1. Назначение сетей. Основные определения и термины. Преимущества использования сетей.

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

В состав сети в общем случае включается следующие элементы:-сетевые компьютеры (оснащенные сетевым адаптером);-каналы связи (кабельные, спутниковые, телефонные, цифровые, волоконно-оптические, радиоканалы и др.);-различного рода преобразователи сигналов;-сетевое оборудование.

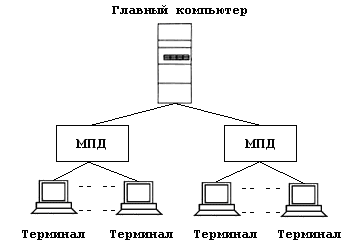
**Коммуникационная сеть** предназначена для передачи данных, также она выполняет задачи, связанные с преобразованием данных. Коммуникационные сети различаются по типу используемых физических средств соединения.Информационная сеть предназначена для хранения информации и состоит из информационных систем. На базе коммуникационной сети может быть построена группа информационных сетей.

**Компьютерная сеть** состоит из информационных систем и каналов связи.Под информационной системой следует понимать объект, способный осуществлять хранение, обработку или передачу информация. В состав информационной системы входят: компьютеры, программы, пользователи и другие составляющие, предназначенные для процесса обработки и передачи данных. **Вычислительная сеть** – это одна из разновидностей распределенных систем, предназначенная для распараллеливания вычислений, за счет чего может быть достигнуто повышение производительности и отказоустойчивости системы.

Под **каналом связи (data link)** следует понимать путь или средство, по которому передаются сигналы. Средство передачи сигналов называют абонентским, или физическим, каналом. **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.**Метод доступа** – это способ определения того, какая из рабочих станций сможет следующей использовать канал связи и как управлять доступом к каналу связи (кабелю).**Топология** – это описание физических соединений в сети, указывающее какие рабочие станции могут связываться между собой. **Архитектура** – это концепция, определяющая взаимосвязь, структуру и функции взаимодействия рабочих станций в сети.

1. Архитектура терминал – главный компьютер.

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


1. Одноранговая архитектура.

**Одноранговая архитектура** (peer-to-peer architecture) – это концепция информационной сети, в которой ее ресурсы рассредоточены по всем взаимодействующим между собой системам.



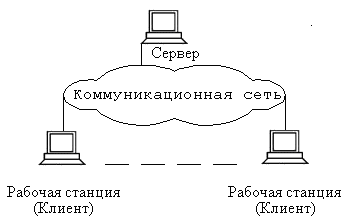
Данная архитектура характеризуется тем, что в ней все системы равноправны.

Одноранговые сети имеют следующие преимущества:они легки в установке и настройке;отдельные ПК не зависят от выделенного сервера;пользователи в состоянии контролировать свои ресурсы;малая стоимость и легкая эксплуатация;минимум оборудования и программного обеспечения;нет необходимости в администраторе (финансовая выгода);хорошо подходят для сетей с количеством пользователей, не превышающим десяти.

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

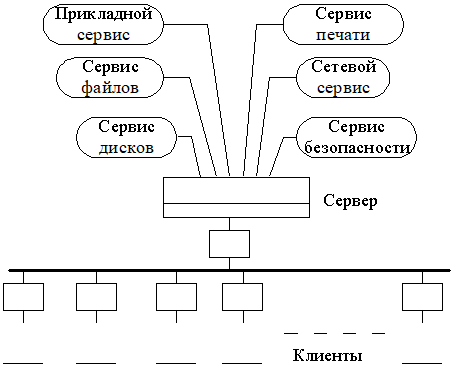
1. Архитектура клиент – сервер.

**Архитектура клиент–сервер** (client-server architecture) – это концепция информационной сети, в которой основная часть ее ресурсов сосредоточена в серверах, обслуживающих своих клиентов.



Сервер - это объект, 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 какой-либо вид сервиса сервера (например, сервис файлов). В этом процессе клиент запрашивает вид обслуживания, устанавливает сеанс, получает нужные ему результаты и сообщает об окончании работы.



1. Топология вычислительной сети. Виды топологий. Топология общая шина.

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

Понятие топологии широко используется при создании сетей. Одним из подходов к классификации топологий ЛВС является выделение двух основных классов топологий: широковещательные и последовательные.В **широковещательных топологиях** ПК передает сигналы, которые могут быть восприняты остальными ПК. К таким топологиям относятся топологии: общая шина, дерево, звезда.В **последовательных топологиях** информация передается только одному ПК. Примерами таких топологий являются: произвольная (произвольное соединение ПК), кольцо, цепочка.

При выборе оптимальной топологии преследуются три основных цели: -обеспечение альтернативной маршрутизации и максимальной надежности передачи данных; -выбор оптимального маршрута передачи блоков данных; -предоставление приемлемого времени ответа и нужной пропускной способности.

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

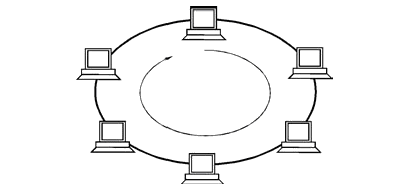


Топология Общая шина предполагает использование одного кабеля, к которому подключаются все компьютеры сети. В случае топологии Общая шина кабель используется всеми станциями по очереди. Принимаются специальные меры для того, чтобы при работе с общим кабелем компьютеры не мешали друг другу передавать 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.

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. Расширение сети требует прекращения ее работы на некоторый период. Сеть характеризуется проблемами с безопасностью, т.к. применяется широковещательный принцип передачи.

1. Топология кольцо. Топология цепочка.

**«Кольцо»** – это топология ЛВС, в которой каждая рабочая станция соединена с двумя другими рабочими станциями, образуя кольцо.



Данные передаются от одной рабочей станции к другой в одном направлении (по кольцу). Каждый ПК работает как повторитель, ретранслируя сообщения к следующему ПК. Если компьютер получает данные, предназначенные для другого компьютера, он передает их дальше по кольцу, в ином случае они дальше не передаются. Основная проблема при кольцевой топологии заключается в том, что каждая рабочая станция должна активно участвовать в пересылке информации, и в случае выхода из строя хотя бы одной из них, вся сеть парализуется. Подключение новой рабочей станции требует краткосрочного выключения сети, т.к. во время установки кольцо должно быть разомкнуто. Топология Кольцо имеет хорошо предсказуемое время отклика, определяемое числом рабочих станций.

