**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ**

**ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ
«ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ГОУ ВО ЛНР «ЛГПУ»)**

Е. Ю. Суворова, В. Н. Шишлакова

КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ

Часть 1

**Учебное пособие
для студентов очной и заочной форм обучения
по направлению подготовки
44.03.05 «Педагогическое образование
(с двумя профилями подготовки)
Начальное образование. Информатика»**

Книта
Луганск
2022

УДК 378.016
ББК 74.484.4
С89

Р е ц е н з е н т ы :

Швыров В. В. – доцент кафедры информационных образовательных технологий и систем Государственного образовательного учреждения высшего образования Луганской народной республики «Луганский государственный педагогический университет» кандидат физико-математических наук, доцент;

Давыскиба О. В – доцент кафедры фундаментальной математики Государственного образовательного учреждения высшего образования Луганской народной республики «Луганский государственный педагогический университет», кандидат педагогических наук, доцент;

Мальцев Я. И. – доцент кафедры прикладной математики Государственного образовательного учреждения высшего образования Луганской народной республики «Луганский государственный университет имени Владимира Даля», кандидат технических наук, доцент

Суворова, Е. Ю., Шишлакова, В. Н.

С89 Компьютерные системы и сети: учебное пособие. Часть 1 / Е. Ю. Суворова, В. Н. Шишлакова; ГОУ ВО ЛНР «ЛГПУ». – Луганск: Книта, 2022. – 140 с.

Учебное пособие (часть 1) содержит теоретический материал по основам функционирования сетей, видам топологий, сетевым компонентам, методам доступа, средам передачи данных, типам оборудования и т.д.

Рекомендовано для студентов очной и заочной форм обучения по направлению подготовки 44.03.05 «Педагогическое образование (с двумя профилями подготовки). Начальное образование. Информатика».

УДК 378.016
ББК 74.484.4

Рекомендовано Учебно-методическим советом ГОУ ВО ЛНР «ЛГПУ» в качестве учебного пособия для студентов очной и заочной форм обучения, обучающихся по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) Начальное образование. Информатика (протокол № 3 от 09.11.2022 г.)

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Компьютеры системы и сети – важная часть сегодняшнего мира, а область их применения охватывает буквально все сферы человеческой деятельности, включая педагогическую. Последние два десятилетия характеризуются динамичным развитием сетевых технологий. Это связано с широкой популярностью, пришедшей к Интернету, развитием веб-технологий, электронной почты, потокового аудио и видео, систем обмена сообщениями в реальном времени и т.п. Повсеместное использование компьютерных сетей требует от современного пользователя, в том числе педагога и преподавателя, наличия соответствующих знаний и навыков. Важное значение в приобретении этих знаний имеет учебная дисциплина «Компьютерные системы и сети». Однако, сетевые технологии сами по себе включают множество концепций и являются достаточно сложным для новичка. Кроме того, профессиональная литература, целиком посвященная компьютерным сетям, слишком избыточна и сложна для понимания студентами непрофильных специальностей и направлений.

В первой части учебного пособия «Компьютерные системы и сети» предпринята попытка компактного изложения основ технологий компьютерных сетей без углубления в детали, объяснения общеупотребительных в настоящее время терминов и определений, связанных с функционированием компьютерных сетей.

Порядок изложения материала следующий: вначале дается общее описание сетевых компьютерных технологий, основы построения и функционирования локальных и глобальных компьютерных сетей, принципы взаимодействия устройств и оборудования сети, приводятся наиболее важные термины и определения; далее рассматриваются базовая модель связи открытых систем OSI, взаимодействие уровней, принципы работы стека коммуникационных протоколов, топология вычислительной сети и методы доступа к данным. Заключительная теоретическая часть посвящена вопросам построения локальных вычислительных сетей и их компонентов,

изучается физическая среда передачи данных и сетевое оборудование.

В довершение, с целью закрепления изложенного в пособии материала, в конце каждого раздела приведены контрольные вопросы, обсуждение которых способствует углублению понимания темы.

В конце издания приведен глоссарий, который упрощает процесс использования пособия и работу с материалом.

1. ОБЗОР И АРХИТЕКТУРА ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

1.1. Основные определения и термины

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 находятся в частном ведении пользователя и занимают некоторую территорию и по территориальному признаку разделяются на:

1. 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.

2. 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:

1. Сетевые компьютеры (оснащенные сетевым адаптером);
2. Операционные системы;
3. Каналы связи (кабельные, спутниковые, телефонные, цифровые, волоконно-оптические, радиоканалы и др.);
4. Различного рода преобразователи сигналов;
5. 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.

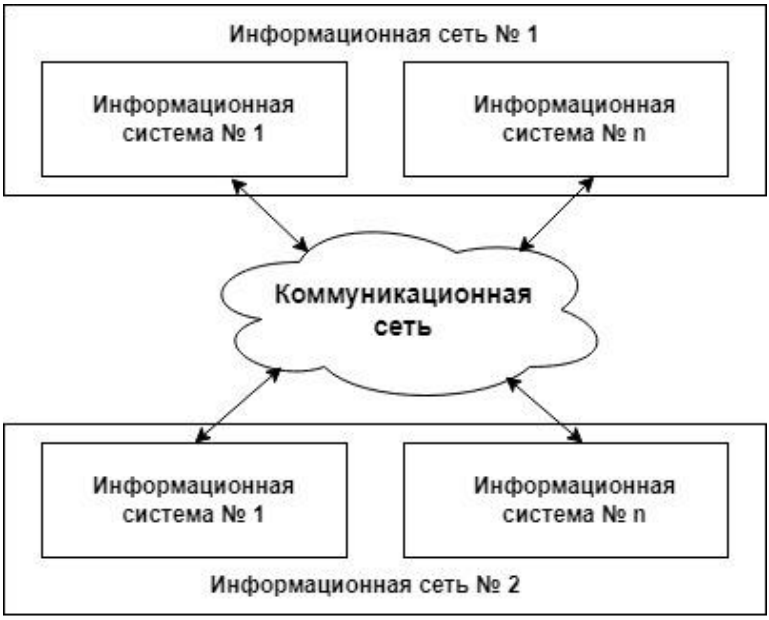

Рисунок 1.1 – Информационные и коммуникационные сети

Компьютерная сеть (сеть передачи данных) – группа устройств, объединенных между собой каким-либо способом с

целью совместного доступа к ресурсам и обмена информацией. состоит из информационных систем и каналов связи (рис. 1.2).

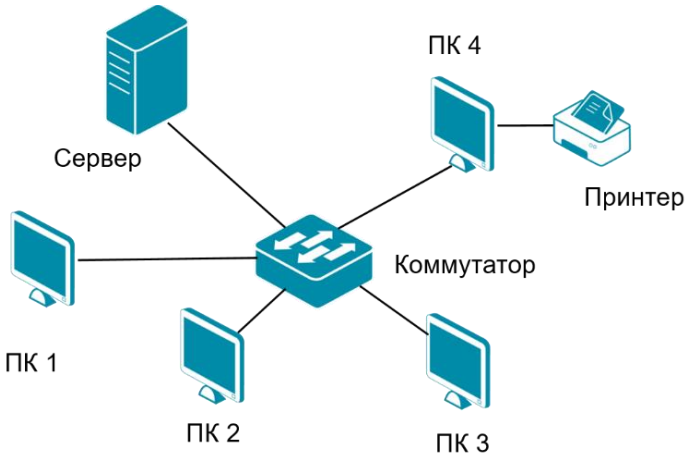

Рисунок 1.2 – Объединение устройств в компьютерной сети

Узел (абонент, хост) – оконечное устройство (компьютер, сетевой принтер, IP-камера, IP-телефон, дисковый массив), непосредственно подключенное к сетеобразующему телекоммуникационному оборудованию.

Сервер – специально выделенный высокопроизводительный компьютер, оснащенный соответствующим программным обеспечением, централизованно управляющий работой сети и/или предоставляющий другим компьютерам свои ресурсы (файлы данных, накопители, процессорное время и т.д.).

Клиентский компьютер (рабочая станция) – компьютер пользователя сети, получающий доступ к ресурсам сервера (серверов).

Пропускная способность – максимально возможная скорость передачи данных по линии связи.

Сегмент сети – логически или физически обособленная часть сети.

Сегментация сети – разделения сети на сегменты с целью уменьшения в них количества узлов, увеличения пропускной способности в расчете на один узел и повышения безопасности.

Среда передачи (канал связи, линия связи) – физическая среда распространения сигналов от источника к приемнику.

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 два вида архитектур: архитектура «клиент-сервер» и одноранговая архитектура. Сети типа «клиент-сервер»: выделяются один или несколько компьютеров, называемых серверами. Одноранговые сети: все компьютеры равноправны.

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.

1.2. Преимущества использования сетей

Компьютерные сети представляют собой вариант сотрудничества людей и компьютеров, обеспечивающего ускорение доставки и обработки информации. Объединять компьютеры в сети начали более 30 лет назад. Когда возможности компьютеров выросли и ПК стали доступны каждому, развитие сетей значительно ускорилось.

Соединенные в сеть компьютеры обмениваются информацией и совместно используют периферийное оборудование и устройства хранения информации.

С помощью сетей можно разделять ресурсы и информацию. Ниже перечислены основные задачи, которые решаются с

помощью рабочей станции в сети, и которые трудно решить с помощью отдельного компьютера.

Компьютерная сеть позволит совместно использовать следующие периферийные устройства:

– принтеры;
– плоттеры;
– дисковые накопители;
– стримеры;
– сканеры;
– факс-модемы и т.п.

Компьютерная сеть позволяет совместно использовать информационные ресурсы:

– каталоги;
– файлы;
– прикладные программы;
– игры;
– базы данных;
– текстовые процессоры и т.п.

Компьютерная сеть позволяет работать с многопользовательскими программами, обеспечивающими одновременный доступ всех пользователей к общим базам данных с блокировкой файлов и записей, обеспечивающей целостность данных. Любые программы, разработанные для стандартных ЛВС, можно использовать в других сетях.

Организация электронной почты. Можно использовать ЛВС как почтовую службу и рассылать служебные записки, доклады и сообщения другим пользователям.

1.3. Архитектура сетей

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 два вида архитектур:

1. Одноранговая архитектура;
2. Архитектура клиент-сервер.

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 (рис. 1.3).

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.

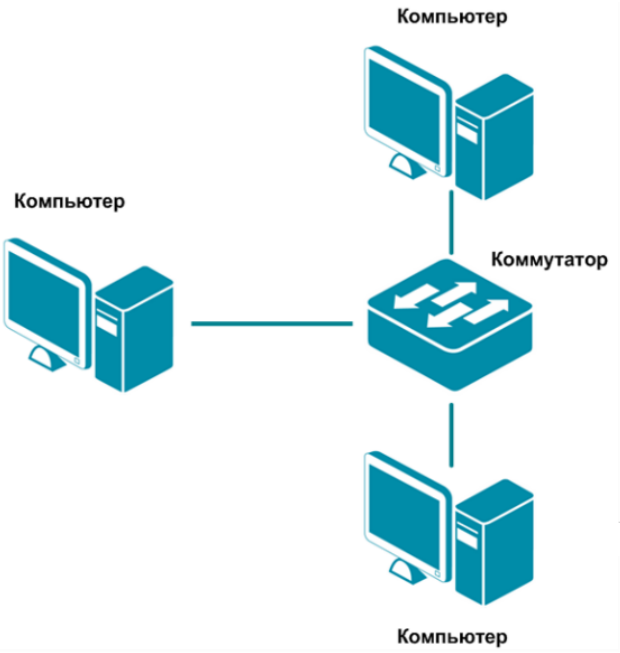

Рисунок 1.3 – Одноранговая архитектура

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. При соединении компьютеров, пользователи могут предоставлять ресурсы и информацию в совместное пользование.

Одноранговые сети имеют следующие преимущества:

– 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. Существенным недостатком одноранговых сетей является отсутствие централизованного администрирования. Использование одноранговой архитектуры не исключает применения в той же сети также архитектуры «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.

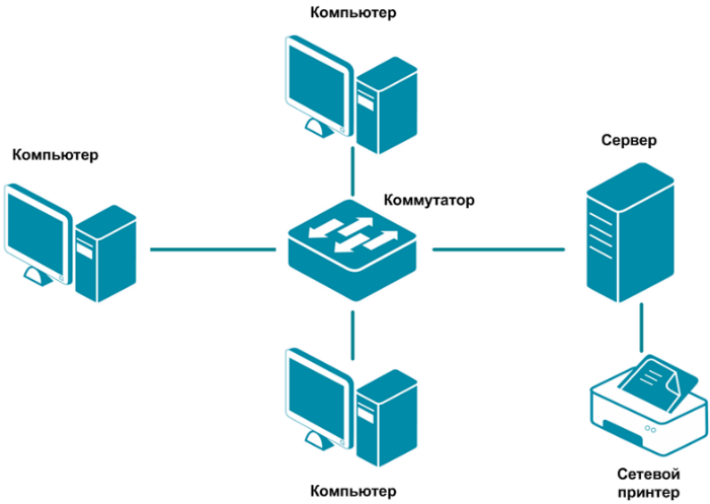

Рисунок 1.4 – Архитектура «Клиент-сервер»

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

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.

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.

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 фирмы Microsoft;

– UNIX фирмы AT&T;

– Linux.

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

Сети на базе серверов имеют лучшие характеристики и повышенную надежность. Сервер владеет 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:

1. Позволяют организовывать сети с большим количеством рабочих станций;

2. Обеспечивают централизованное управление учетными записями пользователей, безопасностью и доступом, что упрощает сетевое администрирование;

3. Эффективный доступ к сетевым ресурсам;

4. 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:

1. Неисправность сервера может сделать сеть неработоспособной, как минимум потерю сетевых ресурсов;

2. Требуют квалифицированного персонала для администрирования;

3. Имеют более высокую стоимость сетей и сетевого оборудования.

1.4. Выбор архитектуры сети

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

Следует выбрать одноранговую сеть, если:

1. Количество пользователей не превышает десяти;
2. Все машины находятся близко друг от друга;
3. Имеют место небольшие финансовые возможности;
4. Нет необходимости в специализированном сервере, таком как сервер БД, факс-сервер или какой-либо другой;
5. Нет возможности или необходимости в централизованном администрировании.

Следует выбрать клиент серверную сеть, если:

1. Количество пользователей превышает десяти;
2. Требуется централизованное управление, безопасность, управление ресурсами или резервное копирование;
3. Необходим специализированный сервер;
4. Нужен доступ к глобальной сети;
5. Требуется разделять ресурсы на уровне пользователей.

Вопросы к разделу 1

1. Дайте определение сети.
2. Чем отличается коммуникационная сеть от информационной?
3. Как разделяются сети по территориальному признаку?
4. Что такое информационная система?
5. Что такое каналы связи?
6. Дайте определение физического канала связи.
7. Дайте определение логического канала связи.

8. Как называется совокупность правил обмена информацией между двумя или несколькими устройствами?

9. Как называется объект, способный осуществлять хранение, обработку или передачу данных, в состав, которого входят компьютер, программное обеспечение, пользователи и др. составляющие, предназначенные для процесса обработки и передачи данных?

10. Каким параметром характеризуется загрузка сети?

11. Что такое метод доступа?

12. Что такое совокупность правил, устанавливающих процедуры и формат обмена информацией?

13. Чем отличается рабочая станция в сети от обычного персонального компьютера?

14. Какие элементы входят в состав сети?

15. Как называется описание физических соединений в сети?

16. Что такое архитектура сети?

17. Как назвать способ определения, какая из рабочих станций сможет следующей использовать канал связи?

18. Перечислить преимущества использования сетей.

19. Чем отличается одноранговая архитектура от клиент серверной архитектуры?

20. Каковы преимущества крупномасштабной сети с выделенным сервером?

21. Какие сервисы предоставляет клиент серверная архитектура?

22. Преимущества и недостатки архитектуры терминал – главный компьютер.

23. В каком случае используется одноранговая архитектура?

24. Что характерно для сетей с выделенным сервером?

25. Как называются рабочие станции, которые используют ресурсы сервера?

26. Что такое сервер?

2. 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 рисунке 2.1 представлена структура базовой модели. Каждый уровень модели OSI 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.

Уровни хост-машины (host layers)	Уровень приложений	7
	Уровень представлений	6
	Сеансовый уровень	5
	Транспортный уровень	4
Уровни среды передачи данных (media layers)	Сетевой уровень	3
	Канальный уровень	2
	Физический уровень	1

Рисунок 2.1 – 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.

2.1. Взаимодействие уровней модели OSI

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

1. Горизонтальную модель на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах;

2. Вертикальную модель на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине.

Рисунок 2.2 – 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 рисунке 2.3.

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.

