***Федеральное агентство по рыболовству***

***Федеральное государственное бюджетное образовательное***

***учреждение высшего образования***

***«Астраханский государственный технический университет»***

**Система менеджмента качества в области образования, воспитания, науки и инноваций сертифицирована DQS**

**по международному стандарту ISO 9001:2015**

**МЕТОДИЧЕСКИЕ Указания ПО КУРСУ**

«**КОМЬЮТЕРНЫЕ, СЕТЕВЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИИ В ЭЛЕКТРОТЕХНИЧЕСКИХ КОМПЛЕКСАХ И СИСТЕМАХ»**

**для аспирантов Направление подготовки**

**13.06.01 - Электро- и теплотехника**

**Направленность подготовки**

**Электротехнические комплексы и системы**

**АСТРАХАНЬ**

**Содержание**

|  |  |
| --- | --- |
| *Основные определения и термины.* | *3* |
| *Семиуровневая модель OSI.* | *8* |
| *Стандарты и стеки протоколов.* | *12* |
| *Топология вычислительной сети и методы доступа.ЛВС и ее компоненты.* | *20* |
| ЛВС и ее компоненты. | *27* |
| *Физическая среда передачи данных.* | *32* |
| *Сетевое оборудование.* | *38* |
| *Установка и настройка сетевой карты.* | *51* |
| *Настройка сетевых протоколов.* | *52* |
| *Настройка удаленного соединения.* | *53* |
| *Настройка доступа к общим ресурсам ЛВС* | *54* |
| *Установка и настройка серверов* | *58* |
| *Моделирование локальной сети.* | *68* |
| *Создание простейшей Web-страницы*  | *68* |
| *Создание изображения и использование на Web-странице* | *71* |
| *Дополнительная литература* | *74* |

##

## Основные определения и термины. Архитектура сетей.

*Сеть* – это совокупность объектов, образуемых устройствами передачи и обработки данных. Международная организация по стандартизации определила вычислительную сеть *как последовательную бит-ориентированную передачу информации между связанными друг с другом независимыми устройствами.*

Сети обычно находится в частном ведении пользователя и занимают некоторую территорию и по территориальному признаку разделяются на:

* Локальные вычислительные сети (ЛВС) или Local Area Network (LAN), расположенные в одном или нескольких близко расположенных зданиях. ЛВС обычно размещаются в рамках какой-либо организации (корпорации, учреждения), поэтому их называют корпоративными.
* Распределенные компьютерные сети, глобальные или Wide Area Network (WAN), расположенные в разных зданиях, городах и странах, которые бывают территориальными, смешанными и глобальными. В зависимости от этого глобальные сети бывают четырех основных видов: городские, региональные, национальные и транснациональные. В качестве примеров распределенных сетей очень большого масштаба можно назвать: Internet, EUNET, Relcom, FIDO.

В состав сети в общем случае включается следующие элементы:

* сетевые компьютеры (оснащенные сетевым адаптером);
* каналы связи (кабельные, спутниковые, телефонные, цифровые, волоконно-оптические, радиоканалы и др.);
* различного рода преобразователи сигналов;
* сетевое оборудование.

Различают два понятия сети: *коммуникационная сеть* и *информационная сеть* (рис. 1.1).

*Коммуникационная сеть* предназначена для передачи данных, также она выполняет задачи, связанные с преобразованием данных. Коммуникационные сети различаются по типу используемых физических средств соединения.

*Информационная сеть* предназначена для хранения информации и состоит из *информационных систем*. На базе коммуникационной сети может быть построена группа информационных сетей:

Под *информационной системой* следует понимать систему, которая является поставщиком или потребителем информации.

Компьютерная сеть состоит из *информационных систем* и *каналов связи*.

Под *информационной системой* следует понимать объект, способный осуществлять хранение, обработку или передачу информация. В состав *информационной системы* входят: компьютеры, программы, пользователи и другие составляющие, предназначенные для процесса обработки и передачи данных. В дальнейшем информационная система, предназначенная для решения задач пользователя, будет называться – *рабочая станция (client)*. Рабочая станция в сети отличается от обычного персонального компьютера (ПК) наличием *сетевой карты* (*сетевого адаптера*), канала для передачи данных и сетевого программного обеспечения.



Рис. 0.1 Информационные и коммуникационные сети

Под *каналом связи* следует понимать путь или средство, по которому передаются сигналы. Средство передачи сигналов называют *абонентским,* или *физическим, каналом*.

*Каналы связи (data link)* создаются по линиям связи при помощи сетевого оборудования и физических средств связи. Физические средства связи построены на основе витых пар, коаксиальных кабелей, оптических каналов или эфира. Между взаимодействующими информационными системами через физические каналы коммуникационной сети и узлы коммутации устанавливаются *логические каналы.*

*Логический канал* – это путь для передачи данных от одной системы к другой. Логический канал прокладывается по маршруту в одном или нескольких физических каналах. *Логический канал* можно охарактеризовать, как маршрут, проложенный через физические каналы и узлы коммутации.

Информация в сети передается *блоками данных* по процедурам обмена между объектами. Эти процедуры называют *протоколами передачи данных.*

*Протокол –* это совокупность правил, устанавливающих формат и процедуры обмена информацией между двумя или несколькими устройствами.

Загрузка сети характеризуется параметром, называемым *трафиком*. *Трафик (traffic) –* это поток сообщений в сети передачи данных. Под ним понимают количественное измерение в выбранных точках сети числа проходящих *блоков данных* и их длины, выраженное в битах в секунду.

Существенное влияние на характеристику сети оказывает *метод доступа*. *Метод доступа* – это способ определения того, какая из рабочих станций сможет следующей использовать канал связи и как управлять доступом к каналу связи (кабелю).

В сети все рабочие станции физически соединены между собою каналами связи по определенной структуре, называемой *топологией*. *Топология* – это описание физических соединений в сети, указывающее какие рабочие станции могут связываться между собой. Тип топологии определяет производительность, работоспособность и надежность эксплуатации рабочих станций, а также время обращения к файловому серверу. В зависимости от топологии сети используется тот или иной метод доступа.

Состав основных элементов в сети зависит от ее архитектуры. *Архитектура* – это концепция, определяющая взаимосвязь, структуру и функции взаимодействия рабочих станций в сети. Она предусматривает логическую, функциональную и физическую организацию технических и программных средств сети. Архитектура определяет принципы построения и функционирования аппаратного и программного обеспечения элементов сети.

В основном выделяют три вида архитектур: архитектура *терминал – главный компьютер*, архитектура *клиент – сервер* и *одноранговая* архитектура.

Современные сети можно классифицировать по различным признакам: по удаленности компьютеров, топологии, назначению, перечню предоставляемых услуг, принципам управления (централизованные и децентрализованные), методам коммутации, методам доступа, видам среды передачи, скоростям передачи данных и т. д. Все эти понятия будут рассмотрены более подробно при дальнейшем изучении курса.

Архитектура сети определяет основные элементы сети, характеризует ее общую логическую организацию, техническое обеспечение, программное обеспечение, описывает методы кодирования. Архитектура также определяет принципы функционирования и интерфейс пользователя.

В данном курсе будет рассмотрено три вида архитектур:

* архитектура терминал – главный компьютер;
* одноранговая архитектура;
* архитектура клиент – сервер.

### Архитектура терминал – главный компьютер

Архитектура терминал – главный компьютер (terminal – host computer architecture) – это концепция информационной сети, в которой вся обработка данных осуществляется одним или группой главных компьютеров.



Рис. 0.2 Архитектура терминал – главный компьютер

Рассматриваемая архитектура предполагает два типа оборудования:

* Главный компьютер, где осуществляется управление сетью, хранение и обработка данных.
* Терминалы, предназначенные для передачи главному компьютеру команд на организацию сеансов и выполнения заданий, ввода данных для выполнения заданий и получения результатов.

Классический пример архитектуры сети с главными компьютерами – системная сетевая архитектура (System Network Architecture – SNA).

### Одноранговая архитектура

Одноранговая архитектура (peer-to-peer architecture) – это концепция информационной сети, в которой ее ресурсы рассредоточены по всем системам. Данная архитектура характеризуется тем, что в ней все системы равноправны.

К *одноранговым* сетям относятся малые сети, где любая рабочая станция может выполнять одновременно функции файлового сервера и рабочей станции. В *одноранговых* *ЛВС* дисковое пространство и файлы на любом компьютере могут быть общими. Чтобы ресурс стал общим, его необходимо отдать в общее пользование, используя службы удаленного доступа сетевых одноранговых операционных систем. В зависимости от того, как будет установлена защита данных, другие пользователи смогут пользоваться файлами сразу же после их создания. *Одноранговые* *ЛВС* достаточно хороши только для небольших рабочих групп.



Рис. 0.3 Одноранговая архитектура

*Одноранговые* *ЛВС* являются наиболее легким и дешевым типом сетей для установки. Они на компьютере требуют, кроме сетевой карты и сетевого носителя, только операционной системы *Windows* 95 или *Windows for Workgroups.* При соединении компьютеров, пользователи могут предоставлять ресурсы и информацию в совместное пользование.

Одноранговые сети имеют следующие преимущества:

* они легки в установке и настройке;
* отдельные ПК не зависят от выделенного сервера;
* пользователи в состоянии контролировать свои ресурсы;
* малая стоимость и легкая эксплуатация;
* минимум оборудования и программного обеспечения;
* нет необходимости в администраторе;
* хорошо подходят для сетей с количеством пользователей, не превышающим десяти.

Проблемой одноранговой архитектуры является ситуация, когда компьютеры отключаются от сети. В этих случаях из сети исчезают виды *сервиса*, которые они предоставляли. Сетевую безопасность одновременно можно применить только к одному ресурсу, и пользователь должен помнить столько паролей, сколько сетевых ресурсов. При получении доступа к разделяемому ресурсу ощущается падение производительности компьютера. Существенным недостатком одноранговых сетей является отсутствие централизованного администрирования.

Использование одноранговой архитектуры не исключает применения в той же сети также архитектуры «терминал – главный компьютер» или архитектуры «клиент – сервер».

### Архитектура клиент – сервер

*Архитектура клиент – сервер* (client-server architecture) – это концепция информационной сети, в которой основная часть ее ресурсов сосредоточена в серверах, обслуживающих своих клиентов (рис. 1.4). Рассматриваемая архитектура определяет два типа компонентов: *серверы и клиенты*.

*Сервер -* это объект, предоставляющий *сервис* другим объектам сети по их запросам. *Сервис* – это процесс обслуживания клиентов.



Рис. 0.4 Архитектура клиент – сервер

Сервер работает по заданиям клиентов и управляет выполнением их заданий. После выполнения каждого задания сервер посылает полученные результаты клиенту, пославшему это задание.

Сервисная функция в архитектуре клиент – сервер описывается комплексом прикладных программ, в соответствии с которым выполняются разнообразные прикладные процессы.

Процесс, который вызывает сервисную функцию с помощью определенных операций, называется *клиентом*. Им может быть программа или пользователь. На рис. 1.5 приведен перечень сервисов в архитектуре клиент – сервер.

*Клиенты* – это рабочие станции, которые используют ресурсы сервера и предоставляют удобные *интерфейсы пользователя*. *Интерфейсы пользователя* это процедуры взаимодействия пользователя с системой или сетью.

Клиент является инициатором и использует электронную почту или другие сервисы сервера. В этом процессе клиент запрашивает вид обслуживания, устанавливает сеанс, получает нужные ему результаты и сообщает об окончании работы.



Рис. 0.5 Модель клиент-сервер

В *сетях с выделенным файловым сервером* на выделенном автономном *ПК* устанавливается серверная сетевая операционная система. Этот *ПК* становится *сервером.* Программное обеспечение (*ПО*)*,* установленное на рабочей станции, позволяет ей обмениваться данными с сервером. Наиболее распространенные сетевые операционная системы:

* NetWare фирмы Novel;
* Windows NT фирмы Microsoft;
* UNIX фирмы AT&T;
* Linux.

Помимо сетевой операционной системы необходимы сетевые прикладные программы, реализующие преимущества, предоставляемые сетью.

Сети на базе серверовимеют лучшие характеристики и повышенную надежность. Сервервладеет главными ресурсами сети,к которым обращаются остальные рабочие станции.

В современной клиент – серверной архитектуре выделяется четыре группы объектов: клиенты, серверы, данные и сетевые службы. Клиенты располагаются в системах на рабочих местах пользователей. Данные в основном хранятся в серверах. Сетевые службы являются совместно используемыми серверами и данными. Кроме того службы управляют процедурами обработки данных.

Сети клиент – серверной архитектуры имеют следующие преимущества:

* позволяют организовывать сети с большим количеством рабочих станций;
* обеспечивают централизованное управление учетными записями пользователей, безопасностью и доступом, что упрощает сетевое администрирование;
* эффективный доступ к сетевым ресурсам;
* пользователю нужен один пароль для входа в сеть и для получения доступа ко всем ресурсам, на которые распространяются права пользователя.

Наряду с преимуществами сети клиент – серверной архитектуры имеют и ряд недостатков:

* неисправность сервера может сделать сеть неработоспособной, как минимум потерю сетевых ресурсов;
* требуют квалифицированного персонала для администрирования;
* имеют более высокую стоимость сетей и сетевого оборудования.

### Выбор архитектуры сети

Выбор архитектуры сети зависит от назначения сети, количества рабочих станций и от выполняемых на ней действий.

Следует выбрать одноранговую сеть, если:

* количество пользователей не превышает десяти;
* все машины находятся близко друг от друга;
* имеют место небольшие финансовые возможности;
* нет необходимости в специализированном сервере, таком как сервер БД, факс-сервер или какой-либо другой;
* нет возможности или необходимости в централизованном администрировании.

Следует выбрать клиент серверную сеть, если:

* количество пользователей превышает десяти;
* требуется централизованное управление, безопасность, управление ресурсами или резервное копирование;
* необходим специализированный сервер;
* нужен доступ к глобальной сети;
* требуется разделять ресурсы на уровне пользователей.

## Семиуровневая модель OSI.

Для единого представления данных в сетях с неоднородными устройствами и программным обеспечением международная организация по стандартам ISO (International Standardization Organization) разработала базовую модель связи открытых систем OSI (Open System Interconnection). Эта модель описывает правила и процедуры передачи данных в различных сетевых средах при организации сеанса связи. Основными элементами модели являются уровни, прикладные процессы и физические средства соединения. На рис. 2.1 представлена структура базовой модели. Каждый уровень моделиOSI выполняет определенную задачу в процессе передачи данных по сети. Базовая модель является основой для разработки сетевых протоколов. OSI разделяет коммуникационные функции в сети на семь уровней, каждый из которых обслуживает различные части процесса области взаимодействия открытых систем.



Рис. 0.2 Модель OSI

Модель OSI описывает только системные средства взаимодействия, не касаясь приложений конечных пользователей. Приложения реализуют свои собственные протоколы взаимодействия, обращаясь к системным средствам. Если приложение может взять на себя функции некоторых верхних уровней модели OSI, то для обмена данными оно обращается напрямую к системным средствам, выполняющим функции оставшихся нижних уровней модели OSI.

Модель OSI можно разделить на две различных модели, как показано на рис.2.2:

* горизонтальную модель на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах;
* вертикальную модель на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине.



Рис. 0.2 Схема взаимодействия компьютеров в базовой эталонной модели OSI

Каждый уровень компьютера–отправителя взаимодействует с таким же уровнем компьютера-получателя, как будто он связан напрямую. Такая связь называется логической или виртуальной связью. В действительности взаимодействие осуществляется между смежными уровнями одного компьютера.

Итак, информация на компьютере-отправителе должна пройти через все уровни. Затем она передается по физической среде до компьютера–получателя и опять проходит сквозь все слои, пока не доходит до того же уровня, с которого она была послана на компьютере-отправителе.

В горизонтальной модели двум программам требуется общий протокол для обмена данными. В вертикальной модели соседние уровни обмениваются данными с использованием интерфейсов прикладных программ API (Application Programming Interface).

Перед подачей в сеть данные разбиваются на пакеты. Пакет (packet) – это единица информации, передаваемая между станциями сети. При отправке данных пакет проходит последовательно через все уровни программного обеспечения. На каждом уровне к пакету добавляется управляющая информация данного уровня (заголовок), которая необходима для успешной передачи данных по сети, как это показано на рис. 2.3, где *Заг* – заголовок пакета, *Кон* – конец пакета.

На принимающей стороне пакет проходит через все уровни в обратном порядке. На каждом уровне протокол этого уровня читает информацию пакета, затем удаляет информацию, добавленную к пакету на этом же уровне отправляющей стороной, и передает пакет следующему уровню. Когда пакет дойдет до *Прикладного* уровня, вся управляющая информация будет удалена из пакета, и данные примут свой первоначальный вид.

Рис. 0.3 Формирование пакета каждого уровня семиуровневой модели

Каждый уровень модели выполняет свою функцию. Чем выше уровень, тем более сложную задачу он решает.

Отдельные уровни модели *OSI* удобно рассматривать как *группы программ*, предназначенных для выполнения конкретных *функций*. Один уровень, к примеру, отвечает за обеспечение преобразования данных из *ASCII* в *EBCDIC* и содержит *программы* необходимые для выполнения этой задачи.

Каждый уровень обеспечивает сервис для вышестоящего уровня, запрашивая в свою очередь, сервис у нижестоящего уровня. Верхние уровни запрашивают сервис почти одинаково: как правило, это требование маршрутизации каких-то данных из одной сети в другую. Практическая реализация принципов адресации данных возложена на нижние уровни.

Рассматриваемая модель определяет взаимодействие открытых систем разных производителей в одной сети. Поэтому она выполняет для них координирующие действия по:

* взаимодействию прикладных процессов;
* формам представления данных;
* единообразному хранению данных;
* управлению сетевыми ресурсами;
* безопасности данных и защите информации;
* диагностике программ и технических средств.

На рис. 2.4 приведено краткое описание функций всех уровней.



Рис. 0.4 Функции уровней

## Стандарты и стеки протоколов.

Спецификации Institute of Electrical and Electronics Engineers IEEE802 определяют стандарты для физических компонентов сети. Эти компоненты – сетевая карта (Network Interface Card – NIC) и сетевой носитель (network media), которые относятся к физическому и канальному уровням модели OSI. Спецификации IEEE802 определяют механизм доступа адаптера к каналу связи и механизм передачи данных. Стандарты IEEE802 подразделяют канальный уровень на подуровни:

* Logical Link Control (LLC) – подуровень управления логической связью;
* Media Access Control (MAC) – подуровень управления доступом к устройствам.

Спецификации IEEE 802 делятся на двенадцать стандартов:

### 802.1

Стандарт 802.1 (Internetworking – объединение сетей) задает механизмы управления сетью на MAC – уровне. В разделе 802.1 приводятся основные понятия и определения, общие характеристики и требования к локальным сетям, а также поведение маршрутизации на канальном уровне, где логические адреса должны быть преобразованы в их физические адреса и наоборот.