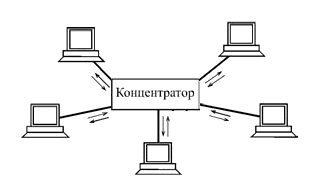
**Чистая кольцевая топология** на практике используется редко. Вместо этого кольцевая топология играет транспортную роль в схеме метода доступа. Кольцо описывает логический маршрут, а пакет передается от одной станции к другой, совершая в итоге полный круг.

В качестве отдельной топологию **«цепочка»,** представляющую «разомкнутое» кольцо. 

В данной топологии сохраняются все особенности и правила топологии «кольцо».

1. Звездообразные топологии.

**«Звезда»** – это топология сети, в которой все рабочие станции присоединены к центральному узлу (например, к концентратору), который устанавливает, поддерживает и разрывает связи между рабочими станциями.

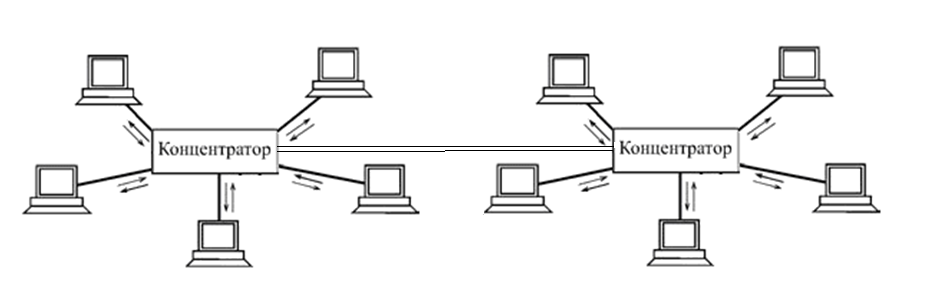


Фактически каждый компьютер через специальный сетевой адаптер подключается отдельным кабелем к объединяющему устройству. При необходимости можно объединять вместе несколько сетей с топологией

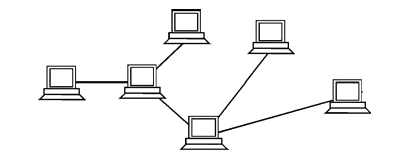
Преимуществом такой топологии является возможность простого исключения неисправного узла. Однако, если неисправен центральный узел, вся сеть выходит из строя.

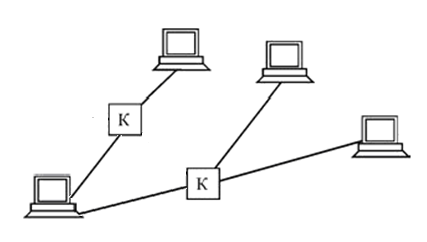
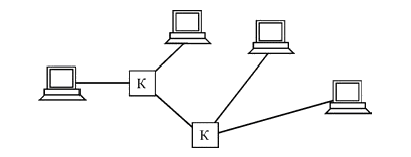
Звездообразная топология обеспечивает защиту от разрыва кабеля. Если кабель рабочей станции будет поврежден, это не приведет к выходу из строя всего сегмента сети. Она позволяет также легко диагностировать проблемы подключения, так как каждая рабочая станция имеет свой собственный кабельный сегмент, подключенный к концентратору.

Однако звездообразная топология имеет и недостатки. Во-первых, она требует много кабеля. Однако в большинстве случаев в такой топологии используется недорогой кабель типа витая пара. Во-вторых, центральные устройства могут быть довольно дороги. В-третьих, кабельные центральные связующие устройства при большом количестве кабеля трудно обслуживать. Сети с топологией звезда ограничены в расширении (увеличения числа компьютеров) – все зависит от числа портов на центральном связующем устройстве.Решением является последовательное соединение нескольких равноправных «звезд». При этом особое внимание необходимо уделить пропускной способности связующих каналов.

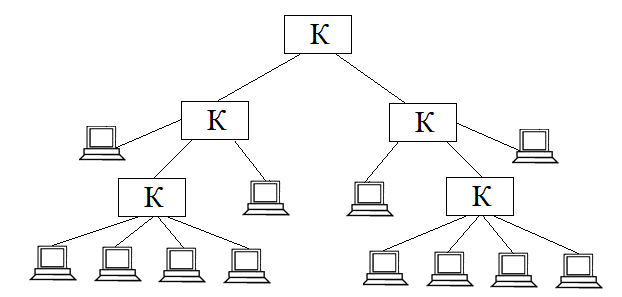
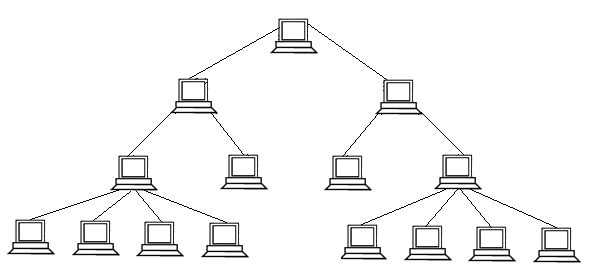


1. Древовидные топологии.

Сетевую топологию **«дерево»** (tree) можно рассматривать как комбинацию нескольких звезд. Причем, как и в случае «звезды», «дерево» может быть активным или истинным. 

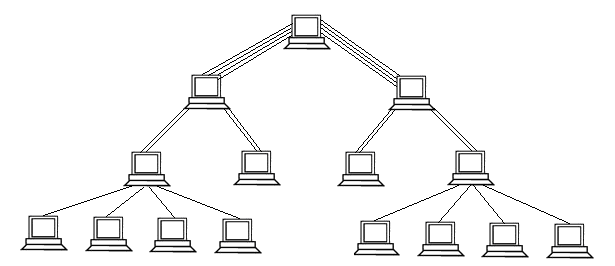
Также **«дерево»** может быть **пассивным**. При **активном «дереве»** в центрах объединения нескольких линий связи находятся центральные компьютеры, а при пассивном – концентраторы (хабы).

В любой древовидной топологии должна четко прослеживаться иерархия подключений. Важнейшую роль при таком построении будет играть узел или устройство, расположенное в вершине дерева.