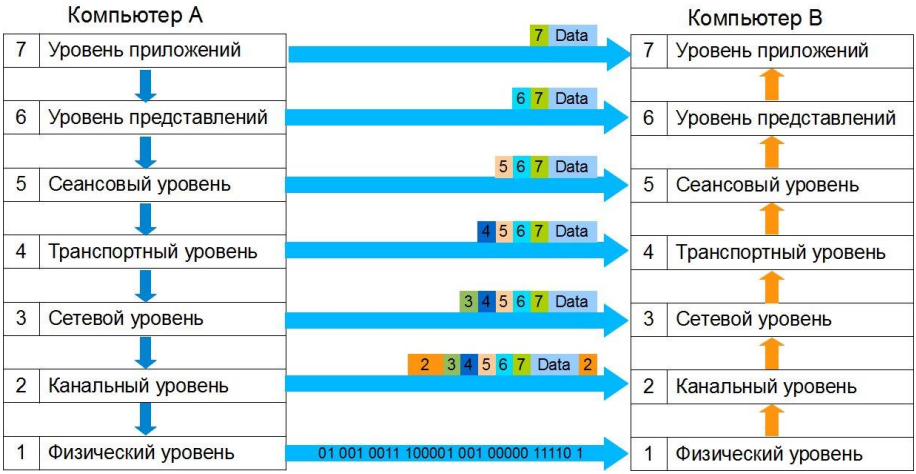

Рисунок 2.3 – Формирование пакета каждого уровня семиуровневой модели

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 одинаково: это требование маршрутизации каких-то данных из одной сети в другую.

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.

В табл. 2.1 приведено краткое описание функций всех уровней.

Таблица 2.1

Функции уровней

№	Уровень	Тип данных	Функции
1	**2**	**3**	**4**
7	Приложений	Пользовательские данные	Предоставление сервисов для сетевых приложений
6	Представлений	Закодированные пользовательские данные	Общий формат представления данных, сжатие и шифрование
5	Сеансовый	Сессии	Установление сессий между приложениями
4	Транспортный	Сегменты	Адресация процессов, сегментация/ повторная сборка данных, управление потоком, надежная доставка
3	Сетевой	Дейтаграммы/пакеты	Передача сообщений между удаленными устройствами, выбор наилучшего маршрута, логическая адресация

Продолжение табл. 2.1

1	2	3	4
2	Канальный	Кадры	Доступ к среде передачи и физическая адресация
1	Физический	Биты	Передача электрических и оптических сигналов между устройствами

2.2. Прикладной уровень (Application layer)

Прикладной уровень обеспечивает прикладным процессам средства доступа к области взаимодействия, является верхним (седьмым) уровнем и непосредственно примыкает к прикладным процессам. В действительности *прикладной уровень – это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам*, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты. Специальные элементы прикладного сервиса обеспечивают сервис для конкретных прикладных программ, таких как программы пересылки файлов и эмуляции терминалов. Если, например, программе необходимо переслать файлы, то обязательно будет использован протокол передачи, доступа и управления файлами FTAM (File Transfer, Access, and Management). В модели OSI прикладная программа, которой нужно выполнить конкретную задачу (например, обновить базу данных на компьютере), посылает конкретные данные в виде *Дейтаграммы* на *прикладной уровень*. Одна из основных задач этого уровня – определить, как следует обрабатывать запрос прикладной программы, другими словами, какой вид должен принять данный запрос.

Единица данных, которой оперирует прикладной уровень, обычно называется сообщением (message).

Прикладной уровень выполняет следующие функции:

– описание форм и методов взаимодействия прикладных процессов;

– передача файлов;

– управление заданиями;

– управление системой и т.д.

– идентификация пользователей по их паролям, адресам, электронным подписям;

– определение функционирующих абонентов и возможности доступа к новым прикладным процессам;

– определение достаточности имеющихся ресурсов;

– организация запросов на соединение с другими прикладными процессами;

– передача заявок представительскому уровню на необходимые методы описания информации;

– выбор процедур планируемого диалога процессов;

– управление данными, которыми обмениваются прикладные процессы и синхронизация взаимодействия прикладных процессов;

– определение качества обслуживания (время доставки блоков данных, допустимой частоты ошибок);

– соглашение об исправлении ошибок и определении достоверности данных;

– согласование ограничений, накладываемых на синтаксис (наборы символов, структура данных).

Указанные функции определяют виды сервиса, которые прикладной уровень предоставляет прикладным процессам. Кроме этого, прикладной уровень передает прикладным процессам сервис, предоставляемый физическим, канальным, сетевым, транспортным, сеансовым и представительским уровнями.

На прикладном уровне необходимо предоставить в распоряжение пользователей уже переработанную информацию. С этим может справиться системное и пользовательское программное обеспечение.

Прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является перенос файлов, обмен почтовыми сообщениями и управление сетью.

К числу наиболее распространенных протоколов верхних трех уровней относятся:

– FTP (File Transfer Protocol) протокол передачи файлов;

– TFTP (Trivial File Transfer Protocol) простейший протокол пересылки файлов;

– X.400 электронная почта;

– Telnet работа с удаленным терминалом;

– SMTP (Simple Mail Transfer Protocol) простой протокол почтового обмена;

– CMIP (Common Management Information Protocol) общий протокол управления информацией;

– SLIP (Serial Line IP) IP для последовательных линий. Протокол последовательной посимвольной передачи данных;

– SNMP (Simple Network Management Protocol) простой протокол сетевого управления;

– FTAM (File Transfer, Access, and Management) протокол передачи, доступа и управления файлами.

2.3. Уровень представления данных (Presentation layer)

Уровень представления данных или представительский уровень представляет данные, передаваемые между прикладными процессами, в нужной форме данные.

Этот уровень обеспечивает то, что информация, передаваемая прикладным уровнем, будет понятна прикладному уровню в другой системе. В случаях необходимости уровень представления в момент передачи информации выполняет преобразование форматов данных в некоторый общий формат представления, а в момент приема, соответственно, выполняет обратное преобразование. Таким образом, прикладные уровни могут преодолеть, например, синтаксические различия в представлении данных. Такая ситуация может возникнуть в ЛВС с неоднотипными компьютерами (IBM PC и Macintosh), которым необходимо обмениваться данными. Так, в полях баз данных информация должна быть представлена в виде букв и цифр, а зачастую и в виде графического изображения. Обрабатывать же эти данные нужно, например, как числа с плавающей запятой.

В основу общего представления данных положена единая для всех уровней модели система ASN.1. Эта система служит для описания структуры файлов, а также позволяет решить проблему шифрования данных. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которым секретность обмена данными обеспечивается сразу для всех

прикладных сервисов. Примером такого протокола является протокол Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP. Этот уровень обеспечивает преобразование данных (кодирование, компрессия и т.п.) прикладного уровня в поток информации для транспортного уровня.

Представительный уровень выполняет следующие основные функции:

– генерация запросов на установление сеансов взаимодействия прикладных процессов;

– согласование представления данных между прикладными процессами;

– реализация форм представления данных;

– представление графического материала (чертежей, рисунков, схем);

– засекречивание данных;

– передача запросов на прекращение сеансов.

Протоколы уровня представления данных обычно являются составной частью протоколов трех верхних уровней модели.

2.4. Сеансовый уровень (Session layer)

Сеансовый уровень – это уровень, определяющий процедуру проведения сеансов между пользователями или прикладными процессами.

Сеансовый уровень обеспечивает управление диалогом для того, чтобы фиксировать, какая из сторон является активной в настоящий момент, а также предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, вместо того чтобы начинать все сначала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется.

Сеансовый уровень управляет передачей информации между прикладными процессами, координирует прием, передачу и выдачу одного сеанса связи. Кроме того, сеансовый уровень

содержит дополнительно функции управления паролями, управления диалогом, синхронизации и отмены связи в сеансе передачи после сбоя вследствие ошибок в нижерасположенных уровнях. Функции этого уровня состоят в координации связи между двумя прикладными программами, работающими на разных рабочих станциях. Это происходит в виде хорошо структурированного диалога. В число этих функций входит создание сеанса, управление передачей и приемом пакетов сообщений во время сеанса и завершение сеанса.

На сеансовом уровне определяется, какой будет передача между двумя прикладными процессами:

1. Полудуплексной (процессы будут передавать и принимать данные по очереди);
2. Дуплексной (процессы будут передавать данные, и принимать их одновременно).

В полудуплексном режиме сеансовый уровень выдает тому процессу, который начинает передачу, маркер данных. Когда второму процессу приходит время отвечать, маркер данных передается ему. Сеансовый уровень разрешает передачу только той стороне, которая обладает маркером данных.

Сеансовый уровень обеспечивает выполнение следующих функций: Установление и завершение на сеансовом уровне соединения между взаимодействующими системами. Выполнение нормального и срочного обмена данными между прикладными процессами. Управление взаимодействием прикладных процессов. Синхронизация сеансовых соединений. Извещение прикладных процессов об исключительных ситуациях. Установление в прикладном процессе меток, позволяющих после отказа либо ошибки восстановить его выполнение от ближайшей метки. Прерывание в нужных случаях прикладного процесса и его корректное возобновление. Прекращение сеанса без потери данных. Передача особых сообщений о ходе проведения сеанса.

Сеансовый уровень отвечает за организацию сеансов обмена данными между оконечными машинами. Протоколы сеансового уровня обычно являются составной частью протоколов трех верхних уровней модели.

2.5. Транспортный уровень (Transport Layer)

Транспортный уровень предназначен для передачи пакетов через коммуникационную сеть. На транспортном уровне пакеты разбиваются на блоки.

На пути от отправителя к получателю пакеты могут быть искажены или утеряны. Хотя некоторые приложения имеют собственные средства обработки ошибок, существуют и такие, которые предпочитают сразу иметь дело с надежным соединением. Работа транспортного уровня заключается в том, чтобы обеспечить приложениям или верхним уровням модели (прикладному и сеансовому) передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем.

Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Транспортный уровень определяет адресацию физических устройств (систем, их частей) в сети. Этот уровень гарантирует доставку блоков информации адресатам и управляет этой доставкой. Его главной задачей является обеспечение эффективных, удобных и надежных форм передачи информации между системами. Когда в процессе обработки находится более одного пакета, транспортный уровень контролирует очередность прохождения пакетов. Если проходит дубликат принятого ранее сообщения, то данный уровень опознает это и игнорирует сообщение.

В функции транспортного уровня входят:

– Управление передачей по сети и обеспечение целостности блоков данных;

– Обнаружение ошибок, частичная их ликвидация и сообщение о неисправленных ошибках;

– Восстановление передачи после отказов и неисправностей;

– Укрупнение или разделение блоков данных;

– Предоставление приоритетов при передаче блоков (нормальная или срочная);

– Подтверждение передачи;

– Ликвидация блоков при тупиковых ситуациях в сети.

Начиная с транспортного уровня, все вышележащие протоколы реализуются программными средствами, обычно включаемыми в состав сетевой операционной системы.

Наиболее распространенные протоколы транспортного уровня включают в себя:

1. TCP (Transmission Control Protocol) протокол управления передачей стека TCP/IP;
2. UDP (User Datagram Protocol) пользовательский протокол дейтаграмм стека TCP/IP;
3. NCP (NetWare Core Protocol) базовый протокол сетей NetWare;
4. SPX (Sequenced Packet eXchange) упорядоченный обмен пакетами стека Novell;
5. TP4 (Transmission Protocol) – протокол передачи класса 4.

2.6. Сетевой уровень (Network Layer)

Сетевой уровень обеспечивает прокладку каналов, соединяющих абонентские и административные системы через коммуникационную сеть, выбор маршрута наиболее быстрого и надежного пути.

Сетевой уровень устанавливает связь в вычислительной сети между двумя системами и обеспечивает прокладку виртуальных каналов между ними. **Виртуальный или логический** канал – это такое функционирование компонентов сети, которое создает взаимодействующим компонентам иллюзию прокладки между ними нужного тракта. Кроме этого, сетевой уровень сообщает транспортному уровню о появляющихся ошибках. Сообщения сетевого уровня принято называть **пакетами** (packet).

В них помещаются фрагменты данных. Сетевой уровень отвечает за их адресацию и доставку.

Прокладка наилучшего пути для передачи данных называется маршрутизацией, и ее решение является главной задачей сетевого уровня. Эта проблема осложняется тем, что самый короткий путь не всегда самый лучший. Часто критерием при выборе маршрута является время передачи данных по этому маршруту; оно зависит от пропускной способности каналов связи и интенсивности трафика, которая может изменяться с течением времени. Некоторые алгоритмы маршрутизации пытаются приспособиться к изменению нагрузки, в то время как другие принимают решения на основе средних показателей за длительное время. Выбор маршрута может осуществляться и по другим критериям, например, надежности передачи.

Протокол канального уровня обеспечивает доставку данных между любыми узлами только в сети с соответствующей типовой топологией. Это очень жесткое ограничение, которое не позволяет строить сети с развитой структурой, например, сети, объединяющие несколько сетей предприятия в единую сеть, или высоконадежные сети, в которых существуют избыточные связи между узлами.

Таким образом, внутри сети доставка данных регулируется канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень. При организации доставки пакетов на сетевом уровне используется понятие номер сети. В этом случае адрес получателя состоит из номера сети и номера компьютера в этой сети.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. **Маршрутизатор** – это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения. Для того чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач (hops) между сетями, каждый раз, выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, по которым проходит пакет.

Сетевой уровень отвечает за деление пользователей на группы и маршрутизацию пакетов на основе преобразования MAC-адресов в сетевые адреса. Сетевой уровень обеспечивает также прозрачную передачу пакетов на транспортный уровень.

Сетевой уровень выполняет функции:

1. Создание сетевых соединений и идентификация их портов.
2. Обнаружение и исправление ошибок, возникающих при передаче через сеть.
3. Управление потоками пакетов.
4. Организация (упорядочение) последовательностей пакетов.
5. Маршрутизация и коммутация.
6. Сегментирование и объединение пакетов.

На сетевом уровне определяется два вида протоколов. Первый вид относится к определению правил передачи пакетов с данными конечных узлов от узла к маршрутизатору и между маршрутизаторами. Именно эти протоколы обычно имеют в виду, когда говорят о протоколах сетевого уровня. Однако часто к сетевому уровню относят и другой вид протоколов, называемых протоколами обмена маршрутной информацией. С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений.

Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

Наиболее часто на сетевом уровне используются протоколы:

1. IP (Internet Protocol) протокол Internet, сетевой протокол стека TCP/IP, который предоставляет адресную и маршрутную информацию;
2. IPX (Internetwork Packet Exchange) протокол межсетевого обмена пакетами, предназначенный для адресации и маршрутизации пакетов в сетях Novell;
3. X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов (частично этот протокол реализован на уровне 2);

4. CLNP (Connection Less Network Protocol) сетевой протокол без организации соединений.

2.7. Канальный уровень (Data Link)

Единицей информации канального уровня являются кадры (frame). **Кадры** – это логически организованная структура, в которую можно помещать данные. Задача канального уровня передавать кадры от сетевого уровня к физическому уровню.

На физическом уровне просто пересылаются биты. При этом не учитывается, что в некоторых сетях, в которых линии связи используются попеременно несколькими парами взаимодействующих компьютеров, физическая среда передачи может быть занята. Поэтому одной из задач канального уровня является проверка доступности среды передачи. Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок.

Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность бит, в начало и конец каждого кадра, чтобы отметить его, а также вычисляет контрольную сумму, суммируя все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит, получатель снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется ошибка.

Задача канального уровня – брать пакеты, поступающие с сетевого уровня и готовить их к передаче, укладывая в кадр соответствующего размера. Этот уровень обязан определить, где начинается и где заканчивается блок, а также обнаруживать ошибки передачи.

На этом же уровне определяются правила использования физического уровня узлами сети. Электрическое представление данных в ЛВС (биты данных, методы кодирования данных и маркеры) распознаются на этом и только на этом уровне. Здесь

обнаруживаются и исправляются (путем требований повторной передачи данных) ошибки.

Канальный уровень обеспечивает создание, передачу и прием кадров данных. Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов. Спецификации IEEE 802.X делят канальный уровень на два подуровня: LLC (Logical Link Control) управление логическим каналом осуществляет логический контроль связи. Подуровень LLC обеспечивает обслуживание сетевого уровня и связан с передачей и приемом пользовательских сообщений. MAC (Media Assess Control) контроль доступа к среде. Подуровень MAC регулирует доступ к разделяемой физической среде (передача маркера, или обнаружение коллизий, или столкновений) и управляет доступом к каналу связи. Подуровень LLC находится выше подуровня MAC.

Канальный уровень определяет доступ к среде и управление передачей посредством процедуры передачи данных по каналу. При больших размерах передаваемых блоков данных канальный уровень делит их на кадры и передает кадры в виде последовательностей. При получении кадров уровень формирует из них переданные блоки данных. Размер блока данных зависит от способа передачи, качества канала, по которому он передается.

