



ный конспект
лекций

Ф СО ПГУ 7.18.2/05

Министерство образования и науки Республики Казахстан
Павлодарский государственный университет им. С. Торайгырова
Кафедра Информатики и информационные системы

ОПОРНЫЙ КОНСПЕКТ Компьютерные сети

Павлодар



т утверждения к
рному конспекту
лекций

Ф СО ПГУ 7.18.1/05

УТВЕРЖДАЮ

Декан ФФМиИТ

_____ С.К.Тлеуенов
«__» _____ 200_ г.

Составитель: Ст. преподаватель Токкожина М.А.

Кафедра Информатика и информационные системы

ОПОРНЫЙ КОНСПЕКТ ЛЕКЦИЙ КОМПЬЮТЕРНЫЕ СЕТИ

Для студентов специальности 050703- Информационные системы
очной и заочной формы обучения

Рекомендована на заседании кафедры от «_» _____ 200_ г. Протокол №__.

Заведующий кафедрой _____ Нурбекова Ж.К.
(подпись)

Одобрена методическим советом факультета ФМиИТ

«__» _____ 200_ г. Протокол № _____

Председатель МС _____ А.Т. Кишубаева
(подпись)

Тема1 Основы построения компьютерных сетей

Вычислительные сети (ВС) появились давно. Еще на заре появления компьютеров (в эпоху больших ЭВМ) существовали огромные системы, известные как системы разделения времени. Они позволяли использовать центральную ЭВМ с помощью удаленных терминалов. Такой терминал состоял из дисплея и клавиатуры. Внешне выглядел как обычный ПК, но не имел собственного процессорного блока. Пользуясь такими терминалами, сотни, а иногда тысячи сотрудников имели доступ к центральной ЭВМ.

Такой режим обеспечивался благодаря тому, что система разделения времени разбивала время работы центральной ЭВМ на короткие интервалы времени, распределяя их между пользователями. При этом создавалась иллюзия одновременного использования центральной ЭВМ многими сотрудниками.

В 70-х годах большие ЭВМ уступили место мини компьютерным системам, использующим тот же режим разделения времени. Но технология развивалась, и с конца 70-х годов на рабочих местах появились персональные компьютеры (ПК). Однако, автономно работающие ПК:

- а) не дают непосредственного доступа к данным всей организации;
- б) не позволяют совместно использовать программы и оборудование.

С этого момента начинается современное развитие компьютерных сетей.

Вычислительной сетью называется система, состоящая из двух или более удаленных ЭВМ, соединенных с помощью специальной аппаратуры и взаимодействующих между собой по каналам передачи данных.

Самая простая сеть (network) состоит из нескольких ПК, соединенных между собой сетевым кабелем. При этом в каждом ПК устанавливается специальная плата сетевого адаптера (NIC), осуществляющая связь между системной шиной компьютера и сетевым кабелем.

Кроме этого, все компьютерные сети работают под управлением специальной сетевой операционной системы (NOS – Network Operation Sistem). Основное назначение компьютерных сетей – совместное использование ресурсов и осуществление интерактивной связи как внутри одной фирмы, так и за ее пределами.

Ресурсы – представляют собой данные (в т. ч. корпоративные базы данных и знаний), приложение (в т. ч. различные сетевые программы), а также периферийные устройства, такие как принтер, сканер, модем и т. д.

До объединения ПК в сеть каждый пользователь должен был иметь свой принтер, плоттер и другие периферийные устройства, а также на каждом из ПК должны были быть установлены одни и те же программные средства, используемые группой пользователей.

Другой привлекательной стороной сети является наличие программ электронной почты и планирования рабочего дня. Благодаря им, сотрудники

эффективно взаимодействуют между собой и партнерами по бизнесу, а планирование и корректировка деятельности всей компании осуществляется значительно проще. Использование компьютерных сетей позволяет: а) повысить эффективность работы персонала фирмы; б) снизить затраты за счет совместного использования данных, дорогостоящих ПУ и программных средств (приложений).

Локальные сети - ЛВС (LAN – Local Area Network) объединяют находящиеся недалеко друг от друга (в соседней комнате или здании) компьютеры. Иногда компьютеры могут находиться на расстоянии нескольких миль и все равно принадлежать локальной сети.

Компьютеры *глобальной сети – ГВС (WAN – Wide Area Network)* могут находиться в других городах или даже странах. Информация проделывает длинный путь, перемещаясь в данной сети. Интернет состоит из тысячи компьютерных сетей, разбросанных по всему миру. Однако, пользователь должен рассматривать Интернет как единую глобальную сеть.

Соединяя компьютеры между собой и давая им возможность общаться друг с другом, вы создаете *сеть*. Соединяя две и более сетей, вы создаете *межсетевое объединение*, называющееся «интернет» (internet – первая буква строчная).

Интернет (с заглавной буквы) – самое большое и популярное межсетевое объединение в мире. Оно объединяет более 20 тыс. компьютерных сетей, расположенных в 130 странах. При этом объединены компьютеры тысяч различных видов, оснащенных различным программным обеспечением. Однако, пользуясь сетью, можно не обращать внимания на эти различия.

При обмене данными как между ПК в ЛВС, так и между ЛВС любое информационное сообщение разбивается программами передачи данных на небольшие блоки данных, которые называются *пакетами*.

Связано это с тем, что данные обычно содержатся в больших по размерам файлах, и если передающий компьютер пошлет его целиком, то он надолго заполнит канал связи и «свяжет» работу всей сети, т. е. будет препятствовать взаимодействию других участников сети. Кроме этого, возникновение ошибок при передаче крупных блоков вызовет большие затраты времени, чем на его повторную передачу.

Пакет – основная единица информации в компьютерных сетях. При разбиении данных на пакеты скорость их передачи возрастает настолько, что каждый компьютер сети получает возможность принимать и передавать данные практически одновременно с остальными ПК.

При разбиении данных на пакеты сетевая ОС к собственно передаваемым данным добавляет специальную добавляющую информацию:

- заголовок, в котором указывается адрес отправителя, а также информация по сбору блоков данных в исходное информационное

сообщение при их приеме получателем;

- трейлер, в котором содержится информация для проверки безошибочности в передаче пакета. При обнаружении ошибки передача пакета должна повториться.

Переключение соединений используется сетями для передачи данных. Оно позволяет средством сети разделить один и тот же физический канал связи между многими устройствами. Различают два основных способа переключения соединений:

- переключение цепей (каналов);
- переключение пакетов.

Переключение цепей создает единое непрерывное соединение между двумя сетевыми устройствами. Пока эти устройства взаимодействуют, ни одно другое не может воспользоваться этим соединением для передачи собственной информации – оно вынуждено ждать, пока соединение освободится и наступит его очередь принимать данные.

Простейший пример переключения цепей – это переключатели для принтеров, позволяющие нескольким ПК использовать один принтер. Одновременно с принтером может работать только один ПК. Какой именно, решит переключатель, который прослушивает сигналы ПК, и как только поступает сигнал с одного из них, он автоматически его подсоединяет и сохраняет это соединение, пока не закончится печатная серия этого ПК. Образуется соединение типа «точка-точка» (point to point), при котором другие ПК не могут воспользоваться соединением, пока оно не освободится и не наступит их очередь. Большинство современных сетей, включая Интернет, используют переключение каналов, являясь сетями с пакетной коммуникацией.

Исходное информационное сообщение от ПК₁ к ПК₂ в зависимости от его размера может следовать одновременно одним пакетом или несколькими. Но т. к. в заголовке каждого из них есть адрес получателя, все они придут в одно и то же место назначения, несмотря на то, что они следовали совершенно различными маршрутами.

