

Министерство образования и науки Российской Федерации
Российский государственный профессионально-педагогический университет
Уральское отделение Российской академии образования

Л.В. Волкова, М.С. Грохульский

ОСНОВЫ ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебное пособие

Допущено УМС по информатике, вычислительной технике и компьютерным технологиям Учебно-методического объединения по ППО в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности 030500.06 – Профессиональное обучение (информатика, вычислительная техника и компьютерные технологии)

Екатеринбург 2006

УДК 004.7(075.8)

ББК 3973 я 73-1

В 67

Волкова Л.В., Грохульский М.С. Основы локальных компьютерных сетей: Учеб. пособие. Екатеринбург: Изд-во Рос. гос. проф.-пед. ун-та, 2006. 145 с.

ISBN 5-8050-0120-9

Учебное пособие раскрывает основные принципы работы локальных компьютерных сетей, а также базовые понятия и определения в этой области. Основное внимание в книге уделено рассмотрению принципов и правил построения, функционирования и администрирования локальных компьютерных сетей на базе стандартных технологий.

Материалы данной книги ориентированы на теоретическую подготовку в области локальных компьютерных сетей на начальном этапе изучения компьютерных коммуникаций и сетей.

Рецензенты: доктор педагогических наук, профессор Б.Е. Стариченко (Уральский государственный педагогический университет); кандидат технических наук, доцент С.В. Кудымов (Российский государственный профессионально-педагогический университет)

ISBN 5-8050-0120-9

© Российский государственный
профессионально-педагогический
университет, 2006

© Волкова Л.В., 2006

© Грохульский М.С., параграф 3.4, 2006

Оглавление

Предисловие.....	4
Раздел 1. Введение в компьютерные сети.....	7
1.1. Основные понятия и определения.....	8
1.2. Линии связи.....	25
1.3. Принципы передачи данных по КС.....	37
Раздел 2. Построение ЛКС на основе стандартных технологий.....	53
2.1. Модель IEEE 802.x.....	54
2.2. Построение ЛКС на физическом уровне.....	61
2.3. Построение ЛКС на канальном уровне.....	85
2.4. Оборудование ЛКС.....	91
Раздел 3. Построение ЛКС средствами MS Windows.....	104
3.1. Сетевая архитектура MS Windows.....	105
3.2. Стек протоколов NetBEUI/SMB.....	111
3.3. Стек протоколов IPX/SPX.....	116
3.4. Построение одноранговой сети.....	121
Заключение.....	139
Список рекомендуемой литературы.....	140
Приложение.....	141
Список используемых сокращений.....	143

Предисловие

Данная книга является частью программно-методического комплекса, включающего:

- учебное пособие «Основы локальных компьютерных сетей»;
- лабораторный практикум «Локальные компьютерные сети»;
- компакт-диск, содержащий электронные пособия «Основы локальных компьютерных сетей: демонстрационные материалы», «Обжим кабеля UTP», презентацию по теме «Сетевая печать», комплекс компьютерных тренажеров, контрольные задания, тесты для самоконтроля, необходимое программное обеспечение, методические рекомендации для преподавателей и студентов по использованию программно-методического комплекса в учебном процессе.

Программно-методический комплекс ориентирован на знакомство с общими принципами функционирования локальных компьютерных сетей, теоретическую и практическую подготовку в области их проектирования и построения студентов, обучающихся по специальностям 050501 Профессиональное обучение (информатика, вычислительная техника и компьютерные технологии) (030500.06); 050501 Профессиональное обучение (электроэнергетика, электротехника и электротехнологии) (030500.19); 080801 Прикладная информатика (в экономике, в образовании) (351400), а также всех, кто начинает изучать компьютерные коммуникации и сети.

Материалы учебного пособия знакомят с основными принципами работы локальных компьютерных сетей, базовыми понятиями и определениями данной сферы знаний. Основное внимание в книге уделено рассмотрению принципов и правил построения, функционирования и администрирования локальных компьютерных сетей (ЛКС). Последовательно рассматриваются все основные этапы установки и настройки сетевого оборудования, инсталляции сетевых компонентов, настройка доступа к ресурсам и организация сетевой печати.

Исследование выполнено при поддержке Российского гуманитарного научного фонда (грант 05-06-06104А).



Для использования учебного пособия в обучении необходимо:

- 1) иметь компакт-диск, прилагаемый к данной книге, содержащий демонстрационные материалы и программное обеспечение;
- 2) убедиться, что на компьютере установлен проигрыватель flash-роликов Flash Player 7.0. Если он отсутствует, то следует позаботиться об

инсталляции этого программного продукта, дистрибутив которого находится в папке **Distrib\FlashPI**;

- 3) убедиться, что на компьютере установлен проигрыватель видеороликов QuickTime Player. Если он отсутствует, то позаботиться об инсталляции этого программного продукта, дистрибутив которого находится в папке **Distrib\QuickTime**.

В книге приняты следующие обозначения:

-  – этот символ используется для выделения определений, важных выводов, замечаний и подсказок;
-  – так отмечены ссылки на лабораторные работы, которые рекомендуется выполнить, обратившись к лабораторному практикуму «Локальные компьютерные сети».

Краткое описание методики обучения с помощью данного учебного пособия смотрите в методических рекомендациях, имеющихся на компакт-диске в папке **Рекомендации\Основы ЛКС**.

Мы выражаем горячую благодарность и признательность за помощь и поддержку в работе над книгой:

- Н.С. Толстой, Т.В. Эстриной – нашим коллегам, которые выступили в роли первых рецензентов работы. Их замечания, рекомендации и вопросы позволили устранить многие содержательные и методические просчеты;
- М.Э. Масленникову и Н.Н. Ожиге, выпускникам Российского государственного профессионально-педагогического университета (РГППУ) 2004 года, оказавшим большую помощь в разработке демонстрационных материалов по теме «Беспроводные локальные компьютерные сети»;
- студентам РГППУ очной и заочной форм обучения, а также его представительств и филиалов, расположенных в Екатеринбурге, Белоярском, Верхней Пышме, Карпинске, Качканаре, Каменске-Уральском, Магнитогорске, Нижнем Тагиле, Омске, Североуральске, Советском; учащимся школы №117 и центра «Одаренность и технологии» (Екатеринбург), принявшим активное участие в апробации материалов книги.

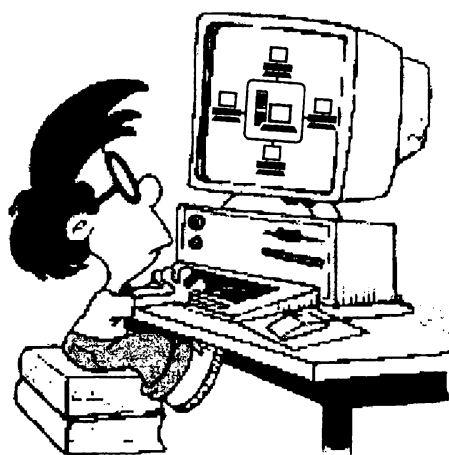
Информацию о порядке приобретения программно-методического комплекса можно получить по телефону (343) 331-67-78.

Если у Вас появились замечания, предложения или информация об ошибках, не сочтите за труд сообщить о них авторам. Наши координаты:

- телефон (3432) 3316–778;
- e-mail: volkova-l-v@yandex.ru.

Раздел 1

Введение в компьютерные сети



1.1. Основные понятия и определения

Рекомендуем познакомиться с демонстрационными материалами раздела «Введение в компьютерные сети» электронного пособия «Основы локальных компьютерных сетей: электронная поддержка», а также материалами документа *История ЛКС и ГКС.htm*, расположенного в папке *Учебная\Доп_материалы*.

☞ *Компьютерная сеть (КС) – это объединение двух и более компьютеров с помощью линий связи¹.*

Основной причиной создания КС является возможность совместного использования ресурсов.

Компьютеры объединяют для того, чтобы полнее реализовать преимущества как персональных компьютеров, так и больших универсальных вычислительных машин. Каждый участник сети пользуется преимуществами, с одной стороны, независимости, а с другой – доступа к совместным ресурсам.

1.1.1. Компоненты компьютерной сети

Основными компонентами любой КС являются ресурсы, серверы, клиенты и среда передачи данных.

☞ *Ресурсы компьютерной сети – файлы, папки, периферийные устройства и другие элементы, совместно используемые пользователями КС.*

Ключевыми ресурсами в КС являются периферийные устройства: принтеры, плоттеры, факсы и другие устройства ввода/вывода.

Кроме этого, компьютеры, объединенные в КС, могут совместно использовать файлы и папки на жестких дисках, информацию, записанную на дискетах, компакт-дисках CD/DVD-ROM, ZIP и Jaz-накопителях, а также любых других устройствах хранения информации, которые можно подключить к персональному компьютеру.

Отметим, что не все устройства, которые подключаются к компьютеру, могут совместно использоваться в КС. Такие устройства, как сканер, дигитайзер, световое перо и др., пригодны только для локального использования, что объясняется особенностями работы с ними.

Для того чтобы компьютеры могли работать в КС, к их операционным системам необходимо добавить специализированные программные модули. На тех компьютерах, ресурсы которых должны быть доступны

¹ Подробнее линии связи рассмотрены в п. 1.2.

пользователям сети, необходимо добавить модули, постоянно находящиеся в режиме ожидания запросов, поступающих по сети от других компьютеров. Обычно такой модуль называется *программным сервером*, так как главная его задача – обслуживать запросы на доступ к ресурсам своего компьютера.

☞ *Программный сервер¹ – программный модуль, который находится в режиме ожидания запросов, поступающих по сети от других компьютеров, и главная задача которого – обслуживать запросы на доступ к ресурсам своего компьютера.*

На компьютерах, пользователи которых хотят получать доступ к ресурсам других компьютеров, устанавливают особые программные модули. Они должны вырабатывать запросы на доступ к удаленным ресурсам и передавать их по сети на нужный компьютер. Такой модуль обычно называют программным клиентом.

☞ *Программный клиент² – специальный программный модуль, который вырабатывает запросы к серверам на доступ к удаленным ресурсам и передает их по КС.*

Клиентские и серверные части операционных систем выполняют основную работу по организации совместного использования ресурсов КС.

Для организации пересылки информации между компьютерами в КС используются различные среды передачи данных, в том числе:

- медный или оптоволоконный кабель;
- радиоволны;
- инфракрасное излучение.

1.1.2. Клиент-серверная архитектура КС

☞ *Способ организации взаимодействия приложений, при котором одна программа выступает как клиент, а другая как сервер, называется клиент-серверной архитектурой.*

Основная задача сервера – находиться в режиме ожидания, пока за тем или иным ресурсом к нему не обратится какой-либо клиент. Сервер может быть перегружен большим количеством запросов и в связи с этим задерживать обслуживание определенного запроса.

¹ Далее сервер.

² Далее клиент.

Программа-клиент формирует запрос, отправляет его по КС на определенный компьютер и взаимодействует с программой-сервером по определенным правилам – *протоколам*, рассматриваемым в п. 1.3. и разд. 3.

Схема взаимодействия между сервером и клиентом представлена на рис. 1.1.

Один компьютер может иметь несколько серверов. Клиент может быть расположен на том же компьютере, что и сервер, и на компьютере, сколько угодно удаленном от сервера (рис. 1.2). От расстояния прямо пропорционально зависит время, требуемое для передачи ответа от сервера.

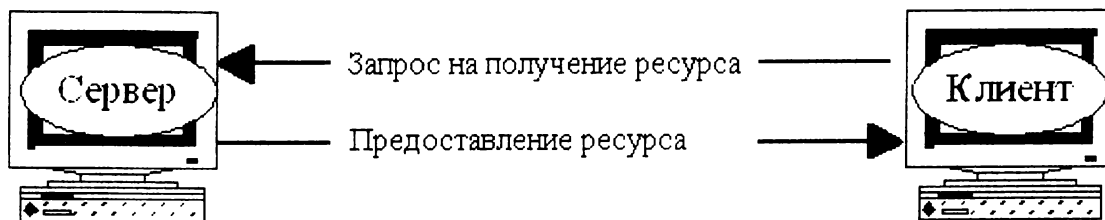


Рис. 1.1. Взаимодействие сервера и клиента в компьютерной сети

Разделение программ на серверную и клиентскую части позволяет размещать их на разных компьютерах, связанных по компьютерной сети, точно так же, как если бы они находились на одном и том же компьютере.

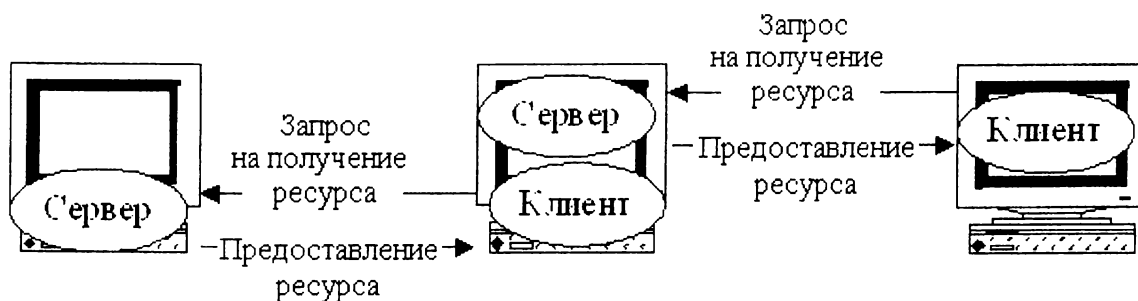


Рис. 1.2. Варианты расположения клиентов и серверов

Задачи, которые должны выполнять серверы, многообразны и сложны. Для того чтобы серверы отвечали современным требованиям, их делают специализированными. Для работы с ними на компьютерах пользователей устанавливают соответствующие клиенты. Ниже приведены краткие характеристики наиболее часто используемых серверов, а также даны примеры клиентов, позволяющих пользователю работать с этими серверами.

Серверы файлов. Серверы файлов управляют доступом пользователей к файлам. Если на компьютере пользователя установлен соответствующий клиент, он получает возможность работать с различными файлами, хранящимися на сервере файлов. Например, пользователь может загрузить

с удаленного компьютера документ Word, после чего работать с этим документом на своем компьютере.

Серверы печати. Серверы печати управляют доступом пользователей к принтерам. Если на компьютере пользователя установлен соответствующий клиент, он получает возможность выводить документы со своего компьютера на принтер, подключенный к серверу печати.

Почтовые серверы. Почтовые серверы управляют передачей сообщений по электронной почте между пользователями сети. Почтовые клиенты, например Outlook Express, позволяют пользователю отправлять и получать сообщения по электронной почте.

Web-серверы. На серверах данного типа хранятся Web-страницы. Web-серверы обеспечивают пересылку Web-страниц, затребованных пользователем. Пользователь работает с Web-серверами посредством программы-клиента, входящего в состав браузера, например Internet Explorer.

FTP-серверы. Данные серверы обеспечивают пересылку (копирование, передачу) файлов в сети Internet с удаленного компьютера на локальный и с локального компьютера на удаленный, а также удаление или переименование файлов на удаленном компьютере. На компьютере пользователя для работы с FTP-серверами должен быть установлен FTP-клиент, например FAR Manager или Internet Explorer¹.

На одном компьютере могут быть установлены различные типы серверов. Например, в КС один компьютер может выполнять функции сервера печати и почтового сервера. В этом случае на нем должны быть установлены два соответствующих программных модуля.

Для того чтобы пользователь мог получить доступ к нескольким специализированным серверам, на его компьютере должны быть установлены соответствующие клиенты. Так, если он желает работать с электронной почтой, а также печатать документы на удаленном принтере, работающем под управлением ОС Windows, ему нужно установить на своем компьютере Outlook Express (Internet Explorer) и клиент для сетей Microsoft.

Наиболее известными и популярными являются клиенты и серверы файлов и печати для сетей Microsoft и NetWare.

☞ *Клиент для сетей Microsoft позволяет пользователю работать с серверами файлов и серверами печати в сетях под управлением операционной системы Windows.*

¹ Internet Explorer обеспечивает работу с серверами различных типов. Для этого в его состав входят соответствующие встроенные клиенты.

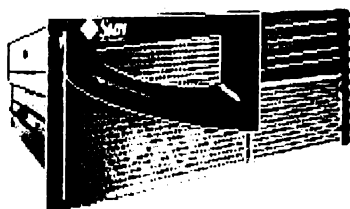
☞ Клиент для сетей NetWare позволяет пользователю работать с серверами файлов и серверами печати в сетях под управлением операционной системы Novell NetWare.

1.1.3. Аппаратные серверы

Термин «аппаратный сервер» чаще всего используется для обозначения компьютера, специально выделенного для файлов, приложений или периферийного оборудования, которые совместно используются в КС. Обычно он представляет собой компьютер с быстродействующим процессором и большим объемом памяти, которые рассчитаны не на выполнение повседневных задач данного компьютера, а для обслуживания многочисленных запросов от клиентов. Примеры аппаратных серверов представлены на рис. 1.3. Серверная программа всегда должна быть готова выполнить запрос, и именно поэтому к компьютерам, на которых работает программа-сервер, предъявляются повышенные требования по надежности и производительности.

Доступ к такому компьютеру чаще всего имеют только администраторы сети для выполнения задач управления, мониторинга и поддержки работоспособности сети.

а



б

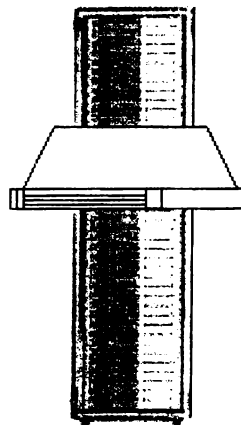


Рис. 1.3. Примеры аппаратных серверов:
а – Sun Fire 280R; б – Proliant DL320_2

К компьютерам, на которых устанавливается в основном только клиентское программное обеспечение, предъявляются менее серьезные требования по надежности и производительности, поскольку стабильность работы клиентского компьютера, как правило, влияет на работу одного человека, а от надежности работы аппаратного сервера может зависеть работа огромного количества клиентов сети.

1.1.4. Классификация компьютерных сетей

Для классификации компьютерных сетей используются различные признаки. С точки зрения практики полезно разделить КС на типы:

- по территориальному признаку, т.е. по величине территории, которую покрывает сеть;
- принципу организации передачи данных;
- физической топологии;
- по способу администрирования.

Помимо этого выделяют КС особого типа – корпоративные (см. п. 1.1.5).

Классификация КС по территориальному признаку

Классификация КС по данному признаку имеет большое практическое значение. Так, от типа КС во многом зависят выбор технологии, на основе которой она может быть построена, и необходимого комплекта сетевого оборудования, а также его физическое расположение¹.

*Локальная компьютерная сеть (ЛКС)*² охватывает небольшую территорию (обычно в радиусе 1–2 км) и, как правило, принадлежит одной организации. ЛКС внедряют на предприятиях для того, чтобы организовать совместное использование аппаратуры и распределенную обработку данных на нескольких компьютерах. ЛКС соединяет компьютеры, принтеры и другое электронное оборудование, позволяя владельцам данной сети совместно использовать общие для сети ресурсы и с высокой скоростью обмениваться различного рода информацией.

Из-за коротких расстояний в ЛКС имеется возможность использования относительно дорогих высококачественных линий связи³, которые позволяют, применяя простые методы передачи данных, достигать высоких скоростей обмена данными. В связи с этим услуги, предоставляемые ЛКС, отличаются широким разнообразием и обычно предусматривают реализацию в режиме реального времени (on-line).

В общем случае можно выделить следующие определяющие характеристики ЛКС:

- небольшой географический масштаб и, как следствие, однородность (схожесть) используемых сетевых технологий для подключения компьютеров в сеть;

¹ Некоторые стандартные технологии и сетевое оборудование рассматриваются в разд. 2.

² Наряду с сокращением ЛКС в различной литературе можно встретить и другие, например LAN (Local Area Networks).

³ Подробнее о линиях связи см. в п. 1.2.

- небольшое количество компьютеров, расположенных на небольшой территории (комната, этаж, здание или несколько расположенных рядом зданий);
- однотипность компьютеров, подключенных к сети;
- полный контроль сети, с управлением которой может справиться один человек или совсем небольшой штат сотрудников (нет делегирования полномочий по управлению). Как следствие – единая сетевая политика внутри всей сети;
- высокая скорость передачи данных между компьютерами (10, 16, 100 и выше Мбит/с)¹, которая сравнима со скоростями работы устройств и узлов компьютера – дисков, внутренних шин обмена данными и т.п.

Появление ЛКС обусловлено двумя основными причинами. Во-первых, компьютеры стали меньше по размерам и дешевле. Вместо больших объемных мейнфреймов, имеющих стоимость несколько миллионов долларов, организации начали осваивать небольшие недорогие машины, называемые мини-компьютерами. Во-вторых, стало очевидным, что компьютеры в офисе могут помочь в решении многих рабочих задач.

Дешевые мини-компьютеры изменили мир. Когда один большой компьютер стоил миллионы долларов, большинство организаций могли себе позволить иметь максимум один такой компьютер. Сегодня средняя организация может приобрести уже несколько таких машин. И, конечно, имея несколько компьютеров в помещении, необходимо предусмотреть способ обмена информацией между ними. Такая потребность и привела в конечном итоге к появлению первых ЛКС.

Глобальная компьютерная сеть (ГКС)² охватывает большие территории (регион, страну, ряд стран) и обеспечивает передачу информации с использованием различных линий связи. В силу того что глобальные сети покрывают огромные расстояния, в них приходится использовать те каналы связи, которые уже имеются в том или ином регионе. Поэтому в большинстве своем это медленные каналы на базе телефонных и телеграфных линий.

Появлению ГКС главным образом способствовали успешное развитие телефонных, телеграфных сетей связи, появление оптоволоконных

¹ Данные о скоростях здесь и далее приведены на основе анализа публикаций за 2004–2005 гг.

² Наряду с сокращением ГКС в различной литературе можно встретить и другие, например WAN (Wide Area Networks).

коммуникационных средств, а также и разработка мини-ЭВМ и сетевой операционной системы UNIX.

Из-за низких скоростей таких линий связи в ГКС набор предоставляемых услуг чаще всего рассчитан на работу в отложенном режиме (off-line). Для устойчивой передачи данных по некачественным линиям связи применяются методы и оборудование, существенно отличающиеся от методов и оборудования, используемых в ЛКС. Как правило, здесь применяются сложные процедуры контроля и восстановления данных, так как наиболее типичный режим передачи данных по каналам общего назначения связан со значительными искажениями сигналов.

В общем случае для ГКС характерны:

- разнообразие типов объединенных компьютеров (IBM, Apple и др.);
- отсутствие единой политики управления КС и защиты передаваемых данных, поскольку локальные и городские сети, входящие в состав глобальных, принадлежат различным организационным структурам;
- большое разнообразие способов соединения компьютеров внутри сети (могут использоваться все среды передачи данных);
- гораздо более низкие скорости передачи данных по сравнению с ЛКС – от 9,6 Кбит/с до 2 Мбит/с, и только на магистральных каналах, соединяющих между собой ЛКС или ГКС, – свыше 2 Мбит/с.

Интернет – это, безусловно, самая большая и популярная ГКС в мире, широко используемая для объединения университетов, учреждений, организаций, фирм, частных пользователей и пр. Она объединяет в себе более 50 млн компьютеров. Число ее пользователей стремительно растет с каждым часом.

Примерами ГКС, отличных от Интернет и функционирующих на российском рынке телекоммуникационных сетей¹, могут служить сети RELCOM, FIDONET, Спринт-сеть, ИНФОТЕЛ.

На сегодняшний день ясно прослеживается тенденция к сближению ЛКС и ГКС в области технологий, используемых для подключения компьютеров. Причиной этому послужили резкое улучшение качества линий связи в глобальных сетях, разработка новых сетевых технологий²,

¹ Подробнее об этих сетях можно узнать, обратившись к учебному пособию «Основы глобальных компьютерных сетей», готовящемуся к изданию, или другой литературе.

² В данном учебном пособии речь будет идти о популярных сетевых технологиях ЛКС.

нового сетевого оборудования. Кроме того, ЛКС в последние несколько лет перестали быть изолированными, чаще всего они имеют выход «в большой мир» через глобальные линии связи.

Городская компьютерная сеть (ГорКС)¹ является менее распространенным типом КС. Такие сети появились сравнительно недавно и предназначены для обслуживания территории крупного города – мегаполиса или некоторого региона. ГорКС обычно охватывает территорию не более 40–50 км. В то время как ЛКС наилучшим образом подходят для совместного использования ресурсов на коротких расстояниях при высокой скорости, а ГКС обеспечивают работу на больших расстояниях, но с ограниченной скоростью, ГорКС занимают некоторое промежуточное положение. Они используют цифровые магистральные линии связи, часто оптоволоконные, со скоростями от 45 Мбит/с, и предназначены для связи ЛКС в масштабе города и их подключения к ГКС. Отдельные ЛКС, образующие ГорКС, при этом могут принадлежать как одной организации, так и нескольким различным организациям.

ГорКС первоначально были разработаны только для передачи данных между ЛКС, ЛКС и ГКС, но сейчас они поддерживают такие услуги, как видеоконференции и интегральная передача голоса, текста и мн. др. Развитие технологии КС рассматриваемого типа осуществлялось местными телефонными компаниями. Исторически сложилось, что такие местные компании всегда обладали слабыми техническими возможностями и из-за этого не могли привлечь крупных клиентов. Чтобы преодолеть свою отсталость и занять достойное место в мире ЛКС и ГКС, они были вынуждены заняться разработкой ГорКС на основе самых современных технологий.

ГорКС являются общественными КС, поэтому их услуги организациям обходятся дешевле, чем построение собственной (частной) сети в пределах города.

Некоторые потенциальные связи между КС различных типов и Интернетом приведены на рис. 1.4. ЛКС и ГорКС могут существовать отдельно или в качестве части ГКС. По аналогии ГКС могут

¹ Наряду с сокращением ГорКС в различной литературе можно встретить и другие, например, MAN (Metropolitan Area Networks).

функционировать отдельно или быть частью Интернета. Кроме того, к ГорКС и к ГКС могут подключаться индивидуальные пользователи.

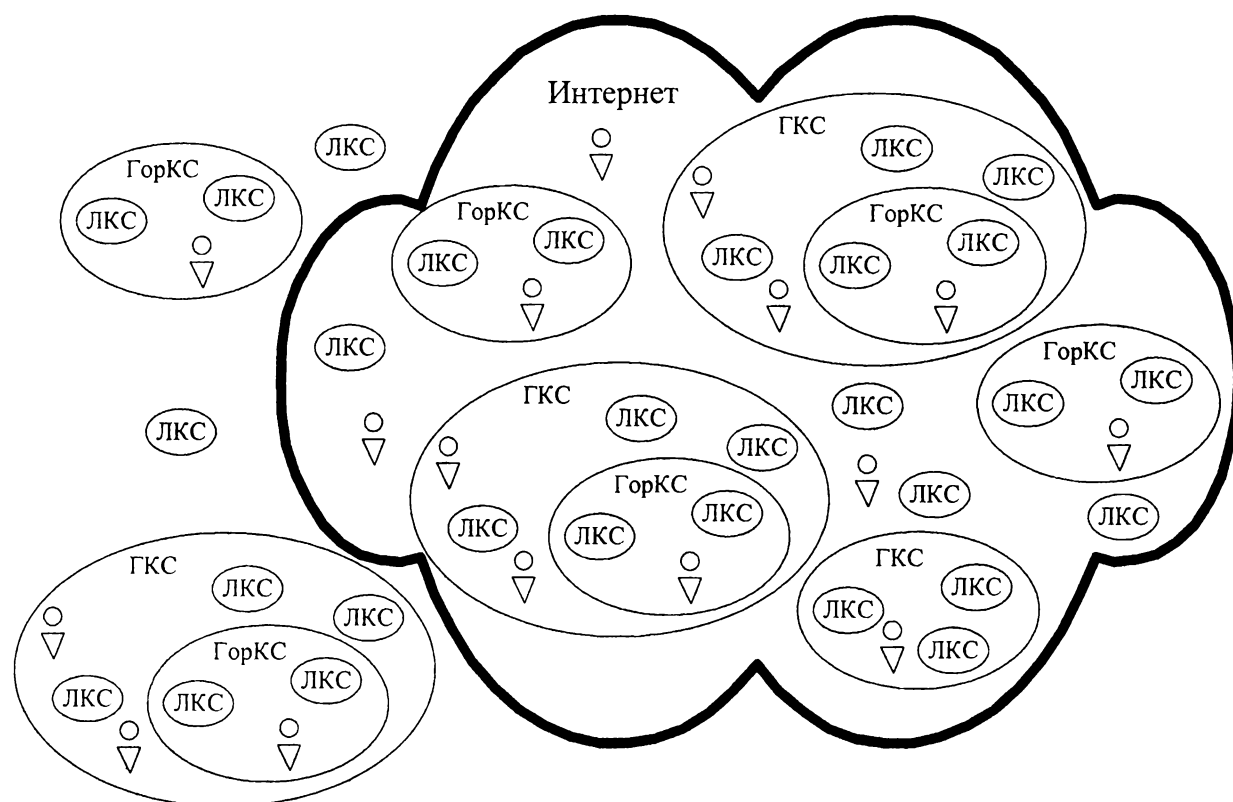


Рис. 1.4. Взаимосвязь между КС различных типов

Классификация КС по принципу организации передачи данных

Данная классификация также имеет большое значение с технической точки зрения. Например, в КС разных типов по-разному организуется доступ компьютеров к среде передачи данных¹, осуществляется контроль ошибок передачи данных, а также используется разное сетевое оборудование.

В зависимости от принципа организации передачи данных выделяют:

- широковещательные КС;
- последовательные КС.

В *широковещательных КС* в каждый момент времени передачу может вести только один узел, остальные узлы могут только принимать информацию. К такому типу КС относится значительная часть ЛКС,

¹ Подробнее этот вопрос рассматривается в разд. 2.

использующих один общий канал связи или одно общее пассивное коммутирующее устройство.

В **последовательных КС** передача данных выполняется последовательно от одного узла к другому и каждый узел ретранслирует принятые данные дальше. К этому типу КС относятся практически все ГКС, ГорКС, а также некоторые ЛКС.

Классификация КС по физической топологии

☞ *Физическая топология – физическое расположение компьютеров, кабелей и других сетевых компонентов в компьютерной сети.*

Классификация КС по данному признаку имеет большое практическое значение. Так, от выбора физической топологии (ФТ) напрямую зависят особенности передачи данных, поведение КС при различных сбоях, необходимый набор сетевого оборудования и др. ФТ влияет и на возможность расширения КС.

Современные ЛКС обычно строятся на базе ФТ «шина», «звезда» или «звезда – шина» (рис. 1.5). Особенности поведения КС с перечисленными ФТ рассматриваются в п. 2.2.1.

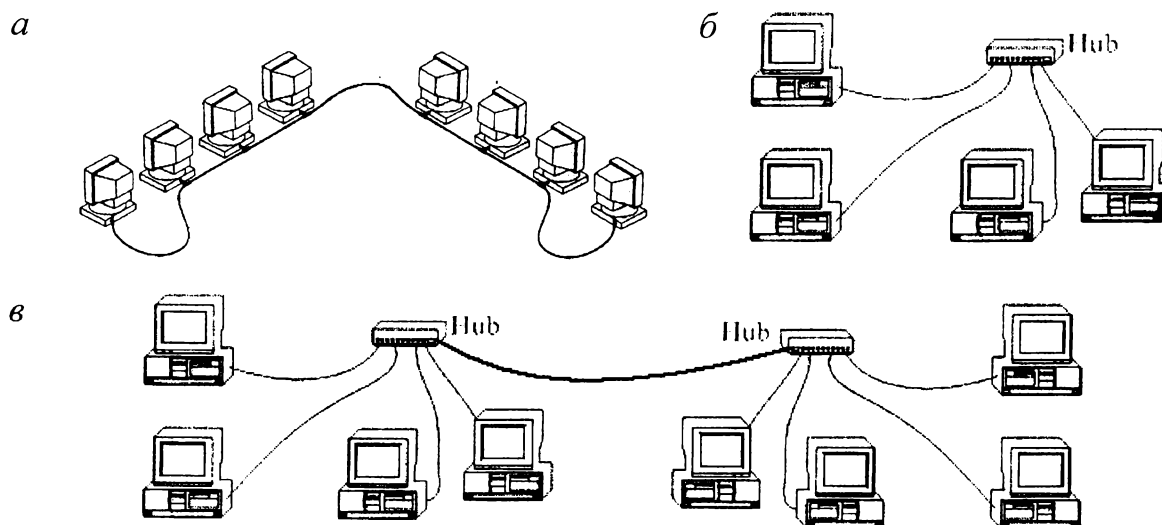


Рис. 1.5. Варианты ФТ ЛКС:

а – «шина»; б – «звезда»; в – «звезда – шина»

ФТ, на базе которых осуществляется построение ГКС, обеспечивают хорошую расширяемость сети¹. К ним относятся «звезда», «иерархическая

¹ В качестве узловых элементов в ФТ ГКС чаще всего выступают маршрутизаторы, основная функция которых обсуждается в п. 1.3.

звезда», «кольцо», «дерево», «полносвязная», «пересекающиеся кольца», «ячеистая», смешанные и др.

Отметим, что в ГКС ФТ «иерархическая звезда» в настоящее время является самой распространенной.

Различные варианты ФТ ГКС показаны на рис. 1.6.

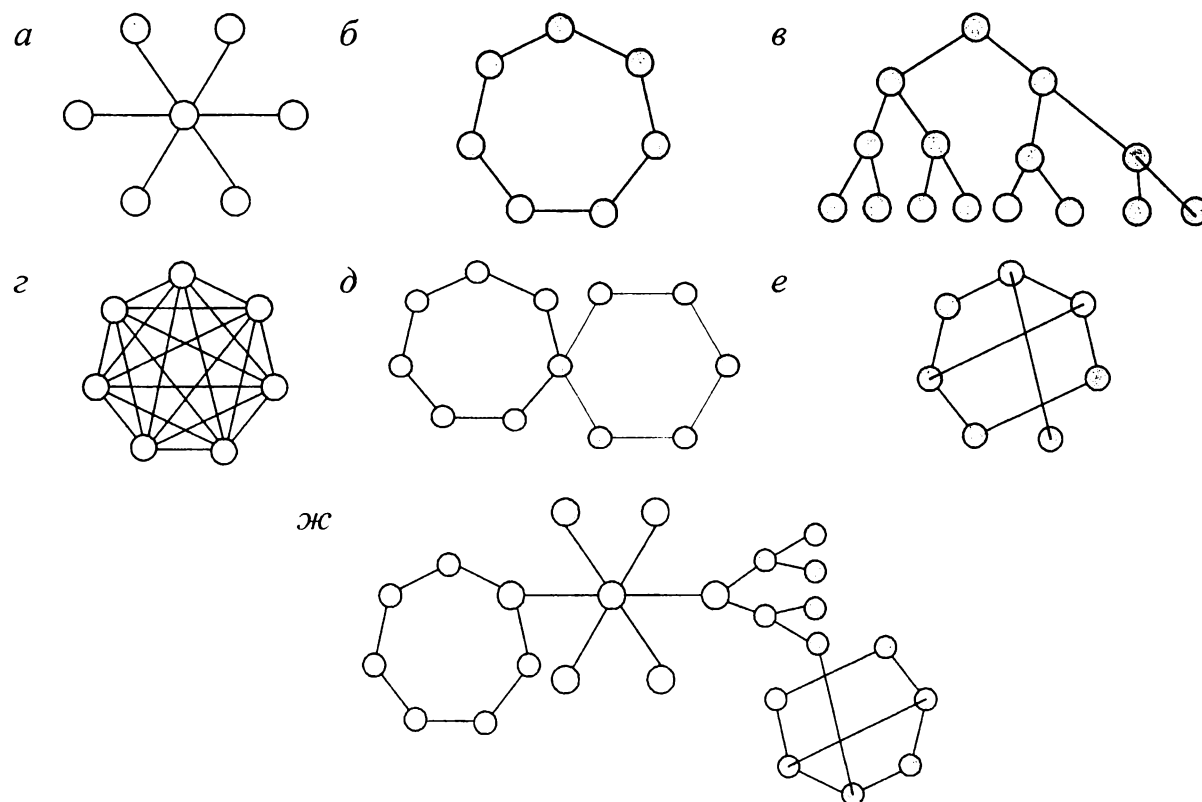


Рис. 1.6. Варианты ФТ ГКС:

- а* – «звезда»; *б* – «кольцо»; *в* – «дерево»; *г* – «полносвязная»;
д – «пересекающиеся кольца»; *е* – «ячеистая»; *ж* – смешанная;
 ○ – маршрутизатор, подключающий ЛКС к ГКС

Классификация КС по способу администрирования

Данная классификация имеет большое практическое значение. От типа зависят, в частности, выбор операционных систем, которые могут быть установлены на компьютерах, а также особенности настройки с их помощью сетевых служб и реализация того или иного подхода по управлению КС.

По способу администрирования, т.е. в зависимости от того, кто и как управляет разделяемыми ресурсами, выделяют следующие типы КС:

- с децентрализованным управлением;
- централизованным управлением;
- со смешанным управлением.

В КС с *децентрализованным управлением* каждый компьютер выполняет функции как сервера, так и клиента, причем каждый пользователь самостоятельно управляет ресурсами своего компьютера¹.

Преимуществами КС такого типа являются их меньшая стоимость по сравнению с сетями с централизованным управлением, отсутствие необходимости использования специальной сетевой операционной системы и обслуживания сети сетевым администратором (или специалистом с соответствующей подготовкой в области компьютерных технологий).

Основными недостатками являются ограниченные возможности расширения КС (вследствие резкого усложнения задач администрирования с увеличением количества компьютеров), потребность в том, чтобы функции администрирования выполнялись на каждой машине, а также меньшая степень безопасности.

В КС с *централизованным управлением* функции администрирования сосредоточены на одном или нескольких центральных компьютерах (чаще всего являющихся аппаратными серверами) со специальной сетевой операционной системой. На этих компьютерах выполняется специальная процедура регистрации пользователей в КС и назначение им различных режимов доступа к сетевым ресурсам.