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.

Канальный уровень может выполнять следующие виды функций:

1. Организация (установление, управление, расторжение) канальных соединений и идентификация их портов.
2. Организация и передача кадров.
3. Обнаружение и исправление ошибок.
4. Управление потоками данных.
5. Обеспечение прозрачности логических каналов (передачи по ним данных, закодированных любым способом).

Наиболее часто используемые протоколы на канальном уровне включают:

1. HDLC (High Level Data Link Control) протокол управления каналом передачи данных высокого уровня, для последовательных соединений;

2. IEEE 802.2 LLC (тип I и тип II) обеспечивают MAC для сред 802.x;

3. Ethernet сетевая технология по стандарту IEEE 802.3 для сетей, использующая шинную топологию и коллективный доступ с прослушиванием несущей и обнаружением конфликтов;

4. Token ring сетевая технология по стандарту IEEE 802.5, использующая кольцевую топологию и метод доступа к кольцу с передачей маркера;

5. FDDI (Fiber Distributed Date Interface Station) сетевая технология по стандарту IEEE 802.6, использующая оптоволоконный носитель;

6. X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов;

7. Frame relay сеть, организованная из технологий X25 и ISDN.

2.8. Физический уровень (Physical Layer)

Физический уровень предназначен для сопряжения с физическими средствами соединения. **Физические средства соединения** – это совокупность физической среды, аппаратных и программных средств, обеспечивающая передачу сигналов между системами. **Физическая среда** – это материальная субстанция, через которую осуществляется передача сигналов. Физическая среда является основой, на которой строятся физические средства соединения. В качестве физической среды широко используются эфир, металлы, оптическое стекло и кварц.

Физический уровень состоит из *Подуровня стыковки со средой* и *Подуровня преобразования передач*и.

Первый из них обеспечивает сопряжение потока данных с используемым физическим каналом связи. Второй осуществляет преобразования, связанные с применяемыми протоколами. Физический уровень обеспечивает физический интерфейс с каналом передачи данных, а также описывает процедуры передачи сигналов в канал и получения их из канала. На этом уровне

определяются электрические, механические, функциональные и процедурные параметры для физической связи в системах. Физический уровень получает пакеты данных от вышележащего канального уровня и преобразует их в оптические или электрические сигналы, соответствующие 0 и 1 бинарного потока. Эти сигналы посылаются через среду передачи на приемный узел. Механические и электрические/оптические свойства среды передачи определяются на физическом уровне и включают:

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

Физический уровень выполняет следующие функции:

1. Установление и разъединение физических соединений.
2. Передача сигналов в последовательном коде и прием.
3. Прослушивание, в нужных случаях, каналов.
4. Идентификация каналов.
5. Оповещение о появлении неисправностей и отказов.

Оповещение о появлении неисправностей и отказов связано с тем, что на физическом уровне происходит обнаружение определенного класса событий, мешающих нормальной работе сети (столкновение кадров, посланных сразу несколькими системами, обрыв канала, отключение питания, потеря механического контакта и т.д.). Виды сервиса, предоставляемого канальному уровню, определяются протоколами физического уровня. Прослушивание канала необходимо в тех случаях, когда к одному каналу подключается группа систем, но одновременно передавать сигналы разрешается только одной из них. Поэтому прослушивание канала позволяет определить, свободен ли он для передачи. В ряде случаев для более четкого определения структуры физический уровень разбивается на несколько подуровней.

Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером. Повторители являются единственным типом оборудования, которое работает только на физическом уровне.

Выполняется преобразование данных, поступающих от более высокого уровня, в сигналы, передающие по кабелю. В глобальных сетях на этом уровне могут использоваться модемы и

интерфейс RS-232C. В локальных сетях для преобразования данных применяют сетевые адаптеры, обеспечивающие скоростную передачу данных в цифровой форме. Пример протокола физического уровня – это широко известный интерфейс RS-232C/CCITT V.2, который является наиболее широко распространенной стандартной последовательной связью между компьютерами и периферийными устройствами.

Можно считать этот уровень отвечающим за аппаратное обеспечение.

Физический уровень может обеспечивать как асинхронную (последовательную), так и синхронную (параллельную) передачу, которая применяется для некоторых мэйнфреймов и мини-компьютеров. На физическом уровне должна быть определена схема кодирования для представления двоичных значений с целью их передачи по каналу связи. Во многих локальных сетях используется манчестерское кодирование.

Примером протокола физического уровня может служить спецификация 10Base-T технологии Ethernet, которая определяет в качестве используемого кабеля неэкранированную витую пару категории 3 с волновым сопротивлением 100 Ом, разъем RJ-45, максимальную длину физического сегмента 100 метров, манчестерский код для представления данных на кабеле, и другие характеристики среды и электрических сигналов.

К числу наиболее распространенных спецификаций физического уровня относятся:

– EIA-RS-232-C, CCITT V.24/V.28 – механические/электрические характеристики несбалансированного последовательного интерфейса;

– EIA-RS-422/449, CCITT V.10 – механические, электрические и оптические характеристики сбалансированного последовательного интерфейса;

– Ethernet – сетевая технология по стандарту IEEE 802.3 для сетей, использующая шинную топологию и коллективный доступ с прослушиванием несущей и обнаружением конфликтов;

– Token ring – сетевая технология по стандарту IEEE 802.5, использующая кольцевую топологию и метод доступа к кольцу с передачей маркера.

2.9. Сетезависимые протоколы

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

Три нижних уровня: физический, канальный и сетевой являются сетезависимыми, т.к. протоколы этих уровней тесно связаны с технической реализацией сети, с используемым коммуникационным оборудованием. Например, переход на оборудование FDDI означает смену протоколов физического и канального уровня во всех узлах сети.

Три верхних уровня сеансовый, уровень представления и прикладной ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют никакие изменения в топологии сети, замена оборудования или переход на другую сетевую технологию. Так, переход от Ethernet на высокоскоростную технологию 100VG-AnyLAN не потребует никаких изменений в программных средствах, реализующих функции прикладного, представительного и сеансового уровней.

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних уровней. Это позволяет разрабатывать приложения, не зависящие от технических средств, непосредственно занимающихся транспортировкой сообщений.

Одна рабочая станция взаимодействует с другой рабочей станцией посредством протоколов всех семи уровней. Это взаимодействие станции осуществляют через различные коммуникационные устройства: концентраторы, модемы, мосты, коммутаторы, маршрутизаторы, мультиплексоры. В зависимости от типа коммуникационное устройство может работать:

– либо только на физическом уровне (повторитель);

– либо на физическом и канальном уровнях (мост);

– либо на физическом, канальном и сетевом уровнях, иногда захватывая и транспортный уровень (маршрутизатор).

Модель OSI представляет собой хотя и очень важную, но только одну из многих моделей коммуникаций. Эти модели и

связанные с ними стеки протоколов могут отличаться количеством уровней, их функциями, форматами сообщений, сервисами, предоставляемыми на верхних уровнях, и прочими параметрами.

2.10. Стеки коммуникационных протоколов

Иерархически организованная совокупность протоколов, решающих задачу взаимодействия узлов сети, называется **стеком коммуникационных протоколов**.

Протоколы соседних уровней, находящихся в одном узле, взаимодействуют друг с другом также в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть **интерфейсом**. Интерфейс определяет набор услуг, которые нижележащий уровень предоставляет вышележащему уровню.

Вопросы к разделу 2

1. Что такое OSI?
2. Каково назначение базовой модели взаимодействия открытых систем?
3. На какие уровни разбита базовая модель OSI?
4. Какие функции несет уровень в модели взаимодействия открытых систем?
5. На какие единицы разбивается информация для передачи данных по сети?
6. Что обеспечивает горизонтальная составляющая модели взаимодействия открытых систем?
7. Какие элементы являются основными элементами для базовой модели взаимодействия открытых систем?
8. Какие функции выполняются на физическом уровне?
9. Какие вопросы решаются на физическом уровне?
10. Какой уровень модели OSI преобразует данные в общий формат для передачи по сети?
11. Какое оборудование используется на физическом уровне?
12. Какие известны спецификации физического уровня?

13. Перечислить функции канального уровня.
14. Какие функции канального уровня?
15. На какие подуровни разделяется канальный уровень и каковы их функции?
16. Функцией какого уровня является засекречивание и реализация форм представления данных?
17. Какие протоколы используются на канальном уровне?
18. Какое оборудование используется на канальном уровне?
19. Какие функции выполняются и какие протоколы используются на сетевом уровне?
20. Какое оборудование используется на сетевом уровне?
21. Перечислить функции транспортного уровня.
22. Какие протоколы используются на транспортном уровне?
23. Перечислить оборудование транспортного уровня.
24. Дайте определение сеансового уровня.
25. Какой уровень отвечает за доступ приложений в сеть?
26. Задачи уровня представления данных.
27. Перечислить функции прикладного уровня.
28. Перечислить протоколы верхних уровней.
29. Дайте определение стандартных стеков коммуникационных протоколов.

3. СТАНДАРТЫ И СТЕКИ ПРОТОКОЛОВ

3.1. Спецификации стандартов

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:

1. Logical Link Control (LLC) – подуровень управления логической связью;

2. Media Access Control (MAC) – подуровень управления доступом к устройствам.

Спецификации IEEE 802 делятся на двенадцать стандартов:

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.

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.

Стандарт 802.3 (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 4B/5B по витой паре, а также имеется функция автопереговоров (Auto-negotiation) для выбора режима работы порта.

100Base-T4 – четырехпарная витая пара. Вместо кодирования 4B/5B 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.

Стандарт 802.4 (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:

1. Все устройства, подключённые к сети, могут передавать данные, только получив разрешение на передачу (маркер);
2. В любой момент времени только одна станция в сети обладает таким правом;
3. 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 (In- formation Symbol Unit – единица передачи информации), состоящей из трёх служебных старт/стоповых битов и восьми битов данных.

Стандарт 802.5 (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.

Стандарт 802.6 (Metropolitan Area Network – городские сети) описывает рекомендации для региональных сетей.

Стандарт 802.7 (Broadband Technical Advisory Group – техническая консультационная группа по широковещательной передаче) описывает рекомендации по широкополосным сетевым технологиям, носителям, интерфейсу и оборудованию.

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.

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.

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

Стандарт 802.11 (Wireless Network – беспроводные сети) описывает рекомендации по использованию беспроводных сетей.

Стандарт 802.12 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/с, 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.

3.2. Протоколы и стеки протоколов

Согласованный набор протоколов разных уровней, достаточный для организации межсетевого взаимодействия, называется **стеком протоколов**. Для каждого уровня определяется набор функций– запросов для взаимодействия с вышележащим 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:

1. Сетевые;
2. Транспортные;
3. Прикладные.

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 Ap- ple 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 предоставляют следующие услуги надежной транспортировки данных между компьютерами. Ниже приведены наиболее популярные транспортные протоколы.

1. ATP (Apple Talk Protocol – Транзакционный протокол Apple Talk) и NBP (Name Binding Protocol – Протокол связывания имен). Сеансовый и транспортный протоколы Apple Talk.

2. NetBIOS (Базовая сетевая система ввода вывода). NetBIOS устанавливает соединение между компьютерами, а NetBEUI предоставляет услуги передачи данных для этого соединения.

3. SPX (Sequenced Packet eXchange – Последовательный обмен пакетами) в NWLink. Протокол Novel NetWare, используемый для обеспечения доставки данных.

4. TCP (Transmission Control Protocol – Протокол управления передачей). Протокол стека TCP/IP, отвечающий за надежную доставку данных.

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 для управления и наблюдения за сетевыми устройствами.

HTTP (Hyper Text Transfer Protocol) – протокол передачи гипертекста и другие протоколы.

3.3. Стек OSI

Следует различать стек протоколов OSI и модель OSI (рис. 3.1). **Стек OSI** – это набор вполне конкретных спецификаций протоколов, образующих согласованный стек протоколов. Этот стек протоколов поддерживает правительство США в своей программе GOSIP. Стек OSI в отличие от других стандартных стеков полностью соответствует модели взаимодействия OSI и включает спецификации для всех семи уровней модели взаимодействия открытых систем.

Распределение протоколов по уровням модели OSI		
7	**Прикладной**	напр., HTTP, SMTP, SNMP, FTP, Telnet, SSH, SCP, SMB, NFS, RTSP, BGP
6	**Представления**	напр., XDR, AFP, TLS, SSL
5	**Сеансовый**	напр., ISO 8327 / CCITT X.225, RPC, NetBIOS, PPTP, L2TP, ASP
4	**Транспортный**	напр., TCP, UDP, SCTP, SPX, RTP, ATP, DCCP, GRE
3	**Сетевой**	напр., IP, ICMP, IGMP, CLNP, OSPF, RIP, IPX, DDP, ARP, RARP
2	**Канальный**	напр., Ethernet, Token ring, HDLC, PPP, X.25, Frame relay, ISDN, ATM, MPLS
1	**Физический**	напр., электрические провода, радиосвязь, волоконно-оптические провода, Wi-Fi

Рисунок 3.1 – Стек OSI

На *физическом* и *канальном* уровнях стек OSI поддерживает спецификации Ethernet, Token Ring, FDDI, а также протоколы LLC, X.25 и ISDN.

На *сетевом* уровне реализованы протоколы, как без установления соединений, так и с установлением соединений.

Транспортный протокол стека OSI скрывает различия между сетевыми сервисами с установлением соединения и без установления соединения, так что пользователи получают нужное качество обслуживания независимо от нижележащего сетевого уровня. Чтобы обеспечить это, транспортный уровень требует, чтобы пользователь задал нужное качество обслуживания. Определены 5 классов транспортного сервиса, от низшего класса 0 до высшего класса 4, которые отличаются степенью устойчивости к ошибкам и требованиями к восстановлению данных после ошибок.

Сервисы *прикладного* уровня включают передачу файлов, эмуляцию терминала, службу каталогов и почту. Из них наиболее перспективными являются служба каталогов (стандарт X.500), электронная почта (X.400), протокол виртуального терминала (VT), протокол передачи, доступа и управления файлами (FTAM), протокол пересылки и управления работами (JTM). В последнее время ISO сконцентрировала свои усилия именно на сервисах верхнего уровня.

3.4. Архитектура стека протоколов Microsoft TCP/IP

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.

Реализация TCP/IP фирмы Microsoft соответствует четырехуровневой модели вместо семиуровневой модели, как показано на рис. 3.2. Модель TCP/IP включает большее число функций на один уровень, что приводит к уменьшению числа уровней. В модели используются следующие уровни:

1. *Уровень Приложения* модели TCP/IP соответствует уровням *Приложения, Представления* и *Сеанса* модели OSI;

2. *Уровень Транспорта* модели TCP/IP соответствует аналогичному уровню *Транспорта* модели OSI;

3. *Межсетевой уровень* модели TCP/IP выполняет те же функции, что и *уровень Сети* модели OSI;

4. *Уровень сетевого интерфейса* модели TCP/IP соответствует *Канальному* и *Физическому* уровням модели OSI.

Через уровень Приложения модели TCP/IP приложения и службы получают доступ к сети.

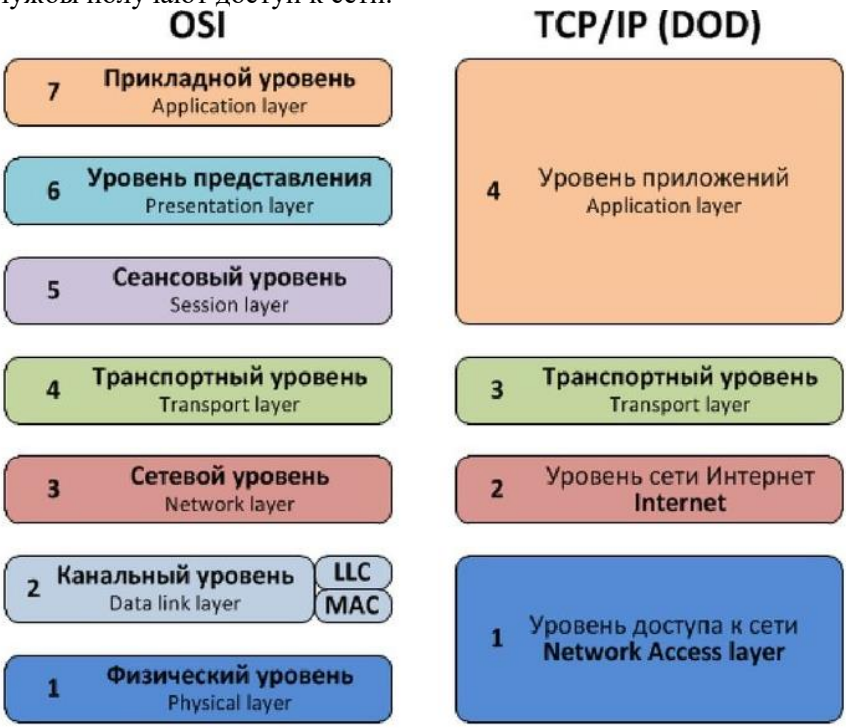

Рисунок 3.2 – Соответствие семиуровневой модели OSI и четырехуровневой модели TCP/IP

Доступ к протоколам TCP/IP осуществляется посредством двух программных интерфейсов (API – Application Programming Interface):

– 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 табл. 3.1 приведено семейство протоколов TCP/IP.