Для сравнения переключения цепей и пакетов допустим, что мы прервали канал в каждом из них. Например, отключив принтер от ПК₁ мы вовсе лишили его возможности печатать. Соединение с переключением цепей требует непрерывного канала связи.

Наоборот, данные в сети с переключением пакетов могут двигаться разными путями, и разрыв не приведет к потере соединения, т. к. есть множество альтернативных маршрутов. Концепция адресации пакетов и их маршрутизации – одна из важнейших в ГВС, в том числе и в Интернет.

Передача данных между компьютерами и прочими устройствами происходит параллельно или последовательно.

Так большинство ПК пользуется параллельным портом для работы с принтером. Термин «параллельно» означает, что данные передаются одновременно по нескольким проводам.

Чтобы послать байт данных по параллельному соединению, ПК одновременно устанавливает весь бит на восьми проводах.

Напротив, последовательное соединение подразумевает передачи данных по очереди, бит за битом. В сетях чаще всего используется именно такой способ работы, когда биты выстраиваются друг за другом и последовательно передаются (и принимаются тоже),

При соединении по сетевым каналам используют три различных метода. Соединение бывает: симплексное, полудуплексное и дуплексное.

О *симплексном соединении* говорят, когда данные перемещаются только в одном направлении (рис. 1.9). *Полудуплексное соединение* позволяет данным перемещаться в обоих направлениях, но в разное время.

И, наконец, *дуплексное соединение* позволяет данным перемещаться в обоих направлениях одновременно.

Основными характеристиками ВС являются:

- операционные возможности сети;
- временные характеристики;
- надежность;
- производительность;
- стоимость.

Операционные возможности сети характеризуются такими условиями, как:

- предоставление доступа к прикладным программным средствам, БД, БЗ, и т. д.;
- удаленный ввод заданий;
- передача файлов между узлами сети;
- доступы к удаленным файлам;
- выдача справок об информационных и программных ресурсах;
- распределенная обработка данных на нескольких ЭВМ и т. д.

Временные характеристики сети определяют продолжительность обслуживания запросов пользователей:

- среднее время доступа, которое зависит от размеров сети, удаленности пользователей, загрузки и пропускной способности каналов связи и т. д.;
- среднее время обслуживания.

Надежностные характеристики определяют надежность как отдельных элементов сети, так и сеть в целом.

Тема 2 Стандартизация сетевых решений

ЛВС на базе ПК получили в настоящее время широкое распространение из-за небольшой сложности и невысокой стоимости. Они используются при автоматизации коммерческой, банковской деятельности, а также для создания распределенных, управляющих и информационно-справочных систем. ЛВС имеют модульную организацию. Их основные компоненты - это (рис. 2.1):

- Серверы* – это аппаратно-программные комплексы, которые исполняют функции управления распределением сетевых ресурсов общего доступа.
- Рабочие станции* – это компьютеры, осуществляющие доступ к сетевым ресурсам, предоставляемым сервером.
- Физическая среда передачи данных (сетевой кабель)* – это коаксиальные и оптоволоконные кабели, витые пары проводов, а также беспроводные каналы связи (инфракрасное излучение, лазеры, радиопередача).

Выделяется два основных типа ЛВС: одноранговые (peer-to-peer) ЛВС и ЛВС на основе сервера (server based). Различия между ними имеют принципиальное значение, т. к. определяют разные возможности этих сетей. Выбор типа ЛВС зависит от:

- размеров предприятия;
- необходимого уровня безопасности;
- объема сетевого трафика;
- финансовых затрат;
- уровня доступности сетевой административной поддержки.

При этом в задачи сетевого администрирования обычно входит:

- управление работой пользователей и защитой данных;
- обеспечение доступа к ресурсам;
- поддержка приложений и данных;
- установка и модернизация прикладного ПО.

В этих сетях все компьютеры равноправны: нет иерархии среди них; нет выделенного сервера. Как правило, каждый ПК функционирует и как рабочая станция (PC), и как сервер, т. е. нет ПК ответственного за администрирование всей сети (рис. 2.2). Все пользователи решают сами, какие данные и ресурсы (каталоги, принтеры, факс-модемы) на своем компьютере сделать общедоступными по сети

Рабочая группа – это небольшой коллектив, объединенный общей целью и интересами. Поэтому в одноранговых сетях чаще всего не более 10 компьютеров. Эти сети относительно просты. Т. к. каждый ПК является одновременно и PC, и сервером. Нет необходимости в мощном центральном сервере или в других компонентах, обязательных для более сложных сетей.

Одноранговые сети обычно дешевле сетей на основе сервера, но требуют более мощных, а стало быть и более дорогих, ПК. Требование к производительности и к уровню защиты для сетевого ПО в них также значительно ниже.

В такие операционные системы, как: MS Windows NT for Workstation; MS Windows 95/98, Windows 2000 встроена поддержка одноранговых сетей. Поэтому, чтобы установить одноранговую сеть, дополнительного ПО не требуется, а для объединения компьютеров применяется простая кабельная система. Одноранговая сеть вполне подходит там, где:

- количество пользователей не превышает 10-15 человек;
- пользователи расположены компактно;
- вопросы защиты данных не критичны;
- в обозримом будущем не ожидается расширения фирмы, и, следовательно, увеличения сети.

Несмотря на то, что одноранговые сети вполне удовлетворяют потребности небольших фирм, возникают ситуации, когда их использование является неуместным. В этих сетях защита предполагает установку пароля на разделяемый ресурс (например, каталог). Централизованно управлять защитой в одноранговой сети очень сложно, т. к.:

- пользователь устанавливает ее самостоятельно ;
- «общие» ресурсы могут находиться на всех ПК, а не только на центральном сервере.

Такая ситуация – угроза для всей сети; кроме того, некоторые пользователи могут вообще не установить защиту. Если вопросы конфиденциальности являются для фирмы принципиальными, то такие сети применять не рекомендуется. Кроме того, так как в этих ЛВС каждый ПК работает и как PC, и как сервер, пользователи должны обладать достаточным уровнем знаний, чтобы работать и как пользователи, и как администраторы своего компьютера. При подключении более 10 пользователей одноранговая сеть может оказаться недостаточно производительной. Поэтому большинство сетей используют выделенные серверы. *Выделенными* называются такие серверы, которые функционируют только как сервер (исключая функции PC

или клиента). Они специально оптимизированы для быстрой обработки запросов от сетевых клиентов и для управления защитой файлов и каталогов.

С увеличением размеров сети и объема сетевого трафика необходимо увеличивать количество серверов. Распределение задач среди нескольких серверов гарантирует, что каждая задача будет выполняться самым эффективным способом из всех возможных.

Круг задач, которые выполняют серверы, многообразен и сложен. Чтобы приспособиться к возрастающим потребностям пользователей, серверы в ЛВС стали специализированными. Так, например, в операционной системе Windows NT Server существуют различные типы серверов (рис. 2.4):

- *Файл-серверы и принт-серверы.* Они управляют доступом пользователей к файлам и принтерам. Так, например, для работы с текстовым документом Вы прежде всего запускаете на своем компьютере (PC) текстовый процессором. Далее требуемый документ текстового процессора, хранящийся на файл-сервере, загружается в память PC и таким образом Вы можете работать с этим документом на PC. Другими словами, файл-сервер предназначен для хранения файлов и данных.
- *Серверы приложений* (в том числе сервер баз данных, WEB –сервер). На них выполняются прикладные части клиент серверных приложений (программ). Эти серверы принципиально отличаются от файл-серверов тем, что при работе с файл-сервером нужный файл или данные целиком копируются на запрашивающую PC, а при работе с сервером приложений на PC пересылаются только результаты запроса. Например, можно по запросу можно получить только список работников, родившихся в сентябре не загружая при этом в свою PC всю базу данных персонала.
- *Почтовые серверы* – управляют передачей электронных сообщений между пользователями сети.
- *Факс-серверы* – управляют потоком входящих и исходящих факсимильных сообщений через один или несколько факс-модемов.
- *Коммуникационные серверы* – управляют потоком данных и почтовых сообщений между данной ЛВС и другими сетями или удаленными пользователями через модем и телефонную линию. Они же обеспечивают доступ к Интернет.
- *Сервер служб каталогов* – предназначен для поиска, хранения и защиты информации в сети. Windows NT Server объединяет PC в логические группы-домены, система защиты которых наделяет пользователей различными правами доступа к любому сетевому ресурсу.

