до конца. Вставить коннектор в соответствующий зажим на инструменте, зажимать рукоятки плавно, чтобы не поломать коннектор (рис. 2.14). После обжима осмотреть коннектор, все контакты должны быть одной длины и утоплены в пластик.



Рис. 2.14. Обжим сетевого кабеля

8. Повторить все работы со вторым концом кабеля. Использовать те же схемы, что и на первом коннекторе, тем самым закончив приготовление Straight-through кабеля.

Cross-over кабель используется для соединения двух компьютеров между собой напрямую. Отличия этого вида от первого в том, что второй конец кабеля имеет другие цветовые схемы, которые будут рассмотрены в лабораторной работе № 4.

9. Для проверки работоспособности кабеля нужно соединить им два компьютера, например с IP-адресами 192.168.1.1 и 192.168.1.2. Затем, например, на компьютере с IP-адресом 192.168.1.2 нажать кнопку **Пуск**, выбрать в меню **Программы** подпункт меню **Сеанс MS-DOS**. В командной строке набрать **ping 192.168.1.1**. В ответ на введенную команду должен быть получен отклик примерно такой, как на рис. 2.15, что свидетельствует о том, что сетевые настройки выполнены правильно.

A screenshot of a Windows 98 command prompt window titled "Сеанс MS-DOS". The window shows the execution of the command "ping 192.168.1.1". The output displays four successful responses, each with a 32-byte size, a response time of less than 10ms, and a TTL of 128. A summary statistics line at the bottom indicates that 4 packets were sent and received, with 0% loss.

```
Microsoft(R) Windows 98
(C)Copyright Microsoft Corp 1981-1999.
E:\WINDOWS\Рабочий стол>ping 192.168.1.1
Обмен пакетами с 192.168.1.1 по 32 байт:
Ответ от 192.168.1.1: число байт=32 время<10мс TTL=128
Ответ от 192.168.1.1: число байт=32 время<10мс TTL=128
Ответ от 192.168.1.1: число байт=32 время<10мс TTL=128
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=128
Статистика Ping для 192.168.1.1:
Пакетов: послано = 4, получено = 4, потеряно = 0 (0% потерь).
Приблизительное время передачи и приема:
наименьшее = 0мс, наибольшее = 1мс, среднее = 0мс
E:\WINDOWS\Рабочий стол>
```

Рис. 2.15. Команда Ping

Лабораторная работа № 3

ОРГАНИЗАЦИЯ РАЗДЕЛЬНОГО ДОСТУПА К ПЕРИФЕРИЙНЫМ УСТРОЙСТВАМ КОМПЬЮТЕРА

Цель работы: изучить принципы и научиться организовывать раздельное пользование ресурсами компьютера, а также приобрести навыки в обеспечении раздельного использования компьютера, организации общих сетевых ресурсов.

Теоретические сведения

Одним из основных применений локальных сетей является организация общего доступа к ресурсам компьютерной системы, а именно файлам, папкам, принтерам, модемам и другому периферийному оборудованию, а также обеспечение защиты информации, хранимой на сетевых компьютерах.

В Windows NT можно установить права доступа к файлам и папкам с указанием пользователей и групп, которые имеют к ним права и предоставляемый уровень доступа. Права доступа к папкам и файлам действуют как по отношению к пользователям, работающим на локальном компьютере, где хранятся эти файлы и папки, так и к пользователям, получающим к ним доступ через сеть (если файлы расположены в разделяемых папках). Кроме того, Windows NT позволяет установить права доступа к разделяемым ресурсам, которые действуют в отношении разделяемых папок в комбинации с собственными правами доступа этих папок и файлов. Главная роль в установлении прав доступа для семейства операционных систем Microsoft Windows NT принадлежит файловой системе NTFS (New Technology File System).

NTFS обеспечивает комбинацию эффективности, надежности и совместимости, отсутствующую в FAT (File Allocation Table – «таблица размещения файлов»). NTFS – единственная файловая система в Windows NT, которая позволяет назначить разрешения для отдельных файлов.

NTFS хранит информацию о файлах в главной файловой таблице – Master File Table (MFT). NTFS имеет встроенные функции

разграничения доступа к данным для различных пользователей и групп пользователей (списки контроля доступа – Access Control Lists (ACL)), а также назначает квоты (ограничения на максимальный объем дискового пространства, занимаемый теми или иными пользователями). NTFS использует систему регистрации для повышения надежности файловой системы.

В системе с моделью безопасности, основанной на ACL, когда субъект запрашивает выполнение операции над объектом, сначала проверяется список разрешенных для этого субъекта операций и только после этого дается (или не дается) доступ к запрошенному действию.

При централизованном хранении списков контроля доступа можно говорить о *матрице доступа*, в которой по осям размещены объекты и субъекты, а в ячейках – соответствующие права.

Список доступа представляет собой структуру данных (обычно таблицу), которая содержит записи ACE (Access Control Entries), определяющие права индивидуального пользователя или группы на специальные системные объекты, такие как программы, процессы или файлы. Каждый объект в системе содержит указатель на свой ACL. Привилегии (полномочия) определяют специальные права доступа, разрешающие пользователю *читать*, *писать* или *исполнять*. В некоторых реализациях ACE могут определять право пользователя или группы на изменение ACL-объекта.

Традиционные ACL-системы назначают права индивидуальным пользователям, и со временем и ростом числа пользователей в системе списки доступа могут стать громоздкими. Выходом является назначение прав группам пользователей, а не персонально.

В сетях ACL представляют список правил, определяющих порты служб или имена доменов, доступных на узле, список узлов и/или сетей, которым разрешен доступ к сервису. Сетевые ACL могут быть настроены как на обычном сервере, так и на маршрутизаторе и могут управлять как входящим, так и исходящим трафиком.

Организация общего доступа к принтеру. Самый простой в исполнении, но самый ограниченный по возможностям вариант сетевого использования принтера, который подразумевает, что принтер, который должен быть доступен нескольким пользователям сети, подключен к одному из компьютеров и сделан общедоступным сетевым ресурсом («расшарен» от англ. share – разделение). После этого пользоваться этим принтером могут все пользователи данной сети.

Порядок выполнения работы

1. Для выполнения работы принтер уже должен быть установлен стандартным способом на компьютере, к которому он физически подключен при помощи параллельного или USB-кабеля:

- перейти в системную папку «**Принтеры**» (рис. 3.1), нажав кнопку **Пуск** и выбрав в меню **Настройка** пункт подменю **Принтеры**;
- выбрать **Установка принтера**. После чего в окне **Установка принтера** выбрать **Локальный компьютер** (рис. 3.2);

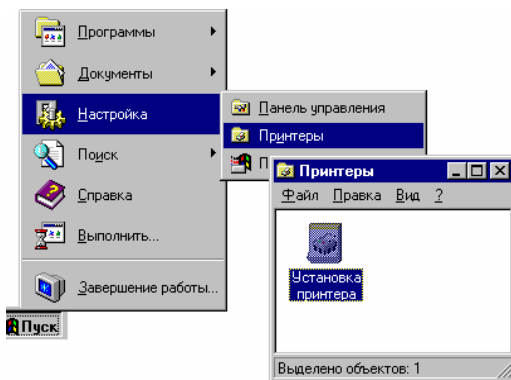


Рис. 3.1. Свойства папки

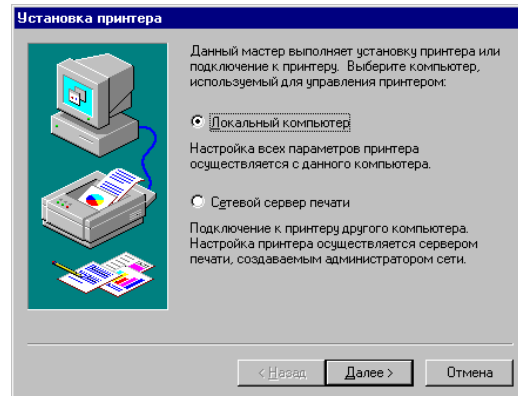


Рис. 3.2. Окно «Установка принтера»

– по окончании установки в папке «**Принтеры**» появится значок нового принтера (рис. 3.3). Принтер готов к печати документов.

2. Чтобы открыть пользователям сети доступ к принтеру, подключенному к компьютеру, для печати документов по сети нужно:

- щелкнуть на значке установленного в вашей системе принтера правой кнопкой мыши и выбрать в появившемся меню пункт **Свойства** (рис. 3.4);

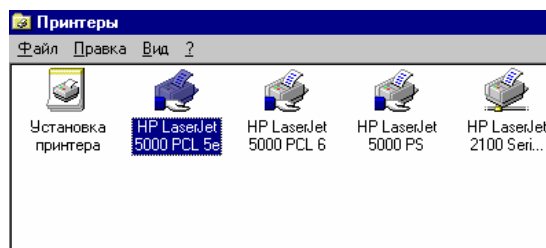


Рис. 3.3. Папка «Принтеры»

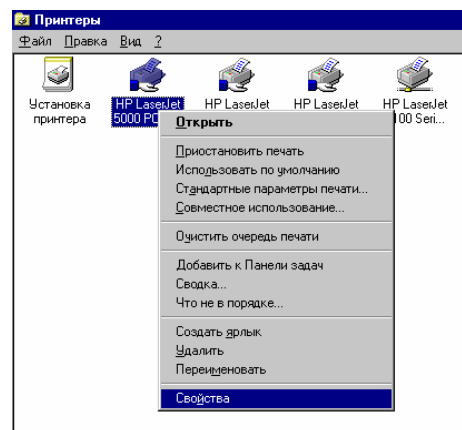


Рис. 3.4. Свойства принтера

– в окне **Свойства принтера** перейти к вкладке **Доступ** (рис. 3.5), нажать **Общий принтер** и ввести в поле **Сетевое имя** (произвольное сетевое имя принтера);

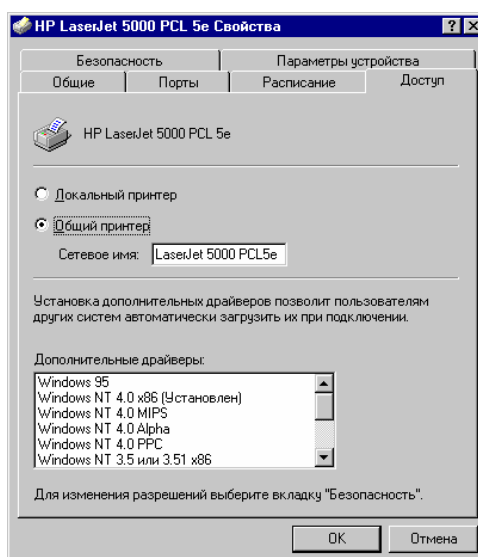



Рис. 3.5. Окно «Свойства принтера»

– щелкнуть на кнопке **ОК**, чтобы сохранить внесенные изменения. Принтер, к которому открыт сетевой доступ, будет отображаться в окне **Принтеры** с помощью специальной метки в виде изображения открытой ладони .

3. Настройка общего доступа к сетевым ресурсам. В Windows NT система организации разграничения доступа выполнена на уровне пользователей, т. е. создается список учетных записей и каждой из них присваиваются папки, к которым данный пользователь может получить доступ. Это очень удобно, не нужно помнить и вводить множество различных паролей, и в то же время система достаточно непривычная:

– выбрать **Свойства папки**, ресурсами которой вы хотите поделиться с пользователями сети, и перейти на закладку **Доступ** (рис. 3.6). Нажать на **Общий ресурс** и ввести **Сетевое имя** (по умолчанию оно будет именем папки, например laborant). Если надо ограничить полный доступ к каталогу по сети, нажать на кнопку **Разрешения...** (рис. 3.6);

– в окне **Разрешения: Общий ресурс** нажать кнопку **Добавить...**. В результате загрузится окно **Добавление пользователей и групп** (рис. 3.7). По умолчанию к каталогу имеют доступ **Все**, причем полный;

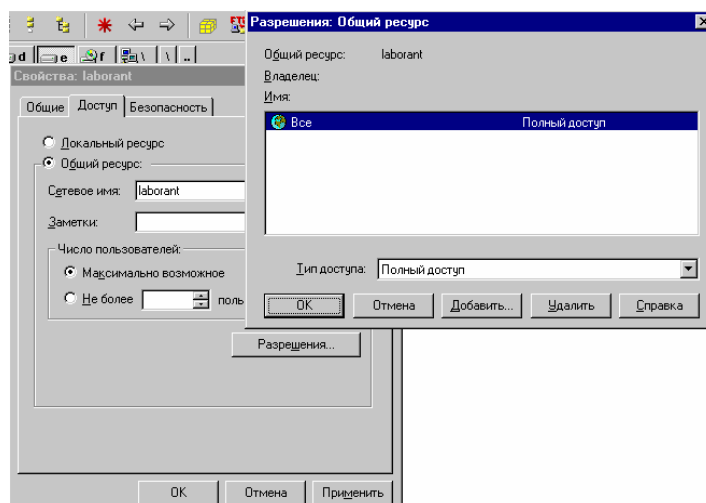


Рис. 3.6. Окно «Свойства: laborant» и «Разрешения: Общий ресурс»

– в окне **Добавление пользователей и групп** можно также выбрать только одну группу (нескольких пользователей), которой разрешено пользоваться данной папкой, например группа **Пользователи**, и назначить ей **Тип доступа**, выбрав нужный из выпадающего списка (нет доступа, чтение, изменение, полный доступ). Затем нажать кнопку **Добавить** (рис. 3.7), в окне **Добавление пользователей и групп** выбрать **Пользователи**, **Тип доступа** – **Чтение**;