### 802.2

Стандарт 802.2 (Logical Link Control – управление логической связью) **определяет функционирование подуровня LLC на канальном уровне модели OSI. LLC обеспечивает интерфейс между методами доступа к среде и сетевым уровнем.**

### 802.3

Стандарт802.3 **(**Ethernet Carrier Sense Multiple Access with Collision Detection – CSMA/CD LANs Ethernet – множественный доступ к сетям Ethernet с проверкой несущей и обнаружением конфликтов) **описывает физический уровень и подуровень MAC для сетей, использующих шинную топологию и коллективный доступ с прослушиванием несущей и обнаружением конфликтов. Прототипом этого метода является метод доступа стандарта Ethernet (10BaseT, 10Base2, 10Base5). Метод доступа CSMA/CD. 802.3 также включает технологии Fast Ethernet (100BaseTx, 100BaseFx, 100BaseFl).**

100Base-Tx – двухпарная витая пара. Использует метод MLT-3 для передачи сигналов 5-битовых порций кода 4В/5B по витой паре, а также имеется функция автопереговоров (Auto-negotiation) для выбора режима работы порта.

100Base-T4 – четырехпарная витая пара. Вместо кодирования 4B/5В в этом методе используется кодирование 8B/6T.

100BaseFx – многомодовое оптоволокно. Эта спецификация определяет работу протокола Fast Ethernet по многомодовому оптоволокну в полудуплексном и полнодуплексном режимах на основе хорошо проверенной схемы кодирования и передачи оптических сигналов, использующейся уже на протяжении ряда лет в стандарте FDDI. Как и в стандарте FDDI, каждый узел соединяется с сетью двумя оптическими волокнами, идущими от приемника (Rx) и от передатчика (Tx).

Этот метод доступа используется в сетях с общей шиной (к которым относятся и радиосети, породившие этот метод). Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Простота схемы подключения - это один из факторов, определивших успех стандарта Ethernet. Говорят, что кабель, к которому подключены все станции, работает в режиме *коллективного доступа (multiply access* – *MA).*

Метод доступа CSMA/CD определяет основные временные и логические соотношения, гарантирующие корректную работу всех станций в сети.

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения. Затем кадр передается по кабелю. Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ. Адрес станции–источника также включен в исходный кадр, поэтому станция-получатель знает, кому нужно послать ответ.

### 802.4

Стандарт802.4 (Token Bus LAN – локальные сети Token Bus) определяет метод доступа к шине с передачей маркера, прототип – ArcNet.

При подключении устройств в ArcNet применяют топологию «шина» или «звезда». Адаптеры ArcNet поддерживают метод доступа Token Bus (маркерная шина) и обеспечивают производительность 2,5 Мбит/с. Этот метод предусматривает следующие правила:

* все устройства, подключённые к сети, могут передавать данные, только получив разрешение на передачу (маркер);
* в любой момент времени только одна станция в сети обладает таким правом;
* кадр, передаваемый одной станцией, одновременно анализируется всеми остальными станциями сети.

В сетях ArcNet используется асинхронный метод передачи данных (в сетях Ethernet и Token Ring применяется синхронный метод), т. е. передача каждого байта в ArcNet выполняется посылкой ISU (Information Symbol Unit – единица передачи информации), состоящей из трёх служебных старт/стоповых битов и восьми битов данных.

### 802.5

Стандарт802.5 (Token Ring LAN – локальные сети Token Ring) описывает метод доступа к кольцу с передачей маркера, прототип – Token Ring.

Сети стандарта Token Ring, так же как и сети Ethernet, используют разделяемую среду передачи данных, которая состоит из отрезков кабеля, соединяющих все станции сети в кольцо. Кольцо рассматривается как общий разделяемый ресурс, и для доступа к нему используется не случайный алгоритм, как в сетях Ethernet, а детерминированный, основанный на передаче станциями права на использование кольца в определенном порядке. Право на использование кольца передается с помощью кадра специального формата, называемого маркером, или токеном.

### 802.6

Стандарт802.6 (Metropolitan Area Network – городские сети) описывает рекомендации для региональных сетей.

### 802.7

Стандарт802.7 (Broadband Technical Advisory Group – техническая консультационная группа по широковещательной передаче) описывает рекомендации по широкополосным сетевым технологиям, носителям, интерфейсу и оборудованию.

### 802.8

Стандарт 802.8 (Fiber Technical Advisory Group – техническая консультационная группа по оптоволоконным сетям) содержит обсуждение использования оптических кабелей в сетях 802.3 – 802.6, а также рекомендации по оптоволоконным сетевым технологиям, носителям, интерфейсу и оборудованию, прототип – сеть FDDI (Fiber Distributed Data Interface).

Стандарт FDDI использует оптоволоконный кабель и доступ с применением маркера. Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. Использование двух колец – это основной способ повышения отказоустойчивости в сети FDDI, и узлы, которые хотят им воспользоваться, должны быть подключены к обоим кольцам. Скорость сети до 100 Мб/с. Данная технология позволяет включать до 500 узлов на расстоянии 100 км.

### 802.9

Стандарт 802.9 (Integrated Voice and Data Network – интегрированные сети передачи голоса и данных) задает архитектуру и интерфейсы устройств одновременной передачи данных и голоса по одной линии, а также содержит рекомендации по гибридным сетям, в которых объединяют голосовой трафик и трафик данных в одной и той же сетевой среде.

### 802.10

В стандарте 802.10 (Network Security – сетевая безопасность) рассмотрены вопросы обмена данными, шифрования, управления сетями и безопасности в сетевых архитектурах, совместимых с моделью OSI.

### 802.11

Стандарт802.11 (Wireless Network – беспроводные сети) описывает рекомендации по использованию беспроводных сетей.

### 802.12

Стандарт802.12 описывает рекомендации по использованию сетей 100VG – AnyLAN со скоростью100Мб/с и методом доступа по очереди запросов и по приоритету (Demand Priority Queuing – DPQ, Demand Priority Access – DPA).

Технология 100VG – это комбинация *Ethernet*и*Token-Ring* со скоростью передачи 100 Мбит/c, работающая на неэкранированных витых парах. В проекте 100Base-VG усовершенствован метод доступа с учетом потребности мультимедийных приложений. В спецификации *100VG*предусматривается поддержка волоконно-оптических кабельных систем. Технология *100VG*использует метод доступа – обработка запросов по приоритету (demand priority access). В этом случае узлам сети предоставляется право равного доступа. Концентратор опрашивает каждый порт и проверяет наличие запроса на передачу, а затем разрешает этот запрос в соответствии с приоритетом. Имеется два уровня приоритетов – высокий и низкий.

Согласованный набор протоколов разных уровней, достаточный для организации межсетевого взаимодействия, называется *стеком протоколов*. Для каждого уровня определяется набор функций–запросов для взаимодействия с выше лежащим уровнем, который называется *интерфейсом*. Правила взаимодействия двух машин могут быть описаны в виде набора процедур для каждого из уровней, которые называются *протоколами*.

Существует достаточно много стеков протоколов, широко применяемых в сетях. Это и стеки, являющиеся международными и национальными стандартами, и фирменные стеки, получившие распространение благодаря распространенности оборудования той или иной фирмы. Примерами популярных стеков протоколов могут служить стек IPX/SPX фирмы Novell, стек TCP/IP, используемый в сети Internet и во многих сетях на основе операционной системы UNIX, стек OSI международной организации по стандартизации, стек DECnet корпорации Digital Equipment и некоторые другие.

Стеки протоколов разбиваются на три уровня:

* сетевые;
* транспортные;
* прикладные.

### Сетевые протоколы

Сетевые протоколы предоставляют следующие услуги: адресацию и маршрутизацию информации, проверку на наличие ошибок, запрос повторной передачи и установление правил взаимодействия в конкретной сетевой среде. Ниже приведены наиболее популярные сетевые протоколы.

* **DDP** (Datagram Delivery Protocol – Протокол доставки дейтаграмм).Протокол передачи данных Apple, используемый в Apple Talk.
* **IP** (Internet Protocol – Протокол Internet). Протокол стека TCP/IP, обеспечивающий адресную информацию и информацию о маршрутизации.
* **IPX** (Internetwork Packet eXchange – Межсетевой обмен пакетами) в NWLink.Протокол Novel NetWare, используемый для маршрутизации и направления пакетов.
* **NetBEUI** (NetBIOS Extended User Interface – расширенный пользовательский интерфейс базовой сетевой системы ввода вывода)**.** Разработанный совместно IBM и Microsoft, этот протокол обеспечивает транспортные услуги для **NetBIOS.**

### Транспортные протоколы

Транспортные протоколы предоставляют следующие услуги надежной транспортировки данных между компьютерами. Ниже приведены наиболее популярные транспортные протоколы.

* **ATP** (Apple Talk Protocol – Транзакционный протокол Apple Talk) и **NBP** (Name Binding Protocol – Протокол связывания имен). Сеансовый и транспортный протоколы Apple Talk.
* **NetBIOS (**Базовая сетевая система ввода вывода)**.** NetBIOS Устанавливает соединение между компьютерами, а **NetBEUI** предоставляет услуги передачи данных для этого соединения.
* **SPX** (Sequenced Packet eXchange – Последовательный обмен пакетами) в NWLink.Протокол Novel NetWare, используемый для обеспечения доставки данных.
* **TCP** (Transmission Control Protocol – Протокол управления передачей).Протокол стека TCP/IP, отвечающий за надежную доставку данных.

### Прикладные протоколы

Прикладные протоколы отвечают за взаимодействие приложений. Ниже приведены наиболее популярные прикладные протоколы.

* **AFP** (Apple Talk File Protocol – Файловый протокол Apple Talk).Протокол удаленного управления файлами Macintosh.
* **FTP** (File Transfer Protocol – Протокол передачи файлов). Протокол стека TCP/IP,используемый для обеспечения услуг по передачи файлов.
* **NCP** (NetWare Core Protocol – Базовый протокол NetWare). Оболочка и редиректоры клиента Novel NetWare.
* **SNMP** (Simple Network Management Protocol – Простой протокол управления сетью).Протокол стека TCP/IP, используемый дляуправления и наблюдения за сетевыми устройствами.
* **HTTP** (Hyper Text Transfer Protocol) – протокол передачи гипертекста и другие протоколы.

Набор многоуровневых протоколов, или как называют стек *TCP/IP*, предназначен для использования в различных вариантах сетевого окружения. Стек *TCP/IP* с точки зрения системной архитектуры соответствует эталонной модели *OSI* (Open Systems Interconnection – взаимодействие открытых систем) и позволяет обмениваться данными по сети приложениям и службам, работающим практически на любой платформе, включая Unix, Windows, Macintosh и другие.



Рис. 0.3 Соответствие семиуровневой модели OSI и четырехуровневой модели TCP/IP

Реализация TCP/IP фирмы Microsoft [1] соответствует четырехуровневой модели вместо семиуровневой модели, как показано на рис. 3.1. Модель TCP/IP включает большее число функций на один уровень, что приводит к уменьшению числа уровней. В модели используются следующие уровни:

* уровень *Приложения* модели TCP/IP соответствует уровням *Приложения, Представления* и *Сеанса* модели OSI;
* уровень *Транспорта* модели TCP/IP соответствует аналогичному уровню *Транспорта* модели OSI;
* *межсетевой* уровень модели TCP/IP выполняет те же функции, что и уровень *Сети* модели OSI;
* уровень сетевого интерфейса модели TCP/IP соответствует *Канальному* и *Физическому* уровням модели OSI.

### Уровень Приложения

Через уровень *Приложения* модели TCP/IP приложения и службы получают доступ к сети. Доступ к протоколам TCP/IP осуществляется посредством двух программных интерфейсов (API – Application Programming Interface):

* Сокеты Windows;
* NetBIOS.

Интерфейс *сокетов Windows,* или как его называют *WinSock*, является сетевым программным интерфейсом, предназначенным для облегчения взаимодействия между различными TCP/IP – приложениями и семействами протоколов.

Интерфейс *NetBIOS* используется для связи между процессами (IPC – Interposes Communications) служб и приложений ОС Windows. *NetBIOS* выполняет три основных функции:

* определение имен NetBIOS;
* служба дейтаграмм NetBIOS;
* служба сеанса NetBIOS.

В таблице 3.1 приведено семейство протоколов TCP/IP.

Таблица 0.1

|  |  |
| --- | --- |
| Название протокола | Описание протокола |
| WinSock | Сетевой программный интерфейс |
| NetBIOS | Связь с приложениями ОС Windows |
| TDI | Интерфейс транспортного драйвера (Transport Driver Interface) позволяет создавать компоненты сеансового уровня. |
| TCP | Протокол управления передачей (Transmission Control Protocol) |
| UDP | Протокол пользовательских дейтаграмм (User Datagram Protocol) |
| ARP | Протокол разрешения адресов (Address Resolution Protocol) |
| RARP | Протокол обратного разрешения адресов (Reverse Address Resolution Protocol) |
| IP | Протокол Internet(Internet Protocol) |
| ICMP | Протокол управляющих сообщений Internet (Internet Control Message Protocol) |
| IGMP | Протокол управления группами Интернета (Internet Group Management Protocol), |
| NDIS | Интерфейс взаимодействия между драйверами транспортных протоколов |
| FTP | Протокол пересылки файлов (File Transfer Protocol) |
| TFTP | Простой протокол пересылки файлов (Trivial File Transfer Protocol) |

### Уровень транспорта

Уровень транспорта TCP/IP отвечает за установления и поддержания соединения между двумя узлами. Основные функции уровня:

* подтверждение получения информации4
* управление потоком данных;
* упорядочение и ретрансляция пакетов.

В зависимости от типа службы могут быть использованы два протокола:

* TCP (Transmission Control Protocol – протокол управления передачей);
* UDP (User Datagram Protocol – пользовательский протокол дейтаграмм).

TCP обычно используют в тех случаях, когда приложению требуется передать большой объем информации и убедиться, что данные своевременно получены адресатом. Приложения и службы, отправляющие небольшие объемы данных и не нуждающиеся в получении подтверждения, используют протокол UDP, который является протоколом без установления соединения.

### Протокол управления передачей (TCP)

Протокол TCP отвечает за надежную передачу данных от одного узла сети к другому. Он создает сеанс с установлением соединения, иначе говоря виртуальный канал между машинами. Установление соединения происходит в три шага:

1. Клиент, запрашивающий соединение, отправляет серверу пакет, указывающий номер порта, который клиент желает использовать, а также код (определенное число) ISN (Initial Sequence number).
2. Сервер отвечает пакетом, содержащий ISN сервера, а также ISN клиента, увеличенный на 1.
3. Клиент должен подтвердить установление соединения, вернув ISN сервера, увеличенный на 1.

Трехступенчатое открытие соединения устанавливает номер порта, а также ISN клиента и сервера. Каждый, отправляемый TCP – пакет содержит номера TCP – портов отправителя и получателя, номер фрагмента для сообщений, разбитых на меньшие части, а также контрольную сумму, позволяющую убедиться, что при передачи не произошло ошибок.

### Пользовательский протокол дейтаграмм (UDP)

В отличие от TCP UDP не устанавливает соединения. Протокол UDP предназначен для отправки небольших объемов данных без установки соединения и используется приложениями, которые не нуждаются в подтверждении адресатом их получения. UDP также использует номера портов для определения конкретного процесса по указанному IP адресу. Однако UDP порты отличаются от TCP портов и, следовательно, могут использовать те же номера портов, что и TCP, без конфликта между службами.

### Межсетевой уровень

Межсетевой уровень отвечает за маршрутизацию данных внутри сети и между различными сетями. На этом уровне работают маршрутизаторы, которые зависят от используемого протокола и используются для отправки пакетов из одной сети (или ее сегмента) в другую (или другой сегмент сети). В стеке TCP/IP на этом уровне используется протокол IP.

### Протокол Интернета IP

Протокол IP обеспечивает обмен дейтаграммами между узлами сети и является протоколом, не устанавливающим соединения и использующим дейтаграммы для отправки данных из одной сети в другую. Данный протокол не ожидает получение подтверждения (ASK, Acknowledgment) отправленных пакетов от узла адресата. Подтверждения, а также повторные отправки пакетов осуществляется протоколами и процессами, работающими на верхних уровнях модели.

К его функциям относится фрагментация дейтаграмм и межсетевая адресация. Протокол IP предоставляет управляющую информацию для сборки фрагментированных дейтаграмм. Главной функцией протокола является межсетевая и глобальная адресация. В зависимости от размера сети, по которой будет маршрутизироваться дейтаграмма или пакет, применяется одна из трех схем адресации.

### Адресация в IP-сетях

Каждый компьютер в сетях TCP/IP имеет адреса трех уровней: физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя).

*Физический, или локальный адрес узла,* определяемый технологией, с помощью которой построена сеть, в которую входит узел. Для узлов, входящих в локальные сети - это МАС–адрес сетевого адаптера или порта маршрутизатора, например, 11-А0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей МАС – адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.

*Сетевой, или IP-адрес*, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла - гибкое, и граница между этими полями может устанавливаться произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

**Символьный адрес, или DNS-имя**, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес используется на прикладном уровне, например, в протоколах FTP или telnet.

## Топология вычислительной сети и методы доступа.

*Топология* *(конфигурация)* – это способ соединения компьютеров в сеть. Тип топологии определяет стоимость, защищенность, производительность и надежность эксплуатации рабочих станций, для которых имеет значение время обращения к файловому серверу.

Понятие топологии широко используется при создании сетей. Одним из подходов к классификации топологий ЛВС является выделение двух основных классов топологий*: широковещательные* и *последовательные*.

В *широковещательных* *топологиях* ПК передает сигналы, которые могут быть восприняты остальными ПК. К таким топологиям относятся топологии: *общая шина, дерево, звезда*.

В *последовательных* *топологиях* информация передается только одному ПК. Примерами таких топологий являются: *произвольная* (произвольное соединение ПК), *кольцо, цепочка*.

При выборе оптимальной топологии преследуются три основных цели:

* обеспечение альтернативной маршрутизации и максимальной надежности передачи данных;
* выбор оптимального маршрута передачи блоков данных;
* предоставление приемлемого времени ответа и нужной пропускной способности.

При выборе конкретного типа сети важно учитывать ее топологию. Основными сетевыми топологиями являются: шинная (линейная) топология, звездообразная, кольцевая и древовидная.

Например, в конфигурации сети ArcNet используется одновременно и линейная, и звездообразная топология. Сети Token Ring физически выглядят как звезда, но логически их пакеты передаются по кольцу. Передача данных в сети Ethernet происходит по линейной шине, так что все станции видят сигнал одновременно.

### Виды топологий

Существуют пять основных топологий (рис. 4.1):

* общая шина (Bus);
* кольцо (Ring);
* звезда (Star);
* древовидная (Tree);
* ячеистая (Mesh).