При этом каждый из серверов может быть реализован как на отдельном компьютере, так и в небольших по объему ЛВС, быть совмещенным на одном компьютере с каким-либо другим сервером. Сервер и ОС работают как единое целое. Без ОС даже самый мощный сервер представляет собой грудку железа. ОС позволяет реализовать потенциал аппаратных ресурсов сервера. К наиболее распространенным сетевым ОС следует отнести:

- Novell NetWare 4.0 и выше;

- OS/2;
- Unix;
- Windows NT 4.0 и выше.

Последняя обеспечивает симметричную многопроцессорную обработку (системные задачи распределяются между всеми доступными процессорами), поддерживает множество аппаратных платформ (Pentium, R4000, RISE и Digit Alpha), длина имени файла до 225 байт, размер файла и диска – до 16 эксабайт (миллиард гигабайт).

Тема 3 Аппаратные средства компьютерных сетей

Существует большое число способов, которыми можно соединить компьютеры между собой в единую компьютерную сеть. Чем больше разных компьютеров, тем больше таких способов соединения. Каждое соединение – это новый маршрут для передачи данных.

Термин «*топология сети*» или просто «*топология*» характеризует физическое расположение компьютеров, сетевых сред передачи данных и других компонентов сети. Топология – это стандартный термин, который:

- используется при описании основной компоновки сети;
- дает способ сравнивать и классифицировать различные сети.

Топология сети обуславливает ее технические характеристики. В частности, выбор той или иной топологии влияет на:

- состав необходимого сетевого оборудования и его характеристики;
- возможность расширения сети и ее надежность;
- способ управления сетью.

При построении сети просто подключить компьютер к сетевому кабелю, соединяющему другие компьютеры, недостаточно. Различные типы кабелей в сочетании с различными сетевыми адаптерами, сетевыми ОС и другими компонентами требуют и различного взаимного расположения компьютеров.

Любая топология сети может диктовать не только тип кабеля, но и способ его прокладки, а также определять метод доступа компьютеров в сеть. Все сети строятся на основе трех базовых топологий: шина (bus); звезда (star); кольцо (ring). Если компьютеры подключены вдоль одного кабеля (сегмента), топология называется "*шина*". В том случае, когда компьютеры подключены к сегментам кабеля, исходящим из одной точки (или концентратора), топология называется "*звезда*". Если кабель, к которому подключены компьютеры, замкнут, то такая топология носит название "*кольцо*".

Данная топология относится к наиболее простым и широко распространенным топологиям. В ней используется один сетевой кабель, именуемый *магистралью* или *сегментом*, вдоль которого подключены все РС сети (рис. 3.1).

1. При передаче пакетов данных каждый компьютер адресует его

конкретному компьютеру ЛВС (РС_к), передавая его по сетевому кабелю в виде электрических сигналов.

2. Пакет в виде электрических сигналов передается по шине в обоих направлениях всем компьютерам сети.

3. Однако, информацию принимает только тот адрес, который соответствует адресу получателя, указанному в заголовке пакета. Так как в каждый момент времени в сети может вести передачу только одна РС, то производительности ЛВС зависит от количества РС, подключенных к шине. Чем их больше, тем больше ожидающих передачи данных, тем ниже производительности сети. Однако, нельзя указать прямую зависимость пропускной способности сети от количества РС, так как на нее также влияет:

- характеристики аппаратного обеспечения РС сети;
- частота, с которой передают сообщения РС;
- тип работающих сетевых приложений;
- тип кабеля и расстояние между РС в сети

Шина – пассивная топология. Это значит, что компьютеры только «слушают» передаваемые по сети данные, но не перемещают их от отправителя к получателю. Поэтому, если один из компьютеров выйдет из строя, это не скажется на работе всей сети (!).

4. Данные в виде электрических сигналов распространяются по всей сети от одного конца кабеля к другому, и, достигая конца кабеля, будут отражаться и занимать шину, что не позволит другим компьютерам осуществлять передачу.

5. Чтобы предотвратить отражение электрических сигналов, на каждом конце кабеля устанавливаются терминаторы (Т), поглощающие сигналы, прошедшие по шине.

6. При значительном расстоянии между РС (например, 180 м для тонкого коаксиального кабеля) в сегменте шины может наблюдаться ослабление электрического сигнала, что может привести к искажению или потере передаваемого пакета данных. В этом случае исходный сегмент следует разделить на два, установив между ними дополнительное устройство – *репитер (повторитель)*, который усиливает принятый сигнал перед тем, как послать его дальше .

Правильно размещенные на длине сети повторители позволяют увеличить длину обслуживаемой сети и расстояние между соседними компьютерами. Следует помнить, что все концы сетевого кабеля должны быть к чему-либо подключены: к РС, терминатору или повторителю.

Разрыв сетевого кабеля или отсоединение одного из его концов приводит к прекращению функционирования сети. Сеть «падает». Сами РС сети остаются полностью работоспособными, но не могут взаимодействовать друг с другом. Если ЛВС на основе сервера, где большая часть программных и информационных ресурсов хранится на сервере, то РС, хотя и остаются работоспособными, но для практической работы малопригодны.

При топологии «звезда» все компьютеры с помощью сегментов кабеля подключаются к центральному компоненту – концентратору (Hub)

Пакеты данных от каждого компьютера направляются к центральному концентратору. Он, в свою очередь, перенаправляет пакеты к месту назначения. Основное достоинство этой топологии в том, что если повреждена какая-либо PC или отдельное соединение между PC и концентратором, вся сеть остается работоспособной. Положительным является и то, что подключение кабеля и управление конфигурацией сети централизовано, а также просто конфигурировать сеть при добавлении новых PC. Как недостатки организации такой топологии следует отметить следующее:

- Так как все PC подключены к центральной точке, то для больших ЛВС значительно увеличивается расход кабеля.
- Если поврежденным оказался сам концентратор, то нарушится и работа всей сети, хотя PC останутся работоспособными.

Концентраторы являются центральным узлом в топологии «звезда». Однако в настоящее время они становятся одним из стандартных компонентов большинства ЛВС.

Среди концентраторов выделяют активные и пассивные. *Активные* концентраторы регенерируют и передают сигналы, также как это делают репитеры. Иногда их называют еще *многопортовыми репитерами*. Они имеют от 8 до 12 портов для подключения компьютеров.

Пассивные концентраторы – это монтажные панели или коммутирующие блоки. Они просто пропускают через себя сигнал, не усиливая и не восстанавливая его. Пассивные, в отличие от активных, не надо подключать к источнику питания. *Гибридными* называют конденсаторы, к которым можно подключить кабели различных типов.

Концентраторы можно соединить между собой. При такой топологии разрыв кабеля, подключенного к концентратору, нарушит работу только одного конкретного сегмента сети .