Таблица 3.1

Семейство протоколов TCP/IP

Протокол	**Описание протокола**
WinSock	Сетевой программный интерфейс
NetBIOS	Связь с приложениями ОС Windows
TDI	Интерфейс транспортного драйвера (Transport DriverInterface) 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)

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

1. Подтверждение получения информации;
2. Управление потоком данных;

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

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 передаче не произошло ошибок.

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 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 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.

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 MAC-адрес сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей MAC-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.

Для определения локального адреса по IP-адресу используется протокол разрешения адреса Address Resolution Protocol (ARP). ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети – протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети, или же протокол глобальной сети (X.25, frame relay), как правило, не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу – нахождение IP-адреса по известному локальному адресу. Он называется реверсивный ARP – RARP (Reverse Address Resolution Protocol) и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

В локальных сетях ARP использует широковещательные кадры протокола канального уровня для поиска в сети узла с заданным IP- адресом. Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня,

указывая в нем известный IP-адрес, и рассылает запрос широковещательно. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным адресом. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP-запросе отправитель указывает свой локальный адрес. ARP-запросы и ответы используют один и тот же формат пакета.

Протокол управления сообщениями Интернета (ICMP – Internet Control Message Protocol) используется IP и другими протоколами высокого уровня для отправки и получения отчетов о состоянии переданной информации. Этот протокол используется для контроля скорости передачи информации между двумя системами. Если маршрутизатор, соединяющий две системы, перегружен трафиком, он может отправить специальное сообщение ICMP – ошибку для уменьшения скорости отправления сообщений.

Узлы локальной сети используют протокол управления группами Интернета (IGMP – Internet Group Management Protocol), чтобы зарегистрировать себя в группе. Информация о группах содержится на маршрутизаторах локальной сети. Маршрутизаторы используют эту информацию для передачи групповых сообщений.

Групповое сообщение, как и широковещательное, используется для отправки данных сразу нескольким узлам.

Network Device Interface Specification – спецификация интерфейса сетевого устройства, программный интерфейс, обеспечивающий взаимодействие между драйверами транспортных протоколов, и соответствующими драйверами сетевых интерфейсов. Позволяет использовать несколько протоколов, даже если установлена только одна сетевая карта.

Этот уровень модели TCP/IP отвечает за распределение IP-дейтаграмм. Он работает с ARP для определения информации, которая должна быть помещена в заголовок каждого кадра. Затем на этом уровне создается кадр, подходящий для используемого типа сети, такого как Ethernet, Token Ring или ATM, затем IP-дейтаграмма помещается в область данных этого кадра, и он отправляется в сеть.

Вопросы к разделу 3

1. Назначение спецификации стандартов IEEE802.
2. Какой стандарт описывает сетевую технологию Ethernet?
3. Какой стандарт определяет задачи управления логической связью?
4. Какой стандарт задает механизмы управления сетью?
5. Какой стандарт описывает сетевую технологию ArcNet?
6. Какой стандарт описывает сетевую технологию Token Ring?
7. Какой стандарт содержит рекомендации по оптоволоконным сетевым технологиям?
8. Что такое интерфейс уровня базовой модели OSI?
9. Что такое протокол уровня базовой модели OSI?
10. Дайте определение стека протоколов.
11. На какие уровни разбиваются стеки протоколов?
12. Назвать наиболее популярные сетевые протоколы.
13. Назвать наиболее популярные транспортные протоколы.
14. Назвать наиболее популярные прикладные протоколы.
15. Перечислить наиболее популярные стеки протоколов.
16. Назначение программных интерфейсов сокетов Windows и NetBIOS.
17. Чем отличается протокол TCP от UDP?
18. Функции протокола IP.
19. Какие существуют виды адресации в IP-сетях?
20. Какой протокол необходим для определения локального адреса по IP-адресу?
21. Какой протокол необходим для определения IP-адреса по локальному адресу?
22. Какой протокол используется для управления сообщениями Интернета?
23. Назначение уровня сетевого интерфейса стека TCP/IP.

4. ТОПОЛОГИЯ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ И МЕТОДЫ ДОСТУПА

4.1. Топология вычислительной сети

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:

1. Обеспечение альтернативной маршрутизации и максимальной надежности передачи данных;
2. Выбор оптимального маршрута передачи блоков данных;
3. 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.

4.2. Виды топологий

Существуют пять основных топологий:
– общая шина (Bus);
– кольцо (Ring);
– звезда (Star);
– древовидная (Tree);

Общая шина – это тип сетевой топологии, в которой рабочие станции расположены вдоль одного участка кабеля, называемого сегментом (рис. 4.1).

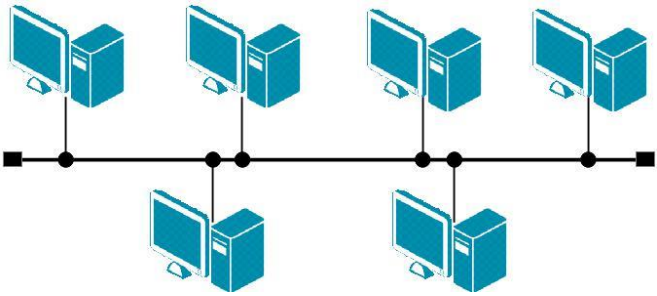

Рисунок 4.1 – Топология Общая шина

Топология Общая шина 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 – это топология ЛВС, в которой каждая станция соединена с двумя другими станциями, образуя кольцо (рис. 4.2). 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, Топология Кольцо имеет хорошо предсказуемое время отклика, определяемое числом рабочих станций.

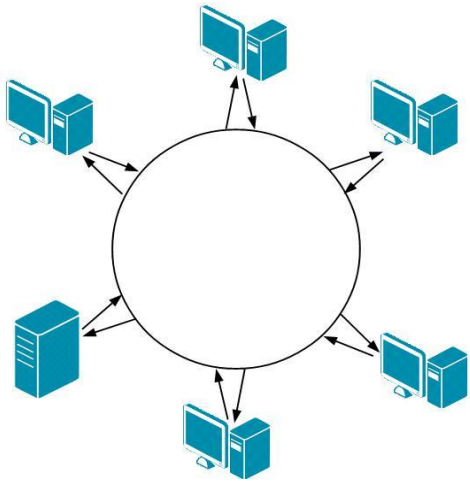

Рисунок 4.2 – Топология Кольцо

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 – это топология ЛВС (рис. 4.3), 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.

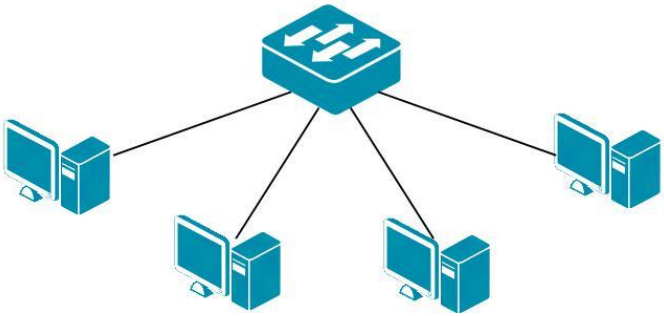

Рисунок 4.3 – Топология Звезда

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. 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. 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.

Топология «дерево» или «расширенная звезда» создается на основе комбинации топологий «звезда» и линейного подключения (рис. 4.4).

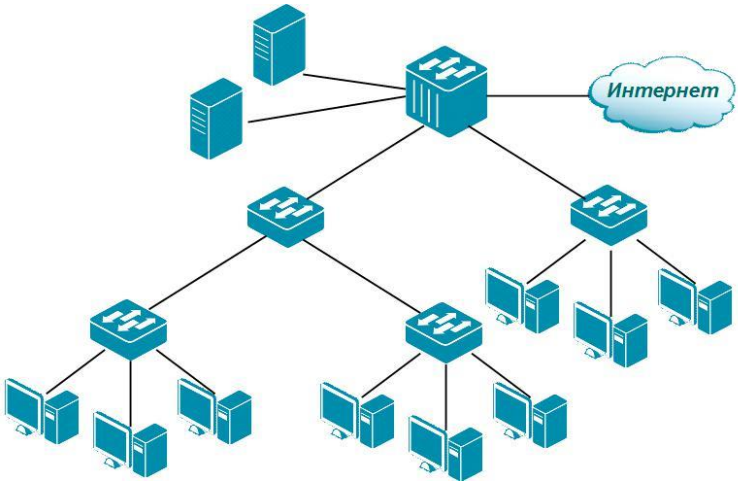

Рисунок 4.4 – Топология «Дерево»

К достоинствам данной топологии можно отнести то, что сеть с данной топологией легко увеличить и легко её контролировать (поиск обрывов и неисправностей). Недостатками является то, что при выходе из строя родительского узла, выйдут из строя и все его дочерние узлы (выход из строя корня — выход из строя всей сети), и также ограничена пропускная способность (доступ к сети может быть затруднён).

4.3. Методы доступа

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 Divi- sion Multiple Access – FDMA) или множественный доступ с разделением длины волны (Wavelength Division Multiple Access – WDMA).

Алгоритм CSMA/CD множественного доступа с прослушиванием несущей и разрешением коллизий приведен на рисунке 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.

Рисунок 4.5 – Алгоритм CSMA/CD

Все сетевые интерфейсные платы запрограммированы на разные псевдослучайные промежутки времени. Стандарт типа Ethernet определяет сеть с конкуренцией, в которой несколько рабочих станций должны конкурировать друг с другом за право доступа к сети.

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

Рисунок 4.6 – Алгоритм ТРМА

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.

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:

1. Гарантирует определенное время доставки блоков данных в сети;
2. Дает возможность предоставления различных приоритетов передачи данных.

Вместе с тем он имеет существенные недостатки:

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

Доступ FDMA основан на разделении полосы пропускания канала на группу полос частот (рис. 4.7), 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.

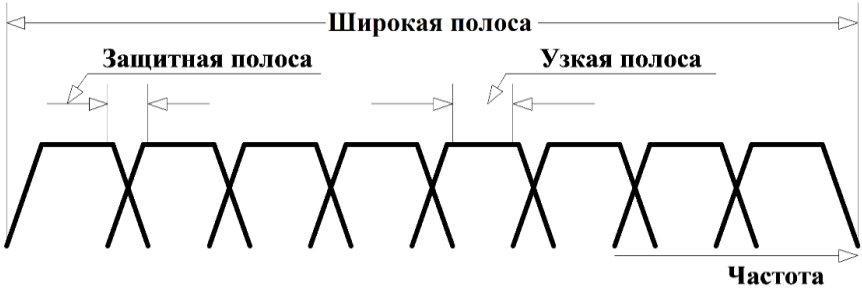

Рисунок 4.7 – Схема выделения логических каналов

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.

Вопросы к разделу 4

1. Что такое топология?
2. Перечислить наиболее используемые типы топологий?
3. Охарактеризовать топологию Общая шина и привести примеры использования данной топологии.
4. Какие сетевые технологии используют топологию Общая шина?

5. Охарактеризовать топологию Кольцо и привести примеры этой топологии.

6. В каких случаях используют топологию Кольцо?

7. Охарактеризовать топологию Звезда и привести примеры использования этой топологии.

8. К какой топологии относится сеть при подсоединении всех компьютеров к общему концентратору?

9. Привести примеры и охарактеризовать древовидную топологию.

10. Что такое ячеистая топология и в каких случаях она используется?

11. Что такое метод доступа и как влияет метод доступа на передачу данных в сети?

12. Какие существуют методы доступа?

13. Охарактеризовать метод доступа с прослушиванием несущей и разрешением коллизий.

14. При каком методе доступа обе станции могут одновременно начать передачу и войти в конфликт?

15. В каких сетевых технологиях используется метод CSMA/CD?

16. Охарактеризовать метод доступа с разделением во времени и перечислить в каких случаях используется данный метод.

17. Что такое маркер?

18. В каком случае рабочая станция может начать передачу данных при использовании метода доступа с передачей полномочия?

19. Охарактеризовать метод доступа с передачей полномочия.

20. Охарактеризовать метод множественного доступа с разделением частоты.

21. Какие существуют варианты использования множественного доступа с разделением во времени?

5. ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ И ИХ КОМПОНЕНТЫ

5.1. Основные 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:

Абонентские системы:

– компьютеры (рабочие станции или клиенты и серверы);

– принтеры;

– сканеры и др.

Сетевое оборудование:

– сетевые адаптеры;

– концентраторы (хабы);

– мосты;

– маршрутизаторы и др.

Коммуникационные каналы:

– кабели;

– разъемы;

– устройства передачи и приема данных в беспроводных технологиях.

Основными ***программными компонентами*** сети являются следующие сетевые **операционные системы**:

– Windows;

– LANtastic;

– NetWare;

– Unix;

– Linux и т.д.

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.

5.2. Рабочие станции

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.

5.3. Сетевые адаптеры

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.

5.4. Файловые серверы

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:

1. Первичный контроллер домена, сервер, на котором хранится база бюджетов пользователей и поддерживается политика защиты.
2. Вторичный контроллер домена, сервер, на котором хранится резервная копия базы бюджетов пользователей и политики защиты.

3. Универсальный сервер, предназначенный для выполнения несложного набора различных задач обработки данных в локальной сети.

4. Сервер базы данных, выполняющий обработку запросов, направляемых базе данных.

5. Proxy сервер, подключающий локальную сеть к сети Internet.

6. Web-сервер, предназначенный для работы с web-информацией.

7. Файловый сервер, обеспечивающий функционирование распределенных ресурсов, включая файлы, программное обеспечение.

8. 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.

9. Сервер удаленного доступа, обеспечивающий сотрудникам, работающим дома торговым агентам, служащим филиалов, лицам, находящимся в командировках, возможность работы с данными сети.

10. 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.

11. Почтовый сервер, предоставляющий сервис в ответ на запросы, присланные по электронной почте.

12. 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.

13. Терминальный сервер, объединяющий группу терминалов, упрощающий переключения при их перемещении.

14. Коммуникационный сервер, выполняющий функции терминального сервера, но осуществляющий также маршрутизацию данных.

15. Видеосервер, который в наибольшей степени приспособлен к обработке изображений, снабжает пользователей видеоматериалами, обучающими программами, видеоиграми, обеспечивает электронный маркетинг. Имеет высокую производительность и большую память.

16. Факс-сервер, обеспечивающий передачу и прием сообщений в стандартах факсимильной связи.

17. Сервер защиты данных, оснащенный широким набором средств обеспечения безопасности данных и, в первую очередь, идентификации паролей.

5.5. Сетевые операционные системы

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 также сетевая 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. Она является прикладной платформой, предоставляет разнообразные виды сетевых служб и поддерживает работу прикладных процессов, реализуемых в сетях. NOS используют архитектуру клиент–сервер или одноранговую архитектуру.

NOS определяет группу протоколов, обеспечивающих основные функции сети. К ним относятся: адресация объектов сети; функционирование сетевых служб; обеспечение безопасности данных; управление сетью.

5.6. Сетевое программное обеспечение

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.

5.7. Защита данных

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

1. Необходимость обеспечения гарантии от разрушений.

2. Необходимость защиты конфиденциальности. Далеко не всегда есть желание, чтобы частная информация была доступна всем;

3. Необходимость защиты от мошенничества. Некоторые расчетные ведомости несут в себе большие денежные суммы, и бывает, пользователи поддаются искушению выписать чек на свое имя.

4. Необходимость защиты от преднамеренных разрушений. В некоторых случаях раздосадованный работник может испортить какую-нибудь информацию.

5.8. Использование паролей и ограничение доступа

Первый шаг к безопасности – это введение пароля. Каждому пользователю ЛВС присваивается пароль – секретное слово, известное только этому пользователю. При вводе пароля высвечиваются звездочки. Сетевая операционная система хранит информацию по всем именам и паролям (в закодированной форме), а также о правах доступа к директориям и другие атрибуты пользователей.

Еще одна возможность защиты данных заключается в ограничении доступа к определенным директориям или определенным серверам. Доступ к дискам рабочих станций выбирается посредством вкладки Управление доступом в программе Сетевое окружение. Доступ между серверами организуется посредством установки доверительных отношений между серверами.