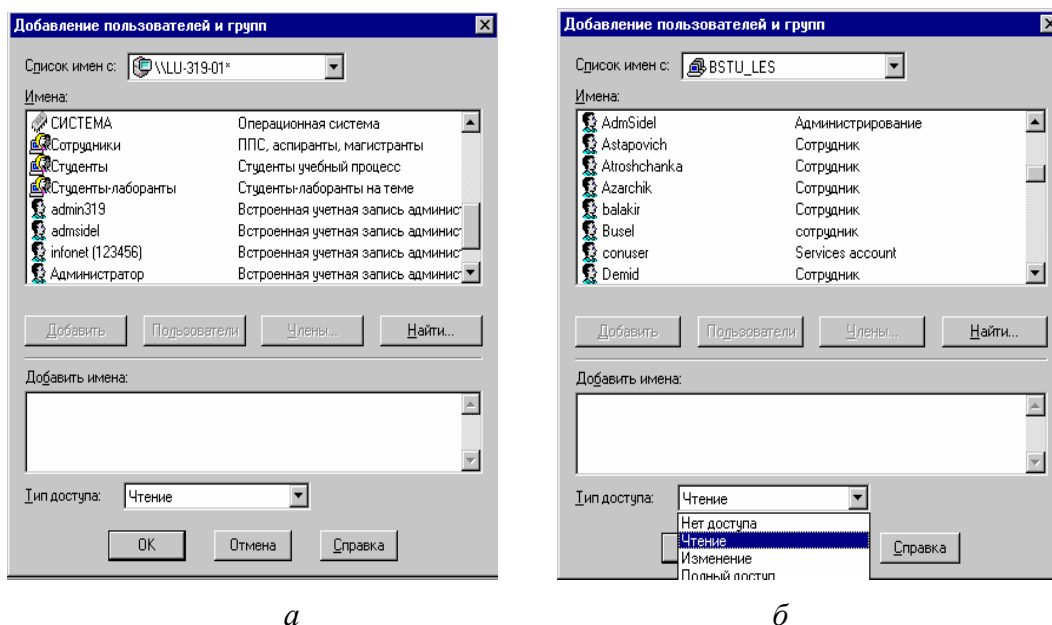


Рис. 3.7. Окно «Добавление пользователей и групп»: а – локальный; б – общий (сетевой)

– если нужны конкретные пользователи, то для их выбора нажать кнопку **Пользователи** (рис. 3.7). В результате загрузится список групп и пользователей, которые зарегистрированы локально на данном компьютере (для этого выбрать из **Списка имен с** имя компьютера, например LU-319-01 (рис. 3.7, а)). Если нужны сетевые группы и пользователи, которые зарегистрированы в домене (сервере), то нужно выбрать из **Списка имен с** имя домена, например BSTU_LES (рис. 3.7, б);

– нажать кнопку **Добавить**, в нижней табличке появится соответствующая надпись (...\Пользователи) (рис. 3.8). Если нужно еще кого-нибудь добавить, то сразу повторить предыдущее действие. Если больше ничего не надо, то щелкнуть **ОК**;

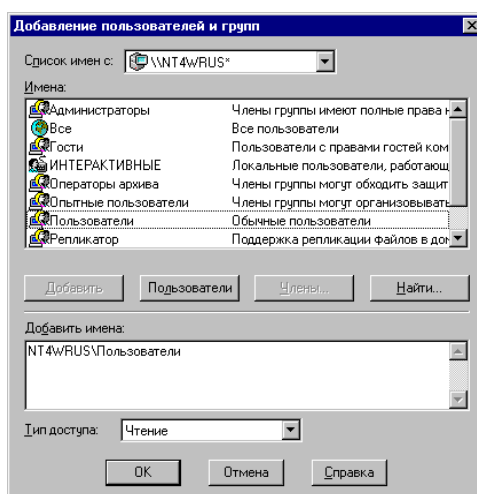


Рис. 3.8. Добавление пользователей и групп

– в окне **Разрешения: Общий ресурс** удалить полный доступ для всех к диску. Выбрать **Все – Полный доступ** (рис. 3.9) и нажать **Удалить** (рис. 3.10). Щелкнуть **ОК**;

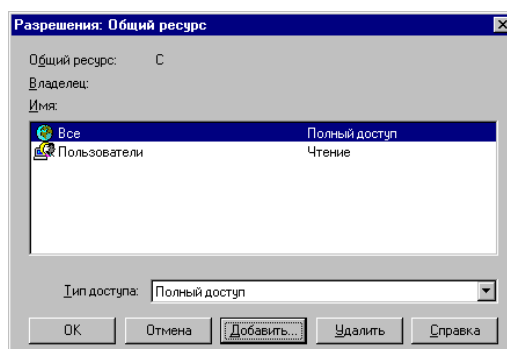


Рис. 3.9. Удаление полного доступа

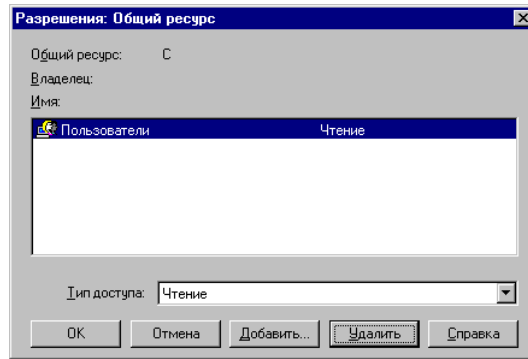


Рис. 3.10. Результат удаления

– вернуться в окно **Свойства: laborant**, нажать **ОК**. Теперь каталог (диск) будет виден в **Сетевом окружении**. К нему может подключиться каждый в соответствии с теми правами доступа, которые назначены.

Лабораторная работа № 4 ОРГАНИЗАЦИЯ ПРОСТЕЙШЕЙ СЕТИ, СОСТОЯЩЕЙ ИЗ ДВУХ КОМПЬЮТЕРОВ

Цель работы: организовать простейшую сеть, состоящую из двух компьютеров, с помощью кабеля.

Теоретические сведения

Для организации простейшей сети, которая состоит из двух компьютеров, нужны две сетевые карты, витая пара, два коннектора RJ-45.

Вся сложность в установке связи между двумя сетевыми картами заключается в особой последовательности контактов при обжиме витой пары. Здесь нужно строго следовать стандарту, иначе сеть просто не будет работать.

В данном случае используется Cross-over кабель. Отличие этого вида кабеля от Straight-through заключается в том, что второй конец кабеля имеет другие цветовые схемы. Первый конец будет идентичен Straight-through кабелю (рис. 4.1, *а*). Если внимательно посмотреть на два конца Cross-over кабеля, то можно заметить, что разница всего лишь в том, что зеленая и оранжевая пара поменялись местами, а именно меняются 1-я с 3-й и 2-я с 6-й (рис. 4.1, *б*).

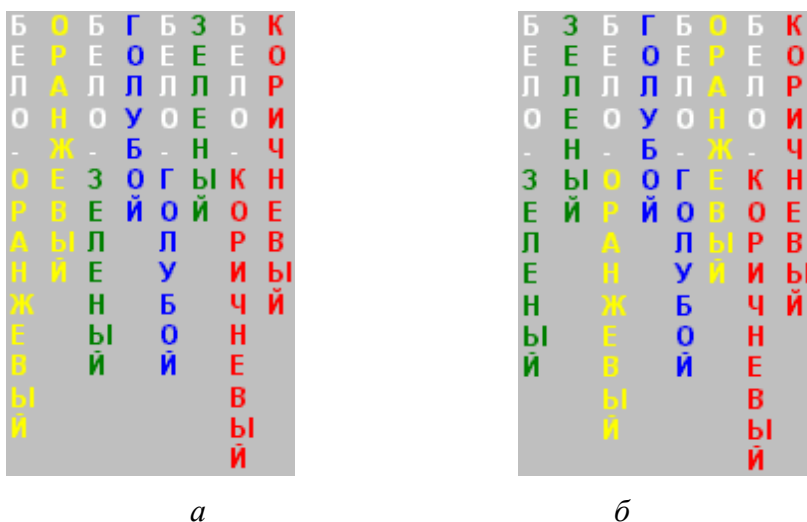


Рис. 4.1. Цветовая схема для Cross-over кабеля:
а – начало кабеля; *б* – конец кабеля

Сеть на два компьютера создают, если есть только еще один компьютер, или для обмена данными с ноутбуком. При дальнейшем расширении сети лучше установить Hub или Switch и заново обжать сетевые кабели.

Порядок выполнения работы

Каждый компьютер при установке сетевой карты получает IP-адрес (см. рис. 1.6 на с. 9). В нашем случае IP-адрес одного компьютера будет 192.168.1.1, а компьютера, с которым нужно организовать сеть, – 192.168.1.2 (маска 255.255.255.0). Компьютеры должны находиться в одной рабочей группе (рис. 4.2), иначе каждый будет являться администратором своего компьютера и иметь равные права в сети, что в будущем может привести к краху сети:

1. Создать локального пользователя администратора, нажав кнопку **Пуск** и выбрав в меню **Программы** команду **Администрирование (Общее)**, а затем **Диспетчер пользователей** (рис. 4.2).

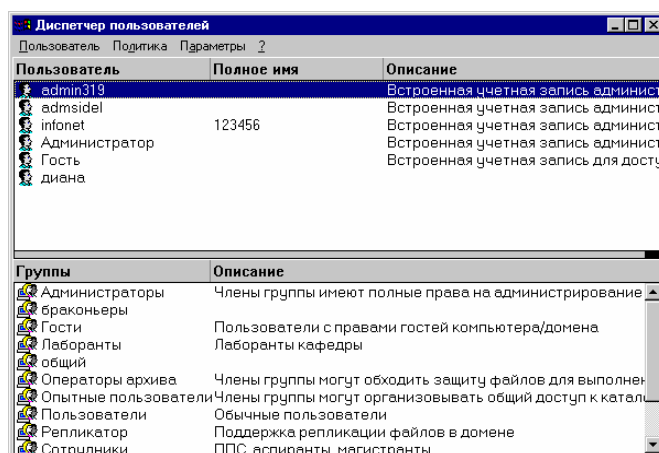


Рис. 4.2. Окно «Диспетчер пользователей»

2. Создать копию admin319. Для этого подсветить пользователя admin319 (рис. 4.2), выбрать пункт меню **Пользователь** → **Копировать**, ввести имя **inonet** и пароль (указан на двери кабинета), щелкнуть **ОК** (рис. 4.3).

3. Выйти из домена, выполнив команды **Сетевое окружение** → **Свойства** → **Изменить** → **Рабочая группа** → **BSTU_LES** (рис. 4.4 и 4.5).

4. Поменять IP-адрес первого компьютера (протокол TCP/IP → IP-адрес 192.168.1.1 маска 255.255.255.0) и IP-адрес второго компьютера (протокол TCP/IP → IP-адрес 192.168.1.2 маска 255.255.255.0).

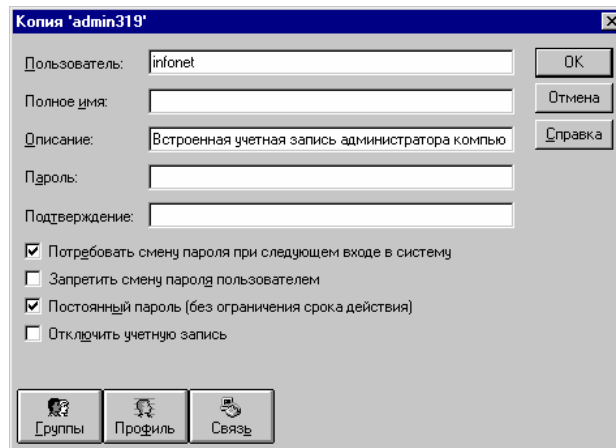


Рис. 4.3. Создание пользователя

5. Чтобы новые изменения вступили в силу, произвести перезагрузку компьютера. После перезагрузки зайти в сетевое окружение.

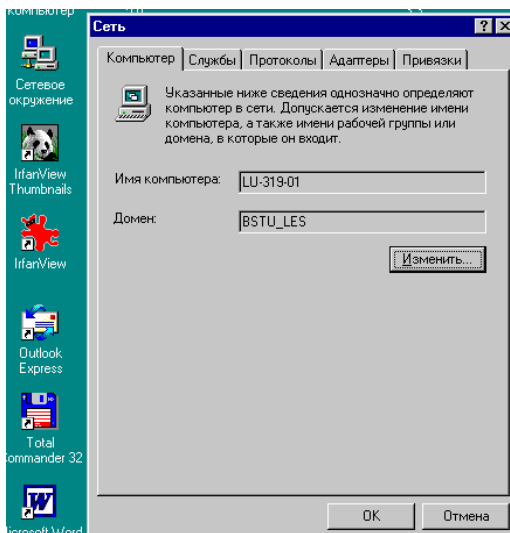


Рис. 4.4. Выход из домена

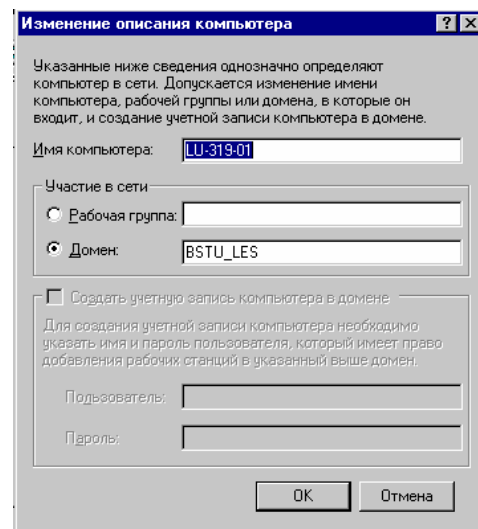


Рис. 4.5. Создание рабочей группы

Если все предыдущие действия выполнены правильно, то в сети будут видны только два компьютера – только те компьютеры, которые находятся в одном сетевом сегменте. Для проверки нужно выполнить команду **Ping** (см. рис. 2.15 на с. 20), как показано в лабораторной работе № 2.