Топология типа «кольцо»

При этой топологии сеть замкнута, образуя неразрывное кольцо (рис. 3.5). Поэтому у кабеля просто не может быть свободного конца, к которому надо подключить терминатор. Начав движение в какой-либо точке кольца (PC₁), пакет данных в конце концов попадает в его начало. Из-за такой особенности данные в кольце движутся всегда в одном направлении.

В отличие от пассивной топологии «шина», здесь каждый компьютер выступает в роли репитера, усиливая сигналы и передавая их следующему компьютеру. В отличие от «звезды» «кольцу» необходим неразрывный путь между всеми сетевыми PC. Поэтому при выходе из строя какой-либо одной PC сеть прекращает функционировать.

Другое слабое место «кольца» состоит в том, что данные проходят

через каждый сетевой компьютер, давая возможность "не очень хорошим" людям заниматься перехватом информации, не предназначенной посторонним. Кроме того, изменение конфигурации сети или подключение новой РС требует остановки всей сети.

Тема 4 Технологии построения и функционирования локальных сетей

На сегодня большая часть компьютерных сетей используют для соединения провода и кабели. Они выступают в качестве среды передачи сигналов между компьютерами. Наиболее распространены: коаксиальный кабель, витая пара, оптоволоконный кабель.

Однако постепенно в нашу жизнь входит беспроводная среда передачи данных. Термин «беспроводная среда» может ввести в заблуждение, т. к. предполагает полное отсутствие проводов. В действительности это не так. Обычно беспроводные компоненты взаимодействуют с сетью, где основная среда передачи данных - кабель. В ЛВС они оказываются наиболее полезными:

- в помещениях, заполненных людьми (приемная и т. п.);
- для людей, которые не работают на одном месте (врач, брокер и т. п.);
- в изолированных помещениях и зданиях (склад, гараж и т. п.);
- в строениях (памятниках архитектуры или истории), где прокладка дополнительных кабельных трасс недопустима.

Для беспроводной передачи данных используют: инфракрасное и лазерное излучение, радиопередачу и телефонию. Эти способы передачи данных в компьютерных сетях, как локальных, так и глобальных, привлекательны тем, что:

- гарантируют определенный уровень мобильности;
- позволяют снять ограничение на длину сети, а использование радиоволн и спутниковой связи делают доступ к сети фактически неограниченным.

До недавнего времени самой распространенной средой передачи данных был коаксиальный кабель: относительно недорогой, легкий и гибкий, безопасный и простой в установке.

Электрические сигналы, кодирующие данные, передаются по жиле. Она изоляцией отделяется от металлической оплетки, которая играет роль заземления и защищает передаваемые по жиле сигналы от:

- внешних электромагнитных шумов (атмосферных, промышленных);

□ перекрестных помех – электрических наводок, вызванных сигналами в соседних проводах.

Используют толстый и тонкий коаксиальный кабель. Их характеристики представлены в таблице 4.1.

Таблица 4.1

Характеристики коаксиального кабеля.

Тип	Диаметр	Эффективная длина сегмента	Скорость передачи	Обозначение по стандарту IEEE 802.3
толстый	1 см	500 м	10 Мбит/с	10 base 5
тонкий	0,5 см	185 м	10 Мбит/с	10 base 2

В обозначении кабелей по стандарту IEEE 802.3 первые две цифры – скорость передачи в Мбит/с, base обозначает, что кабель используется в сетях с узкополосной передачей (baseband network), последняя цифра – эффективная длина сегмента в сотнях метров, при которой уровень затухания сигнала остается в допустимых пределах. Тонкий подключается к сетевым платам непосредственно через *T-коннектор*, толстый – через специальное устройство – *трансивер*.

Различают *обычные* и *пленумные* коаксиальные кабели. Последние обладают повышенными механическими и противопожарными характеристиками и допускают прокладку под полом, между фальшпотолком и перекрытием. При выборе для ЛВС данного типа кабеля следует принимать во внимание, что:

- 1) это среда для передачи речи, видео и двоичных данных;
- 2) позволяет передавать данные на большие расстояния;
- 3) это хорошо знакомая технология, предлагающая достаточный уровень защиты данных.

Если для передачи электрических сигналов воспользоваться обычной парой параллельных проводов для передачи знакопеременного сигнала большой частоты, то возникающие вокруг одного из них магнитные потоки будут вызывать помехи в другом. Для исключения этого явления провода перекручивают между собой.

Самая простая *витая пара (twisted pair)* – это два переплетенных друг вокруг друга изолированных провода. Существует два вида такого кабеля:

- неэкранированная витая пара (UTP);
- экранированная витая пара (STP).

Часто несколько витых пар помещают в одну защитную оболочку (типа телефонного кабеля). Наиболее распространена в ЛВС неэкранированная витая пара стандарта 10 baseT с эффективной длиной сегмента – 100 м.

Определено 5 категорий на основе UTP (таблица 4.2).

Таблица 4.2

Категории кабельных соединений на неэкранированной витой паре

Категория	Скорость передачи (Мбит/с)	Количество пар
1	Телефонный кабель только для передачи речи	1 пара
2	До 4	4 пары
3	До 10	4 пары с 9-ю витками на 1 м
4	До 16	4 пары
5	До 100	4 медных пары

Одной из проблем всех этих кабелей являются перекрестные помехи, т.е. наводки со стороны соседних линий, что может приводить к искажению передаваемых данных. Для уменьшения их влияния используют экран. В кабелях на основе экранированных витых пар каждая пара обматывается фольгой, а сам кабель заключается в медную оплетку, что позволяет передавать данные с более высокой скоростью и на большие расстояния.

При построении развитой кабельной системы ЛВС и для упрощения работы с ней используются следующие компоненты:

- Концентраторы. Для подключения витой пары к компьютеру используется телефонный коннектор RJ-45, который отличается от используемых в современных телефонах и факсах RJ-11 тем, что имеет 8 контактов вместо 4.
- Распределительные стойки и полки, которые позволяют организовать множество соединений и занимают мало места.
- Коммутационные панели. Существуют разные панели расширения. Они поддерживают до 96 портов и скорость передачи до 100 Мбит/с.
- Соединители. Одинарные или двойные витки RJ-45 для подключения к панели расширения или настенным розеткам. Обеспечивают скорость до 100 Мбит/с.
- Настенные розетки к которым можно подключить два или более соединителя.

Достоинством использования компонентов кабельной системы ЛВС является то, что на их основе можно компоновать сети различной топологии. Один из вариантов использования компонентов кабельной системы ЛВС может иметь вид, аналогичный приведенному.

При разработке топологии и построении конкретных ЛВС рекомендуется использовать витую пару в тех случаях, если:

- есть ограничения на материальные затраты при организации ЛВС;
- нужна достаточно простая установка, при которой подключение компьютеров – несложная операция.

Следует воздержаться от использования витой пары, если Вы хотите быть

абсолютно уверенными в целостности данных, передаваемых на большие расстояния с высокой скоростью. В этих случаях более надежным является применение оптоволоконного кабеля.

В оптоволоконном кабеле цифровые данные распространяются по оптическим волокнам в виде модулированных световых импульсов, а не электрических сигналов. Следовательно, его нельзя вскрыть и перехватить данные.

Передача по оптоволоконному кабелю не подвержена электрическим помехам и ведется на чрезвычайно высокой скорости (до 100 Мбит/с, а теоретически возможно до 200 Мбит/с).

Основа кабеля – оптическое волокно – тонкий стеклянный цилиндр (жила), покрытая слоем стекла, называемого оболочкой и имеющей отличный от жилы коэффициент преломления.