5.9. Типовой состав оборудования локальной сети

Фрагмент вычислительной сети включает основные типы коммуникационного оборудования, применяемого сегодня для образования локальных сетей и соединения их через глобальные связи друг с другом (рис. 5.1).

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 (ТА – терминальные адаптеры сетей ISDN, устройства обслуживания цифровых выделенных каналов типа CSU/DSU и т.п.).

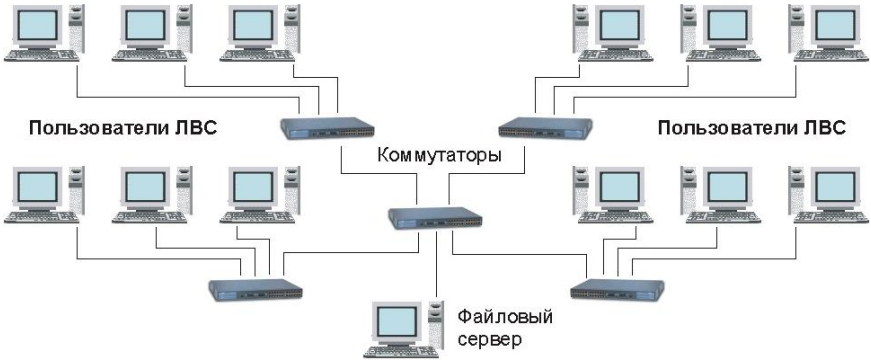

Рисунок 5.1 – Фрагмент сети

Вопросы к разделу 5

1. Перечислите основные компоненты сети.
2. Чем отличается рабочая станция в сети от локального компьютера?
3. Что такое файловый сервер? Какие бывают файловые серверы?
4. Каково назначение первичного контролера домена в сети? Для чего используется вторичный контролера домена?
5. Что такое Proxy-сервер?
6. Какая информация хранится на сервере баз данных?
7. Может ли сервер баз данных и Web-сервер размещаться на одном компьютере?
8. Перечислить сетевое программное обеспечение рабочей станции.
9. Какое назначение СОС?
10. Перечислить наиболее известные сетевые операционные системы.
11. Чем различаются типы сетевых адаптеров?

12. Какую технологию поддерживают последние типы сетевых адаптеров?

13. Что такое сетевая операционная система?

14. Перечислить сетевое программное обеспечение и его назначение.

15. Для чего используется защита данных?

16. Что дает использование паролей и ограничение доступа?

17. Перечислить основные функции сетевых протоколов.

18. Для какой цели используется Web-сервер?

19. Какой сервер необходим для подключения к сети Internet?

20. Какое сетевое оборудование используется для связи между сегментами ЛВС?

6. 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.

6.1. 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.

6.2. 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.

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.

6.3. 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.

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) (рис. 6.1).

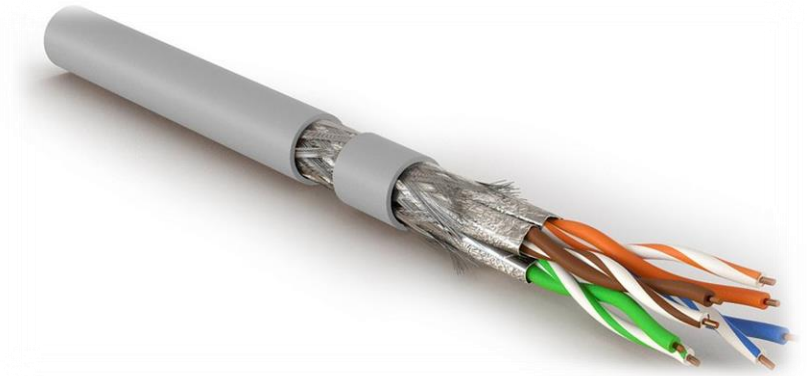

Рисунок 6.1 – Витая пара SF/FTP

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 6.1

Категории витой пары

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

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 6.2

Типы коаксиальных кабелей

Тип	Название, значение сопротивления
1	**2**
RG-8 и RG-11	Thicknet, 50 Ом
RG-58/U	Thinnet, 50 Ом, сплошной центральный медный проводник
RG-58 A/U	Thinnet, 50 Ом, центральный многожильный проводник

Продолжение табл. 6.2

1	2
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 (рис. 6.2). 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 разъемы BNC типа CP-50 и ввиду его небольшой стоимости он становится фактически стандартным для офисных ЛВС. Используется в технологии Ethernet 10Base2, описанной ниже.

Рисунок 6.2 – Кабель RG-58

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 A/U.

Оптоволоконный кабель (Fiber Optic Cable) обеспечивает высокую скорость передачи данных на большом расстоянии (рис. 6.3). 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.

Рисунок 6.3 – Кабель волоконно-оптический

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.

6.4. Кабельные системы Ethernet

10Base-T, 100Base-TX – неэкранированная витая пара (Unshielded Twisted Pair – UTP), 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.6.4).

Рисунок 6.4 – Восьмиконтактные RJ-45

10Base2 – тонкий коаксиальный кабель. Характеристики кабеля:

– приемлемые разъемы – BNC;
– диаметр 0.2 дюйма, RG-58A/U 50 Ом;
– максимальная длина сегмента – 185 м;
– минимальное расстояние между узлами – 0.5 м;
– максимальное число узлов в сегменте – 30.

10Base5 – толстый коаксиальный кабель. Характеристики кабеля:

– волновое сопротивление – 50 Ом;
– максимальная длина сегмента – 500 метров;
– минимальное расстояние между узлами – 2.5 м;
– максимальное число узлов в сегменте – 100.

6.5. Беспроводные технологии

Беспроводные технологии – подкласс информационных технологий, служат для передачи информации на расстояние между двумя и более точками, не требуя связи их проводами. Для передачи информации может использоваться инфракрасное излучение, радиоволны, оптическое или лазерное излучение.

В настоящее время существует множество беспроводных технологий, наиболее часто известных пользователям по их маркетинговым названиям, таким как Wi-Fi, WiMAX, Bluetooth. Все беспроводные технологии можно условно разделить на несколько классов:

– персональные беспроводные сети (Bluetooth);
– локальные беспроводные сети (Wi-Fi);
– беспроводные сети городского масштаба (WiMAX);
– глобальные беспроводные сети. (GPRS).

Bluetooth – это современная технология беспроводной передачи данных, позволяющая соединять друг с другом практически любые устройства: мобильные телефоны, ноутбуки, принтеры, холодильники и т.д. Для соединения необходим встроенный микрочип Bluetooth. Изначально технология предполагала возможность связи на расстоянии не более 10 метров.

Сегодня некоторые фирмы предлагают микросхемы Bluetooth, способные поддерживать связь на расстоянии до 100 метров.

Wi-Fi (Wireless Fidelity – «беспроводное качество») – стандарт на оборудование для широкополосной радиосвязи, предназначенной для организации локальных беспроводных сетей Wireless LAN. Благодаря функции хендовера пользователи могут перемещаться между точками доступа по территории покрытия сети Wi-Fi без разрыва соединения. Разработан консорциумом Wi-Fi Alliance на базе стандартов IEEE 802.11.

Преимущества Wi-Fi:

Позволяет развернуть сеть без прокладки кабеля, может уменьшить стоимость развёртывания и расширения сети.

Недостатки Wi-Fi:

Частотный диапазон и эксплуатационные ограничения в различных странах неодинаковы. Довольно высокое по сравнению с другими стандартами потребление энергии, что уменьшает время жизни батарей и повышает температуру устройства. Самый популярный стандарт шифрования, Wired Equivalent Privacy или WEP, может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости ключа).

WiMAX (Worldwide Interoperability for Microwave Access) – беспроводная технология, разработанная для предоставления пользователям универсальной беспроводной связи на больших расстояниях. Её работа основано на стандарте IEEE 802.16. Большинство телекоммуникационных компаний делают на WiMAX большие ставки и тому есть несколько причин.

Во-первых, это позволяет более эффективно (по сравнению с аналоговыми проводниками) не только предоставлять абонентам доступ в сеть, но и увеличить спектр услуг охватываю всё новые территории.

Во-вторых, такие беспроводные технологии крайне просты в использование, чем их кабельные аналоги. WiMAX и Wi-Fi легко развернуть на любой территории и так же легко увеличить зону покрытия.

Единственным минусом технологии является то, что сигнал достаточно плохо распространяется в городе. Этому способствует обилие зданий из армированного бетона, которые отражают или попросту подавляют сигнал.

General Packet Radio Service (GPRS) – это служба пакетной передачи данных через радиоинтерфейс. Данный сервис обеспечивает постоянное подключение к сети Интернет при помощи и напрямую с мобильного телефона. Технология GPRS отличается мгновенным установлением соединения и высокой скоростью передачи данных. Данные передаются в виде пакетов, что хорошо согласуется потребностями коммуникационных приложений. Все услуги Интернета доступны в сетях провайдеров сотовой связи GSM и TDMA.

Мобильные устройства принято классифицировать по поколениям (G – generation), к которому они принадлежат. Наименование началось с появления телефонов поколения 1G, которые часто называют «кирпичами». Далее последовало второе поколение телефонов или поколение 2G. Их появление привело к переходу от аналоговых к цифровым технологиям.

3G (от анг. Third generation – третье поколение, технологии мобильной связи 3 поколения) – набор услуг, который объединяет как высокоскоростной мобильный доступ с услугами сети интернет, так и технологию радиосвязи, которая создаёт канал передачи данных. Сети третьего поколения 3G работают на частотах дециметрового диапазона, как правило, в диапазоне около 2 ГГц, передавая данные со скоростью до 3,6 Мбит/с. Они позволяют организовывать видеотелефонную связь, смотреть на мобильном телефоне фильмы и телепрограммы и т.д. Прорыв её заключался в много поточности т.е. одновременной загрузки разных видов данных. Разработка с 1990, внедрение с 2002 года.

4G – поколение мобильной связи с повышенными требованиями. К четвёртому поколению принято относить перспективные технологии, позволяющие осуществлять передачу данных со скоростью, превышающей 100 Мбит/с подвижным и 1 Гбит/с – стационарным абонентам.

Вопросы к разделу 6

1. Что такое физическая среда?

2. Что может быть использовано в качестве физической среды передачи данных?

3. Какие вопросы при организации сети решаются на физическом уровне?

4. Что такое кабель?

5. Что такое линии связи?

6. Дать определение каналов связи.

7. Какие проблемы существуют при организации каналов связи?

8. Перечислить типы кабелей, используемых для передачи данных в сети.

9. Каково назначение структурированной кабельной системы?

10. На какие классы подразделяются кабельные системы?

11. Что такое 10BaseT?

12. Какой кабель используется в технологии 10Base2?

13. Какой кабель используется в технологии 10Base5?

14. Назвать какие типы кабелей используют для передачи данных в сети?

15. Какие известны кабельные системы Ethernet?

16. Какие существуют типы оптоволоконных кабелей?

17. Какие технологии беспроводной передачи данных вам известны?

7. СЕТЕВОЕ ОБОРУДОВАНИЕ

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

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.

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.

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.

Основные функции сетевых адаптеров:

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

Гальваническая развязка с коаксиальным кабелем или витой парой. Для этой цели используются импульсные трансформаторы. Иногда для развязки используются оптроны.

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.

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.

Формирование пакета. Сетевой адаптер должен разделить данные на блоки в режиме передачи (или соединить их в режиме приема) данных и оформить в 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.

Доступ к каналу связи. Набор правил, обеспечивающих доступ к среде передачи. Выявление конфликтных ситуаций и контроль состояния сети.

Идентификация своего адреса в принимаемом пакете. Физический адрес адаптера может определяться установкой переключателей, храниться в специальном регистре или прошиваться в ППЗУ.

Преобразование параллельного кода в последовательный код при передаче данных, и из последовательного кода в параллельный при приеме. В режиме передачи данные передаются по каналу связи в последовательном коде.

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.

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.

Рисунок 7.1 – Сетевой адаптер

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.

Основные 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, MCA. 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.

7.2. Повторители и концентраторы

Основная функция **повторителя** (repeater), как 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 (рис. 7.2). 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.

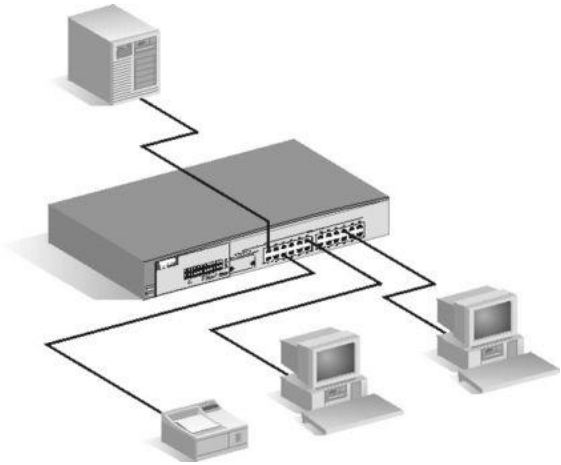

Рисунок 7.2 – Сетевое устройство концентратор

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

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, все компьютеры, подключенные к ним, образуют единый логический сегмент, в котором любая пара взаимодействующих компьютеров полностью блокирует возможность обмена данными для других компьютеров.

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. Учитывая стремительное развитие сетевых технологий, хабы больше не используются в современных сетях.

7.3. Мосты и коммутаторы

Мост (bridge) – ретрансляционная система, соединяющая каналы передачи данных. 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 и канальный уровни различных типов (рис. 7.3). Что касается канального процесса, то он объединяет разнотипные каналы передачи данных в один общий.

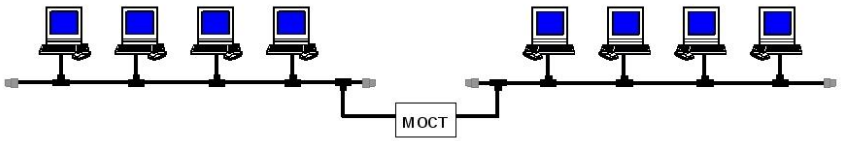

Рисунок 7.3 – Мост, соединяющий две сети разного типа

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.

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 (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 (switch) – устройство, осуществляющее выбор одного из возможных вариантов направления передачи данных. 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. 7.4).

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). 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.

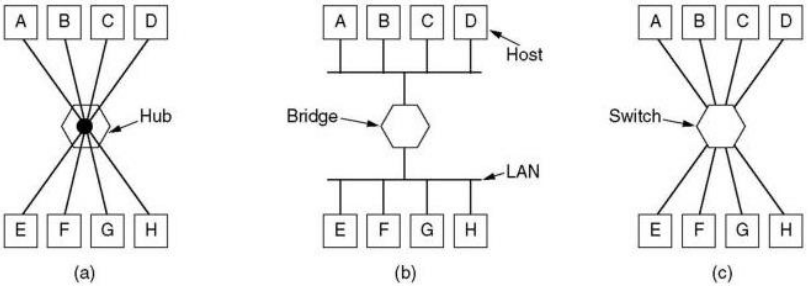

Рисунок 7.4 – Схема работы: a) концентратора, b) моста, c) коммутатора

7.4. Маршрутизаторы

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

Каждый маршрутизатор реализует протоколы физического, канального и сетевого уровней. 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 (рис. 7.5).

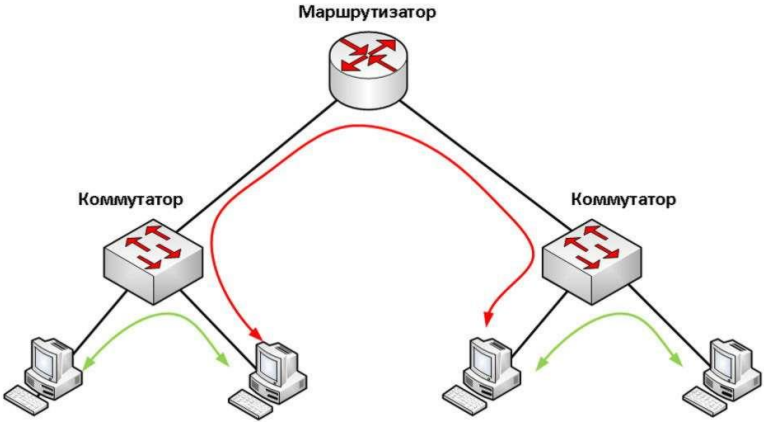

Рисунок 7.5 – Схема работы сетевого маршрутизатора

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.

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.

7.5. Шлюзы

Шлюз (gateway) – ретрансляционная система, обеспечивающая взаимодействие информационных сетей (рис. 7.6). 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.