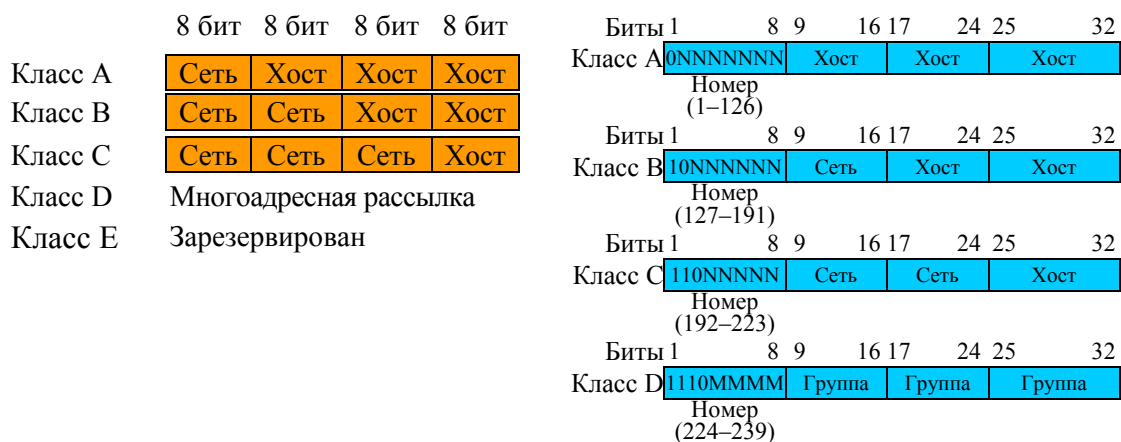
Лабораторная работа № 5

ОРГАНИЗАЦИЯ ЛОКАЛЬНОЙ СЕТИ, ДЕЛЕНИЕ СЕТИ НА СЕГМЕНТЫ (ПОДСЕТИ)

Цель работы: изучить типы и классы IP-адресов, основные принципы деления сети на сегменты (подсети).

Теоретические сведения

IP-адрес представляет собой основной тип адресов, на основе которых производится структуризация сети. IP-адрес состоит из 4 байт, записывается в десятичном виде и каждый байт разделяется точкой. IP-адрес состоит из двух частей: первая часть включает номер сети, вторая часть – номер узла в сети. 128.10.2.30 – традиционная десятичная форма представления адреса, 10000000.00001010.00000010.00011110 – двоичная форма представления этого же адреса [1]. На рис. 5.1 показаны форматы классов IP-адресов и деление IP-адресов на классы.



a

б

Рис. 5.1. Форматы классов IP-адресов (*a*) и деление IP-адресов на классы (*б*)

Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса [1].

Каждому классу сетей соответствуют диапазоны номеров сетей: класс А 1.0.0.0–126.0.0.0; класс В 128.0.0.0–191.255.0.0; класс С 192.0.1.0–223.255.255.0; класс D 224.0.0.0–239.255.255.255; класс E 240.0.0.0–247.255.255.255.

В протоколе IP существует несколько соглашений о специальных адресах: broadcast, multicast, loopback [1].

Различают следующие типы адресов: физический (MAC-адрес 11-A0-17-3D-BC-01), сетевой (IP-адрес 109.26.17.100) и символьный (DNS-имя – доменный адрес, например microsoft.com).

Форматы адреса. IPv4 – IP-адрес, представляющий собой 32-битовое двоичное число 10000000.00001010.00000010.00011110. Традиционной десятичной формой представления адреса является 128.10.2.30.

IPv6 – IP-адрес, имеющий 128-битовое представление, например fe80:0:0:0:200:f8ff:fe21:67cf.

IP-адреса могут быть динамическими или статическими. Они используются для идентификации устройств в сети. С целью взаимодействия по сети IP-адрес должен быть назначен каждому сетевому устройству (в том числе компьютерам, серверам, маршрутизаторам, принтерам и т. д.). Такие устройства в сети называют *хостами*.

Одна часть IP-адреса представляет собой номер сети, другая – идентификатор хоста. Точно так же, как у разных домов на одной улице в адресе присутствует одно и то же название улицы, у хостов в сети в адресе имеется общий номер сети. И точно так же, как у различных домов есть собственный номер дома, у каждого хоста в сети имеется собственный уникальный идентификационный номер – идентификатор хоста. Номер сети используется маршрутизаторами для передачи пакетов в нужные сети, тогда как идентификатор хоста определяет конкретное устройство в этой сети, которому должны быть доставлены пакеты.

Структура. IP-адрес состоит из четырех частей, записанных в виде десятичных чисел с точками (например, 192.168.1.1). Каждую из этих четырех частей называют *октетом*. Октет представляет собой восемь двоичных цифр (например, 11000000, или 192 в десятичном виде). Таким образом, каждый октет может принимать в двоичном виде значения от 00000000 до 11111111, или от 0 до 255 в десятичном виде. На рис. 5.2 показан пример IP-адреса, в котором первые три октета (192.168.1) представляют собой номер сети, а четвертый октет (16) – идентификатор хоста.

Количество двоичных цифр в IP-адресе, которые приходятся на номер сети, и количество цифр в адресе, приходящихся на идентификатор хоста, могут быть различными в зависимости от маски подсети.

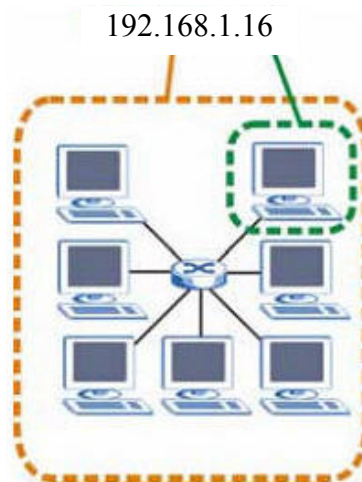


Рис. 5.2. Номер сети и идентификатор хоста

Частные IP-адреса. У каждого хоста в сети Интернет должен быть уникальный адрес. Если сеть изолирована от Интернета (например, связывают два отдела), для хостов без проблем можно использовать любые IP-адреса. Однако уполномоченной организацией по распределению нумерации в сети Интернет (IANA) специально для частных сетей зарезервированы следующие три блока IP-адресов: 10.0.0.0–10.255.255.255; 172.16.0.0–172.31.255.255; 192.168.0.0–192.168.255.255.

Маски подсети. Маска подсети определяет, какая часть адреса относится к хосту и какая – к сети. Для этого используется логическая операция «И» (AND). Операция «И» в двоичной арифметике выполняется очень просто. Она, по сути, представляет собой умножение значений в одинаковых позициях (рис. 5.3). Чтобы определить адрес сети (ту часть IP-адреса, которая устанавливает, к какой сети он относится), достаточно просто перемножить значения позиций двоичного представления IP-адреса и значения соответствующих позиций двоичного представления маски подсети. Результатом является двоичное число, которое нужно снова преобразовать в десятичное, чтобы узнать адрес сети.

		Сеть		Хост	
IP-адрес	172.16.2.160	10101100	00010000	00000010	10100000
Маска сети	255.255.0.0	11111111	11111111	00000000	00000000
Результат операции «И»		10101100	00010000	00000000	00000000
Адрес сети		172	16	0	0

Рис. 5.3. Применение операции «И»

Маршрутизацией называется действие по перенаправлению пакета из одной логической сети (или подсети) в другую. Маска подсети позволяет более рационально использовать адресное пространство (рис. 5.4) и определяет, какие биты являются частью номера сети, а какие – частью идентификатора хоста. Маска подсети включает в себя 32 бита. Если бит в маске подсети равен «1», то соответствующий бит IP-адреса является частью номера сети. Если бит в маске подсети равен «0», то соответствующий бит IP-адреса является частью идентификатора хоста. Маска подсети, выделяющая номер сети (полужирным шрифтом), и идентификатор хоста в IP-адресе, который в десятичном виде записывается как 192.168.1.2, представлены в табл. 5.1.

Таблица 5.1

Пример выделения номера сети и идентификатора хоста в IP-адресе

Наименование	1-й октет (192)	2-й октет (168)	3-й октет (1)	4-й октет (2)
IP-адрес (двоичный)	11000000	10101000	00000001	00000010
Маска подсети (двоичная)	11111111	11111111	11111111	00000000
Номер сети	11000000	10101000	00000001	
Идентификатор хоста				00000010

Маски подсети всегда состоят из серии последовательных единиц, начиная с самого левого бита маски, за которой следует серия последовательных нулей, составляющих в общей сложности 32 бита.

Маску подсети можно определить как количество бит в адресе, представляющих номер сети (количество бит со значением «1»). Например, 8-битной маской называют маску, в которой 8 бит – единичные, а остальные 24 бита – нулевые. Маски подсети записываются в формате десятичных чисел с точками, как и IP-адреса. В следующих примерах показаны двоичная и десятичная запись 8-битной, 16-битной, 24-битной и 29-битной масок подсети (табл. 5.2).

Таблица 5.2

Маски подсети

Маска	Двоичная				Десятичная
	1-й октет	2-й октет	3-й октет	4-й октет	
8-битная	11111111	00000000	00000000	00000000	255.0.0.0
16-битная	11111111	11111111	00000000	00000000	255.255.0.0
24-битная	11111111	11111111	11111111	00000000	255.255.255.0
29-битная	11111111	11111111	11111111	11111000	255.255.255.248

0	00000000	16	00010000	32	00100000	48	00110000	64	01000000	80	01010000	96	01100000	112	01110000
1	00000001	17	00010001	33	00100001	49	00110001	65	01000001	81	01010001	97	01100001	113	01110001
2	00000010	18	00010010	34	00100010	50	00110010	66	01000010	82	01010010	98	01100010	114	01110010
3	00000011	19	00010011	35	00100011	51	00110011	67	01000011	83	01010011	99	01100011	115	01110011
4	00000100	20	00010100	36	00100100	52	00110100	68	01000100	84	01010100	100	01100100	116	01110100
5	00000101	21	00010101	37	00100101	53	00110101	69	01000101	85	01010101	101	01100101	117	01110101
6	00000110	22	00010110	38	00100110	54	00110110	70	01000110	86	01010110	102	01100110	118	01110110
7	00000111	23	00010111	39	00100111	55	00110111	71	01000111	87	01010111	103	01100111	119	01110111
8	00001000	24	00011000	40	00101000	56	00111000	72	01001000	88	01011000	104	01101000	120	01111000
9	00001001	25	00011001	41	00101001	57	00111001	73	01001001	89	01011001	105	01101001	121	01111001
10	00001010	26	00011010	42	00101010	58	00111010	74	01001010	90	01011010	106	01101010	122	01111010
11	00001011	27	00011011	43	00101011	59	00111011	75	01001011	91	01011011	107	01101011	123	01111011
12	00001100	28	00011100	44	00101100	60	00111100	76	01001100	92	01011100	108	01101100	124	01111100
13	00001101	29	00011101	45	00101101	61	00111101	77	01001101	93	01011101	109	01101101	125	01111101
14	00001110	30	00011110	46	00101110	62	00111110	78	01001110	94	01011110	110	01101110	126	01111110
15	00001111	31	00011111	47	00101111	63	00111111	79	01001111	95	01011111	111	01101111	127	01111111
128	10000000	144	10010000	160	10100000	176	10110000	192	11000000	208	11010000	224	11100000	240	11110000
129	10000001	145	10010001	161	10100001	177	10110001	193	11000001	209	11010001	225	11100001	241	11110001
130	10000010	146	10010010	162	10100010	178	10110010	194	11000010	210	11010010	226	11100010	242	11110010
131	10000011	147	10010011	163	10100011	179	10110011	195	11000011	211	11010011	227	11100011	243	11110011
132	10000100	148	10010100	164	10100100	180	10110100	196	11000100	212	11010100	228	11100100	244	11110100
133	10000101	149	10010101	165	10100101	181	10110101	197	11000101	213	11010101	229	11100101	245	11110101
134	10000110	150	10010110	166	10100110	182	10110110	198	11000110	214	11010110	230	11100110	246	11110110
135	10000111	151	10010111	167	10100111	183	10110111	199	11000111	215	11010111	231	11100111	247	11110111
136	10001000	152	10011000	168	10101000	184	10111000	200	11001000	216	11011000	232	11101000	248	11111000
137	10001001	153	10011001	169	10101001	185	10111001	201	11001001	217	11011001	233	11101001	249	11111001
138	10001010	154	10011010	170	10101010	186	10111010	202	11001010	218	11011010	234	11101010	250	11111010
139	10001011	155	10011011	171	10101011	187	10111011	203	11001011	219	11011011	235	11101011	251	11111011
140	10001100	156	10011100	172	10101100	188	10111100	204	11001100	220	11011100	236	11101100	252	11111100
141	10001101	157	10011101	173	10101101	189	10111101	205	11001101	221	11011101	237	11101101	253	11111101
142	10001110	158	10011110	174	10101110	190	10111110	206	11001110	222	11011110	238	11101110	254	11111110
143	10001111	159	10011111	175	10101111	191	10111111	207	11001111	223	11011111	239	11101111	255	11111111

Рис. 5.4. Адресное пространство

Размер сети. Количество разрядов в номере сети определяет максимальное количество хостов (табл. 5.3), которые могут находиться в такой сети. Чем больше бит в номере сети, тем меньше бит остается на идентификатор хоста в адресе. IP-адрес с идентификатором хоста из всех нулей представляет собой IP-адрес сети (например, 192.168.1.0 с 24-битной маской подсети). IP-адрес с идентификатором хоста из всех единиц представляет собой широковещательный адрес данной сети (например, 192.168.1.255 с 24-битной маской подсети). Поэтому такие IP-адреса не могут использоваться в качестве идентификаторов отдельных хостов.