Каждое стеклянное оптоволокно передает сигналы только в одном направлении, поэтому кабель состоит из двух волокон с отдельными коннекторами (рис. 4.8). Жесткость обеспечивает покрытие из пластика, а прочность – волокна кевлара. Оптоволоконный кабель рекомендуется использовать:

- при передаче данных на большие расстояния с высокой скоростью по надежной среде передачи.

Не рекомендуется использовать:

- при ограниченности денежных средств;
- при отсутствии навыков установки и корректного подключения оптоволоконных сетевых устройств.

В современных компьютерных сетях для передачи кодированных сигналов по сетевому кабелю наибольшее применение находят две наиболее распространенные технологии:

- узкополосная передача сигналов;
- широкополосная передача сигналов.

Узкополосные (baseband) системы передают данные в виде цифрового сигнала одной частоты.

Сигналы представляют собой дискретные электрические или световые импульсы. При таком способе вся емкость коммуникационного канала используется для передачи одного сигнала или, другими словами, цифровой сигнал использует всю полосу пропускания кабеля. *Полоса пропускания* – это разница между max и min частотой, которая может быть передана по кабелю. Каждое устройство в таких сетях посылает данные в *обоих направлениях*, а некоторые могут одновременно их передавать и принимать.

Широкополосные (broadband) системы передают данные в виде аналогового сигнала, который использует некоторый интервал частот (рис. 4.10). Сигналы представляют собой непрерывные (а не дискретные) электронные или оптические волны. При таком способе сигналы передаются по физической среде в одном направлении.

Если обеспечить необходимую полосу пропускания, то по одному

сетевому кабелю одновременно можно передавать несколько сигналов (например, кабельного телевидения, телефона и передача данных).

Каждой передающей системе выделяется часть полосы пропускания. Все устройства (в. т. ч. и компьютеры) настраиваются так, чтобы работать с выделенной им частью полосы пропускания.

В широкополосной системе сигнал передается только в одном направлении. Для возможности приема и передачи каждым из устройств необходимо обеспечить два пути прохождения сигнала. Для этого можно:

- использовать два кабеля;
- разбить полосу пропускания кабеля *на два канала*, которые работают с разными частотами: один канал на передачу, другой – на прием.

Данные, хранимые в РС и передаваемые между ними в ЛВС, представляются в цифровом виде. Каждое информационное сообщение (пакет) – это строка битов, содержащая закодированную информацию.

Так как кабель содержит всего две проводящие жилы, то в каждый момент времени по нему можно передать только один бит информации (последовательная передача данных).

1. При широкополосной передаче цифровые данные РС перед передачей по сетевому кабелю преобразуются в аналоговый несущий сигнал синусоидальной формы:

$$u = U \cdot \sin(\omega t + \varphi)$$

Это преобразование называется *модуляцией*. В зависимости от того, какой из параметров данного сигнала изменяется различают три типа модуляции: амплитудную, частотную и фазовую. Рассмотрим два из них.

При *амплитудной модуляции (АМ)* используется несущий сигнал постоянной частоты (ω_0). Для передачи бита со значением «1» передается волна несущей частоты. Отсутствие сигнала означает передачу бита «0», т. е.:

$$u = U_m \cdot \sin(\omega_0 t + \varphi_0), \quad \text{где} \quad \begin{array}{l} 1 \text{ при бите «1»} \\ 0 \text{ при бите «0»} \end{array}$$

При *частотной модуляции (ЧМ)* используется сигнал несущей с двумя частотами. В этом случае бит «1» представляется сигналом несущей частоты ω_1 , а бит «0» – частоты ω_2 , т. е.:

$$u = U_0 \cdot \sin(\omega_m t + \varphi_0), \quad \text{где} \quad \begin{array}{l} \omega_1 \text{ при бите «1»} \\ \omega_2 \text{ при бите «0»} \end{array}$$

Обратный процесс - процесс преобразования аналогового сигнала в цифровые данные на РС, которая принимает переданный ей модулированный сигнал называется *демодуляцией*.

2. При узкополосной передаче используется двуполярный дискретный сигнал. При этом кодирование в сетевом адаптере передающей РС цифровых данных в цифровой сигнал выполняется напрямую.

Наиболее простым и часто используемым является кодирование *методом без возврата к нулю (NRZ – Non Return to Zero)*, в котором бит «1»

представляется положительным напряжением (H – высокий уровень), а бит «0» – отрицательным напряжением (L – низкий уровень). Т. е. сигнал всегда выше или ниже нулевого напряжения, откуда и название метода.

Как при передаче аналоговых, так и цифровых сигналов, если следующие друг за другом биты равны (оба «0» или оба «1»), то трудно сказать, когда кончается один и начинается другой. Для решения этой задачи приемник и передатчик надо синхронизировать, т. е. одинаково отсчитывать интервалы времени.

Это можно выполнить либо введя дополнительную линию для передачи синхроимпульсов (что не всегда возможно, да и накладно), либо использовать специальные методы передачи данных: асинхронный или автоподстройки.

Асинхронная передача и автоподстройка. При низких скоростях передачи сигналов используется метод асинхронной передачи, при больших скоростях эффективнее использовать метод автоподстройки. Как передатчик, так и приемник снабжены генераторами тактовых импульсов, работающими на одной частоте. Однако невозможно, чтобы они работали абсолютно синхронно, поэтому их необходимо периодически подстраивать. Аналогично обыкновенным часам, которые необходимо периодически корректировать.

При *асинхронной передаче* генераторы синхронизируются в начале передачи каждого пакета (или байта) данных и предполагается, что за это время не будет рассогласования генераторов, которые бы вызвали ошибки в передаче. При этом считается, что все *пакеты одной длины* (например, байт). Синхронизация тактового генератора приемника достигается тем, что:

- перед каждым пакетом (байтом) посылается дополнительный «старт-бит», который всегда равен «0»;
- в конце пакета посылается еще один дополнительный «стоп-бит», который всегда равен «1».

Если данные не передаются, линия связи находится в состоянии «1» (состояние незанятости). Начало передачи вызывает переход от «1» к «0», что означает начало «старт-бита». Этот переход используется для синхронизации генератора приемника.

При *передаче с автоподстройкой* используется метод Манчестерского кодирования, при котором:

- тактовый генератор приемника синхронизируется при передаче каждого бита;
- и следовательно, можно посылать *пакеты любой длины*.

Синхронизация сигнала данных достигается обеспечением перехода от «H»-уровня к «L»-уровню или наоборот, в середине каждого бита данных (рис. 4.14). Эти переходы служат для синхронизации тактового генератора приемника. Биты данных кодируются: «0» – при переходе «L» → «H» и «1» – при переходе «H» → «L»

Если информация не передается, в линии данных нет никаких

переходов и тактовые генераторы передатчика и приемника рассогласованы.

При этом виде кодирования переходы происходят не только в середине каждого бита данных, но и между битами, когда два последовательных бита имеют одно и то же значение.

После простоя линии необходима предварительная синхронизация генератора, которая достигается посылкой *фиксированной последовательности битов* (преамбула и биты готовности).

Например, можно использовать преамбулу из восьми битов: 11111110, где первые 7 битов используются для начальной синхронизации, а последний – для сообщения приемнику, что преамбула окончилась, т. е. далее пойдут биты данных.

Плата сетевого адаптера (СА)

Плата сетевого адаптера выступает в качестве физического интерфейса или соединения между компьютером и сетевым кабелем. Платы вставляются в слоты расширения системной шины всех сетевых компьютеров и серверов. Назначение платы сетевого адаптера:

- подготовка данных, поступающих от компьютера, к передаче по сетевому кабелю;
- передача (или прием) данных другому компьютеру;
- управление потоком данных между компьютером и кабельной системой.