Рис. 0.4 Типы топологий

### Общая шина

Общая шина это тип сетевой топологии, в которой рабочие станции расположены вдоль одного участка кабеля, называемого сегментом.



Рис. 0.2 Топология *Общая шина*

Топология *Общая шина* (рис. 4.2) предполагает использование одного кабеля, к которому подключаются все компьютеры сети. В случае топологии *Общая шина* кабель используется всеми станциями по очереди. Принимаются специальные меры для того, чтобы при работе с общим кабелем компьютеры не мешали друг другу передавать и принимать данные. Все сообщения, посылаемые отдельными компьютерами, принимаются и прослушиваются всеми остальными компьютерами, подключенными к сети. *Рабочая станция* отбирает адресованные ей сообщения, пользуясь *адресной* информацией. Надежность здесь выше, так как выход из строя отдельных компьютеров не нарушит работоспособность сети в целом. Поиск неисправности в сети затруднен. Кроме того, так как используется только один кабель, в случае обрыва нарушается работа всей сети. Шинная топология - это наиболее простая и наиболее распространенная топология сети.

Примерами использования топологии общая шина является сеть 10Base–5 (соединение ПК толстым коаксиальным кабелем) и 10Base–2 (соединение ПК тонким коаксиальным кабелем).

### Кольцо



Рис. 0.3 Топология *Кольцо*

*Кольцо –* это топология ЛВС, в которой каждая станция соединена с двумя другими станциями, образуя кольцо (рис.4.3). Данные передаются от одной рабочей станции к другой в одном направлении (по кольцу). Каждый ПК работает как повторитель, ретранслируя сообщения к следующему ПК, т.е. данные, передаются от одного компьютера к другому как бы по эстафете. Если компьютер получает данные, предназначенные для другого компьютера, он передает их дальше по кольцу, в ином случае они дальше не передаются. Очень просто делается запрос на все станции одновременно. Основная проблема при кольцевой топологии заключается в том, что каждая рабочая станция должна активно участвовать в пересылке информации, и в случае выхода из строя хотя бы одной из них, вся сеть парализуется. Подключение новой рабочей станции требует краткосрочного выключения сети, т.к. во время установки кольцо должно быть разомкнуто. Топология *Кольцо* имеет хорошо предсказуемое время отклика, определяемое числом рабочих станций.

Чистая кольцевая топология используется редко. Вместо этого кольцевая топология играет транспортную роль в схеме метода доступа. Кольцо описывает логический маршрут, а пакет передается от одной станции к другой, совершая в итоге полный круг. В сетях Token Ring кабельная ветвь из центрального концентратора называется MAU (Multiple Access Unit). MAU имеет внутреннее кольцо, соединяющее все подключенные к нему станции, и используется как альтернативный путь, когда оборван или отсоединен кабель одной рабочей станции. Когда кабель рабочей станции подсоединен к MAU, он просто образует расширение кольца: сигналы поступают к рабочей станции, а затем возвращаются обратно во внутреннее кольцо

### Звезда

*Звезда –* это топология ЛВС (рис.4.4), в которой все *рабочие станции* присоединены к центральному узлу (например, к концентратору), который устанавливает, поддерживает и разрывает связи между рабочими станциями. Преимуществом такой топологии является возможность простого исключения неисправного *узла*. Однако, если неисправен центральный узел, вся сеть выходит из строя.

В этом случае каждый компьютер через специальный сетевой адаптер подключается отдельным кабелем к объединяющему устройству. При необходимости можно объединять вместе несколько сетей с топологией *Звезда,* при этом получаются разветвленные конфигурации сети. В каждой точке ветвления необходимо использовать специальные соединители (распределители, повторители или устройства доступа).



Рис. 0.4 Топология *Звезда*

Примером звездообразной топологии является топология Ethernet с кабелем типа *Витая пара* 10BASE-T, центром *Звезды* обычно является Hub.

Звездообразная топология обеспечивает защиту от разрыва кабеля. Если кабель рабочей станции будет поврежден, это не приведет к выходу из строя всего сегмента сети. Она позволяет также легко диагностировать проблемы подключения, так как каждая рабочая станция имеет свой собственный кабельный сегмент, подключенный к концентратору. Для диагностики достаточно найти разрыв кабеля, который ведет к неработающей станции. Остальная часть сети продолжает нормально работать.

Однако звездообразная топология имеет и недостатки. Во-первых, она требует много кабеля. Во-вторых, концентраторы довольно дороги. В-третьих, кабельные концентраторы при большом количестве кабеля трудно обслуживать. Однако в большинстве случаев в такой топологии используется недорогой кабель типа *витая пара*. В некоторых случаях можно даже использовать существующие телефонные кабели. Кроме того, для диагностики и тестирования выгодно собирать все кабельные концы в одном месте. По сравнению с концентраторами ArcNet концентраторы Ethernet и MAU Token Ring достаточно дороги. Новые подобные концентраторы включают в себя средства тестирования и диагностики, что делает их еще более дорогими.

Метод доступа – это способ определения того, какая из рабочих станций сможет следующей использовать ЛВС. То, как сеть управляет доступом к каналу связи (кабелю), существенно влияет на ее характеристики. Примерами методов доступа являются:

* множественный доступ с прослушиванием несущей и разрешением коллизий (Carrier Sense Multiple Access with Collision Detection – CSMA/CD);
* множественный доступ с передачей полномочия (Token Passing Multiple Access – TPMA) или метод с передачей маркера;
* множественный доступ с разделением во времени (Time Division Multiple Access – TDMA);
* множественный доступ с разделением частоты (Frequency Division Multiple Access – FDMA) или множественный доступ с разделением длины волны (Wavelength Division Multiple Access – WDMA).

### CSMA/CD

Алгоритм множественного доступа с прослушиванием несущей и разрешением коллизий приведен на рис. 4.5.

*Метод множественного доступа с прослушиванием несущей и разрешением коллизий (CSMA/CD)* устанавливает следующий порядок: если рабочая станция хочет воспользоваться сетью для передачи данных, она сначала должна проверить состояние канала: начинать передачу станция может, если канал свободен. В процессе передачи станция продолжает прослушивание сети для обнаружения возможных конфликтов. Если возникает конфликт из-за того, что два узла попытаются занять канал, то обнаружившая конфликт интерфейсная плата, выдает в сеть специальный сигнал, и обе станции одновременно прекращают передачу. Принимающая станция отбрасывает частично принятое сообщение, а все рабочие станции, желающие передать сообщение, в течение некоторого, случайно выбранного промежутка времени выжидают, прежде чем начать сообщение.

Все сетевые интерфейсные платы запрограммированы на разные псевдослучайные промежутки времени. Если конфликт возникнет во время повторной передачи сообщения, этот промежуток времени будет увеличен. Стандарт типа *Ethernet* определяет сеть с конкуренцией, в которой несколько рабочих станций должны конкурировать друг с другом за право доступа к сети.



Рис. 0.5 Алгоритм *CSMA/CD*

### TPMA

Алгоритм множественного доступа с передачей полномочия, или маркера, приведен на рис. 4.6.

*Метод с передачей маркера* – это метод доступа к среде, в котором от рабочей станции к рабочей станции передается маркер, дающий разрешение на передачу сообщения. При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит это сообщение по сети. Каждая станция между передающей станцией и принимающей видит это сообщение, но только станция – адресат принимает его. При этом она создает новый маркер.

Маркер (token), или полномочие, – уникальная комбинация битов, позволяющая начать передачу данных.

Каждый узел принимает пакет от предыдущего, восстанавливает уровни сигналов до номинального уровня и передает дальше. Передаваемый пакет может содержать данные или являться маркером. Когда рабочей станции необходимо передать пакет, ее адаптер дожидается поступления маркера, а затем преобразует его в пакет, содержащий данные, отформатированные по протоколу соответствующего уровня, и передает результат далее по *ЛВС*.



Рис. 0.6 Алгоритм TPMA

Пакет распространяется по *ЛВС* от адаптера к адаптеру, пока не найдет своего адресата, который установит в нем определенные биты для подтверждения того, что данные достигли адресата, и ретранслирует его вновь в *ЛВС*. После чего пакет возвращается в узел из которого был отправлен. Здесь после проверки безошибочной передачи пакета, узел освобождает *ЛВС*, выпуская новый маркер. Таким образом, в *ЛВС* с передачей маркера невозможны коллизии (конфликты). Метод с передачей маркера в основном используется в кольцевой топологии.

Данный метод характеризуется следующими достоинствами:

* гарантирует определенное время доставки блоков данных в сети;
* дает возможность предоставления различных приоритетов передачи данных.

Вместе с тем он имеет существенные недостатки:

* в сети возможны потеря маркера, а также появление нескольких маркеров, при этом сеть прекращает работу;
* включение новой рабочей станции и отключение связаны с изменением адресов всей системы.

### TDMA

Множественный доступ с разделением во времени основан на распределении времени работы канала между системами (рис.4.7).

Доступ *TDMA* основан на использовании специального устройства, называемого тактовым генератором. Этот генератор делит время канала на повторяющиеся циклы. Каждый из циклов начинается сигналом *Разграничителем*. Цикл включает *n* пронумерованных временных интервалов, называемых ячейками. Интервалы предоставляются для загрузки в них блоков данных.



Рис. 0.7 Структура множественного доступа с разделением во времени

Данный способ позволяет организовать передачу данных с коммутацией пакетов и с коммутацией каналов.

Первый (простейший) вариант использования интервалов заключается в том, что их число (n) делается равным количеству абонентских систем, подключенных к рассматриваемому каналу. Тогда во время цикла каждой системе предоставляется один интервал, в течение которого она может передавать данные. При использовании рассмотренного метода доступа часто оказывается, что в одном и том же цикле одним системам нечего передавать, а другим не хватает выделенного времени. В результате – неэффективное использование пропускной способности канала.

Второй, более сложный, но высокоэкономичный вариант заключается в том, что система получает интервал только тогда, когда у нее возникает необходимость в передаче данных, например при асинхронном способе передачи. Для передачи данных система может в каждом цикле получать интервал с одним и тем же номером. В этом случае передаваемые системой блоки данных появляются через одинаковые промежутки времени и приходят с одним и тем же временем запаздывания. Это режим передачи данных с имитацией коммутации каналов. Способ особенно удобен при передаче речи.

### FDMA

Доступ *FDMA* основан на разделении полосы пропускания канала на группу полос частот (Рис. 4.8), образующих *логические каналы*.

Широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. Размеры узких полос могут быть различными.

При использовании FDMA, именуемого также *множественным доступом с разделением волны* WDMA, широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. В каждой узкой полосе создается логический канал. Размеры узких полос могут быть различными. Передаваемые по логическим каналам сигналы накладываются на разные несущие и поэтому в частотной области не должны пересекаться. Вместе с этим, иногда, несмотря на наличие защитных полос, спектральные составляющие сигнала могут выходить за границы логического канала и вызывать шум в соседнем логическом канале.



Рис. 0.8 Схема выделения логических каналов

В оптических каналах разделение частоты осуществляется направлением в каждый из них лучей света с различными частотами. Благодаря этому пропускная способность физического канала увеличивается в несколько раз. При осуществлении этого мультиплексирования в один световод излучает свет большое число лазеров (на различных частотах). Через световод излучение каждого из них проходит независимо от другого. На приемном конце разделение частот сигналов, прошедших физический канал, осуществляется путем фильтрации выходных сигналов.

Метод доступа FDMA относительно прост, но для его реализации необходимы передатчики и приемники, работающие на различных частотах.

## ЛВС и ее компоненты.

Компьютерная сеть состоит из трех основных аппаратных компонент и двух программных, которые должны работать согласованно. Для корректной работы устройств в сети их нужно правильно инсталлировать и установить рабочие параметры.

Основными аппаратными компонентами сети являются следующие:

1. Абонентские системы:
* компьютеры (рабочие станции или клиенты и серверы);
* принтеры;
* сканеры и др.
1. Сетевое оборудование:
* сетевые адаптеры;
* концентраторы (хабы);
* мосты;
* маршрутизаторы и др.
1. Коммуникационные каналы:
* кабели;
* разъемы;
* устройства передачи и приема данных в беспроводных технологиях.

Основными программными компонентами сети являются следующие:

1. Сетевые операционные системы, где наиболее известные из них это:
* Windows NT;
* Windows for Workgroups;
* LANtastic;
* NetWare;
* Unix;
* Linux и т.д.
1. Сетевое программное обеспечение (Сетевые службы):
* клиент сети;
* сетевая карта;
* протокол;
* служба удаленного доступа.

ЛВС (Локальная вычислительная сеть) – это совокупность компьютеров, каналов связи, сетевых адаптеров, работающих под управлением сетевой операционной системы и сетевого программного обеспечения.

В *ЛВС* каждый *ПК* называется *рабочей станцией*, за исключением одного или нескольких компьютеров, которые предназначены для выполнения функций *файл-серверов.* Каждая *рабочая станция* и *файл-сервер* имеют *сетевые карты (адаптеры)*, которые посредством *физических каналов* соединяются между собой. В дополнение к локальной операционной системе на каждой рабочей станции активизируется сетевое программное обеспечение, позволяющее станции взаимодействовать с файловым сервером.

Компьютеры, входящие в ЛВС клиент – серверной архитектуры, делятся на два типа: *рабочие станции, или клиенты*, предназначенные для пользователей, и *файловые серверы*, которые, как правило, недоступны для обычных пользователей и предназначены для управления ресурсами сети.

Аналогично на файловом сервере запускается сетевое программное обеспечение, которое позволяет ему взаимодействовать с рабочей станцией и обеспечить доступ к своим файлам.

Рабочая станция (workstation) – это абонентская система, специализированная для решения определенных задач и использующая сетевые ресурсы. К сетевому программному обеспечению рабочей станции относятся следующие службы:

* клиент для сетей;
* служба доступа к файлам и принтерам;
* сетевые протоколы для данного типа сетей;
* сетевая плата;
* контроллер удаленного доступа.

Рабочая станция отличается от обычного автономного персонального компьютера следующим:

* наличием сетевой карты (сетевого адаптера) и канала связи;
* на экране во время загрузки ОС появляются дополнительные сообщения, которые информируют о том, что загружается сетевая операционная система;
* перед началом работы необходимо сообщить сетевому программному обеспечению имя пользователя и пароль. Это называется процедурой входа в сеть;
* после подключения к ЛВС появляются дополнительные сетевые дисковые накопители;
* появляется возможность использования сетевого оборудования, которое может находиться далеко от рабочего места.

Для подключения *ПК* к сети требуется устройство сопряжения, которое называют сетевым адаптером, интерфейсом, модулем, или картой. Оно вставляется в гнездо материнской платы. Карты сетевых адаптеров устанавливаются на каждой рабочей станции и на файловом сервере. Рабочая станция отправляет запрос через сетевой адаптер к файловому серверу и получает ответ через сетевой адаптер, когда файловый сервер готов.

Сетевые адаптеры вместе с сетевым программным обеспечением способны распознавать и обрабатывать ошибки, которые могут возникнуть из-за электрических помех, коллизий или плохой работы оборудования.

Последние типы сетевых адаптеров поддерживают технологию *Plug and Play (вставляй и работай)*. Если сетевую карту установить в компьютер, то при первой загрузке система определит тип адаптера и запросит для него драйверы.

Различные типы сетевых адаптеров отличаются не только методами доступа к каналу связи и протоколами, но еще и следующими параметрами:

* скорость передачи;
* объем буфера для пакета;
* тип шины;
* быстродействие шины;
* совместимость с различными микропроцессорами;
* использованием прямого доступа к памяти (DMA);
* адресация портов ввода/вывода и запросов прерывания;
* конструкция разъема.

Сервер – это компьютер, предоставляющий свои ресурсы (диски, принтеры, каталоги, файлы и т.п.) другим пользователям сети.

Файловый сервер обслуживает рабочие станции. В настоящее время это обычно быстродействующий *ПК* на базе процессоров Pentium, работающие с тактовой частотой 500 Мгц и выше, с объемом *ОЗУ 128Мбт* или более. Чаще всего файловый сервер выполняет только эти функции. Но иногда в малых *ЛВС* файл–сервер используется еще и в качестве рабочей станции. На файловом сервере должна стоять сетевая операционная система, а также сетевое программное обеспечение. К сетевому программному обеспечению сервера относятся сетевые службы и протоколы, а также средства администрирования сервера.

Файловые серверы могут контролировать доступ пользователей к различным частям файловой системы. Это обычно осуществляется разрешением пользователю присоединить некоторую файловую систему (или каталог) к рабочей станции пользователя для дальнейшего использования как локального диска.

По мере усложнения возлагаемых на серверы функций и увеличения числа обслуживаемых ими клиентов происходит все большая специализация серверов. Существует множество типов серверов.

* Первичный контроллер домена, сервер, на котором хранится база бюджетов пользователей и поддерживается политика защиты.
* Вторичный контроллер домена, сервер, на котором хранится резервная копия базы бюджетов пользователей и политики защиты.
* Универсальный сервер, предназначенный для выполнения несложного набора различных задач обработки данных в локальной сети.
* Сервер базы данных, выполняющий обработку запросов, направляемых базе данных.
* Proxy сервер, подключающий локальную сеть к сети Internet.
* Web–сервер, предназначенный для работы с web–информацией.
* Файловый сервер, обеспечивающий функционирование распределенных ресурсов, включая файлы, программное обеспечение.
* Сервер приложений, предназначенный для выполнения прикладных процессов. С одной стороны, взаимодействует с клиентами, получая задания, а с другой стороны, работает с базами данных, подбирая данные, необходимые для обработки.
* Сервер удаленного доступа, обеспечивающий сотрудникам, работающим дома торговым агентам, служащим филиалов, лицам, находящимся в командировках, возможность работы с данными сети.
* Телефонный сервер, предназначенный для организации в локальной сети службы телефонии. Этот сервер выполняет функции речевой почты, автоматического распределения вызовов, учет стоимости телефонных разговоров, интерфейса с внешней телефонной сетью. Наряду с телефонией сервер может также передавать изображения и сообщения факсимильной связи.
* Почтовый сервер, предоставляющий сервис в ответ на запросы, присланные по электронной почте.
* Сервер доступа, дающий возможность коллективного использования ресурсов пользователями, оказавшимися вне своих сетей (например, пользователями, которые находятся в командировках и хотят работать со своими сетями). Для этого пользователи через коммуникационные сети соединяются с сервером доступа и последний предоставляет нужные ресурсы, имеющиеся в сети.
* Терминальный сервер, объединяющий группу терминалов, упрощающий переключения при их перемещении.
* Коммуникационный сервер, выполняющий функции терминального сервера, но осуществляющий также маршрутизацию данных.
* Видеосервер, который в наибольшей степени приспособлен к обработке изображений, снабжает пользователей видеоматериалами, обучающими программами, видеоиграми, обеспечивает электронный маркетинг. Имеет высокую производительность и большую память.
* Факс–сервер, обеспечивающий передачу и прием сообщений в стандартах факсимильной связи.
* Сервер защиты данных, оснащенный широким набором средств обеспечения безопасности данных и, в первую очередь, идентификации паролей.