Таблица 5.3

Максимально возможное число хостов

Маска подсети		Размер идентификатора хоста, бит	Максимальное количество хостов	
8-битная	255.0.0.0	24	$2^{24}-2$	16 777 214
16-битная	255.255.0.0	16	$2^{16}-2$	65 534
24-битная	255.255.255.0	8	2^8-2	254
29-битная	255.255.255.248	3	2^3-2	6

Формат записи. Поскольку маска всегда является последовательностью единиц слева, дополняемой серией нулей до 32 бит, можно просто указывать количество единиц, а не записывать значение каждого октета. Обычно записывается «/» после адреса и количество единичных бит в маске (сетевой префикс). Например, адрес 192.1.1.0 /25 представляет собой адрес 192.1.1.0 с маской 255.255.255.128. Некоторые возможные маски подсети в обоих форматах даны в табл. 5.4.

Таблица 5.4

Альтернативный формат записи маски подсети

Маска подсети	Альтернативный формат записи	Последний октет (в двоичном виде)	Последний октет (в десятичном виде)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

Формирование подсетей. С помощью подсетей одну сеть можно разделить на несколько сетей. Сеть компании имеет адрес 192.168.1.0 (маска подсети 255.255.255.0). Первые три октета адреса (192.168.1) представляют собой номер сети, а оставшийся октет – идентификатор хоста, что позволяет использовать в сети максимум $2^8 - 2 = 254$ хоста.

Сеть до ее деления на подсети показана на рис. 5.5.

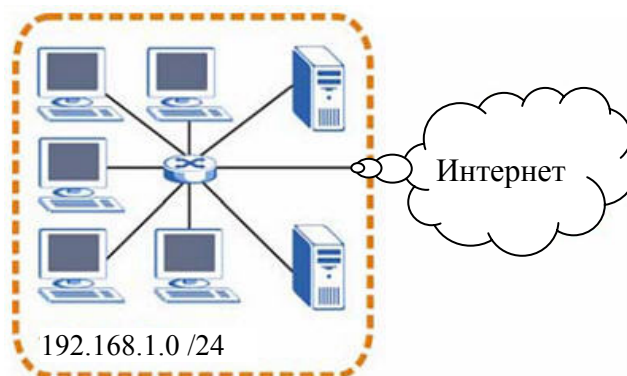


Рис. 5.5. Пример формирования подсетей до деления на подсети

Чтобы разделить сеть 192.168.1.0 на две отдельные подсети, можно «позаимствовать» один бит из идентификатора хоста. В этом случае маска подсети станет 25-битной (255.255.255.128, или /25).

«Одолженный» бит идентификатора хоста может быть либо нулем, либо единицей, что дает нам две подсети: 192.168.1.0 /25 и 192.168.1.128 /25. Сеть после ее деления на подсети показана на рис. 5.6. Теперь она включает в себя две подсети: **A** и **B**.

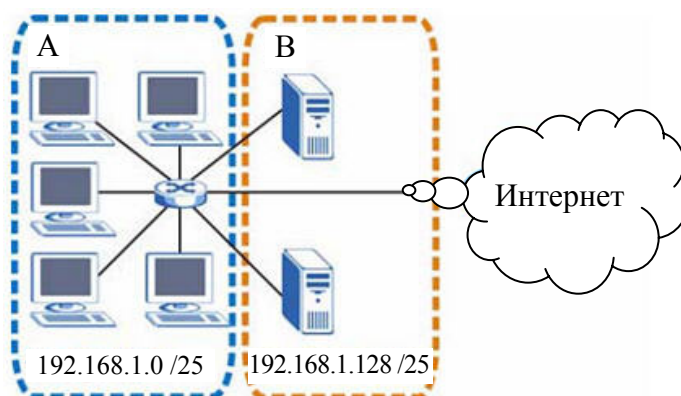


Рис. 5.6. Пример формирования подсетей после деления на подсети

В 25-битной подсети на идентификатор хоста выделяется 7 бит, поэтому в каждой подсети может быть максимум $2^7 - 2 = 126$ хостов (идентификатор хоста из всех нулей – это сама подсеть, а из всех единиц – широковещательный адрес для подсети). Адрес 192.168.1.0 с маской 255.255.255.128 является адресом подсети **A**, а адрес 192.168.1.127 с маской 255.255.255.128 является ее широко-вещательным адресом. Таким образом, наименьший IP-адрес, который может быть закреплен за действительным хостом в подсети **A**, – это 192.168.1.1, а наибольший – 192.168.1.126. Аналогичным образом диапазон идентификаторов хоста для подсети **B** составляет от 192.168.1.129 до 192.168.1.254.

Когда количество хостов в подсети неодинаково, более эффективным явилось бы разбиение сети на подсети разного размера с использованием масок переменной длины (VLSM (Variable Length Subnet Mask) – совокупность присвоенных одному адресу масок подсетей).

Маска подсети переменной длины позволяет более эффективно использовать выделенное организации адресное пространство протокола IP, значительное уменьшение количества маршрутной информации внутри домена за счет объединения маршрутов.

На рис. 5.7 сеть класса А с адресом 10.0.0.0 сначала разделяется на подсети с сетевым префиксом /16 (маска подсети 255.255.0.0). Общее количество получаемых подсетей – 254. В каждой подсети поддерживается до 65 534 ($2^{16} - 2 = 65\,534$) индивидуальных адресов хостов. Полученная подсеть с адресом 10.253.0.0 при делении с сетевым префиксом /24 содержит 254 подсети, каждая из которых поддерживает до 254 ($2^8 - 2 = 254$) индивидуальных адресов хостов. При дальнейшем делении с сетевым префиксом /27 подсеть с адресом 10.253.1.0 состоит из 6 подсетей с номерами, кратными 32, каждая из которых поддерживает до 30 ($2^5 - 2 = 30$) индивидуальных номеров хостов.

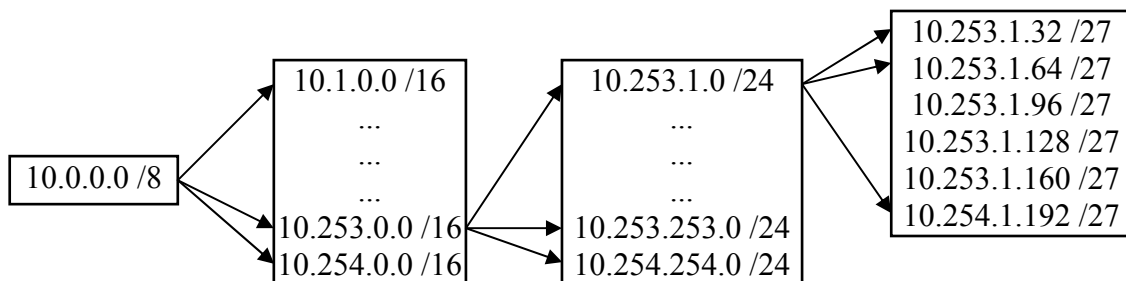


Рис. 5.7. Пример деления адресов подсетей с использованием масок переменной длины

Каждый маршрутизатор может объединять свои подсети в одной записи в сообщении об обновлении. Структура подсетей вне организации не видна, поэтому маршрутизатор (M1) показывает в сети Интернет маршрут с адресом 10.0.0.0 (рис. 5.8).

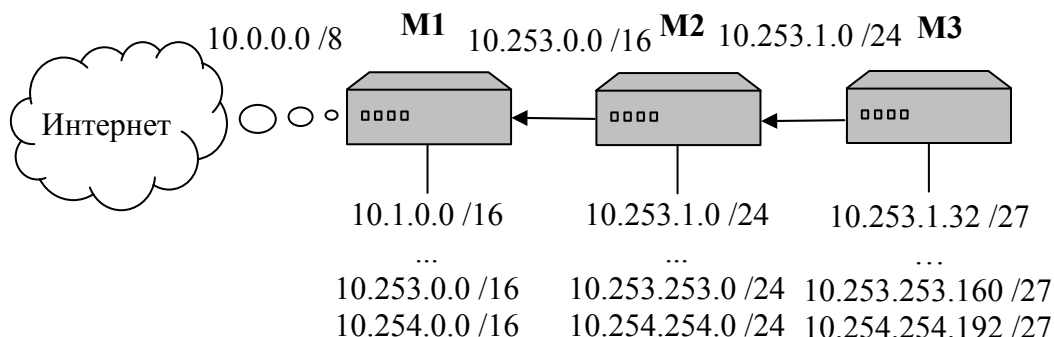


Рис. 5.8. Объединение маршрутов с помощью маски подсети переменной длины

При делении сети на подсети с использованием маски подсети переменной длины администратор должен проверить диапазон адресов, который должен иметь достаточное количество бит для формирования требуемого числа подсетей.

Порядок выполнения работы

1. Разделить на четыре подсети:

– для разделения 24-битного адреса на четыре подсети потребуется «одолжить» два бита идентификатора хоста, чтобы получить четыре возможные комбинации (00, 01, 10 и 11). Маска подсети состоит из 26 бит (11111111.11111111.11111111.11000000), т. е. 255.255.255.192;

– каждая подсеть (табл. 5.5–5.8) содержит 6 битов идентификатора хоста, что в сумме дает $2^6 - 2 = 62$ хоста для каждой подсети (идентификатор хоста из всех нулей – это сама подсеть, а из всех единиц – широковещательный адрес для подсети).

Таблица 5.5

Подсеть 1

IP-адрес/маска подсети	Номер сети	Значение последнего октета
IP-адрес (десятичный)	192.168.1	0
IP-адрес (двоичный)	11000000.10101000.00000001	00000000
Маска подсети (двоичная)	11111111.11111111.11111111	11000000

Окончание табл. 5.5

IP-адрес/маска подсети	Номер сети	Значение последнего октета
Адрес подсети 192.168.1.0	Наименьший идентификатор хоста: 192.168.1.1	
Широковещательный адрес 192.168.1.63	Наибольший идентификатор хоста: 192.168.1.62	

Таблица 5.6

Подсеть 2

IP-адрес/маска подсети	Номер сети	Значение последнего октета
IP-адрес (десятичный)	192.168.1	64
IP-адрес (двоичный)	11000000.10101000.00000001	01000000
Маска подсети (двоичная)	11111111.11111111.11111111	11000000
Адрес подсети 192.168.1.64	Наименьший идентификатор хоста: 192.168.1.65	
Широковещательный адрес 192.168.1.127	Наибольший идентификатор хоста: 192.168.1.126	

Таблица 5.7

Подсеть 3

IP-адрес/маска подсети	Номер сети	Значение последнего октета
IP-адрес (десятичный)	192.168.1	128
IP-адрес (двоичный)	11000000.10101000.00000001	10000000
Маска подсети (двоичная)	11111111.11111111.11111111	11000000
Адрес подсети 192.168.1.128	Наименьший идентификатор хоста: 192.168.1.129	
Широковещательный адрес 192.168.1.191	Наибольший идентификатор хоста: 192.168.1.190	

Таблица 5.8

Подсеть 4

IP-адрес/маска подсети	Номер сети	Значение последнего октета
IP-адрес (десятичный)	192.168.1	192
IP-адрес (двоичный)	11000000.10101000.00000001	11000000
Маска подсети (двоичная)	11111111.11111111.11111111	11000000
Адрес подсети 192.168.1.192	Наименьший идентификатор хоста: 192.168.1.193	
Широковещательный адрес 192.168.1.255	Наибольший идентификатор хоста: 192.168.1.254	

2. Разделить на восемь подсетей:

– для создания восьми подсетей используется 27-битная маска (000, 001, 010, 011, 100, 101, 110 и 111). Значения последнего октета IP-адреса для каждой подсети представлены в табл. 5.9;

Таблица 5.9

Восемь подсетей

Подсеть	Адрес подсети	Первый адрес	Последний адрес	Широковещательный адрес
1	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31
2	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63
3	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
4	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127
5	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159
6	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191
7	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223
8	192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255

– сводная информация по планированию подсетей для сети с 24-битным номером сети приведена в табл. 5.10.

Таблица 5.10

Планирование подсетей для сети с 24-битным номером

Количество «одолженных» битов идентификатора хоста	Маска подсети	Количество подсетей	Количество хостов в подсети
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Пример. Рассчитать количество подсетей и хостов в подсети на основе IP-адреса и маски подсети 59.124.163.151 /27 (/27 – префикс сети или сетевая маска). В формате двоичных чисел 11111111.11111111.11111111.11100000. В формате десятичных чисел 255.255.255.224. В четвертом поле (последний октет) 11100000 первые 3 бита определяют число подсетей ($2^3 = 8$), а последние 5 бит – число хостов подсети ($2^5 = 32$).

Диапазон IP первой подсети 0–31 (32 хоста), но 0 – это номер подсети, а 31 – это broadcast. Максимальное число хостов данной подсети – 30.

Первая подсеть: 59.124.163.0. Broadcast первой подсети: 59.124.163.31.

Диапазон IP второй подсети с 59.124.163.32 по 59.124.163.63.

Вторая подсеть: 59.124.163.32. Broadcast второй подсети: 59.124.163.63.

Диапазон IP восьмой подсети с 59.124.163.224 по 59.124.163.255.

Восьмая подсеть: 59.124.163.224. Broadcast восьмой подсети: 59.124.163.255.

IP-адрес 59.124.163.151 находится в пятой подсети. Пятая подсеть: 59.124.163.128 /27.

Диапазон IP пятой подсети с 59.124.163.128 по 59.124.163.159. Broadcast пятой подсети: 59.124.163.159.

Лабораторная работа № 6

ОРГАНИЗАЦИЯ УДАЛЕННОГО ДОСТУПА К СЕТИ

Цель работы: научиться организовывать удаленный доступ к сети Интернет через модем по коммутируемому беспарольному доступу.

Теоретические сведения

Удаленный доступ включает в себя различные типы и варианты взаимодействия компьютеров, сетей и приложений. Для удаленного доступа, как правило, характерна несимметричность взаимодействия, когда с одной стороны имеется центральная крупная сеть или центральный компьютер, а с другой – отдельный удаленный терминал, компьютер или небольшая сеть, требующие доступ к информационным ресурсам центральной сети.