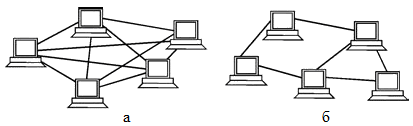
На практике эффективно исполнять роль вершины дерева в пассивном варианте топологии устройство типа «концентратор» не может – целесообразно использовать «коммутатор».

**Сетевая топология «fat tree»** (утолщенное дерево), изобретенная Charles E. Leiserson, является дешевой и эффективной схемой построения суперкомпьютеров.



В отличие от классической топологии «дерево», в которой все связи между узлами одинаковы, связи в «утолщенном дереве» становятся более широкими (производительными по пропускной способности) с каждым уровнем по мере приближения к корню дерева. Часто используют удвоение пропускной способности на каждом уровне.

1. Ячеистые топологии.

**В сеточной (ячеистой) (mesh)** топологии компьютеры связываются между собой не одной, а многими линиями связи, образующими сетку.

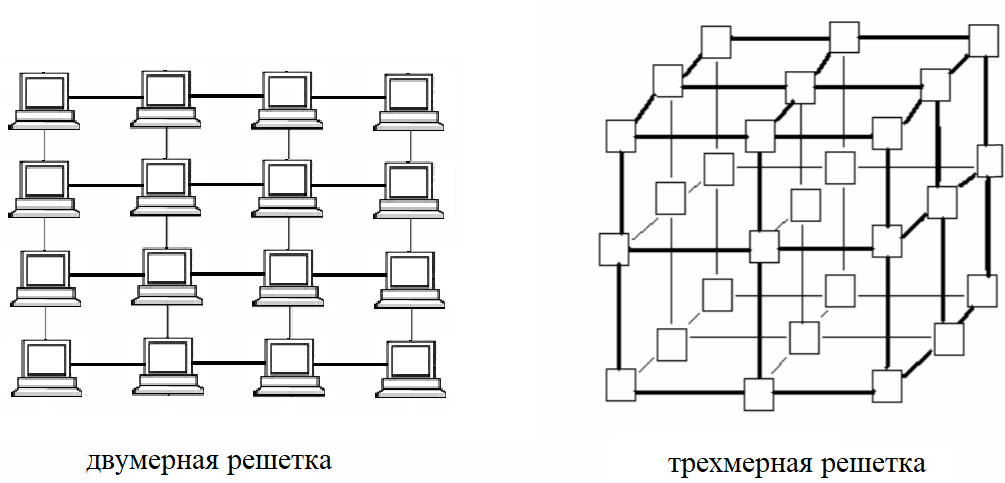
В полной сеточной топологии каждый компьютер напрямую связан со всеми остальными компьютерами. В этом случае при увеличении числа компьютеров резко возрастает количество линий связи. Кроме того, любое изменение в конфигурации сети требует внесения изменений в сетевую аппаратуру всех компьютеров, поэтому полная сеточная топология не получила широкого распространения.

Частичная сеточная топология предполагает прямые связи только для самых активных компьютеров, передающих максимальные объемы информации. Остальные компьютеры соединяются через промежуточные узлы.

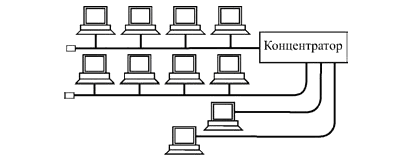
Сеточная топология позволяет выбирать маршрут для доставки информации от абонента к абоненту, обходя неисправные участки. С одной стороны, это увеличивает надежность сети, с другой же – требует существенного усложнения сетевой аппаратуры, которая должна выбирать маршрут.



**Решетчетая** − это топология, в которой узлы образуют регулярную многомерную решетку. При этом каждое ребро решетки параллельно ее оси и соединяет два смежных узла вдоль этой оси.Одномерная «решетка» – это цепь, соединяющая два внешних узла (имеющие лишь одного соседа) через некоторое количество внутренних (у которых по два соседа – слева и справа). При соединении обоих внешних узлов получается топология «кольцо». Двух- и трехмерные решетки (рис. 2.12) используются в архитектуре суперкомпьютеров.

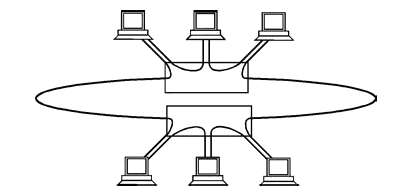


1. Комбинированные топологии.

Наиболее распространены **звездно-шинная** (star-bus) (рис. 12) и **звездно-кольцевая** (star-ring) (рис. 13).

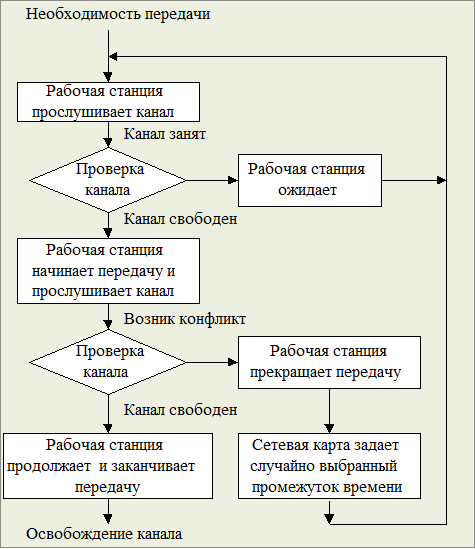
В «звездно – шинной» топологии используется комбинация шины и «пассивной звезды». К концентратору подключаются как отдельные компьютеры, так и целые шинные сегменты. В данной топологии может использоваться и несколько концентраторов, соединенных между собой и образующих так называемую магистральную, опорную шину. К каждому из концентраторов при этом подключаются отдельные компьютеры или шинные сегменты. В результате получается «звездно – шинное дерево».

В звездно – кольцевой топологии в кольцо объединяются не сами компьютеры, а специальные концентраторы (прямоугольник на рис. 13), к которым в свою очередь подключаются компьютеры с помощью звездообразных двойных линий связи. В действительности все компьютеры сети включаются в замкнутое кольцо, так как внутри концентраторов линии связи образуют замкнутый контур. Данная топология дает возможность комбинировать преимущества звездной и кольцевой топологий.



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

1. Метод доступа CSMA/CD.