Сетевые операционные системы **(**Network Operating System – NOS) – это комплекс программ, обеспечивающих в сети обработку, хранение и передачу данных.

Для организации сети кроме аппаратных средств, необходима такжесетевая операционная система. Операционные системы сами по себе не могут поддерживать сеть. Для дополнения какой-нибудь *ОС* сетевыми средствами необходима процедура инсталляции сети.

Сетевая операционная система необходима для управления потоками сообщений между рабочими станциями и файловым сервером. Онаявляется прикладной платформой, предоставляет разнообразные виды сетевых служб и поддерживает работу прикладных процессов, реализуемых в сетях. NOSиспользуют архитектуру клиент–сервер или одноранговую архитектуру.

NOSопределяет группу протоколов, обеспечивающих основные функции сети. К ним относятся:

* адресация объектов сети;
* функционирование сетевых служб;
* обеспечение безопасности данных;
* управление сетью.

*Клиент для сетей* обеспечивает связь с другими компьютерами и серверами, а также доступ к файлам и принтерам.

*Сетевая карта* является устройством, физически соединяющим компьютер с сетью. Для каждой сетевой карты устанавливаются свои драйверы, значение IRQ (требования к прерыванию) и адреса ввода/вывода.

*Протоколы* используются для установления правил обмена информацией в сетях.

*Служба удаленного доступа* позволяет делать файлы и принтеры доступными для компьютеров в сети.

Применение многопользовательских версий прикладных программ резко увеличивают производительность. Многие системы управления базами данных позволяют нескольким рабочим станциям работать с общей базой данных. Большинство деловых прикладных программ также являются многопользовательскими.

Защита данных от несанкционированного доступа при работе в ЛВС необходима по следующим причинам:

* *Необходимость обеспечения гарантии от разрушений*. При работе в сети неопытных пользователей возможно уничтожение файлов и каталогов.
* *Необходимость защиты конфиденциальности*. Далеко не всегда есть желание, чтобы частная информация была доступна всем;
* *Необходимость защиты от мошенничества*. Некоторые расчетные ведомости несут в себе большие денежные суммы, и бывает, пользователи поддаются искушению выписать чек на свое имя.
* *Необходимость защиты от преднамеренных разрушений*. В некоторых случаях раздосадованный работник может испортить какую-нибудь информацию.

Фрагмент вычислительной сети включает основные типы коммуникационного оборудования, применяемого сегодня для образования локальных сетей и соединения их через глобальные связи друг с другом.

Для построения локальных связей между компьютерами используются различные виды кабельных систем, сетевые адаптеры, концентраторы, повторители. Для связей между сегментами локальной вычислительной сети используются концентраторы, мосты, коммутаторы, маршрутизаторы и шлюзы.

Для подключения локальных сетей к глобальным связям используются:

* специальные выходы (WAN–порты) мостов и маршрутизаторов;
* аппаратура передачи данных по длинным линиям – модемы (при работе по аналоговым линиям);
* устройства подключения к цифровым каналам (TA – терминальные адаптеры сетей ISDN, устройства обслуживания цифровых выделенных каналов типа CSU/DSU и т.п.).

На рис. 5.1 приведен фрагмент вычислительной сети.



Рис. 0.5 Фрагмент сети

## Физическая среда передачи данных.

Физическая среда является основой, на которой строятся физические средства соединения. Сопряжение с *физическими средствами соединения* посредством физической среды обеспечивает *Физический уровень*. В качестве физической среды широко используются эфир, металлы, оптическое стекло и кварц. На физическом уровне находится носитель, по которому передаются данные. Среда передачи данных может включать как кабельные, так и беспроводные технологии. Хотя физические кабели являются наиболее распространенными носителями для сетевых коммуникаций, беспроводные технологии все более внедряются благодаря их способности связывать глобальные сети.

На физическом уровне для физических кабелей определяются механические и электрические (оптические) свойства среды передачи, которые включают:

* тип кабелей и разъемов;
* разводку контактов в разъемах;
* схему кодирования сигналов для значений 0 и 1.

Канальный уровень определяет доступ к среде и управление передачей посредством процедуры передачи данных по каналу. В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

## Кабели связи, линии связи, каналы связи

Для организации связи в сетях используются следующие понятия:

* кабели связи;
* линии связи;
* каналы связи.

*Кабель связи* — это длинномерное изделие электротехнической промышленности. Из кабелей связи и других элементов (монтаж, крепеж, кожухи и т.д.) строят *линии связи*. Прокладка линии внутри здания задача достаточно серьезная. Длина линий связи колеблется от десятков метров до десятков тысяч километров. В любую более-менее серьезную линию связи кроме кабелей входят: траншеи, колодцы, муфты, переходы через реки, море и океаны, а также грозозащита (равно как и другие виды защиты) линий. Очень сложны охрана, эксплуатация, ремонт линий связи; содержание кабелей связи под избыточным давлением, профилактика (в снег, дождь, на ветру, в траншее и в колодце, в реке и на дне моря). Большую сложность представляют собой юридические вопросы, включающие согласование прокладки линий связи, особенно в городе. Вот чем линия (связи) отличается от кабеля. Называть кабель связи линией — все равно что асфальт, еще в кузове самосвала, именовать готовой автострадой. Разница примерно такая же.

По уже построенным линиям организуют *каналы связи*. Причем если линию, как правило, строят и сдают сразу всю, то каналы связи вводят постепенно. Уже по линии можно дать связь, но такое использование крайне дорогостоящих сооружений очень неэффективно. Поэтому применяют аппаратуру каналообразования (или, как раньше говорили, уплотнение линии). По каждой электрической цепи, состоящей из двух проводов, обеспечивают связь не одной паре абонентов (или компьютеров), а сотням или тысячам: по одной коаксиальной паре в междугородном кабеле может быть образовано до 10800 каналов тональной частоты (0,3 – 3,4 КГц) или почти столько же цифровых, с пропускной способностью 64 Кбит/с.

При наличии кабелей связи создаются линии связи, а уже по линиям связи создаются каналы связи. Линии связи и каналы связи заводятся на узлы связи. Линии, каналы и узлы образуют первичные сети связи.

## Типы кабелей и структурированные кабельные системы

В качестве среды передачи данных используются различные виды кабелей: коаксиальный кабель, кабель на основе экранированной и неэкранированной витой пары и оптоволоконный кабель. Наиболее популярным видом среды передачи данных на небольшие расстояния (до 100 м) становится *неэкранированная витая пара*, которая включена практически во все современные стандарты и технологии локальных сетей и обеспечивает пропускную способность до 100 Мб/с (на кабелях категории 5). *Оптоволоконный кабель* широко применяется как для построения локальных связей, так и для образования магистралей глобальных сетей. Оптоволоконный кабель может обеспечить очень высокую пропускную способность канала (до нескольких Гб/с) и передачу на значительные расстояния (до нескольких десятков километров без промежуточного усиления сигнала).

В качестве среды передачи данных в вычислительных сетях используются также электромагнитные волны различных частот – КВ, УКВ, СВЧ. Однако пока в локальных сетях радиосвязь используется только в тех случаях, когда оказывается невозможной прокладка кабеля, например, в зданиях. Это объясняется недостаточной надежностью сетевых технологий, построенных на использовании электромагнитного излучения. Для построения глобальных каналов этот вид среды передачи данных используется шире – на нем построены спутниковые каналы связи и наземные радиорелейные каналы, работающие в зонах прямой видимости в СВЧ диапазонах.

Очень важно правильно построить фундамент сети – кабельную систему. В последнее время в качестве такой надежной основы все чаще используется *структурированная кабельная система*.

*Структурированная кабельная система* (Structured Cabling System – SCS) – это набор коммутационных элементов (кабелей, разъемов, коннекторов, кроссовых панелей и шкафов), а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях.

Преимущества структурированной кабельной системы.

* *Универсальность.* Структурированная кабельная система при продуманной организации может стать единой средой для передачи компьютерных данных в локальной вычислительной сети.
* *Увеличение срока службы.* Срок старения хорошо структурированной кабельной системы может составлять 8-10 лет.
* *Уменьшение стоимости добавления новых пользователей и изменения их мест размещения.* Стоимость кабельной системы в основном определяется не стоимостью кабеля, а стоимостью работ по его прокладке.
* *Возможность легкого расширения сети.* Структурированная кабельная система является модульной, поэтому ее легко наращивать, позволяя легко и ценой малых затрат переходить на более совершенное оборудование, удовлетворяющее растущим требованиям к системам коммуникаций.
* *Обеспечение более эффективного обслуживания.* Структурированная кабельная система облегчает обслуживание и поиск неисправностей.
* *Надежность.* Структурированная кабельная система имеет повышенную надежность, поскольку обычно производство всех ее компонентов и техническое сопровождение осуществляется одной фирмой-производителем.

## Кабельные системы

Выделяют два больших класса кабелей: электрические и оптические, которые принципиально различаются по способу передачи по ним сигнала.

Отличительная особенность оптоволоконных систем – высокая стоимость как самого кабеля (по сравнению с медным), так и специализированных установочных элементов (розеток, разъемов, соединителей и т. п.). Правда, главный вклад в стоимость сети вносит цена активного сетевого оборудования для оптоволоконных сетей.

Оптоволоконные сети применяются для горизонтальных высокоскоростных каналов, а также все чаще стали применяться для вертикальных каналов связи (межэтажных соединений).

Оптоволоконные кабели в будущем смогут составить реальную конкуренцию медным высокочастотным, поскольку стоимость производства медных кабелей снижаться не будет, ведь для него нужна очень чистая медь, запасов которой на земле гораздо меньше, чем кварцевого песка, из которого производят оптоволокно.

Основные поставщики оптоволоконного кабеля для России – Mohawk/CDT, Lucent Technologies и AMP.

## Типы кабелей

Существует несколько различных типов кабелей, используемых в современных сетях. Ниже приведены наиболее часто используемые типы кабелей. Множество разновидностей медных кабелей составляют класс электрических кабелей, используемых как для прокладки телефонных сетей, так и для инсталляции ЛВС. По внутреннему строению различают кабели на витой паре и коаксиальные кабели.

### Кабель типа «витая пара» (twisted pair)

*Витой парой* называется кабель, в котором изолированная пара проводников скручена с небольшим числом витков на единицу длины. Скручивание проводов уменьшает электрические помехи извне при распространении сигналов по кабелю, а *экранированные витые пары* еще более увеличивают степень помехозащищенности сигналов.

Кабель типа «витая пара» используется во многих сетевых технологиях, включая Ethernet, ARCNet и IBM Token Ring.

Кабели на витой паре подразделяются на: неэкранированные (UTP – Unshielded Twisted Pair) и экранированные медные кабели. Последние подразделяются на две разновидности: с экранированием каждой пары и общим экраном (STP – Shielded Twisted Pair) и с одним только общим экраном (FTP – Foiled Twisted Pair). Наличие или отсутствие экрана у кабеля вовсе не означает наличия или отсутствия защиты передаваемых данных, а говорит лишь о различных подходах к подавлению помех. Отсутствие экрана делает неэкранированные кабели более гибкими и устойчивыми к изломам. Кроме того, они не требуют дорогостоящего контура заземления для эксплуатации в нормальном режиме, как экранированные. Неэкранированные кабели идеально подходят для прокладки в помещениях внутри офисов, а экранированные лучше использовать для установки в местах с особыми условиями эксплуатации, например, рядом с очень сильными источниками электромагнитных излучений, которых в офисах обычно нет.

Кабели классифицируются по категории, указанным в таблице 6.1. Основанием для отнесения кабеля к одной из категорий служит максимальная частота передаваемого по нему сигнала.

Таблица 0.2

|  |  |
| --- | --- |
| Категория | Частота передаваемого сигнала, (МГц) |
| 3 | 16 |
| 4 | 20 |
| 5 | 100 |
| 5+ | 300 |
| 6 | 200 |
| 7 | 600 |

### Коаксиальные кабели

*Коаксиальные* *кабели* используются в радио и телевизионной аппаратуре. *Коаксиальные* *кабели*могут передавать данные со скоростью 10 Мбит/с на максимальное расстояние от 185 до 500 метров. Они разделяются на *толстые* и *тонкие* в зависимости от толщины. Типы коаксиальных кабелей приведены в таблице 6.2.

Таблица 0.2

|  |  |
| --- | --- |
| Тип | Название, значение сопротивления |
| RG-8 и RG-11 | Thicknet, 50 Ом |
| RG-58/U | Thinnet, 50 Ом, сплошной центральный медный проводник |
| RG-58 А/U | Thinnet, 50 Ом, центральный многожильный проводник |
| RG-59 | Broadband/Cable television (широковещательное и кабельное телевидение), 75 Ом |
| RG-59 /U | Broadband/Cable television (широковещательное и кабельное телевидение), 50 Ом |
| RG-62 | ARCNet, 93 Ом |

Кабель Thinnet, известный как кабель RG-58, является наиболее широко используемым физическим носителем данных. Сети при этом не требуют дополнительного оборудования и являются простыми и недорогими. Хотя *тонкий коаксиальный кабель (Thin* *Ethernet)* позволяет передачу на меньшее расстояние, чем толстый, но для соединений *с тонким кабелем* применяются стандартные байонетные разъемы *BNC* типа *СР-50* и ввиду его небольшой стоимости он становится фактически стандартным для офисных ЛВС. Используется в технологии *Ethernet* *10Base2,* описанной ниже.

*Толстый коаксиальный кабель**(Thick Ethernet)*имеет большую степень помехозащищенности, большую механическую прочность, но требует специального приспособления для прокалывания кабеля, чтобы создать ответвления для подключения к ЛВС. Он более дорогой и менее гибкий, чем тонкий. Используется в технологии *Ethernet* *10Base5*, описанной ниже. Сети ARCNet с посылкой маркера обычно используют кабель RG-62 А/U.

### Оптоволоконный кабель

Оптоволоконный кабель (Fiber Optic Cable) обеспечивает высокую скорость передачи данных на большом расстоянии. Они также невосприимчивы к интерференции и подслушиванию. В *оптоволоконном кабеле* для передачи сигналов используется свет. Волокно, применяемое в качестве световода, позволяет передачу сигналов на большие расстояния с огромной скоростью, но оно дорого, и с ним трудно работать.

Для установки разъемов, создания ответвлений, поиска неисправностей в *оптоволоконном кабеле*необходимы специальные приспособления и высокая квалификация. *Оптоволоконный кабель* состоит из центральной стеклянной нити толщиной в несколько микрон, покрытой сплошной стеклянной оболочкой. Все это, в свою очередь, спрятано во внешнюю защитную оболочку.

Оптоволоконные линии очень чувствительны к плохим соединениям в разъемах. В качестве источника света в таких кабелях применяются *светодиоды* (*LED - Light Emitting Diode*), а информация кодируется путем изменения интенсивности света. На приемном конце кабеля детектор преобразует световые импульсы в электрические сигналы.

Существуют два типа оптоволоконных кабелей – одномодовые и многомодовые. Одномодовые кабели имеют меньший диаметр, большую стоимость и позволяют передачу информации на большие расстояния. Поскольку световые импульсы могут двигаться в одном направлении, системы на базе оптоволоконных кабелей должны иметь входящий кабель и исходящий кабель для каждого сегмента. Оптоволоконный кабель требует специальных коннекторов и высококвалифицированной установки.

## Кабельные системы Ethernet

### 10Base-T, 100Base-TX

Неэкранированная витая пара (Unshielded Twisted Pair – UTP) – это кабель из скрученных пар проводов.

Характеристики кабеля:

* диаметр проводников 0.4 – 0.6 мм (22~26 AWG), 4 скрученных пары (8 проводников, из которых для 10Base-T и 100Base-TX используются только 4). Кабель должен иметь категорию 3 или 5 и качество data grade или выше;
* максимальная длина сегмента 100 м;
* разъемы восьми контактные RJ-45.



Рис. 0.6 восьми контактные RJ-45

В таблице 6.3 приведены сигналы, соответствующие номерам контактов разъема RJ-45.

Таблица 0.3

|  |  |  |
| --- | --- | --- |
| Тип | Каскадирование | Нормальный режим |
| 1 | RD+ (прием) | TD+ (передача) |
| 2 | RD- (прием) | TD- (передача) |
| 3 | TD+ (передача) | RD+ (прием) |
| 4 | Не используется | Не используется |
| 5 | Не используется | Не используется |
| 6 | TD- (передача) | RD- (прием) |
| 7 | Не используется | Не используется |
| 8 | Не используется | Не используется |

### 10Base2

* Тонкий коаксиальный кабель;
* Характеристики кабеля: диаметр 0.2 дюйма, RG-58A/U 50 Ом;
* Приемлемые разъемы – BNC;
* Максимальная длина сегмента – 185 м;
* Минимальное расстояние между узлами – 0.5 м;
* Максимальное число узлов в сегменте – 30.

### 10Base5

* Толстый коаксиальный кабель;
* Волновое сопротивление – 50 Ом;
* Максимальная длина сегмента – 500 метров;
* Минимальное расстояние между узлами –: 2.5 м;
* Максимальное число узлов в сегменте – 100.

## Беспроводные технологии

Методы беспроводной технологии передачи данных (Radio Waves) являются удобным, а иногда незаменимым средством связи. Беспроводные технологии различаются по типам сигнала, частоте (большая частота означает большую скорость передачи) и расстоянию передачи. Большое значение имеют помехи и стоимость. Можно выделить три основных типа беспроводной технологии:

* радиосвязь;
* связь в микроволновом диапазоне;
* инфракрасная связь.

### Радиосвязь

Технологии радиосвязи пересылают данные на радиочастотах и практически не имеют ограничений по дальности. Она используется для соединения локальных сетей на больших географических расстояниях. Радиопередача в целом имеет высокую стоимость и чувствительна к электронному и атмосферному наложению, а также подвержена перехватам, поэтому требует шифрования для обеспечения уровня безопасности.

### Связь в микроволновом диапазоне

Передача данных в микроволновом диапазоне (Microwaves) использует высокие частоты и применяется как на коротких, так и на больших расстояниях. Главное ограничение заключается в том, чтобы передатчик и приемник были в зоне прямой видимости. Используется в местах, где использование физического носителя затруднено. Передача данных в микроволновом диапазоне при использовании спутников может быть очень дорогой.

### Инфракрасная связь

Инфракрасные технологии (Infrared transmission), функционируют на очень высоких частотах, приближающихся к частотам видимого света. Они могут быть использованы для установления двусторонней или широковещательной передачи на близких расстояниях. При инфракрасной связи обычно используют светодиоды (LED – *Light Emitting Diode*) для передачи инфракрасных волн приемнику. Инфракрасная передача ограничена малым расстоянием в прямой зоне видимости и может быть использована в офисных зданиях.