1. Подготовка данных. Плата сетевого адаптера принимает циркулирующие по системной шине параллельные данные, организует их для последовательной (побитовой) передачи.

Этот процесс завершается переводом цифровых данных компьютера в электрические или оптические сигналы, которые и передаются по сетевым кабелям. Отвечает за это преобразование *трансивер*.

2. Сетевой адрес. Помимо преобразования данных плата СА должна указать свой адрес, чтобы ее можно было отличить от других плат. За каждым производителем СА закреплен стандартом IEEE некоторый интервал адресов. Производители «прошивают» эти адреса в микросхеме плат. Благодаря этому, каждый СА и, следовательно, каждый сетевой компьютер имеет уникальный адрес в сети.

При передаче данные из памяти компьютера через системную шину поступают в СА. Обычно они поступают быстрее, чем их способна передать плата СА, поэтому она должна иметь буфер для их временного хранения. Это позволяет согласовать скорости передачи по шине без потерь производительности и искажения данных.

3. Передача и управление данными. Перед посылкой данных по сети плата СА проводит «электронный диалог» с принимающим СА, во время которого они «оговариваются»:

- максимальный размер блока передаваемых данных;
- объем данных, передаваемый без подтверждения о получении;
- интервалы между передачами блоков;

- объем данных, который может принять СА, не переполняясь;
- скорость передачи данных.

Все эти действия каждый СА выполняет в строго определенной последовательности в соответствии со строго определенными правилами, которые называются *протоколами* и подробно будут рассматриваться ниже.

Тема 5 Технологии построения и функционирования глобальных сетей

Аппаратное и программное обеспечение, работающие в сети, разрабатываются в разных фирмах. Для того чтобы оно было совместимо между собой, международной организацией по стандартам (ISO) была разработана *базовая эталонная модель открытых систем (OSI – Open System Interconnection model)*.

Эта модель описывает многоуровневую архитектуру сети, при которой все сетевые функции разделены на семь уровней (рис. 6.1). Каждому уровню соответствуют определенные сетевые операции, оборудование и протоколы.

Протокол – это четко определенный набор правил и соглашений для взаимодействия одинаковых уровней сети.

Интерфейс определяет услуги, которые нижний уровень предоставляет верхнему и способ доступа к ним.

Задача каждого уровня – предоставление услуг вышестоящему уровню, «маскирую» детали реализации этих услуг. Когда два компьютера в сети работают друг с другом, каждый из сетевых уровней обменивается данными с себе подобным (на основе протокола этого уровня).

Эта логическая или виртуальная связь изображена на рис. 6.2. пунктирной линией. Однако реальная передача данных происходит на самом нижнем – физическом уровне, где находится физическая среда передачи (сетевой кабель). Т. е. на самом деле данные перемещаются:

- сверху вниз от прикладного уровня к физическому;
- в рамках физического уровня горизонтально по сетевому кабелю к компьютеру – приемнику данных;
- полученные данные затем двигаются вверх по уровням сетевой модели (рис. 6.2).

Сетевая модель ISO/OSI определяет сеть в терминах нескольких функциональных уровней. Каждый сетевой уровень включает строго определенные функции и применяет для этого один или несколько протоколов:

- физический уровень передает данные по сетевым каналам и включает в себя аппаратные средства, необходимые для этого;
- канальный - предохраняет данные от повреждения на физическом уровне;

- сетевой - передает данные от одного сетевого компьютера к другому;
- транспортный - передает данные от одного приложения к другому;
- сеансовый – это сетевой интерфейс пользователя;
- представительский - занимается проблемами сетевого интерфейса к принтерам, мониторам и преобразованием форматов файлов;
- прикладной – это набор широко используемых сетевых приложений.

Каждый из семи уровней определяет перечень услуг, которые он предоставляет смежным уровням, реализуя определенный набор сетевых функций.

1. Физический уровень

- обеспечивает физический путь для передачи кодированных сигналов;
- устанавливает характеристики этих сигналов (амплитуда, частота, длительность и т.д.);
- определяет способ соединения СА с кабелем, тип разъемов, способ передачи;
- обеспечивает поддержку потока битов, содержание которых на этом уровне не имеет значения;
- отвечает за кодирование данных и синхронизацию битов.

2. Канальный уровень

- определяет правила совместного использования физического уровня узлами сети;
- передает информацию адресованными порциями – кадрами;
- определяет формат кадра и способ, согласно которому узел сети решает, когда можно передать или принять кадр.
- Кадры данных содержат сообщения верхних уровней (пакеты). Другие кадры, такие как маркеры или подтверждения приема, используют методы обнаружения и коррекции ошибок. С точки зрения верхних уровней, канальный и физический обеспечивают безошибочную передачу пакетов данных.

Пример. В состав любого пакета входит информация для контроля правильности передачи. Так в трейлер пакета Интернет записывается контрольная сумма (КС) пакета. Она получается путем разбиения пакета на сегменты по 16 бит, которые представляются целыми числами, складываются и записываются в трейлер.

При приеме вычисляется новая КС и сравнивается с принятой. Если они равны, то посылается подтверждение и выдается новый пакет. Если не равны, то посылается сообщение «несовпадение» и передача пакета повторяется.

Если пакет не дошел или не дошел сигнал подтверждения, передающая станция, не получив пакет в течение некоторого времени, посылает пакет еще раз (реализую, так называемый, режим "time-out")

Существуют более мощные методы защиты от ошибок (циклические коды, коды Хэминга и т.д.), а также алгоритмы переспроса и повторения пакетов.

3. Сетевой уровень

Отвечает за буферизацию и маршрутизация в сети. Маршрутизация – существенная функция при работе в глобальных сетях (с коммутацией пакетов), когда необходимо определить маршрут передачи пакета, выполнить перевод логических адресов узлов сети в физические.

В ЛВС между любой парой узлов есть прямой путь (маршрут), поэтому основная функция этого уровня сводится к буферизации пакетов.

4. Транспортный уровень

- с передающей стороны переупаковывает информационные сообщения: длинные разбиваются на несколько пакетов, короткие объединяются в один;
- с принимающей стороны собирает сообщения из пакетов.

Так как сетевой уровень обеспечивает буферизацию, то несколько узлов могли передать свои сообщения в один и тот же узел сети. Моменты прибытия пакетов могут чередоваться. Задача этого уровня – правильная сборка пакетов каждого сообщения без смещения и потерь.

Транспортный уровень является границей, выше которой в качестве единицы информации рассматривается только сообщение, ниже – управляемый сетью пакет данных.

5. Сеансовый уровень

Позволяет двум приложениям на разных рабочих станциях устанавливать, использовать и завершать соединение, называемое *сеансом*. Сеанс создается по запросу процесса пользователя. В запросе определены: назначение сеанса связи (адрес); партнер, например, соответствующий прикладной процесс в другом узле.

Сеанс может начаться только в том случае, если прикладной процесс партнера активен и согласен связаться. На этом уровне выполняются такие функции, как распознавание имен и защита, необходимые для связи двух приложений в сети. Любой пользователь, введя имя и пароль и вошедший в сеть, создает сеанс.

6. Уровень представления

Его функция заключается в преобразовании сообщений, используемых прикладным уровнем, в некоторый общепринятый формат обмена данными между сетевыми компьютерами.

Целью преобразования сообщения является сжатие данных и их защита. В интерфейсе выше этого уровня поле данных сообщения имеет

явную смысловую форму; ниже этого уровня поле данных сообщений и пакетов рассматривается как передаточный груз и их смысловое значение не влияет на обработку.