Преимуществами КС с централизованным управлением можно считать обеспечение высокого уровня безопасности, легкость управления большой сетью, централизованное хранение данных обо всех сетевых ресурсах.

Несмотря на многочисленные преимущества, КС рассматриваемого типа имеют и недостатки. Основными из них являются необходимость приобретения дорогого специализированного программного обеспечения (например, сетевой операционной системы), более дорогого и производительного аппаратного обеспечения для серверных компьютеров, а также обязательность постоянной поддержки работоспособности компьютеров, осуществляющих управление КС. В случае выхода их из строя сетевые ресурсы окажутся недоступными для всех пользователей сети.

¹ Подробнее ЛКС с децентрализованным управлением рассматриваются в разд. 3.

В КС со *смешанным управлением* в определенном сочетании реализованы принципы централизованного и децентрализованного управления (например, под централизованным управлением решаются только задачи с высшим приоритетом, связанные с обработкой больших объемов информации).

1.1.5. Корпоративные КС

Слово «корпорация» означает объединение предприятий, работающих под централизованным управлением и решающих общие задачи. Корпорация является сложной, многопрофильной структурой и вследствие этого имеет распределенную иерархическую систему управления. Кроме того, предприятия, отделения и административные офисы, входящие в корпорацию, как правило, расположены на достаточном удалении друг от друга. Для централизованного управления таким объединением предприятий используется *корпоративная сеть (КорКС)*.

КорКС называются также сетями масштаба предприятия. Они объединяют большое количество компьютеров в офисах фирмы (организации, предприятия), расположенных в одном или нескольких рядом расположенных зданиях, в черте города или даже разбросанных по всему миру, в одну внутреннюю КС и подключают ее к Интернет. Возможны подключения КорКС и к другим ГКС.

Эти сети могут охватывать относительно небольшую территорию, город, регион или даже континент. Число компьютеров может измеряться сотнями, а пользователей – тысячами. В зависимости от особенностей расположения офисов конкретной корпорации (фирмы, организации, предприятия), компьютеры которой объединены в КС, т.е. по территориальному признаку, КорКС может быть отнесена к одному из трех типов, рассмотренных ранее, – ЛКС, ГорС или ГКС. Тип КорКС по территориальному признаку позволяет определять набор сетевых технологий, на основе которых будет осуществляться ее построение.

Поскольку в рамках КорКС объединяется достаточно большое количество компьютеров, в подавляющем большинстве случаев такие КС имеют централизованное управление. Смешанное управление используется реже, а децентрализованное организовывать вообще нет смысла.

В общем случае можно выделить несколько определяющих характеристик КорКС:

- большое количество компьютеров на всех территориях одного предприятия, организации, фирмы и т.д.;

- возможная (но не обязательная) разнотипность компьютеров (IBM, Apple и др.);
- расположение компьютеров в пределах нескольких ЛКС, ГорКС или даже ГКС. Как следствие – разнообразие способов (технологий) соединения компьютеров (например, использование и кабельных, и беспроводных линий связи);
- наличие в составе КорКС связанных между собой ЛКС, – как обязательных и ГорКС и/или ГКС – как возможных компонентов;
- централизованное (в некоторых случаях смешанное) управление сетью, высокий уровень защиты передаваемых данных, для поддержки которой предусмотрены механизмы делегирования полномочий по управлению сетью.

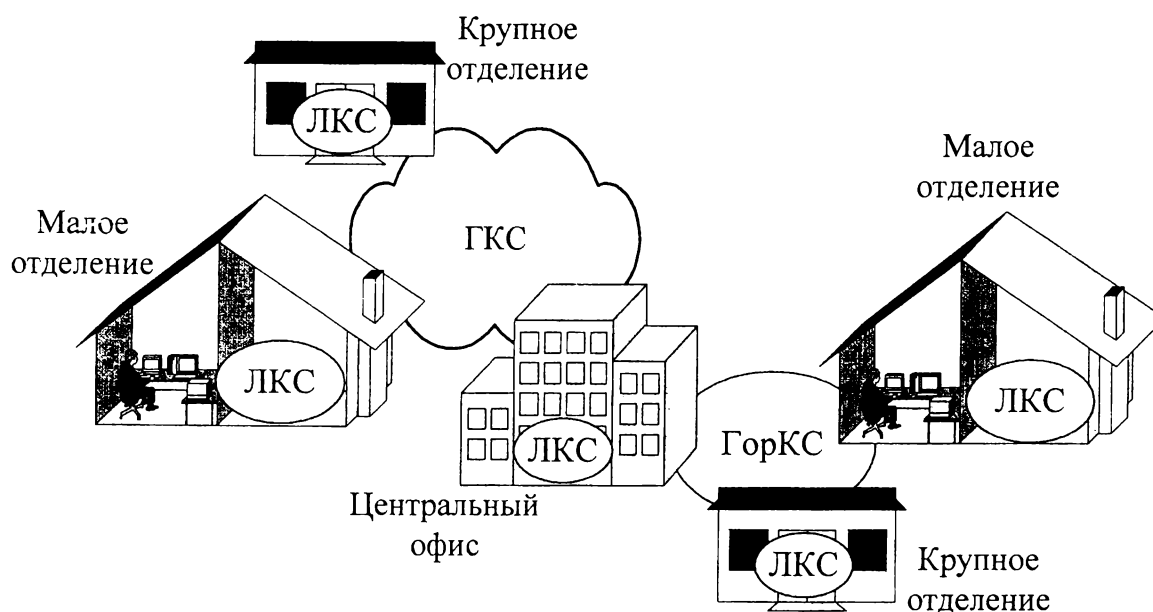


Рис. 1.7. Обобщенная функциональная схема КорКС

Основная задача КорКС заключается в обеспечении передачи информации между различными приложениями, используемыми в организации. Под *приложением* понимается программное обеспечение, которое непосредственно нужно пользователю, – базы данных, электронная почта и т.д. КорКС позволяет взаимодействовать приложениям, зачастую расположенным в географически отдаленных областях, и обеспечивает доступ к ним всех пользователей. На рис. 1.7 показана обобщенная функциональная схема КорКС.

Резюме

1. Основной причиной организации КС является возможность совместного использования ресурсов.
2. Для того чтобы совместно использовать ресурсы сети, на компьютеры пользователей устанавливают специальные программные модули – серверы и/или клиенты.
3. Наиболее часто в сети устанавливаются серверы файлов, печати, почтовый, Web, FTP. Для работы со специализированными серверами на компьютерах пользователей должны быть установлены соответствующие им клиенты.
4. По территориальному признаку КС разделяют на локальные, глобальные и городские.
5. По принципу организации передачи данных различают широко-вещательные и последовательные КС.
6. ЛКС чаще всего строят на основе ФТ «шина», «звезда», «звезда – шина».
7. При построении ГКС используется множество ФТ. Наиболее часто встречающимися являются «звезда», «кольцо», «дерево», «полносвязная», «пересекающиеся кольца», «ячеистая» и смешанная.
8. По способу администрирования КС можно разделить на сети с децентрализованным, централизованным или смешанным управлением.
9. КорКС являются особым типом КС. В подавляющем большинстве случаев такие КС имеют централизованное управление. По территориальному признаку они могут относиться к любому из типов – ЛКС, ГорКС или к ГКС. Основная задача КорКС заключается в обеспечении передачи информации между различными приложениями, используемыми в организации.

Вопросы для контроля

- 1) Что такое «компьютерная сеть»? С какой целью организуются КС?
- 2) Приведите примеры ресурсов КС.
- 3) Какие периферийные устройства не могут быть ресурсами КС? Почему?
- 4) Что такое «сервер», «клиент» КС?
- 5) Какие типы серверов Вам известны? Дайте краткую характеристику каждого из них.
- 6) Какие клиенты КС Вам известны? С какими типами серверов они позволяют взаимодействовать?

- 7) Какие основные требования предъявляются к аппаратным серверам? Чем они отличаются от требований, предъявляемых к аппаратным клиентам?
- 8) Какие среды передачи данных используются в КС?
- 9) Какие основания классификации КС и типы компьютерных сетей внутри каждой из них Вам известны? Дайте им краткую характеристику.

1.2. Линии связи

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами разделов «Физический уровень модели OSI» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы» и «Введение в беспроводные сети», «Видеоматериалы» электронного пособия «Беспроводные компьютерные сети».

1.2.1. Архитектура

☞ *Линия связи – это совокупность физических сред, по которым передаются информационные сигналы, и аппаратных средств, при помощи которых эти сигналы передаются и/или принимаются.*

Линия связи состоит в общем случае из физической среды, по которой передаются электрические информационные сигналы, аппаратуры приема/передачи данных (Data Circuit terminating Equipment – DCE) и промежуточной аппаратуры (рис. 1.8).

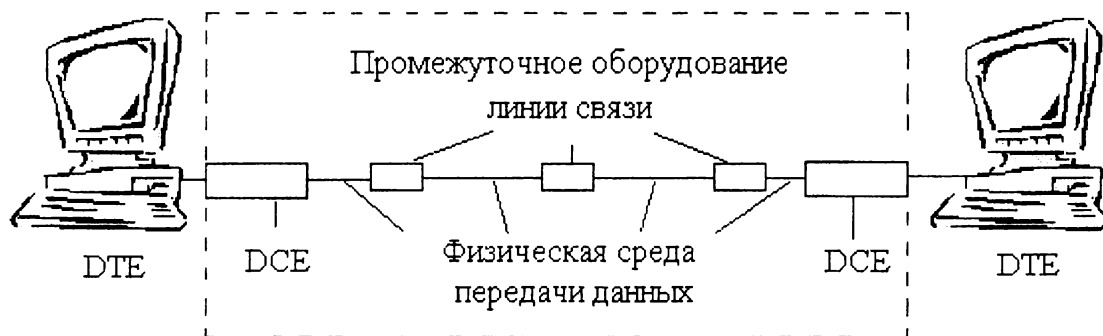


Рис. 1.8. Архитектура линии связи

Аппаратура приема/передачи данных непосредственно связывает компьютеры или ЛКС пользователя с физической средой передачи данных и является пограничным оборудованием. В качестве примеров DCE-устройств можно привести модемы, устройства подключения к цифровым каналам.

☞ *DCE – это устройство, связывающее узлы сети с физической средой передачи данных.*

DCE-устройства преобразуют сигналы, которые затем передаются по КС, проверяют правильность их передачи удаленным узлам и т.п.

Физическая среда передачи данных может представлять собой кабель, т.е. набор проводов, изоляционных и защитных оболочек и соединитель-

ных разъемов, а также земную атмосферу или космическое пространство, через которые распространяются электромагнитные волны.

В глобальных, реже в корпоративных сетях необходимо обеспечить качественную передачу сигналов на расстояния в сотни или тысячи километров. Поэтому без усилителей сигналов, установленных через определенные расстояния, построить территориальную линию связи невозможно. Для этого используется *промежуточная аппаратура*¹. В ЛКС промежуточная аппаратура может совсем не использоваться, так как в этом типе сетей расстояния между узлами² небольшие.

Аппаратура пользователя, вырабатывающая данные для передачи по линии связи и подключаемая непосредственно к DCE-устройствам, обобщенно носит название «оконечное оборудование данных» (Data Terminal Equipment – DTE).

☞ *DTE – это устройство, вырабатывающее сигналы для передачи по линии связи.*

Примерами DTE-устройств могут служить сетевые платы, устанавливаемые на компьютере для его подключения к КС.

Отметим, что DTE-устройства не входят в состав линии связи.

В одной линии связи может быть организовано несколько каналов связи.

☞ *Канал связи – путь передачи электрических сигналов между двумя или несколькими точками.*

С целью организации канала связи используются временное, частотное, кодовое и другие виды разделения. Например, письмо можно отправить либо железнодорожной, либо воздушной почтой. При этом в одной линии связи – пространстве – существуют несколько каналов связи – железнодорожная перевозка и воздушная почта.

Если канал полностью монополизирован линией связи, он может называться *физическим каналом* и в этом случае совпадает с линией связи. Примером может служить передача немодулированных сигналов по линии связи. При передаче модулированных сигналов может быть организовано несколько каналов связи.

¹ Примерами промежуточной аппаратуры, используемой в ЛКС, могут служить повторители, усилители и концентраторы, о которых пойдет речь в разд. 2.

² Узел – это точка соединения в сети. В общем случае узел представляет собой устройство, запрограммированное или спроектированное для распознавания и обработки запросов на передачу информации другим узлам.

1.2.2. Типы линий связи

В зависимости от среды передачи данных выделяют следующие типы линий связи, которые используются в КС:

- 1) проводные;
- 2) кабельные;
- 3) беспроводные.

Рассмотрим перечисленные типы линий связи более подробно.

Проводные линии связи представляют собой провода без каких-либо изолирующих или экранирующих оплеток, проложенные между столбами и висящие в воздухе. По таким линиям связи традиционно передаются телефонные или телеграфные сигналы, но при отсутствии других возможностей эти линии используются и для передачи компьютерных данных. Скоростные качества и помехозащищенность этих линий оставляют желать много лучшего. Сегодня проводные линии связи быстро вытесняются кабельными.

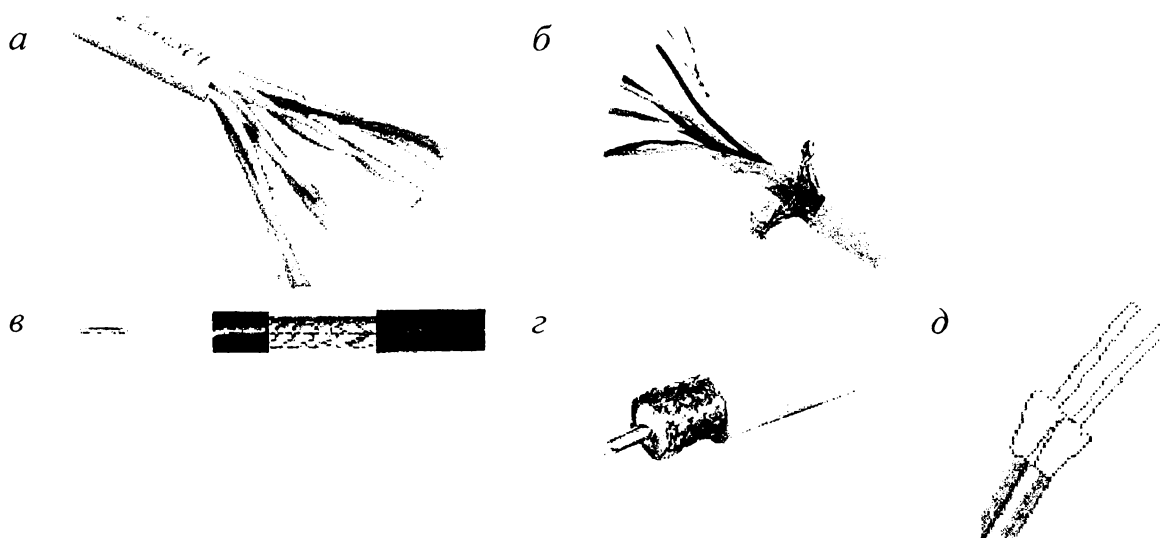


Рис. 1.9. Кабели:

a – UTP; *б* – STP; *в* – RG-58; *г* – RG-8; *д* – волоконно-оптический

В КС применяются три основных типа кабелей:

- витая пара – неэкранированный кабель (Unshielded Twisted Pair – UTP) и экранированный кабель (Shielded Twisted Pair – STP), представленные на рис. 1.9, *a*, *б*;
- коаксиальные кабели с медной жилой (Registered Grade – RG) – RG-58 и RG-8 (рис. 1.9, *в*, *г*);

- волоконно-оптический кабель (рис. 1.9, д).

Кабельные линии связи представляют собой достаточно сложную конструкцию. Кабель состоит из проводников, заключенных в один или несколько слоев изоляции: электрической, электромагнитной, механической, климатической и т.п.

Более подробно типы кабелей, используемых в ЛКС, рассматриваются далее в данном разделе.

Бывают ситуации, когда кабель применить нельзя, например при прохождении линии связи через местность, в которой здания располагаются на значительном расстоянии друг от друга, или же для связи с мобильным пользователем сети (шофер грузовика, врач, совершающий обход, и т.п.). В этом случае используют беспроводные линии связи. Примеры беспроводных сетей приведены на рис. 1.10.

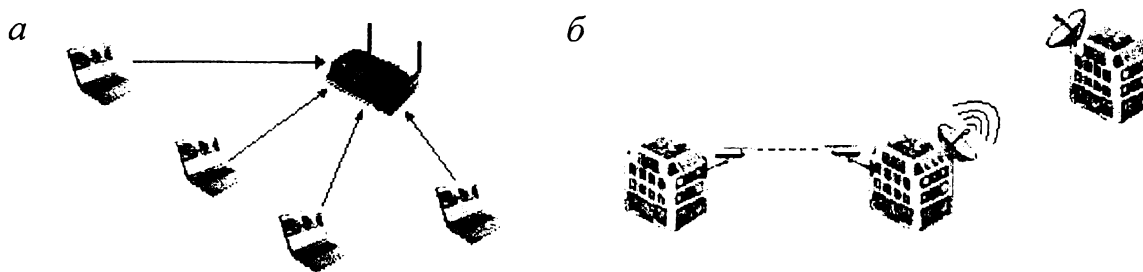


Рис. 1.10. Беспроводная компьютерная сеть:
а – внутри офиса; б – между зданиями

Идея беспроводной среды весьма привлекательна, так как ее компоненты:

- 1) гарантируют определенный уровень мобильности;
- 2) позволяют снять ограничения на максимальную протяженность сети, накладываемые любыми из кабельных линий связи.

Беспроводные компьютерные сети чаще всего организуются:

- если люди, работающие с сетью, не имеют постоянного рабочего места (например, для работников склада);
- в помещениях, где планировка часто меняется (например, в помещениях, где организуются выставки);
- в строениях, где прокладывать кабель запрещено (памятники истории или архитектуры);
- для развертывания временной сети (например, для проведения конференции).

Беспроводная сеть не всегда означает полное отсутствие проводов в КС. Широко распространены КС, где беспроводные компоненты взаимодействуют с сетью, в которой в качестве среды передачи используется кабель. Пример такой сети представлен на рис. 1.11.

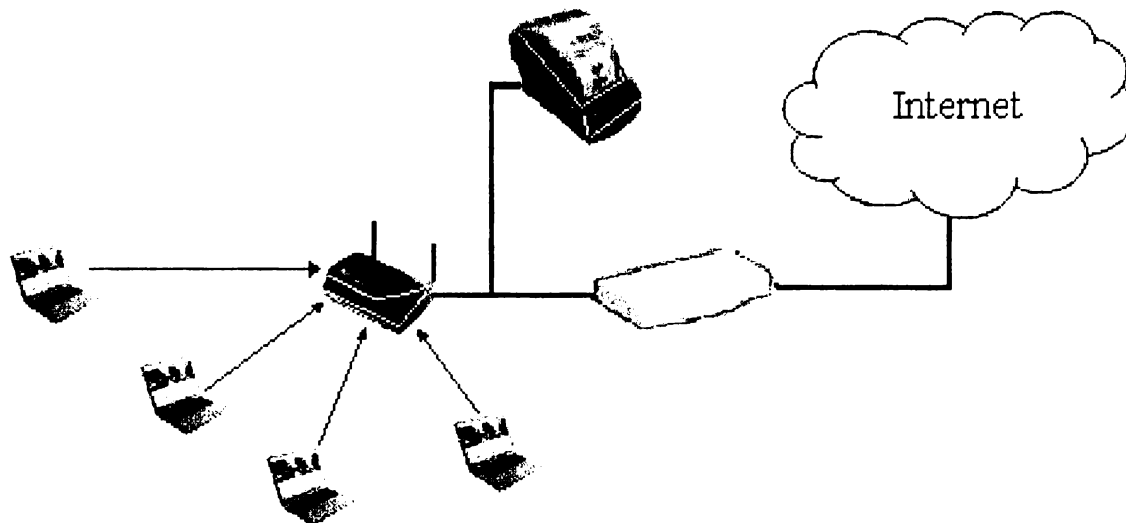


Рис. 1.11. Пример компьютерной сети, использующей проводные и беспроводные линии связи

В компьютерных сетях для передачи данных используются аналоговые и цифровые (дискретные) сигналы. ЛКС практически всегда основаны на передаче цифровых сигналов по кабелю. Аналоговые сигналы используются в основном в глобальных сетях. В городских сетях можно встретить оба варианта.

Отметим, что по кабелям любого типа, используемым при построении компьютерных сетей, могут передаваться и аналоговые, и цифровые сигналы. Какой именно тип сигнала будет передаваться по линии связи, целиком зависит от используемого в сети промежуточного оборудования.

В зависимости от типа промежуточного оборудования все линии связи делятся:

- на аналоговые;
- цифровые.

В аналоговых линиях промежуточная аппаратура предназначена для усиления аналоговых сигналов. Такие линии связи традиционно применялись в телефонных сетях для связи АТС между собой.

В цифровых линиях связи «работают» дискретные сигналы. С помощью таких сигналов передаются компьютерные данные (оцифрованная речь, изображение и др.). В этих линиях связи используется проме-

жуточная аппаратура, которая улучшает форму цифровых сигналов и обеспечивает их последовательную передачу.

1.2.3. Основные характеристики линий связи

Напомним некоторые факты, изучаемые в школьном курсе физики.

Частота характеризует количество колебаний некоторой величины (например, напряжения) за секунду. Она выражается в Герцах (Гц) и означает число периодов колебаний за секунду. Также используются большие величины – Мегагерцы (МГц); $1 \text{ МГц} = 10^6 \text{ Гц}$. В самом простом случае колебания можно представить как синусоидальные волны (рис. 1.12). Иными словами, синусоидальное колебание, частота которого составляет 8 МГц, в течение одной секунды восемь миллионов раз проходит через максимум. Чем выше частота, тем больше скорость передачи данных.

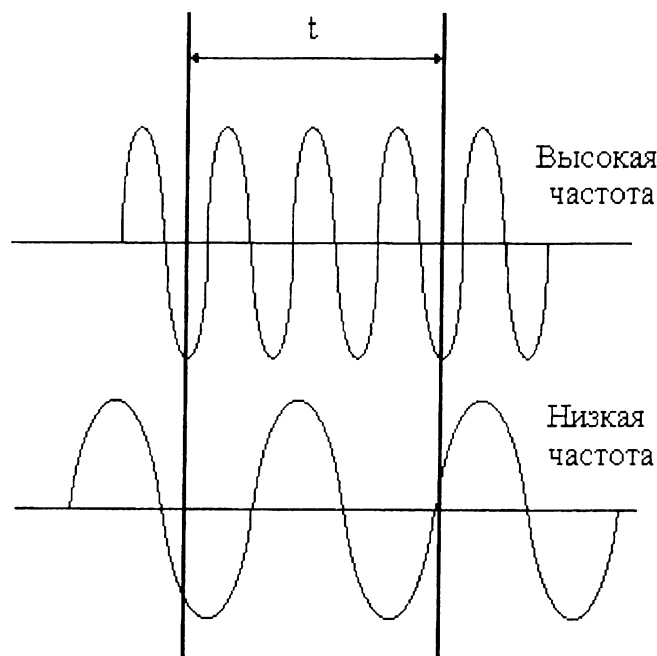


Рис. 1.12. График частоты сигналов

Здесь мы вплотную подошли к рассмотрению такой характеристики линий связи, как полоса пропускания.

☞ *Полоса пропускания – это разница между максимальной и минимальной частотой сигналов, которые можно передать по кабелю.*

Например, диапазон 902–928 МГц предоставляет полосу пропускания 26 МГц. Эта полоса пропускания является основным ограничивающим фактором для скорости передачи сигналов и данных в любой коммуникационной технологии, использующей данный диапазон частот.

Полоса пропускания в определенной степени характеризует линию связи. Она указывает, что теоретически физическая среда способна обеспечить работу в данном диапазоне частот. Рабочая полоса пропускания (в реальных рабочих условиях) может значительно изменяться под воздействием, например, помех.

☞ *Помеха – электрический сигнал, искажающий сигналы, передающие данные.*

Распространение сигналов и помех по сети напоминает распространение звуковых сигналов. С помехами мы сталкиваемся, когда разговаривают множество людей и нам трудно разобрать, кто именно и что сказал, и даже идентифицировать какой-либо голос, если его перекрывает другой.

Полоса пропускания и физическая среда, поддерживающая эту передачу, более точно характеризуются не частотой, а количеством битов в секунду, которые фактически передаются, т.е. пропускной способностью линии связи.

☞ *Пропускная способность линии связи характеризует максимально возможную скорость передачи данных по линии связи.*

Пропускная способность измеряется в битах в секунду – бит/с, а также в производных единицах, таких как килобит в секунду (Кбит/с), мегабит в секунду (Мбит/с) и т.д.

К другим физическим характеристикам линий связи разных типов относится *предельно допустимое расстояние между узлами сети*, обеспечивающее правильную передачу сигнала. Для разных частот и физических сред такое расстояние будет разным. С ростом частоты эта величина будет уменьшаться. Длина такого расстояния зависит от затухания.

☞ *Затухание – это ослабление сигнала по мере его прохождения по линии связи.*

Чем более подвержена физическая среда воздействию помех, тем сильнее затухает в ней сигнал.

С затуханием мы сталкиваемся, когда кто-нибудь находится слишком далеко от нас, и мы не можем понять, что именно нам сказали.

Помехоустойчивость линии определяет ее способность уменьшать уровень помех, создаваемых во внешней среде, на внутренних проводниках. Помехоустойчивость линии зависит от типа используемой

физической среды, а также от экранирующих и подавляющих помехи средств самой линии. Наименее помехоустойчивыми являются радиолнии, хорошей устойчивостью обладают кабельные линии и отличной – волоконно-оптические линии, малочувствительные к внешнему электромагнитному излучению. Обычно для уменьшения влияния помех, появляющихся из-за внешних электромагнитных полей, проводники экранируют и/или скручивают.

1.2.4. Особенности передачи данных в компьютерных сетях

Существует много способов физического создания и передачи сигнала: электрические импульсы могут проходить по медному проводу, импульсы света – по стеклянному или пластмассовому волокну, радиосигналы передаются по воздуху; лазерные импульсы передаются в инфракрасном диапазоне.

В вычислительной технике для представления данных используется двоичный код. Внутри компьютера единицам и нулям данных соответствуют дискретные электрические сигналы.

☞ *Представление данных в виде электрических или оптических сигналов называется кодированием.*

Существуют различные способы кодирования двоичных цифр 1 и 0. В компьютерных сетях применяют три способа: потенциальное, импульсное кодирование и модуляцию.

При *потенциальном кодировании* информативным является уровень сигнала в определенные моменты времени. При этом единице соответствует один уровень напряжения, а нулю – другой (рис. 1.13, а).

При *импульсном кодировании* для представления цифр 1 и 0 используются импульсы различной или одной полярности (рис. 1.13, б).

☞ *Немодулированные сигналы – это сигналы, полученные при использовании потенциального или импульсного способа кодирования.*

Аналогичные подходы используются для кодирования данных и передачи их между двумя компьютерами по линиям связи. Однако эти линии связи отличаются по своим электрическим характеристикам от тех, которые существуют внутри компьютера. Главное отличие внешних линий связи от внутренних состоит в их гораздо большей протяженности, а также

в том, что они проходят вне экранированного корпуса по пространствам, зачастую подверженным воздействию сильных электромагнитных помех. Кроме этого, немодулированные сигналы быстро затухают, поэтому потенциальное и импульсное кодирование редко используют для передачи данных на расстояния свыше 500 м.

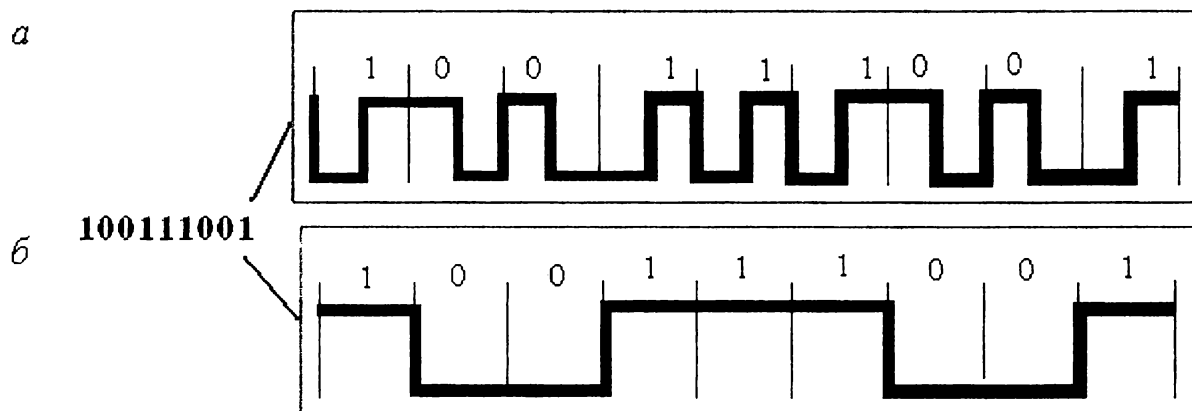


Рис. 1.13. Кодирование:

а – потенциальное, *б* – импульсное

Передавать данные на большие расстояния позволяет *модуляция* – специфический способ представления данных, который никогда не используется внутри компьютера. При модуляции данные передаются в виде аналогового сигнала. Сигналы кодируются аналоговой (непрерывной) электромагнитной или световой (тоже электромагнитной) волной.

☞ *Модулированные сигналы – это сигналы, полученные при использовании модуляции для кодирования.*

В ЛКС модулированные сигналы, как правило, не используются, а применяются немодулированные. При передаче данных в глобальных и городских сетях используются оба типа сигналов.

Повторители и усилители – это устройства, регенерирующие электрические или световые сигналы для увеличения расстояния, на которые сигнал может распространяться. Все эти устройства усиливают сигнал перед его повторной передачей.

☞ *Повторитель – устройство, предназначенное для компенсации затухания в среде передачи данных путем усиления немодулированных сигналов в целях увеличения масштабов их распространения.*

☞ *Усилитель – устройство, предназначенное для компенсации затухания в среде передачи данных путем усиления модулированных сигналов в целях увеличения масштабов их распространения.*

По сути дела, происходит следующее: когда пакеты данных поступают на повторитель, устройство принимает их и преобразует в ту форму, которую они имели перед отправлением. Повторитель фактически не воздействует ни на данные, ни на адресную информацию. Однако он заново создает сигнал с «нулевой отметки», а не просто пересылает исходный сигнал. Если пакет был поврежден при поступлении на вход повторителя, он таким и останется на его выходе.

При передаче модулированных сигналов для увеличения пропускной способности линии связи очень часто используют мультиплексирование.

☞ *Мультиплексирование – процесс совмещения нескольких сигналов, передаваемых в одной физической среде.*

☞ *Мультиплексор – это устройство, которое объединяет информацию, поступающую по нескольким каналам ввода, и выдает ее по одному выходному каналу.*

На принимающей стороне мультиплексированные сигналы восстанавливаются, т.е. отделяются друг от друга в специальном устройстве – демультимплексоре.

☞ *Демультимплексор – это устройство, выполняющее операцию, обратную той, которую осуществляет мультиплексор.*

Рассмотрим этот способ передачи сигнала на примере кабельного телевидения. В телевизор встроено устройство декодирования сигналов, которое выделяет один канал и отбрасывает остальные. Благодаря этому зритель может выбрать желаемую программу.

1.2.5. Методы передачи данных

Простейший метод передачи информации называется *симплексным*: данные передаются только в одном направлении – от отправителя к получателю. Этот метод применяется в радио- и телевидении. Он не позволяет определять и исправлять ошибки во время передачи, поэтому к получателю не всегда приходят корректные данные.

Понятно, что симплексная передача данных в компьютерных сетях недостаточна, так как необходим обмен информацией, т.е. передача сигналов в двух направлениях, а не в одном.

Более эффективным считается *полудуплексный* метод передачи данных. При его использовании информация может передаваться в двух направлениях, но только попеременно. Он позволяет определять ошибки и исправлять их, посылая запросы на повторную передачу данных. Полудуплекс применяется в большинстве модемов и коротковолновых приемниках.

Самым эффективным методом передачи данных является *дуплекс* (*полнодуплексная передача*), когда данные пересылаются в двух направлениях одновременно.

Резюме

1. Линия связи состоит в общем случае из физической среды, по которой передаются электрические информационные сигналы, аппаратуры передачи данных и промежуточной аппаратуры.
2. Для передачи данных в компьютерных сетях используются два типа линий связи: кабельные и беспроводные.
3. В зависимости от промежуточной аппаратуры различают аналоговые и цифровые линии связи.
4. Выделяют несколько основных характеристик линий связи: полоса пропускания, пропускная способность, предельно допустимое расстояние между узлами сети, затухание и помехоустойчивость.
5. Исходные данные перед отправкой по линии связи кодируются. По сети передаются либо модулированные, либо немодулированные сигналы.
6. Повторители и усилители предназначены для компенсации затухания в среде передачи данных путем усиления сигналов в целях увеличения расстояния, на которое они распространяются.
7. Для одновременной передачи многих сигналов по одной линии связи используется мультиплексирование.
8. Для передачи сигналов по линиям связи может использоваться симплексный, полудуплексный или дуплексный метод.

Вопросы для контроля

- 1) Что понимают под линией связи?
- 2) Какова архитектура линии связи? Дайте краткую характеристику каждому из компонентов, входящих в ее состав.

- 3) Почему сетевые платы относят и к DCE-устройствам, и к DTE-устройствам?
- 4) В чем, на Ваш взгляд состоят сходство и различие между линией связи и каналом связи?
- 5) Какие типы линий связи, применяемых для передачи данных в компьютерных сетях, Вам известны? Дайте краткую характеристику каждого из них.
- 6) Перечислите и опишите основные характеристики линий связи.
- 7) С какими проблемами использования различных линий связи в компьютерных сетях Вам уже доводилось сталкиваться? Приведите примеры.
- 8) В чем состоит разница между аналоговыми и дискретными сигналами? Укажите достоинства и недостатки использования каждого из этих типов сигналов.
- 9) Какие способы кодирования сигналов, используемые в компьютерных сетях, Вам известны? Дайте каждому из них краткую характеристику.
- 10) Каковы особенности передачи немодулированных сигналов?
- 11) Каковы особенности передачи модулированных сигналов?
- 12) Какие устройства используются для усиления сигнала в немодулированных системах?
- 13) Какие устройства используются для усиления сигнала в модулированных системах?
- 14) С какой целью в компьютерных сетях используется мультиплексирование?
- 15) Какие способы передачи данных по сети Вам известны? Дайте им краткую характеристику.

1.3. Принципы передачи данных по КС

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами раздела «Модель OSI» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы», а также материалами документа *Стандартизация(организации).htm*, расположенного в папке *Учебная\Доп_материалы*.

1.3.1. Поточковая и пакетная передача данных

Данные обычно содержатся в больших файлах. При потоковой передаче файлы с данными передаются как единое целое. При использовании такого метода передачи данных остальные компьютеры вынуждены долго ждать, так как время передачи файла может быть весьма продолжительным.

В связи с этим потоковая передача данных в КС используется крайне редко. Вместо нее организуется *пакетная передача данных*. Рассмотрим принципы ее организации.

Чтобы многие компьютеры могли работать в сети одновременно, прежде чем передать большие файлы по кабелю или по какому-либо другому каналу связи, их разбивают на маленькие фрагменты (их размер для большинства сетей – от 512 байт до 4 Кбайт), с которыми могут работать сетевые устройства.

Разбиение передаваемых данных на маленькие фрагменты предоставляет ряд преимуществ:

- компьютеры в КС могут передавать данные по очереди. Один компьютер, передающий большое количество данных, не монополизирует канал связи;
- если в КС происходит сбой и фрагмент данных теряется, то требуется передать заново только его, а не весь файл;
- в зависимости от ФТ КС и типа соединения каждый фрагмент данных может проходить к адресату разными путями. Следовательно, если один из путей перегружен или вышел из строя, эти фрагменты данных могут достичь адресата другими путями. Эффективность и надежность передачи при этом существенно повышаются.

Для того чтобы операционная система (ОС) на компьютере-получателе могла правильно сформировать исходный блок данных из фрагментов, полученных в произвольном порядке по КС, ОС компьютера-отправителя

к каждому такому блоку данных добавляет *заголовок* (как адрес на почтовом конверте), содержащий специальную информацию:

- адрес получателя;
- адрес отправителя;
- номер фрагмента в общей последовательности, обеспечивающий правильность сборки данных на принимающей стороне;
- размер фрагмента данных, передаваемого в пакете.

Заголовок размещается в начале фрагмента данных. В конце может быть добавлен *трейлер*. Заголовок, фрагмент данных и трейлер в совокупности образуют *пакет*, который и становится минимальной единицей информации, передаваемой в КС. На рис. 1.14 показана структура типичного пакета данных, передаваемого по КС.

Содержимое трейлера – это, чаще всего, информация для проверки ошибок, обеспечивающая корректность передачи данных. Ее часто называют *контрольной суммой*.

Контрольная сумма вычисляется как функция от фрагмента данных, передаваемых внутри пакета, причем не обязательно только путем суммирования. Компьютер-получатель повторно вычисляет контрольную сумму по известному алгоритму и в случае ее совпадения с контрольной суммой, вычисленной компьютером-отправителем, делает вывод о том, что пакет был передан через КС без ошибок. При несовпадении контрольных сумм на стороне компьютера-получателя фиксируется ошибка, о чем уведомляется компьютер-отправитель.

Существует несколько алгоритмов вычисления контрольной суммы, отличающихся вычислительной сложностью и высокой способностью обнаруживать ошибки в данных¹.