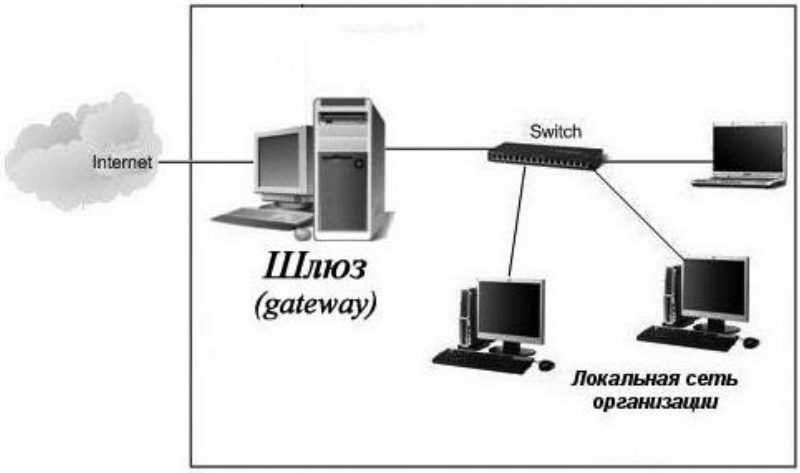

Рисунок 7.6 – Взаимодействие сетей с различными наборами протоколов через шлюз

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.

Вопросы к разделу 7

1. Назначение сетевого адаптера.
2. Какие параметры необходимо устанавливать у сетевого адаптера?
3. Перечислить функции сетевых адаптеров.
4. Что такое физический адрес адаптера?
5. Как определить физический адрес адаптера?
6. Какие есть типы сетевых адаптеров?
7. На каком уровне сетевой модели OSI используется сетевой адаптер?
8. Каково назначение повторителя?
9. В каких случаях ставят сетевой повторитель?
10. Что такое сетевой концентратор и каково его назначение?
11. На каком уровне сетевой модели OSI используется Hub?
12. Назначение моста.
13. На каком уровне сетевой модели OSI используется мост?
14. Какие сегменты сети может соединять мост?
15. Назначение коммутатора.

16. На каком уровне сетевой модели OSI используется коммутатор?

17. Каково различие между мостом и коммутатором?

18. Назначение маршрутизатора.

19. На каком уровне сетевой модели OSI используется маршрутизатор?

20. Каково различие между маршрутизаторами и мостами?

21. Что такое шлюз и каково его назначение.

22. На каком уровне сетевой модели OSI используется шлюз?

8. ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К СЕТЯМ

При организации и эксплуатации сети важными требованиями при работе являются следующие:

– производительность;
– надежность и безопасность;
– расширяемость и масштабируемость;
– прозрачность;
– поддержка разных видов трафика;
– управляемость;
– совместимость.

8.1. Производительность

Производительность – это характеристика сети, позволяющая оценить, насколько быстро информация передающей рабочей станции достигнет до приемной рабочей станции.

На производительность сети влияют следующие характеристики сети:

– конфигурация;
– скорость передачи данных;
– метод доступа к каналу;
– топология сети;
– технология.

Если производительность сети перестает отвечать предъявляемым к ней требованиям, то администратор сети может прибегнуть к различным приемам:

1. Изменить конфигурацию сети таким образом, чтобы структура сети более соответствовала структуре информационных потоков;
2. Перейти к другой модели построения распределенных приложений, которая позволила бы уменьшить сетевой трафик;
3. Заменить мосты более скоростными коммутаторами.

Но самым радикальным решением в такой ситуации является переход на более скоростную технологию. Если в сети используются традиционные технологии Ethernet или Token Ring,

то переход на Fast Ethernet, FDDI или 100VG-AnyLAN позволит сразу в 10 раз увеличить пропускную способность каналов.

С ростом масштаба сетей возникла необходимость в повышении их производительности. Одним из способов достижения этого стала их микросегментация. Она позволяет уменьшить число пользователей на один сегмент и снизить объем широковещательного трафика, а значит, повысить производительность сети.

Первоначально для микросегментации использовались маршрутизаторы, которые, вообще говоря, не очень приспособлены для этой цели. Решения на их основе были достаточно дорогостоящими и отличались большой временной задержкой и невысокой пропускной способностью. Более подходящими устройствами для микросегментации сетей стали коммутаторы. Благодаря относительно низкой стоимости, высокой производительности и простоте в использовании они быстро завоевали популярность.

Таким образом, сети стали строить на базе коммутаторов и маршрутизаторов. Первые обеспечивают высокоскоростную пересылку трафика между сегментами, входящими в одну подсеть, а вторые передают данные между подсетями, ограничивали распространение широковещательного трафика, решали задачи безопасности и т.д.

Виртуальные ЛВС (VLAN) обеспечивают возможность создания логических групп пользователей в масштабе корпоративной сети. Виртуальные сети позволяют организовать работу в сети более эффективно.

8.2. Надежность и безопасность

Важнейшей характеристикой вычислительных сетей является надежность. Повышение надежности основано на принципе предотвращения неисправностей путем снижения интенсивности отказов и сбоев за счет применения электронных схем и компонентов с высокой и сверхвысокой степенью интеграции, снижения уровня помех, облегченных режимов работы

схем, обеспечение тепловых режимов их работы, а также за счет совершенствования методов сборки аппаратуры.

Отказоустойчивость – это такое свойство вычислительной системы, которое обеспечивает ей как логической машине возможность продолжения действий, заданных программой, после возникновения неисправностей. Введение отказоустойчивости требует избыточного аппаратного и программного обеспечения. Направления, связанные с предотвращением неисправностей и отказоустойчивостью, основные в проблеме надежности. На параллельных вычислительных системах достигается как наиболее высокая производительность, так и, во многих случаях, очень высокая надежность. Имеющиеся ресурсы избыточности в параллельных системах могут гибко использоваться как для повышения производительности, так и для повышения надежности.

Следует помнить, что понятие надежности включает не только аппаратные средства, но и программное обеспечение. Главной целью повышения надежности систем является целостность хранимых в них данных.

Безопасность – одна из основных задач, решаемых любой нормальной компьютерной сетью. Проблему безопасности можно рассматривать с разных сторон – злонамеренная порча данных, конфиденциальность информации, несанкционированный доступ, хищения и т.п.

Обеспечить защиту информации в условиях локальной сети всегда легче, чем при наличии на фирме десятка автономно работающих компьютеров. Практически в вашем распоряжении один инструмент – резервное копирование (backup). Для простоты давайте называть этот процесс резервированием. Суть его состоит в создании в безопасном месте полной копии данных, обновляемой регулярно и как можно чаще. Для персонального компьютера более или менее безопасным носителем служат дискеты. Возможно использование стримера, но это уже дополнительные затраты на аппаратуру.

Легче всего обеспечить защиту данных от самых разных неприятностей в случае сети с выделенным файловым сервером. На сервере сосредоточены все наиболее важные файлы, а уберечь одну машину куда проще, чем десять. Концентрированность

данных облегчает и резервирование, так как не требуется их собирать по всей сети.

Экранированные линии позволяют повысить безопасность и надежность сети. Экранированные системы гораздо более устойчивы к внешним радиочастотным полям.

8.3. Прозрачность

Прозрачность – это такое состояние сети, когда пользователь, работая в сети, не видит ее. Коммуникационная сеть является прозрачной относительно проходящей сквозь нее информации, если выходной поток битов, в точности повторяет входной поток. Но сеть может быть непрозрачной во времени, если из-за меняющихся размеров очередей блоков данных изменяется и время прохождения различных блоков через узлы коммутации. Прозрачность сети по скорости передачи данных указывает, что данные можно передавать с любой нужной скоростью.

Если в сети по одним и тем же маршрутам передаются информационные и управляющие (синхронизирующие) сигналы, то говорят, что сеть прозрачна по отношению к типам сигналов.

Если передаваемая информация может кодироваться любым способом, то это означает, что сеть прозрачна для любых методов кодировок.

Прозрачная сеть является простым решением, в котором для взаимодействия локальных сетей, расположенных на значительном расстоянии друг от друга, используется принцип Plug-and-play (подключись и работай).

Прозрачное соединение. Служба прозрачных локальных сетей обеспечивает сквозное (end-to-end) соединение, связывающее между собой удаленные локальные сети. Привлекательность данного решения состоит в том, что эта служба объединяет удаленные друг от друга на значительное расстояние узлы как части локальной сети. Поэтому не нужно вкладывать средства в изучение новых технологий и создание территориально распределенных сетей (Wide-Area Network – WAN). Пользователям требуется только поддерживать локальное соединение, а провайдер

службы прозрачных сетей обеспечит беспрепятственное взаимодействие узлов через сеть масштаба города (Metropolitan-Area Network – MAN) или сеть WAN. Службы Прозрачной локальной сети имеют много преимуществ. Например, пользователь может быстро и безопасно передавать большие объемы данных на значительные расстояния, не обременяя себя сложностями, связанными с работой в сетях WAN.

8.4. Поддержка разных видов трафика

Трафик в сети складывается случайным образом, однако в нем отражены и некоторые закономерности. Как правило, некоторые пользователи, работающие над общей задачей, (например, сотрудники одного отдела), чаще всего обращаются с запросами либо друг к другу, либо к общему серверу, и только иногда они испытывают необходимость доступа к ресурсам компьютеров другого отдела. Желательно, чтобы структура сети соответствовала структуре информационных потоков. В зависимости от сетевого трафика компьютеры в сети могут быть разделены на группы (сегменты сети). Компьютеры объединяются в группу, если большая часть порождаемых ими сообщений, адресована компьютерам этой же группы.

Для разделения сети на сегменты используются мосты и коммутаторы. Они экранируют локальный трафик внутри сегмента, не передавая за его пределы никаких кадров, кроме тех, которые адресованы компьютерам, находящимся в других сегментах. Таким образом, сеть распадается на отдельные подсети. Это позволяет более рационально выбирать пропускную способность имеющихся линий связи, учитывая интенсивность трафика внутри каждой группы, а также активность обмена данными между группами.

Однако локализация трафика средствами мостов и коммутаторов имеет существенные ограничения. С другой стороны, использование механизма виртуальных сегментов, реализованного в коммутаторах локальных сетей, приводит к полной локализации трафика; такие сегменты полностью изолированы друг от друга, даже в отношении

широковещательных кадров. Поэтому в сетях, построенных только на мостах и коммутаторах, компьютеры, принадлежащие разным виртуальным сегментам, не образуют единой сети.

Для того чтобы эффективно консолидировать различные виды трафика в сети ATM, требуется специальная предварительная подготовка (адаптация) данных, имеющих различный характер: кадры – для цифровых данных, сигналы импульсно-кодовой модуляции – для голоса, потоки битов – для видео. Эффективная консолидация трафика требует также учета и использования статистических вариаций интенсивности различных типов трафика.

8.5. Управляемость

ISO внесла большой вклад в стандартизацию сетей. Модель управления сети является основным средством для понимания главных функций систем управления сети. Эта модель состоит из 5 концептуальных областей:

1. Управление эффективностью;
2. Управление конфигурацией;
3. Управление учетом использования ресурсов;
4. Управление неисправностями;
5. Управление защитой данных.

Цель *управления эффективностью* – измерение и обеспечение различных аспектов эффективности сети для того, чтобы межсетевая эффективность могла поддерживаться на приемлемом уровне. Примерами переменных эффективности, которые могли бы быть обеспечены, являются пропускная способность сети, время реакции пользователей и коэффициент использования линии.

Управление эффективностью включает несколько этапов:

1. Сбор информации об эффективности по тем переменным, которые представляют интерес для администраторов сети;

2. Анализ информации для определения нормальных (базовая строка) уровней;

3. Определение соответствующих порогов эффективности для каждой важной переменной таким образом, что превышение

этих порогов указывает на наличие проблемы в сети, достойной внимания.

Цель *управления конфигурацией* – контролирование информации о сетевой и системной конфигурации для того, чтобы можно было отслеживать и управлять воздействием на работу сети различных версий аппаратных и программных элементов. Т.к. все аппаратные и программные элементы имеют эксплуатационные отклонения, погрешности (или то и другое вместе), которые могут влиять на работу сети, такая информация важна для поддержания гладкой работы сети.

Каждое устройство сети располагает разнообразной информацией о версиях, ассоциируемых с ним. Чтобы обеспечить легкий доступ, подсистемы управления конфигурацией хранят эту информацию в базе данных. Когда возникает какая-нибудь проблема, в этой базе данных может быть проведен поиск ключей, которые могли бы помочь решить эту проблему.

Цель *управления учетом использования ресурсов* – измерение параметров использования сети, чтобы можно было соответствующим образом регулировать ее использование индивидуальными или групповыми пользователями. Такое регулирование минимизирует число проблем в сети (т.к. ресурсы сети могут быть поделены исходя из возможностей источника) и максимизирует равнодоступность к сети для всех пользователей.

Цель *управления неисправностями* – выявить, зафиксировать, уведомить пользователей и (в пределах возможного) автоматически устранить проблемы в сети, с тем чтобы эффективно поддерживать работу сети. Так как неисправности могут привести к простоям или недопустимой деградации сети, управление неисправностями, по всей вероятности, является наиболее широко используемым элементом модели управления сети ISO.

Управление неисправностями включает в себя несколько шагов:

– определение симптомов проблемы;

– изолирование проблемы;

– устранение проблемы;

– проверка устранения неисправности на всех важных подсистемах;

– регистрация обнаружения проблемы и ее решения.

Цель *управления защитой данных* – контроль доступа к сетевым ресурсам в соответствии с местными руководящими принципами, чтобы сделать невозможными саботаж сети и доступ к чувствительной информации лицам, не имеющим соответствующего разрешения. Например, одна из подсистем управления защитой данных может контролировать регистрацию пользователей ресурса сети, отказывая в доступе тем, кто вводит коды доступа, не соответствующие установленным.

Подсистемы управления защитой данных работают путем разделения источников на санкционированные и несанкционированные области. Для некоторых пользователей доступ к любому источнику сети является несоответствующим.

Подсистемы управления защитой данных выполняют следующие функции:

– идентифицируют чувствительные ресурсы сети (включая системы, файлы и другие объекты);

– определяют отображения в виде карт между чувствительными источниками сети и набором пользователей;

– контролируют точки доступа к чувствительным ресурсам сети;

– регистрируют несоответствующий доступ к чувствительным ресурсам сети.

8.6. Совместимость

Концепция программной совместимости впервые в широких масштабах была применена разработчиками системы IBM/360. Основная задача при проектировании всего ряда моделей этой системы заключалась в создании такой архитектуры, которая была бы одинаковой с точки зрения пользователя для всех моделей системы независимо от цены и производительности каждой из них. Огромные преимущества такого подхода, позволяющего сохранять существующий задел программного обеспечения при переходе на

новые (как правило, более производительные) модели, были быстро оценены как производителями компьютеров, так и пользователями, и начиная с этого времени практически все фирмы-поставщики компьютерного оборудования взяли на вооружение эти принципы, поставляя серии совместимых компьютеров. Следует заметить, однако, что со временем даже самая передовая архитектура неизбежно устаревает и возникает потребность внесения радикальных изменений в архитектуру и способы организации вычислительных систем.

В настоящее время одним из наиболее важных факторов, определяющих современные тенденции в развитии информационных технологий, является ориентация компаний-поставщиков компьютерного оборудования на рынок прикладных программных средств.

Этот переход выдвинул ряд новых требований. Прежде всего, такая вычислительная среда должна позволять гибко менять количество и состав аппаратных средств и программного обеспечения в соответствии с меняющимися требованиями решаемых задач. Во-вторых, она должна обеспечивать возможность запуска одних и тех же программных систем на различных аппаратных платформах, т.е. обеспечивать мобильность программного обеспечения. В-третьих, эта среда должна гарантировать возможность применения одних и тех же человеко-машинных интерфейсов на всех компьютерах, входящих в неоднородную сеть. В условиях жесткой конкуренции производителей аппаратных платформ и программного обеспечения сформировалась концепция открытых систем, представляющая собой совокупность стандартов на различные компоненты вычислительной среды, предназначенных для обеспечения мобильности программных средств в рамках неоднородной, распределенной вычислительной системы.

Вопросы к разделу 8

1. Какие основные требования предъявляются к сетям?
2. Что такое производительность сети?

3. Какие характеристики влияют на производительность сети?

4. Какие есть способы повышения производительности сетей?

5. Как обеспечить высокоскоростную пересылку трафика?

6. Чем обеспечивается надежность сети?

7. Что такое отказоустойчивость?

8. Перечислить задачи безопасности данных в сети.

9. Для какой цели используется резервное копирование?

10. Чем обеспечивается безопасность сетей в клиент-серверной архитектуре?

11. Для какой цели устанавливаются экранированные линии в сети?

12. Что такое прозрачность сетей?

13. В каком случае линия прозрачна по отношению к типам сигналов?

14. Что такое прозрачное соединение?

15. Что используется для разделения сети на сегменты?

16. Каким образом можно уменьшить трафик в сети?