На этом уровне работает утилита ОС, называемая *редиректор*. Ее назначение – переадресовать операции ввода/вывода к ресурсам сервера.

7. Прикладной уровень

Представляет собой окно для доступа прикладных процессов к сетевым услугам. Он обеспечивает услуги, напрямую поддерживающие приложение пользователей, такие как программное обеспечение для передачи файлов, доступа к БД и электронной почтой. Прикладной уровень управляет:

- общим доступом к сети;
- потоком данных;
- обработкой ошибок.

Основная идея модели OSI заключается в том, что каждому уровню отводится конкретная роль. Благодаря этому общая задача передачи данных расчленяется на ряд отдельных легкообозримых задач.

Операционная система управляет ресурсами компьютера, а сетевая операционная система обеспечивает управление аппаратными и программными ресурсами всей сети. Тем не менее, для передачи данных в сети нужен еще один компонент – протокол.

Протокол – это правила и технические процедуры, позволяющие нескольким компьютерам при объединении в сеть общаться друг с другом. Отметим три основных момента, касающихся протоколов:

1. Существует множество протоколов. И хотя все они участвуют в реализации связи, каждый протокол имеет:

- различные цели;
- выполняет определенные задачи;
- обладает своими преимуществами и ограничениями.

Протоколы реализуются через заголовки, которые добавляются к пакетам по мере того, как они передаются по уровням. Каждый заголовок связывается с конкретным уровнем и в каждом последующем уровне воспринимается как часть пакета .

При поступлении пакета в принимающий узел, заголовки соответствующих уровней используются для вызова заданной функции в принимающем узле. При передаче пакета выше этот заголовок изымается. И компьютер-отправитель, и компьютер-получатель должны выполнять каждое действие одинаковым способом с тем, чтобы пришедшие по сети данные совпали с отправленными.

Если, например, два протокола будут по-разному разбивать данные на пакеты или по-разному добавлять данные (о последовательности пакетов, синхронизации и т. д.), то тогда компьютер, использующий один из протоколов, не сможет связаться с компьютером, на котором работает другой протокол.

На работу протоколов ряда уровней оказывает влияние, является ли сеть с коммутацией соединений или с коммутацией пакетов. Широкое развитие межсетевых объединений («интернет»), компонентами которых являются ЛВС, привело к тому, что данные из одной ЛВС в другую могут передаваться по одному из возможных маршрутов. Протоколы, которые поддерживают такую передачу, называются *маршрутизируемыми протоколами*. И их роль постоянно возрастает.

Существует несколько стандартных стеков протоколов, разработанных разными фирмами. Протоколы этих стеков выполняют работу, специальную для своего уровня. Однако коммуникационные задачи, которые возложены на сеть, приводят к разделению протоколов на три типа : прикладные протоколы; транспортные протоколы и сетевые протоколы.

Прикладные протоколы работают на верхнем уровне модели OSI и обеспечивают взаимодействие приложений и обмен данными между ними.

Транспортные протоколы поддерживают сеансы связи между компьютерами и гарантируют надежный обмен данными между ними.

Сетевые протоколы обеспечивают услуги связи. Эти протоколы управляют: адресацией, маршрутизацией, проверкой ошибок и запросами на повторную передачу.

Тема 6 Сетевое программное обеспечение

Сетевая архитектура – это комбинация *стандартов, топологий и протоколов*, необходимых для создания работоспособной сети. В соответствии со стандартными протоколами физического уровня выделяют три основные сетевые архитектуры: Ethernet (протокол 802,3) и Fast Ethernet (протокол 802,30); ArcNet (протокол 802,4); Token Ring (протокол 802.5). Рассмотрим каждую из сетевых архитектур более подробно.

Ethernet Это самая популярная в настоящее время сетевая архитектура. Она использует:

- физические топологии «шина», «звезда» или «звезда –шина»;
- логическую топологию «шина»;
- узкополосную передачу данных со скоростями 10 и 100 Мбит/с;
- метод доступа – CSMA/CD.

Поле «Тип протокола» используется для идентификации протокола сетевого уровня (IPX и IP) – маршрутизируемый или нет. Спецификация Ethernet выполняет функции физического и канального уровня модели OSI. Различают несколько стандартов сетевых архитектур Ethernet:

- 10BaseT – на основе витой пары;
- 10Base2 – на тонком коаксиале;
- 10Base5 – на толстом коаксиале;
- 10BaseFL – на оптоволокне;
- 10BaseX – со скоростью передачи 100 Мбит/с, который включает в себя ряд спецификаций в зависимости от среды передачи.

Рассмотрим наиболее распространенные стандарты данной архитектуры, применяемые при построении ЛВС.

Физическая топология представляет собой «звезду» на основе витой пары, соединяющей все узлы сети с концентратором, используя две пары проводов: одну для передачи, другую – для приема .

Логически (т.е. по системе передачи сигналов) данная архитектура представляет собой «шину» как и все архитектуры Ethernet. Концентратор выступает как многопортовый репитер. Длина сегмента от 2,5 до 100 м. ЛВС стандарта 10BaseT может обслуживать до 1024 компьютеров.

Достоинством является возможность использования распределительных стоек и панелей коммутации, что позволяет легко перекоммутировать сеть или добавить новый узел без остановки работы сети. Новейшие концентраторы позволяют расширять топологию сети, соединив

отдельные концентраторы между собой магистралью на основе коаксиального или оптоволоконного кабеля и получить топологию «звезда – шина».

Сеть такого типа ориентирована на тонкий коаксиальный кабель с максимальной длиной сегмента 185 м и возможностью подключения к одному сегменту до 30 ЭВМ .

Эта сетевая архитектура физически и логически представляет собой «шину». С использованием репитеров может быть увеличена общая протяженность сети введением дополнительных сегментов. Однако при этом необходимо учитывать *правило 5-4-3*. Сеть на тонком коаксиале может состоять максимум из 5 сегментов кабеля, соединенных 4 репитерами. При этом только к 3 сегментам можно подключать рабочие станции. Два из пяти сегментов являются межрепитерными связями и служат только для увеличения длины сети. Максимальное число компьютеров до 1024, а общая длина сети до 925м.

Сетевая архитектура на толстом Ethernet логически и физически представляет собой «шину» (рис. 7.5). Магистральный сегмент (т. е. главный кабель, к которому подключаются трансиверы для связи с РС) имеет длину до 500 м и возможность подключения до 100 компьютеров. С использованием репитеров, которые также подключаются к магистральному сегменту через трансиверы, общая длина сети может составить 2500 м.

При расширении сети справедливо правило 5–4–3 и возможно комбинирование тонкого и толстого кабеля. В этом случае в качестве магистрали, способной передавать данные на большие расстояния, используется толстый кабель, а в качестве ответвляющих сегментов используют тонкий.

Данная архитектура строится на оптоволоконном кабеле, доступ к которому со стороны компьютеров и репитеров осуществляется с помощью трансиверов. На сегодняшний день в основном используются внешние трансиверы.

Особенность этих трансиверов в том, что их передатчики преобразуют электрические сигналы от ЭВМ в световые импульсы, а приемники – световые в электрические. Популярность использования 10BaseFL обусловлена:

- высокой помехозащищенностью;
- возможностью прокладки кабеля между репитерами на большие расстояния, т. к. длина сегмента до 2 – 4 км;
- использование повторителей позволяющих реализовать «каскадные звезды» путем соединения оптических ответвителей.

На рынке предлагаются ответвители типа коаксиал-волокно и ответвители типа волокно-коаксиал.