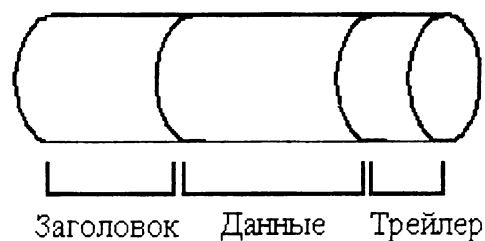


Рис. 1.14. Общая структура пакета компьютерной сети

¹ Знакомство с подобными алгоритмами выходит за рамки данного учебного пособия.

1.3.2. Многоуровневая архитектура компьютерной сети

Тезис о пользе стандартизации, справедливый для всех отраслей, в компьютерных сетях приобретает особое значение. КС обеспечивает соединение различного оборудования разных производителей; в связи с этим проблема совместимости является одной из наиболее острых. Без принятия всеми производителями общепринятых правил разработки оборудования прогресс в деле построения КС был бы невозможен, поэтому все их развитие в конечном счете отражено в стандартах – любая новая технология только тогда приобретает «законный» статус, когда ее содержание закрепляется в соответствующем стандарте.

В КС идеологической основой стандартизации является многоуровневый подход к разработке средств сетевого взаимодействия. Именно на основе этого подхода были разработаны несколько сетевых моделей взаимодействия открытых систем, ставшие своего рода универсальными языками сетевых специалистов. Далее понятия «сетевая модель», «открытая система», «стандарты», «спецификации», «многоуровневый подход» будут рассмотрены более подробно.

Сетевые модели, стандарты и спецификации

Восприятие информации человеком в значительной степени зависит от ее визуализации. Мы лучше понимаем что-либо, когда видим это своими глазами. Абстрактные концепции не имеют конкретных форм, однако, чтобы их было легче понять, используются визуальные модели структуры, процессов или отношений.

Мы встречаемся с наглядными моделями на каждом шагу. Генетики условно изображают структуру молекулы ДНК в виде двойной спирали. В физической модели атома электроны и протоны представлены в виде шариков, что позволяет наглядно выразить то, что нельзя увидеть непосредственно.

Назначение *сетевых моделей* – помочь описать и понять процесс сетевой коммуникации. Кроме того, они служат основой стандартизации оборудования и программного обеспечения КС. Если разные поставщики сетевых продуктов используют одну и ту же модель, их продукты будут совместимы друг с другом. В сетевой модели представлено, как должны происходить процессы коммуникации. Если поставщики придерживаются стандартов на каждом уровне таких моделей, их оборудование будет совместимо с оборудованием других поставщиков.

Компоненты КС стандартизируются и специфицируются не только сетевыми моделями. Многочисленные организации разрабатывают и публикуют *спецификации* сетевого оборудования и программного обеспечения. Конечно, спецификации не являются законом. Организации, разрабатывающие *стандарты*, не входят в состав правительства и не могут принуждать к соблюдению стандартов. Поставщик может отклоняться от стандартов как ему заблагорассудится, однако это не в его интересах. Собственные продукты, работающие только с продуктами этого же поставщика, непопулярны. В первые годы развития сетевых технологий производители могли не обращать внимания на стандарты, однако в настоящее время совместимость с другими продуктами является одним из основных требований.

☞ *Стандарты – документированные соглашения, содержащие технические спецификации или другие точные критерии, которых следует придерживаться в качестве правил, директив или необходимых примеров, определяющих соответствие материалов, продуктов, процессов и услуг своему назначению.*

Признанной организацией по стандартизации является Всемирная федерация национальных организаций по стандартизации (International Standardization Organization – ISO), однако это далеко не единственная организация, разрабатывающая и публикующая стандартизирующие спецификации на сетевые компоненты. Приведем примеры других международных органов стандартизации, отличных от ISO:

- Международная комиссия по электротехнике (International Electrotechnical Commission – IEC);
- Международный союз телекоммуникаций (International Telecommunications Union – ITU);
- Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers – IEEE).

Под открытыми спецификациями понимаются опубликованные, общедоступные спецификации, соответствующие стандартам и принятые в результате достижения согласия после всестороннего обсуждения всеми заинтересованными сторонами.

В широком смысле *открытой системой* может быть названа любая система (компьютер, КС, ОС, другие аппаратные и программные продукты), которая построена в соответствии с открытыми спецификациями.

Многоуровневый подход к разработке средств сетевого взаимодействия

Организация взаимодействия между устройствами в КС является сложной задачей. Для решения сложных задач используется универсальный прием – декомпозиция, т.е. разбиение одной сложной задачи на несколько более простых задач-модулей. Процедура декомпозиции включает в себя четкое определение функций каждого модуля, решающего определенную задачу, и правил взаимодействия между ними. В результате достигается логическое упрощение задачи, появляется возможность модификации отдельных модулей без изменения остальной части системы.

При декомпозиции часто используют *многоуровневый подход*. Он заключается в том, что все множество модулей разбивают на уровни. Уровни образуют иерархию, т.е. имеются вышележащие и нижележащие уровни (рис. 1.15).

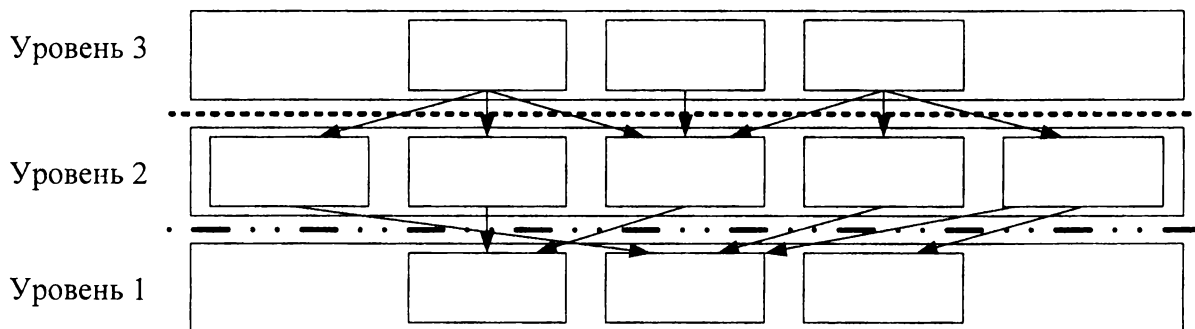


Рис. 1.15. Представление иерархии задач в многоуровневом подходе:

- функции, предоставляемые уровнем 2 уровню 3;
- · — · · — функции, предоставляемые уровнем 1 уровню 2

Множество модулей, составляющих каждый уровень, сформировано таким образом, что для выполнения своих задач они обращаются с запросами только к модулям непосредственно примыкающего нижележащего уровня. С другой стороны, результаты работы всех модулей, принадлежащих некоторому уровню, могут быть переданы только модулям соседнего вышележащего уровня. Такая иерархическая декомпозиция задачи предполагает четкое определение функций каждого отдельного уровня и тех результатов, которые нижележащий уровень предоставляет вышележащему. В результате иерархической декомпозиции достигается

относительная независимость уровней, а значит, и возможность их легкой замены.

Многоуровневое представление средств сетевого взаимодействия имеет свою специфику, связанную с тем, что в процессе обмена информацией участвуют два компьютера, поэтому необходимо организовать согласованную работу двух «иерархий». При передаче данных оба участника сетевого обмена должны принять множество соглашений. Например, должны быть согласованы уровни и форма электрических сигналов, способ определения длины сообщений, методы контроля достоверности и т.п. Соглашения должны быть приняты для всех уровней, начиная от самого низкого до самого высокого.

На рис. 1.16 показана модель взаимодействия двух узлов КС. С каждой стороны средства взаимодействия представлены тремя уровнями. Процедура взаимодействия этих узлов может быть описана в виде набора правил взаимодействия каждой пары соответствующих уровней обеих участвующих сторон. Наборы правил и методов взаимодействия объектов КС, охватывающие основные процедуры, алгоритмы и форматы взаимодействия, обеспечивающие корректность согласования, преобразования и передачи данных в КС в пределах одного уровня, но в разных узлах, называют *протоколами*.

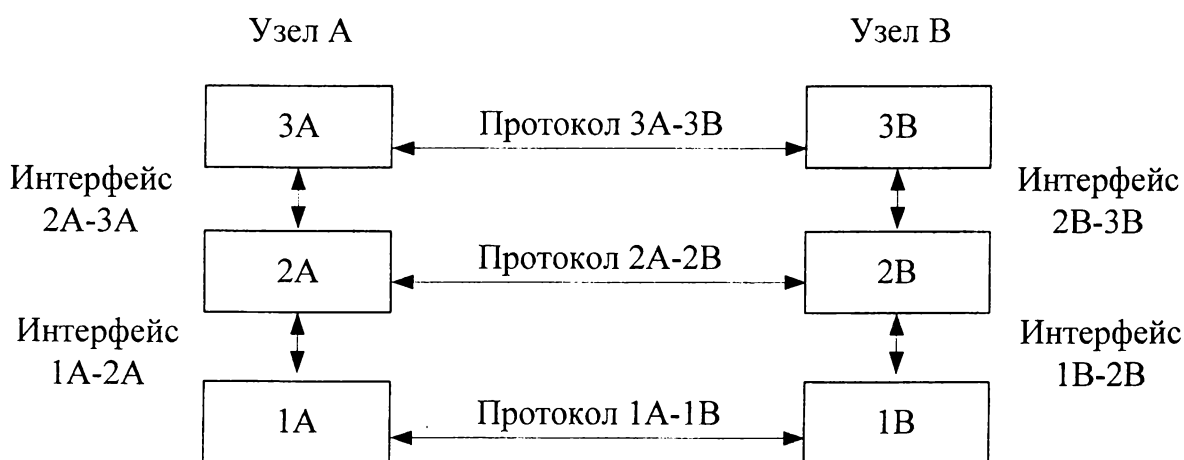


Рис. 1.16. Модель взаимодействия двух узлов КС на трех уровнях

Модули, реализующие протоколы соседних уровней и находящиеся в одном узле, также взаимодействуют друг с другом в соответствии с четко определенными правилами и с помощью стандартизированных форматов сообщений. Эти правила принято называть *интерфейсом*. Интерфейс определяет набор сервисов, предоставляемый данным уровнем соседнему уровню в одном узле.

Таким образом, средства взаимодействия каждого из уровней должны обрабатывать, во-первых, свой собственный протокол, а во-вторых, интерфейсы с соседними уровнями.

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в КС, называется *стеком протоколов*.

Протоколы могут быть реализованы как программно, так и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней, как правило, – чисто программными средствами.

Эталонная модель взаимодействия КС

В начале 1980-х гг. несколько международных организаций по стандартизации, в число которых вошла ISO, разработали сетевую модель, которая сыграла значительную роль в развитии КС. Эта модель получила название модели взаимодействия открытых систем (Open System Interconnection – OSI). Модель OSI была разработана с учетом большого опыта, приобретенного при создании КС в 1970-е гг.

Для реальных систем полная открытость является недостижимым идеалом. Как правило, даже в системах, называемых открытыми, этому определению соответствуют лишь некоторые части.

Модель OSI касается только одного аспекта открытости, а именно открытости средств взаимодействия устройств, связанных с КС. Здесь под открытой системой понимается сетевое устройство, готовое взаимодействовать с другими сетевыми устройствами с использованием стандартных правил, определяющих формат, содержание и значение применяемых и отправляемых сообщений.

В мире КС модель OSI – это «модель моделей». Она является на сегодняшний день своеобразным эталоном и обсуждается практически в каждой книге по КС.

В модели OSI все функции, реализуемые сетевыми компонентами, полностью обеспечивающие обмен данными по КС, распределены между семью уровнями: прикладным, представительским, сеансовым, транспортным, сетевым, канальным и физическим.

На каждом уровне реализуется определенное количество функций, обеспечивающих один из семи этапов обмена данными, передаваемыми по КС. Чем выше уровень, тем сложнее задача, на решение которой он ориентирован. Наиболее простые функции реализуются на физическом уровне, а наиболее сложные – на прикладном.

1.3.3. Функции уровней модели OSI

Самым верхним в иерархии эталонной модели OSI является **прикладной уровень**. Для пользователя этот уровень является главным средством взаимодействия с сетью. Одна из основных функций этого уровня – обеспечение обмена данными между приложениями пользователя и представительским уровнем (рис. 1.17).



Рис. 1.17. Основная функция прикладного уровня модели OSI

Единица данных, которой оперирует прикладной уровень, обычно называется *сообщением*.

Интерфейс между прикладным уровнем и приложениями пользователя, который реализуется операционной системой, позволяет скрыть от пользователя работу всех остальных уровней модели OSI.

Примером может являться работа пользователя с программой электронной почты. Пользователь при помощи специальных команд, предусмотренных клиентом электронной почты (например, Outlook Express), формирует запрос на получение новых сообщений

от почтового сервера. Как только это произойдет, автоматически генерируется запрос к протоколу прикладного уровня, после чего устанавливается соединение с целью извлечения необходимых файлов. Каким образом компьютеры между собой «договариваются» о передаче данных, как будут формироваться пакеты и о многом другом, рядовой пользователь КС не знает, да и не должен знать.

Представительский уровень модели OSI, получив данные от прикладного или сеансового уровня, организует их *представление*, куда входят:

- 1) *Сжатие и распаковка данных*. На стороне компьютера-отправителя происходит сжатие данных с целью их быстрой передачи по сети. На стороне компьютера-получателя уровень представления обеспечивает распаковку данных.
- 2) *Шифрование и расшифровка данных*. На стороне компьютера-отправителя осуществляется преобразование данных в закодированную форму таким образом, чтобы они не могли быть прочитаны

посторонними лицами. На стороне компьютера-получателя эти данные расшифровываются.

- 3) *Трансляция протоколов.* Речь идет о преобразовании данных из формата, понятного одному протоколу, в формат, с которым могут работать другие протоколы. Это необходимо для обмена данными между разными платформами и операционными системами.
- 4) *Преобразование схем кодирования данных.* Далеко не все компьютерные системы используют одну и ту же схему кодирования данных, поэтому на уровень представления данных возложены обязанности по установлению соответствия между несовместимыми схемами кодирования данных, например между ASCII (американский стандартный код обмена информацией) и EBCDIC (расширенный двоичный код обмена информацией). Уровень представления данных также используется для согласования различных числовых форматов с плавающей точкой.

На представительском уровне решается также вопрос о том, чем должен быть обработан запрос компьютера-отправителя – им самим (т.е. он является локальным) или удаленным компьютером (запрос адресован удаленному серверу сети).

Сеансовый уровень позволяет двум приложениям на разных компьютерах устанавливать, использовать и завершать соединение, называемое сеансом. На этом уровне выполняются такие функции, как распознавание имен пользователей и защита информации, необходимые для связи двух приложений в сети.

Сеансовый уровень обеспечивает синхронизацию между пользовательскими задачами посредством расстановки в потоке данных *контрольных точек*. Таким образом, в случае ошибки потребуется заново передать только данные, следующие за последней контрольной точкой. Этот уровень управляет диалогом между взаимодействующими процессами, т.е. регулирует, какая из сторон когда, как долго и т. д. должна осуществлять передачу данных по сети.

Транспортный уровень реализует ряд очень важных функций, к числу которых относятся:

- 1) *Разбиение данных на пакеты.* Транспортный уровень разбивает исходный блок данных на пакеты. Структура пакета определяется протоколом, который используют два компьютера – получатель и отправитель. На этом же уровне к пакету добавляется информация,

которая помогает компьютеру-получателю восстановить исходные данные из случайной последовательности пакетов.

- 2) *Обнаружение ошибок передачи данных.* В обязанности транспортных протоколов входят обнаружение пакетов, которые не были корректно распознаны сетевыми устройствами и автоматическая генерация запроса на их повторную передачу.
- 3) *Поддержка целостности данных.* Именно этот уровень отвечает за надежную и своевременную передачу данных по сети.
- 4) *Подтверждение приема данных.* Эта важная функция реализуется не всеми транспортными протоколами.
- 5) *Обнаружение дубликатов пакетов.* Протоколы транспортного уровня отвечают за то, чтобы на сеансовый уровень поступали пакеты только в единственном экземпляре. Все дубликаты отбрасываются.
- 6) *Упорядочивание пакетов.* Это касается пакетов, которые могли прийти в произвольном порядке. Транспортный уровень может определять первоначальный порядок пакетов и соответствующим образом упорядочить их перед передачей на сеансовый уровень.
- 7) *Разрешение числовых и символьных адресов.* Каждый компьютер может иметь несколько адресов. Пользователи при работе с КС обычно используют *символьные адреса*. Эти адреса предназначены для запоминания пользователями и поэтому несут смысловую нагрузку. Примером могут служить адреса `www.fox_kids.com` и `comp1`. Символьные адреса удобны для пользователя, но их использование ограничено пересылкой данных внутри одной компьютерной сети небольших размеров. Для разрешения указанной проблемы используются *числовые составные адреса*. В них поддерживается двухуровневая иерархия: адрес делится на номер сети и номер узла. Например, в адресе `1C9FDB42:2E702A1D` слева от двоеточия – адрес сети, а справа – адрес узла. Подобное деление позволяет передавать сообщения между сетями только на основании номера сети: номер узла используется только после доставки сообщения в нужную сеть точно так же, как название улицы используется почтальоном только после того, как письмо доставлено в нужный город. Таким образом, в функции транспортного уровня модели OSI входит установка соответствия между символьными и числовыми составными адресами.
- 8) *Пересылка данных между приложениями.* Современные операционные системы являются многозадачными. Это позволяет пользователям выполнять несколько сетевых программ одновременно. Протоколы

транспортного уровня отвечают за правильную пересылку данных, поступающих из КС, между приложениями. Например, если на компьютере пользователя запущены Internet Explorer и Outlook Express, то файлы с сервера электронной почты должны быть переданы Outlook Express, а Web-страницы – Internet Explorer.

Сетевой уровень отвечает за реализацию следующих функций:

- 1) *Адресация сообщений.* На этом уровне к пакету данных добавляется информация об адресах отправителя и получателя.
- 2) *Разрешение имен.* Проведем опять-таки аналогию с работой почтовой службы. Письмо доставлено в нужный город (пакет переслан в нужную КС), после чего были определены улица и номер дома, куда его нужно доставить (определен компьютер, которому необходимо передать данные). Остается решить последнюю и немаловажную задачу – выяснить номер квартиры адресата (определить сетевой интерфейс на компьютере, на который должны быть переданы данные). На одном компьютере может быть установлено несколько сетевых плат, каждая из которых способна передавать и отправлять данные в КС. Однозначно определить, какой именно сетевой плате должны быть переданы данные, позволяют *аппаратные адреса*, не имеющие иерархической структуры (как и номера квартир). Такой адрес обычно используется только аппаратурой, поэтому его стараются сделать по возможности компактным и записывают в виде двоичного, восьмеричного или шестнадцатеричного значения, например 11-AD-5B-96-E1-21.

В обязанности сетевого уровня входит установка соответствия между числовыми составными и аппаратными адресами.

- 3) *Маршрутизация.* На сетевом уровне определяется наилучший путь от компьютера-отправителя к компьютеру-получателю. Протоколы маршрутизации сетевого уровня не отвечают за доставку данных по конечному адресу, а только находят наилучший путь.

Например, письмо отправителя пересылается из одного почтового отделения в другое, пока не достигнет того отделения, которое отвечает за доставку писем к дому адресата. Специальный персонал – сортировщики писем – в каждом из почтовых отделений определяет дальнейший маршрут движения каждого конкретного письма.

Подобным образом данные от компьютера-отправителя к компьютеру-получателю пересылаются через один или несколько маршрутизаторов.

☞ *Маршрутизатор* – это устройство, способное направлять пакеты через несколько сетей.

Обмениваясь информацией, маршрутизаторы определяют лучший путь для передачи данных. Если какой-либо маршрутизатор не способен передавать большие блоки данных, посланные компьютером-отправителем, на сетевом уровне эти блоки разбиваются на меньшие.

Сетевой уровень компьютера-получателя собирает их и приводит в исходное состояние.

Отметим, что единицу данных, передаваемую по КС, именно на сетевом уровне принято называть пакетом.

Протоколы, работающие на **канальном уровне**, должны обеспечивать (по возможности) безошибочную передачу по месту назначения наборов данных, передаваемых по физическому носителю. Поскольку носителей, совершенно исключаящих ошибки, не существует, в протоколах канального уровня предусмотрен механизм контроля ошибок и повторной передачи искаженных пакетов.

При потоковом способе передачи данных по КС каждый из компьютеров на время монополизирует среду передачи данных. Все другие компьютеры ожидают своей очереди. При использовании пакетного способа компьютерам необходимо договариваться между собой о том, кто, когда и сколько данных может передать за один раз. Если компьютеры не могут решить вопросы разделения среды передачи данных, то в КС наступает хаос (как на оживленном перекрестке в случае выхода из строя светофора).

Порядок доступа компьютеров к разделяемой среде передачи данных определяется на канальном уровне модели OSI.

На этом же уровне на компьютере-получателе необработанный битовый поток, проходящий по физическому носителю, перехватывается и собирается в пакет для отправки вышестоящим уровням. Электронное представление данных (способы кодирования, используемые при передаче информации по средством физических носителей; наборы бит и пр.) известны только канальному уровню.

Наборы бит, которые формируются на канальном уровне из пакетов, принято называть *кадрами*.

Физический уровень предназначен для передачи бит (нулей и единиц) от одного компьютера к другому. Содержание самих бит на данном уровне значения не имеет.

Физический уровень формирует сигналы, которые переносят данные, поступившие от всех вышележащих уровней, определяет способ передачи сигналов по сетевому кабелю.

Этот уровень отвечает за кодирование данных и синхронизацию бит, гарантируя, что переданная единица будет воспринята именно как единица, а не как ноль. Наконец, физический уровень устанавливает длительность каждого бита и способ перевода бита в соответствующие электрические или оптические импульсы, передаваемые по сетевому кабелю.

На физическом уровне осуществляется передача потока бит в физической среде (например, по сетевому кабелю). На этом уровне определяется способ соединения сетевого кабеля с платой сетевого адаптера, в частности количество контактов в разъемах и их функции, а также реализуются электрический, оптический, механический и функциональный интерфейсы с кабелем.

1.3.4. Особенности передачи данных в модели OSI

За исключением самого нижнего уровня модели OSI (физического), никакой иной уровень не может непосредственно переслать пакет соответствующему уровню другого компьютера. Информация с любого из уровней на компьютере-отправителе должна пройти через все нижележащие уровни. Затем она передается по сетевому кабелю на компьютер-получатель и проходит снизу вверх по уровням, начиная с физического и заканчивая тем, с которого они были посланы.

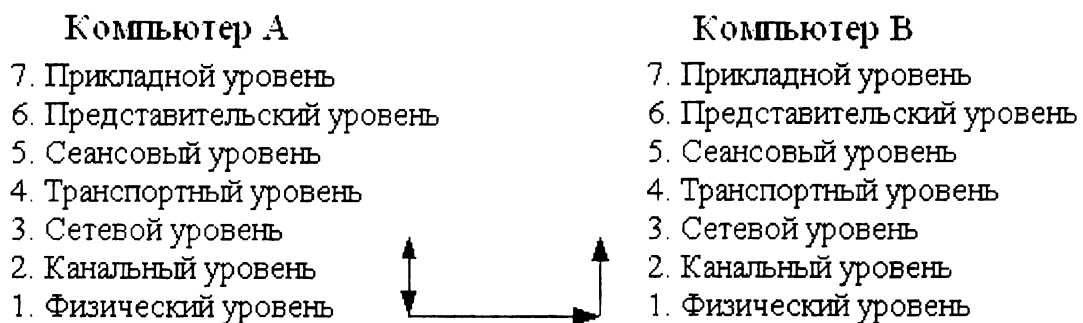


Рис. 1.18. Передача пакета между сетевыми уровнями двух узлов

Например, если с сетевого уровня передается пакет с компьютера А, он спускается через канальный и физический уровни и по сетевому кабелю попадает в компьютер В, где поднимается через физический и канальный уровни и достигает сетевого уровня (рис. 1.18).

Пакеты с данными собираются и разбираются в соответствии с моделью OSI. Процесс их формирования начинается на прикладном уровне модели OSI, т.е. там, где «рождаются» данные. Каждый фрагмент данных, который надо переслать по сети, проходит сверху вниз все семь уровней.

На каждом уровне компьютера-отправителя к исходному фрагменту данных добавляются заголовок и трейлер, предназначенные для соответствующего уровня компьютера-получателя. Например, заголовок и трейлер, добавленные на транспортном уровне компьютера-отправителя, будут прочитаны на транспортном уровне компьютера-получателя.

После формирования пакета¹ прикладной уровень направляет его вниз представительскому уровню. На этом уровне на основе информации, полученной из заголовка прикладного уровня, протоколом представительского уровня выполняются требуемые действия и добавляются к пакету свои собственные заголовок и трейлер². Полученный в результате пакет представительского уровня передается вниз сеансовому уровню, который также добавляет свою служебную информацию, и т.д. Наконец пакет достигает низшего, физического уровня, который, собственно, и передает его по линиям связи компьютеру-получателю. К этому моменту исходный фрагмент данных «обрастает» заголовками и трейлерами всех уровней.

На физическом уровне к исходным данным не добавляется ничего. Это связано с тем, что компьютер-отправитель и компьютер-получатель взаимодействуют на этом уровне непосредственно.

На принимающей стороне все происходит в обратном порядке по мере передачи данных от физического уровня к прикладному. На канальном уровне посредством соответствующего протокола анализируется корректность передачи пакета канального уровня, а также выполняются действия на основе информации, содержащейся в его заголовке. После этого заголовок и трейлер канального уровня отбрасываются, пакет сетевого уровня передается выше – на сетевой уровень модели OSI. Аналогичные действия выполняются и на остальных уровнях – с сетевого по прикладной. В результате отбрасывания заголовка и трейлера на прикладном уровне на компьютере-получателе будет «извлечен» исходный фрагмент данных.

¹ Здесь мы будем использовать термин «пакет» вне зависимости от уровня.

² В литературе по КС обычно говорят про этот процесс, что пакет прикладного уровня *инкапсулируется* (вкладывается) в пакет представительского уровня.

На рис. 1.19 показан процесс формирования пакетов различных уровней на компьютере-отправителе и их разборка на компьютере-получателе в соответствии с моделью OSI (32–7 и T2–7 – заголовки и трейлеры уровней модели OSI с соответствующим номером).

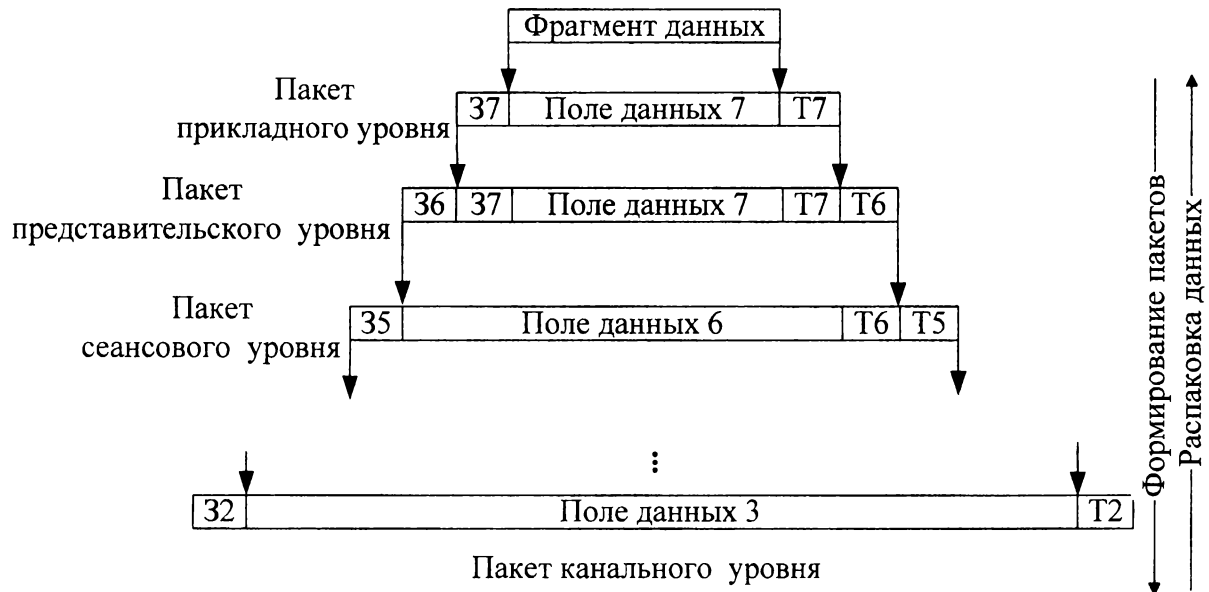


Рис. 1.19. Формирование и разборка пакетов на различных уровнях модели OSI

Резюме

1. В компьютерных сетях используются два способа передачи данных: потоковый и пакетный. На сегодняшний день пакетная передача данных является наиболее популярной.
2. В КС идеологической основой стандартизации является многоуровневый подход к разработке средств сетевого взаимодействия.
3. Сетевые модели помогают описать и понять процесс сетевой коммуникации. Наиболее известной общепринятой сетевой моделью является OSI. Модель OSI – широко распространенный метод описания работы сетевых компонентов, особенностей их взаимодействия при осуществлении передачи данных по КС. Производители твердо придерживаются ее при проектировании сетевых продуктов.
4. Компоненты КС стандартизируются и специфицируются не только сетевыми моделями. Для подобных целей используют спецификации и стандарты сетевого оборудования и программного обеспечения.
5. В модели OSI сетевые функции распределены между семью уровнями: прикладным, представительским, сеансовым, транспортным, сетевым, канальным и физическим. Каждый уровень реализует определенный

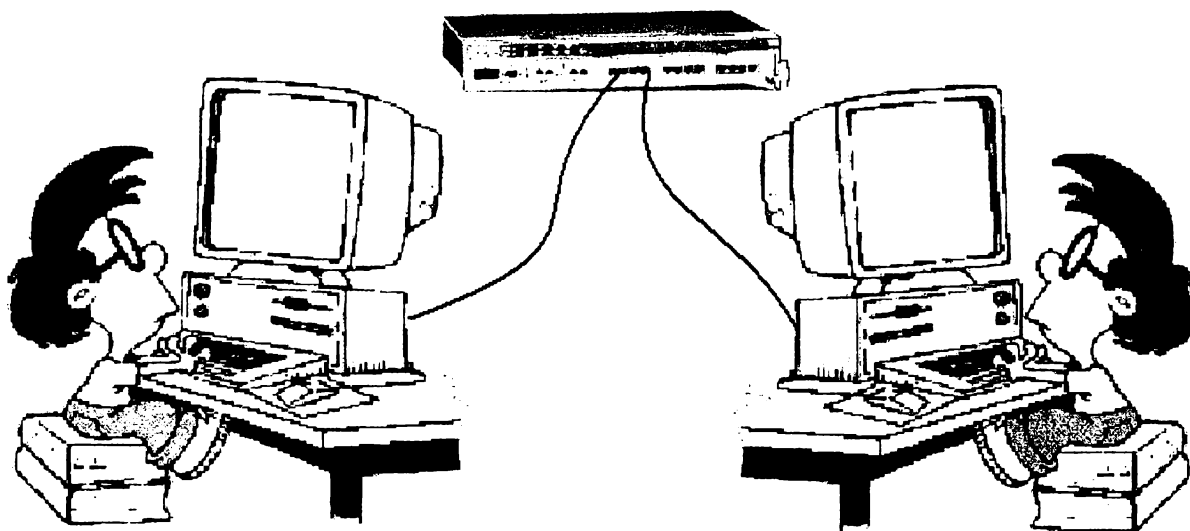
набор функций, обеспечивая один из семи этапов обмена данными, передаваемыми по КС. Чем выше уровень, тем более сложную задачу он решает.

6. Сетевые компоненты, реализующие функции одного и того же уровня, но в разных узлах КС, взаимодействуют посредством протоколов.
7. Для организации взаимодействия уровней в пределах одного узла КС используются интерфейсы.
8. Пакеты с данными формируются и разбираются в соответствии с моделью OSI.

Вопросы для контроля

- 1) В чем состоит преимущество пакетного способа передачи данных по сравнению с потоковым?
- 2) Какова структура пакета, передаваемого по компьютерной сети? Каково содержание каждого из его компонентов?
- 3) Для чего разрабатываются модели компьютерных сетей?
- 4) Каково назначение спецификаций и стандартов?
- 5) В чем заключается различие между спецификациями и стандартами?
- 6) Какие системы называют открытыми?
- 7) В чем заключается многоуровневый подход при построении модели КС?
- 8) Какие организации, занимающиеся разработкой спецификаций и стандартов в области компьютерных сетей, Вам известны?
- 9) Что называется протоколом, интерфейсом в модели OSI?
- 10) Что понимают под стеком протоколов?
- 11) Каковы основные функции каждого из уровней модели OSI?
- 12) В чем особенности взаимодействия соседних уровней одного узла?
- 13) В чем особенности взаимодействия одинаковых уровней разных узлов?
- 14) Каков порядок формирования пакетов на компьютере-отправителе и разборки пакетов на компьютере-получателе?
- 15) Каковы особенности формирования пакетов на физическом уровне модели OSI?
- 16) В чем состоят сходство и отличие понятий «сообщение», «пакет», «кадр»?

Раздел 2
Построение ЛКС
на основе стандартных технологий



2.1. Модель IEEE 802.x

2.1.1. Общая характеристика

В 1980 г. в Институте инженеров по электронике (Institute of Electrical and Electronics Engineers – IEEE) был организован Комитет 802 по стандартизации ЛКС. Результатом работы данного комитета явилось принятие набора стандартов IEEE 802.x (802.1, 802.2,..., 802.12), которые содержат рекомендации по проектированию ЛКС.

Стандарты IEEE 802.x охватывают только физический и канальный уровни модели OSI. Это связано с тем, что эти уровни в наибольшей степени отражают специфику ЛКС. Остальные уровни в значительной степени имеют общие черты как для локальных, так для корпоративных и глобальных сетей.

☞ *Стандарты IEEE 802.x определяют способы, в соответствии с которыми сетевые адаптеры осуществляют доступ к физической среде и передают по ней данные.*

Специфика ЛКС нашла свое отражение в разделении функций **канального уровня** модели OSI между уровнем управления логической связью и уровнем управления доступом к среде (рис. 2.1).

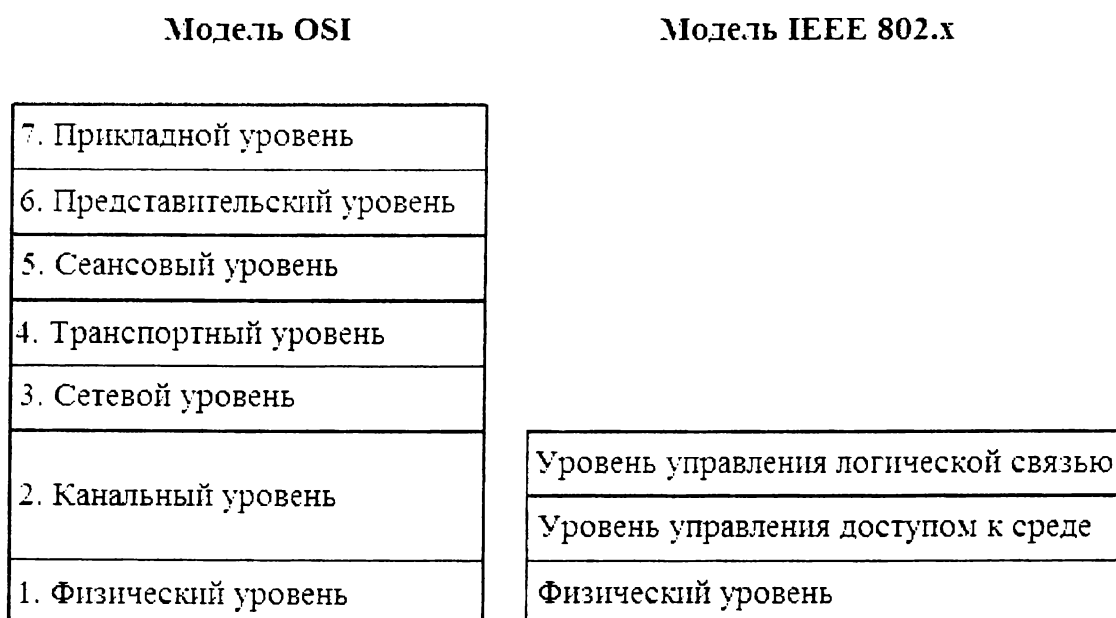


Рис. 2.1. Связь модели OSI с моделью IEEE 802.x

Уровень управления логической связью (Logical Link Control – LLC). Отвечает за передачу пакетов данных между компьютерами с различной степенью надежности, а также реализует функции интерфейса с

прилежащим к нему сетевым уровнем. На уровне LLC существует несколько режимов работы, отличающихся наличием или отсутствием процедур восстановления пакетов в случае их потери или искажения.

Уровень управления доступом к среде (Media Access Control – MAC). Обеспечивает доступ плат сетевого адаптера к физической среде передачи данных. Этот уровень появился из-за существования в ЛКС разделяемой среды передачи данных. Он обеспечивает корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение того или иного компьютера в сети. Кроме этого, он обеспечивает интерфейс с физическим уровнем модели OSI.

☞ *Уровни MAC и LLC взаимно независимы – каждый протокол уровня MAC может применяться с любым протоколом уровня LLC, и наоборот.*

2.1.2. Стандарты IEEE 802.x

Структура стандартов IEEE 802.x приведена в табл. 2.1. Ниже дана краткая характеристика стандартов, разработанных различными подкомитетами IEEE 802:

- 802.1 – описывают особенности работы, общие для всех технологий ЛКС, связь модели OSI с тремя уровнями модели IEEE 802, а также особенности построения более сложных сетей на основе базовых физических топологий;
- 802.2 – описывают протоколы уровня LLC;
- 802.3, 802.4, 802.5, 802.12 – описывают MAC и физический уровень для технологий ЛКС, использующих кабельные линии связи;
- 802.11 – описывают MAC и физический уровень для технологий ЛКС, использующих беспроводные линии связи;
- 802.6 – описывают сети мегаполисов (крупных городов);
- 802.7 – техническая консультационная группа стандартов по широкополосной передаче;
- 802.8 – техническая консультационная группа стандартов по волоконно-оптическим сетям;
- 802.9 – описывают технологии компьютерных сетей передачи голоса и данных;
- 802.10 – описывают протоколы сетевой безопасности.