## Сетевое оборудование.

## Сетевые адаптеры, или NIC (Network Interface Card).

### Назначение.

Сетевые адаптеры – это сетевое оборудование, обеспечивающее функционирование сети на физическом и канальном уровнях.

Сетевой адаптер относится к периферийному устройству компьютера, непосредственно взаимодействующему со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами. Это устройство решает задачи надежного обмена двоичными данными, представленными соответствующими электромагнитными сигналами, по внешним линиям связи. Как и любой контроллер компьютера, сетевой адаптер работает под управлением драйвера операционной системы, и распределение функций между сетевым адаптером и драйвером может изменяться от реализации к реализации.

Компьютер, будь то сервер или рабочая станция, подключается к сети с помощью внутренней платы – сетевого адаптера (хотя бывают и внешние сетевые адаптеры, подключаемые к компьютеру через параллельный порт). Сетевой адаптер вставляется в гнездо материнской платы. Карты сетевых адаптеров устанавливаются на каждой рабочей станции и на файловом сервере. Рабочая станция отправляет запрос к файловому серверу и получает ответ через сетевой адаптер, когда файловый сервер готов. Сетевые адаптеры преобразуют параллельные коды, используемые внутри компьютера и представленные маломощными сигналами, в последовательный поток мощных сигналов для передачи данных по внешней сети. Сетевые адаптеры должны быть совместимы с кабельной системой сети, внутренней информационной шиной ПК и сетевой операционной системой.

### Настройка сетевого адаптера и трансивера

Для работы ПК в сети надо правильно установить и настроить сетевой адаптер. Для адаптеров, отвечающих стандарту PnP, настройка производится автоматически. В ином случае необходимо настроить линию запроса на прерывание IRQ (Interrupt Request Line) и адрес ввода/вывода (Input/Output address). Адрес ввода/вывода – это трехзначное шестнадцатеричное число, которое идентифицирует коммуникационный канал между аппаратными устройствами и центральным процессором. Чтобы сетевой адаптер функционировал правильно, должны быть настроены линия IRQ и адрес ввода/вывода. Запросы на прерывание IRQ и адреса ввода/вывода для основных устройств приведены в таблице 7.1.

Обычно сетевая карта работает с конфликтами, если двум устройствам назначен один и тот же ресурс (запроса на прерывание или адрес ввода/вывода). Сетевые карты поддерживают различные типы сетевых соединений. Физический интерфейс между самой сетевой картой и сетью называют трансивером (transceiver) – это устройство, которое как получает, так и посылает данные. Трансиверы на сетевых картах могут получать и посылать цифровые и аналоговые сигналы. Тип интерфейса, который использует сетевая карта, часто может быть физически определен на сетевой карте. Перемычки, или джамперы (маленькие перемычки, соединяющие два контакта), могут быть настроены для указания типа трансивера, который должна использовать сетевая карта в соответствии со схемой сети. Например, перемычка в одном положении может включить разъем RJ-45 для поддержки сети типа витая пара, в другом – поддержку внешнего трансивера.

Таблица 7.3

|  |  |  |
| --- | --- | --- |
| Стандартное применение | Запрос на прерывание | Диапазон ввода/вывода |
| Системный таймер | IRQ0 |  |
| Клавиатура | IRQ1 |  |
| Вторичный контроллер IRQ или видеокарта | IRQ2 |  |
| Прерывание от асинхронного последовательного порта СОМ2 и СОМ4 | IRQ3 | От 2F0 до 2FF |
| Прерывание от асинхронного последовательного порта СОМ1 и СОМ3 | IRQ4 | От 3F0 до 3FF |
| Обычно свободен (может быть занят параллельным портом LPT2) | IRQ5 |  |
| Контроллер флоппи-диска | IRQ6 |  |
| Прерывание от параллельного принтерного порта LPT1 | IRQ7 |  |
| Аппаратный таймер | IRQ8 |  |
| Обычно свободен  | IRQ9 | От 370 до 37F |
| Обычно свободен (может быть занят первичным контроллером SCSI) | IRQ10 |  |
| Обычно свободен (может быть занят вторичным контроллером SCSI) | IRQ11 | IRQ11 |
| Мышь PS/2 | IRQ12 | IRQ12 |
| Прерывание от сопроцессора  | IRQ13 | IRQ13 |
| Прерывание от первичного контроллера жесткого диска | IRQ14 | IRQ14 |
| Обычно свободен (может быть занят вторичным контроллером жесткого диска IDE) | IRQ15 | IRQ15 |

### Функции сетевых адаптеров

Сетевые адаптеры производят семь основных операций при приеме или передачи сообщения:

1. *Гальваническая развязка* с коаксиальным кабелем или витой парой. Для этой цели используются импульсные трансформаторы. Иногда для развязки используются оптроны.
2. *Прием (передача) данных*. Данные передаются из ОЗУ ПК в адаптер или из адаптера в память ПК через программируемый канал ввода/вывода, канал прямого доступа или разделяемую память.
3. *Буферизация*. Для согласования скоростей пересылки данных в адаптер или из него со скоростью обмена по сети используются буфера. Во время обработки в сетевом адаптере, данные хранятся в буфере. Буфер позволяет адаптеру осуществлять доступ ко всему пакету информации. Использование буферов необходимо для согласования между собой скоростей обработки информации различными компонентами ЛВС.
4. *Формирование пакета.* Сетевой адаптер должен разделить данные на блоки в режиме передачи (или соединить их в режиме приема) данных и оформитьв виде кадра определенного формата. Кадр включает несколько служебных полей, среди которых имеется адрес компьютера назначения и контрольная сумма кадра, по которой сетевой адаптер станции назначения делает вывод о корректности доставленной по сети информации.
5. *Доступ к каналу связи.* Набор правил, обеспечивающих доступ к среде передачи. Выявление конфликтных ситуаций и контроль состояния сети.
6. *Идентификация своего адреса* в принимаемом пакете. Физический адрес адаптера может определяться установкой переключателей, храниться в специальном регистре или прошиваться в ППЗУ*.*
7. *Преобразование* параллельного кода впоследовательный код при передачеданных, и из последовательного кода в параллельный при приеме. В режиме передачи данные передаются по каналу связи в последовательном коде.
8. *Кодирование и декодирование данных.* На этом этапе должны быть сформированы электрические сигналы, используемые для представления данных. Большинство сетевых адаптеров для этой цели используют манчестерское кодирование. Этот метод не требует передачи синхронизирующих сигналов для распознавания единиц и нулей по уровням сигналов, а вместо этого для представления 1 и 0 используется перемена полярности сигнала.
9. *Передача или прием импульсов.* В режиме передачи закодированные электрические импульсы данных передаются в кабель (при приеме импульсы направляются на декодирование).

Сетевые адаптеры вместе с сетевым программным обеспечением способны распознавать и обрабатывать ошибки, которые могут возникнуть из-за электрических помех, коллизий или плохой работы оборудования.

Последние типы сетевых адаптеров поддерживают технологию *Plug and Play (вставляй и работай)*. Если сетевую карту установить в компьютер, то при первой загрузке система определит тип адаптера и запросит для него драйверы. Внешний вид адаптера показан на рис. 7.1.



Рис. 7.7 Вид адаптера

### Базовый, или физический, адрес

Некоторые сетевые адаптеры имеют возможность использовать оперативную память ПК в качестве буфера для хранения входящих и исходящих пакетов данных. Базовый адрес (Base Memory Address) представляет собой шестнадцатеричное число, которое указывает на адрес в оперативной памяти, где находится этот буфер. Важно выбрать базовый адрес без конфликтов с другими устройствами.

### Типы сетевых адаптеров

Сетевые адаптеры различаются по типу и разрядности используемой в компьютере внутренней шины данных – ISA, EISA, PCI, MCA.

Сетевые адаптеры различаются также по типу принятой в сети сетевой технологии – Ethernet, Token Ring, FDDI и т.п. Как правило, конкретная модель сетевого адаптера работает по определенной сетевой технологии (например, Ethernet). В связи с тем, что для каждой технологии сейчас имеется возможность использования различных сред передачи данных (тот же Ethernet поддерживает коаксиальный кабель, неэкранированную витую пару и оптоволоконный кабель), сетевой адаптер может поддерживать как одну, так и одновременно несколько сред. В случае, когда сетевой адаптер поддерживает только одну среду передачи данных, а необходимо использовать другую, применяются трансиверы и конверторы.

Различные типы сетевых адаптеров отличаются не только методами доступа к среде и протоколами, но еще и следующими параметрами:

* скорость передачи;
* объем буфера для пакета;
* тип шины;
* быстродействие шины;
* совместимость с различными микропроцессорами;
* использование прямого доступа к памяти (DMA);
* адресация портов ввода/вывода и запросов прерывания;
* конструкция разъема.

Наиболее известны следующие типы адаптеров:

Адаптеры Ethernet представляют собой плату, которая вставляется в свободный слот материнской (системной) платы компьютера. Из-за широкого распространения компьютеров с системной магистралью ISA существует широкий спектр адаптеров, предназначенных для установки в слот ISA, а также производятся адаптеры, совместимые с шиной. Чаще всего адаптеры Ethernet имеют для связи с сетью два внешних разъема: для коаксиального кабеля (разъем BNC) и для кабеля на витой паре. Для выбора типа кабеля применяются перемычки или переключатели, которые устанавливаются перед подключением адаптера к сети.

Адаптеры Fast Ethernet производятся изготовителями с учетом определенного типа среды передачи. Сетевой кабель при этом подключается непосредственно к адаптеру (без трансивера).

Оптические адаптеры стандарта 10BASE-FL могут устанавливаться в компьютеры с шинами ISA, PCI, МСА. Эти адаптеры позволяют отказаться от внешних преобразователей среды и от микротрансиверов. При установке этих адаптеров возможна реализация полнодуплексного режима обмена информацией. Для повышения универсальности в оптических адаптерах сохраняется возможность соединения по витой паре с разъемом RJ-45.

Для спецификации 100BASE-FX соединение концентратора и адаптера по оптоволокну осуществляется с использованием оптических соединителей типа SC или ST. Выбор типа оптического соединителя (SC или ST) зависит от того, новая или старая это инсталляция. Для этой спецификации выпускаются сетевые адаптеры, совместимые с шиной PCI. Адаптеры способны поддерживать как полудуплексный, так и полнодуплексный режим работы. Для облегчения настройки и эксплуатации на переднюю панель адаптера вынесено несколько индикаторов состояния. Кроме того, существуют модели адаптеров, способные работать как по одномодовому, так и по многомодовому оптоволоконному кабелю.

Сетевые адаптеры для технологии Gigabit Ethernet предназначены для установки в сервера и мощные рабочие станции. Для повышения эффективности работы они способны поддерживать полнодуплексный режим обмена информацией.

Адаптеры FDRI могут использоваться на разнообразных рабочих станциях и в устройствах межсетевого взаимодействия – мостах и маршрутизаторах. Существуют адаптеры FDDI, предназначенные для работы со всеми распространенными шинами: ISA, EISA, VESA Local Bus (VLB) и т. д. В сети FDDI такие устройства, как рабочие станции или мосты и подсоединяются к кольцу через адаптеры одного из двух типов: с двойным (DAS) или одиночным (SAS) подключением. Адаптеры DAS осуществляют физическое соединение устройств как с первичным, так и со вторичным кольцом, что повышает отказоустойчивость сети. Такой адаптер имеет два разъема (розетки) оптического интерфейса. Адаптеры SAS подключают рабочие станции к концентратору FDDI через одиночную оптоволоконную линию в звездообразной топологии. Эти адаптеры представляют собой плату, на которой наряду с электронными компонентами установлен оптический трансивер с разъемом (розеткой) оптического интерфейса.

## Повторители и концентраторы

Основная функция *повторителя* (repeater), как это следует из его названия, – повторение сигналов, поступающих на его порт. Повторитель улучшает электрические характеристики сигналов и их синхронность, и за счет этого появляется возможность увеличивать общую длину кабеля между самыми удаленными в сети узлами.

Многопортовый повторитель часто называют *концентратором* (concentrator) или *хабом* (hub), что отражает тот факт, что данное устройство реализует не только функцию повторения сигналов, но и концентрирует в одном центральном устройстве функции объединения компьютеров в сеть. Практически во всех современных сетевых стандартах концентратор является необходимым элементом сети, соединяющим отдельные компьютеры в сеть.

Концентратор или Hub представляет собой сетевое устройство, действующее на физическом уровне сетевой модели OSI.

Отрезки кабеля, соединяющие два компьютера или какие либо два других сетевых устройства, называются *физическими сегментам,* поэтому концентраторы и повторители, которые используются для добавления новых физических сегментов, являются средством физической структуризации сети.

Концентратор – устройство, у которого суммарная пропускная способность входных каналов выше пропускной способности выходного канала. Так как потоки входных данных в концентраторе больше выходного потока, то главной его задачей является концентрация данных. При этом возможны ситуации, когда число блоков данных, поступающее на входы концентратора, превышает его возможности. Тогда концентратор ликвидирует часть этих блоков.

Ядром концентратора является процессор. Для объединения входной информации чаще всего используется множественный доступ с разделением времени. Функции, выполняемые концентратором, близки к задачам, возложенным на мультиплексор. Наращиваемые (модульные) концентраторы позволяют выбирать их компоненты, не думая о совместимости с уже используемыми. Современные концентраторы имеют порты для подключения к разнообразным локальным сетям.

Концентратор является активным оборудованием. Концентратор служит центром (шиной) звездообразной конфигурации сети и обеспечивает подключение сетевых устройств. В концентраторе для каждого узла (ПК, принтеры, серверы доступа, телефоны и пр.) должен быть предусмотрен отдельный порт.

Наращиваемые концентраторы представляют собой отдельные модули, которые объединяются при помощи быстродействующей системы связи. Такие концентраторы предоставляют удобный способ поэтапного расширения возможностей и мощности ЛВС.

Концентратор осуществляет электрическую развязку отрезков кабеля до каждого узла, поэтому короткое замыкание на одном из отрезков не выведет из строя всю ЛВС.



Рис. 7.2 Логический сегмент, построенный с использованием концентраторов

Концентраторы образуют из отдельных физических отрезков кабеля общую среду передачи данных – *логический сегмент*. Логический сегмент также называют доменом коллизий, поскольку при попытке одновременной передачи данных любых двух компьютеров этого сегмента, хотя бы и принадлежащих разным физическим сегментам, возникает блокировка передающей среды. Следует особо подчеркнуть, что, какую бы сложную структуру ни образовывали концентраторы, например путем иерархического соединения (рис. 7.2), все компьютеры, подключенные к ним, образуют единый логический сегмент, в котором любая пара взаимодействующих компьютеров полностью блокирует возможность обмена данными для других компьютеров.



Рис. 7.3 Внешний вид концентратора

На рис. 7.3 показан внешний вид концентратора Концентраторы поддерживают технологию plug and play и не требуют какой-либо установки параметров. Необходимо просто спланировать свою сеть и вставить разъемы в порты хаба и компьютеров.

### Планирование сети с хабом

При выборе места для установки концентратора примите во внимание следующие аспекты:

* местоположение;
* расстояния;
* питание.

Выбор места установки концентратора является наиболее важным этапом планирования небольшой сети. Хаб разумно расположить вблизи геометрического центра сети (на одинаковом расстоянии от всех компьютеров). Такое расположение позволит минимизировать расход кабеля. Длина кабеля от концентратора до любого из подключаемых к сети компьютеров или периферийных устройств не должна превышать 100 м.

Концентратор можно поставить на стол или закрепить его на стене с помощью входящих в комплект хаба скоб. Установка хаба на стене позволяет упростить подключение кабелей, если они уже проложены в офисе.

При планировании сети есть возможность наращивания (каскадирования) хабов.

### Преимущества концентратора

Концентраторы имеют много преимуществ. Во-первых, в сети используется топология звезда, при которой соединения с компьютерами образуют лучи, а хаб является центром звезды. Такая топология упрощает установку и управление сети. Любые перемещения компьютеров или добавление в сеть новых узлов при такой топологии весьма несложно выполнить. Кроме того, эта топология значительно надежнее, поскольку при любом повреждении кабельной системы сеть сохраняет работоспособность (перестает работать лишь поврежденный луч). Светодиодные индикаторы хаба позволяют контролировать состояние сети и легко обнаруживать неполадки.

Различные производители концентраторов реализуют в своих устройствах различные наборы вспомогательных функций, но наиболее часто встречаются следующие:

* объединение сегментов с различными физическими средами (например, коаксиал, витая пара и оптоволокно) в единый логический сегмент;
* автосегментация портов – автоматическое отключение порта при его некорректном поведении (повреждение кабеля, интенсивная генерация пакетов ошибочной длины и т. п.);
* поддержка между концентраторами резервных связей, которые используются при отказе основных;
* защита передаваемых по сети данных от несанкционированного доступа (например, путем искажения поля данных в кадрах, повторяемых на портах, не содержащих компьютера с адресом назначения);
* поддержка средств управления сетями – протокола SNMP, баз управляющей информации MIB.

## Мосты и коммутаторы

*Мост* (bridge) – ретрансляционная система, соединяющая каналы передачи данных.



Рис. 7.4 Структура моста

В соответствии с базовой эталонной моделью взаимодействия открытых систем мост описывается протоколами физического и канального уровней, над которыми располагаются канальные процессы. Мост опирается на пару связываемых им физических средств соединения, которые в этой модели представляют физические каналы. Мост преобразует физический (1A, 1B) и канальный (2A, 2B) уровни различных типов (рис. 9.4). Что касается канального процесса, то он объединяет разнотипные каналы передачи данных в один общий.

*Мост* (bridge), а также его быстродействующий аналог – *коммутатор* (switching hub), делят общую среду передачи данных на логические сегменты. Логический сегмент образуется путем объединения нескольких физических сегментов (отрезков кабеля) с помощью одного или нескольких концентраторов. Каждый логический сегмент подключается к отдельному порту моста/коммутатора. При поступлении кадра на какой-либо из портов мост/коммутатор повторяет этот кадр, но не на всех портах, как это делает концентратор, а только на том порту, к которому подключен сегмент, содержащий компьютер-адресат.

Мосты могут соединять сегменты, использующие разные типы носителей, например 10BaseT (витая пара) и 10Base2 (тонкий коаксиальный кабель). Они могут соединять сети с разными методами доступа к каналу, например сети Ethernet (метод доступа CSMA/CD) и Token Ring (метод доступа TPMA).

### Различие между мостом и коммутатором

Разница между мостом и коммутатором состоит в том, что мост в каждый момент времени может осуществлять передачу кадров только между одной парой портов, а коммутатор одновременно поддерживает потоки данных между всеми своими портами. Другими словами, мост передает кадры последовательно, а коммутатор параллельно.