множественный доступ с прослушиванием несущей и разрешением коллизий (Carrier Sense Multiple Access with Collision Detection – CSMA/CD);1. Если рабочая станция хочет воспользоваться сетью для передачи данных, она сначала должна проверить состояние канала: начинать передачу станция может, если канал свободен. 2.В процессе передачи станция продолжает прослушивание сети для обнаружения возможных конфликтов. 3. 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.4. Принимающая станция отбрасывает частич-но принятое сообщение, а все рабочие станции, желающие передать сообщение, в течение некоторого, случайно выбранного промежутка времени выжидают, прежде чем начать сообщение.

5. Все сетевые интерфейсные платы запрограммированы на разные псевдослучайные промежутки времени. Если конфликт возникнет во время повторной передачи сообщения, этот промежуток времени будет увеличен.

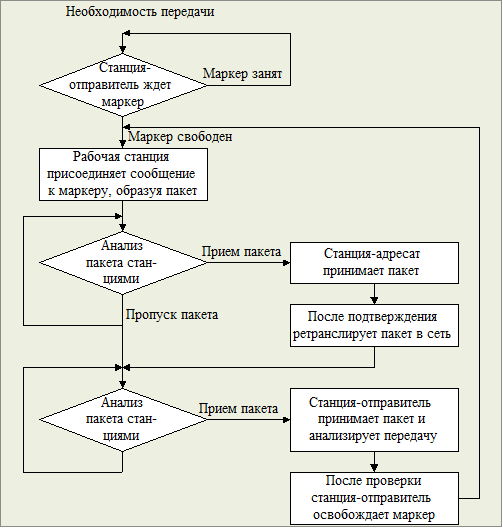
1. Метод доступа CSMA/CA. Метод доступа Demand Priority.

централизованный метод доступа (Demand Priority – с запросом приоритета);

В методе доступа Demand Priority концентратор выступает в роли «арбитра» − проблема доступа к разделяемой среде решается через передачу запросов на передачу концентратору, который циклически прослушивает всех абонентов по очереди и даёт право передачи абоненту, следующему по порядку за тем, который закончил передачу. Величина времени доступа в таком случае в отличии от обычного CSMA/CD гарантирована. В данном методе доступа реализованы два уровня приоритетов: низкий − для обычных приложений и высокий − для мультимедийных. Запросы с высоким уровнем приоритета (высокоприоритетные) обслуживаются раньше, чем запросы с нормальным приоритетом (низкоприоритетные). 1. Если приходит запрос высокого приоритета, то нормальный порядок обслуживания прерывается, и после окончания приема текущего пакета обслуживается запрос высокого приоритета. 2. Если таких высокоприоритетных запросов несколько, то возврат к нормальной процедуре обслуживания происходит только после полной обработки всех этих запросов. Можно сказать, что высокоприоритетные запросы обслуживаются вне очереди, но они образуют свою очередь. 3. При этом концентратор следит за тем, чтобы не была превышена установленная величина гарантированного времени доступа для низкоприоритетных запросов. Если высокоприоритетных запросов слишком много, то запросы с нормальным приоритетом автоматически переводятся им в ранг высокоприоритетных. Типичная величина времени повышения приоритета равна 200—300 мс (устанавливается при конфигурировании сети).

1. Метод доступа TPMA.

множественный доступ с передачей полномочия (Token Passing Multiple Access – TPMA) или метод с передачей маркера;

Это метод доступа к среде, в котором от рабочей станции к рабочей станции передается маркер, дающий разрешение на передачу сообщения. Маркер (token), или полномочие, – уникальная комбинация бит, позволяющая начать передачу данных.1.При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит это сообщение по сети. 2.Каждая станция между передающей станцией и принимающей видит это сообщение, но только станция – адресат принимает его. При этом она создает новый маркер.3. Пакет распространяется по сети 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 сеть. 4. После этого пакет возвращается в узел из которого был отправлен. Здесь после проверки безошибочной передачи пакета, узел освобождает сеть, выпуская новый маркер или начинает передачу следующего пакета. В сети с передачей маркера невозможны коллизии (конфликты).

1. Метод доступа TDMA.

множественный доступ с разделением во времени (Time Division Multiple Access – TDMA);

Данный метод характеризуется следующими достоинствами: гарантирует определенное время доставки блоков данных в сети;дает возможность предоставления различных приоритетов передачи данных.Вместе с тем он имеет существенные недостатки:в сети возможны потеря маркера, а также появление нескольких маркеров, при этом сеть прекращает работу;включение новой рабочей станции и отключение связаны с изменением адресов всей системы.

В данном методе доступа часто ограничивают число последовательных передач между одними и теми же узлами, что обеспечить принцип «чередования», т.е. исключить возможность «захвата сети» одной парой передающих и принимающих абонентов, например, при использовании подтверждения передачи.

Множественный доступ с разделением во времени основан на распределении времени работы канала между системами.

R20

1.Доступ TDMA основан на использовании специального устройства, называемого тактовым генератором. Этот генератор делит время канала на повторяющиеся циклы. 2.Каждый из циклов начинается сигналом Разграничителем. Цикл включает n пронумерованных временных интервалов, называемых ячейками. 3.Интервалы предоставляются для загрузки в них блоков данных.

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

**Второй**, более сложный, но высокоэкономичный вариант заключается в том, что система получает интервал только тогда, когда у нее возникает необходимость в передаче данных, например, при асинхронном способе передачи. Для передачи данных система может в каждом цикле получать интервал с одним и тем же номером. В этом случае передаваемые системой блоки данных появляются через одинаковые промежутки времени и приходят с одним и тем же временем запаздывания. При наличии свободных интервалов абоненту по запросу может предоставляться несколько временных ячеек.Данный вариант организации доступа к сети особенно удобен при передаче речи.

1. Метод доступа FDMA и WDMA.

множественный доступ с разделением частоты (Frequency Division Multiple Access – FDMA) или множественный доступ с разделением длины волны (Wavelength Division Multiple Access – WDMA).

Доступ FDMA основан на разделении полосы пропускания канала на группу полос частот, образующих логические каналы.

R21

Широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. Размеры узких полос могут быть различными.В целом, метод доступа FDMA относительно прост, но для его реализации необходимы передатчики и приемники, работающие на различных частотах. **Аспекты метода доступа FDMA:**1. В каждой узкой полосе создается логический канал. 2. Размеры узких полос могут быть различными. 3. Передаваемые по логическим каналам сигналы накладываются на разные несущие и поэтому в частотной области не должны пересекаться. 4. 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.