Легко заметить, что технологии ЛКС, использующие кабельные линии связи, отличаются друг от друга только на MAC и физическом уровнях. На

уровне LLC различий между ними нет. Между технологиями ЛКС, использующими кабельные и беспроводные линии, связи различия существуют на всех уровнях модели IEEE 802.x.

Таблица 2.1

Структура стандартов IEEE 802.x

802.1 (общие определения ЛКС, связь модели IEEE 802 с моделью OSI, построение более сложных сетей на основе базовых топологий)						
Канальный уровень	LLC	802.2 (передача пакетов данных между узлами локальной сети, интерфейс с сетевым уровнем модели OSI)				
		Синхронный, дейтаграммный, с обнаружением и без коррекции ошибок				
Физический уровень	MAC	802.3 Ethernet (CSMA/CD)	802.4 Token Bus	802.5 Token Ring	802.12 100VG- AnyLAN по приоритету запроса)	802.11 Беспроводные сети (CSMA/CA)
		10Base2 (RG-58); 10Base5 (RG-8); 10BaseT, 100BaseTX, 100BaseTX, 100BaseT4 (UTP); 10BaseFL, FOIRL, 100BaseFX (опто- волокно)	STP 4 Мбит/с, STP 16 Мбит/с, UTP		100VG- AnyLAN (UTP)	802.11 (инфракрасное излучение, лазер, радиоволны) 802.11a, 802.11b (радиоволны)

2.1.3. Bluetooth

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами темы «Bluetooth» раздела «Типы беспроводных сетей» электронного пособия «Беспроводные компьютерные сети».

☞ *Bluetooth – это внедренное в микрочип невыключающееся радиопристройство ближнего действия.*

Технология Bluetooth была представлена шведским производителем мобильных средств связи Ericson в 1994 г. как средство, позволяющее портативным компьютерам совершать звонки по мобильным телефонам. С тех пор несколько тысяч компаний работают над тем, чтобы технология Bluetooth стала стандартом множества маломощных, действующих на близком расстоянии беспроводных устройств.

Bluetooth описывается стандартом IEEE 802.15.1. Эта технология обеспечивает построение так называемых персональных беспроводных сетей (Wireless Personal Area Network – WPAN). В КС Bluetooth предусматривает поддержку следующих основных областей применения:

- 1) точки доступа для ввода данных (в том числе посредством голоса);
- 2) альтернатива соединительным кабелям;
- 3) организация эпизодических сетей.

2.1.4. Уровень управления логической связью

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами тем «Синхронная передача сигналов», «Асинхронная передача сигналов» раздела «Канальный уровень модели OSI» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».

По наиболее существенным свойствам протоколы данного подуровня делятся на следующие виды:

- асинхронный/синхронный;
- с предварительным установлением соединения/дейтаграммный;
- с обнаружением искаженных данных/без обнаружения;
- с обнаружением потерянных данных/без обнаружения;
- с восстановлением искаженных и потерянных данных/без восстановления.

Для передачи данных по линиям связи может быть выбран асинхронный или синхронный способ.

При *асинхронной передаче* информация посылается посимвольно с произвольными интервалами времени. Каждый передаваемый символ содержит некоторое число бит данных, которые предваряются стартовым битом и завершаются одним, полуторами или двумя стоповыми битами (рис. 2.2, а).

В этом методе для синхронизации используется стартовый бит, расположенный в начале каждого символа. Когда стартовый бит попадает в принимающее устройство, оно в этот момент синхронизирует свои внутренние часы с часами передающего устройства.

При *синхронной передаче* все обмены данными осуществляются пакетами, структура которых была рассмотрена ранее (см. рис. 1.10). Каждый пакет предваряется байтами синхронизации (рис. 2.2, б). Байт синхронизации – это байт, содержащий заранее известный код, например 0111110, который оповещает о приходе пакета данных. При его получении приемник должен установить байтовую синхронность с передатчиком, т.е. правильно понимать начало очередного байта пакета. Все биты пакета передаются непрерывным потоком, что значительно ускоряет передачу данных.

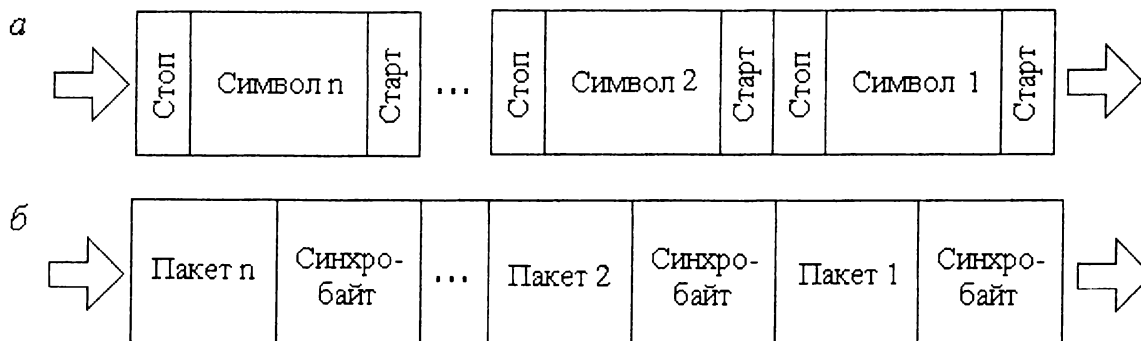


Рис. 2.2. Передача на уровне байт:
а – асинхронная; б – синхронная

На уровне LLC платы сетевых адаптеров «договариваются» между собой, каким из двух способов – синхронными или асинхронным – они будут передавать данные. Передача данных между двумя компьютерами возможна только в том случае, если их сетевые платы поддерживают один и тот же способ. В противном случае установить связь будет невозможно.

Все современные ЛКС поддерживают только синхронный способ передачи данных; в глобальных и городских сетях есть целый ряд технологий, базирующихся на асинхронном способе.

При *дейтаграммной передаче* (без установления соединения) пакет посылается в сеть «без предупреждения», и никакой ответственности за его утерю протокол не несет. Предполагается, что сеть всегда готова принять пакет от конечного узла. Дейтаграммный метод работает быстро, так как никаких предварительных действий перед отправкой данных не выполняется. Однако при таком методе трудно организовать отслеживание факта доставки пакета узлу назначения. Этот метод не гарантирует его доставку. Такой метод передачи данных используется, например, в сетях Ethernet, о которых пойдет речь в следующих главах.

Передача с установлением соединения более надежна, но требует больше времени для передачи данных. В этом случае узлу-получателю отправляется служебный пакет с предложением установить соединение. Если узел-получатель согласен с этим, он посылает в ответ другой служебный пакет, подтверждающий установление соединения и предлагающий некоторые параметры связи. После того как узел-отправитель перешлет узлу-получателю еще один служебный пакет с подтверждением приема параметров, соединение считается установленным. Теперь можно передавать пакеты, содержащие пользовательские данные. После передачи некоторого законченного набора данных, например определенного файла, узел-отправитель инициирует разрыв данного логического соединения, посылая соответствующий служебный пакет.

Протокол передачи данных с установлением соединения используется в беспроводных локальных сетях (БЛКС).

В обязанности уровня LLC входят обнаружение ошибок передачи данных, связанных с искажением бит в принятом пакете данных или с потерей пакета, и, по возможности, их корректировка.

Протоколы с обнаружением ошибок без их коррекции используют в сетях, в которых искажения и потери пакетов являются очень редким событием, например кабельными ЛКС.

Если в сети искажения и потери пакетов случаются часто, то желательно уже на уровне LLC использовать протокол с коррекцией ошибок. Примером сетей, использующих протоколы с коррекцией ошибок, могут служить беспроводные ЛКС.

2.1.5. Уровень управления доступом к среде

Механизм, называемый доступом к среде передачи данных, реализуется на MAC-уровне модели IEEE 802.x. Хотя теоретически механизм доступа к среде должен быть универсальным, на практике

различают несколько способов его реализации. Приведем примеры популярных протоколов MAC-уровня, которые используются в ЛКС:

- множественный доступ с контролем несущей и обнаружением коллизий (Carrier Sense-Multiply Access with Collision Detection – CSMA/CD), использующийся в сетях Ethernet;
- множественный доступ с контролем несущей и предотвращением коллизий (Carrier Sense Multiple Access with Collision Avoidance – CSMA/CA), использующийся в беспроводных компьютерных сетях;
- доступ с передачей маркера (Token Ring);
- доступ по приоритету запроса (используется в сетях 100VG-AnyLAN).

Резюме

1. Модель IEEE 802.x описывает правила построения ЛКС.
2. Стандарты IEEE 802.x определяют способы, в соответствии с которыми сетевые адаптеры осуществляют доступ к физической среде и передают по ней данные.
3. Большую популярность сегодня приобретает технология Bluetooth, позволяющая объединить в компьютерную сеть множество маломощных, действующих на близком расстоянии беспроводных устройств.

Вопросы для контроля

- 1) Что такое IEEE 802.x и какова его роль?
- 2) Каким уровням модели OSI соответствует модель IEEE 802.x?
- 3) Какие стандарты IEEE 802.x Вам известны? Дайте каждому из них краткую характеристику.
- 4) Каковы функции уровня LLC? MAC? Каковы наиболее существенные свойства протоколов этих уровней?
- 5) Почему протоколы уровня LLC, использующиеся в беспроводных ЛКС, как правило, не используются в кабельных ЛКС, и наоборот?
- 6) Какие основные характеристики протоколов уровня LLC, применяемые в кабельных и беспроводных компьютерных сетях, Вам известны?
- 7) Каковы основные области применения технологии Bluetooth?

2.2. Построение ЛКС на физическом уровне

2.2.1. Построение кабельных ЛКС

В рамках физического уровня модели IEEE 802.x определяются особенности расположения, состав и основные характеристики физических компонентов ЛКС. Для каждой из технологий предлагаются решения, гарантирующие работоспособность ЛКС, построенной в соответствии со стандартами.

Далее будут рассмотрены правила построения кабельных ЛКС (КЛКС), распространенных сегодня в России: 10Base2, 10BaseT и 100BaseTX. При описании расположения основного сетевого оборудования мы будем использовать понятие «физическая топология», которое было введено в п. 1.1.

10Base2 и 10BaseT относятся к технологиям, позволяющим компьютерам обмениваться данными со скоростью 10 Мбит/с (число 10 в названии технологии обозначает именно этот факт). Эти сети носят обобщенное название «*Ethernet*».

100BaseTX – это одна из технологий, позволяющих компьютерам обмениваться данными со скоростью 100 Мбит/с. Она носит обобщенное название «*Fast Ethernet*».

Во всех перечисленных КЛКС передаются *немодулированные сигналы* (слово «Base» обозначает именно этот факт) и используется *потенциальное кодирование* данных.

Технология 10Base2

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами тем «Шина» раздела «Топологии» и «Технология 10Base2» раздела «Технологии локальных сетей» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».

Физическая топология. Технология 10Base2 описывает построение ЛКС, имеющей ФТ «шина». Для подключения компьютеров к сети используется тонкий коаксиальный кабель, именуемый магистралью (рис. 2.3). Этот тип ФТ считается наиболее простым и до недавнего времени был весьма распространен.

В ФТ «шина» сигналы, передаваемые одним компьютером, распространяются по всей сети. В один временной интервал может

передавать данные только один компьютер, в связи с чем скорость передачи данных существенно зависит от количества компьютеров, подключенных к магистрали.

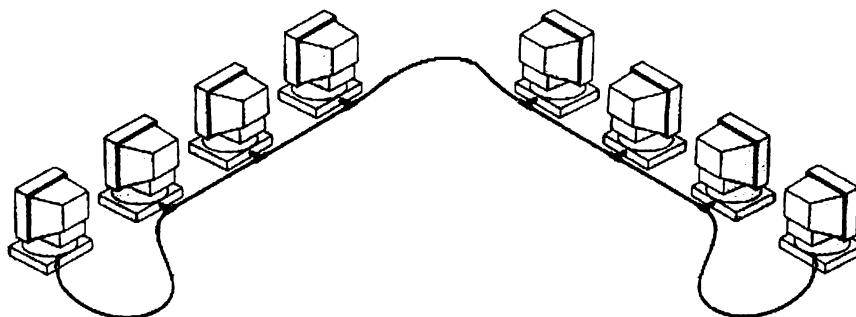


Рис. 2.3. Компьютерная сеть 10Base2

Отметим, что прямой зависимости между скоростью передачи данных по сети с ФТ «шина» и количеством компьютеров в ней нет. На быстродействие КС оказывают влияние также и другие факторы, например тип аппаратного обеспечения сетевых компьютеров, тип работающих сетевых приложений и др.

Достоинствами компьютерных сетей с ФТ «шина» являются простота расширения сети (для добавления компьютера достаточно его подключить к магистрали) и экономичность (для соединения всех компьютеров требуется небольшое количество кабеля).

Главный недостаток ФТ «шина» состоит в том, что если происходит разрыв кабеля (или один из пользователей вынимает разъем из гнезда сетевой платы), то вся сеть прекращает функционировать. При этом место сбоя очень часто трудно обнаружить без специального оборудования.

Отметим, что в случае простого отключения компьютера работоспособность сети не нарушается.

Тонкий коаксиальный кабель. Самый простой коаксиальный кабель состоит из центральной жилы (обычно медной), которая окружена диэлектрическим изоляционным слоем, отделяющим ее от металлической оплетки. Электрические сигналы, кодирующие данные, передаются по жиле.

Оплетка защищает жилу от электрических шумов и перекрестных помех. Снаружи кабель покрыт непроводящим слоем – резиной, тефлоном или пластиком (рис. 2.4). Пример кабеля RG-58 был приведен на рис.1.5, в.

Коаксиальный кабель малочувствителен к внешним помехам. Он гибок, прост в установке и относительно недорог. При построении

компьютерных сетей используют коаксиальный кабель только с сопротивлением 50 Ом.

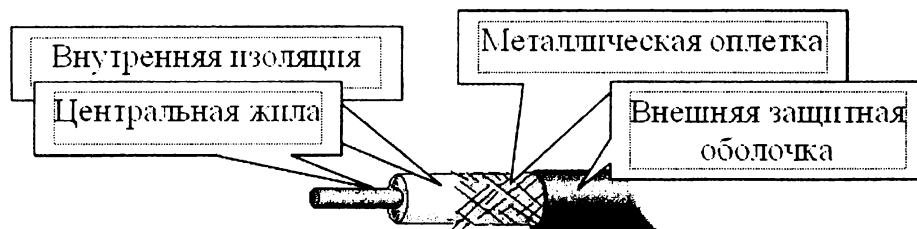


Рис. 2.4. Строение коаксиального кабеля

Главный недостаток коаксиальных кабелей – ограниченная пропускная способность; так, в ЛКС «потолок» составляет 10 Мбит/с.

Производители кабелей создали специальную маркировку для различных типов кабелей. Тонкий коаксиальный кабель относится к группе, которая называется семейством RG-58.

Подключение компьютеров в сети 10Base2. Для подключения компьютеров в сеть по технологии 10Base2 на каждом из них необходимо установить сетевой адаптер с разъемом BNC (рис. 2.5, а). Для подключения кабеля RG-58 к сетевым адаптерам используются BNC-коннекторы, BNC-T-коннекторы, BNC-терминаторы (рис. 2.5, б–д). Также как и кабель RG-58, они должны иметь волновое сопротивление 50 Ом.

Схемы подключения тонкого коаксиального кабеля к сетевым адаптерам внутри сегмента и по его краям различаются. Технология 10Base2 описывает три схемы, изображенные на рис. 2.6.

Для подключения компьютеров внутри сегмента кабеля RG-58 используются два BNC-коннектора и один BNC-T-коннектор.

На концах каждого из сегментов кабеля RG-58 должны быть установлены BNC-терминаторы. На одном конце сегмента устанавливается BNC-терминатор без заземления, на втором – с заземлением.

Наличие терминаторов обязательно. В случае отсутствия хотя бы одного из них возникает отражение сигнала, вследствие чего вся сеть выходит из строя.

Такая же ситуация характерна и при разрыве кабеля в любом из сегментов кабельной системы КС (сеть разрывается на два фрагмента, на одном конце каждого из них отсутствует терминатор).

Для того чтобы каждый компьютер в сети 10Base2 мог корректно распознать коллизию, вводятся следующие ограничения, которые учитываются при проектировании:

- длина сегмента кабеля RG-58 не должна превышать 185м;
- минимальная длина кабеля RG-58 между двумя компьютерами составляет 1м;
- к одному сегменту кабеля RG-58 можно подключить не более 30 компьютеров.

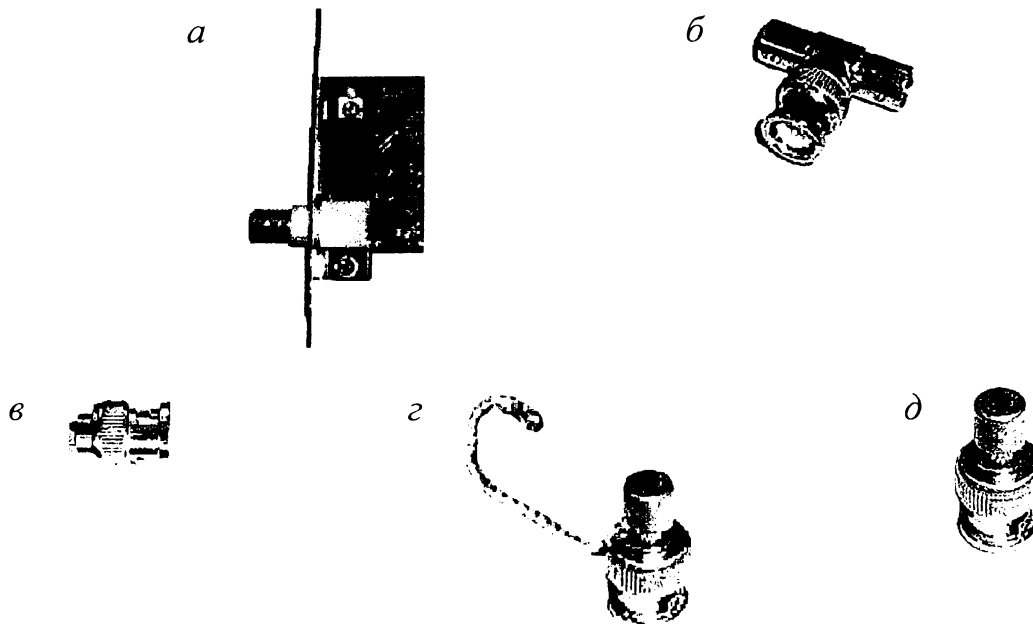


Рис. 2.5. Аксессуары для подключения сетевого оборудования в 10Base2:
а – сетевой адаптер с разъемом BNC; б – BNC-T-коннектор;
в – BNC-коннектор; г – BNC-терминатор с заземлением;
д – BNC-терминатор без заземления

Использование повторителей. Для того чтобы преодолеть ограничение в общую длину сегмента КС, составляющее 185м, в сетях 10Base2 используются повторители.

Для того чтобы все узлы компьютерной сети 10Base2 корректно распознавали сигнал коллизии, количество повторителей, которые используются для увеличения общей длины сети, не должно превышать четырех. Соответственно, общее количество сегментов может быть не более пяти, каждый из которых не более 185 м. Кроме этого, технология 10Base2 разрешает подключать компьютеры только к трем сегментам из пяти. Схема и правила подключения компьютеров внутри сегментов были рассмотрены ранее.

Данные ограничения получили особое название – «правило 3–4–5». Пример сети 10Base2, для которой оно выполняется, приведен на рис. 2.7.

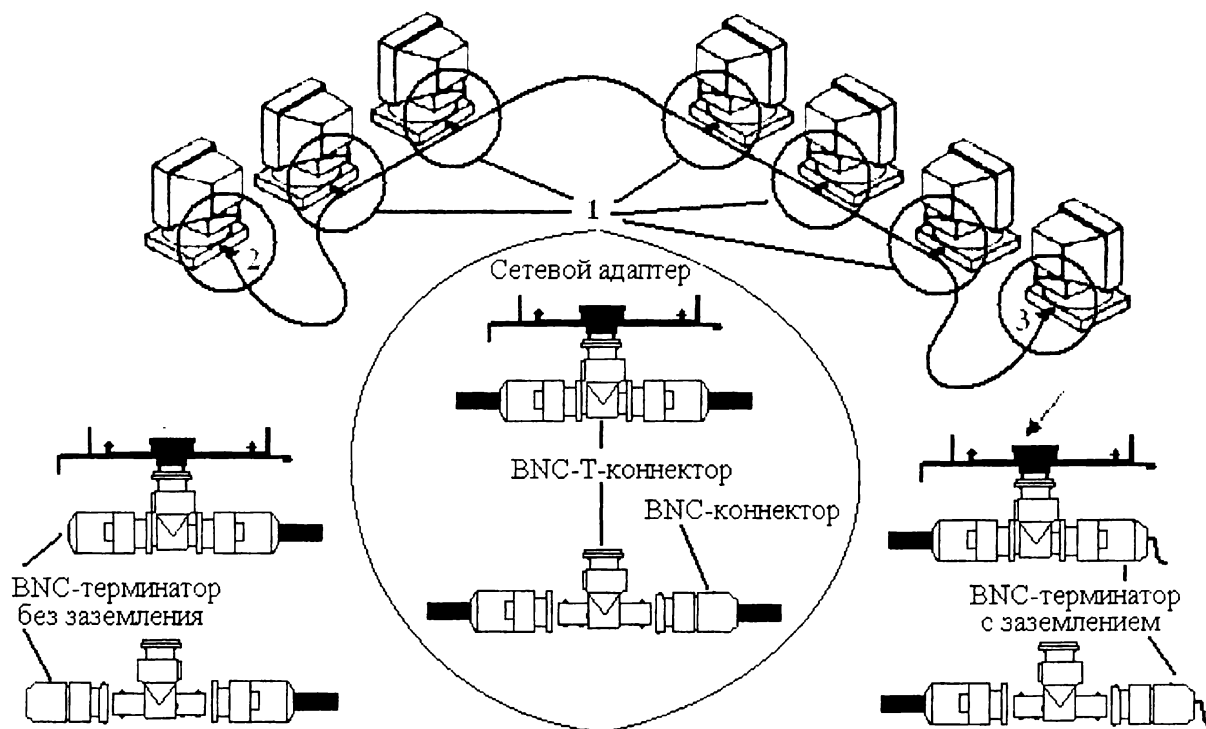


Рис. 2.6. Схемы подключения кабеля RG-58 к сетевым адаптерам

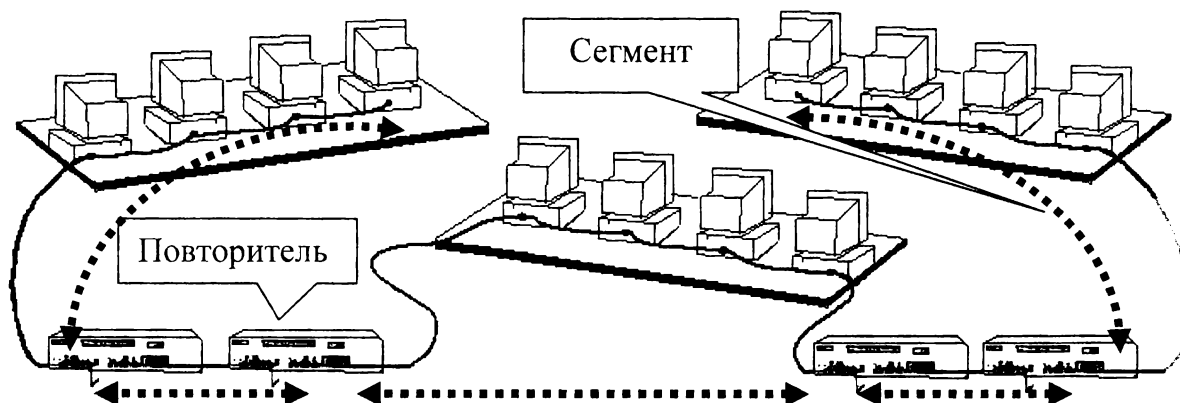


Рис. 2.7. Подключение компьютеров в сети 10Base2 по «правилу 3–4–5»

Технология 10BaseT

После изучения материалов данной темы рекомендуем познакомиться с демонстрационными материалами тем «Звезда», «Точка – точка», «Звезда – шина» раздела «Топологии» и «Технология 10BaseT», «10Base2/10BaseT» раздела «Технологии локальных сетей» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».

Физические топологии. Сети 10BaseT базируются на использовании одной из самых популярных ФТ компьютерных сетей – «звезда». В ней все

компьютеры с помощью сегментов кабеля подключаются к центральному компоненту – концентратору. Этот концентратор носит особое название – «hub». Сигналы, полученные от любого из компьютеров в сети, повторяются через hub сразу всем другим компьютерам, которые подключены к его портам. Схема подключения компьютеров в сети 10BaseT с ФТ «звезда» представлена на рис. 2.8.

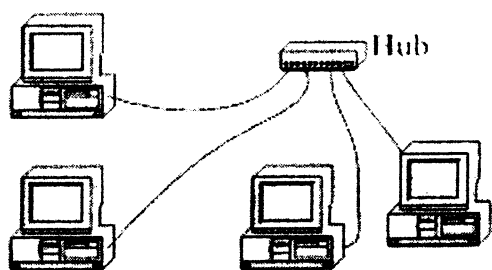


Рис. 2.8. Сеть 10BaseT с физической топологией «звезда»

Централизованное подключение компьютеров к сети позволяет избежать «падения» всей сети при отключении одного из компьютеров или повреждении сегмента кабеля. В этом случае будет нарушена связь только с одним компьютером (который отключен или который подключается к концентратору нерабочим сегментом кабеля).

Несмотря на то что ФТ «звезда» весьма устойчива к сбоям в сети, она имеет ряд недостатков. Так, при выходе из строя концентратора вся сеть становится неработоспособной. Еще один недостаток связан с тем, что количество портов у концентратора, к которым можно подключить компьютеры, ограничено. В связи с этим необходимо еще до развертывания КС учитывать перспективы ее дальнейшего развития. Концентратор должен иметь достаточное количество портов для подключения всех компьютеров в сети, а также некоторое (заранее подсчитанное) количество свободных портов, зарезервированных на случай расширения сети.

Кроме этого, при развертывании сети, имеющей ФТ «звезда», тратится большое количество кабеля.

При построении КС 10BaseT очень часто используется комбинированная топология «звезда – шина», которая сочетает отдельные свойства простых ФТ «звезда» и «шина».

Обычно схема выглядит так: несколько сетей с физической топологией «звезда» на основе hub объединяются при помощи магистральной шины (коаксиального кабеля и/или кабеля UTP). Компьютеры подключаются к концентраторам, образуя «звезды». Сигналы, полученные от любого из компьютеров в сети, повторяются через концентраторы всем другим компьютерам (рис. 2.9).

ФТ «звезда – шина» обладает целым рядом достоинств. Так, при обрыве кабеля между компьютером и концентратором, выходе из строя компьютера работоспособность компьютерной сети не нарушается. Все остальные компьютеры продолжают обмениваться данными.

При выходе из строя концентратора прекращает работать только одна «звезда», в которой он является центральным компонентом.

При обрыве кабеля между hub «звезда – шина» разбивается на работоспособные КС меньших размеров (с ФТ «звезда» и/или «звезда – шина»).

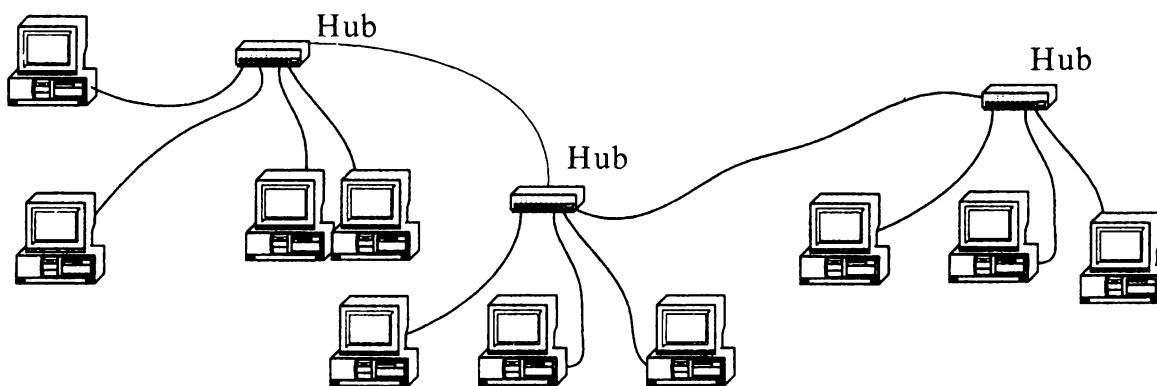


Рис. 2.9. Сеть 10BaseT с физической топологией «звезда – шина»

Кроме подключения компьютеров к КС по ФТ «звезда» и «звезда – шина» технология 10BaseT позволяет осуществлять прямые подключения компьютеров друг к другу.

☞ *Соединение, при котором два компьютера подключаются друг к другу отдельной линией связи, называется соединением типа «точка – точка».*

Подключения данного типа занимают особое место в компьютерных сетях. Это обусловлено тем, что линия связи напрямую соединяет сетевые платы, установленные на компьютерах.

В связи с этим для каждого из точечных соединений требуются две сетевые платы. Легко подсчитать, что для соединения компьютера с двумя другими на нем потребуется установить две сетевые платы, с тремя – три и т.д.

Неэкранированная витая пара. При построении сетей 10BaseT используется кабель «неэкранированная витая пара (UTP)». Витая пара состоит из двух изолированных медных проводов. В настоящее время разработаны стандарты, определяющие шесть категорий кабеля UTP. В сетях 10BaseT из них используются только два:

- **Категория 3:** кабель, способный передавать данные со скоростью до 16 Мбит/с. Предназначен как для передачи данных, так и для передачи голоса. Состоит из четырех витых пар.
- **Категория 5:** кабель специально разработан для поддержки высокоскоростных компьютерных сетей. Способен передавать данные со скоростью 10 Мбит/с – 1 Гбит/с. Волновое сопротивление кабеля этой категории равно 100 Ом. Он состоит из четырех витых пар.

Структура кабелей UTP категорий 3 и 5 представлена на рис. 2.10, пример приведен на рис. 1.5, а.

Одна из потенциальных проблем для любых типов электрических кабелей – перекрестные помехи. Незэкранированная витая пара особенно страдает от таких электрических наводок.

Подключение компьютеров к сети.

Для подключения компьютеров к сети 10BaseT на каждом из них устанавливается сетевая плата 10BaseT, имеющая разъем RJ-45 для подключения кабеля UTP. Для подключения кабелем компьютеров к концентратору или напрямую друг к другу используются коннекторы RJ-45. В качестве центрального компонента выступает концентратор 10BaseT, имеющий порты RJ-45 для подключения компьютеров (рис. 2.11).

Точно так же, как и в сетях 10Base2, вводятся некоторые ограничения:

- максимальная длина сегмента кабеля – 100м;
- общая длина всех сегментов кабеля не более 2500м;
- максимальное количество узлов в сети – 1024.

☞ *Технология 10BaseT основана на использовании незэкранированной витой пары UTP категории 3 или 5 (преимущественно категории 5).*

Для сетей 10BaseT также действует «правило 3–4–5», но в связи с особенностями подключения компьютеров оно содержит иные требования, чем для сетей 10Base2. Так, в сети, построенной по технологии 10BaseT, должны выполняться следующие условия:

- 1) в сети можно использовать не более четырех центральных компонентов – концентраторов и повторителей;

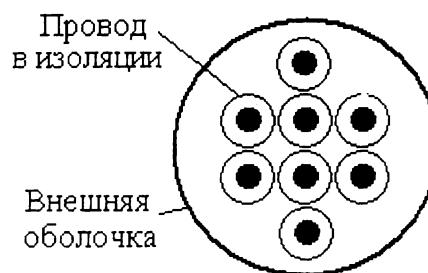


Рис. 2.10. Структура кабеля UTP категорий 3 и 5

- 2) компьютеры можно присоединять только к трем из четырех центральных компонентов компьютерной сети;
- 3) между двумя любыми компьютерами должно быть не более пяти сегментов кабеля.

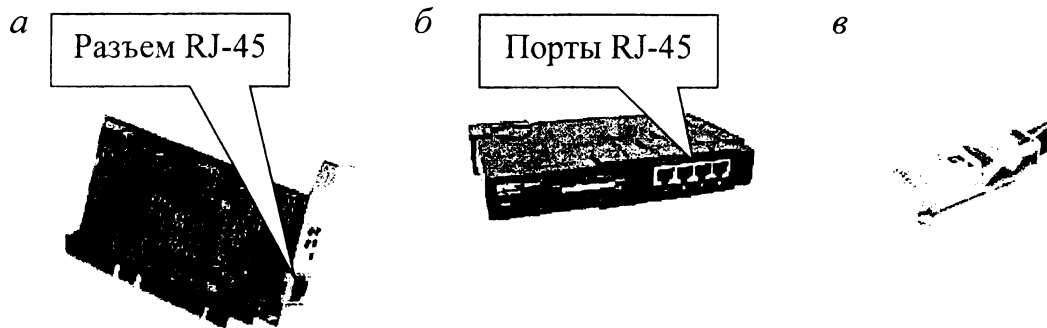


Рис. 2.11. Оборудование для подключения компьютеров в сети 10BaseT:

а – сетевой адаптер; б – концентратор 10BaseT; в – коннектор RJ-45.

Пример сети 10BaseT, для которой выполняется «правило 3–4–5», приведен на рис. 2.12.

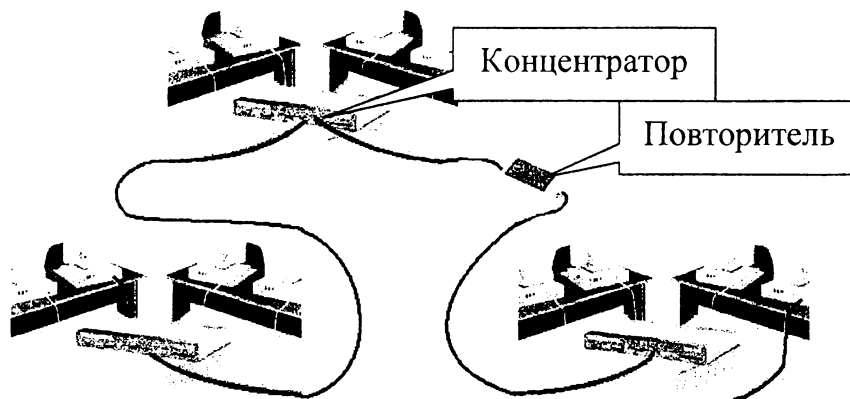


Рис. 2.12. Подключение компьютеров в сети 10BaseT по «правилу 3–4–5»

■ После изучения тем «Технология 10Base2» и «Технология 10BaseT» Вы можете перейти к выполнению лабораторной работы 1 «Ethernet 10 Мбит/с», лабораторной работы 2 «Подключение сетевых устройств кабелем UTP» лабораторного практикума «Локальные компьютерные сети».

Технология 100BaseTX

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами тем «Технология 100BaseTX», «10BaseT/100BaseTX» раздела «Технологии локальных сетей» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».

Физические топологии. Стандартные технологии Fast Ethernet допускают использование при построении КС двух типов концентраторов – класса I и класса II.

Концентраторы Fast Ethernet класса I поддерживают все или несколько спецификаций Fast Ethernet и могут иметь порты трех типов физического уровня: 100BaseTX, 100BaseFX и 100BaseT4.

Концентраторы Fast Ethernet класса II поддерживают только какую-то одну спецификацию: либо 100BaseTX, либо 100BaseFX, либо 100BaseT4.

Примеры концентраторов Fast Ethernet класса I и класса II приведены на рис. 2.13.

Если в сети используется концентратор класса I, то компьютеры могут быть подключены только по ФТ «звезда». В случае использования концентратора класса II могут быть реализована ФТ «звезда» или «звезда – шина».

Помимо этого допускается подключение компьютеров по типу «точка – точка».

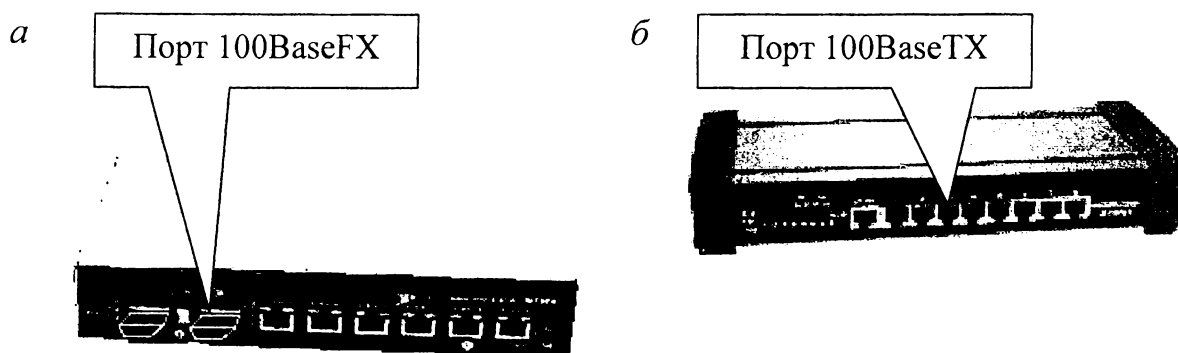


Рис. 2.13. Концентраторы Fast Ethernet:

а – класса I; б – класса II

Подключение компьютеров к сети. Для подключения компьютеров к сети используется кабель UTP пятой категории, структура которого рассматривалась выше. При этом на каждом из концов кабеля должны

быть установлены, как и по технологии 10BaseT, коннекторы RJ-45 (см. рис. 2.11, в).