Типы взаимодействующих систем. На рис. 6.1 приведены основные схемы удаленного доступа, отличающиеся типом взаимодействующих систем: терминал – компьютер (1); компьютер – компьютер (2); компьютер – сеть (3); сеть – сеть (4).

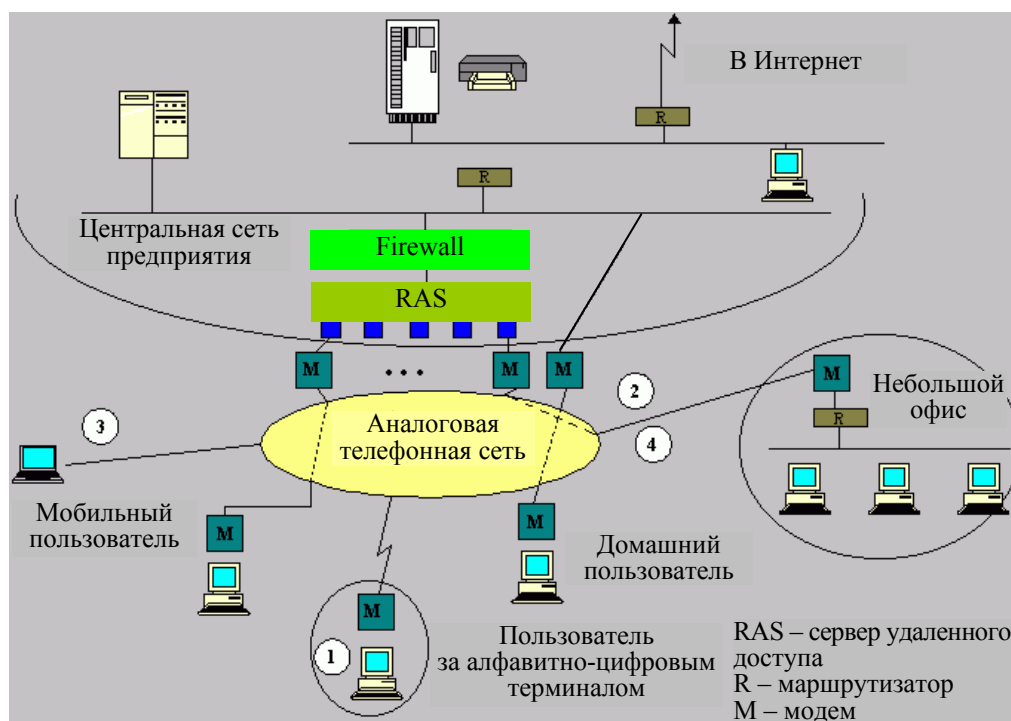


Рис. 6.1. Общая схема удаленного доступа

Типы предоставляемого сервиса. Схемы удаленного доступа могут отличаться также и типом сервиса, который предоставляется удаленному клиенту. Наиболее часто используется удаленный доступ к файлам, базам данных, принтерам, обмен с центральной сетью сообщениями электронной почты или факсами [3].

Терминальный доступ. Это способ, при котором пользователь получает возможность удаленно работать с компьютером таким же образом, как если бы он управлял им с помощью локально подключенного терминала. В данном режиме он может запускать на выполнение программы на удаленном компьютере и видеть результаты их работы.

Любой вариант терминального доступа требует, чтобы компьютер центрального подразделения предприятия был непосредственно подключен к территориальной сети, с помощью которой осуществляется доступ, т. е. к телефонной сети. Наиболее популярным средством является протокол telnet TCP/IP.

Удаленный узел. В отличие от систем терминального доступа, превращающих компьютер пользователя в эмулятор экрана центрального компьютера, средства поддержки режима удаленного узла (remotenode) делают вызывающий компьютер полноправным членом локальной сети. Это достигается за счет того, что на удаленном компьютере работают те же протоколы, что и в компьютерах центральной локальной сети, за исключением протоколов канального и физического уровня.

На этом уровне вместо традиционных протоколов Ethernet или Token Ring работают модемные протоколы (физический уровень) и канальные протоколы соединений «точка – точка», например PPP. Эти протоколы используются для передачи по телефонным сетям пакетов сетевого уровня и других протоколов верхних уровней. Таким образом, осуществляется полноценная связь удаленного узла с остальными узлами сети.

Сервис удаленного узла обеспечивает данному узлу транспортное соединение с локальной сетью, поэтому на удаленном узле могут использоваться все те сервисы, которые доступны локальным клиентам сети, например сервис telnet или администрирование Windows NT.

Основное отличие удаленного узла от локальных – низкая скорость сетевого обмена (до 28,8 Кб/с). Данная скорость обмена делает проблематичным работу многих приложений, написанных в расчете на работу по локальной сети.

Удаленное управление. Существует множество систем удаленного управления, поддерживающих эмуляцию графического экрана настольных операционных систем, при наличии в них протокола эмуляции терминала по сети.

Для эмуляции среды операционной системы Windows необходимо иметь дополнительные программные средства, которые включают как клиентскую, так и серверную части программы эмуляции терминала. Для повышения производительности этих средств применяют также сжатие и кэширование данных.

Порядок выполнения работы

Для использования удаленного доступа через модемное соединение к сети Интернет необходимо:

1. Подключить модем, произвести настройку порта и параметров сети. Правой кнопкой мыши щелкнуть на значке **Сетевое окружение** и в появившемся меню выбрать пункт **Свойства** (рис. 6.2).

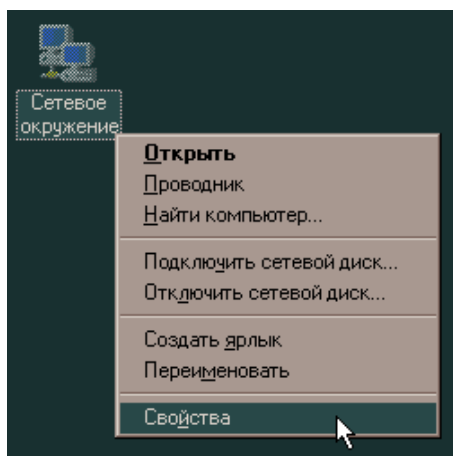


Рис. 6.2. Свойства компьютера

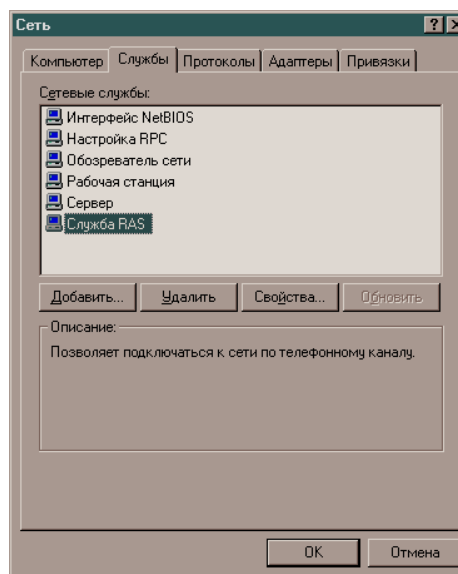


Рис. 6.3. Окно «Сеть»

2. Выбрать закладку **Службы** (рис. 6.3). Обратить внимание на наличие **Службы RAS** (Remote Access Service). Если ее нет, то ее необходимо будет установить:

- выбрать кнопку **Добавить...**;
- в процессе установки **Службы RAS** появится окно **Установка службы удаленного доступа** (рис. 6.4). Оно появится, если при

наличии **Службы RAS** выбрать ее в списке, после чего нажать кнопку **Свойства**;

– в этом окне (см. рис. 6.3 на с. 45) нажать кнопку **Сеть...**. Появится окно **Настройка сети** (рис. 6.5);

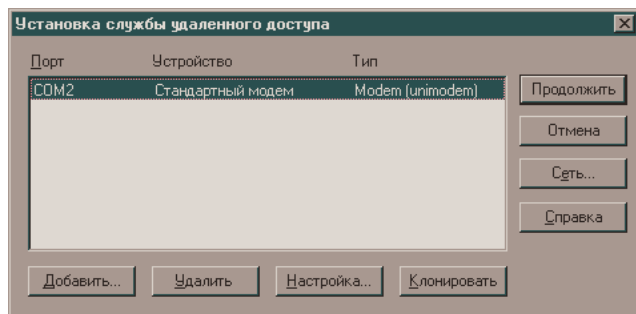


Рис. 6.4. Окно «Установка службы удаленного доступа»

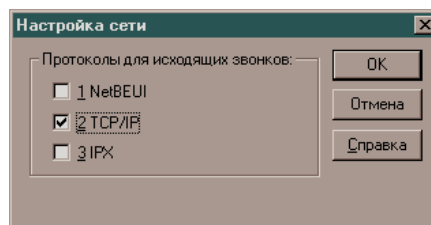


Рис. 6.5. Окно «Настройка сети»

– поставить галочку напротив пункта **2 TCP/IP** (рис. 6.5). Нажать кнопку **ОК**;

– вернуться к окну **Установка службы удаленного доступа** (рис. 6.4);

– выбрать кнопку **Настройка...**. Появится окно **Использование порта** (рис. 6.6);

– установить параметр **Только исходящие звонки**. Далее щелкнуть **ОК** и во вновь появившемся окне **Установка службы удаленного доступа** нажать кнопку **Продолжить** (рис. 6.4).

3. Настройка параметров протокола TCP/IP:

– в окне **Сеть** (рис. 6.3) выбрать закладку **Протоколы** (рис. 6.7);

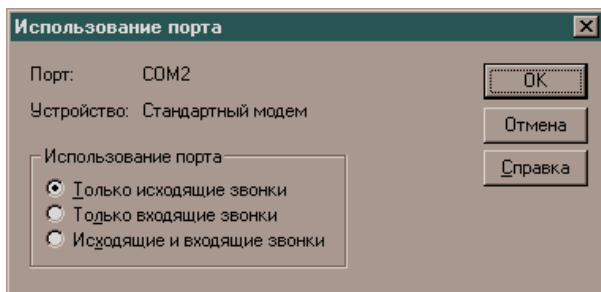


Рис. 6.6. Окно «Использование порта»

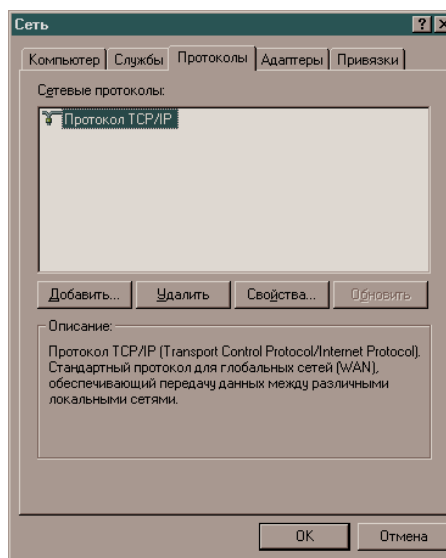


Рис. 6.7. Вкладка «Протоколы»

- если протокол TCP/IP установлен, нажать кнопку **Свойства....** Если нет, то его необходимо установить. Для этого нажать кнопку **Добавить...;**
- выбрать вкладку **Адрес IP** (рис. 6.8);
- все вводные поля в этом окне должны быть пусты;
- выбрать вкладку **DNS** (рис. 6.9) и убедиться в том, что вводные поля этой вкладки тоже пусты, за исключением полей с названием **Имя узла:**, в которое нужно ввести свой логин (имя пользователя), и **Домен:**, в которое нужно ввести имя домена (если есть);

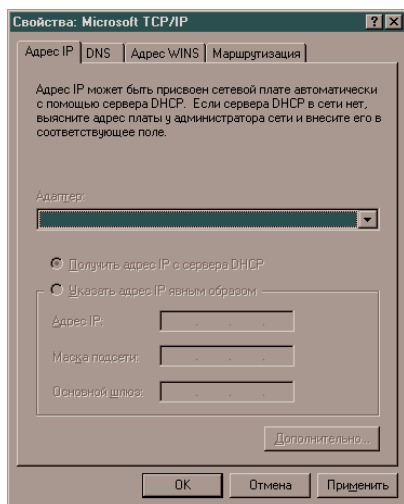


Рис. 6.8. Вкладка «Адрес IP»

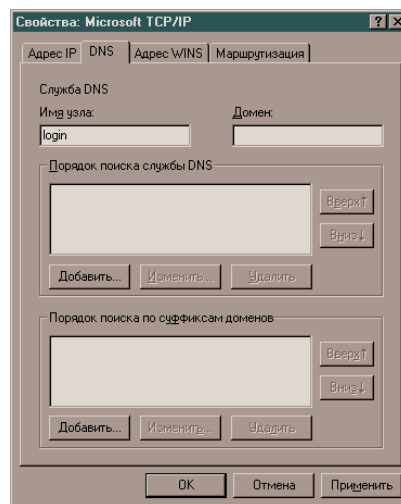


Рис. 6.9. Вкладка «DNS»

- на вкладке **Адрес WINS** (рис. 6.10) все поля тоже должны быть пусты;
- на вкладке **Маршрутизация** убрать галочку напротив **Включить маршрутизацию IP** (рис. 6.11). Теперь нажать кнопку **ОК**.