Этот стандарт, иногда называемый Fast Ethernet, является расширением существующей сетевой архитектуры Ethernet и соответствует

протоколу физического уровня IEEE 802.30. Его особенностью является то, что он сохранил стандартный для Ethernet метод доступа CSMA/CD, от которого отходили разработчики других технологий повышенной скорости передачи в сети. Сохранение метода доступа означает, что имеющиеся в наличие драйверы для Ethernet будут работать без изменений.

Преимуществом этой технологии, появившейся в конце 1993 года, является то, что степень ее совместимости с Ethernet-сетями, позволяет интегрировать ее в эти сети с помощью двухскоростных сетевых адаптеров или мостов. Данная сетевая архитектура использует физическую топологию «звезда» или «звезда – шина» (подобно 10BaseT), где все кабели подключаются к концентратору. Различают три спецификации среды:

- 100BaseT4 (UTR категории 3, 4 или 5 с 4-мя парами);
- 100BaseTX (UTR или STP категории 5 с 2-мя парами);
- 100BaseFX (двужильный оптоволоконный кабель).

Для реализации этой технологии необходимо две пары проводов или двужильный оптокабель, чтобы организовать дуплексную передачу сигналов по традиционной CSMA/CD, используя одну пару для передачи, а другую – для приема.

Сегментация сети Мы уже рассматривали задачу построения сети из нескольких сегментов. В частности, если не хватает длины одного сегмента для соединения всех пользователей сети, то можно через репитер подключить еще один сегмент. Но иногда возникает и другая задача. Пусть имеем сегмент сети с очень интенсивным трафиком, который снижает производительность всей сети. Повысить ее производительность можно, если разделить перегруженный сегмент на два и соединить их с помощью моста или маршрутизатора. Тогда трафик в каждом сегменте уменьшится, т.к. меньшее число компьютеров в каждом из сегментов попытается осуществить передачу, и время доступа к кабелю сокращается. Сегментация может помочь и при ограничении доступа к конфиденциальной информации.

Это простая, гибкая и недорогая сетевая архитектура, поддерживающая протокол физического уровня IEEE 802.4:

- физическая топология - «звезда», «шина», «звезда – шина»;
- логическая топология – упорядоченное «кольцо»;
- широкополосная передача данных 2,5 Мбит/с и 20 Мбит/с (для ArcNet Plus);
- метод доступа маркерный;
- средой передачи может быть:
 - коаксиальный кабель (длиной 600 м при «звезде» и 300 м при «шине»);
 - витая пара (максимальная длина 244 м – при «звезде» и «шине»);

Компьютеры могут быть коаксиальным кабелем связаны в шину или в иных случаях подключены к концентраторам, которые могут быть: пассивными;

активными; интеллектуальными. *Пассивные* концентраторы просто осуществляют коммутацию кабельных соединений сети. *Активные* – восстанавливают и ретранслируют сигнал. *Интеллектуальные* – обнаруживают изменения в сети и удаленно управляют работой сетевых устройств.

Особенность маркерного доступа ArcNet (рис.7.9) состоит в том, что:

- все компьютеры имеют свои сетевые адреса;
- маркер передается между компьютерами согласно их номерам;
- маркер двигается от компьютера с меньшим номером к компьютеру с более высоким номером, хотя тот может находиться на другом конце сети;
- приемник, получив маркер, добавляет к нему свой пакет, который, дойдя до адресата, освобождает маркер.

Полепредупреждения	Начало заголовок	Адрес		Тип протокола	Данные	Полеконтрольнойсуммы
		приемника	источника			

Пакет передачи информации в ArcNet

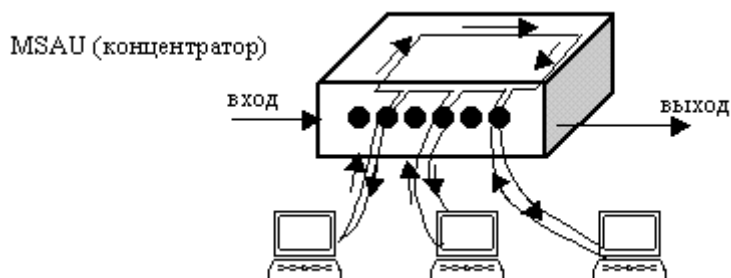
Общее количество узлов: 255 – ArcNet; 2047 – Arc Net Plus. ArcNet – это одна из самых старых сетевых архитектур, реализованная недавно фирмой DataPoint в более современную ArcNet Plus. Однако на смену этим архитектурам приходят более современные и производительные. Одной из таких архитектур является FDDI, которая будет рассмотрена ниже. А сейчас познакомимся с давно используемой и хорошо зарекомендовавшей себя архитектурой.

Данная сетевая архитектура была разработана и внедрена фирмой IBM еще в 1984 г. как часть предложенного ею способа объединить в сеть весь ряд выпускаемых IBM компьютеров: персональные компьютеры; средние ЭВМ и мейнфреймы. Разрабатывая эту технологию, IBM ставила задачу обеспечить простоту монтажа кабеля – витой пары – соединяющего компьютер с сетью через розетку. Token Ring является реализацией протокола физического уровня IEEE 802.5:

- физическая топология – «звезда»;
- логическая топология – «кольцо»;
- узкополосный тип передачи;
- скорость передачи 4 и 16 Мбит/с;
- соединение неэкранированной и экранированной витой пары;
- метод доступа – маркерное кольцо.

Стартовый разделитель	Управление доступом	Управление кадрами	Адрес		Данные	Циклический код	Конец кадра	Статус кадра
			приемника	источника				

Аппаратные компоненты Логическое кольцо в этой сетевой архитектуре организуется концентратором, который называется модулем множественного доступа (MSAU – MultyStation Access Unit) или интеллектуальным модулем множественного доступа (SMAU – Smart Multystation Access Unit). Кабели (витые пары) соединяют клиентов и серверов с MSAU, который работает по принципу других концентраторов.



При соединении компьютеров он включается в кольцо. IBM MSAU имеет 10 портов соединения. К нему можно подключить до 8 компьютеров. Каждое кольцо может содержать до 33 концентраторов.

Общее число компьютеров – 72 при использовании UTP и 260 при использовании STP. Другие производители выпускают MSAU большей емкости (в зависимости от модели). Расширение логического кольца на базе концентраторов позволяет увеличить общее количество узлов в сети .

При этом расстояние между концентраторами до 45м (152м), а каждая РС соединяется с MSAU: при UTP - сегментом до 45м; при STR - сегментом до 100м. Расстояние между MSAU можно увеличить до 365, установив репитер.

Известны две модели сетевых плат на 4 и 16 Мбит/с. Платы на 16Мбит/с могут обеспечить передачу более длинных кадров, что сокращает количество передач для одного и того же объема данных.

Мониторинг системы Компьютер, который первым начал работу, наделяется системой Token Ring особыми функциями. Этот компьютер:

- должен наблюдать за работой всей системы;
- осуществляет текущий ее контроль;
- проверяет корректность отправки и получения кадров;
- отслеживает кадры, проходящие по кольцу более одного раза;
- гарантирует, что в кольце одновременно находится лишь один маркер.
- После появления в сети нового компьютера система иницирует его, чтобы он стал частью кольца. Это включает в себя: проверку уникальности адреса; уведомление всех узлов сети о появлении нового узла.

В «теоретической» кольцевой топологии вышедший из строя компьютер останавливает движение маркера, что в свою очередь

останавливает работу всей сети. В реальных сетевых архитектурах Token Ring используются интеллектуальные концентраторы, которые в состоянии обнаружить отказавшую сетевую плату (PC) и во время отключить ее.

Эта процедура позволяет “обойти” отказавший компьютер, поэтому маркер продолжает свое движение. Таким образом, отказавший компьютер не влияет на работу сети.