Примеры концентраторов, которые используются для подключения компьютеров, приведены на рис. 2.13. Для подключения кабеля UTP они должны иметь порты RJ-45 и стандартную маркировку «100BaseTX» или «10/100Ethernet».

При подключении компьютеров должны учитываться ограничения:

- длина кабельного сегмента не более 100 м;
- в случае использования концентраторов класса II расстояние сегмента кабеля между ними не должно превышать 5 м;
- общая длина всех кабельных сегментов не более 205 м.

Совместное использование технологий 10BaseT и 100BaseTX. Для безболезненного и постепенного перехода организаций от технологии 10BaseT, основанной на использовании UTP пятой категории, к технологии 100BaseTX были разработаны концентраторы и сетевые платы, поддерживающие оба этих стандарта. В маркировке таких сетевых устройств указывается «10/100», например «10BaseT/100BaseTX» или «10/100 Ethernet».

Всего в настоящее время определено четыре различных режимов работы, которые могут поддерживать такие устройства:

- 10BaseT – полудуплексная передача данных по двум витым парам кабеля UTP категории 3;
- 10BaseT full duplex – дуплексная передача данных по двум витым парам кабеля UTP категории 3;
- 100BaseTX – полудуплексная передача данных по двум витым парам кабеля UTP категории 5;
- 100BaseTX full duplex – дуплексная передача данных по кабелю UTP категории 5.

Это позволяет сетевым устройствам договариваться о том, на какой скорости они будут передавать данные по сети. Процесс выбора скорости передачи данных реализуется через *автопереговоры*.

Переговорный процесс происходит при включении питания устройства, а также может быть инициирован в любой момент модулем управления устройством. Режим 10BaseT имеет самый низкий приоритет в переговорном процессе, а режим 100BaseTX full duplex – самый высокий.

Устройство, начавшее процесс автопереговоров, посылает своему партнеру сообщение, в котором предлагает самый приоритетный, поддерживаемый данным узлом, режим взаимодействия.

Если узел-партнер поддерживает функцию автопереговоров и также может поддерживать предложенный режим, он подтверждает выбор предложенного режима работы, и на этом переговоры заканчиваются.

Если же узел-партнер может поддерживать менее приоритетный режим, он указывает его в ответе, и этот режим выбирается в качестве рабочего. Таким образом, всегда выбирается наиболее приоритетный общий для узлов режим.

Узел, который поддерживает только технологию 10BaseT, каждые 16 мс посылает сигналы для проверки целостности линии, связывающей его с соседним узлом. Такой узел не понимает запрос с предложением выбрать режим работы, который делает ему узел с функцией автопереговоров, и продолжает посылать свои сигналы. Узел, получивший в ответ на свой запрос только сигналы проверки целостности линии, понимает, что его партнер может работать только по стандарту 10BaseT, и устанавливает этот режим работы и для себя.

Важно, что дуплексный режим работы может поддерживаться только коммутаторами, о которых пойдет речь в п. 2.4. Концентраторы же могут поддерживать только полудуплексную передачу данных, что объясняется их принципами работы. В связи с этим в дуплексном режиме 100BaseTX компьютеры могут работать, только если одновременно выполняются два условия:

- 1) сетевые адаптеры, установленные на компьютерах, поддерживают режим 100BaseTX full duplex;
- 2) компьютеры подключены к коммутатору, поддерживающему режим 100BaseTX full duplex, или соединены напрямую по типу «точка–точка».

Во всех остальных случаях компьютерная сеть будет работать в менее приоритетном режиме.

☞ *С другими стандартными технологиями построения кабельных ЛКС можно познакомиться, обратившись к материалам электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».*

2.2.2. Построение беспроводных ЛКС

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами разделов «Физические топологии» и «Физический уровень 802.11» электронного пособия «Беспроводные компьютерные сети».

Применение беспроводных ЛКС

Можно выделить три наиболее распространенные области применения беспроводных локальных компьютерных сетей (БЛКС):

- 1) расширение кабельных компьютерных сетей;
- 2) кочевой доступ;
- 3) создание эпизодических сетей.

Можно указать массу ситуаций, в которых БЛКС нашли себя как альтернатива кабельным:

- здания с большими открытыми площадями, типичные для предприятий обрабатывающей промышленности;
- операционные этажи фондовых бирж и склады;
- старые здания с недостаточным объемом проложенных витых пар, в которых запрещено сверление каналов под проводку;
- небольшие офисы, в которых установка и эксплуатация кабельных ЛКС неэкономичны.

Во всех названных случаях БЛКС представляют эффективную и более привлекательную альтернативу. Как правило, в организации наряду с БЛКС существуют кабельная компьютерная сеть для поддержки серверов и нескольких стационарных рабочих станций. Например, на предприятиях офисная территория обычно отделена от заводских этажей, но должна быть с ними связана с целью организации сети. Таким образом, беспроводные и кабельные ЛКС одного здания обычно объединяются. Такая область применения беспроводных сетей называется *расширением кабельных ЛКС*.

Кочевой доступ предполагает беспроводный канал связи между концентратором ЛКС и мобильным информационным терминалом, снабженным антенной, таким как лэптоп или ноутбук. Одним из примеров применения такого соединения является передача сотрудником, вернувшимся из командировки, данных из персонального портативного компьютера на сервер в офисе. Кочевой доступ также полезен в обширной среде,

такой как предприятие, функционирующее за пределами блока зданий. В обоих случаях пользователи со своими портативными компьютерами могут перемещаться и могут связываться с серверами кабельной ЛКС из различных мест.

Эпизодическая сеть – это временная БЛКС, настроенная для срочного удовлетворения потребностей, связанных с передачей данных между компьютерами (рис. 2.14).

Например, сотрудники, каждый из которых обладает лэптопом или карманным компьютером, встречаются в конференц-зале и соединяют свои компьютеры в эпизодическую сеть только на время заседания.

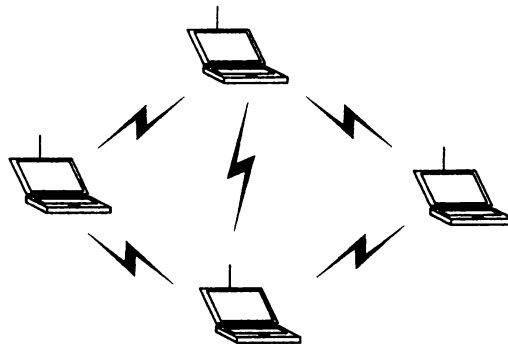


Рис. 2.14. Пример эпизодической сети

Топологии беспроводных ЛКС

Как правило, выделяют три основные топологии БЛКС:

- 1) «точка – точка»;
- 2) «один – ко многим»;
- 3) «многие – ко многим».

В топологии «точка – точка» два узла сети соединяются непосредственно друг с другом. По данной топологии обычно связывают два сегмента кабельных ЛКС по беспроводной линии связи (рис. 2.15).

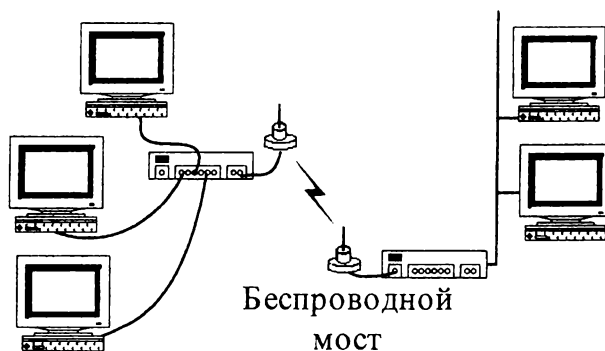


Рис. 2.15. Беспроводная ЛКС с топологией «точка – точка»

Эта топология наиболее применима при соединении двух сегментов сети, разнесенных на значительное расстояние.

В топологии «один – ко многим» один центральный узел обслуживает несколько узлов, выступая в роли транслятора между ними (рис. 2.16).

Хорошим примером использования такой топологии может послужить система сотовой связи. Центральный узел, как правило, оснащается мощной антенной и передатчиком, позволяющим относительно маломощным мобильным узлам работать на достаточном удалении.

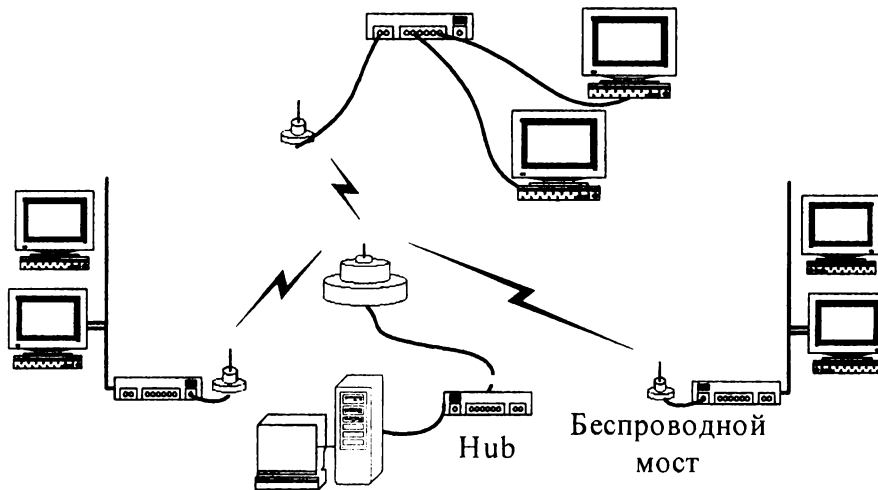


Рис. 2.16. Беспроводная ЛКС с топологией «один – ко многим»¹

В топологии «многие – ко многим» каждый узел сети может одновременно осуществлять обмен данными с несколькими или со всеми другими узлами (рис. 2.17).

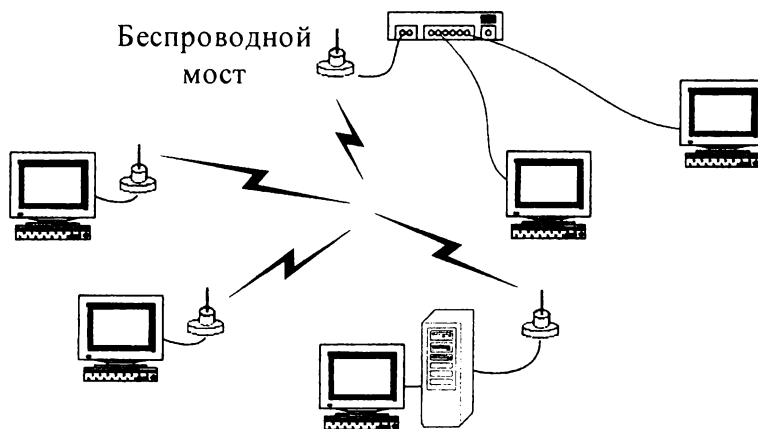


Рис. 2.17. Беспроводная ЛКС с топологией «многие – ко многим»

Радиус действия беспроводной сети в данной топологии обычно весьма невелик – чаще всего рабочие станции располагаются в пределах одного помещения.

¹ Функции мостов рассматриваются далее в этом разделе.

Инфракрасные сети

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами темы «IrDA» раздела «Типы беспроводных сетей» электронного пособия «Беспроводные компьютерные сети».

Инфракрасная передача предполагает несколько существенных преимуществ:

- спектр для такой связи обычно не ограничен, что дает возможность получать высокие скорости передачи;
- для использования инфракрасного излучения не требуется лицензия;
- инфракрасное излучение диффузно отражается от светлоокрашенных объектов (таким образом, можно использовать отражение от потолка).

Инфракрасное излучение не проникает сквозь стены или другие непрозрачные объекты. Это дает два преимущества: во-первых, связь в инфракрасном диапазоне легче защитить от прослушивания, чем связь, основанную на радиочастотной передаче; во-вторых, в каждой комнате здания может существовать своя инфракрасная конфигурация; эти конфигурации не будут интерферировать между собой, что позволяет создавать значительные инфракрасные ЛКС.

Следует также отметить несколько недостатков рассматриваемой среды. Многие устройства, используемые внутри помещений, дают существенное фоновое излучение в инфракрасном диапазоне, что создает «шум» в сети. Значительное влияние оказывают и другие источники, например свет из окна. Все это вынуждает использовать передатчики большой мощности, что обуславливает необходимость учитывать вопросы безопасности для зрения.

Стандарт IEEE 802.11 описывает два альтернативных метода передачи данных в инфракрасном диапазоне:

- 1) рассеянное инфракрасное излучение;
- 2) отраженное инфракрасное излучение.

При использовании *рассеянного инфракрасного излучения* в помещении есть одна базовая станция, находящаяся в пределах прямой видимости остальных станций ЛКС. Как правило, такая выделенная станция располагается на потолке и действует как многопортовый повторитель. Связь осуществляется следующим образом: передатчик базовой станции

повторяет рассеянный сигнал, который могут принимать все другие инфракрасные приемники, находящиеся в охваченном диапазоне, а для передачи данных на выделенную станцию используются направленные лучи, нацеленные на базовый модуль станции (рис. 2.18, а).

При использовании *отраженного инфракрасного излучения* все инфракрасные передатчики области сфокусированы и нацелены на точку на диффузно отражающем потолке (рис. 2.18, б). Инфракрасное излучение поступает на потолок и отражается от него, после чего принимается всеми приемниками области.

Такой метод имеет существенные недостатки: а) требуется потолок, отражающий инфракрасное излучение в заданном диапазоне длин волн (850 – 950 нм); б) радиус действия всей системы ограничен 10 м.

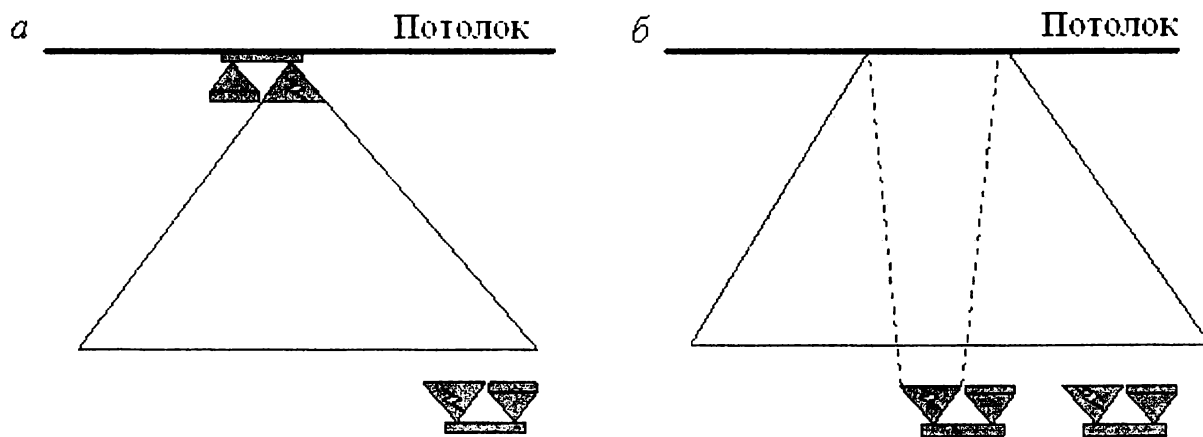


Рис. 2.18. Конфигурация инфракрасной БЛС:

а – рассеянное инфракрасное излучение; б – отраженное инфракрасное излучение

Пример типичной БЛКС с инфракрасной передачей приведен на рис. 2.19. Имеется несколько (по одной на комнату) размещенных на потолке базовых станций. Каждая базовая станция обеспечивает связь между несколькими стационарными и мобильными рабочими станциями, находящимися в обслуживаемой комнате. Между собой базовые станции соединяются проводом, они также связаны с сервером, который может выступать как точка доступа к кабельной ЛКС или ГКС. Кроме того, могут существовать конференц-залы, в которых отсутствуют базовые станции, а связь организуется эпизодическим образом.

Инфракрасные лучи не только требуют прямую видимость, но также чувствительны к погодным условиям; поэтому стандарты БЛКС описывают использование инфракрасного излучения только внутри помещений.

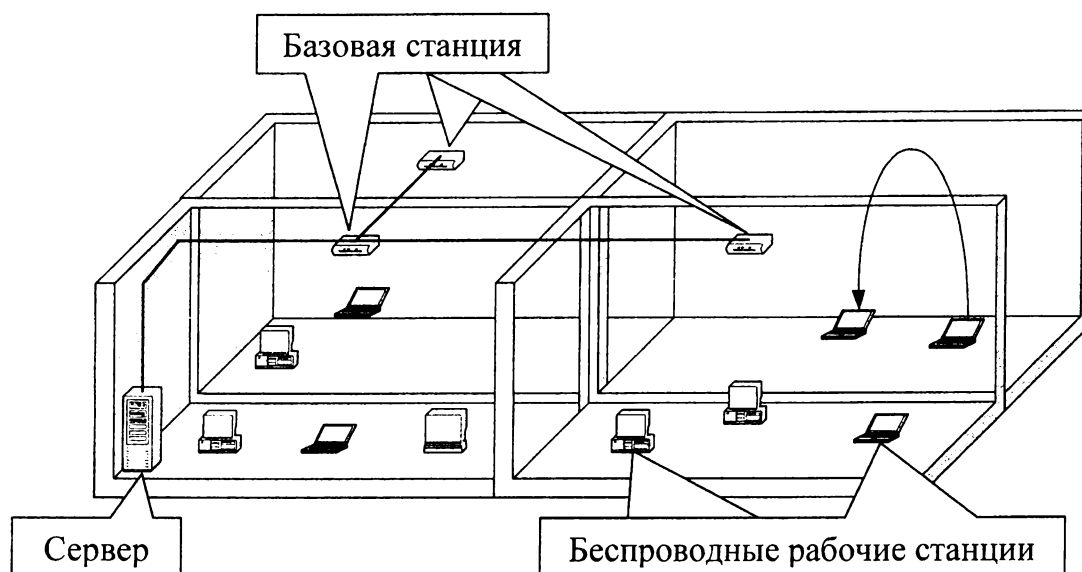


Рис. 2.19. Пример БЛКС, использующей инфракрасное излучение

Сети Wi-Fi

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами тем «HomeRF», «DECT» и «IEEE 802.11» раздела «Типы беспроводных сетей» электронного пособия «Беспроводные компьютерные сети».

Использование радиочастотной передачи в расширенном спектре предлагается в двух частотных диапазонах: один – в пределах частоты 915 МГц, другой – в диапазоне от 2,4 ГГц до 2,4835 ГГц. Этот диапазон мы будем кратко обозначать 2,4 ГГц. Диапазон 915 МГц не требует прямой видимости в отличие от диапазона 2,4 ГГц, но поскольку в европейских странах и в России он сильно загружен другими средствами связи, то его рекомендуется использовать только внутри зданий. Диапазон 2,4 ГГц может использоваться как внутри зданий, так и снаружи. При наружном использовании мощность передатчика не должна превышать 100 милливатт; при внутреннем – его не должно быть «слышно» снаружи здания.

Спецификация IEEE 802.11 описывает использование двух принципиально различающихся методов радиопередачи в расширенном спектре:

- 1) метода прямой последовательности (Direct Sequence Spread Spectrum – DSSS);
- 2) метода частотных скачков (Frequency Hopping Spread Spectrum – FHSS).

После разработки стандарта IEEE 802.11 дальнейшее развитие технологий БЛКС шло в направлении более высоких и менее загруженных участков спектра радиопередач. Речь идет о диапазоне ISM¹, занимающем полосу в 150 МГц от 5,725 до 5,875 ГГц. Обычно этот спектр обозначают кратко – 5 ГГц.

В январе 1997 г. Федеральная правительственная комиссия США по средствам связи (Federal Communications Commission – FCC) разрешила использовать для нелицензированных радиочастотных сетей диапазон 5 ГГц. Всего в нем выделено два участка (5,15–5,35 ГГц и 5,725–5,825 ГГц); их общая полоса пропускания составляет 300 МГц. Через два года после этого выходит стандарт IEEE 802.11a, который описывает построение БЛКС, использующих радиопередачу в диапазоне 5 ГГц.

Стандарт IEEE 802.11a определяет следующие скорости передачи данных: 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с. При работе на частоте 2,4 ГГц радиус действия составляет 300 м, а на частоте 5 ГГц – 100 м.

В отличие от IEEE 802.11 стандарт 802.11a использует не расширенный спектр, а ортогональное частотное уплотнение (Orthogonal Frequency Division Multiplexing – OFDM). При OFDM используются несколько несущих сигналов на различных частотах, посредством каждого из которых осуществляется передача части битов. Ввиду этого стандарты IEEE 802.11 и IEEE 802.11a на физическом уровне предусматривают разные методы передачи радиосигналов, и устройства 802.11 не могут напрямую взаимодействовать с устройствами 802.11a.

Стандарт IEEE 802.11b – это расширение спецификации IEEE 802.11, предусматривающее использование метода радиопередачи DSSS и допускающее скорости передачи данных 5,5 и 11 Мбит/с. Он описывает работу БЛКС в диапазоне 2,4 ГГц².

Сетевые устройства, соответствующие стандарту IEEE 802.11 и использующие метод доступа DSSS, могут взаимодействовать с устройствами IEEE 802.11b (один и тот же метод радиопередачи), а устройства, использующие метод FHSS, – не могут (разные методы радиопередачи).

¹ Industrial, Scientific, Medical – промышленный, научный и медицинский диапазон, радиопередача в котором не требует получения лицензии.

² Для получения более высокой скорости при неизменной полосе используется манипуляция дополнительным кодом. Эта манипуляция является достаточно сложной. Ее рассмотрение выходит за рамки данного учебного пособия.

Стандарт IEEE 802.11 описывает три основные спецификации физического уровня модели IEEE 802.x, представленные в табл. 2.2¹.

Таблица 2.2

Спецификации стандарта IEEE 802.11 физического уровня модели IEEE 802.x

Стандарты				
802.11		802.11a		802.11b
Инфра-красная передача	915 и 2,4 ГГц; расширенный спектр; DSSS;	915 и 2,4 ГГц; расширенный спектр; FHSS;	5 ГГц; OFDM; 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с	2,4 ГГц; расширенный спектр; DSSS; 5,5 Мбит/с; 11 Мбит/с

Сети Bluetooth

Bluetooth использует небольшие приемопередатчики малого радиуса действия – 10–40 м – не обязательно в зоне прямой видимости² (рис. 2.20). Между соединяемыми устройствами могут быть различные препятствия.

В диапазоне 2,4 ГГц ISM два устройства Bluetooth, находящиеся на расстоянии до 10 м, могут совместно использовать пропускную способность до 720 Кбит/с. Одной из важнейших особенностей Bluetooth является автоматическая установка соединения между Bluetooth-устройствами, находящимися в пределах досягаемости.

Bluetooth, как и технология 802.11, использует метод радиопередачи в расширенном спектре FHSS.

Bluetooth-устройства могут устанавливать соединения типов «точка – точка», когда имеются только два устройства, и «точка – много точек», когда одно устройство одновременно работает с несколькими другими. В последнем случае устройство, которое обслуживает несколько соединений, называется Master (главное), а подключенные устройства – Slave (управляемые). Сеть Bluetooth с соединениями типа «точка–много точек» представлена на рис. 2.21, а. Кроме устройств, которые активно обмениваются данными, но являются управляемыми, есть еще множество неактивных

¹ На сегодняшний день стандартизированы и другие спецификации беспроводной связи в ЛКС. С ними можно познакомиться, обратившись к электронному пособию «Беспроводные компьютерные сети».

² Сегодня на рынке сетевого оборудования представлены модули Bluetooth, обеспечивающие связь на расстоянии 100 м.

управляемых устройств, которые не могут обмениваться данными с управляющим, пока заняты все каналы, но тем не менее, остаются синхронизированными с ним. Такая структура называется «Piconet».

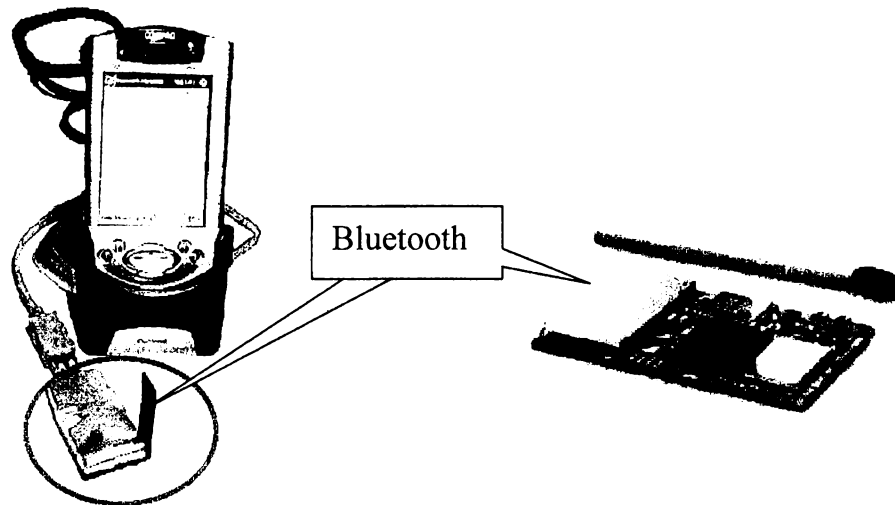


Рис. 2.20. Bluetooth-устройства

Иными словами, Piconet – это сеть, содержащая устройства, которые общаются между собой с соблюдением протоколов Bluetooth. По определению, все устройства Bluetooth равноправны, но тем не менее при образовании Piconet одно из них становится главным, управляющим, а другие – подчиненными. Главное устройство синхронизирует частоту и ее изменения для всех остальных устройств в Piconet.

В случае необходимости любое управляемое устройство в Piconet может стать управляющим, поменявшись ролью со старым «лидером».

Для распознавания любого устройства в сети выделяется трехразрядный MAC-адрес.

Поскольку в Bluetooth используются трехразрядные MAC-адреса, то в одной сети Piconet может быть не более 8 устройств ($2^3 = 8$).

Несколько независимых и несинхронизируемых сетей Piconet, между которыми возможен обмен информацией, образуют распределенную сеть Scatternet. Такие сети могут иметь топологию типов «точка – точка» и «точка – много точек».

На количество устройств, входящих в Scatternet, ограничений не накладываемся. Логические связи могут быть весьма разнообразными и изменяться как угодно.

В каждой пикосети действует только одно основное устройство, однако подчиненные устройства могут входить в различные пикосети. Кроме того,

основное устройство одной пикосети может являться подчиненным в другой (рис. 2.21, б).

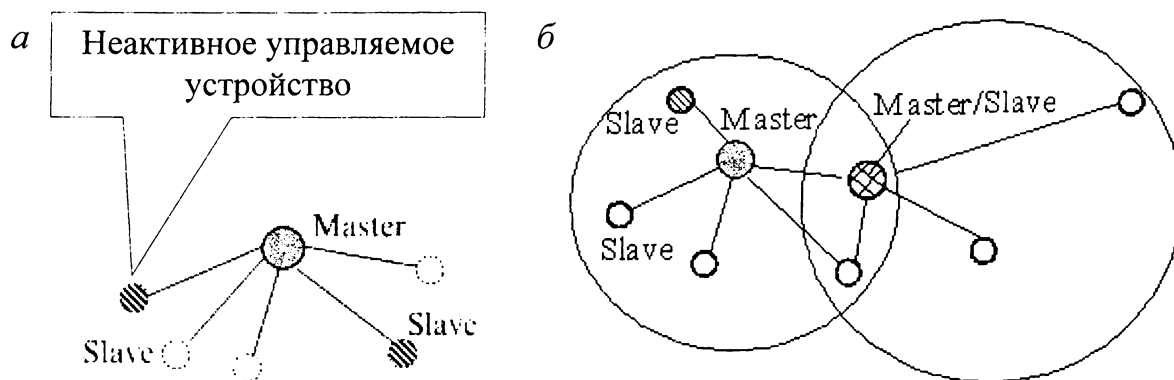


Рис. 2.21. Сети Bluetooth:
а – Piconet; б – Scatternet

Единственное условие: различные Piconet, входящие в один Scatternet, должны иметь разные каналы связи, т.е. работать на различных частотах и иметь различные алгоритмы смены частот (hopping). Всего стандарт 802.15.1 предусматривает 10 вариантов регулярной смены частот.

Резюме

1. На сегодняшний день в России функционируют сети 10Base2, 10BaseT, 100BaseTX, основанные на использовании кабельных линий связи.
2. Правила построения сетей 10Base2, 10BaseT, 100BaseTX на физическом и канальном уровне описывает модель IEEE 802.x.
3. Для построения кабельных ЛКС чаще всего используются физические топологии «шина», «звезда», «звезда – шина». Допустимо подключение компьютеров по типу «точка – точка».
4. В качестве среды передачи данных в современных ЛКС чаще всего используется кабель UTP 5-й категории.
5. Процесс выбора скорости передачи данных в сетях 10/100 Ethernet реализуется через автопереговоры.
6. Наиболее распространенными областями применения беспроводных ЛКС являются: расширение кабельных сетей – кочевой доступ и создание эпизодических сетей.
7. Как правило используются три топологии беспроводных ЛКС: «точка – точка», «один – ко многим» и «многие – ко многим».
8. Стандарт IrDA позволяет создавать инфракрасные ЛКС с высокой скоростью передачи данных.

9. Наибольшей популярностью в России пользуются беспроводные компьютерные сети Wi-Fi, построение которых описывает стандарт IEEE 802.11.
10. Все большую популярность в России приобретают компьютерные сети Bluetooth, построение которых описывает стандарт IEEE 802.15.1.

Вопросы для контроля

- 1) Какие стандартные технологии, позволяющие построить ЛКС, работающую на скорости 10 Мбит/с, Вам известны? Дайте краткую характеристику каждой из них.
- 2) Какие стандартные технологии, позволяющие построить ЛКС, работающую на скорости 100 Мбит/с, Вам известны? Дайте краткую характеристику каждой из них.
- 3) Какие основные правила построения сетей 10Base2, 10BaseT Вам известны?
- 4) Какие основные правила построения сетей 100BaseTX Вам известны?
- 5) В чем состоят сходство и отличие сетей 10BaseT и 100BaseTX?
- 6) Для чего в сетях 10BaseT/100BaseTX используется механизм автопереговоров и какова схема его реализации?
- 7) Какая физическая топология, на Ваш взгляд, наиболее устойчива к различным сбоям, возникающим при передаче сигналов по кабельной ЛКС? Какая наименее? Почему?
- 8) Какие области применения беспроводных ЛКС Вам известны? Приведите примеры.
- 9) Каковы особенности построения беспроводных ЛКС с физическими топологиями «точка – точка»? «один – ко многим»? «многие – ко многим»?
- 10) Каковы особенности построения сетей IrDA на физическом уровне модели OSI?
- 11) Каковы особенности построения сетей Wi-Fi на физическом уровне модели OSI?
- 12) Каковы особенности работы Bluetooth на физическом уровне модели OSI?
- 13) Каковы особенности построения сетей Piconet? С чем связаны вводимые ограничения?

- 14) Каковы основные правила объединения сетей Piconet в Scatternet?
- 15) Какие методы кодирования сигналов используются в беспроводных ЛКС, основанных на радиопередаче сигналов?
- 16) Совместимы ли на физическом уровне технологии 802.11 и 802.11a, 802.11 и 802.11b, 802.11a и 802.11b? Почему?
- 17) Совместимы ли на физическом уровне технологии Wi-Fi и Bluetooth, IrDA и Wi-Fi, IrDA и Bluetooth? Почему?

2.3. Построение ЛКС на канальном уровне

2.3.1. Протоколы канального уровня: общая характеристика

К основным режимам работы протоколов уровня LLC, которые поддерживаются ЛКС, относятся следующие:

- осуществление только синхронного способа передачи данных;
- использование в кабельных сетях, например в Ethernet 802.3, дейтаграммной передачи данных с обнаружением ошибок и без их коррекции;
- использование в беспроводных ЛКС, например в Ethernet 802.11, передачи данных с предварительным установлением соединения, а также с коррекцией ошибок.

Наиболее популярными на сегодняшний день протоколами уровня управления доступом к среде передачи данных, которые используются в современных ЛКС, являются:

- 1) CSMA/CD, использующийся в кабельных сетях Ethernet;
- 2) CSMA/CA, использующийся в беспроводных компьютерных сетях.

Компьютерных сетей, основанных на использовании доступа с передачей маркера и доступа по приоритету запроса, сегодня в России практически нет, поэтому здесь мы ограничимся рассмотрением только методов доступа CSMA/CD и CSMA/CA.

☞ *С методами доступа, используемымися в сетях Token Ring и 100VG-AnyLAN, Вы можете познакомиться, обратившись к демонстрационным материалам электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».*

2.3.2. CSMA/CD

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами темы «CSMA/CD» раздела «Канальный уровень модели OSI» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».

В сетях Ethernet (10Base2, 10BaseT, 100BaseTX и др.) используется метод доступа CSMA/CD – весьма быстродействующий и эффективный метод предоставления доступа к кабелю, по которому передаются данные. Рассмотрим особенности его работы.

Чтобы получить возможность передавать пакеты, станция должна убедиться, что среда передачи данных свободна. Для этого компьютеры перед передачей данных проверяют состояние несущей: занят ли канал связи передачей других данных или нет.

Если среда свободна, то узел имеет право начать передачу пакета. Пакет в сетях Ethernet состоит из семи частей, структура которых представлена в табл. 2.3:

- 1) *Преамбула*. Содержит семь синхронизирующих байт.
- 2) *Начальный разграничитель пакета*. Состоит из одного байта. Разграничитель пакета позволяет определить начало заголовка (это первый байт, который будет следовать сразу за ним).
- 3) *Адрес назначения*. Это аппаратный адрес узла-получателя.
- 4) *Адрес источника*. Это поле содержит аппаратный адрес узла-отправителя пакета.
- 5) *Тип*. Используется для идентификации протокола сетевого уровня.
- 6) *Данные*. Может содержать любую информацию объемом от 46 до 1500 байт.
- 7) *Контрольная последовательность*. Позволяет выявить ошибки передачи пакета; используется для проверки того, достигла ли остальная часть пакета места назначения без повреждения.

Таблица 2.3

Структура пакета сети Ethernet 802.3

Название части пакета	Структура части пакета				
	Преамбула	Начальный разграничитель пакета	Адрес назначения	Адрес источника	Тип
Заголовок					
Данные	Данные				
Трейлер	Контрольная последовательность				

Все станции, подключенные к кабелю, могут распознать факт передачи пакета, и та станция, которая узнает собственный аппаратный адрес в заголовке пакета, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю пакет с подтверждением получения данных. Адрес станции-источника содержится

в любом из передаваемых по сети пакетов, поэтому станция-получатель легко выясняет, кому нужно послать ответ.

Может случиться так, что кабель прослушивают два компьютера и, не обнаружив сигналов, начинают передавать данные одновременно. Механизм прослушивания среды и пауза между передаваемыми пакетами не могут предотвратить возникновения такой ситуации, когда две или более станции одновременно решают, что среда передачи данных свободна, и начинают передавать свои пакеты. Это приводит к столкновению пакетов, перемещающихся по КС. Такое явление называется *коллизией* (collision). Пакеты сталкиваются в общем кабеле, в результате чего происходит искажение информации – методы кодирования, используемые в Ethernet, не позволяют выделять сигналы каждой станции из общего сигнала.

☞ *Коллизия – столкновение (наложение) сигналов, в результате которого искажаются данные, передаваемые по КС.*

Для возникновения коллизии не обязательно, чтобы несколько станций начали передачу абсолютно одновременно; такая ситуация маловероятна. Гораздо вероятней, что коллизия возникает из-за того, что один узел начинает передачу раньше другого, но до второго узла сигналы первого просто не успевают дойти к тому времени, когда второй узел решает начать передачу своего пакета. Таким образом, коллизия – это следствие разделения среды передачи данных многих компьютеров (множественного доступа).

Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими в кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется коллизия (collision detection – CD).

Для увеличения вероятности скорейшего обнаружения коллизии всеми станциями сети станция, которая обнаружила коллизию, прерывает передачу своего пакета и усиливает ситуацию коллизии посылкой в сеть специальной последовательности из 32 бит, называемой jam-последовательностью. После этого она делает паузу, равную случайному периоду времени, а затем, если сеть свободна, возобновляет передачу данных. Все остальные станции также прерывают передачу данных на случайный промежуток времени.

Если после возобновления передачи данных вновь возникает коллизия, то передача данных приостанавливается еще раз. Всего метод CSMA/CD предусматривает до 16 попыток передачи пакетов. Невозможность передать данные и за такое количество попыток чаще всего свидетельст-

вует о сбое в работе сетевого оборудования (например, концентратора) или переполнении канала связи.

Коллизия – это нормальная ситуация в работе сетей, использующих CSMA/CD. Их вероятность невелика. При повышении интенсивности трафика в сети (количества передаваемых данных) она возрастает, при понижении – снижается практически до нуля.

В сетях, использующих метод доступа CSMA/CD, полностью избежать коллизий невозможно. Четкое распознавание коллизий всеми станциями сети является необходимым условием корректной работы сети. Если какая-либо передающая станция не распознает коллизию и решит, что пакет данных ею передан верно, то он будет утерян. Из-за наложения сигналов при коллизии информация в пакете исказится, и он будет отбракован принимающей станцией. Скорее всего, искаженная информация будет повторно передана каким-либо протоколом верхнего уровня, но повторная передача сообщения произойдет только через несколько секунд. По сравнению с микросекундными интервалами, которыми оперируют ЛКС, – это очень значительная задержка по времени.

В связи с этим для всех сетей, основанных на CSMA/CD, вводятся ограничения на размеры домена коллизий.

☞ *Домен коллизий – это часть сети Ethernet, все узлы которой распознают коллизию независимо от того, в какой части данной сети эта коллизия возникла.*

Это выражается в том, что стандартные технологии Ethernet 802.3 на физическом уровне описывают ограничения по таким параметрам, как общая длина всех сегментов кабеля, количество подключений компьютеров, количество сетевых устройств, их тип.