**Аспекты метода доступа WDMA:1.**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. 2.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. 3.На приемном конце разделение частот сигналов, прошедших физический канал, осуществляется путем фильтрации выходных сигналов.

1. Принципы передачи информации по сети. Понятие протокола. Понятие инкапсуляции и декапсуляции. (недоделан)

Информация в локальных сетях, как правило, передается отдельными порциями, кусками, называемыми в различных источниках пакетами (packets), кадрами (frames) или блоками. Причем предельная длина этих пакетов строго ограничена (обычно величиной в несколько килобайт). Ограничена длина пакета и снизу (как правило, несколькими десятками байт).

Важнейшим параметром является так называемое время доступа к сети (access time), которое определяется как временной интервал между моментом готовности абонента к передаче (когда ему есть, что передавать) и моментом начала этой передачи.

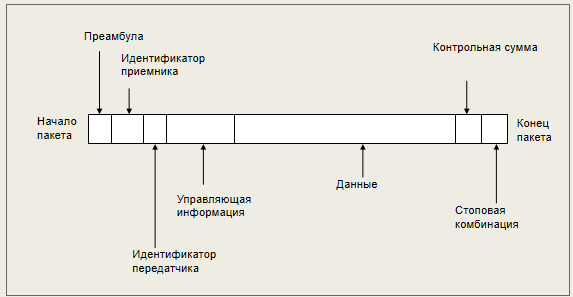
Фактически, это время ожидания абонентом начала своей передачи. Естественно, оно не должно быть слишком большим, иначе величина реальной, интегральной скорости передачи информации между приложениями сильно уменьшится даже при высокоскоростной связи.Ожидание начала передачи связано с тем, что в сети не может происходить несколько передач одновременно.

Существует некоторая оптимальная длина пакета (или оптимальный диапазон длин пакетов), при которой средняя скорость обмена информацией по сети будет максимальна. Эта длина не является неизменной величиной, она зависит от уровня помех, метода управления обменом, количества абонентов сети, характера передаваемой информации, и от многих других факторов. Имеется диапазон длин, который близок к оптимуму.

1. Назначение пакетов и их структура.

Структура и размеры пакета в каждой сети жестко определены стандартом на данную сеть и связаны, прежде всего, с аппаратурными особенностями данной сети, выбранной топологией и типом среды передачи информации. Кроме того, эти параметры зависят от используемого протокола (порядка обмена информацией).

Но существуют некоторые общие принципы формирования структуры пакета, которые учитывают характерные особенности обмена информацией по любым локальным сетям.

В наиболее общем случае пакет содержит в себе следующие 7 основных полей.

**Стартовая комбинация бит** (преамбула) - обеспечивает предварительную настройку аппаратуры адаптера или другого сетевого устройства на прием и обработку пакета. Это поле может полностью отсутствовать или же сводиться к единственному стартовому биту.

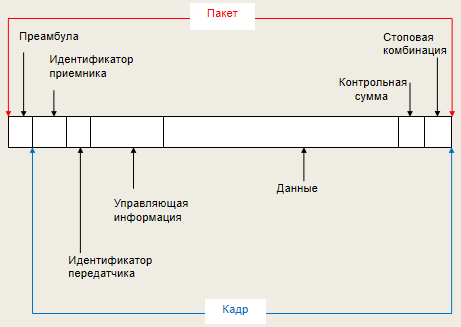
**Сетевой адрес** (идентификатор) принимающего абонента, то есть индивидуальный или групповой номер, присвоенный каждому принимающему абоненту в сети. Этот адрес позволяет приемнику распознать пакет, адресованный ему лично, группе, в которую он входит, или всем абонентам сети одновременно (при широком вещании).

**Сетевой адрес (идентификатор**) передающего абонента, то есть индивидуальный номер, присвоенный каждому передающему абоненту. Этот адрес информирует принимающего абонента, откуда пришел данный пакет. Включение в пакет адреса передатчика необходимо в том случае, когда одному приемнику могут попеременно приходить пакеты от разных передатчиков

**Служебная информация**, которая может указывать на тип пакета, его номер, размер, формат, маршрут его доставки, на то, что с ним надо делать приемнику и т.д.

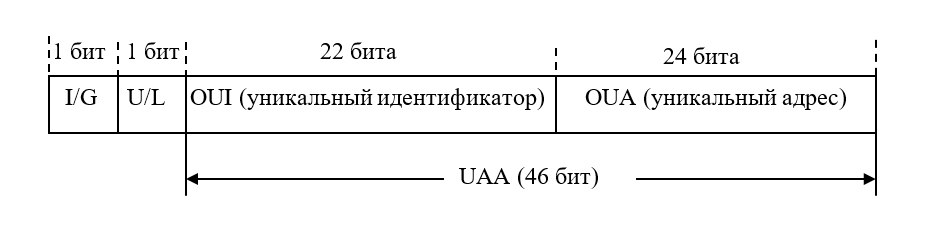
**Данные (поле данных)** – это та информация, ради передачи которой используется пакет. В отличие от всех остальных полей пакета поле данных имеет переменную длину, которая, собственно, и определяет полную длину пакета. Существуют специальные управляющие пакеты, которые не имеют поля данных.

**Контрольная сумма пакета** – это числовой код, формируемый передатчиком по определенным правилам и содержащий в свернутом виде информацию обо всем пакете. Приемник, повторяя вычисления, сделанные передатчиком, с принятым пакетом, сравнивает их результат с контрольной суммой и делает вывод о правильности или ошибочности передачи пакета. Если пакет ошибочен, то приемник или исправляет ошибки, или запрашивает повторную передачу пакета.

**Стоповая комбинация** служит для информирования аппаратуры принимающего абонента об окончании пакета, обеспечивает выход аппаратуры приемника из состояния приема. Это поле может отсутствовать, если используется самосинхронизирующийся код, позволяющий определять момент окончания передачи пакета.

1. MAC-адреса и их структура.

В качестве стандартного выбран 48-битный формат адреса, что соответствует примерно 280 триллионам различных адресов.С тем, чтобы распределить возможные диапазоны адресов между многочисленными изготовителями сетевых адаптеров, была предложена следующая структура адреса.