Мосты используются только для связи локальных сетей с глобальными, то есть как средства удаленного доступа, поскольку в этом случае необходимость в параллельной передаче между несколькими парами портов просто не возникает.



Рис. 7.5 Соединение двух сетей при помощи двух каналов

Когда появились первые устройства, позволяющие разъединять сеть на несколько доменов коллизий (по сути фрагменты ЛВС, построенные на hub-ах), они были двух портовыми и получили название мостов (bridge-ей). По мере развития данного типа оборудования, они стали многопортовыми и получили название коммутаторов (switch-ей). Некоторое время оба понятия существовали одновременно, а позднее вместо термина «мост» стали применять «коммутатор». Далее в этой теме будет использоваться термин «коммутатор» для обозначения этих обеих разновидностей устройств, поскольку все сказанное ниже в равной степени относится и к мостам, и к коммутаторам. Следует отметить, что в последнее время локальные мосты полностью вытеснены коммутаторами.

Нередки случаи, когда необходимо соединить локальные сети, в которых различаются лишь протоколы физического и канального уровней. Протоколы остальных уровней в этих сетях приняты одинаковыми. Такие сети могут быть соединены мостом. Часто мосты наделяются дополнительными функциями. Такие мосты обладают определенным *интеллектом* (интеллектом в сетях называют действия, выполняемые устройствами) и фильтруют сквозь себя блоки данных, адресованные абонентским системам, расположенным в той же сети. Для этого в памяти каждого моста имеются адреса систем, включенных в каждую из сетей. Блоки, проходящие через *интеллектуальный* мост, дважды проверяются, на входе и выходе. Это позволяет предотвращать появление ошибок внутри моста.

Мосты не имеют механизмов управления потоками блоков данных. Поэтому может оказаться, что входной поток блоков окажется большим, чем выходной. В этом случае мост не справится с обработкой входного потока, и его буферы могут переполняться. Чтобы этого не произошло, избыточные блоки выбрасываются. Специфические функции выполняет мост в радиосети. Здесь он обеспечивает взаимодействие двух радиоканалов, работающих на разных частотах. Его именуют *ретранслятором*.

Мосты (bridges) оперируют данными на высоком уровне и имеют совершенно определенное назначение. Во-первых, они предназначены для соединения сетевых сегментов, имеющих различные физические среды, например для соединения сегмента с оптоволоконным кабелем и сегмента с коаксиальным кабелем. Мосты также могут быть использованы для связи сегментов, имеющих различные протоколы низкого уровня (физического и канального).

### Коммутатор

*Коммутатор* (switch) – устройство, осуществляющее выбор одного из возможных вариантов направления передачи данных.



Рис. 7.6 Внешний вид коммутатора Switch 2000

В коммуникационной сети коммутатор является ретрансляционной системой (система, предназначенная для передачи данных или преобразования протоколов), обладающей свойством прозрачности (т.е. коммутация осуществляется здесь без какой-либо обработки данных). Коммутатор не имеет буферов и не может накапливать данные. Поэтому при использовании коммутатора скорости передачи сигналов в соединяемых каналах передачи данных должны быть одинаковыми. Канальные процессы, реализуемые коммутатором, выполняются специальными интегральными схемами. В отличие от других видов ретрансляционных систем, здесь, как правило, не используется программное обеспечение.



Рис. 7.7 Структура коммутатора

Вначале коммутаторы использовались лишь в территориальных сетях. Затем они появились и в локальных сетях, например, частные учрежденческие коммутаторы. Позже появились коммутируемые локальные сети. Их ядром стали коммутаторы локальных сетей.

Коммутатор (Switch) может соединять серверы в кластер и служить основой для объединения нескольких рабочих групп. Он направляет пакеты данных между узлами ЛВС. Каждый коммутируемый сегмент получает доступ к каналу передачи данных без конкуренции и видит только тот трафик, который направляется в его сегмент. Коммутатор должен предоставлять каждому порту возможность соединения с максимальной скоростью без конкуренции со стороны других портов (в отличие от совместно используемого концентратора). Обычно в коммутаторах имеются один или два высокоскоростных порта, а также хорошие инструментальные средства управления. Коммутатором можно заменить маршрутизатор, дополнить им наращиваемый маршрутизатор или использовать коммутатор в качестве основы для соединения нескольких концентраторов. Коммутатор может служить отличным устройством для направления трафика между концентраторами ЛВС рабочей группы и загруженными файл-серверами.

### Коммутатор локальной сети

*Коммутатор локальной сети* (local-area network switch) – устройство, обеспечивающее взаимодействие сегментов одной либо группы локальных сетей.

Коммутатор локальной сети, как и обычный коммутатор, обеспечивает взаимодействие подключенных к нему локальных сетей (рис.7.8). Но в дополнение к этому он осуществляет преобразование интерфейсов, если соединяются различные типы сегментов локальной сети. Чаще всего это сети Ethernet, кольцевые сети IBM, сети с оптоволоконным распределенным интерфейсом данных.



Рис. 7.8 Схема подключения локальных сетей к коммутаторам

В перечень функций, выполняемых коммутатором локальной сети, входят:

* обеспечение сквозной коммутации;
* наличие средств маршрутизации;
* поддержка простого протокола управления сетью;
* имитация моста либо маршрутизатора;
* организация виртуальных сетей;
* скоростная ретрансляция блоков данных.

## Маршрутизатор

*Маршрутизатор* (router) – ретрансляционная система, соединяющая две коммуникационные сети либо их части.

Каждый маршрутизатор реализует протоколы *физического* (1А, 1B), *канального* (2А, 2B) и *сетевого* (3A, 3B) уровней, как показано на рис.7.9. Специальные сетевые процессы соединяют части коммутатора в единое целое. Физический, канальный и сетевой протоколы в разных сетях различны. Поэтому соединение пар коммуникационных сетей осуществляется через маршрутизаторы, которые осуществляют необходимое преобразование указанных протоколов. Сетевые процессы выполняют взаимодействие соединяемых сетей.

Маршрутизатор работает с несколькими каналами, направляя в какой-нибудь из них очередной блок данных.

Маршрутизаторы обмениваются информацией об изменениях структуры сетей, трафике и их состоянии. Благодаря этому, выбирается оптимальный маршрут следования блока данных в разных сетях от абонентской системы-отправителя к системе-получателю. Маршрутизаторы обеспечивают также соединение административно независимых коммуникационных сетей.



Рис. 7.9 Структура маршрутизатора

Архитектура маршрутизатора также используется при создании узла коммутации пакетов.

### Различие между маршрутизаторами и мостами

Маршрутизаторы превосходят мосты своей способностью фильтровать и направлять пакеты данных на сети. Так как маршрутизаторы работают на сетевом уровне, они могут соединять сети, использующие разную сетевую архитектуру, методы доступа к каналам связи и протоколы.

Маршрутизаторы не обладают такой способностью к анализу сообщений как мосты, но зато могут принимать решение о выборе оптимального пути для данных между двумя сетевыми сегментами.

Мосты принимают решение по поводу адресации каждого из поступивших пакетов данных, переправлять его через мост или нет в зависимости от адреса назначения. Маршрутизаторы же выбирают из таблицы маршрутов наилучший для данного пакета.

В поле зрения маршрутизаторов находятся только пакеты, адресованные к ним предыдущими маршрутизаторами, в то время как мосты должны обрабатывать все пакеты сообщений в сегменте сети, к которому они подключены.

Тип топологии или протокола уровня доступа к сети не имеет значения для маршрутизаторов, так как они работают на уровень выше, чем мосты (сетевой уровень модели OSI). Маршрутизаторы часто используются для связи между сегментами с одинаковыми протоколами высокого уровня. Наиболее распространенным транспортным протоколом, который используют маршрутизаторы, является IPX фирмы Novell или TCP фирмы Microsoft.

Необходимо запомнить, что для работы маршрутизаторов требуется один и тот же протокол во всех сегментах, с которыми он связан. При связывании сетей с различными протоколами лучше использовать мосты. Для управления загруженностью трафика сегмента сети также можно использовать мосты.

## Шлюзы

*Шлюз* (gateway) – ретрансляционная система, обеспечивающая взаимодействие информационных сетей.



Рис. 7.80 Структура шлюза

Шлюз является наиболее сложной ретрансляционной системой, обеспечивающей взаимодействие сетей с различными наборами протоколов всех семи уровней. В свою очередь, наборы протоколов могут опираться на различные типы физических средств соединения.

В тех случаях, когда соединяются информационные сети, то в них часть уровней может иметь одни и те же протоколы. Тогда сети соединяются не при помощи шлюза, а на основе более простых ретрансляционных систем, именуемых маршрутизаторами и мостами.

Шлюзы оперируют на верхних уровнях модели OSI (сеансовом, представительском и прикладном) и представляют наиболее развитый метод подсоединения сетевых сегментов и компьютерных сетей. Необходимость в сетевых шлюзах возникает при объединении двух систем, имеющих различную архитектуру. Например, шлюз приходится использовать для соединения сети с протоколом TCP/IP и большой ЭВМ со стандартом SNA. Эти две архитектуры не имеют ничего общего, и потому требуется полностью переводить весь поток данных, проходящих между двумя системами.

В качестве шлюза обычно используется выделенный компьютер, на котором запущено программное обеспечение шлюза и производятся преобразования, позволяющие взаимодействовать нескольким системам в сети. Другой функцией шлюзов является преобразование протоколов. При получении сообщения IPX/SPX для клиента TCP/IP шлюз преобразует сообщения в протокол TCP/IP.

Шлюзы сложны в установке и настройке. Шлюзы работают медленнее, чем маршрутизаторы.

## Установка и настройка сетевой карты.

**Цель:** научиться подключать компьютер в локальную сеть.

**Оборудование:** IBM-PC совместимый компьютер, сетевая карта.

**Программное обеспечение**: MS Windows.

**Порядок выполнения работы:**

Для подключения компьютера к локальной сети необходимо:

1. Установить сетевую карту (выполняется условно)
	1. выключить и обесточить компьютер,
	2. снять защитный корпус системного блока
	3. физически установить сетевую карту в слот, соответствующий ее интерфейсу.
2. Подключить к сетевой карте сетевой кабель. Проверить подключение другого конца кабеля к концентратору (витая пара) или сегменту сетевого кабеля (коаксиальный кабель).
3. Включить компьютер. Установить драйвер сетевой карты (автоматически или самостоятельно).
* Нажмите кнопку **Пуск** на панели задач. Выберете пункт **Настройка -> Панель Управления**. **-> Сетевые подключения**
* Вызовите свойства объекта **Подключение по локальной сети**
* Определите и исследуйте компоненты, используемые этим подключение. Заполните теблицу:

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Вопрос** | **ответ** |
|  | Какие компоненты используются подключением по локальной сети? |  |
|  | Выводится или нет значок, уведомляющий о подключении по локальной сети? |  |
|  | Где находится этот значок? |  |
|  | Как называется компонент, обеспечивающий управление сетевым трафиком, включая скорость передачи м службы приоритетов? |  |
|  | Какая сетевая карта установлена на компьютере? |  |
|  | Назовите дату выпуска драйвера сетевой карты? |  |
|  | Назовите версию драйвера? |  |
|  | Назовите поставщика драйвера? |  |
|  | Сетевая карат поддерживает управление электропитанием компьютера? |  |
|  | Что такое брандмауэр Windows?  |  |
|  | Включен ли брандмауэр на вашем компьютере? |  |
|  | Напишите IP адрес вашего компьютера? |  |
|  | К какому классу сетей относится эта подсеть? |  |
|  | Напишите адрес шлюза? |  |
|  | Почему не указан DNS сервер? |  |

1. Установить и настроить сетевые протоколы и IP адреса.
	1. Поменяйте класс сети на любой другой.
	2. Назначьте шлюзом компьютер вашего соседа справа.

**Вопросы к защите:**

1. Порядок установки и настройки сетевой карты.
2. Что такое: BNC-коннектор, UTP, RG-58, RJ-15, 10Base-T
3. Локальная сеть. Признаки классификации сетей.
4. Топология сетей. Физические среды передачи данных.
5. Какому уровню модели OSI соответствует: установка сетевой карты и подключение к ЛВС, драйвер сетевой карты.

## Настройка сетевых протоколов.

**Цель:** научиться настраивать сетевые протоколы для работы в локальной и глобальных сетях.

**Оборудование:** IBM-PC совместимый компьютер, сетевая карта.

**Программное обеспечение**: MS Windows.

**Время:** 2 урока.

**Порядок выполнения работы:**

1. Проверить подключение к сетевой карте сетевого кабеля. Проверить подключение другого конца кабеля к концентратору (витая пара) или сегменту сетевого кабеля (коаксиальный кабель).
2. Нажмите кнопку **Пуск** на панели задач. Выберете пункт **Настройка -> Панель Управления**. **-> Сетевые подключения**
3. Вызовите свойства объекта **Подключение по локальной сети**
4. Определите: какой протокол установлен по умолчанию на вашем компьютере (см компоненты, используемые подключением).
5. Настройка протокола:
	1. Вызовите свойства **Протокола Интернета (TCP/IP)**.
	2. Заполните таблицу

|  |  |
| --- | --- |
| IP адрес |  |
| Маска подсети |  |
| Основной шлюз |  |
| Предпочитаемый DNS-сервер |  |
| Альтернативный DNS-сервер |  |

* 1. проверьте работу сетевого интерфейса командой ping IP-адрес и работу сервера DNS командой ping доменное\_имя. Заполните таблицу

|  |  |
| --- | --- |
| IP адрес соседа справа | Время отзыва:  |
| IP адрес самой машины | Время отзыва: |
| IP адрес центральной машины в аудитории | Время отзыва: |
| Сколько пакетов было передано за одно пингование: |  |
| Запишите команду пингования DNS сервера |  |

1. Проверьте работу маршрутизации командой tracert IP-адрес (tracert доменное\_имя). Заполните таблицу:

|  |  |
| --- | --- |
| Сетевая плата |  |
| Используемые протоколы |  |
| IP-адрес |  |
| Маска подсети |  |
| Доменное имя компьютера |  |
| DNS-сервер(ы) |  |
| Шлюз |  |

**Вопросы к защите:**

1. Порядок настройки стека протоколов TCP/IP.
2. Что такое: IP-адрес, маска подсети, доменное имя, DNS-сервер, шлюз.
3. Маршрутизация. Принципы маршрутизации.
4. Назначение и принцип работы сервиса ARP.
5. Как определить доступность вычислительной системы по сети?

## Настройка удаленного соединения.

**Цель:** научиться устанавливать и настраивать удаленное соединение в локальной сети

**Оборудование:** IBM-PC совместимый компьютер, сетевая карта.

**Программное обеспечение**: MS Windows.

**Время:** 2 урока.

**Порядок выполнения работы:**

1. Проверить подключение к сетевой карте сетевого кабеля. Проверить подключение другого конца кабеля к концентратору (витая пара) или сегменту сетевого кабеля (коаксиальный кабель).
2. Нажмите кнопку **Пуск** на панели задач. Выберете пункт **Настройка -> Панель Управления**. **-> Сетевые подключения**
3. В панели сетевых задач выберите создания нового подключения. Опишите ваши действия для подключения компьютера в сеть Интернет, в локальную сеть. Опишите настройки брандмауэра.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Настроим выход в Интернет с помощью карты «Волга телеком»:
2. Настроим выход в Интернет с помощью карты «Диалог М»
	1. Фазы установления соединения:
		* набор номера
		* согласование параметров связи
		* проверка имени пользователя и пароля
		* вход в сеть
		* установка соединения

**Вопросы к защите:**

1. Порядок настройки удаленного доступа в сеть.
2. Что такое: ISP, DCE, DTE, канал передачи данных, модем.
3. Модемы: назначение, типы, выполняемые функции, протоколы.
4. Протоколы канального уровня: UUCP, SLIP, PPP.
5. Фазы установления удаленного соединения.

## Настройка доступа к общим ресурсам ЛВС

**Цель:** научиться устанавливать и настраивать доступ к общим ресурсам ЛВС

**Оборудование:** IBM-PC совместимый компьютер, сетевая карта.

**Программное обеспечение**: MS Windows.

**Время:** 2 урока.

**Порядок выполнения работы:**

1. Создать у себя на компьютере, на диске D папку с названием группы.
2. Настроить к ней общий доступ с полными правами.
3. Организовать доступ к сетевым принтерам.
4. В ней создать текстовый файл со следующими характеристиками: имя файла – фамилия (или фамилии студентов, работающих за этим компьютером), содержимое – IP адрес компьютера, его имя в сети, имя рабочей группы, перечислить все компьютеры в этой рабочей группе, указать сетевое имя принтера и его спецификацию.
5. Передать свой файл по сети всем студентам на занятии.
6. Забрать такой же файл с компьютера справа, добавив к его имени знак «+».
7. Создать папку с ограниченными правами (только для чтения). Протестируйте свою папку с чужого компьютера на возможность записи в ней.
8. Построить схему ЛВС, которую вы исследовали.

**Дополнительная информация:**

Настройка сетевого доступа к дискам

Вы можете открыть пользователям локальной сети доступ к дискам вашего компьютера, что позволит им просматривать, редактировать и сохранять файлы на этих дисках, создавать и удалять папки, прослушивать хранящиеся на вашем компьютере аудиозаписи, устанавливать с вашего винчестера различные программы. Совместное использование дисковых ресурсов может быть необходимо, например, в случае, если только ваш компьютер во всей сети оснащен приводом CD-ROM или DVD.

Чтобы открыть пользователям локальной сети доступ к дисковым ресурсам вашего компьютера, необходимо проделать следующее:

* откройте системное окно Мой компьютер;
* щелкните правой кнопкой мыши на изображении диска, к которому вы хотите открыть доступ по сети, и выберите в появившемся меню пункт Свойства;
* в открывшемся окне Свойства: локальный диск перейдите ко вкладке Доступ и выберите пункт Если вы хотите открыть доступ к корневой папке диска, щелкните здесь (для MS Windows XP), в другой операционной системе семейства Windows достаточно установить переключатель в положение Общий ресурс;
* в разделе Сетевой совместный доступ и безопасность установите флажок рядом с пунктом Открыть общий доступ к этой папке и введите в поле Общий ресурс сетевое имя своего диска — оно будет отображаться в папке Сетевое окружение других пользователей локальной сети (рис. 1);
* если вы хотите открыть пользователям сети полный доступ к своему диску, то есть разрешить им создавать, удалять, перемещать и переименовывать файловые объекты на вашем винчестере, установите флажок рядом с пунктом Разрешить изменение файлов по сети. Если флажок сброшен, пользователи смогут обращаться к диску в режиме «только чтение»;
* щелкните на кнопке ОК, чтобы сохранить внесенные вами изменения. Диск, к которому открыт доступ из локальной сети, будет показан в папке Мой компьютер с помощью специальной метки в виде изображения открытой ладони.