2.3.3. CSMA/CA

После изучения данной темы рекомендуем познакомиться с материалами раздела «Канальный уровень 802.11» электронного пособия «Беспроводные компьютерные сети».

Беспроводные ЛКС используют метод доступа к среде передачи данных с контролем несущей и предотвращением коллизий (CSMA/CA). Работа методов доступа CSMA/CA имеет существенные отличия от CSMA/CD. Станция, желающая передавать данные, тестирует канал связи, и, если не обнаружено активности, станция ожидает в течение некоторого случайного промежутка времени, а затем передает пакет, если среда передачи данных все еще свободна. Если пакет приходит целым,

принимающая станция посылает специальный пакет с подтверждением приема данных. Если передающая станция не получила такой пакет (в силу того, что не был получен пакет данных или пришел поврежденный пакет с подтверждением), делается предположение, что произошла коллизия, и пакет данных передается снова через случайный промежуток времени.

Механизм явного подтверждения эффективно решает проблемы помех. Однако он добавляет некоторые дополнительные накладные расходы (пересылка пакетов с подтверждениями), которых нет в кабельных сетях. Поэтому беспроводные сети Ethernet 802.11 будут всегда работать медленнее, чем эквивалентные им кабельные сети Ethernet 802.3.

2.3.4. Канальный уровень Bluetooth

После изучения данной темы рекомендуем ознакомиться с материалами раздела «Канальный уровень Bluetooth» электронного пособия «Беспроводные компьютерные сети».

Основным протоколом канального уровня модели OSI для технологии Bluetooth является протокол управления логическими каналами и адаптацией (Logical Link Control and Adaptation Protocol – L2CAP), который предусматривает два типа передачи данных. Спецификация регламентирует один асинхронный канал обмена данными или до трех синхронных каналов передачи голоса.

Синхронная связь с установлением соединения (Circuit-switched Synchronous Connection Oriented links – SCO) рассчитана на установление симметричного соединения «точка – точка» и служит преимущественно для передачи речевых сообщений. Скорость передачи информации при использовании SCO равна 64 кбит/с.

Асинхронная связь без установления соединений (Asynchronous Connectionless Links – ACL) обеспечивает асимметричную передачу данных и предназначена для их пакетной передачи. Она поддерживает симметричные и асимметричные соединения типа «точка – много точек».

По асинхронному каналу асимметричная связь осуществляется на скорости 721 кбит/с в одном направлении и 57,6 кбит/с – в другом. При симметричном обмене скорость в обоих направлениях достигает 432,6 кбит/с.

Резюме

1. Основные режимы работы протоколов уровня управления логической связью, которые поддерживаются ЛКС, во многом зависят от физической среды, используемой для передачи данных.

2. ЛКС, использующие кабельные соединения, практикуют самые быстрые и, одновременно, самые ненадежные методы передачи данных.
3. ЛКС, использующие беспроводные соединения, чувствительны к качеству линий связи, поэтому они задействуют весьма надежные методы передачи данных в ущерб скорости передачи данных.
4. На сегодняшний день в ЛКС активно используются два основных метода доступа к среде передачи данных: CSMA/CD и CSMA/CA. Все большую популярность приобретают беспроводные компьютерные сети малого радиуса действия Bluetooth.

Вопросы для контроля

- 1) Какие основные режимы работы протоколов уровня управления логической связью для кабельных и беспроводных ЛКС Вам известны?
- 2) Какова схема работы компьютерной сети, использующей метод доступа CSMA/CD? В каких компьютерных сетях его используют?
- 3) Какова схема работы компьютерной сети, использующей метод доступа CSMA/CA? В каких компьютерных сетях его используют?
- 4) Каковы особенности построения беспроводных ЛКС Wi-Fi на канальном уровне модели OSI?
- 5) Каковы особенности построения сетей Bluetooth на канальном уровне модели OSI?
- 6) Совместимы ли на канальном уровне технологии 802.11 и 802.11a; 802.11 и 802.11b; 802.11a и 802.11b? Почему?
- 7) Совместимы ли на канальном уровне технологии Wi-Fi и Bluetooth; IrDA и Wi-Fi; IrDA и Bluetooth? Почему?

2.4. Оборудование ЛКС

2.4.1. Сетевые адаптеры

После изучения материалов данной темы рекомендуем познакомиться с демонстрационными материалами тем «Сетевые адаптеры», «Совместимость сетевых плат» раздела «Сетевые компоненты Win 2000» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».

Платы сетевого адаптера функционируют в качестве физического интерфейса между компьютером и физической средой передачи данных. Платы устанавливаются в слоты расширения или интегрируются на материнской плате компьютеров.

Основные функции сетевого адаптера:

- подготовка данных, поступающих от компьютера, к передаче по сетевому кабелю;
- передача данных другому компьютеру;
- управление потоком данных между компьютером и кабелем;
- прием данных из кабеля и перевод их в форму, понятную центральному процессору компьютера.

Для того чтобы обеспечить физическое соединение между компьютером и сетью, к соответствующему разъему платы подключается сетевая кабель (рис. 2.22, а).

Перед тем как послать данные в сеть, плата сетевого адаптера должна перевести их из формы, понятной компьютеру, в форму, в которой они могут передаваться по сетевому кабелю.

Внутри компьютера данные передаются по шинам. Шина – это несколько проводников, расположенных параллельно друг другу. Так как линий несколько, то и биты данных передаются по ним блоками, а не последовательно.

Современные компьютеры имеют 32- и 64-разрядные шины данных. Это означает, что они способны передавать данные блоками по 32 и 64 бита соответственно.

В сетевом кабеле данные перемещаются в виде потока бит. Такой тип передачи называют последовательным, потому что биты следуют друг за другом. Иными словами, кабель – это своего рода дорога с одной полосой. По таким «дорогам» данные в каждый момент времени движутся в одном направлении.

Плата сетевого адаптера принимает параллельные данные и организует их для последовательной пересылки. Этот процесс завершается переводом цифровых данных компьютера в электрические и оптические сигналы, передающиеся по сетевым кабелям. Осуществляет такое преобразование трансивер, пример которого представлен на рис. 2.22, б.

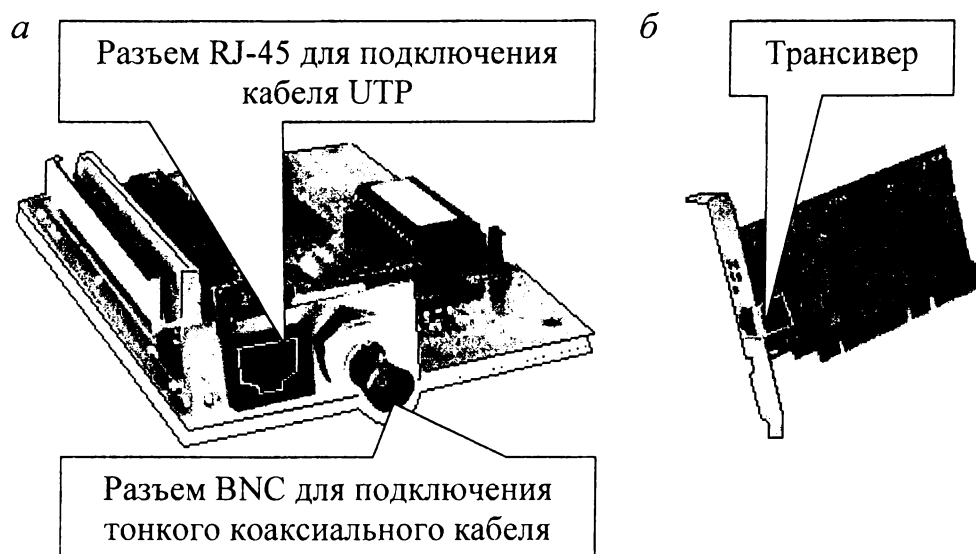


Рис. 2.22. Платы сетевого адаптера:

а – интегрированная на материнской плате; б – устанавливаемая в слот расширения

Плата сетевого адаптера, помимо преобразования данных, должна указать свое местонахождение, или адрес, чтобы ее могли отличить от остальных плат. Производители сетевых плат имеют в своем распоряжении строго определенные (несовпадающие) диапазоны аппаратных адресов, которые им выделяются специальным комитетом. Они «прошиваются» в ПЗУ сетевых адаптеров при производстве. Таким образом, аппаратные адреса сетевых плат всегда уникальны. Для всех существующих технологий ЛКС аппаратный адрес имеет формат 6 байт, например 11-A0-17-3D-BC-01.

Поскольку аппаратные адреса сетевых адаптеров используются протоколами MAC-уровня модели OSI, их очень часто называют MAC-адресами. Далее мы будем придерживаться именно такого названия.

Перед тем как послать данные в сеть, плата сетевого адаптера проводит электронный диалог с принимающей платой, во время которого они «обговаривают»:

- максимальный размер блока передаваемых данных (пакета);
- объем данных, пересылаемых без подтверждения о получении;
- интервалы между передачами блоков данных;

- интервал, в течение которого необходимо послать подтверждение;
- объем данных, которые может принять каждая плата без переполнения буфера;
- скорость передачи данных.

Очевидно, что все перечисленные функции относятся к уровню LLC модели IEEE 802.x.

Если новая (более сложная и быстрая) плата взаимодействует с устаревшей (медленной) платой, то они должны найти общую для них обеих скорость передачи. Схемы современных плат сетевого адаптера позволяют им приспособиться к медленной скорости старых плат. Например, если одна сетевая плата может передавать данные со скоростью 10 Мбит/с, а вторая – 10/100 Мбит/с, то будет выбрана наименьшая из скоростей – 10 Мбит/с.

Каждая плата оповещает другую сетевую плату о своих параметрах, принимает информацию о чужих параметрах и подстраивается под них. После того как все детали определены, начинается обмен данными.

Для того чтобы обеспечить совместимость компьютера и сети, плата сетевого адаптера должна соответствовать внутренней структуре компьютера (архитектуре шины данных). Например, плата, которая нормально работает в компьютере Apple, может не подойти для компьютера IBM ввиду того, что в них могут быть несовместимые разъемы для установки сетевого адаптера на системной плате.

Для того чтобы две сетевые платы могли понять друг друга, они должны разговаривать на одном и том же языке. Если одна плата будет передавать модулированные сигналы, а другая – немодулированные, то в сети начнется хаос и данные ни передать, ни принять будет невозможно.

Таким образом, внутри одной ЛКС должна быть совместимость по передаваемым сигналам.

Для того чтобы две сетевые платы могли передавать и принимать данные, циркулирующие в КС, они должны использовать один и тот же метод доступа к разделяемой среде передачи данных.

Сетевая плата может поддерживать несколько стандартных технологий. Например, сетевой адаптер 10/100 Ethernet может быть использован при построении КС 10BaseT, 100BaseTX (при совместимости всех других параметров).

Для того чтобы передавать данные по кабельным линиям связи, сетевая плата должна быть подключена к ним. Тип разъема на сетевой плате должен соответствовать типу кабеля, подключаемого к сетевому адаптеру.

Если сетевая плата предназначена для подключения к беспроводным линиям связи, то она также имеет свои конструктивные особенности. На рис. 2.23 представлены примеры сетевых плат для подключения компьютеров к беспроводным линиям связи.

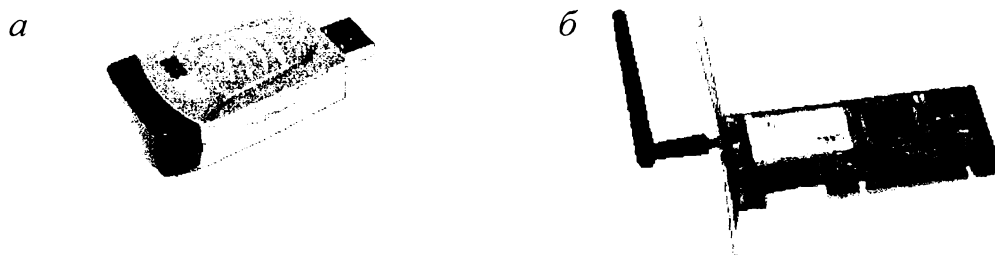


Рис. 2.23. Примеры сетевых плат для подключения к беспроводным линиям связи:
а – инфракрасным; б – радио

Таким образом, для того чтобы сетевые адаптеры могли взаимодействовать, они должны быть совместимы с компьютерами, на которых установлены, и использовать одинаковые протоколы канального и физического уровней.

Драйверы сетевых плат (сетевые драйверы) отвечают за управление всеми внешними связями компьютера. Для каждой используемой модели сетевой платы необходимо установить соответствующий сетевой драйвер. Если в компьютере имеется несколько сетевых плат разного типа, то для каждой платы следует установить собственный драйвер. Однако если в компьютере используются две одинаковые платы, достаточно одного драйвера. По существу, драйверы обеспечивают сетевое соединение компьютеров на канальном уровне.

■ После изучения темы «Сетевые адаптеры» Вы можете перейти к выполнению лабораторной работы 3 «Установка сетевого адаптера» в лабораторном практикуме «Локальные компьютерные сети».

2.4.2. Повторители и усилители

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами темы «Типы сигналов» раздела «Физический уровень модели OSI» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».

Повторители и усилители – это устройства, работающие на физическом уровне модели OSI. Они регенерируют электрические или световые сигналы для увеличения расстояния, на которое сигнал может распространяться. Примеры используемого в сетях Ethernet повторителя и

работающего в КС усилителя, которые базируются на оптоволоконных линиях связи, приведены на рис. 2.24.

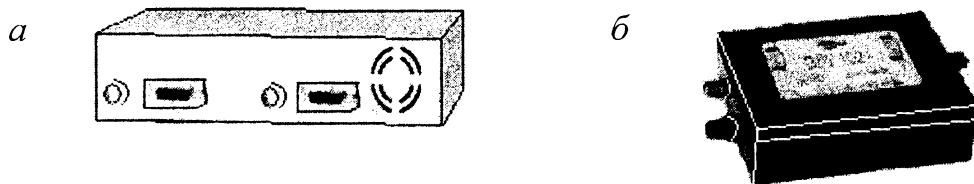


Рис. 2.24. Устройства, усиливающие сигналы, передаваемые по ЛКС:
а – повторитель; б – усилитель

2.4.3. Концентраторы

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами темы «Звезда» раздела «Топологии» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».

Концентратор является устройством, которое используется для подключения компьютеров в физических топологиях «звезда» и «звезда-шина». Это устройство напоминает обычную металлическую коробку с несколькими портами для подключения сетевого кабеля. Концентратор может быть рассчитан на подключение различного количества компьютеров, от 4- и 5-портовых для дома и малых ЛКС до больших модулей, имеющих 24 порта и более.

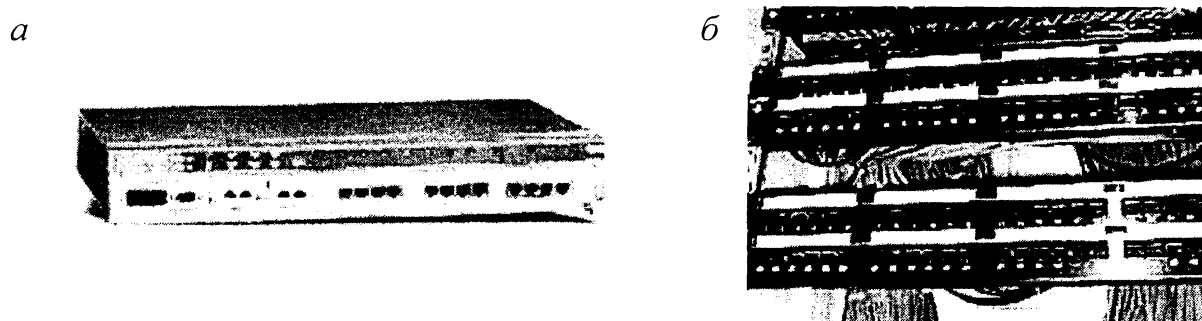


Рис. 2.25. Примеры концентраторов:
а – активный, б – пассивный (патч-панель)

Концентраторы подразделяются на активные и пассивные. *Активные концентраторы* регенерируют и передают сигналы так же, как повторители (их называют и многопортовыми повторителями). Каждый сигнал, поступивший на любой из портов активного концентратора, повторяется на все другие порты. Активные концентраторы надо обязательно подключать к электросети (рис. 2.25, а).

К *пассивным концентраторам* относятся, например, монтажные или коммутирующие панели. Они просто пропускают через себя сигнал, не

усиливая и не восстанавливая его. Пассивные концентраторы не надо подключать к электросети (рис. 2.25, б).

2.4.4. Коммутаторы и мосты

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами темы «Коммутаторы» раздела «Технологии локальных сетей» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».

Ограничения, накладываемые на размеры домена коллизий в сетях Ethernet и Fast Ethernet, не позволяют организовать компьютерную сеть на большей территории. Для того чтобы иметь возможность включать в сеть узлы, расположенные на расстоянии нескольких сот метров (и даже километров), используются не концентраторы, а мосты и/или коммутаторы.

Мосты и коммутаторы работают на двух нижних уровнях модели OSI – физическом и канальном. Напомним, что наборы бит, которые формируются на канальном уровне из пакетов, принято называть кадрами.

Мост (bridge) является средством передачи кадров между двумя (или более) сегментами – доменами коллизий. Мост анализирует заголовок кадра – его интересуют MAC-адреса источника и получателя. Мост прослушивает кадры, приходящие каждый на свой порт, и составляет списки MAC-адресов узлов, подключенных к этим портам (по адресам источника). Если приходящий кадр имеет адрес назначения, принадлежащий тому же сегменту, то этот кадр мостом *фильтруется* – никуда не транслируется. Если адрес назначения известен мосту и относится к другому сегменту, мост транслирует этот кадр в соответствующий порт. Если положение адресата назначения еще не известно мосту, кадр транслируется во все порты (кроме того, откуда пришел). Широковещательные (всем компьютерам в сети) и многоадресные кадры также транслируются во все порты. Трансляция предполагает доступ к сегменту по обычной схеме: ожидание отсутствия несущей, передача кадра и, в случае коллизий, повторные попытки передачи. Для выполнения этих процедур мост должен иметь буферную память для промежуточного хранения кадров, а также память для хранения списков MAC-адресов узлов сегментов всех портов.

Коммутатор (switch) в принципе выполняет те же функции, что и мост, но предназначен для несколько иных целей. Он используется как средство сегментации – уменьшения количества узлов в доменах коллизий. В пре-

дельном случае – при микросегментации – к каждому порту коммутатора подключается только один узел. При этом коммутатор должен направить в нужный порт каждый входящий кадр, что предъявляет высокие требования к производительности процессора коммутатора. Если к порту коммутатора подключается один узел (станция или другой коммутатор), то появляется возможность работы в дуплексном режиме. При этом коллизии как таковые отсутствуют.

Существуют два основных подхода к коммутации – с промежуточным хранением и «на лету».

Технология с *промежуточным хранением* (store and forward) предполагает, что каждый кадр, пришедший в порт, целиком принимается в буферную память. Далее процессор анализирует его заголовок, адрес источника использует для построения своих таблиц, а по адресу назначения определяет порт, в который кадр должен быть передан. В случае многоадресной или широковещательной передачи это будет группа из всех остальных портов. Передача в порт(ы) производится по мере его (их) освобождения согласно процедуре CSMA/CD. После успешной передачи (во все требуемые порты) кадр из памяти удаляется, освобождая место. Недостатком технологии с промежуточным хранением является значительная задержка передачи кадров – по меньшей мере на время приема кадра.

Коммутация на лету (on-the-fly) выполняется по возможности без промежуточного хранения. Порт принимает кадр, одновременно анализируя его поле заголовка. Как только пройдут биты адреса назначения, коммутатор уже может пересылать кадр в порт назначения, если он не занят. В случае, если порт назначения занят, промежуточное хранение неизбежно. Коммутация на лету вносит минимальную задержку, что, безусловно, можно отнести к достоинствам данной технологии.

В отличие от мостов, число портов которых невелико (часто всего два), коммутаторы имеют множество портов. В зависимости от производительности коммутатор может быть блокирующим или неблокирующим. *Неблокирующий коммутатор* способен обрабатывать все кадры, входящие на все его порты с максимальной скоростью, которую обеспечивает среда передачи.

Для скорости 10 Мбит/с и при не очень большом количестве портов это достигается относительно просто; высокие скорости создают определенные трудности, особенно при большом количестве портов. В мостах с задачей коммутации успешно справляется один процессор. В коммутаторах для достижения приемлемой производительности каждый порт (или

группа портов) снабжается своим процессором, и эти процессоры работают параллельно. Всеми процессорами коммутатора управляет центральный процессор коммутатора.

Конструктивно коммутаторы могут иметь несколько вариантов исполнения в зависимости от их назначения и производительности:

- *коммутаторы с фиксированным количеством портов* – самые дешевые устройства (количество портов – 24–30);
- *модульные коммутаторы* – могут иметь до сотни портов. Стоимость их достаточно высока по сравнению со стоимостью коммутаторов с фиксированным количеством портов, производительность, как правило, тоже выше;
- *стековые коммутаторы* – позволяют объединять сразу несколько коммутаторов.

Производительность коммутаторов рассматривается в двух аспектах: это максимальное количество кадров, обрабатываемых за единицу времени, и максимальное количество бит, пропускаемых за единицу времени. Однако даже при высокой пропускной способности коммутатора возможны перегрузки, если ряд портов будет состязаться за право передачи кадров в один и тот же порт. При перегрузке буфер начнет переполняться, и часть пакетов будет теряться без уведомления источника и получателя. Конечно, протоколы верхних уровней модели OSI заметят пропажу кадров и организуют их повторную передачу, но это потребует определенного времени. В результате коммутатор может даже замедлить работу сетевых приложений.

Мосты и коммутаторы позволяют разбивать сеть на отдельные сегменты – домены коллизий. Это означает, что коллизии не распространяются за границы сегментов (хотя кадры, поврежденные коллизиями рядом коммутаторов распространяются беспрепятственно). На рис. 2.26 представлена ситуация, когда за счет использования одного коммутатора единая сеть будет разбита на два сегмента, каждый из которых будет представлять отдельный домен коллизий, не превосходящий, например, 2500 м (для сети 10BaseT).

Однако широковещательные и многоадресные кадры при применении обычных мостов (коммутаторов) будут путешествовать по всей сети, вызывая ее нежелательную загрузку. Локализацию широковещательного и многоадресного трафика позволяют осуществлять интеллектуальные

коммутаторы, поддерживающие виртуальные локальные сети (Virtual Local Networks – VLAN)¹.

Топологические ограничения, относящиеся к сетям на повторителях и концентраторах («правило 3–4–5»), справедливы для каждого домена коллизий.

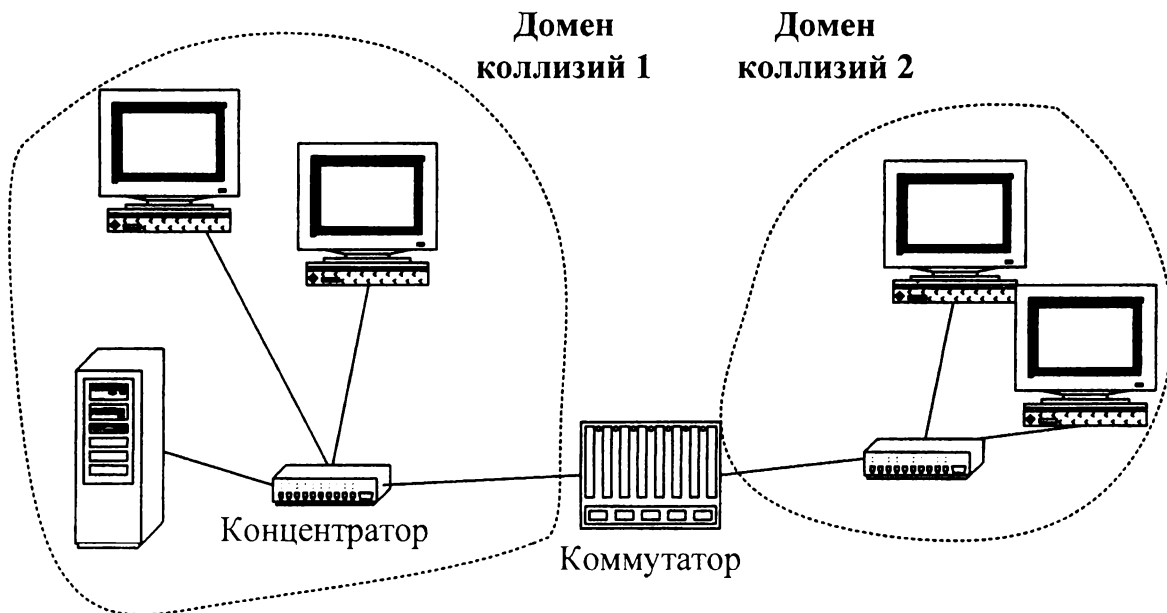


Рис. 2.26. Сеть Ethernet (Fast Ethernet), состоящая из двух доменов коллизий

Поскольку мосты и коммутаторы используют в своей работе только MAC-адреса, затруднено распознавание принадлежности того или иного компьютера к определенному логическому сегменту – сам адрес не содержит никакой информации по этому поводу. Мост (коммутатор) достаточно упрощенно представляет деление сети на сегменты – он запоминает, через какой порт на него поступили данные, предназначенные для этого компьютера, и в дальнейшем передает все пакеты, предназначенные для данного компьютера, на этот порт. Точной топологии связей между логическими сегментами мост (коммутатор) не знает. Из-за этого применение данных устройств приводит к значительным ограничениям – сегменты должны быть соединены таким образом, чтобы в сети не образовывались замкнутые контуры. Таким образом, сеть, построенная с применением обычных мостов и коммутаторов, не должна

¹ Более подробно VLAN будут рассмотрены в учебном пособии «Основы корпоративных компьютерных сетей», которое готовится к изданию.

иметь петель – между любой парой узлов в ней должен существовать только один путь.

На рис. 2.27 приведены примеры коммутатора и моста.

☞ *Примеры сетевого оборудования различных производителей Вы можете посмотреть, обратившись к электронной энциклопедии «NetHARD».*

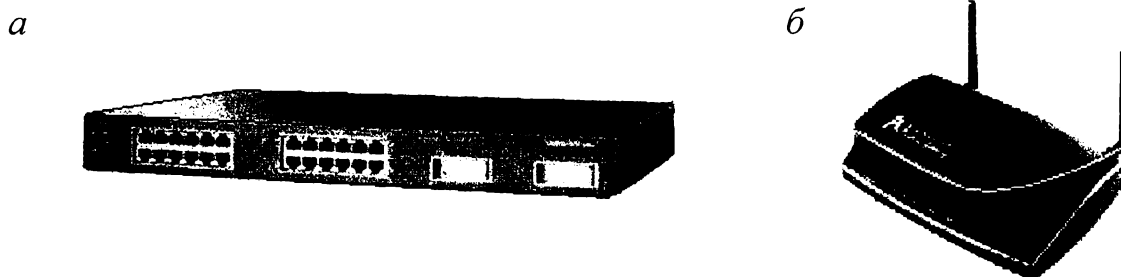


Рис. 2.27. Оборудование КС:
а – коммутатор; б – беспроводной мост

■ *После изучения темы «Коммутаторы и мосты» Вы можете перейти к выполнению лабораторной работы 4 «Ethernet 100 Мбит/с. Использование коммутаторов» в лабораторном практикуме «Локальные компьютерные сети».*

2.4.5. Принтеры

После изучения данной темы рекомендуем познакомиться с презентацией «Организация сетевой печати в среде Windows» (файл Сетевая печать\Сетевая печать.ppt).

Использование принтеров было одним из основных мотивов создания компьютерных сетей вообще, и в настоящее время, спустя десятилетия, это одна из главных причин организации ЛКС. В большинстве случаев пользователи должны регулярно печатать документы, но они не делают этого непрерывно, поэтому расходы по обеспечению отдельным принтером каждого служащего, которому он необходим, представляются неоправданными. Кроме того, индивидуальные принтеры занимают достаточно много места на рабочих столах и значительно увеличивают нагрузку системных администраторов, связанную с обслуживанием оборудования.

Важной проблемой является расположение принтеров в сети. Необходимо найти конкретные места для размещения принтеров, которые удовлетворяли бы требованиям пользователей сети.

В сети с выделенным сервером соединение принтера и сервера способно свести к минимуму объем сетевого трафика, создаваемого процессом печати, так как при этом очередь заданий на печать обычно располагается на том же сервере (рис. 2.28, а).

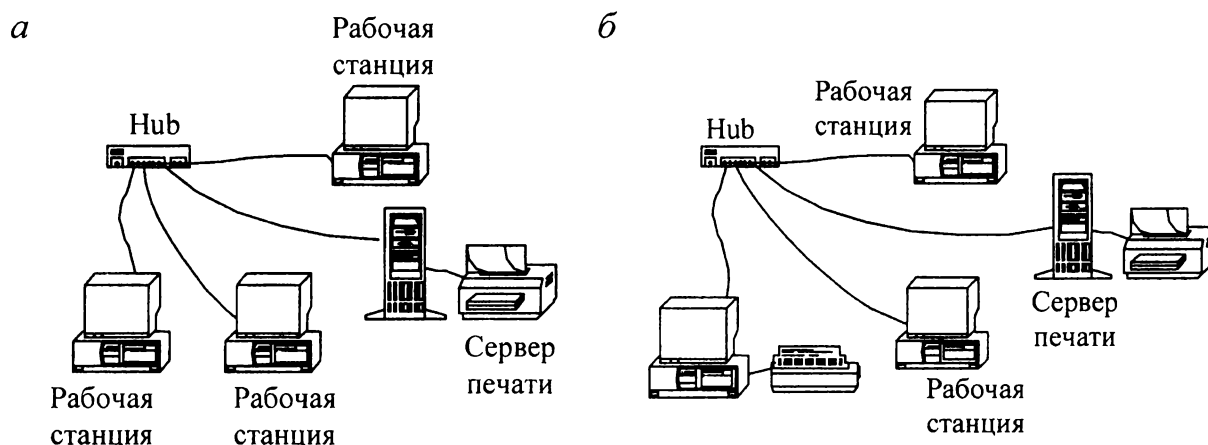


Рис. 2.28. Подключение принтера:

а – к выделенному серверу; б – к рабочей станции и выделенному серверу

Недостатки этого метода связаны с тем, что использование параллельных или последовательных соединений ограничивает как максимальное расстояние между принтером и сервером, так и общее количество принтеров, которые можно подключить к серверу. Например, если сервер расположен в монтажном шкафу или информационном центре, доступ пользователей к принтерам может быть в значительной степени ограничен.

Рабочие станции используют такие же параллельные и последовательные соединения, как и выделенные серверы, с аналогичными ограничениями по расстоянию между принтером и компьютером, однако они расположены намного ближе к пользователям и количество рабочих станций в сети на порядок больше, чем серверов. Последнее обстоятельство позволяет с большей свободой находить удобные для пользователей места расположения принтеров (рис. 2.28, б). С другой стороны, рабочие станции могут генерировать дополнительный сетевой трафик, если очередь заданий на печать располагается на другом компьютере. Кроме того, выполнение печати будет дополнительной нагрузкой на процессор рабочей станции.

Одним из наиболее популярных решений для сетевой печати является подключение принтеров непосредственно к сетевому кабелю при помощи самостоятельного сервера печати, который принимает форму либо платы сетевого адаптера, устанавливаемой в принтер (рис. 2.29, а), либо специализированного устройства (принт-сервера), взаимодействующего с

принтером через параллельный кабель (рис. 2.29, б). Этот метод позволяет расположить принтер в произвольном месте КС. Очередь заданий на печать всегда должна располагаться на каком-либо из компьютеров, которым может быть как сервером, так и рабочей станцией.

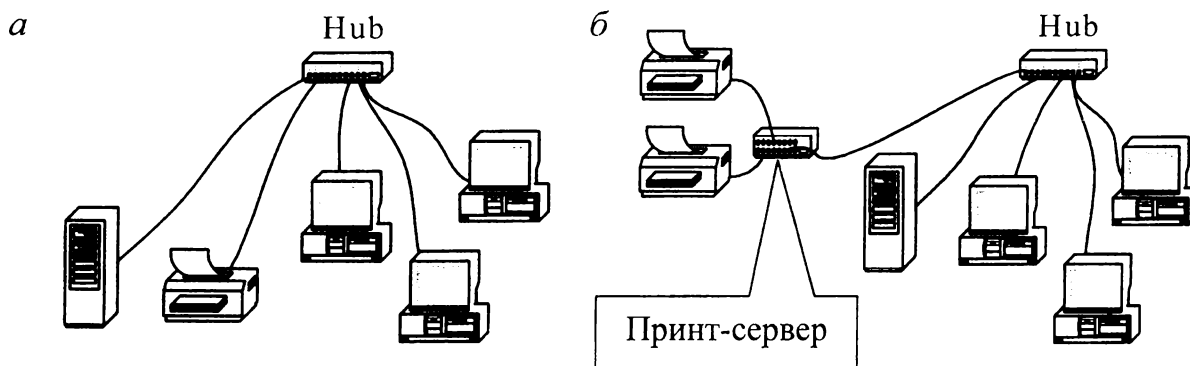


Рис. 2.29. Прямые соединения принтера с сетью при помощи:
а – сетевого адаптера, встроенного в принтер; б – принт-сервера

Резюме

1. Основным оборудованием ЛКС являются сетевые адаптеры, повторители, усилители, концентраторы, коммутаторы и мосты.
2. Все основное сетевое оборудование ЛКС работает на физическом уровне модели OSI. Сетевые адаптеры и коммутаторы дополнительно обеспечивают выполнение целого ряда функций канального уровня.
3. К числу основных ресурсов ЛКС относятся принтеры. Сетевой принтер может подключаться к аппаратному серверу, рабочей станции или иметь прямое соединение с сетью.

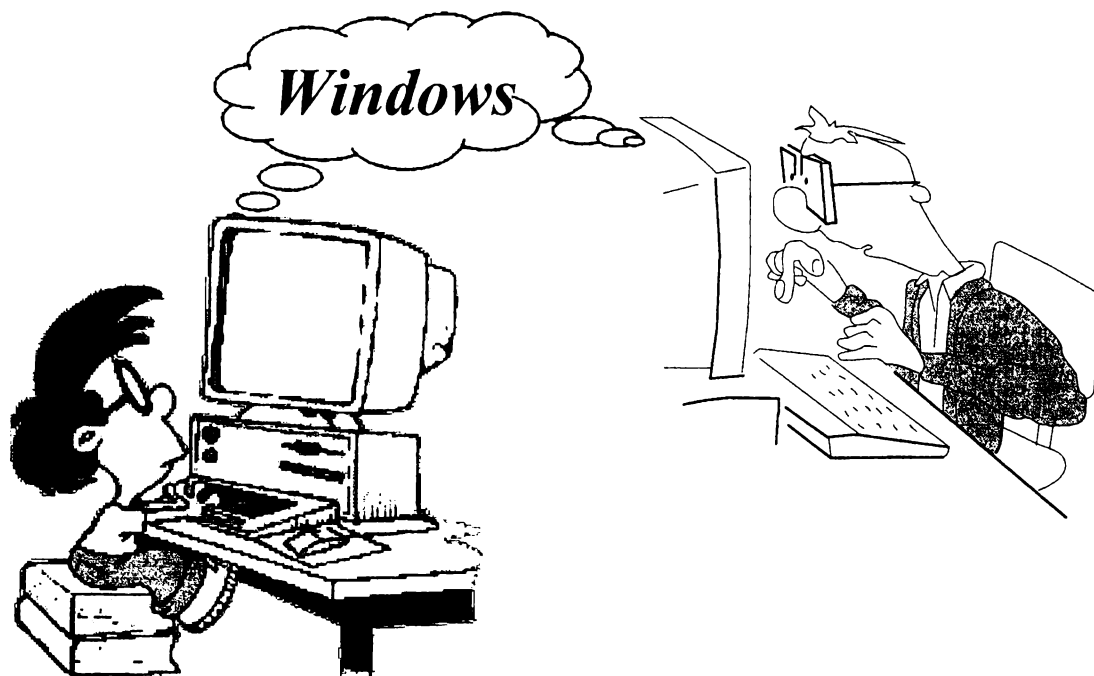
Вопросы для контроля

- 1) Какие функции выполняет сетевой адаптер?
- 2) Какие основные характеристики сетевых адаптеров Вам известны?
- 3) Какие критерии совместимости сетевых адаптеров Вы можете перечислить?
- 4) На каком уровне модели OSI работает сетевой адаптер? Свой ответ аргументируйте.
- 5) На каком уровне модели OSI работает драйвер сетевого адаптера? Свой ответ аргументируйте.
- 6) На каком уровне модели OSI работает повторитель? усилитель?
- 7) Каковы принципы работы коммутаторов? мостов?
- 8) На каком уровне модели OSI работает коммутатор? мост? Свой ответ аргументируйте.

- 9) В чем состоит сходство между работой коммутатора и моста? В чем между ними разница?
- 10) Какова схема подключения в ЛКС принтеров? Каковы достоинства и недостатки каждого из этих вариантов организации сетевой печати?
- 11) Какова разница между принт-сервером и сервером печати?

Раздел 3

Построение ЛКС средствами MS Windows



3.1. Сетевая архитектура MS Windows

В рамках разд. 2 было продемонстрировано решение одной из главных, но вместе с тем наиболее простых задач построения ЛКС – проектирование размещения базового сетевого оборудования, компьютеров, выбор физической среды передачи данных и т.п.

Теперь сконцентрируем свое внимание на особенностях построения ЛКС на пяти верхних уровнях модели OSI: сетевом, транспортном, сеансовом, представительском и прикладном.

3.1.1. Сетевые компоненты: общая характеристика

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами раздела «Сетевые компоненты Windows» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».

Чтобы передать по локальной сети данные от одного компьютера к другому, необходимо не только оборудование, организованное в соответствии с одной из стандартных технологий, но и сетевое программное обеспечение (ПО), которое должно собрать передаваемые данные в пакет. Таким ПО, прежде всего, являются сетевые операционные системы.