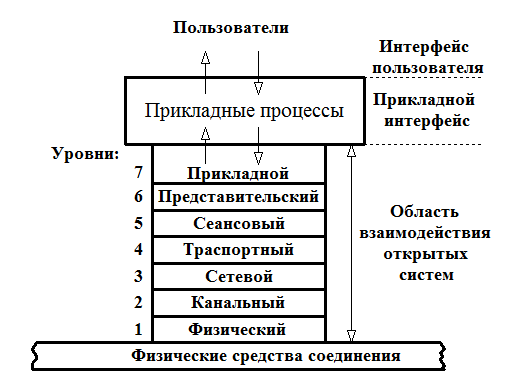
Младшие 24 разряда кода адреса называются OUA (Organizationally Unique Address) – уникальный адрес. Именно их присваивает каждый из зарегистрированных производителей сетевых адаптеров. Всего возможно свыше 16 миллионов комбинаций, то есть каждый изготовитель может выпустить 16 миллионов сетевых адаптеров.

Следующие 22 разряда кода называются OUI (Organizationally Unique Identifier) – уникальный идентификатор. IEEE присваивает один или несколько OUI каждому производителю сетевых адаптеров. Это позволяет исключить совпадения адресов адаптеров от разных производителей. Всего возможно свыше 4 миллионов разных OUI, это означает, что теоретически может быть зарегистрировано 4 миллиона производителей.

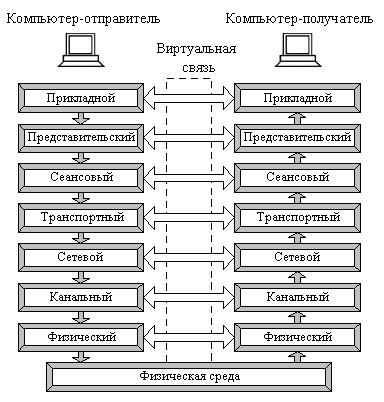
Вместе OUA и OUI называются UAA (Universally Administered Address) – универсально управляемый адрес или IEEE-адрес.Старший бит I/G (Individual/Group) указывает на тип адреса. Если он установлен в 0, то индивидуальный, если в 1, то групповой (многопунктовый или функциональный). Пакеты с групповым адресом получат все имеющие этот групповой адрес сетевые адаптеры. Причем групповой адрес определяется 46-ю младшими разрядами.Второй управляющий бит U/L (Universal/Local) называется флажком универсального/местного управления и определяет, как был присвоен адрес данному сетевому адаптеру. Обычно он установлен в 0. Установка бита U/L в 1 означает, что адрес задан не производителем сетевого адаптера, а организацией, использующей данную сеть. Для широковещательной передачи (то есть передачи всем абонентам сети одновременно) применяется специально выделенный адрес − все 48 битов которого установлены в единицу. Его принимают все абоненты сети независимо от их индивидуальных и групповых адресов.

1. Семиуровневая модель OSI . Назначение. Взаимодействие уровней модели OSI. Понятие горизонтальной и вертикальной модели.

Эта модель описывает правила и процедуры передачи данных в различных сетевых средах при организации сеанса связи.

1. Каждый уровень модели OSI выполняет определенную задачу в процессе передачи данных по сети. 2. Базовая модель, являющаяся основой для разработки сетевых протоколов, разделяет коммуникационные функции в сети на семь уровней, каждый из которых обслуживает различные части процесса области взаимодействия открытых систем.3. Модель OSI описывает только системные средства взаимодействия, не касаясь приложений конечных пользователей. Приложения реализуют свои собственные протоколы взаимодействия, обращаясь к системным средствам. Если приложение может взять на себя функции некоторых верхних уровней модели OSI, то для обмена данными оно обращается напрямую к системным средствам, выполняющим функции оставшихся нижних уровней модели OSI.

4. Каждый уровень модели выполняет свою функцию. Чем выше уровень, тем более сложную задачу он решает.5. Отдельные уровни модели OSI удобно рассматривать как группы программ, предназначенных для выполнения конкретных функций. 6. Каждый уровень обеспечивает сервис для вышестоящего уровня, запрашивая в свою очередь, сервис у нижестоящего уровня. Верхние уровни запрашивают сервис почти одинаково: как правило, это требование маршрутизации каких-то данных из одной сети в другую. Практическая реализация принципов адресации данных возложена на нижние уровни.

**Модель OSI можно разделить на две различных модели, как показано на следующем рисунке**: **горизонтальную** модель на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах; **вертикальную** модель на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине.

Каждый уровень компьютера–отправителя взаимодействует с таким же уровнем компьютера-получателя, как будто он связан напрямую. Такая связь называется логической или виртуальной связью.

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).

1. Уровни модели OSI: прикладной уровень (Application layer)

1. Прикладной уровень обеспечивает прикладным процессам средства доступа к области взаимодействия, является верхним (седьмым) уровнем и непосредственно примыкает к прикладным процессам. 2. В действительности прикладной уровень – это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, например, таким как файлы или гипертекстовые Web-страницы и т.д., а также организуют свою совместную работу, например, с помощью протокола электронной почты, или FTP и т.д. 3. Одна из основных задач этого уровня - определить, как следует обрабатывать запрос прикладной программы, другими словами, какой вид должен принять данный запрос.4. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением (message).

**Прикладной уровень выполняет следующие функции:**описание форм и методов взаимодействия прикладных процессов;согласование требований к различным видам работ (например, передача файлов, управление заданиями, управление системой и т.д.) и управление ими.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.

Можно говорить, что прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является перенос файлов, обмен почтовыми сообщениями, управление сетью и т.д. **Прикладной уровень. Функции**К числу наиболее распространенных протоколов верхних трех уровней относятся:HTTP (HyperText Transfer Protocol) — протокол прикладного уровня передачи данных, изначально в виде гипертекстовых документов в формате HTML, в настоящее время используется для передачи произвольных данных;FTP (File Transfer Protocol) — протокол передачи файлов по сети;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;POP3 (Post Office Protocol, Version 3) — стандартный протокол, используемый клиентами электронной почты для получения почты с удалённого сервера по TCP-соединению;IMAP4 (Internet Message Access Protocol, Version 4) —  протокол прикладного уровня для доступа к электронной почте;CMIP (Common Management Information Protocol) — общий протокол управления информацией;SNMP (Simple Network Management Protocol) — простой протокол сетевого управления;FTAM (File Transfer, Access, and Management) — протокол передачи, доступа и управления файлами.