Рис. 1. Настройка общего доступа к локальному ресурсу

*ПРИМЕЧАНИЕ*

*В целях безопасности не рекомендуется открывать доступ к диску или логическому дисковому разделу, на котором установлена Microsoft Windows. Кто-либо из пользователей локальной сети может случайно или намеренно внести изменения в системные файлы, в результате чего Windows придет в неработоспособное состояние.*

Управление сетевым доступом к папкам

Открытие сетевого доступа к дискам и дисковым разделам является потенциально опасным для хранящихся на винчестере данных, поскольку пользователь локальной сети может случайно или намерено уничтожить, переименовать или изменить файлы, предназначенные только для вашего личного пользования. С точки зрения безопасности лучше открыть доступ не к диску в целом, а к одной дисковой директории, предназначенной для совместного использования в локальной сети. Вы можете назначить такой папке произвольное сетевое имя, например, аналогичное системному имени дискового раздела, благодаря чему пользователям будет казаться, что они работают непосредственно с диском вашего компьютера, в то время как доступ к каким-либо ресурсам за пределами данной директории будет для них закрыт. Чтобы настроить сетевой доступ к какой-либо папке на жестком диске компьютера, необходимо проделать описанные ниже шаги.

* Перейдите на один из дисков своего компьютера и создайте папку с произвольным именем, которую вы хотите сделать доступной из локальной сети.
* Щелкните на значке папки правой кнопкой мыши и в появившемся меню выберите пункт Свойства.
* В открывшемся окне Свойства папки перейдите к вкладке Доступ.
* В разделе Сетевой совместный доступ и безопасность установите флажок рядом с пунктом Открыть общий доступ к этой папке и введите в поле Сетевой ресурс сетевое имя вашей папки. Оно может совпадать с именем вашего диска, например С, D, Е или F, либо быть произвольным, например, Netfolder. Папка, сетевое имя которой совпадает с именем одного из дисковых разделов, фактически может находится на любом диске. Например, папка с сетевым именем С может храниться на диске D. Локальное и сетевое имя папки могут быть различными.
* Если вы хотите открыть пользователям сети полный доступ к данной папке, установите флажок рядом с пунктом Разрешить изменение файлов по сети. Если флажок сброшен, пользователи смогут обращаться к папке в режиме «только чтение».
* Щелкните на кнопке О К, чтобы сохранить внесенные вами изменения. Папка, к которой открыт сетевой доступ, будет отображаться в окне Проводника с помощью специальной метки в виде изображения открытой ладони.
* Управление доступом к локальному принтеру

Вы можете открыть пользователям локальной сети доступ к принтеру, подключенному к вашему компьютеру, чтобы они могли печатать свои документы по сети. Для этого:

* перейдите в системную папку Принтеры и факсы, выполнив команды Пуск
* Панель управления Принтеры и другое оборудование Принтеры и факсы;
а щелкните на значке установленного в вашей системе принтера правой кнопкой мыши и выберите в появившемся меню пункт Свойства;
* перейдите к вкладке Доступ диалогового окна Свойства: Принтер, установите переключатель в положение Общий доступ к данному принтеру и введите в поле Сетевое имя произвольное сетевое имя принтера;
* щелкните на кнопке ОК, чтобы сохранить внесенные изменения. Принтер, к которому открыт сетевой доступ, будет отображаться в окне Принтеры и факсы с помощью специальной метки в виде изображения открытой ладони.

Подключение сетевого принтера

Если принтер подключен не к вашему, а к другому компьютеру локальной сети, вы можете использовать его для распечатки своих документов. Для этого:

* а перейдите в системную папку Принтеры и факсы, выполнив команды Пуск Панель управления Принтеры и другое оборудование Принтеры и факсы;
* щелкните на пункте Установка принтера в командном меню Задачи печати;
* в появившемся окне Мастера установки принтеров нажмите на кнопку Далее;
* в следующем окне Мастера установки принтеров выберите пункт Сетевой принтер, подключенный к другому компьютеру и снова нажмите Далее;
* в следующем окне установите переключатель в положение Обзор принтеров и щелкните на кнопке Далее;
* в предложенном списке принтеров, доступных в локальной сети, выберите нужный и снова нажмите Далее (рис. 2);
* если вы хотите сделать этот принтер используемым в вашей системе по умолчанию, установите в следующем окне переключатель в положение Да и щелкните на кнопке Далее;
* настройка сетевого принтера завершена. Нажмите на кнопку Готово, чтобы покинуть окно Мастера установки принтеров. Теперь все документы, распечатываемые вами из приложений Windows, будут направляться на этот принтер.


Рис.2. Выбор сетевого принтера из списка

Подключение сетевого диска

Некоторые программы MS Windows, работающие с файловыми ресурсами других сетевых компьютеров (например, сетевая версия бухгалтерского пакета «1С») требуют, чтобы физический диск или дисковый раздел удаленного компьютера был подключен к вашей системе как сетевой диск. Сетевые диски отображаются в системном окне Мой компьютер наравне с вашими локальными дисками, вы можете обращаться к ним и работать с их содержимым так же, как с содержимым собственного винчестера. Для того чтобы подключить к системе сетевой диск, необходимо выполнить следующие операции:

* щелкните правой кнопкой мыши на расположенном на Рабочем столе Windows значке Мой компьютер и выберите в появившемся меню пункт Подключить сетевой диск. На экране появится окно одноименного Мастера подключения сетевого диска;
* выберите в меню Диск символ, которым будет обозначаться подключаемый к вашей системе сетевой диск, затем щелкните на расположенной рядом кнопке Обзор;
* в открывшемся окне Обзор папки выберите из списка доступный для совместного использования диск удаленного компьютера и нажмите кнопку ОК.
* если вы хотите, чтобы соединение с данным сетевым диском автоматически восстанавливалось всякий раз при включении вашего компьютера, в окне Мастера подключения сетевого диска установите флажок рядом с функцией Восстанавливать при входе в систему. Щелкните на кнопке Готово.

Созданный вами сетевой диск будет обозначен в окне Мой компьютер выбранным вами символом и сетевым именем компьютера, которому фактически принадлежит. Например, сетевой диск Е on Veronika (К:) является диском Е подключенного к сети компьютера Veronika, но в вашей системе он обозначен символом К.

Чтобы отключить сетевой диск, щелкните на его изображении в окне Мой компьютер правой кнопкой мыши и в появившемся контекстном меню выберите пункт Отключить.

**Вопросы к защите:**

* 1. Каким образом внешний компьютер идентифицируется на вашем компьютере?
	2. Дайте определение одноранговых локальных вычислительных сетей.
	3. Как осуществить доступ к Вашим каталогам с другого ПК?
	4. В каких случаях лучше использовать МАСТЕР НАСТРОЙКИ СЕТИ, а в каких лучше самостоятельно настроить

## Установка и настройка серверов.

**Цель:** на примере программ запустить FTP и HTTP сервера у себя на компьюетере

**Оборудование:** IBM-PC совместимый компьютер, сетевая карта.

**Программное обеспечение**: MS Windows, Cerberus FTP Server, WWW File Share PRO 4.0

**Время:** 2 урока.

**Порядок выполнения работы:**

1. Ознакомиться с описанием и назначение программ.
2. Выяснить IP адрес, компьютера на котором работаете. Выяснить адрес proxy – сервера в локальной сети.

|  |  |
| --- | --- |
| IP адрес |  |
| IP PROXY server |  |

1. Установить программу Cerberus FTP Server, предназначенную для запуска FTP сервера.

1. Выбрать тип лицензии: для бизнеса или домашнего использования. Выбирайте Personal Use.



2. Создать аккаунт по умолчанию. Обычно это anonymous, т.е. любой человек, зная ip-адрес вашего сервера, сможет войти на него. Для анонима можно не задавать пароль.



Initial Root - это корневая папка FTP сервера, к которой впоследствии вы сможете добавить другие доступные пользователям папки.

3. Последняя опция дает возможность включить определение IP-адреса FTP для того, чтобы сервер был доступен не только из локальной сети, но и из внешнего интернета. Так же эта настройка открывает 21-й порт для обмена данными. Если у вас установлен файрвол (а он обязательно должен быть установлен!), то разрешите в нем использование этого порта.



Все, жмем кнопку Finish и наш FTP переходит в режим Online, готовясь принять первых посетителей. О режиме работы сервера сигнализирует зеленый или красный индикатор в статусной строке главного окна сервера:



На вкладке LOG отображаются все серверные сообщения о подключениях к FTP, передвижениях по каталогам, запросах на download/upload и прочее...
Вкладка CONNECTIONS показывает всех подключенных в данный момент пользователей. Список обновляется в режиме реального времени. Если кликнуть на любом пользователе правой кнопкой, то можно получить 2 команды управления подключением: Terminate User (принудительно выбросить пользователя с вашего FTP) и Block Address (блокировать данный IP-адрес, чтобы какой-нибудь хулиган не смог попасть на сервер).
На вкладке TRANSFERS видны производимые с файлами операции: процент скачивания/закачивания, прошедшее и оставшееся время, имя пользователя, имя файла и пр.
И, наконец, на вкладке STATISTICS отображается сводная информация о работе FTP сервера:  общее число подключений, число подключений в данный момент, количество удачно/неудачно скаченных с сервера и закаченных на него файлов.

Дефолтовый-то аккаунт мы создали, но никакие каталоги для него еще недоступны, посетители при входе на FTP будут видеть только пустую папку ftproot.

Для определения параметров аккаунта выберите в меню "Configuration - User Management" или нажмите на панели инструментов кнопку с изображением человечков:



Разберемся с настройками аккаунта для анонима.
- Отключение аккаунта производится простым снятием галочки в окошке "Cerberus User Accounts- Property".
- Там же можно задать пароль, дважды кликнув по слову "Password".
- Simultaneous Logins - число одновременных заходов для данного аккаунта. Выставьте необходимое значение или оставьте Unlimited по умолчанию. Чем больше посетителей входят одновременно на ваш сервер, тем больше ресурсов они будут потреблять. Представьте себе, что получится, если 10 человек будут одновременно качать к себе 10 фильмов? А 50 человек? Лично мне было бы жалко мой жесткий диск :)
- Simple Directories - быстрое отключение всех виртуальных каталогов. В этом случае пользователи снова увидят лишь пустой каталог ftproot

Теперь научимся подключать каталоги. В окошке "Virtual Root Directory for" жмем на кнопку "...", выбираем нужный каталог (который, кстати, может быть расположен на любом подключенном носителе: CD, другой раздел жесткого диска, FDD и пр.), затем кнопку "Add" - выбранный каталог добавлен в дерево ftproot. Теперь настроим для него права (permissions): скачивание, закачка на сервер, переименование, удаление, создание каталогов, отображение скрытых файлов. Комбинация прав может быть любой для каждого каталога и каждой группы пользователей.

Кстати, еще немного о пользователях. Может быть, у вас есть информация, которой можно поделиться лишь с избранными? Легко! Создайте для них отдельный паролированный аккаунт. Делается это нажатием кнопки "New":



Обратите внимание, что здесь произошли некоторые изменения по сравнению с анонимным логином, а именно:
- название группы является так же логином, который нужно будет ввести в FTP-клиенте для корректного подключения к серверу
- задан пароль для группы special
- число одновременных подключений ограничено 5 логинами
- отключена возможность анонимного подключения именно для этой группы! Не забывайте снимать галочку, если создаете особые группы, иначе любой гость без ввода пароля сможет увидеть ваши секретные данные :)

Опции"NT Users" мы касаться не будем, она дает возможность использовать учетные записи компьютеров для подключения к FTP. Оставим эту возможность отключенной.

Сервер запущен, пользователи оповещены, вы наблюдаете за операциями, ощущая себя великим и могучим :) Все довольны... Но что делать, если вдруг объявится какой-нибудь доморощенный кулхацер, смыслом никчемной жизни которого является процесс устраивания подлянок другим? Если он вдруг начнет устраивать ддос-атаку на ваш FTP или просто будет хулиганить в публичных каталогах, закачивания вам массу никчемных файлов, вирусов и пр. ? Каждый раз кликать по его нику и делать "Terminate User" - рука устанет. Для таких случаев Cerberus предоставляет в наше несколько инструментов:



На вкладке General можно четко разграничить возможность доступа к серверу, добавляя целые диапазоны IP-адресов в "черный" или "белый" списки: deny / allow.
Но можно указать и конкретный IP-адрес, если снять галочку с опции "Assign a Range of addresses".

Вкладка "Auto-Blocking" более интересна:



"Enable Auto-Blocking (DoS Protection)" - рекомендую сразу же включить эту опцию, будет только лучше. Ее цель: определять и блокировать подозрительные подключения.
Наример, кто-то долго и безостановочно пытается подключиться к вашему FTP в надежде методом перебора найти логин/пароль для какой-либо группы пользователей? Установите значение "Failed Login Attempts before Auto-Block" (число неудачных попыток логина перед автоблокировкой) "5" и через это число попыток наглому пользователю будет блокирован доступ к серверу. Время и режим блокировки определите чуть ниже: блокировать на ХХ минут или навсегда. Все блокированные адреса помещаются в окно "IP addresses (being watched)", откуда ошибочно блокированный адрес можно удалить кнопкой "Delete".

И напоследок пробежимся по настройкам самого сервера.



"Use idle connection time" - по истечении указанного времени неактивные пользователи будут отключены от сервера



Здесь, в принципе, все просто и понятно: настройка логирования - что писать в логи (системные сообщения, команды, ошибки, подключения) и куда сохранять файл лога.



Здесь можно настроить дополнительные интерфейсы сервера. Напрммер, если у вас есть реальный IP и вы хотите сделать свой FTP доступным из внешнего интернета, то можете создать новый интерфейс, наример, 194.146.135.129. Для локальной же сети можно включить отдельный интерфейс 10.10.10.10. Дефолтовый интерфейс 127.0.0.1 будет пригоден для тестирования сервера в пределах одного компьютера.
Переключение или включение дополнительных интерфейсов можно производить в главном окне сервера - "Interface".



Это сообщения вашего сервера, которые выдаются пользователю при подключении и отключении от FTP.



Укажите, какое время использовать при отображении каталогов: мировое или локальное, которое сейчас установлено на вашем компьютере. Здесь же можно подавить вывод информационных стартовых сообщений.



Возможность удаленного администрирования сервера.



Определение размеров буферов приема-передачи, установка FTP сервера как системного сервиса (чтобы мог стартовать одновременно с операционной системой), запрет на передачу файлов "сервер-сервер" (Deny FXP Transfers - некоторые клиенты умеют делать такую передачу)

Любите статистику? Тогда для вас команда меню "Tools - Generate Statistics", которая создаст html-страницу с подробнейшей информацией об использовании FTP: кто, куда, когда и сколько...

1. Создайте систему папок. Разграничьте доступ к ним по следующим параметрам:
	1. Download. Укажите какие настройки необходимы:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Upload. Укажите какие настройки необходимы:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Download и Upload. Укажите какие настройки необходимы:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Вход по паролю. Укажите какие настройки необходимы:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Закачайте с соседнего компьютера фалы на ваш FTP-сервер. Опишите последовательность операций:
	1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Создайте несколько пользователей. Укажите для них разные папки и разные права доступа.

Укажите для каждой папки строку доступа с другого компьютера:

|  |  |  |
| --- | --- | --- |
| папка | Права | Строка доступа |
|  | Чтение |  |
|  | Изменение |  |
|  | Чтение и изменение |  |

1. Настройте доступ к вашим папкам через FAR-менеджер, предварительно его установив.

**FAR - настройка доступа по FTP**

Откройте FAR, нажмите **ALT+F2**

****Выберете FTP и нажмите **SHIFT+F4**

****

Нажмите **СОХРАНИТЬ**

Далее **ALT+F2** выберете созданное FTP и соединитесь с сервером.

Укажите строку доступа до серверов других компьютеров к одной из папок:

|  |  |  |  |
| --- | --- | --- | --- |
| Ws40-01 |  | Ws40-06 |  |
| Ws40-02 |  | Ws40-07 |  |
| Ws40-03 |  | Ws40-08 |  |
| Ws40-04 |  | Ws40-09 |  |
| Ws40-05 |  | Ws40-10 |  |

1. Установите программу WWW File Share PRO 4.0, предназначенную для запуска HTTP сервера.
2. Создайте страницу текста о себе, разместите на ней свое фото. Это можно выполнить в редакторе Word. Затем сохраните этот текст, как HTML-документ.
3. Разместите этот документ в соответствующей папке WEB-сервера.
4. Настройте доступ к файлам и папкам через HTTP сервер.

Укажите для каждой папки строку доступа с другого компьютера:

|  |  |  |
| --- | --- | --- |
| папка | Права | Строка доступа |
|  | Чтение |  |
|  | Изменение |  |
|  | Чтение и изменение |  |

**Вопросы к защите:**

1. Можно ли открывать файлы на редактирование по FTP-протоколу?
2. Какие операции с файлами позволяет выполнять FTP-протокол?
3. Какие операции с файлами позволяет выполнять HTTP-протокол?
4. Можно ли разграничить доступ к файлам через HTTP протокол?
5. Что такое LOGIN, NIC, PASSWORD? Что требуется для указания доступа через FTP протокол?
6. Перечислите программы, которые являются FTP или HTTP серверами?
7. Какие программы позволяют сохранять данные в виде web-страницы?

## Моделирование локальной сети.

**Цель:** научиться строить локальную сеть с помощью программы S2NETtest

**Оборудование:** IBM-PC совместимый компьютер, сетевая карта.

**Программное обеспечение**: MS Windows.

**Порядок выполнения работы:**

1. Загрузить программу.
2. Прочитать описание (помощь).
3. Приступить к выполнению 7 работ.
4. Зарисовать каждый из экранов (таблица 11х11) и записать соответствующее задание. Записать использованное оборудование и стоимость установки сети.
5. Придумать свое задание: текстовое и поле для заполнения.

**Вопросы к защите:**

1. Какое оборудование требуется для работы сети?
2. Что такое концентратор, репитер, маршрутизатор, шлюз?
3. Какие типы кабелей используются для прокладки ЛВС?
4. Какие типы хабов бывают?
5. Перечислите характеристики хабов, сетевых карт.

# *Создание простейшей Web-страницы*

**Цель работы:** Получение практических навыков работы в изучение языка гипертекстовой разметки, подготовка материалов к их публикации в Интернет, создание документов, имеющих формат, принятый в Интернете, Web-страниц, написанных на языке HTML.. .

**Теоретические сведения.**

*Создание Web-документов*

Автономные Web-документы используют язык HTML (HyperText Markup Language — язык разметки гипертекста).

Гипертекст, то есть расширенный текст, включает дополнительные элементы: иллюстрации, ссылки, вставные объекты.