17. Дать определение управляемости сетей и перечислить основные функции управления сетями.

18. Что включается в управление эффективностью?

19. Для какой цели используется управление неисправностями?

20. Для чего необходимо управление конфигурацией?

21. Какова цель управления защитой данных?

22. Какие функции подсистемы управления защитой данных?

23. Дайте определение понятия совместимости сетей.

ЗАКЛЮЧЕНИЕ

Тема «Компьютерные сети» очень широка и многогранна, а быстрый рост числа компьютерных сетей и их развитие сопровождаются сменой или совершенствованием сетевых технологий. Изучая информатику, важно понимать базовые основы и принципы построения и функционирования компьютерных сетей. Именно с этой точки зрения мы постарались изложить материал в данном учебном пособии. Авторы попытались оптимизировать классические объёмы информации, касающейся темы основ сетевых технологий и одновременно систематизировать отдельные сведения о новых технологиях и стандартах.

В первой части учебного пособия «Компьютерные системы и сети» изложены основные принципы построения и функционирования локальных и глобальных компьютерных сетей, их структуры, сетевые компоненты, а также перспективы их развития. Приведены виды топологий, используемые для физического соединения компьютеров в сети, методы доступа к каналу связи, физические среды передачи данных. Передача данных в сети рассматривается на базе эталонной базовой модели, разработанной Международной организацией по стандартам взаимодействия открытых сетей. Также в издании приводятся правила и процедуры передачи данных между информационными системами, типы сетевого оборудования, их назначение и принципы работы. Описывается сетевое программное обеспечение, используемое для организации сетей. Изучаются наиболее популярные сетевые операционные системы, их достоинства и недостатки. Рассматриваются принципы межсетевого взаимодействия. Приводятся основные принципы безопасности в сетях передачи данных, касающиеся главным образом симметричного шифрования и шифрования с открытыми ключами, помехоустойчивых кодов, методов и средств защиты от удаленных атак. Основное внимание уделяется решению технических вопросов, которые возникают при ежедневном обслуживании компьютерной сети, в частности диагностика функционирования протокола TCP/IP.

Теоретический материал учебного пособия дополнен иллюстрациями, которые в наглядной форме поясняют

теоретические основы сетевых технологий, а также представляют их практическую реализацию. В конце каждого раздела предлагаются контрольные вопросы для обсуждения.

Авторы надеются, что этот материал поможет читателю разобраться в многообразии современных сетевых технологий и компьютерных терминологий. Для расширения знаний и получения практических навыков моделирования и администрирования сетей рекомендуем продолжить обучение с использованием второй части учебного пособия «Компьютерные системы и сети», содержащего лабораторный практикум.

ГЛОССАРИЙ

1000Base-LX – стандарт на сегменты сети Gigabit Ethernet на оптоволоконном кабеле с длиной волны света 1,3 мкм.

1000Base-SX – стандарт на сегменты сети Gigabit Ethernet на оптоволоконном кабеле с длиной волны света 0,85 мкм.

1000Base-CX – стандарт на сегменты сети Gigabit Ethernet на экранированной витой паре.

100Base-FX – обозначение технологии Fast Ethernet по стандарту 802.3 сети Fast Ethernet для передачи больших сообщений по многомодовому оптоволокну в полудуплексном и полнодуплексном режимах.

100Base-T4 – обозначение технологии Fast Ethernet по стандарту 802.3 со скоростью 100 Мб/с для четырех парной витой пары. Вместо кодирования 4B/5B в этом методе используется кодирование 8B/6T.

100Base-TX – обозначение технологии сети Fast Ethernet по стандарту 802.3 для передачи больших сообщений с использованием метода MLT-3 для передачи сигналов 5-битовых порций кода 4B/5B по витой паре, а также наличие функции авто переговоров
(Auto-negotiation) для выбора режима работы порта.

10Base2 – обозначение технологии Ethernet по стандарту 802.3 со скоростью передачи данных 10 Мб/с для тонкого коаксиального кабеля.

10Base5 – обозначение технологии Ethernet по стандарту 802.3 со скоростью передачи данных 10 Мб/с для толстого коаксиального кабеля.

10Base-FL – стандарт на сегменты сети Ethernet на оптоволоконном кабеле.

10BaseT – обозначение технологии Ethernet по стандарту 802.3 со скоростью передачи данных 10 Мб/с для кабеля «витая пара».

А

Адаптер (adapter) – устройство либо программа для согласования параметров входных и выходных сигналов в целях сопряжения объектов. Административная система (management

system) – система, обеспечивающая управление сетью либо ее частью.

Адрес (address) – закодированное обозначение пункта отправления либо назначения данных.

Адрес IP – адрес, однозначно определяющий компьютер в сети (адрес состоит из 32 двоичных разрядов и не может повторяться во всей сети TCP/IP). Адрес IP обычно разбивается на четыре октета по восемь двоичных разрядов (один байт); каждый октет преобразуется в десятичное число и отделяется точкой, например, 102.54.94.97.

Аналоговый сигнал (analog signal) – сигнал, величина которого непрерывно изменяется во времени. Аналоговый сигнал обеспечивает передачу данных путем непрерывного изменения во времени.

Аналого-дискретное преобразование (analog-to-digital conversion) – процесс преобразования аналогового сигнала в дискретный сигнал.

Анонимные подключения – эта функция, которая разрешает удаленный доступ к ресурсам компьютера по учетной записи компьютера без предъявления имени и пароля с правами, определяемыми этой учетной записью.

Архитектура – концепция, определяющая модель, структуру, выполняемые функции и взаимосвязь компонентов сети. Архитектура охватывает логическую, физическую и программную структуры и функционирование сети, а также элементы, характер и топологию взаимодействия элементов.

Асинхронная передача – метод передачи основанный на пересылки данных по одному символу. При этом промежутки между передачами символов могут быть не равными.

Б

База данных (БД) – совокупность взаимосвязанных данных, организованная по определенным правилам в виде одного или группы файлов.

Базовый порт ввода/вывода (base I/O port) – адрес памяти, по которому центральный процессор и адаптер проверяют наличие сообщений, которые они могут оставлять друг для друга.

Безопасность данных (data security) – концепция защиты программ и данных от случайного либо умышленного изменения, уничтожения, разглашения, а также несанкционированного использования.

Блок данных (data unit) – последовательность символов фиксированной длины, используемая для представления данных или самостоятельно передаваемая в сети.

Бод (baud) – термин, используемый для измерения скорости модема, который описывает количество изменений состояния, происходящих за одну секунду в аналоговой телефонной линии.

Булева алгебра – алгебраическая структура с тремя операциями И, ИЛИ, НЕ.

Буфер (buffer) – временная область, которую устройство использует для хранения входящих данных перед тем, как они смогут быть обработаны на входе, или для хранения исходящих данных до тех пор, пока не появится возможность их передачи.

Буфер (buffer) – запоминающее устройство, используемое между объектами при передаче данных для временного хранения данных с целью согласования скоростей.

В

Витая пара (twisted-pair cable) – два скрученных изолированных провода, которые используются для передачи электрических сигналов.

Виртуальная сеть – сеть, характеристики которой в основном определяются ее программным обеспечением.

Виртуальные локальные вычислительные сети (ВЛВС) – логические наложения на коммутируемое объединение сетей, определяющие группы пользователей. Это означает, что пользователь или система, подключенные к физическому порту, могут участвовать в нескольких ВЛВС – группах, поскольку логическая сеть не обязана подчиняться ограничениям физической. Границы ВЛВС задают область локального вещания. Обычно потоки данных в ВЛВС коммутируются на уровне 2, в то время как трафик между ВЛВС маршрутизируется, с использованием внешнего маршрутизатора.

Волновое сопротивление, импеданс (impedance) – полное электрическое сопротивление переменному току, включающее активную и реактивную составляющие. Измеряется в омах.

Выделенная линия (dedicated line) – (точка-точка) частная или адресуемая линия, наиболее популярная в глобальных вычислительных сетях. Обеспечивает полнодуплексную полосу пропускания, установив постоянное соединение каждой оконечной точки через мосты и маршрутизаторы с несколькими ЛВС.

Выделенный сервер (dedicated server) – сетевой сервер, который действует только как сервер и не предназначен для использования в качестве клиентской машины.

Г

Гигабайт (gigabyte) – обычно 1000 мегабайтов. Точно 1024 мегабайт, где 1 мегабайт равен 1 048 576 байтам (220).

Гиперсреда – технология представления любых видов информации в виде блоков, ассоциативно связанных друг с другом, не требующая подтверждения о приеме от принимающей стороны.

Гипертекст – текст, представленный в виде ассоциативно связанных друг с другом блоков.

Гипертекстовый протокол HTTP – протокол сети Internet, описывающий процедуры обмена блоками гипертекста.

Главный контроллер домена (Primary Domain Controller, PDC) – компьютер, на котором устанавливается Windows NT Server в режиме PDC для хранения главной копии базы данных учетных записей.

Глобальная вычислительная сеть, ГВС (Wide Area Network, WAN) – компьютерная сеть, использующая средства связи дальнего действия.

Группа (group) – совокупность пользователей, определяемая общим именем и правами доступа ресурсам.

Д

Данные (data) – информация, представленная в формализованном виде, пригодном для автоматической обработки при возможном участии человека.

Дейтаграммы (datagrams) – сообщения, которые не требуют подтверждения о приеме от принимающей стороны.

Термин, используемый в некоторых протоколах для обозначения пакета.

Дефрагментация (defragmentation) – процесс воссоздания больших PDU (пакетных блоков данных) на более высоком уровне из набора более мелких PDU с нижнего уровня.

Диагностическое программное обеспечение (diagnostic software) – специализированные программы или специфические системные компоненты, которые позволяют исследовать и наблюдать систему с целью определения, работает она правильно или нет, и попробовать определить причину проблемы.

Дискретный сигнал (discrete signal) – сигнал, имеющий конечное, обычно небольшое, число значений. Практически всегда дискретный сигнал имеет два либо три значения. Нередко его называют также цифровым сигналом.

Домен (domain) – совокупность компьютеров, использующих операционную систему Windows NT Server, имеющих общую базу данных и систему защиты. Каждый домен имеет неповторяющееся имя.

Доменная система имен (DNS – Domain Name System) – система обозначений для сопоставления адресов IP и имен, понятных пользователю, используется в сети Internet. Система DNS иногда называется службой DNS.

Доступ (access) – операция, обеспечивающая запись, модификацию, чтение или передачу данных.

Драйвер (driver) – компонент операционной системы, взаимодействующий с внешним устройством или управляющий выполнением программ.

Драйвер устройства (device driver) – программа, которая обеспечивает взаимодействие между операционной системой и конкретными устройствами с целью ввода/вывода данных для этого устройства.

Е

Единообразный локатор ресурсов (Uniform Resource Locator, URL) – идентификатор, или адрес ресурсов, в сети Internet. Обеспечивает гипертекстовые связи между документами WWW.

Ж

Жесткий диск (hard disk) – накопитель данных в вычислительных системах.

З

Заголовок кадра (frame preamble) – служебная информация Канального уровня модели OSI, добавляемая в начало кадра.

Запрос прерывания (IRQ – interrupt request) – сигнал, посылаемый центральному процессору от периферийного устройства. Сообщает о событии, обработка которого требует участие процессора.

Запросчик (requester, LAN requester) – (редиректор) программа, находящаяся на компьютере клиенте. Переадресует на соответствующий сервер запросы на сетевые услуги со стороны работающих на этом же компьютере приложений.

Затухание (attenuation) – ослабление сигнала при удалении его от точки испускания.

Звезда (star topology) – вид топологии, при котором каждый компьютер подключен к центральному компоненту, называемому концентратором.

Зеркальные диски (disk mirroring) – уровень 1 технологии RAID, при которой часть жесткого диска (или весь жесткий диск) дублируется на одном или нескольких жестких дисках. Позволяет создавать резервную копию данных.

И

Изображение (image) – графическая форма представления данных, предназначенная для зрительного восприятия.

Импульсно-кодовая модуляция – ИКМ (PCM – Pulse Code Modulation) – метод преобразования аналогового сигнала телефонии в дискретный сигнал.

Интернет – совокупность компьютеров, объединенных в глобальную сеть.

Информационная сеть (information network) – сеть, предназначенная для обработки, хранения и передачи данных.

Информационная система (information system) – объект, способный осуществлять хранение, обработку или передачу данных. К информационной системе относятся: компьютеры,

программы, пользователи и другие составляющие, предназначенные для процесса обработки и передачи данных.

Информационно-поисковая система – (IRS – Information Retrieval System) – система, предназначенная для поиска информации в базе данных.

Информация (information) – совокупность фактов, явлений, событий, представляющих интерес, подлежащих регистрации и обработке.

Информация (information) – данные, обработанные адекватными им методами.

Инфракрасный канал (infrared channel) – канал, использующий для передачи данных инфракрасное излучение. Инфракрасный канал работает в диапазоне высоких частот, где сигналы мало подвержены электрическим помехам.

К

Кабель (cable) – один либо группа изолированных проводников, заключенных в герметическую оболочку.

Кадр (frame) – блок информации канального уровня.

Кадр данных (data frame) – базовая упаковка битов, которая представляет собой PDU (пакетный блок данных), посланный с одного компью- тера на другой по сетевому носителю.

Канал (link) – среда или путь передачи данных.

Канал передачи данных (data channel) – кабели и инфраструктура сети.

Канальный уровень (Date link layer) –второй уровень модели OSI. Здесь из последовательности битов, поступающих от физического уровня, формируются кадры.

Клиент (client) – компьютер в сети, который запрашивает ресурсы или услуги от некоторых других компьютеров.

Клиент (client) – объект информационной сети, использующий сервис, предоставляемый другими объектами.

Клиент-сервер (client-server) – модель вычислений, при которой некоторые компьютеры запрашивают услуги (клиенты), а другие отвечают на такие запросы на услуги (сервер).

Коаксиальный кабель (coaxial cable) – кабель, состоящий из изолированных друг от друга внутреннего и внешнего проводников. Коаксиальный кабель имеет один либо несколько

центральных медных проводников, покрытых диэлектрической изоляцией, которая для защиты центральных проводников от внешних электромагнитных воздействий покрыта металлической оплеткой (сеткой) либо трубкой.

Коаксиальный кабель (coaxial cable) – тип кабеля, который использует центральный проводник, обернутый изолирующим слоем, окруженный плетеной металлической сеткой и внешней оболочкой или экранирующим слоем.

Коллизия (collision) – ситуация, когда две рабочие станции пытаются одновременно занять канал (использовать рабочую среду – кабель).

Коммуникационная сеть – сеть, предназначенная для передачи данных, также она выполняет задачи, связанные с преобразованием данных.

Коммутатор (switch) – устройство или программа, осуществляющие выбор одного из возможных вариантов направления передачи данных. Коммутаторы кадров – многопортовые мосты уровня доступа к среде передачи, работающие со скоростью этой среды и гарантирующие на порядок более высокую пропускную способность при связывании клиентских и серверных систем по сравнению с концентраторами для среды с разделяемым доступом. При сегментации ЛВС коммутаторы кадров обеспечивают лучшие показатели цена/производительность и меньшие задержки, чем традиционные связки мостов и маршрутизаторов.

Коммутаторы ячеек – устройства, реализующие АТМ-коммутацию данных, разделенных на короткие ячейки фиксированного размера. Ориентация на установление соединений позволяют АТМ обеспечивать классы (качество) обслуживания, пригодные для всех видов мультимедийного трафика, включая данные, голос и видео.

Концентратор или hub (concentrator or hub) – связующий компонент сети, к которому подключаются все компьютеры в сети топологии «Звезда». Концентратор обеспечивает связь компьютеров друг с другом при использовании витой пары, также используется в сетях FDDI для подключения компьютеров в центральном узле.

Концентратор MSAU (Multi Station Access Unit) – устройство для доступа к множеству станций, которое осуществляет маршрутизацию пакета к следующему узлу в сетях с метод доступа с передачей маркера.

Корпоративная сеть (enterprise network) – крупномасштабная сеть, обычно соединяющая многие локальные сети.

Л

Лазерный принтер (laser printer) – принтер, в котором изображение символов печатаются лазерным лучом и переносятся на бумагу методом ксерографии.

Логический диск (logical disk) – часть физического диска, отформатированная под конкретную файловую систему и имеющая свое буквен- ное наименование.

Логический канал (logical channel) – путь, по которому данные передаются от одного порта к другому. Логический канал прокладывается в одном либо последовательности физических каналов и через уровни области взаимодействия.

Локальная группа (local group) – В Windows NT Server – учетная запись, определенная на конкретном компьютере. Включает учетные записи пользователей данного компьютера.

Локальная сеть (Local-Area Network) – сеть, системы которой расположены на небольшом расстоянии друг от друга.