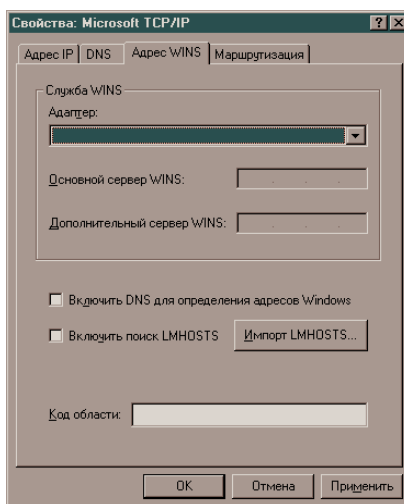


Рис. 6.10. Вкладка «Адрес WINS»

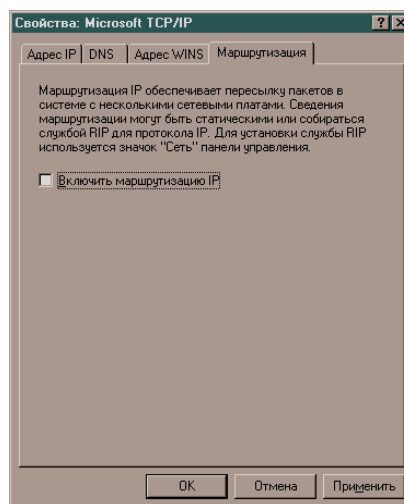


Рис. 6.11. Вкладка «Маршрутизация»

4. Подключение **Удаленного доступа к сети** (DialUp-соединения):

– на **Рабочем столе** двойным щелчком по значку **Мой компьютер** открыть окно (рис. 6.12);

– двойным щелчком мыши запустить приложение **Удаленный доступ к сети** (рис. 6.13);

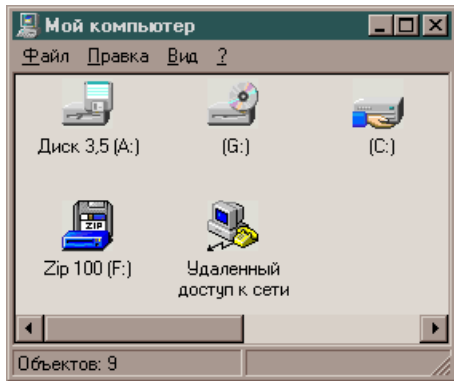


Рис. 6.12. Окно «Мой компьютер»

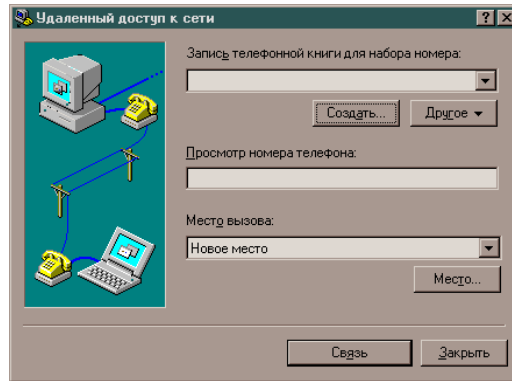


Рис. 6.13. Окно «Удаленный доступ к сети»

– в окне **Удаленный доступ к сети** нажать кнопку **Создать...** (рис. 6.13). Откроется окно **Создать запись телефонной книги**;

– на вкладке **Общие** (рис. 6.14) нужно ввести следующее: **Название** – название телефонной книги, например **Beltelecom**; **Заметки** – краткое описание соединения (можно и не заполнять); **Телефон** – телефон для дозвона, например **8600100**; **Использовать** – поскольку в системе один модем, через который необходимо производить данное соединение, то он уже будет в этом окне;

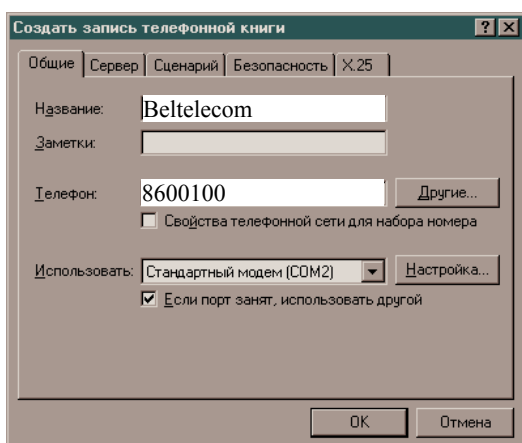


Рис. 6.14. Окно «Создать запись телефонной книги»

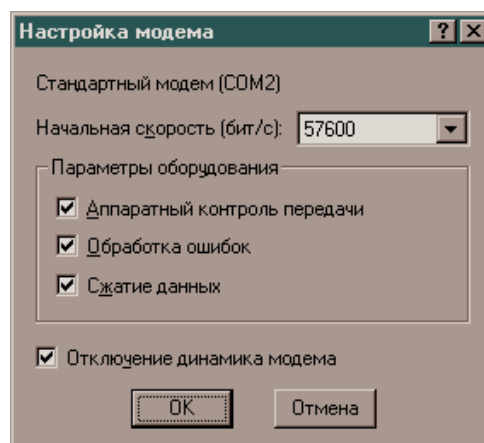


Рис. 6.15. Окно «Настройка модема»

– нажать кнопку **Настройка...** (рис. 6.14). Поставить все четыре галочки, а в окне **Начальная скорость** лучше оставить значение, которое было установлено драйвером модема (рис. 6.15);

– перейти к вкладке **Сервер** (рис. 6.16). Из трех сетевых протоколов нужно оставить только **TCP/IP** и поставить галочки напротив параметров **Разрешить программное сжатие данных** и **Разрешить расширения PPP LCP**;

– нажать кнопку **Настройка TCP/IP...** и в появившемся окне **Настройка протокола PPP для TCP/IP** привести все в соответствие с рис. 6.17, после чего щелкнуть **ОК**;

– в окне **Тип сервера удаленного доступа**, как правило, уже установлено: **PPP: Windows NT, Windows 95 Plus, Интернет**, если нет, то нажать стрелку вниз и выбрать этот тип сервера (рис. 6.16);

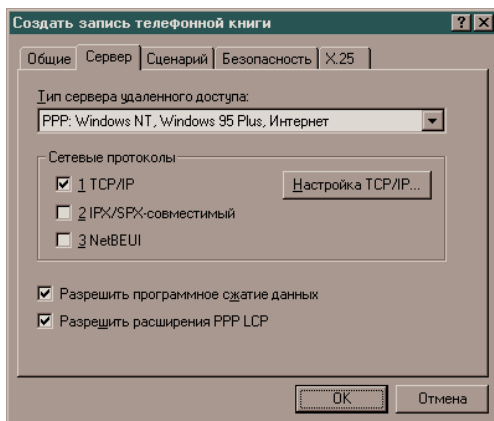


Рис. 6.16. Вкладка «Сервер»

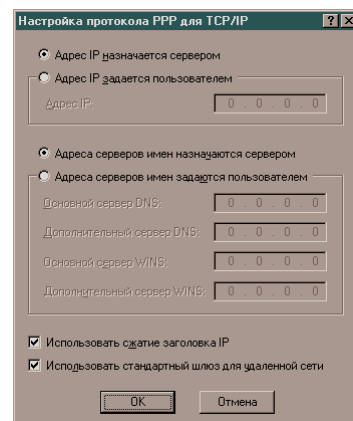


Рис. 6.17. Окно «Настройка протокола PPP для TCP/IP»

– перейти к закладке **Сценарий** (рис. 6.18) и выбрать параметр **Не используется**;

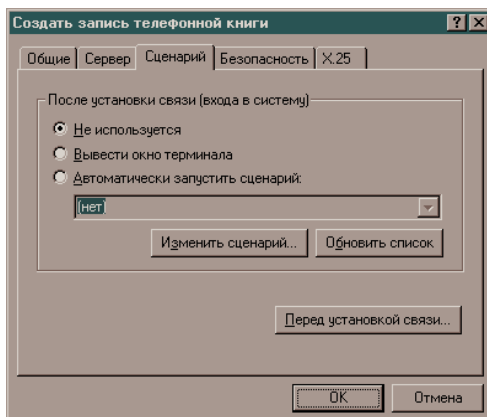


Рис. 6.18. Вкладка «Сценарий»

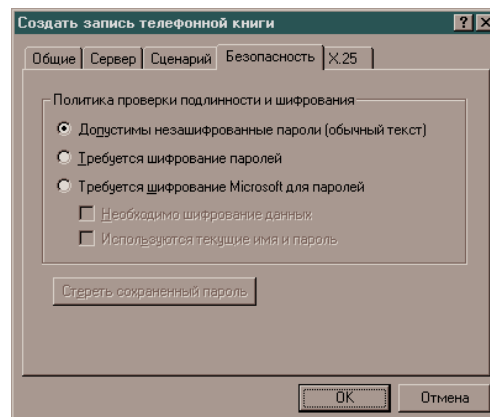


Рис. 6.19. Вкладка «Безопасность»

- на вкладке **Безопасность** (рис. 6.19) выбрать **Допустимы незашифрованные пароли (обычный текст)**;
- перейти к вкладке **X.25** (рис. 6.20) и убедиться, что все поля на ней пусты, после чего щелкнуть **ОК**. В результате программа установки вернется в окно **Удаленный доступ к сети**. Нажать кнопку **Закрыть** (рис. 6.21);
- перезагрузить компьютер;
- после перезагрузки компьютера запустить ярлык соединения с **Beltelecom**. Откроется окно **Удаленный доступ к сети** (рис. 6.21).

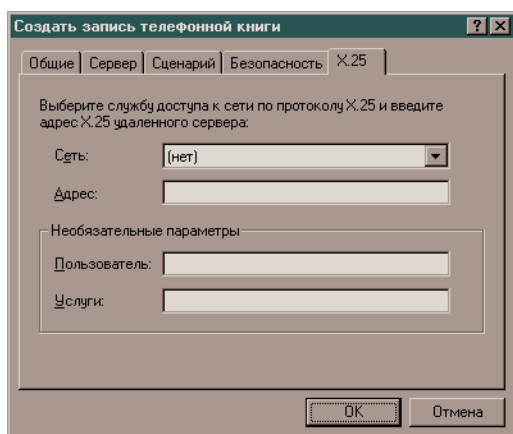


Рис. 6.20. Вкладка «X.25»

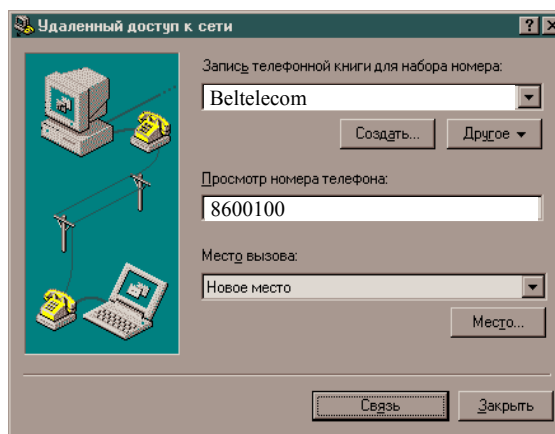


Рис. 6.21. Окно «Удаленный доступ к сети»

5. Для того чтобы подключиться к Интернет:
- нажать кнопку **Связь**. Появится окошко **Подключение к Beltelecom** (рис. 6.22);

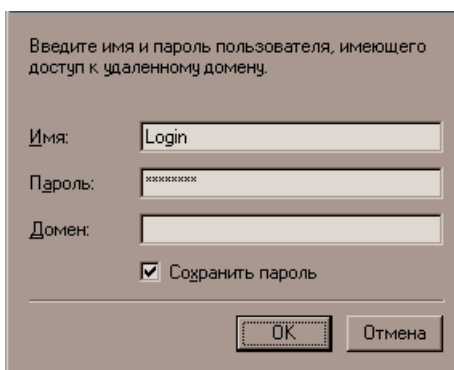


Рис. 6.22. Окно «Подключение к Beltelecom»

- в поле **Имя** ввести свой логин, полученный при регистрации. В поле **Пароль** набрать пароль, полученный при регистрации. В поле

Домен ввести BSTU_LES (или оставить пустым). Чтобы не набирать пароль каждый раз при подключении к Интернет, поставить галочку напротив надписи **Сохранить пароль**. Теперь нажать **ОК**;

– модем начнет «дозваниваться» (рис. 6.23);

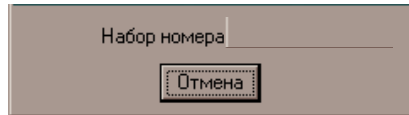


Рис. 6.23. «Дозвон» модема

6. Если набор номера происходит в тоновом режиме, нужно вернуться в окно **Удаленный доступ к сети** (рис. 6.21) и, нажав кнопку **Другое**, выбрать верхний пункт в меню. Добавить перед номером телефона латинскую букву **p** (**8p600100**). Если набор номера осуществляется в импульсном режиме, то добавить перед номером **w** (**8w600100**). После завершения работы не забывать разорвать соединение.

Лабораторная работа № 7

ОРГАНИЗАЦИЯ РАБОЧЕЙ ГРУППЫ, ДОМЕНА. ПОДКЛЮЧЕНИЕ КОМПЬЮТЕРА К ДОМЕНУ

Цель работы: научиться организовывать рабочие группы, домен, а также подключать компьютер к домену.

Теоретические сведения

В сетевой операционной системе Windows NT сети могут быть смоделированы в одной из двух различных форм: рабочая группа или домен.

Windows NT Workstation разрабатывалась как операционная система для отдельной настольной рабочей станции или как равноправный сервер для небольшой рабочей группы. Одним из ограничений Windows NT Workstation является невозможность одновременной поддержки более десяти серверных соединений.

Рабочая группа. Рабочая группа – это логическое объединение компьютеров, обычно не более десяти, которые могут разделять свои ресурсы. Однако при этом каждый компьютер рабочей группы имеет собственную базу учетных данных, содержащую информацию только о его локальных пользователях. Рабочая группа создается для организации простейшего совместного доступа к сетевым файлам, принтерам и приложениям. В пределах рабочей группы не поддерживается централизованная аутентификация ресурсов пользователя или группы пользователей. Сами пользователи сети при этом должны иметь бюджет с соответствующими привилегиями для любой системы, к которой они хотят получить доступ через системную консоль или через сеть (рис. 7.1). На компьютерах рабочей группы могут быть установлены и Windows NT Server, и Windows NT Workstation. И пользователи, и ресурсы каждого члена рабочей группы администрируются средствами данного компьютера. Таким образом, рабочая группа не дает всех тех возможностей, которые несет в себе централизованная доменная справочная служба.