Под разметкой понимается использование специальных кодов, легко отделяемых от смыслового содержания документа и используемых для реализации гипертекста. Применение этих кодов подчиняется строгим правилам, определяемым спецификацией языка HTML

Особенность описания документа средствами языка HTML связана с принципиальной невозможностью достижения абсолютной точности воспроизведения исходного документа.

Документ будет широкодоступен в Интернете, и поэтому неизвестно, как будет организовано его воспроизведение. Документ может быть представлен на графическом экране, выведен в чисто текстовом виде или просто «прочитан» программой синтеза речи.

Разметка HTML во всех этих случаях должна быть принята во внимание.

Язык HTML предназначен не для форматирования документа, а для его функциональной разметки.

Документы обычно начинаются с заголовков. Свойство части документа «быть заголовком» — это не особенность форматирования документа, а характеристика его содержания.

Конкретное средство отображения документа (браузер) выбирает свой способ пред­ставления части документа, описанной как заголовок.

Управляющие конструкции языка HTML называются тегами и вставляются непосредственно в текст документа. Все теги заключаются в угловые скобки <...>.

Сразу после открывающей скобки помещается ключевое слово, определяющее тег, например <DIV>.

Теги *HTML* бывают *парными* и *непарными.*

*Непарные* теги оказывают воздействие на весь документ или определяют разовый эффект в месте своего появле­ния. При использовании парных тегов в документ добавляются *открывающий* и *закрывающий* теги, которые воздействуют на часть документа, заключенную между ними.

Закрывающий тег отличается от открывающего наличием символа «/» (косая черта) перед ключевым словом (</DIV>).

Закрытие парных тегов выполняется так, чтобы соблюдались правила вложения.

<В><I> На этот текст воздействуют два тега</I></В>

Эффект применения тега может видоизменяться путем добавления *атрибутов.*

В парных тегах атрибуты добавляются *только к открывающему тегу.*

Атрибуты представляют собой дополнительные ключевые слова, отделяемые от ключевого слова, определяющего тег, и от других атрибутов пробелами и размещаемые до завершающего тег символа «>».

Способ применения некоторых атрибутов требует указания *значения атрибута.* Значение атрибута отделяется от ключевого слова атрибута символом «=» (знак равенства) и заключается в кавычки.

<Н1 ALIGN="LEFT">

*Определение HTML как языка разметки основывается на том, что при удалении из документа всех тегов получается текстовый документ, совершенно эквивалент­ный по содержанию исходному гипертекстовому документу.*

При отображении документа *HTML* сами теги *не отображаются,* но влияют на способ отображения остальной части документа.

Создание документов *HTML,* то можно представить себе два способа их формирования. Первый состоит в разметке существующего (или создаваемого) документа *вручную.* При этом автор или редактор добавляет в документ теги разметки. Эту работу можно выполнять в *текстовом редакторе или редакторе HTML,* имеющем специальные элементы управления для упрощения ввода тегов. В обоих этих случаях работа ведется средствами языка *HTML, и* человек, выполняющий эту работу, должен знать и уметь применять этот язык.

Принципы другого подхода можно понять на основе изучения работы текстовых процессоров. Информацию о форматировании документа также можно рассматри­вать как «разметку», добавляемую в форматируемый документ.

Однако для использования текстового процессора не требуется никаких знаний о формате документа и «языке разметки»: изменения, отображаемые на экране, вносятся в документ автоматически. Такой принцип соответствия экранного изображения реальному получил название *WYSIWYG* (от английского *What You See Is What You Get — Что видите, то и получаете).*

Простейший редактор *WYSIWYG* для языка *HTML,* FrontPage Express, входит в состав операционной системы Windows 98.

Первый способ позволяет создавать более универсальные, более качественные и более разнообразные документы. Второй способ проще освоить, так как он не тре­бует знания языка *HTML.* Однако в этом *случае* используются средства *формати­рования* вместо средств *описания,* что может иногда приводить к нежелательным последствиям.

**Ход работы.**

***Упражнение 1. Создание простейшей Web-страницы***

Запустите текстовый редактор Блокнот (Пуск > Программы > Стандартные *>* Блокнот).

 Введите следующий документ:

<НТМL>

<HEAD>

<ТIТLЕ>Заголовок документа< /ТIТLЕ>

</HEAD>

<BODY>

Содержание документа

</BODY>

</HTML>

Сохраните этот документ под именем first.html.

Перед сохранением убедитесь, что сброшен флажок - Не показывать расширения для зарегистрированных типов файлов (Пуск *>* Настройка *>* Свойства папки *>* Вид). В про­тивном случае редактор Блокнот может автоматически добавить в конец имени расширение ТХТ.

Запустите программу Internet Explorer (Пуск *>* Программы *>* Internet Explorer).

Дайте команду Файл *>*Открыть. Щелкните на кнопке Обзор и откройте файл first.html.

Посмотрите, как отображается этот файл — простейший корректный документ *HTML.*

Где отображается содержимое элемента TITLE?

 Где отображается содер­жимое элемента BODY?

Как отображаются слова «Содержание» и «документа», введенные в двух отдель­ных строчках? Почему? Проверьте, что происходит при уменьшении ширины окна.

***Упражнение 2. Изучение приемов форматирования абзацев.***

Если это *упражнение* выполняется не сразу после предыдущего, откройте документ first, html в программе Блокнот.

Удалите весь текст, находящийся между тегами <BODY> и </BODY>.

Текст, который будет вводиться в последующих пунктах этого упражнения, необходимо поместить после тега <BODY>, а его конкретное содержание может быть любым.

Введите заголовок первого уровня, заключив его между тегами <Н1 > и </Н1 >.

Введите заголовок второго уровня, заключив его между тегами <Н2> и </Н2>.

Введите отдельный абзац текста, начав его с тега <Р>.

Пробелы и символы пере­вода строки можно использовать внутри абзаца произвольно.

Введите тег горизонтальной линейки <HR>.

Введите еще один абзац текста, начав его с тега <Р>.

Сохраните этот документ под именем paragraph. html.

Запустите обозреватель Internet Explorer (Пуск > Программы *>* Internet Explorer).

Дайте команду Файл *>* Открыть. Щелкните на кнопке Обзор и откройте файл
paragraph.htm.

Посмотрите, как отображается этот файл. Установите соответствие между

элементами кода *HTML* и фрагментами документа, отображаемыми на экране.

В этом упражнении вы создали документ *HTML с* разметкой абзацев. Определите, как влияют теги *HTML* на отображение соответствующих частей документа.

Упражнение 3. Создание гиперссылок

Если это упражнение выполняется не сразу после предыдущего, откройте документ first, html в программе Блокнот.

Удалите весь текст, находящийся между тегами <BODY> и </BODY>.

Текст, который будет вводиться в последующих пунктах этого упражнения, необхо­димо поместить после тега <BODY>.

Введите фразу: Текст до ссылки.

Введите тег: <А HREF="first html.">.

Введите фразу: Ссылка.

Введите закрывающий тег </А>.

Введите фразу: Текст после ссылки.

Сохраните документ под именем link.. html

Запустите обозреватель Internet Explorer (Пуск > Программы > Internet Explorer).

Дайте команду Файл > Открыть. Щелкните на кнопке Обзор и откройте файл link.. html

Убедитесь в том, что текст между тегами <А> и </А> выделен как ссылка (цветом и подчеркиванием).

Щелкните на ссылке и убедитесь, что при этом загружается документ, на кото­рый указывает ссылка.

 Щелкните на кнопке Назад на панели инструментов, чтобы вернуться к пре­дыдущей странице. Убедитесь, что ссылка теперь считается «просмотренной» и отображается другим цветом.

**Контрольные вопросы.**

1. Перечислить назначение элементов:

<BODY>, <STYLE>, <META>, <HEAD>, <A> <|/a>, <BASE>

2. Понятие гипертекстовые ссылки, атрибуты.

Содержание отчета.

1. Название и цель работы.

2. Краткие сведения по теории и порядку выполнения работы.

3. Выводы по работе.

# *Создание изображения и использование на Web-странице*

**Цель работы**: Получение практических навыков работы в изучение языка гипертекстовой разметки, подготовка материалов к их публикации в Интернет. .

**Теоретические сведения.**

Графические иллюстрации в большинстве случаев являются неотъемлемой частью Web-документов. Сегодня графические элементы Web-страниц используют два основ­ных формата — *GIF и JPEG* (новый формат *PNG* пока еще нельзя считать общеприня­тым). Все графические браузеры, предназначенные для отображения Web-страниц на экране компьютера, способны распознавать и отображать файлы этих форматов.

Файлы формата *GIF (Graphic Interchange Format)* имеют расширение .GIF. Изобра­жения в этом формате содержат 256 цветов, заданных индексной палитрой. Файл упакован и может занимать значительно меньше места, чем неупакованный растро­вый рисунок (например, в формате .BMP).

Спецификация формата *GIF89a* позволяет создавать файлы .GIF, обладающие специальными возможностями:

Один из цветов изображения может быть объявлен *прозрачным.* Это означает, что в соответствующих местах сквозь него будет проглядывать фон Web-стра­ницы, что позволяет задать не только прямоугольную форму рисунка, но и де­лает его более естественным.

*Чересстрочные изображения* при их приеме из Интернета прорисовываются постепенно, вначале грубо, а затем все более и более четко. Это «скрадывает» время, необходимое на их загрузку из Интернета, особенно при приеме информации по медленным линиям.

*GIF-анимация* превращает обычный рисунок в небольшой видеоролик. В стандартном файле с расширением .GIF хранится набор кадров, а также сценарий их отображения.

Файлы формата JPEG *(Joint Photographic Expert Group —* по названию группы исследователей, предложившей этот формат, читается «джей-пег») могут иметь расширение JPEG или JPG. Формат предназначен для хранения фотографических изображе­ний, использующих 24-разрядный цвет.

**Ход работы.**

***Упражнение 1. Создание изображения и использование его на Web-странице***

 Откройте программу Paint (Пуск *\** Программы *>* Стандартные > Paint). Задайте размеры нового рисунка, например 50x50 точек (Рисунок > Атрибуты).

 Выберите красный цвет переднего плана и зеленый цвет фона. Залейте рисунок фоновым цветом.

 Инструментом Кисть нанесите произвольный красный рисунок на зеленый фон.

 Сохраните рисунок под именем picl .gif (в формате GIF).

 Дайте команду Рисунок *>* Атрибуты. Установите флажок Использовать прозрачный цвет фона. Щелкните на кнопке Выбор цвета и выберите зеленый цвет, уже использованный на рисунке в качестве фонового.

Сохраните рисунок еще раз под именем pic2.gif (в формате GIF) и закройте про­грамму Paint.

Если это упражнение выполняется не сразу после предыдущего, откройте доку­мент first, htm в программе Блокнот.

Удалите весь текст, находящийся между тегами <BODY> и </BODY>. Текст, который будет вводиться в последующих пунктах этого упражнения, необхо­димо поместить после тега <BODY>.

Введите произвольный текст (протяженностью 4-5 строк) и установите тек­стовый курсор в его начало.

 Введите тег <IMG SRC="pic1 .gif" ALIGN="BOTTOM">.

 Сохраните документ под именем picture. html.

 Запустите обозреватель Internet Explorer (Пуск > Программы > Internet Explorer).

 Дайте команду Файл *>* Открыть. Щелкните на кнопке Обзор и откройте файлpicture.htm. Посмотрите на получившийся документ, обращая особое внимание на изображение.

Вернитесь в программу Блокнот и измените значение атрибута: ALIGN="TOP".
Сохраните файл под тем же именем.

 Вернитесь в программу Internet Explorer и щелкните на кнопке Обновить на панели инструментов. Посмотрите, как изменился вид страницы при изменении атри­бутов.

 Вернитесь в программу Блокнот и измените значение атрибута: ALIGN="LEFT". Сохраните файл под тем же именем.

 Вернитесь в программу Internet Explorer и щелкните на кнопке Обновить на панели инструментов. Посмотрите, как изменился вид страницы при изменении атри­бутов.

 Вернитесь в программу Блокнот и добавьте в тег <IMG> атрибуты: HSPACE=40VSPACE=20. Сохраните файл под тем же именем.

 Вернитесь в программу Internet Explorer и щелкните на кнопке Обновить на панели инструментов. Посмотрите, как изменился вид страницы при изменении атри­бутов.

 Вернитесь в программу Блокнот и измените имя рисунка: SRC="pic2.gif". Сохра­ните файл под тем же именем.

 Вернитесь в программу Internet Explorer и щелкните на кнопке м Обновить на панели инструментов. Посмотрите, как изменился вид страницы при изменении атри­бутов. В чем различие между двумя созданными рисунками?

***Упражнение 2. Приемы форматирования текста***

 Если это упражнение выполняется не сразу после предыдущего, откройте доку­мент first.htm в программе Блокнот.

Удалите весь текст, находящийся между тегами <BODY> и </BODY>. Текст, который будет вводиться в последующих пунктах этого упражнения, необходимо поместить после тега <BODY>, а его конкретное содержание может быть любым.

 Введите тег <BASEFONT SIZE="5" COLOR="BROWN">. Он задает вывод текста по умолчанию увеличенным шрифтом и коричневым цветом.

 Введите произвольный абзац текста, который будет выводиться шрифтом, задан­ным по умолчанию. Начните этот абзац с тега <Р>.

 Введите теги: <Р> <FONT SIZE="-2" FACE="ARIAL" COLOR="GREEN">.

 Введите очередной абзац текста, закончив его тегом </FONT>.

 В следующем абзаце используйте по своему усмотрению парные теги: <В> (полу­жирный шрифт), <1> (курсив), <U> (подчеркивание), <S> (вычеркивание),
<SUB> (нижний индекс), <SUP> (верхний индекс).

 В следующем абзаце используйте по своему усмотрению парные теги: <ЕМ> (выде­ление), <STRONG> (сильное выделение), <CODE> (текст программы), <KBD> (кла­виатурный ввод), <SAMP> (пример вывода), <VAR> (компьютерная переменная).

 Сохраните полученный документ под именем format html..

 Запустите обозреватель Internet Explorer (Пуск > Программы > Internet Explorer).

 Дайте команду Файл *>* Открыть. Щелкните на кнопке Обзор и откройте файл format. html.

 Изучите, как использованные элементы *HTML* влияют на способ отображения текста.

 Вернитесь в программу Блокнот и измените документ так, чтобы элементы, за­дающие форматирование, были вложены друг в друга. Сохраните документ под тем же именем.

 Вернитесь в программу Internet Explorer и щелкните на кнопке Обновить на панели инструментов. Посмотрите, как изменился вид страницы.

**Контрольные вопросы.**

1. Как влияют атрибуты тега <IMG> на способ отображения изображения.
2. Какие элементы языка HTML, которые могут использоваться для форматирования текста документа.
3. Как эти элементы воздействуют на отображение документа, и какие элементы можно вкладывать друг в друга.

***Дополнительная литература***

1. Якубайтис Э.А. Информационные сети и системы: Справочная книга. – М.: Финансы и статистика, 1996.
2. Бэрри Нанс. Компьютерные сети пер. с англ. – М.: БИНОМ, 1996.
3. Основы современных компьютерных технологий под редакцией А.Д. Хомоненко– СПб КОРОНА принт, 1998.
4. Ресурсы Microsoft Windows NT Workstation 4.0 пер. с англ. яз. BNV – СПб, 1998.
5. Титтел Эд, Хадсон Курт, Дж. Майкл Стюард Networking Essentials – СПб ПИТЕР, 1999.
6. Титтел Эд, Хадсон Курт, Дж. Майкл Стюард TCP/IP – СПб ПИТЕР, 1999.
7. Компьютерные сети: Учебный курс Microsoft Corporation – М.: Издательский отдел «Русская редакция», 1999.
8. Глоссарий сетевых терминов http://www.bilim.com/koi8/library/glossary/
9. Справочник Novell Netware 4 С.Б. Орлов, по заказу ИИЦ "Попурри", 1994. http://www.citforum.kts.ru/operating\_systems/nw4/
10. CISCO Internetworking Technology Overview Сервер Марк-ИТТ, Владимир Плешаков http://www.citforum.ru/win/nets/ito/index.shtml.
11. Стэн Шатт Мир компьютерных сетей пер. с англ. – К.: BHV, 1996 – 288 c.: – ISBN 5–7733–0028–1.
12. Модель OSI Сервер BiLiM Systems Ltd.
13. http://www.citforum.ru/win/nets/switche/osi.shtml.
14. Руководство по сетям Ethernet для начинающих –
http://www.citforum.ru/win/nets/ethernet/starter.shtml.
15. Базовые технологии локальных сетей
http://www.citforum.ru/win/nets/protocols2/index.shtml.
16. Введение в IP-сети http://www.citforum.ru/win/nets/ip/contents.shtml
17. Практическое руководство по сетям Plug-and-Play Ethernet http://www.citforum.ru/win/nets/ethernet/pract.shtml.
18. Семейство протоколов TCP/IP
http://www.citforum.ru/win/internet/tifamily/index.shtml.
19. Статическая IP-маршрутизация, Дмитрий Карпов http://www.citforum.ru/win/internet/tifamily/iproutng.shtml.
20. Протоколы TCP/IP Д. Комер "Межсетевой обмен с помощью TCP/IP" http://www.citforum.ru/win/internet/comer/contents.shtml.
21. Протокол IP Радик Усманов
http://www.citforum.ru/win/internet/tifamily/ipspec.shtml.
22. Операционные системы http://citforum.ru/operating\_systems/index.shtml.
23. Концентраторы. http://www.idcom.ru/rationet/sysint/active.htm#nic.
24. Структурированные кабельные системы http://www.idcom.ru/rationet/sysint/cabsys.htm#magistral.
25. Типы соединений по витой паре http://ixbt.stack.net/comm/cable\_utp.html.
26. Кабельные системы Ethernet http://www.bilim.com/koi8/bay/netgear/cables.htm.
27. Кабельные системы http://old.pcweek.ru/97\_40/koi/re1.htm.
28. Физический уровень 100Base-FX - многомодовое оптоволокно http://www.citforum.ru/nets/protocols2/2\_06\_06.shtml.
29. Средства согласования протоколов на физическом и канальном уровнях http://www.citforum.ru/win/nets/tpns/glava\_3.shtml.
30. Кабельные каналы http://www.idcom.ru/rationet/sysint/chanels.htm.
31. Роль коммуникационных протоколов и функциональное назначение основных типов оборудования корпоративных сетей. Н. Олифер, В. Олифер, ЦИТ http://www.citforum.ru/win/nets/protocols/index.shtml.
32. Физическая структуризация локальной сети. Повторители и концентраторы. Н. Олифер, В. Олифер, ЦИТ http://www.citforum.ru/win/nets/protocols/1\_03\_04.shtml.
33. Сетевые операционные системы. Н. А. Олифер, В. Г. Олифер, ЦИТ, http://www.citforum.kcn.ru/operating\_systems/sos/contents.shtml.
34. Технология корпоративных сетей. М. Кульгин. – СПб ПИТЕР, 1999.