1. Уровни модели OSI: уровень представления данных (Presentation layer)

1. Уровень представления данных или представительский уровень представляет данные, передаваемые между прикладными процессами, в нужной форме.2. 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. 3. 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.

4. 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.5. Представительский уровень обеспечивает преобразование данных (кодирование, компрессия и т.п.), поступающих с прикладного уровня, в соответствующую форму, которые далее в виде потока информации поступают на транспортный уровень.

**Представительный уровень выполняет следующие основные функции:**генерация запросов на установление сеансов взаимодействия прикладных процессов;согласование представления данных между прикладными процессами;реализация форм представления данных;преобразование данных (кодирование, компрессия и т.д.);засекречивание данных (шифрование);передача запросов при необходимости на прекращение сеансов.

1. Уровни модели OSI: сеансовый уровень (Session layer).

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

Аспекты:1. 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.2. Сеансовый уровень управляет сеансом передачи информации между прикладными процессами, координирует прием, передачу и выдачу одного сеанса связи. Кроме того, сеансовый уровень может содержать дополнительно функции управления паролями, управления диалогом, синхронизации и отмены связи в сеансе передачи после сбоя вследствие ошибок в нижерасположенных уровнях. 3. На сеансовом уровне определяется, какой будет передача между двумя прикладными процессами:полудуплексной (процессы будут передавать и принимать данные по очереди) − сеансовый уровень выдает маркер данных тому процессу, который начинает передачу; когда второму процессу приходит время отвечать, маркер данных передается ему; разрешается передача только той стороне, которая обладает маркером данных;дуплексной (процессы будут передавать данные, и принимать их одновременно).

**Сеансовый уровень обеспечивает выполнение следующих функций:**установление и завершение на сеансовом уровне соединения между взаимодействующими системами;управление выполнением 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.

Протоколы сеансового уровня обычно являются составной частью протоколов трех верхних уровней модели. Но есть и отдельные протоколы, относящиеся прежде всего к сеансовому уровню:ADSP (AppleTalk Data Stream);ASP (AppleTalk Session);RPC (Remote Procedure Call);PAP (Password Authentication Protocol).

1. Уровни модели OSI: транспортный уровень (Transport Layer)

1. Транспортный уровень предназначен для управления передачей пакетов через коммуникационную сеть. 2. На транспортном уровне сообщение (message), приходящее с вышележащих уровней, разбивается на блоки. Фактически это является началом формирования пакета.3. На пути от отправителя к получателю пакеты могут быть искажены или утеряны. 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. 4. 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.

Данный уровень гарантирует доставку блоков информации адресатам и управляет этой доставкой. Фактически, 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 данных;-       обнаружение ошибок, частичная их ликвидация (за счет использование избыточных кодов) и сообщение о неисправленных ошибках;-       восстановление передачи после отказов и неисправностей;-       укрупнение блоков или разделение данных на блоки;-       предоставление приоритетов при передаче (нормальная или срочная);-       подтверждение передачи;-       ликвидация передаваемых структур 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:TCP (Transmission Control Protocol) протокол управления передачей стека TCP/IP;UDP (User Datagram Protocol) пользовательский протокол дейтаграмм стека TCP/IP;NCP (NetWare Core Protocol) базовый протокол сетей NetWare;SPX (Sequenced Packet eXchange) упорядоченный обмен пакетами стека Novell;SCTP (Stream Control Transmission Protocol);TP4 (Transmission Protocol) – протокол передачи класса 4.

1. Уровни модели OSI: сетевой уровень (Network Layer).

1. Сетевой уровень обеспечивает прокладку виртуальных каналов, соединяющих абонентские и административные системы через коммуникационную сеть, выбор маршрута наиболее быстрого и надежного пути передачи данных.2. Виртуальный или логический канал − это такое функционирование компонентов сети, которое создает взаимодействующим компонентам иллюзию прокладки между ними нужного тракта. 3. 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.4. Время передачи, как главный критерий выбора маршрута, 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.5. Сетевой уровень сообщает транспортному уровню о появляющихся ошибках, связанных с адресацией и маршрутизацией.

6. Сообщения на сетевом уровне принято называть пакетами (packet). В них помещаются фрагменты (блоки) данных. Сетевой уровень отвечает за их адресацию и маршрутизацию.7. Для регулирования доставки данных внутри сети достаточно канального уровня и его протоколов (передавать данные можно по физическому (MAC) адресу), а вот доставкой данных между сетями занимается именно сетевой уровень, т.к. данный процесс требует определение оптимального маршрута передачи – при этом используется именно сетевой, а не физический, адрес, который состоит из номера сети и номера компьютера в этой сети. Соответственно сетевой уровень должен уметь выполнять преобразования MAC-адресов в сетевые адреса и обратно.

8. На практике 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.9. Сетевой уровень также отвечает за деление пользователей на группы.10. Сетевой уровень обеспечивает также прозрачную передачу пакетов на транспортный уровень.

**Сетевой уровень выполняет функции:** Создание сетевых соединений и идентификация их портов.Обнаружение и исправление ошибок (связанных с адресацией и маршрутизацией), возникающих при передаче через коммуникационную сеть.Управление потоками пакетов.Организация (упорядочение) последовательностей пакетов.Маршрутизация и коммутация.Сегментирование и объединение пакетов.

**На сетевом уровне определяется два вида протоколов.** Определение 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). Протоколы обмена маршрутной информацией. С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений, о состоянии сети, траффике в определенных точках сети, каналах и т.д.

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

**Наиболее часто на сетевом уровне используются протоколы:**  IP (Internet Protocol) протокол Internet, сетевой протокол стека TCP/IP, который предоставляет адресную и маршрутную информацию; IPX (Internetwork Packet Exchange) протокол межсетевого обмена пакетами, предназначенный для адресации и маршрутизации пакетов в сетях Novell; X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов (частично этот протокол реализован на канальном уровне);CLNP (Connection Less Network Protocol) сетевой протокол без организации соединений.

1. Уровни модели OSI: канальный уровень (Data Link)

1. Главная задача канального уровня − брать пакеты, поступающие с сетевого уровня и готовить их к передаче, укладывая в кадр соответствующего размера, который далее передается физическому уровню. Этот уровень обязан определить, где начинается и где заканчивается блок, а также обнаруживать ошибки передачи.