Для небольшой группы компьютеров модель рабочей группы может оказаться весьма полезной. В больших сетях необходимость поддержки индивидуальных бюджетов и паролей для всей группы смешанных ресурсов связана с дополнительными неудобствами.

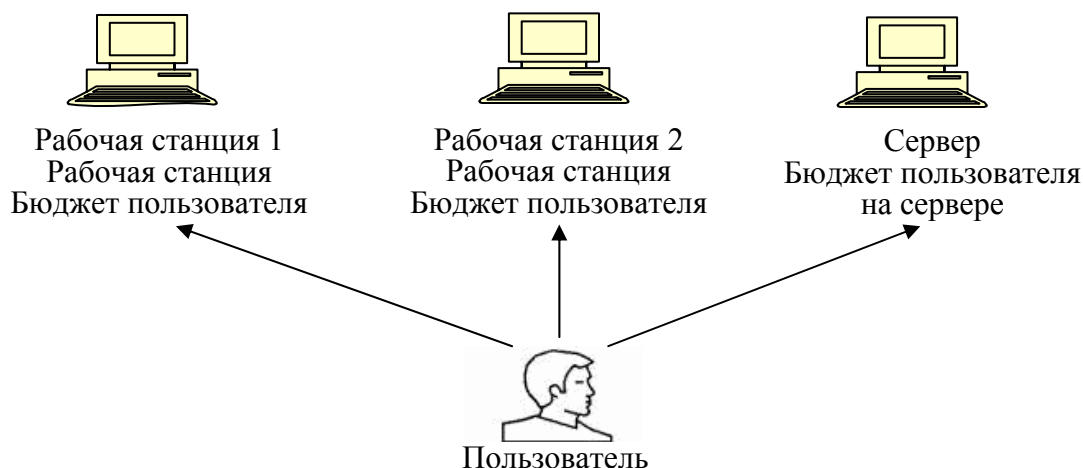


Рис. 7.1. Модель рабочей группы NT

Описание подключения к рабочей группе была дано в лабораторной работе № 4.

Домен. Для облегчения задач управления большой группой сетевых ресурсов используют домен Windows NT – основную единицу администрирования и обеспечения безопасности в Windows NT. Для домена существует общая база данных учетной информации пользователей домена (user accounts) и ресурсов домена – компьютеров (computer accounts) и принтеров (printer accounts).

Членами домена являются как пользователи, так и компьютеры. При отсутствии доменной организации каждый компьютер Windows NT Workstation и Windows NT Server хранит собственную базу учетных данных пользователей – SAM (Security Access Manager). В этой базе хранится вся необходимая системе информация о пользователе: имя, пароль (в зашифрованном виде) и так называемый SID (Security Identifier). Каждый SID является уникальным числом. При изменении имени пользователя его SID не изменяется. Поэтому домен обеспечивает централизованную службу аутентификации с единственной базой данных безопасности, содержащей информацию обо всех пользователях и группах внутри сети. Пользователи подтверждают принадлежность к домену, после чего получают доступ к любым ресурсам, определенным для конкретного бюджета или группы пользователей (рис. 7.2).

В домене обязательно есть сервер Windows NT Server, выполняющий роль первичного контроллера домена – PDC (Primary Domain Controller). Этот контроллер хранит первичную копию базы данных учетной информации пользователей домена – SAM PD. Все

изменения учетной информации сначала производятся именно в этой копии. Основной контроллер домена всегда существует в единственном экземпляре [1].



Рис. 7.2. Модель домена NT

Кроме основного контроллера, в домене могут находиться несколько резервных контроллеров – BDC (Backup Domain Controllers). Эти контроллеры хранят реплики базы учетных данных. Все резервные контроллеры в дополнение к основному могут обрабатывать запросы пользователей на логический вход в домен. База данных SAM BD всегда является копией базы SAM PD.

Членами домена могут быть также компьютеры, на которых установлены Windows NT Server, не назначенные на роль PDC или BDC. Такие серверы называются отдельно стоящими серверами (Stand-alone servers) или серверами – членами доменами (Member servers). На таких компьютерах, освобожденных от функций аутентификации пользователей и ведения справочной базы данных, могут более производительнее выполняться ответственные приложения или файл- и принт-сервисы. Stand-alone серверы не могут быть оперативно переконфигурированы в PDC или BDC, для этого требуется переинсталляция.

База данных безопасности домена NT поддерживается на сервере Windows NT, который выступает в роли первичного контроллера домена (PDC).

Windows NT не предназначена для работы исключительно как контроллер домена. В доменах малого и среднего размеров Windows NT может одновременно выполнять функции сервера для файлов, принтеров или приложений. В больших же доменах намного выгоднее выделять для этих целей отдельный сервер, что позволяет значительно повысить производительность.

Разница между доменом и рабочей группой. Основное различие между рабочими группами и доменами заключается в способе управления сетевыми ресурсами. Компьютеры в домашних сетях обычно входят в состав рабочих групп, а компьютеры в сетях на рабочих местах – в состав доменов.

В рабочей группе:

1) все компьютеры являются одноранговыми узлами сети – ни один компьютер не может контролировать другой;

2) на каждом компьютере находится несколько учетных записей пользователя. Для использования любого компьютера, принадлежащего рабочей группе, необходимо иметь на этом компьютере свою учетную запись;

3) в рабочей группе обычно насчитывается до 20 компьютеров;

4) все компьютеры должны находиться в одной локальной сети или подсети.

В домене:

– один или более компьютеров являются серверами (администраторы сети используют серверы для контроля безопасности и разрешений для всех компьютеров домена, что позволяет легко изменять настройки, так как изменения автоматически производятся для всех компьютеров);

– если пользователь имеет учетную запись в домене, он может войти в систему на любом компьютере (не требуется иметь учетную запись на самом компьютере);

– в домене могут быть сотни или тысячи компьютеров;

– компьютеры могут принадлежать различным локальным сетям.

Порядок выполнения работы

1. Подключение компьютера к домену:

– войти в компьютер как **Администратор**;

– нажать кнопку **Пуск** и выбрать в меню **Настройка** команду **Панель управления**. Дважды щелкнуть значок **Сеть**. На экране появится диалоговое окно **Сеть** с набором вкладок, позволяющих внести необходимые изменения;

– открыть вкладку **Компьютер**. Нажать кнопку **Изменить...** (рис. 7.3);

– ввести в поле **Домен** – имя домена (BSTU_LES), к которому присоединяется компьютер, и поставить галочку у **Создать учетную запись компьютера в домене** (рис. 7.4);

– ввести логин администратора домена в поле **Пользователь** и пароль администратора в поле **Пароль**. Подтвердить успешное подключение к домену, нажав кнопку **ОК**;

– закрыть все окна и перезагрузить компьютер.

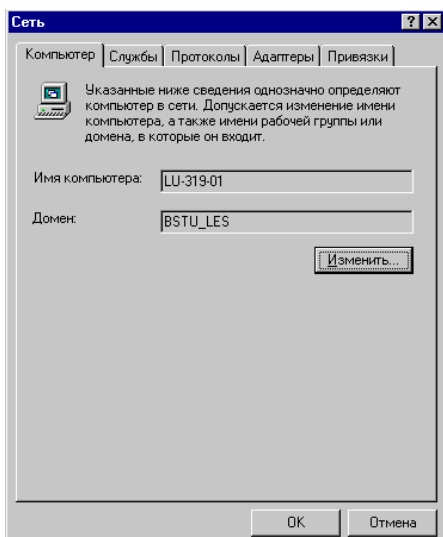


Рис. 7.3. Вкладка «Компьютер»

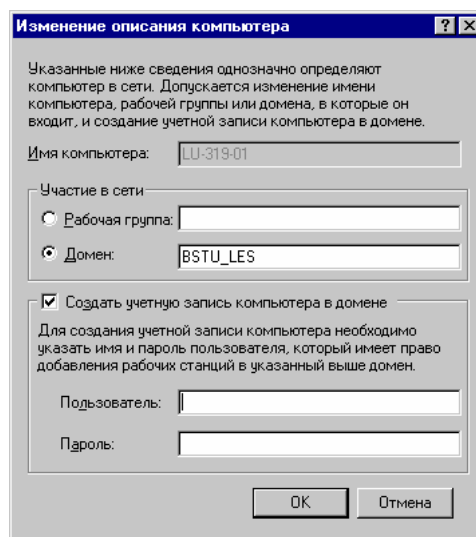


Рис. 7.4. Создание учетной записи

2. Присоединение компьютера к домену можно осуществить через добавление учетной информации компьютера на сервере:

– войти в **Windows NT Server** как **Администратор**, запустить **Server Manager**;

– в меню **Computer** выбрать пункт **Add to Domain**, в поле **Computer Type** выбрать **Windows NT Workstation** или **Server**;

– в поле **Computer Name** набрать имя компьютера (например, LU-319-01) и нажать кнопку **Add**.

Лабораторная работа № 8

ОРГАНИЗАЦИЯ ПОЛЬЗОВАТЕЛЕЙ И ГРУПП ПОЛЬЗОВАТЕЛЕЙ. УСТАНОВКА ПРАВ И ДОПУСКОВ

Цель работы: разобраться в организации раздельного пользования компьютером, а также научиться обеспечивать раздельное пользование компьютером, который используется несколькими лицами.

Теоретические сведения

В модели рабочих групп каждый пользователь управляет частью ресурсов сети, т. е. является администратором своего компьютера. Модель рабочих групп хорошо работает для небольших сетей с небольшим числом пользователей.

Бюджет – это запись в базе данных для конкретного пользователя, которая включает идентификатор, имя пользователя, пароль, а также права и допуски, которыми владеет пользователь. При включении в сеть большого количества компьютеров или пользователей возникают сложности управления их бюджетами. Необходимо разработать и организовать структуру, позволяющую централизовать администрирование (с сервера). Для этого создаются локальные и глобальные пользователи и группы.

С этой целью необходимо:

- оценить всех потенциальных пользователей системы;
- установить права пользователей, входящих в данную группу, построить окружение;
- создать локальные группы пользователей на каждой рабочей станции;
- для ресурсов рабочей станции указать допуски тех или иных рабочих групп;
- аналогичные группы создать на контроллере домена (глобальные);
- включить локальные группы пользователей на каждой рабочей станции;
- создать глобальные бюджеты для каждого пользователя.

После этого пользователь автоматически получит право работать в домене и использовать ресурсы, предоставляемые локальным группам.

Учетные записи пользователей. Набор действий, которые можно выполнить с помощью диспетчера пользователей, определяется правами текущего пользователя. Эти права в основном зависят от того, членом каких групп этот пользователь является. Windows NT включает несколько *встроенных групп*, автоматически устанавливаемых на компьютер [2].

Самыми важными встроенными группами являются:

1) администраторы – разрешается выполнять все команды диспетчера пользователей;

2) опытные пользователи – разрешается создавать учетные записи пользователей и групп, а также изменять и удалять эти учетные записи. Кроме того, им разрешается добавлять пользователей в группы опытных пользователей, пользователей и гостей и удалять пользователей из этих групп;

3) пользователи – могут создавать группы, изменять или удалять созданные ими группы, а также включать других пользователей в эти группы.

Учетная запись пользователя содержит набор сведений о нем, таких как его имя и пароль для входа в систему, а также права и разрешения, предоставленные пользователю для работы с системой и доступа к ее ресурсам.

Существуют встроенные учетные записи пользователей:

– администратор определяет ответственного администратора рабочей станции. Этот пользователь управляет всеми сторонами работы компьютера Windows NT;

– гость может создавать файлы и удалять свои файлы, а также читать другие файлы, если системный администратор специально предоставил для гостя разрешение на чтение этих файлов. Встроенная учетная запись гостя предназначена для того, чтобы пользователь, который работает на компьютере очень редко, мог войти в систему и получить к ней ограниченный доступ. При установке эта учетная запись не содержит пароля.

Группы пользователей. Группы используются для объединения учетных записей пользователей. Включение пользователя в группу означает предоставление ему всех прав и разрешений, заданных для группы. Это свойство групп позволяет быстро предоставить общие возможности ряду пользователей.

Политика безопасности. Диспетчер пользователей позволяет установить три вида политики безопасности:

1) политика учетных записей определяет режим использования паролей для всех учетных записей, а также необходимость блокировки учетных записей при превышении заданного числа неудачных попыток входа в систему за определенное время;

2) политика прав пользователей определяет права, присваиваемые группам и отдельным пользователям;

3) политика аудита определяет набор событий безопасности, для которых выполняется аудит.

Администрирование пользователей состоит в создании учетной информации пользователей (определяющей имя пользователя, принадлежность пользователя к различным группам пользователей, пароль пользователя), а также в определении прав доступа пользователя к ресурсам сети (компьютерам, каталогам, файлам, принтерам и т. п.).

Типы операций доступа – это действия объектов над субъектами. Операции могут быть либо разрешены, либо запрещены, либо вообще не иметь смысла для данной пары объекта и субъекта. Права и разрешения, данные группе, автоматически предоставляются ее членам, позволяя администратору рассматривать большое количество пользователей как единицу учетной информации.

Доступ к ресурсам компьютера для пользователей домена обеспечивается за счет механизма включения в локальную группу отдельных пользователей домена и глобальных групп домена. Включенные пользователи и группы получают те же права доступа, что и другие члены данной группы. Механизм включения глобальных групп в локальные является основным средством централизованного администрирования прав доступа в домене Windows NT (рис. 8.1).