Работа в сети – одна из основных функций MS Windows¹, и поэтому основу этой операционной системы в значительной степени составляет ее сетевая архитектура, главными компонентами которой являются клиенты, редиректор, серверы, сетевые протоколы, сетевой адаптер и его драйвер.

На рис. 3.1 представлена модель, символизирующая соответствие сетевых компонентов Windows уровням модели OSI.

Сетевые адаптеры и их драйверы были рассмотрены в разд. 2 данного учебного пособия. Далее мы остановимся на рассмотрении функций каждого из остальных сетевых компонентов Windows.

Напомним, что протокол – это формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне модели OSI, но в разных узлах.

Существует множество протоколов. И хотя все они участвуют в реализации связи, каждый из них предназначен для определенных задач и обладает своими преимуществами и недостатками. Функции протокола

¹ Далее в тексте просто Windows.

определяются тем уровнем, на котором он работает. Если, например, какой-то протокол работает на физическом уровне, это означает, что он обеспечивает прохождение пакетов через плату сетевого адаптера и далее – в сетевой кабель. Если же протокол работает на канальном уровне, то он регулирует доступ к среде передачи данных или управляет логической связью между компьютерами.

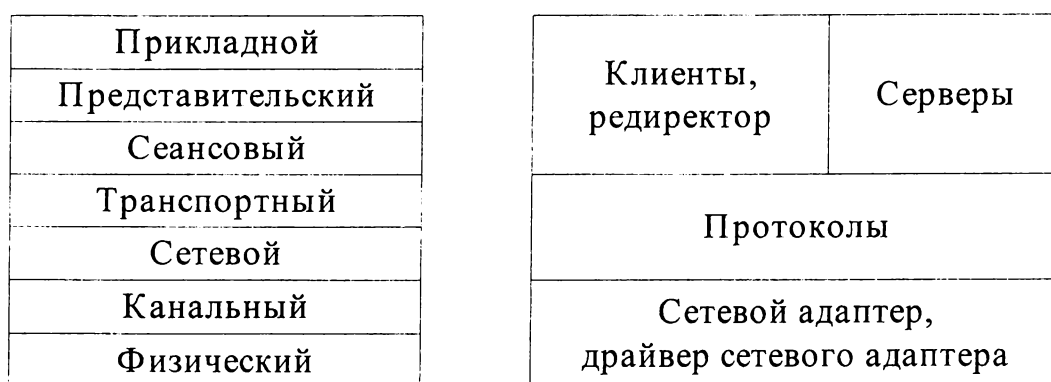


Рис. 3.1. Соответствие сетевых компонентов Windows модели OSI

Несколько протоколов, работающих совместно и обеспечивающих работу компьютеров в сети на верхних пяти уровнях модели OSI, образуют так называемый *стек протоколов*. В совокупности протоколы определяют полный набор функций и возможностей стека.

В настоящее время в компьютерных сетях используется большое количество стеков коммуникационных протоколов. В этом учебном пособии Вы познакомитесь со стеками протоколов ЛКС, поддерживаемых Windows, – NetBEUI/SMB, IPX/SPX и NWLinkIPX/SPX/NetBIOS¹.

Каждый из стеков протоколов по-разному разбивает данные на пакеты и добавляет служебную информацию (о последовательности пакетов, синхронизации для проверки ошибок и т.п.). Ввиду этого компьютер, который использует один из стеков протоколов, не сможет успешно связаться с компьютером, на котором работает неидентичный стек. Например, если на одном компьютере будет установлен стек протоколов IPX/SPX, а на другом – NetBEUI/SMB, то компьютеры не смогут взаимодействовать. Если же на обоих компьютерах будут установлены одни и

¹ Сейчас все чаще в ЛКС используют стек протоколов TCP/IP, являющийся основой построения корпоративных и глобальных сетей. В связи с этим в рамках данного учебного пособия он не рассматривается. С особенностями функционирования компьютерных сетей на основе TCP/IP Вы можете познакомиться, обратившись к учебному пособию «Принципы функционирования глобальных компьютерных сетей» или другой литературе.

те же стеки протоколов, компьютеры будут благополучно обмениваться информацией.

Серверные функции Windows реализует через работу служб.

☞ *Служба Windows – это программа или процесс, которая выполняет специфическую системную функцию, особенно на нижнем (близком к аппаратному обеспечению) уровне.*

Сетевые службы обеспечивают работу с такими общедоступными ресурсами КС, как файлы, принтеры и др. Например, **Служба доступа к файлам и принтерам для сетей Microsoft (File and Printer Sharing for Microsoft Networks)** обеспечивает доступ других компьютеров к ресурсам компьютера пользователя, используя сеть Microsoft (компьютеры этой сети работают под управлением ОС Windows).

Кроме перечисленных в Windows имеется большое количество других служб, которые позволяют организовать совместное использование других ресурсов или же функции управления КС.

Клиентская служба обеспечивает подключение или запрос к службам других компьютеров. Она может также обращаться к программному обеспечению, которое доступно компьютеру или программе при установке соединения (о видах клиентских служб см. далее в этом параграфе).

Все версии Windows включают службу **Клиент для сетей Microsoft (Client for Microsoft Networks)**, которая устанавливается автоматически сразу после инсталляции драйвера сетевого адаптера. С помощью этой службы приложения, установленные на компьютере, получают доступ к ресурсам других компьютеров сети. Основное назначение **Клиента для сетей Microsoft** – обеспечение доступа к файлам и принтерам сети Microsoft.

Подключившись к сети и установив службу **Клиент для сетей Microsoft**, можно открывать файлы как на локальных, так и на сетевых дисках с помощью одной и той же последовательности действий. Это возможно благодаря особому сетевому компоненту Windows – *редиректору (redirector)*. Редиректор обеспечивает связи между приложением и операционной системой, необходимые для получения приложением данных через сеть.

Для компьютера, инициирующего запрос по сети, редиректор играет главную роль в создании сетевого соединения. Его задача – заставить приложение на локальной машине полагать, что оно получает данные с локального, а не сетевого диска. Суть применения редиректора: место хранения запрашиваемого файла не должно иметь значения, метод доступа пользователя к нему должен быть единым.

Например, что случится, если Вы запустите программу и откроете файл, хранящийся на сетевом диске? С точки зрения программы сеть не существует. Она знает только о существовании нескольких доступных дисков, с именами, состоящими из букв с двоеточиями, например **F:**, **B:**, **C:** и т.д. Таким образом, необходимо задействовать тот уровень операционной системы, задача которого заключается в предоставлении программам обычного интерфейса, основанного на буквенных обозначениях дисков. Но делать это необходимо и в случае, когда приложению требуются данные, хранящиеся в сетевом устройстве. Программы полагают, что они обращаются к локальным дискам, однако их запросы информации с сетевых дисков должны перехватываться и направляться по сети. Эти функции и выполняет редиректор.

Для унификации именования ресурсов на удаленном компьютере используется универсальное соглашение о присвоении имен (Universal Naming Convention – *UNC*), в котором имя ресурса представляется в виде \\<имя_сервера>\<имя_ресурса>, например \\server\documents.

При обращении к ресурсу имя ресурса передается соответствующему редиректору, который обслуживает клиентскую службу. После выделения из *UNC*-имени имени сервера редиректор принимает решение о перенаправлении полученного запроса в сеть к другому серверу или же передаче его на обработку ОС, работающей на том же компьютере.

Помимо **Клиента для сетей Microsoft** в состав Windows входит вторая клиентская служба – для доступа к ресурсам Novell NetWare. В клиентских версиях Windows (например, в Windows 2000/XP Professional) эта служба называется «Служба клиента для NetWare» (**Client Service for NetWare**). В серверных версиях (например, в Windows 2000/2003 Server) она называется «Служба шлюза для NetWare» (**Gateway Services for NetWare – GSNW**). Данная служба обеспечивает выполнение в Windows основных функций NetWare по доступу к файлам и принтерам.

3.1.2. Сетевые интерфейсы

В Windows включены три основных стека протоколов (TCP/IP, NetBEUI/SMB и NWLink/IPX/SPX/NetBIOS). На компьютере, работающем под управлением Windows, можно применять любой из этих протоколов в одиночку, а также любые два или все три стека одновременно. Использовать несколько протоколов на одном компьютере позволяет *интерфейс транспортных протоколов* (Transport Driver Interface – TDI). Он представляет собой некую прослойку между стеками протоколов, клиентами и

интерфейсом прикладного программирования (Application Programming Interface – API).

Подобные пограничные уровни стандартизируют процесс разработки программ, позволяя программистам создавать службы с согласованным интерфейсом. В результате любая служба, расположенная над TDI, может обмениваться данными с любым стеком протоколов, расположенным под TDI.

Сетевые адаптеры и драйверы сетевых адаптеров, расположенные ниже сетевых протоколов, отделены от них другим пограничным уровнем, который в целом функционирует так же, как TDI. Этот уровень носит название «спецификация драйверов сетевых интерфейсов» (Network Driver Interface Specification – NDIS) и обеспечивает интерфейс между протоколами и сетевыми платами. Как и в случае TDI, уровень NDIS обеспечивает обмен данными между любым стеком протоколов и любыми сетевыми адаптерами, установленными на компьютере. Взаимосвязь сетевых компонентов Windows посредством интерфейсов TDI и NDIS представлена на рис. 3.2.

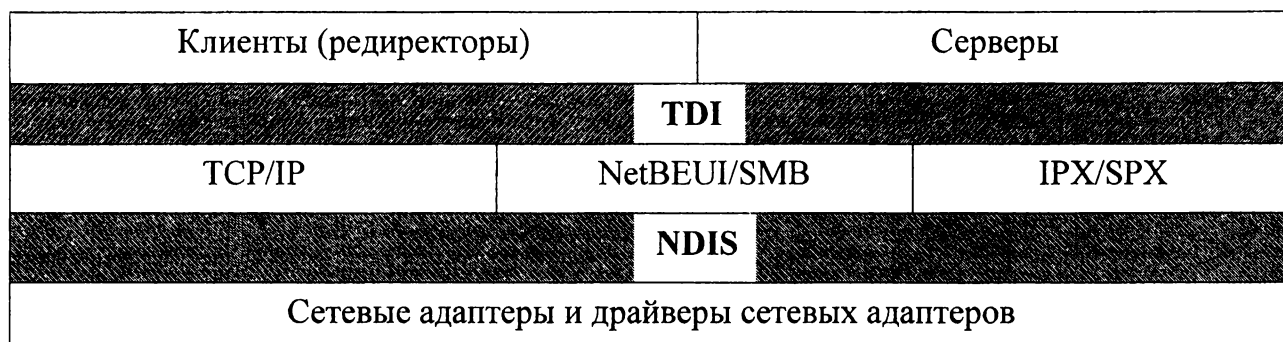


Рис. 3.2. Взаимодействие сетевых компонентов через интерфейсы TDI и NDIS

Спецификация драйверов сетевых интерфейсов – это набор описаний и программного кода, стандартизирующий порядок использования и взаимодействия компонентов разных уровней модели OSI, начиная с физического (канального) и заканчивая транспортным. NDIS подчиняются следующие группы сетевого программного обеспечения:

- *стек протоколов*, который обеспечивает взаимодействие между сетевыми узлами. Он помещает данные в пакеты на стороне отправителя и извлекает их оттуда на стороне получателя;
- *драйвер сетевого адаптера*, который управляет сетевой платой. Он работает на уровне доступа к среде передачи данных, пересылая пакеты от стека протоколов сетевому адаптеру и наоборот;

- менеджер протоколов, который управляет взаимодействием между стеком протоколов и драйвером сетевой платы.
- После изучения данной темы Вы можете перейти к выполнению лабораторной работы 5 «Установка имен компьютеров, служб и протоколов» в лабораторном практикуме «Локальные компьютерные сети».

Резюме

1. Основными компонентами сетевого программного обеспечения являются: сетевые адаптеры и соответствующие им драйверы, сетевые протоколы, клиенты, редиректоры и серверы. Каждый из этих компонентов выполняет свои, строго определенные, функции, обеспечивающие совместное использование ресурсов в КС.
2. TDI представляет собой пограничный уровень между модулями протоколов транспортного уровня, клиентами и интерфейсами приложений. Любой модуль, расположенный над TDI (клиент, интерфейс приложений или сервер), может обмениваться данными с любым модулем протоколов, расположенным под TDI.
3. Для поддержки сетевых протоколов и привязки их к драйверам сетевых плат Windows использует NDIS.

Вопросы для контроля

- 1) На каком уровне модели OSI работает каждый из сетевых компонентов Windows?
- 2) Каковы функции каждого из известных Вам сетевых компонентов Windows?
- 3) Что такое «служба Windows»? Приведите примеры популярных служб Windows.
- 4) Каковы функции службы доступа к файлам и принтерам для сетей Microsoft? для сетей NetWare?
- 5) Каковы функции клиента для сетей Microsoft? для сетей NetWare?
- 6) В чем состоят сходство и различие между службой шлюза для NetWare и клиентской службой для доступа к ресурсам Novell NetWare?
- 7) Перечислите названия стеков протоколов ЛКС, которые поддерживаются ОС Windows?
- 8) Что такое TDI? Какова его роль?
- 9) Что такое NDIS? Какова его роль?

3.2. Стек протоколов NetBEUI/SMB

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами раздела «Стек протоколов NetBEUI/SMB» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».

3.2.1. Общая характеристика

Фирмы Microsoft и IBM совместно работали над сетевыми средствами для персональных компьютеров. Стек протоколов NetBEUI/SMB является продуктом их совместной деятельности.

Он работает на четырех верхних уровнях модели OSI (транспортном, сеансовом, представительском и прикладном).

Стек включает в себя два протокола – NetBEUI и SMB. На рис. 3.3 представлено соответствие стека протоколов NetBEUI/SMB модели OSI.

Модель OSI	NetBEUI/SMB
Прикладной	SMB
Представительский	
Сеансовый	
Транспортный	NetBEUI
Сетевой	–
Канальный	802.3 (Ethernet), 802.5 (Token Ring), Fast Ethernet, Gigabit Ethernet и др.
Физический	

Рис. 3.3. Соответствие стека протоколов NetBEUI/SMB модели OSI

Работа стека протоколов NetBEUI/SMB не зависит от протоколов физического и канального уровней. Поэтому данный стек можно устанавливать в компьютерных сетях, построенных на основе любой из стандартных сетевых технологий ЛКС.

3.2.2. Протокол NetBEUI

Общая характеристика

Расширенный пользовательский интерфейс базовой системы ввода/вывода (NetBIOS Extended User Interface – NetBEUI) – усовершенствованный вариант базовой системы ввода-вывода (Network Basic Input/Output System – NetBIOS), разработанной фирмой IBM еще в 1984 г. Он разрабатывался специально для локальных сетей Ethernet. В связи с

этим он компактен, высокоэффективен, потребляет немного ресурсов. Кроме этого, он ориентирован на использование в своей работе аппаратных адресов сетевых адаптеров.

Вы уже знакомы с тем, что для идентификации компьютеров в сети используется MAC-адресация. Каждой плате сетевого адаптера присваивается уникальный номер, например 11-AD-5B-96-E1-21. Но запоминать и оперировать такими адресами пользователю крайне неудобно. При разработке стека протоколов NetBEUI/SMB в первую очередь выдвигались требования по упрощению реализации, минимизации используемых ресурсов и снижению усилий на администрирование. В связи с этим было предложено использовать вместо MAC-адресов символические имена NetBIOS.

Имена NetBIOS

Имя NetBIOS состоит из символов и цифр. Общая длина такого имени составляет 16 знаков. Оно используется для идентификации сетевого ресурса. Последний, 16-й символ в имени используется Microsoft для идентификации сервисов, предоставляемых компьютером. Имя, которое пользователь присваивает компьютеру во время установки Windows, в действительности является именем NetBIOS – единственным идентификатором компьютера, который необходим протоколу NetBEUI.

Разрешением MAC-адресов в имена NetBIOS (установлением между ними соответствия) занимается один из компьютеров в сети, носящий специальное название – «Master Browser».

☞ *Master Browser – это сетевой компьютер, поддерживающий список компьютеров и услуг, доступный в данной сети, а также распространяющий этот список между другими браузерами.*

Выбор компьютера на роль Master Browser определяется приоритетом ОС, установленной на данном компьютере. Порядок следования ОС в соответствии с ростом их приоритета выглядит следующим образом: Windows 3.11, Windows 9x, Windows NT Workstation, Windows 2000 Professional, Windows XP, Windows NT Server, Windows 2000 Server, Windows 2003 Server.

При включении станция посылает широковещательный пакет¹ с целью определить, какой из компьютеров в рабочей группе является Master Browser. В ответ на ее запрос приходят данные о том, какой из компью-

¹ Пакет, предназначенный всем компьютерам в сети.

теров на данный момент является Master Browser. После получения данных о Master Browser новый компьютер включается в работу сети (происходит распознавание его имени).

Виды имен NetBIOS

Имена NetBIOS бывают двух типов. *Индивидуальные имена*, как правило, используются для взаимодействия с некоторым отдельным компьютером, *групповые* – позволяют объединять компьютеры по некоторому признаку. Например, в одну группу можно включить все компьютеры, установленные в бухгалтерии, в другую – из отдела кадров и т.д. На рис. 3.4 изображена ЛКС, состоящая из 4 компьютеров. Каждому из компьютеров присвоено индивидуальное имя NetBIOS (**comp1**, ..., **comp4**). Все компьютеры сети объединены в группу **Group1**. Теперь запомнить имена всех компьютеров гораздо проще, чем MAC-адреса установленных на них сетевых плат.

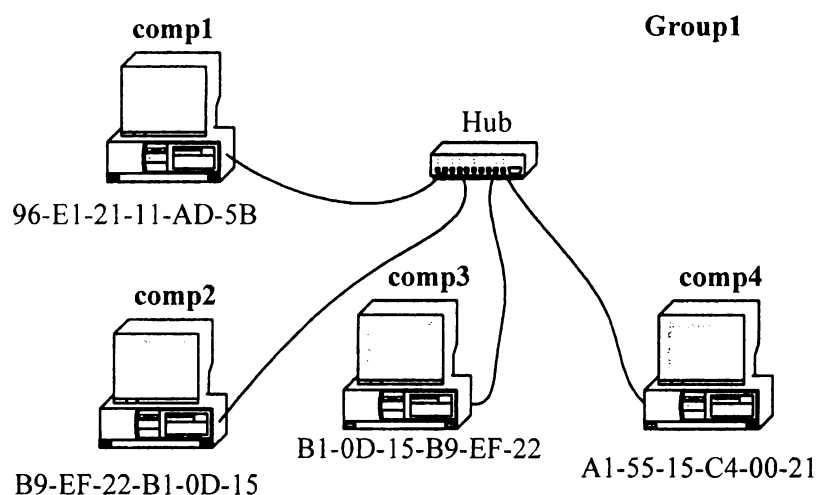


Рис. 3.4. Индивидуальные и групповые имена NetBIOS

Для того чтобы переслать данные компьютеру, MAC-адрес которого 11-AD-5B-96-E1-21, достаточно будет указать только имя – **comp4**, которое пользователю запомнить гораздо легче, чем набор из шести шестнадцатеричных чисел.

Использование MAC-адресации и имен NetBIOS для идентификации компьютеров в сети существенно ограничивает использование стека протоколов NetBEUI в ЛКС¹. Рассмотрим ситуацию, представленную на рис. 3.5.

¹ Он рассчитан на сети, насчитывающие не более 200 рабочих станций.

Для увеличения производительности сервера ЛКС в него была установлена дополнительная сетевая карта. В результате сеть была разбита на две подсети. Пользователи из разных подсетей подключаются к разным концентраторам.

Компьютер **Пользователь1** из одной подсети пытается послать пакет компьютерам **Пользователь2** и **Пользователь3**.

MAC-адреса компьютеров и имена NetBIOS не содержат никакой информации о сетях, которым принадлежат компьютеры. Поэтому протокол NetBEUI не умеет работать с составными сетями, содержащими несколько подсетей. Таким образом, пакет с данными, посланный от компьютера **Пользователь1**, может быть доставлен только компьютеру **Пользователь2**. Пакет, посланный компьютеру **Пользователь3**, находящемуся в другой подсети, будет утерян.

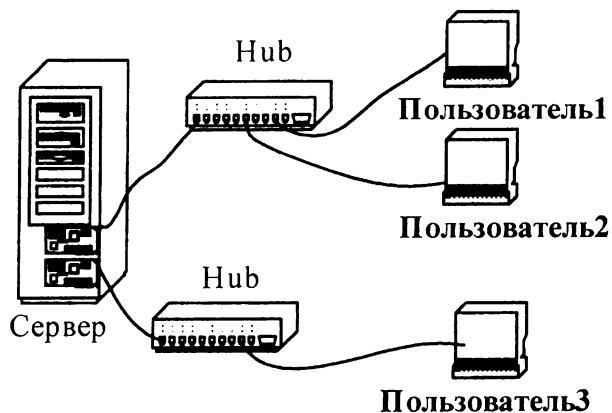


Рис. 3.5. Схема компьютерной сети

Таким образом, протокол NetBEUI не поддерживает маршрутизацию. Если сеть состоит из нескольких сегментов, то данные не могут быть переданы из одного локального сегмента в другой.

Таким образом, протокол NetBEUI не поддерживает маршрутизацию. Если сеть состоит из нескольких сегментов, то данные не могут быть переданы из одного локального сегмента в другой.

3.2.3. Протокол SMB

Блок сообщения сервера (Server Message Block – SMB) – это протокол, который выполняет функции сеансового, представительского и прикладного уровней. Этот протокол используется между компьютерами для общего доступа к файлам, принтерам, файлам электронной почты и пр. SMB является клиент-серверным протоколом типа «запрос–ответ».

Принцип работы SMB достаточно прост: в общем случае клиент посылает запрос, а сервер посылает в ответ запрошенную информацию (рис. 3.6). Исключения составляют случаи, когда клиент пробует получить ресурс в исключительное право доступа, а этот ресурс уже кем-то занят. В этом случае сервер посылает извещение об отказе.

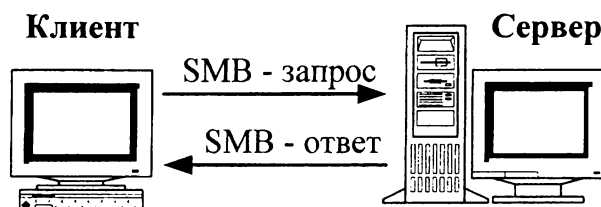


Рис. 3.6. Работа протокола SMB

- После изучения данной темы Вы можете перейти к выполнению лабораторной работы 6 «Мониторинг сети средствами MS Network Monitor», после чего выполнить лабораторную работу 7 «Мониторинг стека протоколов NetBEUI/ SMB» в лабораторном практикуме «Локальные компьютерные сети».

Резюме

1. Стек протоколов NetBEUI/SMB работает на четырех верхних уровнях модели OSI и включает в себя два протокола – NetBEUI и SMB.
2. Каждый протокол, входящий в стек NetBEUI/SMB, выполняет строго определенный набор функций в зависимости от тех уровней модели OSI, на которых он работает.
3. В компьютерной сети, работающей на основе стека протоколов NetBEUI/SMB, для взаимодействия компьютеров наряду с MAC-адресами используются имена NetBIOS.
4. Использование MAC-адресации и имен NetBIOS для идентификации компьютеров в сети существенно ограничивает использование стека протоколов NetBEUI в ЛКС.

Вопросы для контроля

- 1) Каковы преимущества и недостатки использования стека протоколов NetBEUI/SMB?
- 2) Какие протоколы входят в состав стека NetBEUI/SMB?
- 3) На каких уровнях модели OSI работает каждый из протоколов, входящих в состав NetBEUI/SMB?
- 4) Какой способ адресации компьютеров использует протокол NetBEUI? Каковы достоинства и недостатки этого способа?
- 5) Какие функции в компьютерной сети выполняет Master Browser?
- 6) Какова технология выбора в сети Master Browser?
- 7) Какой протокол называется маршрутизированным? Какие преимущества есть у протоколов такого типа?
- 8) Почему протокол NetBEUI не может осуществлять маршрутизацию пакетов в КС?
- 9) Какие функции выполняет протокол SMB?

3.3. Стек протоколов IPX/SPX

После изучения данной темы рекомендуем познакомиться с демонстрационными материалами раздела «Стек протоколов IPX/SPX» электронного пособия «Основы локальных компьютерных сетей: демонстрационные материалы».

3.3.1. Общая характеристика

Стек протоколов IPX/SPX работает на пяти верхних уровнях модели OSI (сетевом, транспортном, сеансовом, представительском и прикладном). На рис. 3.7 представлено соответствие стека протоколов IPX/SPX модели OSI.

Уровни модели OSI	IPX/SPX
Прикладной	NCP, SAP
Представительский	
Сеансовый	
Транспортный	SPX
Сетевой	IPX, RIP, NLSP
Канальный	802.3 (Ethernet), 802.5 (Token Ring), Fast Ethernet, Gigabit Ethernet и др.
Физический	

Рис. 3.7. Соответствие стека протоколов IPX/SPX модели OSI

Работа стека протоколов IPX/SPX не зависит от протоколов физического и канального уровней. Поэтому данный стек можно устанавливать в компьютерных сетях, построенных на основе любой из стандартных сетевых технологий ЛКС.

Стек протоколов IPX/SPX – интеллектуальная собственность фирмы Novell. Благодаря протоколам, которые совместимы с этими протоколами (например, NWLinkIPX/SPX/NetBIOS), их применение не ограничено сетями NetWare¹.

3.3.2. Протоколы сетевого уровня

Протокол IPX

В отличие от NetBEUI Internet-протокол обмена пакетами (Internet Packet Exchange – IPX) является маршрутизируемым. Маршрутизируе-

¹ См. далее общую характеристику стека протоколов NWLink/IPX/SPX/NetBIOS.

мость протокола IPX обеспечивается несколько иной схемой адресации компьютеров, чем в протоколе NetBEUI.

На уровне IPX компьютерам назначаются логические сетевые адреса. IPX-адрес состоит из четырехбайтового (32-битового) сетевого номера и

1C9FDB42 : 2E702A1DAF01

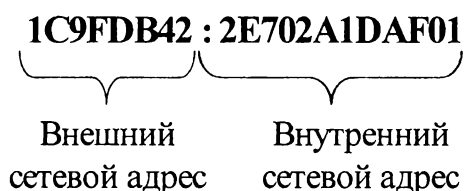


Рис. 3.8. Полный IPX-адрес

шестибайтового (48-битового) узлового номера (рис. 3.8). Сетевой номер, или *внешний сетевой адрес*, идентифицирует физический сегмент, к которому подключен компьютер. Сетевые адреса устанавливаются сетевым администратором на серверах. Внутренний номер, или *внутренний сетевой адрес*, – это аппаратный адрес, что очень удобно, поскольку избавляет от необ-

ходимости транслировать имена, назначенные программными средствами в имена аппаратных средств.

При использовании такой схемы адресации усилия по настройке и управлению сетью сводятся к минимуму.

Адреса IPX могут выдаваться сетевым администратором, но предпочтительней получить зарегистрированный номер сети IPX от Novell. Это позволяет обеспечить уникальность IPX-адресов.

Еще одной важной особенностью протокола IPX является поддержка сокетов (socket).

☞ *Сокет – виртуальная связь между приложением и протоколом, позволяющая нескольким приложениям использовать один и тот же протокол.*

При связывании приложения с определенным сокетом драйвер реализации протокола автоматически распознает пакеты, предназначенные для этого приложения, и напрямую направляет их адресату.

Таким образом, в заголовке пакета, помимо адреса узла и адреса сети, появляется еще идентификатор сокета, на который должен быть отправлен пакет.

Протокол RIP и NLSP

Служебные протоколы: протокол маршрутизации данных (Routing Information Protocol – RIP) и протокол маршрутизации на основании состояния канала (NetWare Link Services Protocol – NLSP) – позволяют автоматизировать процесс настройки и маршрутизации пакетов. Они

«снабжают» маршрутизаторы информацией о принадлежности узла той или иной сети.

Чтобы найти наилучший путь, каждый компьютер в сети с протоколом IPX каждые 60 с средствами протокола RIP передает специальный широковещательный запрос по всем известным каналам. После этого возвращается своеобразное «эхо». По времени задержки эхо-сигнала определяется кратчайший путь, ведущий в заданное место.

Протокол NLSP выполняет те же самые функции, что и RIP, но обновляет таблицу маршрутизации только после изменения конфигурации связей.

Протокол IPX использует информацию, полученную от протоколов RIP и NLSP, для пересылки пакетов в узел назначения или следующему маршрутизатору, предоставляющему путь к узлу назначения.

3.3.3. Протокол SPX

Поскольку IPX не поддерживает обработку ошибок, в некоторых случаях он дополняется средствами протокола последовательного обмена пакетами (Sequenced Packet Exchange – SPX), работающего на транспортном уровне модели OSI. Этот протокол ориентирован на установление соединений. Он гарантирует установление надежного соединения перед отправлением данных по сети. Поскольку протокол SPX обеспечивает корректность работы соединения, то он отвечает и за обработку искаженных пакетов и других ошибок. Таким образом, он обеспечивает связь между узлами сети, исключая любые ошибки. В случае потери или ошибки пакет пересылается повторно. При этом SPX не посылает следующий пакет до тех пор, пока не получит подтверждение получения предшествующего.

3.3.4. Протоколы NCP и SAP

Протокол ядра NetWare (NetWare Core Protocol – NCP) работает на сеансовом, представительском и прикладном уровнях модели OSI.

Он является основным протоколом прикладного уровня в стеке протоколов IPX/SPX. Используется для печати, совместного использования файлов, рассылки сообщений электронной почты и предоставления доступа к каталогам.

NCP представляет собой язык общения серверов и клиентов в среде NetWare. Клиенты передают свои запросы на запись или чтение файлов, на создание очереди заданий, на поиск в дисковых каталогах и т.д. в виде NCP-сообщений. NCP-пакет вкладывается (инкапсулируется) в пакет SPX.

Каждому запросу соответствует отклик, который так же, как и NCP-запрос, вкладывается в SPX-пакет.

Протокол уведомления о службах (Service Advertisement Protocol – SAP) – это протокол объявления об услугах. Серверы сети NetWare используют данный протокол для уведомления всех клиентов сети и других серверов о своем статусе и доступных услугах.

Клиенты также располагают возможностью послать запрос SAP в случае необходимости воспользоваться определенной службой. Их запрос передается по сетевому сегменту. Сервер в данном сетевом сегменте может ответить на этот запрос, передав информацию о степени доступности запрашиваемой службы.

3.3.5. Стек протоколов NWLink/IPX/SPX/NetBIOS

NWLink IPX/SPX/NetBIOS – совместимый с IPX/SPX стек протоколов. NWLink могут использовать клиенты Windows для обращения к клиент-серверным приложениям на серверах Novell NetWare, а также клиенты NetWare для обращения к клиент-серверным приложениям на серверах Windows. NWLink позволяет компьютерам под управлением Windows связываться с другими сетевыми устройствами, например принтерами, использующими IPX/SPX. NWLink можно также применять в малых сетях, где есть только клиенты Microsoft.

Транспортный драйвер NWLink включает протоколы IPX, SPX, RIPX (RIP поверх IPX), NBIPX (NetBIOS поверх IPX)¹ и SAP. SPX обеспечивает надежную доставку, поддерживая порядок следования пакетов и подтверждений. Протокол RIPX выполняет функции протоколов RIP и IPX в стеке протоколов IPX/SPX.

■ После изучения данной темы Вы можете перейти к выполнению лабораторной работы 8 «Мониторинг стека протоколов IPX/SPX» в лабораторном практикуме «Локальные компьютерные сети».

Резюме

1. Стек протоколов IPX/SPX работает на пяти верхних уровнях модели OSI (сетевом, транспортном, сеансовом, представительском и прикладном) и включает в себя шесть протоколов: NCP, SAP, SPX, IPX, RIP и NLSP.

¹ Для этого используются специализированные пакеты. В результате компьютеры получают возможность обмениваться данными, используя индивидуальные и групповые имена NetBIOS.

2. Протоколы в стеке протоколов IPX/SPX выполняют функции, закрепленные за теми уровнями модели OSI, на которых они работают.
3. В отличие от NetBEUI, IPX является маршрутизируемым.
4. На уровне IPX компьютерам назначаются логические сетевые адреса. IPX-адрес состоит из сетевого и узлового номеров. Такая адресация обеспечивает маршрутизируемость протокола IPX.
5. NWLinkIPX/SPX/NetBIOS – совместимый с IPX/SPX стек протоколов. Он включает протоколы IPX, SPX, RIPX, NBIPX и SAP.

Вопросы для контроля

- 1) Каковы преимущества и недостатки использования стека протоколов IPX/SPX?
- 2) На каких уровнях модели OSI работает каждый из протоколов, входящих в состав IPX/SPX?
- 3) Какой способ адресации компьютеров использует протокол IPX? Каковы достоинства и недостатки этого способа?
- 4) Какие протоколы входят в состав стека IPX/SPX? Дайте краткую характеристику каждого из них.
- 5) С какой целью был разработан стек протоколов NWLink/IPX/SPX? Каковы его преимущества?
- 6) Назовите общие и отличительные характеристики стеков протоколов NWLink/IPX/SPX и IPX/SPX.

3.4. Построение одноранговой сети

3.4.1. Подходы к управлению сетевыми ресурсами

Посредством ЛКС в систему объединяются персональные компьютеры, расположенные на многих удаленных рабочих местах, которые используют совместно оборудование, программные средства и информацию. Рабочие места сотрудников перестают быть изолированными и объединяются в единую систему.

Концепция равного доступа ко всем ресурсам сети со стороны каждого пользователя не отвечает насущным задачам. Представьте, например, последствия передачи в совместное использование каталога с бухгалтерской документацией. По этой причине в ЛКС используют специальные механизмы, позволяющие ограничить доступ к общим ресурсам сети.

Управление сетевыми ресурсами средствами Windows 9x

Первоначально для ограничения доступа к ресурсу использовалась следующая схема:

- 1) Ресурс, каталог или принтер, выделяется в сеть под определенным именем.
- 2) Для каждого режима доступа к ресурсу назначается определенный пароль.
- 3) При обращении к ресурсу пользователь предъявляет пароль и получает соответствующий ему уровень доступа.

Если для ресурса не устанавливался пароль, то любой пользователь получал доступ к этому ресурсу. Если пароль был установлен, но пользователь не предъявил его или предъявил неправильный пароль, то в доступе отказывалось совсем.

Таким образом, пользователю сети было необходимо знать и помнить некоторое множество паролей к используемым им ресурсам.

Это, естественно, было сложно, и забывчивость пользователей оборачивалась частыми простоями из-за невозможности подключения к ресурсу, что побуждало пользователя записывать пароли на бумажках и, как следствие, вело к снижению защищенности систем.

Для решения данной проблемы был предложен профиль пользователя (user profile).

☞ *Профиль пользователя – это набор персональных данных, настроек и параметров работы компьютера, связанных с определенным пользователем.*

Профиль пользователя в Windows 9x содержал:

- список каталогов, где пользователь хранил свои документы;
- список сетевых ресурсов и паролей к ним;
- настройки параметров экрана, шрифтов, цветовых гамм и т.д.;
- список программ, с которыми работает пользователь.

Таким образом, пользователь избавлялся от необходимости каждый раз при подключении к сетевому каталогу вводить пароль – система сама извлекала его из его профиля.

Сам профиль представлял собой набор файлов и каталогов, внутри которых и хранилась вся информация, связанная с пользователем.

Однако на одном компьютере в разное время могли работать разные люди, стало быть, необходимо было хранить несколько профилей и уметь определять их принадлежность.

Управление сетевыми ресурсами средствами Windows 2000/XP/2003

Следующим шагом в облегчении управления сетью стало использование сетевых имен пользователей (*user name*, *logon name*) для определения режима доступа к сетевым ресурсам.

☞ *Сетевое имя пользователя – символическое имя, идентифицирующее пользователя в сети.*

Для сохранения конфиденциальности информации наряду с сетевым именем пользователю назначался персональный *пароль (user password)*, при помощи которого производили аутентификацию пользователя и шифрование конфиденциальных данных в его *профиле*.

Сетевое имя пользователя, его пароль и профиль объединили в новом понятии «учетная запись пользователя (*user account*)».

Для удобства администрирования пользователей стали объединять в группы, которым и присваивают права доступа к сетевым ресурсам. Для этого создаются *учетные записи групп пользователей*. Каждая учетная запись пользователя может быть включена в состав нескольких учетных записей групп пользователей.

Администратор, создавая и группируя учетные записи и наделяя их разными правами, обеспечивает более высокую защиту данных.

Соотношение между сетевым именем, паролем, профилем и учетными записями проиллюстрировано на рис. 3.9.

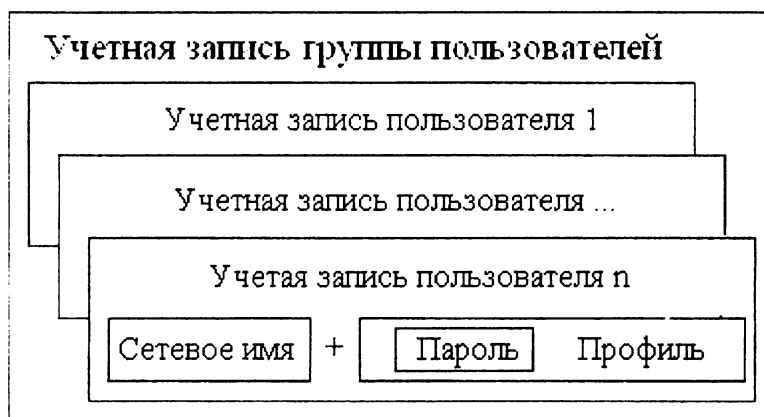


Рис. 3.9. Взаимосвязь понятий «сетевое имя», «пароль», «профиль», «учетная запись пользователя», «учетная запись группы пользователей»

3.4.2. Классификация ЛКС

С точки зрения администрирования ЛКС можно выделить следующие типы ЛКС:

- одноранговые;
- с централизованным управлением.