М

Магистраль (backbone) – основной кабель, от которого кабели трансиверов идут к компьютерам, повторителям и мостам.

Манчестерское кодирование – схема передачи двоичных данных, применяемая во многих сетях. При передаче бита, равного 1, в течение временного интервала, который отведен для его передачи, значение сигнала меняется с положительного на отрицательное. При передаче бита равного 0, в течение временного интервала, который отведен для его передачи, значение сигнала меняется с отрицательного на положительное.

Маркер (token) – уникальная комбинация битов. Когда рабочая станция в ЛВС получает маркер, она имеет право начать передачу данных. Маршрутизатор (router) – протокол –

ориентированное устройство, соединяющее две сети, иногда с абсолютно разными уровнями MAC (канальный уровень, контроль доступа к среде).

Маршрутизация (routing) – процесс определения в коммуникационной сети пути, по которому блок данных может достигнуть адресата.

Маска сети (network mask) – 32-битовое число, по которому можно определить диапазон IP-адресов, находящихся в одной
IP-сети/подсети. Масштабируемость – это возможность увеличить вычислительную мощность Web-сайта или компьютерной системы (в частности выполнение большего числа операций или транзакций за определенный период времени) за счет установки большего числа процессоров или их замены на более мощные.

Мегабайт (megabyte) – 1048576 байтов.

Метод доступа – способ определения, какая рабочая станция сможет следующей использовать ЛВС. Кроме того, также называется набор правил, используемых сетевым оборудованием, чтобы направлять поток сообщений через сеть, а также один из основных признаков, по которым различают компоненты сетевого оборудования.

Метод доступа к каналу (channel access method) – правила, используемые для определения, какой компьютер может посылать данные по сети, тем самым предотвращающее потерю данных из-за коллизий.

Метод доступа – набор правил, обеспечивающих арбитраж доступа к среде передачи. Примерами методов доступа являются CSMA/CD (Ethernet) и передача маркера (Token Ring).

Метод множественного доступа с прослушиванием несущей и разрешением коллизий (CSMA/CD) – метод доступа к каналу связи, который 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, в случае, когда два узла попытаются занять канал, то обнаружившая

конфликт интерфейсная плата, выдает в сеть специальный сигнал, и обе станции одновременно прекращают передачу.

Метод обработки запросов по приоритету – метод доступа к каналу связи, где всем узлам сети предоставляется право равного доступа. Концентратор опрашивает каждый порт и проверяет наличие запроса на передачу затем решает этот запрос в соответствии с приоритетом.

Метод с передачей маркера или полномочия (ТРМА) – метод доступа к каналу связи, в котором от компьютера к компьютеру передается маркер, дающий разрешение на передачу сообщения. При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит его по сети. Каждая станция, находящаяся между передающей и принимающей «видит» это сообщение, но только станция-адресат принимает его. При этом она создает новый маркер.

Микроядро (microkernel) – центральная часть операционной системы, выполняющая основные функции управления системой.

Модем (modem) – сокращение от МОДулятор-ДЕМодулятор – устройство связи, позволяющее компьютеру передавать данные по обычной телефонной линии. При передаче преобразует цифровые сигналы в аналоговые. При приеме преобразует аналоговые сигналы в цифровые.

Монитор сети (network monitor) – программно-аппаратное устройство, которое отслеживает сетевой трафик. Проверяет пакеты на уровне кадров, собирает информацию о типах пакетов и ошибках.

Мост (bridge) – это устройство, позволяющее рабочим станциям одной сети обращаться к рабочим станциям другой. Мосты используются для разделения ЛВС на маленькие сегменты. Выполняет соединение на канальном уровне модели OSI. Мост преобразует физический и канальный уровни различных типов. Используется для увеличения длины или количества узлов.

Мост-маршрутизатор (bridge-router) – сетевое устройство, которое объединяет лучшие функции моста и маршрутизатора.

Мультиплексор (multiplexor) – устройство, позволяющее разделить канал передачи на два или более подканала. Может быть

реализован программно. Кроме того, используется для подключения нескольких линий связи к компьютеру.

Н

Нейронная сеть (neural network) – сеть, образованная взаимодействующими друг с другом нервными клетками, либо моделирующими их поведение компонентами.

Несущая (carrier) – непрерывный сигнал, на который накладывается другой сигнал, несущий информацию.

Неэкранированная витая пара (UTP – Unshielded Twisted Pair) – 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.

О

Оболочка (shell) – программное обеспечение, которое реализует взаимодействие пользователя с операционной системой (пользовательский интерфейс).

Обработка запросов по приоритету (demand priority) – высокоскоростной метод доступа к каналу, используемый сетями 100VG-Any LAN в топологии звезда.

Общий ресурс (shared resource) – любое устройство, данные или программа.

Одноранговая архитектура (peer-to-peer architecture) – концепция информационной сети, в которой каждая абонентская система может предоставлять и потреблять ресурсы.

Октет – байт.

Оперативная память (main memory) – память, предназначенная для хранения данных и команд, необходимых процессору для выполнения им операций.

Оптический кабель (optical cable) – кабель, передающий сигналы света. Для создания оптического кабеля используются световоды, каждый из которых имеет несколько слоев защитных покрытий, улучшающих механические и оптические характеристики этих световодов.

Оптический канал (optical channel) – канал, предназначенный для передачи сигналов света.

Оптоволокно (optical fiber) – среда, по которой цифровые данные передаются в виде модулированных световых импульсов.

П

Пакет – это единица информации, передаваемый между станциями сети. Используется на сетевом уровне модели OSI.

Пароль (password) – признак, подтверждающий право пользователя или прикладной программы на использование какого-нибудь ресурса.

Передача данных (data communications) – процесс транспортирования данных из одной системы в другую.

Повторитель или репитер (repeater) – устройство, усиливающее сигналы с одного отрезка кабеля и передающее их в другой отрезок без изменения содержания. Повторители увеличивают максимальную длину трассы ЛВС.

Полномочие (token) – специальный символ или группа символов, разрешающая системе передачу кадров.

Полоса пропускания (bandwidth) – разность между максимальной и минимальной частотой в заданном диапазоне; диапазон частот, на которых может работать носитель.

Пользователь (user) – юридическое либо физическое лицо, использующее какие-либо ресурсы, возможности.

Порт (port) – точка доступа к устройству либо программе. Различают физические и логические порты.

Провайдер (provider) – организация, которая обеспечивает подключение к Internet и другие услуги за определенную плату.

Протокол – набор правил, регламентирующих порядок сборки пакетов, содержащих данные и управляющую информацию, на рабочей станции-отправителе для передачи их по сети, а также порядок разборки пакетов по достижении ими рабочей станции-получателя.

Р

Распределитель (hub) – центр ЛВС или кабельной системы с топологией звезда. В этой роли могут быть файл-серверы или концентраторы.

Они содержат сетевое программное обеспечение и управляют коммуникациями внутри сети, а также могут работать как шлюзы к другим ЛВС.

Редиректор для протоколов (redirector) – компонент набора протоколов или сетевой операционной системы, ответственный за перехват запросов от приложений и распределение их между локальной или удаленной службами сети.

Реестр (registry) – архив БД Windows NT для хранения информации о конфигурации компьютера, включая аппаратные средства, установленное программное обеспечение, установки окружения и др.

С

Сеанс – сообщение, в котором предполагается создание логической связи для обмена сообщений. Сеанс должен быть сначала установлен, после этого происходит обмен сообщениями. После окончания обмена сеанс должен быть закрыт.

Сегмент (segment) – часть сети, ограниченная ретранслирующими устройствами (повторителями, мостами, маршрутизаторами и шлюзами).

Сервер – это компьютер сети, предоставляющий сервис другим объектам по их запросам.

Сетевая служба (network service) – вид сервиса, предоставляемого сетью

Сеть (network) – взаимодействующая совокупность сетевых узлов, связанных друг с другом каналами связи, предназначенная для передачи информации.

Слот адаптера (adapter slot) – гнездо, встроенное в материнскую плату. Стандарт RS-232 – промышленный стандарт для последовательных соединений.

Т

Телекоммуникация (telecommunication) – область деятельности, предметом которой являются методы и средства передачи информации.

Терминал (terminal) – устройство ввода/вывода данных и команд в систему или сеть.

Тестирование (testing) – процесс проверки правильности функционирования устройства либо программного обеспечения.

Технология RAID – используется для построения отказоустойчивости систем. Имеет пять уровней. 1 уровень – зеркализация дисков, 2 уровень – чередование дисков с записью кода коррекции ошибок, 3 уровень – код коррекции ошибок в виде четности, 4 уровень – чередование дисков блоками, 5 уровень – чередование с контролем четности.

Тип кадра (frame type) – один из четырех стандартов, которые определяют структуру пакета Ethernet: Ethernet 802.3, Ethernet 802.2, Ethernet SNAP или Ethernet II.

Транзакция – короткий во времени цикл взаимодействия объектов, включающий запрос - выполнение задания – ответ.

Трансивер – устройство, предназначенное осуществлять передачу данных с сетевых интерфейсных плат в физическую среду.

Трафик – поток данных.

У

Удаленная регистрация (remote logon) – подключение по сети к другому компьютеру пользователя, зарегистрированного на своем ПК по своей учетной записи.

Удаленный доступ (dial-up) – доступ к системе или по сети к другому компьютеру пользователя, зарегистрированного на своем ПК по своей учетной записи.

Удаленный доступ (remote access) – технология взаимодействия абонентских систем с локальными сетями через территориальные коммуникационные сети.

Утилита (utility) – программа, выполняющая какую-либо функцию сервиса.

Узел (node) – точка присоединения к сети; устройство, подключенное к сети.

Учетная запись (account) – информация, хранящаяся в базе данных Windows NT (учетная запись пользователя, компьютера, группы).

Ф

Факсимильная связь (facsimile) – процесс передачи через коммуникационную сеть неподвижных изображений и текста.

Физическая среда (physical media) – материальная субстанция, через которую осуществляется передача сигналов.

Фрагментация (fragmentation) – процесс разделения длинного пакета данных с более высокого уровня на последовательность более коротких пакетов на нижнем уровне.

Х

Характеристический файл данных (characterization data file) – файл, содержащий информацию о конфигурационных возможностях конкретной модели принтера, включая поддерживающую разрешающую способность.

Ц

Центральный процессор (central processing unit) – управляющий и вычислительный модуль компьютера. Устройство, которое интерпретирует и выполняет команды.

Циклический избыточный код (CRC – Cyclical Redundancy Check) – число, получаемое в результате математических преобразований над пакетом данных и исходными данными. При доставке пакета вычисления повторяются. Если результат совпадает, то пакет принят без ошибок.

Цифровая линия (digital line) – линия связи, передающая информацию только в двоичной (цифровой) форме.

Цифровая сеть комплексных услуг (ISDN – Integrated Services Digital Network) – цифровая сеть связи, обеспечивающая коммутацию каналов и коммутацию пакетов.

Ч

Четность (parity) – способ контроля за безошибочной передачей блоков данных с помощью добавления контрольных битов.

Ш

Шина (bus) – специализированный набор параллельных линий в персональном компьютере.

Шина (bus) – канал передачи данных, отдельные части которого называются сегментами.

Широковещательная передача (broadcast) – технология передачи сигналов, таких как сетевые данные, посредством использования передатчика какого-либо типа для посылки этих сигналов по коммуникационному носителю.

Шифрование (encryption) – преобразование информации для ее защиты от несанкционированного доступа.

Шлюз (gateway) – устройство, посредством которого соединяются сети разных архитектур.

Э

Экран (shielding) – металлическая оплетка или цилиндр, навитый из фольги. Защищает передаваемые данные, уменьшая внешние электрические помехи, которые называются шумом.

Экранированная витая пара (Shielded Twisted-Pair, STP) – витая пара, окруженная заземленной металлической оплеткой, которая служит экраном.

Электронная почта (email) – компьютерная система обмена сообщениями, где текст и файлы могут быть посланы от одного пользователя к одному или многим другим пользователям в той же сети.

Эталонная модель взаимодействия открытых систем (OSI – Open System Interconnection) – семиуровневая модель, которая стандартизирует уровни услуг и виды взаимодействия между системами в информационной сети при передаче данных.

Эфир (ether) – пространство, через которое распространяются волны электромагнитного спектра и прокладываются каналы радиосетей и инфракрасных сетей. Электромагнитное поле не нуждается в специальном носителе.

Я

Язык HTML – инструментальное программное обеспечение, использующее технологию гипертекста.

Язык описания страниц (page description language) – язык программирования, который описывает вид страницы для печати. Используется для компоновки изображения страницы.

Язык структурированных запросов (SQL – Structured Query Language) – язык управления базами данных, используемый для запроса, обновления и управления реляционными базами данных.

Ячеистая топология сети (mesh network topology) – топология, используемая в глобальных вычислительных сетях. К любому узлу существует несколько маршрутов.

СПИСОК ИСТОЧНИКОВ

1. Васин, Н. Н. Основы построения инфокоммуникационных систем и сетей: учеб. для вузов / Н. Н. Васин, В. А. Вострикова, Р. Р. Диязитдинов и др.; под ред. Н. Н. Васина. – Самара, ПГУТИ, 2017. – 220 с.

2. Кузин, А. В. Компьютерные сети: учеб. пособие / А. В. Кузин, Д. А. Кузин. – М.: Форум, 2018. – 704 с.

3. Куроуз, Д. Компьютерные сети. Нисходящий подход / Д. Куроуз, К. Росс. – М.: Эксмо, 2016. – 912 с.

4. Максимов, Н. В. Компьютерные сети: учеб. пособие / Н. В. Максимов, И. И. Попов. – М.: Форум, 2017. – 320 с.

5. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация: пер. с англ. – М.: ООО «И. Д. Вильямс», 2015. – 736 с.

6. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл; пер. с англ. А. Гребенькова. – М.: Питер, 2019. – 960 с.

7. Гойхман, В. Аналитический обзор протоколов Интернета вещей / В. Гойхман, А. Савельева // Технологии и средства связи. – № 4. – 2016. – С. 32–37.

8. Яницкая, Т. С. Учебно-методический комплекс по дисциплине «Сети и телекоммуникации» / Т. С. Яницкая. – Тольятти: ПВГУС, 2016. – 228 с.

9. Пескова, С. Н. Сети и телекоммуникации. учебное пособие / С. Н. Пескова, А. П. Кузин, А. С. Волков. – М.: ИЦ «Академия». – 2018. – 222 с.

10. Ватаманюк, А. Создание и обслуживание локальных сетей / А. Ватаманюк. – Питер, 2016. – 512 с.

11. Олифер, Н. А. Проблемы построения корпоративных сетей. Учебное пособие / В. Г. Олифер, Н. А. Олифер. – М.: – Центр информационных технологий, 2016. – 258 с.

12. Шэнк, Д. Технология клиент-сервер и ее приложения. Руководство Novell. – М., 2015. – 442 с.

13. Максимов, Н. В. Компьютерные сети: учебное пособие / Н. В. Максимов, И. И. Попов. – 6-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА-М, 2021. – 464 с.

14. Кузин, А. В. Компьютерные сети: учебное пособие / А. В. Кузин, Д. А. Кузин. – 4-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА-М, 2020. – 190 с.

15. Исаченко, О. В. Программное обеспечение компьютерных сетей: учебное пособие / О. В. Исаченко. – 2-е изд., испр. и доп. – М.: ИНФРА-М, 2020. – 158 с.

16. Катунин, Г. П. Основы инфокоммуникационных технологий: учебник / Катунин Г. П. – Саратов: Ай Пи Эр Медиа, 2018. – 797 с. – ISBN 978-5-4486-0335-8. – Текст: электронный // IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/74561.html (дата обращения: 24.09.2022). – Режим доступа: для авторизир. пользователей. – DOI: https://doi.org/10.23682/74561

17. Компьютерные сети: учебник / В. Г. Карташевский [и др.]. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016. – 267 с. – Текст: электронный // IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/71846.html (дата обращения: 26.08.2022). – Режим доступа: для авторизир. пользователей

ДЛЯ ЗАМЕТОК

Учебное издание

СУВОРОВА Евгения Юрьевна
ШИШЛАКОВА Виктория Николаевна

КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ

Часть 1

Учебное пособие

Редактор – Суворова Е. Ю.
Корректор – Шишлакова В. Н.
Верстка – Суворова Е. Ю.

Подписано в печать 26.12.2022. Бумага офсетная.
Гарнитура Times New Roman.
Печать ризографическая. Формат 60×84/16. Усл. печ. л. 8,14.
Тираж 50 экз. Заказ № 147.

Издатель
ГОУ ВПО ЛНР «ЛГПУ»
«Книта»
ул. Оборонная, 2, г. Луганск, ЛНР, 91011. Т/ф: (0642)58-03-20
e-mail: knitaizd@mail.ru