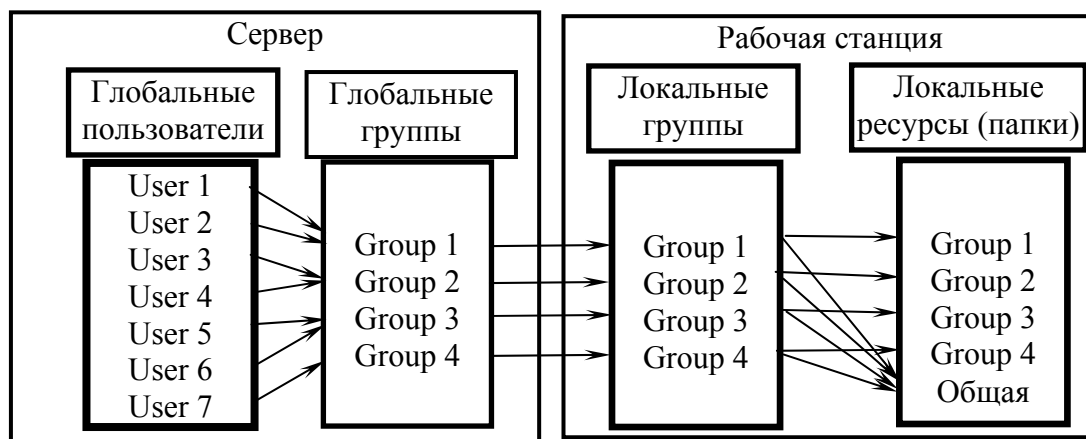


Рис. 8.1. Централизованное администрирование прав доступа в домене

Локальная группа не может содержать другие локальные группы. Поэтому в сети, использующей модель рабочей группы, нет возможности определить на одном компьютере всех пользователей сети и предоставить им доступ к ресурсам других компьютеров. В любом случае локальная группа объединяет некоторое число пользователей и глобальных групп, которым присваивается общее имя – имя локальной группы. Локальные группы могут включать пользователей и глобальные группы не только данного домена, но и любых доверяемых доменов.

Права пользователей определяются для отдельных пользователей на выполнение немногочисленных действий, касающихся реорганизации их операционной среды. Возможности пользователя являются частью так называемого профиля пользователя (User Profile), который можно изменять с помощью утилиты User Profile Editor. Профиль наряду с описанными возможностями включает и установки среды пользователя на его рабочем компьютере, такие как цвета, шрифты, набор программных групп и их состав [2].

Разрешение на доступ к каталогам и файлам. Администратор может управлять доступом пользователей к каталогам и файлам в разделах диска, отформатированных под файловую систему NTFS. Для защиты файла или каталога необходимо установить для него разрешения.

Управление профилями пользователей. Когда пользователь локально входит первый раз в какой-либо компьютер, то для него по умолчанию создается профиль. Все настройки среды (цвет фона, обои, шрифты и т. п.) автоматически сохраняются в подкаталоге Profiles системного каталога данного компьютера, например C:\WINNT\Profiles*username*, где *username* – имя пользователя. Профиль хранится в файле с именем *ntuser.dat*.

Порядок выполнения работы

1. Создание учетных записей и групп пользователей, управление существующими записями, а также настройка политики безопасности, например прав пользователей и политики аудита, проводится с помощью **Диспетчера пользователей**:

– нажать кнопку **Пуск** и выбрать в меню **Программы** команду **Администрирование (Общее)** (рис. 8.2). Дважды щелкнуть значок **Диспетчер пользователей**;

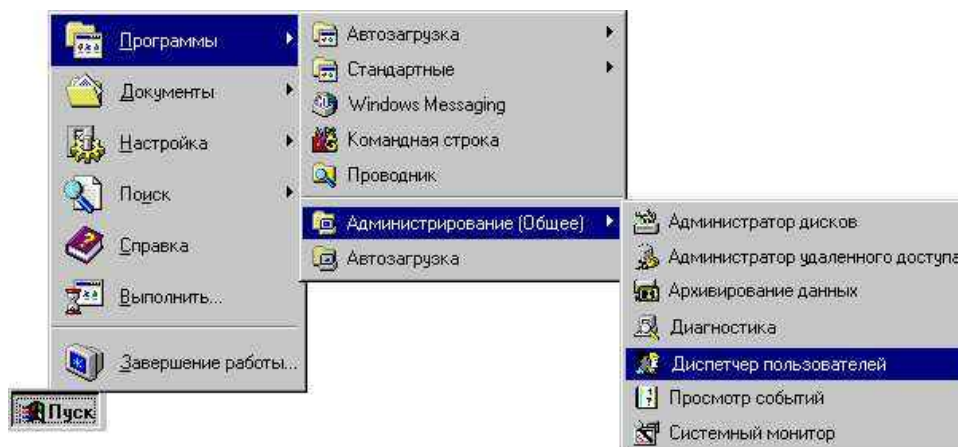


Рис. 8.2. Меню «Пуск»

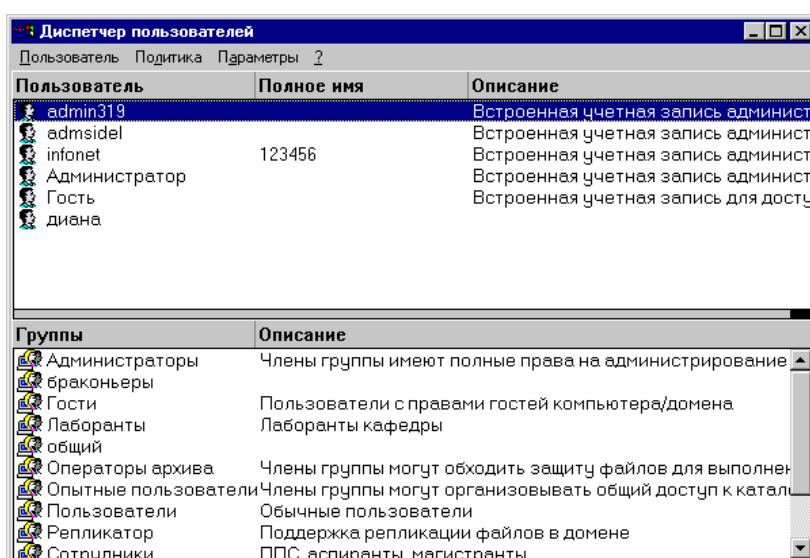


Рис. 8.3. Окно «Диспетчер пользователей»

- на экране появится окно **Диспетчера пользователей** (рис. 8.3);
- выбрать пункт меню **Пользователь**, далее **Создать пользова-**
теля (рис. 8.4), если надо создать нового пользователя, или **Создать**
группу (рис. 8.5), если надо создать новую группу.

2. Для нового локального пользователя:

- в поле **Пользователь** ввести имя пользователя (логин, например infonet). В поле **Пароль** ввести пароль, а в поле **Подтверждение** повторить ввод того же самого пароля (рис. 8.4);

– нажать кнопку **Группы** (рис. 8.4), чтобы выбрать те группы, в которые должен входить только что созданный локальный пользователь. Для этого выбрать имя группы в окне **Не член групп** (рис. 8.6) и нажать кнопку **Добавить**. После выбора принадлежности к группам щелкнуть **ОК**.

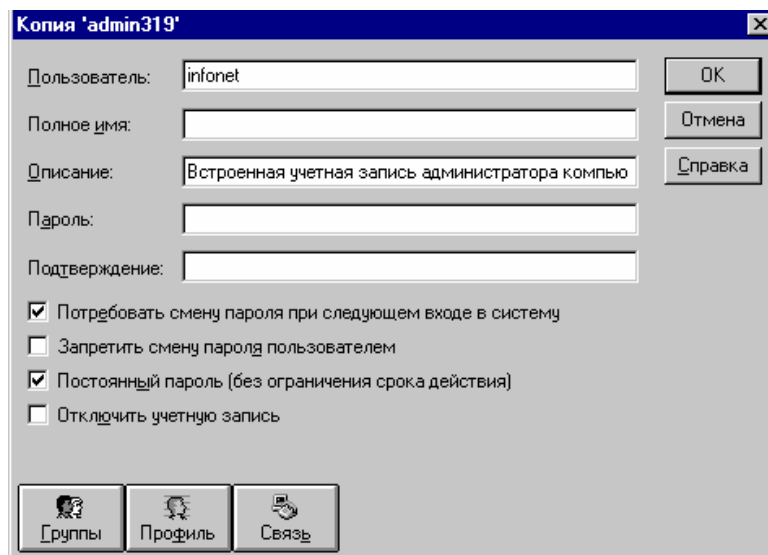


Рис. 8.4. Создание нового локального пользователя

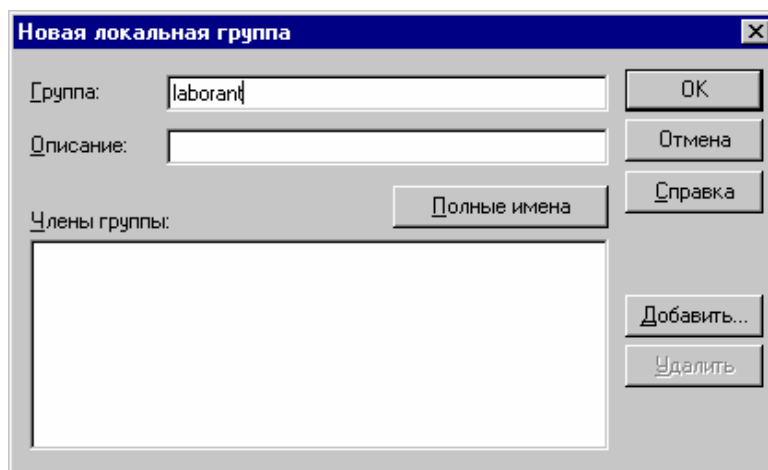


Рис. 8.5. Создание новой локальной группы

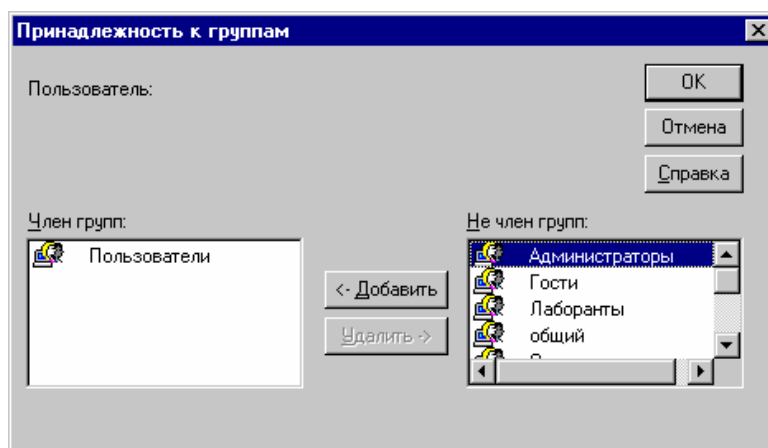


Рис. 8.6. Принадлежность к группам

3. Для новой локальной группы нужно добавить пользователей, которые должны входить в данную группу:

– нажать кнопку **Добавить...** (рис. 8.5). Выбрать нужного пользователя и нажать кнопку **Добавить** (рис. 8.7);

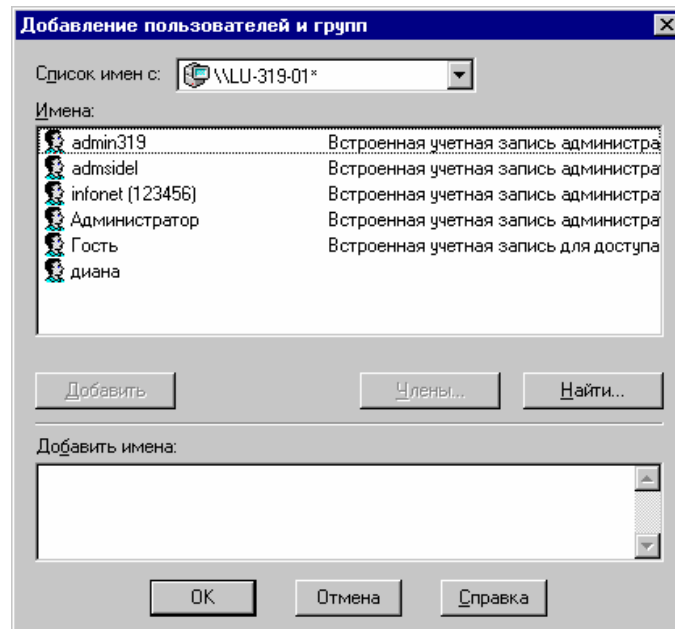


Рис. 8.7. Добавление пользователей и групп

– можно выбрать нескольких пользователей, повторив операцию. После выбора щелкнуть **ОК**.

ЛИТЕРАТУРА

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2000. – 672 с.
2. Олифер, В. Г. Основы сетей передачи данных: курс лекций / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2003. – 248 с.
3. Атрощенко, О. А. Компьютерные технологии в лесном хозяйстве: учеб. пособие / О. А. Атрощенко. – Минск: БГТУ, 2006. – 328 с.

СОДЕРЖАНИЕ

Предисловие.....	3
Лабораторная работа № 1. Внутреннее устройство компьютера, установка сетевого адаптера и программного обеспечения.....	4
Лабораторная работа № 2. Планирование сети и выбор сетевого оборудования, подключение кабелей	11
Лабораторная работа № 3. Организация раздельного доступа к периферийным устройствам компьютера.....	21
Лабораторная работа № 4. Организация простейшей сети, состоящей из двух компьютеров	28
Лабораторная работа № 5. Организация локальной сети, деление сети на сегменты (подсети)	31
Лабораторная работа № 6. Организация удаленного доступа к сети.....	43
Лабораторная работа № 7. Организация рабочей группы, домена. Подключение компьютера к домену.....	52
Лабораторная работа № 8. Организация пользователей и групп пользователей. Установка прав и допусков	57
Литература	64

**ИНФОРМАЦИОННЫЕ СЕТИ
И ПЕРЕДАЧА ИНФОРМАЦИИ
В ИСУЛХ**

Составитель **Сидельник** Николай Ярославович

Редактор *Е. С. Ватеичкина*
Компьютерная верстка *Е. С. Ватеичкина*

Учреждение образования
«Белорусский государственный технологический университет».
220006. Минск, Свердлова, 13а.
ЛИ № 02330/0549423 от 08.04.2009.