Как уже говорилось ранее, компьютер – владелец ресурса проводит идентификацию пользователя по паролю доступа к ресурсу или по его учетной записи. Во втором случае необходимо, чтобы на всех компьютерах присутствовали учетные записи всех пользователей.

Такой подход используется в *одноранговых сетях*: каждый компьютер имеет локальную для него базу данных, содержащую пароли доступа или учетные записи пользователей, по которым он определяет режим использования ресурса.

В *сети с централизованным управлением* база данных едина для всей компьютерной сети.

В рамках данного учебного пособия мы рассматриваем принципы построения только одноранговых ЛКС.

Сети с централизованным управлением подробно рассматриваются в учебном пособии «Основы корпоративных сетей»¹.

3.4.3. Построение одноранговой сети на основе Windows 9x

В ОС Windows 9x, как уже говорилось ранее, применяется простейший подход к управлению доступом к сетевым ресурсам – режим доступа определяется паролем. Кроме этого, используется и профиль пользователя. Файл, содержащий этот список, находится в корневом каталоге Windows; имя сетевого профиля определяется как сетевое имя пользователя с добавлением к нему расширения **.pwl**, (например, **ivanov.pwl**).

В начале работы пользователь должен ввести имя и пароль, после чего система загрузит его профиль. При обращении к ресурсу система ищет соответствующий ему пароль в **pwl**-файле пользователя и автоматически передает его на другой компьютер.

Для построения одноранговой сети на основе Windows 9x необходимо выполнить следующие шаги:

- 1) Установить на всех компьютерах сетевые адаптеры и соответствующие им драйверы.
- 2) Установить сетевые протоколы. Если необходимо, настроить привязки протоколов к сетевым платам. По умолчанию, одновременно с установкой драйвера сетевой карты и сетевого протокола автоматически устанавливается служба «Клиент для сетей Microsoft».
- 3) Установить на компьютерах, которые будут предоставлять свои ресурсы в сеть (каталоги и принтеры), службу доступа к файлам и принтерам для сетей Microsoft. Если необходимо, то настроить привязки протоколов к сетевым службам.
- 4) Выделить ресурсы в сеть (открыть к ним общий доступ), назначив им имена и пароли на разные уровни доступа.
- 5) Настроить сетевую печать.
- 6) На рабочих местах пользователей настроить вход в операционную оболочку с предъявлением пароля и убедиться, что созданы необходимые профили пользователей.
- 7) Для каждого профиля пользователя создать необходимые подключения к сетевым дискам, убедившись, что пароли доступа сохранены в профиле пользователя.

¹ Данное учебное пособие готовится к выпуску в издательстве РГППУ.

■ После изучения данной темы Вы можете перейти к выполнению заданий темы «Построение одноранговой сети в Windows 9x» лабораторной работы 9 «Построение одноранговой сети средствами MS Windows» в лабораторном практикуме «Локальные компьютерные сети».

3.4.4. Одноранговые сети на основе Windows 2000/XP/2003

Управление сетевыми ресурсами

Несмотря на то что ОС Windows 2000/XP/2003 рассчитаны на создание сети с централизованным управлением, на их основе можно построить и одноранговую сеть, обеспечивающую взаимодействие с компьютерами предыдущих версий Windows. Подходы в построении такой сети значительно отличаются от сети на основе Windows 9x.

Одним из многих преимуществ ОС Windows 2000/XP/2003 перед Windows 9x является возможность надежной защиты ресурсов. Эти ОС позволяют защитить любой каталог и любой отдельный файл, предоставив права доступа к нему дифференцированно различным группам пользователей.

Эти ОС позволяют организовать защиту данных на сетевом уровне (при обращении к ним с удаленного компьютера). Дополнительно на томах NTFS может быть настроен доступ к ресурсу на файловом уровне (при работе пользователя на локальном компьютере).

Для гибкой настройки прав доступа в Windows 2000/XP/2003 существуют локальные службы безопасности: служба управления учетными записями (Security Account Manager – SAM) и локальная служба безопасности (Local Security Authority – LSA). Эти службы производят идентификацию пользователя при входе в систему и контролируют практически все его действия в ходе работы.

Для каждой учетной записи пользователя в системе устанавливаются права на запуск приложений, доступ к файлам и каталогам, возможность конфигурировать параметры системы и т.д.

Для удобства администрирования пользователей объединяют в группы, которым и присваивают права. Каждая учетная запись пользователя может быть включена в состав нескольких групп.

Существуют несколько встроенных групп и встроенных учетных записей пользователей, представленных в табл. 3.1.

Таблица 3.1

Перечень встроенных учетных записей пользователей и групп пользователей в Windows 2000/XP/2003

Пользователь/ группа	Характеристика
<i>Встроенная учетная запись пользователя</i>	
Администратор (Administrator)	Обладает правом практически полного контроля системы, а также возможностью создавать новые группы и пользователей
Гость (Guest)	Практически полностью бесправный пользователь, по умолчанию эта учетная запись заблокирована (не используется)
<i>Встроенная учетная запись группы пользователей</i>	
Администраторы (Administrators)	Все члены группы администраторов компьютера обладают правами администратора
Пользователи (Users)	Члены этой группы обладают ограниченным набором прав по запуску приложений и конфигурации компьютера, которые необходимы для ежедневной работы
Опытные пользователи (Power users)	Члены этой группы обладают несколько расширенным набором прав, достаточным для подключения некоторых устройств и их конфигурации
Гости (Guests)	Члены этой группы – случайные пользователи, которые не имеют учетных записей на компьютере
Операторы архива (Backup Operators)	Члены этой группы имеют право на создание архивов и восстановление системы
Операторы печати (Print Operators)	Члены этой группы имеют право создавать, удалять и управлять общими точками печати на серверах печати

В некоторых случаях при определении прав доступа к каталогам, файлам и сетевым ресурсам полезно использовать следующую встроенную псевдогруппу и следующих псевдопользователей:

- **Система (System)** – представляет собой учетную запись, от имени которой действует собственно ОС на данном компьютере.
- **Владелец создатель (Creator owner)** – псевдоним учетной записи пользователя, от имени которого был создан объект.

- **Все (Everyone)** – все пользователи, в том числе и не опознанные системой, предъявившие неверный пароль и т.д. – буквально «все на свете».

Разрешение общих ресурсов

В начале работы пользователь обязан ввести имя и пароль, которые проверяются в локальной системе безопасности.

При подключении к сетевому ресурсу компьютеру – владельцу ресурса автоматически посылается текущее имя и пароль пользователя, тот проверяет его в собственной локальной базе учетных записей и, при успешной идентификации, в дальнейшем использует данные именно из локальной базы.

Разрешения на доступ к общей папке назначаются учетным записям пользователей и учетным записям групп пользователей.

У общей папки всего три разрешения, описанных в табл. 3.2.

Таблица 3.2

Разрешения общих папок

Разрешение	Возможности
Чтение (Read)	Просматривать имена и содержимое файлов и подпапок, входить в подпапки и запускать программы
Изменение (Change)	Создавать в папке файлы и подпапки, изменять содержимое файлов, удалять подпапки и файлы, а также выполнять все действия, доступные при наличии разрешения Read (Чтение) . Не имеет полномочий изменять существующий вид доступа
Полный доступ (Full Control)	Изменять разрешения файла (только NTFS), а также выполнять все действия, доступные при наличии разрешения Change (Изменение)

К наиболее важным характеристикам разрешений общих ресурсов относят следующие:

- разрешения применяются только к общей папке целиком, а не к входящим в нее файлам и подпапкам;
- для вновь созданного общего ресурса по умолчанию назначается разрешение **Полный доступ (Full Control)** для группы **Everyone (Все)** в ОС Windows 2000 и **Чтение (Read)** для группы **Everyone (Все)** в ОС Windows XP/2003;

- разрешения общей папки не ограничивают доступ к ней пользователей, работающих на том компьютере, где она хранится. Они применяются только к пользователям, которые подключаются к папке через сеть;
- разрешения общей папки – единственный способ защитить информацию на томах FAT и FAT 32 в любой из ОС Windows.

Разрешения NTFS

Администратор может управлять доступом пользователей к каталогам и файлам в разделах диска, отформатированных под файловую систему NTFS.

Для защиты файла или папки необходимо установить для него разрешение.

☞ *Разрешение NTFS – это набор правил, сопоставленных с файлами и папками и определяющих, какие пользователи и с какими ограничениями могут получить доступ к объекту.*

Создав на компьютере с Windows 2000/XP/2003 общие ресурсы, сетевой администратор с помощью разрешения NTFS определяет, какие пользователи и группы имеют доступ к файлам и папкам локального ресурса и что они могут делать с их содержимым¹.

Разрешения NTFS применяются только на томах NTFS и не действуют на томах, отформатированных под FAT или FAT 32.

Система безопасности NTFS работает как при доступе к файлам и папкам того компьютера, на котором они расположены, так и через сеть.

В табл. 3.3 перечислены основные разрешения NTFS для папок и файлов, а также права доступа, которые они представляют.

Очевидно, что одни режимы включают другие, например режим **Изменение** включает в себя режимы **Чтение** и **Запись**.

Права доступа могут устанавливаться как для папок, так и для файлов, в этом случае они немного различаются по смыслу.

Обычно права доступа наследуются от папки к подпапке, но могут быть установлены индивидуально.

Определение режима доступа к ресурсу

Для каждого режима доступа может быть установлено три варианта значения: **Разрешить**, **Запретить** и **Не установлен**. Режим может быть установлен для учетной записи как пользователя, так и группы.

¹ Такими же правами обладают члены групп **Операторы архива** и **Опытные пользователи**.

Таблица 3.3

Стандартные разрешения NTFS для папок и файлов

Разрешение	Возможности
Полный доступ (Full Control)	Менять разрешения на доступ к папке, удалять подпапки и файлы, а также выполнять действия, обеспечиваемые всеми другими разрешениями NTFS для папок
Изменение (Modify)	Удалять папку, а также выполнять все действия, обеспечиваемые разрешениями на запись, чтение и выполнение
Чтение и выполнение (Read&Execute)	Перемещаться по папке для доступа к другим файлам и папкам, даже если пользователь не имеет права на доступ к этим папкам, а также выполнять все действия, предоставляемые разрешениями на чтение и просмотр содержимого папки. Позволяет выполнять приложения в управляемой папке и во всех вложенных папках
Список содержимого папки (List Folder Contents)¹	Просматривать имена файлов и подпапок папки
Чтение (Read)	Просматривать содержащиеся в папке файлы и подпапки, а также ее свойства (имя владельца, разрешения и атрибуты файловой системы)
Запись (Write)	Создавать в папке новые файлы и подпапки, изменять атрибуты папки, а также просматривать имя ее владельца и тип разрешения
Запретить (Deny)	Запрещать все ранние разрешения

☞ При определении результирующего режима доступа на файловом (сетевом) уровне для пользователя действуют следующие правила:

- Из всех режимов доступа, установленных для учетных записей групп и персонально для пользователя, берется режим, определяющий наиболее широкие возможности. Например, из вариантов **Чтение** и **Изменение** будет выбран режим **Изменение**.
- Разрешения накапливаются. Например, если пользователю предоставлено разрешение **Чтение** на основании его принадлежности к группе с

¹ Данное разрешение определено только для папок.

полномочием **Чтение** и одновременно он является членом группы с разрешением **Чтение и выполнение**, то итоговое разрешение Пользователя – **Чтение и выполнение**.

- Если на каком-либо этапе установлено значение режима **Запретить**, этот режим имеет абсолютный приоритет.
- Если в результате не определено ни одно значение для режима доступа, принимается режим **В доступе отказано**.

Файловая система NTFS проверяет режим доступа непосредственно для объекта доступа.

Пусть, например, пользователю был запрещен доступ к папке, но был разрешен доступ к файлу внутри этой папки. При попытке «спуститься» по дереву папок пользователь не сможет открыть файл, но если он напрямую укажет полный путь к файлу (UNC-имя ресурса¹), то проблем не возникнет.

В первом случае LSA была осуществлена проверка доступа к объекту «папка», а во втором к объекту «файл».

Комбинирование прав доступа к ресурсу

В Windows 2000/XP/2003 существует возможность гибко задавать режимы доступа к файлам и папкам при обращении к ним по сети, используя комбинации разрешений доступа к сетевому ресурсу и разрешения доступа на уровне файловой системы.

☞ Для определения прав доступа к ресурсу выполняют следующие действия:

- Определяется результирующий доступ к ресурсу по сети исходя из комбинаций режимов доступа для групп, куда входит пользователь, и индивидуальной учетной записи пользователя – берется режим с наибольшими правами доступа.
- Определяется результирующий режим доступа к объекту на уровне файловой системы: из всех комбинаций режимов доступа «группа/пользователь» выбирается режим с наибольшими правами доступа.
- Из результатов применения двух предыдущих правил выбирается режим с наименьшими правами доступа.

¹ См. п. 3.1.1. «Сетевые компоненты: общая характеристика».

- ☞ *Обратившись к приложению данного учебного пособия, Вы можете познакомиться с несколькими примерами, иллюстрирующими применение правил комбинирования прав доступа к ресурсу через сеть и на уровне файловой системы.*

Вложенные сетевые ресурсы

При определении режима доступа к вложенному сетевому ресурсу также действует принцип проверки режима непосредственно для объекта.

Рассмотрим пример. Пусть каталог верхнего уровня **Ресурс 1** выделен как один сетевой ресурс, а один из его подкаталогов, **Ресурс 2**, выделен как другой сетевой ресурс (рис. 3.10). В результате режим доступа к каталогу **Данные** будет различаться в зависимости от того, как пользователь произвел подключение по сети.

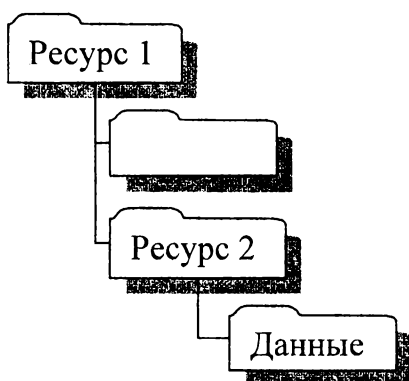


Рис. 3.10. Иерархия расположения общих ресурсов

Допустим, для учетной записи **Иванов** установлены следующие режимы доступа по сети: **Ресурс 1 – Чтение**, **Ресурс 2 – Изменение**.

Если **Иванов** подключился по сети к ресурсу **Ресурс 1**, а затем по дереву папок спустился до ресурса **Данные**, то он сможет лишь читать содержимое папки и файлов, хранящихся в ней. Если же он подключится к ресурсу **Ресурс 2**, то он сможет изменять и удалять содержимое папки **Данные**, включая файлы и подпапки.

- ☞ *Использование вложенных сетевых ресурсов не рекомендуется, так как это запутывает и усложняет контроль доступа к информации.*

Порядок построения ОЛКС

Для построения одноранговой сети на основе Windows 2000/XP/2003 необходимо выполнить следующие действия:

- 1) Установить на всех компьютерах сетевые адаптеры и соответствующие им драйверы.
- 2) Настроить необходимые протоколы и сетевые службы. Установить привязки сетевых служб к протоколам, а протоколов к сетевым картам.
- 3) На всех компьютерах сети создать необходимые учетные записи пользователей, учитывая, что для пользователя необходима учетная запись с одинаковым именем и паролем как на рабочем месте, так и на

всех компьютерах, ресурсы которых он планирует использовать по сети. Включить созданные учетные записи в необходимые группы пользователей.

- 4) На компьютерах создать сетевые ресурсы, определить к ним режимы доступа по сети и на уровне файловой системы для соответствующих групп пользователей и/или индивидуально для учетных записей пользователей.
- 5) Настроить сетевую печать.

■ После изучения данной темы Вы можете перейти к выполнению заданий темы «Построение одноранговой сети в Windows 2000/XP/2003» лабораторной работы 9 «Построение одноранговой сети средствами MS Windows» в лабораторном практикуме «Локальные компьютерные сети».

3.4.5. Сетевая печать

После изучения данной темы рекомендуем познакомиться с презентацией «Организация сетевой печати в среде Windows», расположенной в файле **Сетевая печать\Сетевая печать.ppt**.

Технологии печати в Windows

☞ Введем несколько определений, которыми мы будем пользоваться при дальнейшем изложении материала:

- *Устройство печати (print device)* – физическое устройство печати¹.
- *Сервер печати (print server)* – компьютер, который получает документы от клиентов и пересылает их на принтер.
- *Драйвер принтера (printer driver)* – это программный интерфейс между операционной системой и устройством печати.

ОС семейства Windows для организации печати могут использовать две различные технологии – прямую печать и спулинг.

При *прямой печати* приложение, инициирующее печать, последовательно передает задание непосредственно на принтер. В случае, когда печатается несколько листов, это может занять достаточно много времени, в течение которого приложение не выполняет никакой другой работы. Данную технологию использовали первые версии ОС Windows.

¹ Устройство печати, как правило, называют просто принтером.

При использовании технологии *спулинга* (*spooling*) приложение формирует задание на печать, передает его специальной системной службе – спулеру (*spooler*) и продолжает свою работу в обычном режиме.

☞ *Процесс временного хранения работ, предназначенных для печати, на жестком диске носит название буферизации (spooling).*

Спулер формирует из полученных заданий очередь. Выбрав первое задание из очереди, он начинает передавать его драйверу принтера. По завершению обработки одного задания он приступает к следующему и так далее, пока очередь не закончится.

Пользователь имеет возможность отменить задание или переместить его вверх или вниз по очереди.

Очередь физически представляет собой набор файлов, хранящихся на диске. Возможна ситуация переполнения диска, в этом случае новые задания приниматься к печати не будут.

На стороне клиента тоже организуется очередь печати, куда помещаются задания на печать от локальных приложений.

Далее задания на печать отправляются по сети на сервер печати. При этом если на сервере переполнена очередь, то задание остается в локальной очереди на печать.

Все версии ОС Windows, начиная с 9x, используют технологию спулинга.

Сетевая печать в Windows 2000/XP/2003

Наряду со стандартными возможностями по организации сетевой печати Windows 2000/XP/2003 предоставляет расширенные возможности по организации сетевой и локальной печати. Это стало возможным благодаря использованию логических принтеров (*logical printer*).

☞ *Логический принтер – программное обеспечение, реализующее интерфейс доступа и управления устройством печати.*

Логический принтер контролирует различные аспекты процесса печати, например определяет, куда будет послан документ, отправленный на печать, – в локальный порт, файл или на удаленный общий ресурс печати.

Приложения посылают задания печати логическому принтеру, а тот направляет их уже конкретному физическому печатающему устройству, которое может быть подключено как к локальной машине, так и к серверу печати, расположенному где-то в сети.

Существование логических принтеров позволяет создавать различные конфигурации печати, предназначенные для обслуживания одного физического принтера.

На рис. 3.11 представлен самый простой случай – использование одного логического принтера для работы одного устройства печати.



Рис. 3.11. Один логический принтер – одно устройство печати

Очень часто при совместном использовании принтера требуется напечатать документ какого-то пользователя или группы пользователей немедленно и обойти документы, ожидающие своей очереди на устройстве печати. Это можно сделать, создав несколько логических принтеров для одного устройства печати и назначив им различные уровни приоритета. Если два принтера связаны с одним устройством печати, первыми будут печататься документы, направленные на логический принтер с самым высоким уровнем приоритета (рис. 3.12).

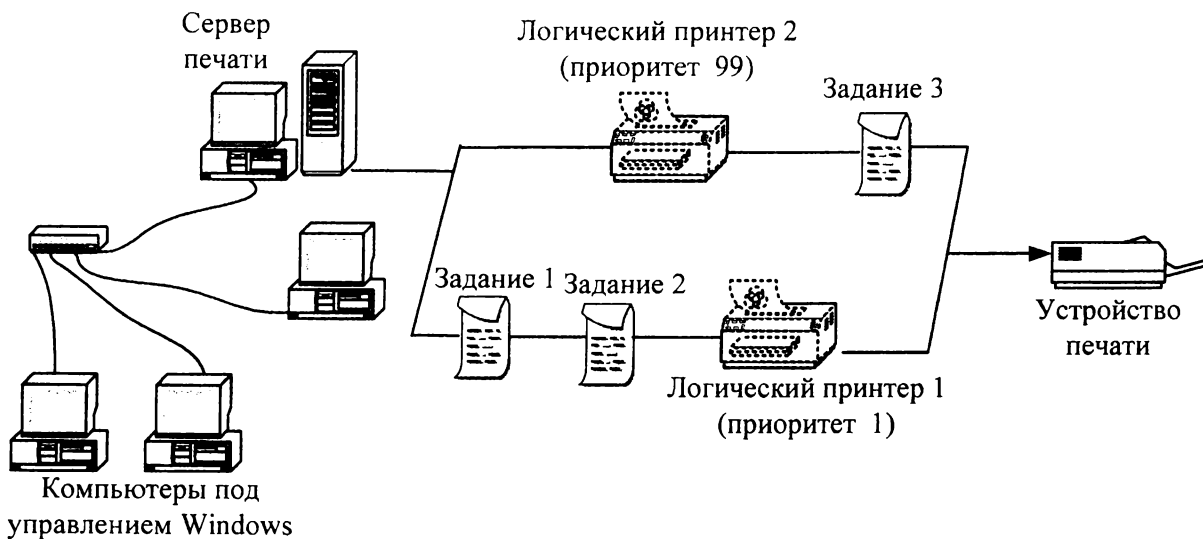


Рис. 3.12. Несколько логических принтеров – одно устройство печати

Большие возможности по оптимизации сетевой печати предоставляет использование пула принтеров.

☞ Пул принтеров состоит из двух или больше идентичных устройств печати, связанных с одним логическим принтером.

Подобная схема максимизирует использование устройств печати и уменьшает время ожидания пользователем печати своего документа. Использование логического принтера для организации пула принтеров изображено на рис. 3.13.

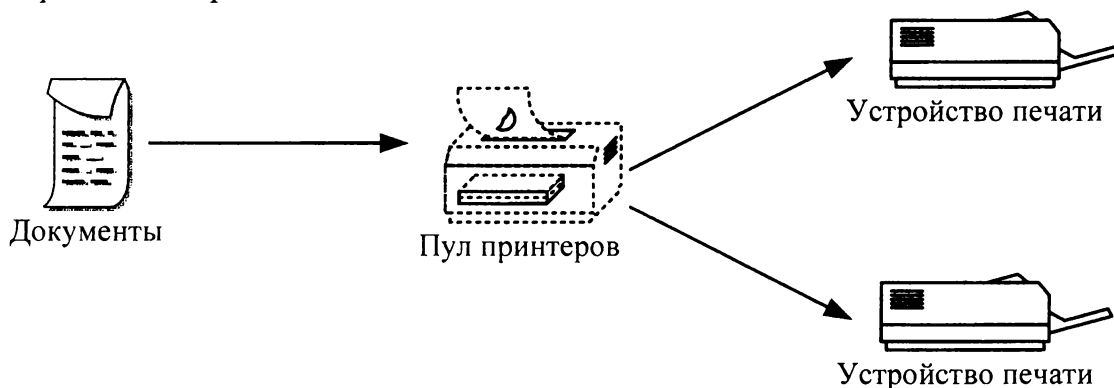


Рис. 3.13. Организация пула принтеров

Можно выделить основные характеристики пула принтеров:

- 1) Все устройства в пуле должны быть одной модели и функционировать как одно устройство. Все установки параметров печати относятся ко всему пулу.
- 2) Порты принтера могут быть одного или разных типов (параллельные, последовательные или сетевые).
- 3) Когда пул принтеров получает документ, диспетчер очереди печати проверяет состояние физических устройств печати, чтобы определить, которое из них свободно.
- 4) Если одно устройство внутри пула останавливает печать, например, когда в нем кончается бумага, это задержит только один документ, посланный на данное устройство печати. Другие документы продолжают печататься на других устройствах пула, в то время как задержанный документ ждет, пока нефункционирующее устройство не будет исправлено или пока он не будет послан на печать заново.

Администрирование принтеров

К задачам администрирования принтеров в ОС Windows 2000/XP/2003 относятся действия по управлению принтерами, а именно:

- определение прав доступа к сетевому принтеру;
- изменение параметров настройки сетевой печати;
- управление серверами печати;
- управление документами, передаваемыми на сервер печати;
- приостановка, возобновление, отмена печати.

Все пользователи КС по умолчанию имеют право выводить документы на печать. Управлять принтерами и серверами печати могут члены групп **Администраторы, Операторы печати, Операторы сервера, Опытные пользователи**, а также **Владелец-создатель**. Этот список групп устанавливается в Windows по умолчанию и может быть изменен посредством *базовых разрешений для принтеров*.

Базовые разрешения для принтеров позволяют ограничить круг лиц, обладающих правами на администрирование принтера и определить уровень их доступа, включая управление принтерами и документами, выводимыми на печать.

В Windows 2000/XP/2003 три уровня разрешений для принтеров:

- 1) печать;
- 2) управление документами;
- 3) управление принтерами.

Каждый из этих уровней определяет набор базовых разрешений, представленных в табл. 3.4.

Таблица 3.4

Базовые разрешения для принтеров

Уровень доступа	Набор разрешений		
	Печать	Управление документами	Управление принтерами
1	2	3	4
Печать документа	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Приостановка, возобновление, повтор и отмена печати пользователем отосланного на печать документа.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Подключение к принтеру	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Управление параметрами заданий печати для всех документов	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Приостановка, возобновление печати документов других пользователей	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Отмена печати всех документов	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Совместное использование принтера	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Окончание табл. 3.4

1	2	3	4
Изменение свойств принтера	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Удаление принтера	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Изменение разрешений принтера	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

■ После изучения темы Вы можете перейти к выполнению лабораторной работы 10 «Настройка сетевой печати в MS Windows» в лабораторном практикуме «Локальные компьютерные сети».

Резюме

1. Концепция равного доступа ко всем ресурсам сети со стороны каждого пользователя часто не отвечает насущным задачам работы в ЛКС. По этой и многим другим причинам в ЛКС используют специальные механизмы, позволяющие ограничить доступ к общим ресурсам сети.
2. С точки зрения администрирования компьютерные сети можно разбить на два типа: одноранговые и с централизованным управлением.
3. Для ограничения доступа пользователей к сетевым ресурсам могут быть использованы система паролей или учетные записи.
4. ОЛКС значительно отличаются от сети на основе Windows 9x и Windows 2000/XP/2003. Последняя из перечисленных ОС позволяет защитить любой каталог и любой отдельный файл, предоставив права доступа к нему дифференцированно различным группам пользователей.
5. ОС Windows 9x и Windows 2000/XP/2003 позволяют организовать защиту данных на сетевом уровне. Дополнительно на томах NTFS в Windows 2000/XP/2003 может быть настроен доступ к ресурсу на уровне файловой системы.
6. Использование принтеров – это одна из главных причин организации локальных компьютерных сетей.
7. Операционные системы Windows 9x и Windows 2000/XP/2003 для организации сетевой печати используют технологию спулинга.
8. Наряду со стандартными возможностями по организации сетевой печати, которые есть в Windows 9x, Windows 2000/XP/2003 предоставляет расширенные возможности по организации сетевой и локальной печати. Для этого используются логические принтеры.

Вопросы для контроля

- 1) Зачем в компьютерной сети разграничивают права доступа к сетевым ресурсам?
- 2) Какие подходы к ограничению доступа к сетевым ресурсам Вам известны? Какие достоинства и недостатки имеет каждый из них?
- 3) Что такое «профиль пользователя», «сетевое имя пользователя», «учетная запись пользователя», «учетная запись группы пользователей»?
- 4) В чем состоит принципиальное отличие одноранговых сетей от сетей с централизованным управлением?
- 5) Какой подход к управлению доступом к сетевым ресурсам используется в Windows 2000/XP/2003? В чем состоит его преимущество по сравнению с тем, который используется в Windows 9x?
- 6) Какие встроенные учетные записи пользователей и групп пользователей в Windows 2000/XP/2003 Вам известны? Дайте общую характеристику каждой из них.
- 7) Какие разрешения общих ресурсов, используемые в Windows 2000/XP/2003, Вам известны?
- 8) Какие разрешения NTFS, используемые в Windows 2000/XP/2003, Вам известны?
- 9) Какие общие правила комбинирования прав доступа к сетевому ресурсу на сетевом и файловом уровнях Вам известны? Приведите примеры их использования.
- 10) Каковы принципы определения режима доступа к вложенному сетевому ресурсу? Приведите примеры их использования.
- 11) Для чего в Windows 2000/XP/2003 используются встроенные псевдопользователи и псевдогруппы?
- 12) Какова последовательность развертывания одноранговой сети средствами Windows 9x? Windows 2000/XP/2003?
- 13) Какие технологии печати, использующиеся в ОС Windows, Вам известны? Дайте краткую характеристику каждой из них.
- 14) Что такое «устройство печати», «логический принтер», «драйвер принтера», «сервер печати»?
- 15) Перечислите способы сочетания логических принтеров и устройств печати, которые используются в Windows 2000/XP/2003. Каковы преимущества и ограничения каждого из них?
- 16) Перечислите основные этапы настройки сетевой печати в Windows 2000/XP/2003.

Заключение

В результате работы с данным учебным пособием Вы познакомились:

- с основными понятиями и определениями, связанными с КС, имеющими важное значение для понимания принципов построения и функционирования ЛКС;
- принципами построения ЛКС на основе стандартных технологий;
- основным сетевым оборудованием ЛКС и принципами его работы;
- принципами взаимодействия компьютеров в ЛКС на основе стеков протоколов NetBEUI/SMB, IPX/SPX и NWLinkIPX/SPX/NetBIOS;
- с принципами построения одноранговых ЛКС и организации сетевой печати средствами ОС Windows.

Для лучшего закрепления материала рекомендуем сочетать его изучение с выполнением заданий лабораторного практикума «Локальные компьютерные сети».

Далее Вы можете перейти к изучению материалов программно-методических комплексов «Основы глобальных компьютерных сетей», «Глобальная компьютерная сеть Internet» и «Корпоративные компьютерные сети»¹.

¹ Перечисленные программно-методические комплексы готовятся к выпуску в издательстве РГППУ.

Список рекомендуемой литературы

Основной

Вычислительные системы, сети и телекоммуникации /В.Л. Бройдо. – СПб.: Питер, 2002. – 688 с.

Информатика: Учеб. 3-е изд., перераб /Под ред. Н.В. Макаровой. – М.: Финансы и статистика, 2005. – 768 с.

Компьютерные сети: Принципы, технологии, протоколы /В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2001. – 672 с.

Математика и информатика: Учеб. пособие для студентов пед. вузов /Под ред. В.Д. Будаева, Н.Л. Стефановой. – М.: Высш. шк., 2004. – 349 с.

Могилев А.В. Информатика: Учеб. пособие для студентов пед. вузов. – 3-е изд., перераб. и доп. – М.: Изд. центр «Академия», 2004. – 848 с.

Основы современных компьютерных технологий: Учеб. /Под ред. А.Д. Хомоненко. – СПб.: КОРОНА принт, 2005. – 672 с.

Пятибратов А.П. и др. Вычислительные системы, сети и телекоммуникации: Учеб. – 2-е изд., перераб. и доп. – М.: Финансы и статистика, 2002. – 512 с.

Дополнительной

Гук М. Аппаратные средства локальных сетей: Энцикл. – СПб.: Питер, 2002. – 576 с.

Компьютерные сети+: Учеб. курс: Офиц. пособие Microsoft для самостоят. подготовки /Пер. с англ. Microsoft Corporation. – М.: Изд.-торг. дом «Рус. редакция», 2000. – 552 с.

Локальные сети: Полное руководство /НТИ; Под ред. В.В. Самойленко. – Киев: Век+; СПб.: КОРОНА принт, 2002. – 400 с.

Столлингс В. Беспроводные линии связи и сети: Пер. с англ. – М.: Изд. дом «Вильямс», 2003. – 640 с.

Столлингс В. Передача данных. – 4-е изд. – СПб.: Питер, 2004. – 750 с.

Управление сетевой средой Microsoft Windows 2000: Учеб. курс MCSA/MCSE; Пер. с англ. Microsoft Corporation. – М.: Изд.-торг. дом «Рус. редакция», 2003. – 896 с.

Примеры комбинирования прав доступа к ресурсу

Задача 1

Учетная запись пользователя **Иванов** включена в группы **Кадры** и **Программисты**, и в сеть выделена папка **Документы1**. Для доступа к этой папке установлены режимы, приведенные в таблице. Определить результирующие права доступа пользователя **Иванов** при его обращении к папке **Документы1** по сети.

Учетные записи пользователей и групп пользователей	Кадры	Программисты	Иванов
Режимы доступа к ресурсу по сети	Полный доступ	Изменение	–
Режимы доступа к ресурсу на уровне файловой системы	Чтение	Изменение	Запись

Решение:

На сетевом уровне для учетной записи **Иванов** персонально никаких режимов не установлено, но из прав для групп **Кадры** и **Программисты** наследуется режим **Полный доступ** как режим с наибольшими правами доступа.

На уровне файловой системы учетная запись **Иванов** будет иметь режим, допускающий **Изменение** как режим с наибольшими правами доступа из вариантов **Чтение**, **Изменение**, **Запись**.

Результатом комбинирования прав доступа по сети и на уровне файловой системы будет режим **Изменение** как режим с наименьшими правами доступа из двух вариантов – **Полный доступ** и **Изменение**. При обращении к папке **Документы1** по сети пользователь, вошедший в систему под учетной записью **Иванов**, будет иметь возможность удалять папку, а также выполнять все действия, обеспечиваемые разрешениями на **Запись**, **Чтение** и **Выполнение**.

Задача 2

Учетная запись пользователя **Иванов** включена в группы **Кадры** и **Программисты**, и в сеть выделена папка **Документы2**. Для доступа к этой папке установлены режимы, приведенные в таблице. Определить результирующие права доступа пользователя **Иванов** при его обращении к папке **Документы2** по сети.

Учетные записи пользователей и групп пользователей	Кадры	Программисты	Иванов
Режимы доступа к ресурсу по сети	Чтение	Изменение	Нет доступа
Режимы доступа к ресурсу на уровне файловой системы	Чтение	Изменение	Полный доступ

Решение:

Так как на сетевом уровне для учетной записи пользователя **Иванов** определен режим **Нет доступа**, то независимо от разрешений на уровне файловой системы в доступе к ресурсу по сети ему будет отказано.

Список используемых сокращений

БЛКС	беспроводная локальная компьютерная сеть
КС	компьютерная сеть
ЛКС	локальная компьютерная сеть
ОС	операционная система
ПО	программное обеспечение
ACL	Asynchronous Connectionless Links (асинхронная связь без установления соединения)
CAN	Corporation Area Network (корпоративная компьютерная сеть)
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance (метод доступа с контролем несущей и предотвращением коллизий)
CSMA/CD	Carrier Sense Multiple Access with Collision Detection (метод доступа с контролем несущей и обнаружением коллизий)
DCE	Data Circuit Terminating Equipment (аппаратура передачи данных)
DSSS	Direct Sequence Spread Spectrum (метод прямой последовательности)
DTE	Data Terminal Equipment (устройство, вырабатывающее данные для передачи по линии связи)
FCC	Federal Communications Commission (Федеральная правительственная комиссия США по средствам связи)
FHSS	Frequency Hopping Spread Spectrum (метод частотных скачков)
IEEE	Institute of Electrical and Electronics Engineers (Институт инженеров по электронике)
IPX	Internet Packet Exchange (Internet-протокол обмена пакетами)
L2CAP	Logical Link Control and Adaptation Protocol (протокол управления логическими каналами и адаптацией)
LAN	Local Area Network (локальная компьютерная сеть)
LLC	Logical Link Control (уровень управления логической связью)
LSA	Local security authority (локальная служба безопасности)
MAC	Media Access Control (уровень управления доступом к среде)

NCP	NetWare Core Protocol (протокол ядра NetWare)
NDIS	Network Driver Interface Specification (спецификации драйверов сетевых интерфейсов)
NetBEUI	NetBIOS Extended User Interface (расширенный пользовательский интерфейс базовой системы ввода/вывода)
NetBIOS	Network Basic Input/Output System (базовая система ввода/вывода)
NLSP	NetWare Link Services Protocol (протокол маршрутизации на основе состояния канала)
OFDM	Orthogonal Frequency Division Multiplexing (ортогональное частотное уплотнение)
OSI	Open System Interconnection (модель взаимодействия открытых систем)
RG	Registered Grade (коаксиальный кабель)
RIP	Routing Information Protocol (протокол маршрутизации данных)
SAM	Security account manager (служба управления учетными записями)
SAP	Service Advertisement Protocol (протокол уведомления о службах)
SCO	Circuit-switched Synchronous Connection Oriented links (синхронная связь с установлением соединения)
SMB	Server Message Block (блок сообщения сервера)
SNAP	Sub Network Access Protocol (протокол доступа к подсети)
SPX	Sequenced Packet Exchange (протокол последовательного обмена пакетами)
STP	Shielded twisted pair (экранированная витая пара)
TDI	Transport Driver Interface (интерфейс транспортных протоколов)
UNC	Universal Naming Convention (универсальное соглашение о присвоении имен)
UTP	Unshielded Twisted Pair
WAN	Wide-Area Network (глобальная компьютерная сеть)

Волкова Любовь Викторовна
Грохульский Максим Сергеевич

Основы компьютерных сетей

Учебное пособие

Редактор Н.М. Юркова

Печатается по постановлению редакционно-издательского совета
университета

Подписано в печать 19.06.06. Формат 70x108/16. Бумага для множ.
аппаратов. Печать плоская. Усл. печ. л. 8,2. Уч.-изд. л. 9,0. Тираж 100 экз.

Заказ № 213

Издательство Российского государственного профессионально-
педагогического университета. Екатеринбург, ул. Машиностроителей, 11.

Ризограф РГППУ. Екатеринбург, ул. Машиностроителей, 11.