2. Поэтому, единицей информации канального уровня являются кадры (frame). Фактически, кадры – это логически организованная структура, в которую можно помещать данные.

3. На физическом уровне просто пересылаются биты в виде физических сигналов. 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 определение доступ к среде и управление передачей посредством процедуры передачи данных по каналу.

4. 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.

5. 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.

6. На этом же уровне определяются правила использования физического уровня узлами сети. Физическое (электрическое) представление данных в сетях (биты данных, методы кодирования данных и маркеры) распознаются на этом и только на этом уровне.

**Спецификации IEEE 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, обнаружение коллизий или столкновений) и управляет доступом к каналу связи. Подуровень LLC находится выше подуровня МАC.

**Канальный уровень может выполнять следующие виды функций:**  Организация (установление, управление, расторжение) канальных соединений и идентификация их портов.Формирование и передача кадров.Обнаружение и исправление ошибок.Управление потоками данных.Обеспечение прозрачности логических каналов (передачи по ним данных, закодированных любым способом).

HDLC (High Level Data Link Control) протокол управления каналом передачи данных высокого уровня, для последовательных соединений;PPP (Point-To-Point Protocol, протокол прямого соединения между двумя узлами);SLIP (Serial Line Internet Protocol, по сути, предшественник PPP, который по-прежнему используется в микроконтроллерах);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;FDDI (Fiber Distributed Date Interface Station) сетевая технология по стандарту IEEE 802.6, использующая оптоволоконный носитель;X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов.

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.

1. Уровни модели OSI: физический уровень (Physical Layer).

1. 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.

2. Физический уровень состоит из Подуровня стыковки со средой и Подуровня преобразования передачи. Первый из них обеспечивает сопряжение потока данных с используемым физическим каналом связи. Второй осуществляет преобразования, связанные с применяемыми протоколами. 3. Физический уровень обеспечивает физический интерфейс с каналом передачи данных, а также описывает процедуры передачи сигналов в канал и получения их из канала. 4. На этом уровне определяются электрические, механические, функциональные и процедурные параметры для физической связи в системах. Фактически, физический уровень получает пакеты данных от вышележащего канального уровня и преобразует их в оптические или электрические сигналы, соответствующие 0 и 1 бинарного потока.

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:**  Установление и разъединение физических соединений. Передача сигналов в последовательном коде и прием. Прослушивание, в нужных случаях, каналов. Идентификация каналов. 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.).

**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.

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

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.

Преобразование данных в сигналы, передающие по кабелю в глобальных сетях выполняют модемы. В локальных сетях для преобразования данных применяют сетевые адаптеры, обеспечивающие скоростную передачу данных в цифровой форме.

Fu1

В ряде случаев для более четкого опре-деления структуры физи-ческий уровень разби-вается на несколько подуровней. Например, физический уровень беспроводной сети делится на три подуровня.

Физический уровень может обеспечивать как асинхронную (последовательную) так и синхронную (параллельную) передачу.

К числу наиболее распространенных спецификаций физического уровня относятся: 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;FDDI (Fiber Distributed Date Interface Station) сетевая технология по стандарту IEEE 802.6, использующая оптоволоконный носитель. и т.д.Краткое описание функций уровней модели OSI

|  |  |  |
| --- | --- | --- |
| Наименование  уровня | Функция | Тип данных (PDU, protocol data units) |
| Прикладной | Представляет набор интерфейсов, позволяющий получить  доступ к сетевым службам. Согласует требования к процессу передачи и т.д. | Сообщение (message) |
| Представления | Преобразует данные, например, в общий формат, засекречивает и т.д. | Сообщение (message) |
| Сеансовый | Поддержка взаимодействия (сеанса) между процессами | Сообщение (message) |
| Транспортный | Управляет передачей данных по сети, обеспечивает требуемый  уровень надежности (исправление ошибок, подтверждение передачи и т.д.) | Блоки / Дейтаграммы  Разбиение сообщения на блоки  фактически является началом процесса  формирования пакета |
| Сетевой | Маршрутизация, управление потоками данных, адресации  сообщений для доставки, преобразование логических сетевых адресов  и имен в соответствующие им физические | Пакет (packet) |
| Канальный | Управляет формирование кадров (LLC) и доступом к среде (MAC) | Кадр (frame) |
| Физический | Битовые протоколы передачи данных. Передача и приём потока байтов  через физическое устройство. Контроль (физический, технический)  за процессом передачи | На «входе» кадр в виде набора бит  данных, на «выходе» – физический сигнал |

1. Спецификации стандартов 802.1 – 802.10

Стандарт IEEE 802.1 (Internetworking – объединение сетей) задает механизмы управления сетью на MAC-уровне. Стандарт IEEE 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 IEEE 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 множественный доступ с прослушиванием несущей и обнаружением коллизий.

Стандарт IEEE 802.4 (Token Bus LAN – локальные сети Token Bus) определяет метод доступа к шине с передачей маркера. Прототипом сети является ArcNet.Стандарт IEEE 802.5 (Token Ring LAN – локальные сети Token Ring) описывает метод доступа к кольцу с передачей маркера, прототип – Token Ring.Стандарт IEEE 802.6 (Metropolitan Area Network – городские или муниципальные сети) описывает рекомендации для региональных сетей.Стандарт IEEE 802.7 (Broadband Technical Advisory Group – техническая консультационная группа по широковещательной передаче) описывает рекомендации по широкополосным сетевым технологиям, носителям, интерфейсу и оборудованию.

Стандарт IEEE 802.8 (Fiber Technical Advisory Group –техническая консультационная группа по оптоволоконным сетям) содержит обсуждение использования оптических кабелей в сетях со стандартом 802.3 – 802.6, а также рекомендации по оптоволоконным сетевым технологиям, носителям, интерфейсу и оборудованию, прототип – сеть FDDI (Fiber Distributed Data Interface).Стандарт IEEE 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 IEEE 802.10 (Network Security – сетевая безопасность) рассмотрены вопросы обмена данными, шифрования (на основе криптографического преобразования информации), управления сетями и безопасности в сетевых архитектурах, совместимых с моделью OSI.

1. Спецификации стандартов 802.11 – 802.22.

Стандарт IEEE 802.11 (Wireless Network – беспроводные сети) описывает рекомендации по использованию беспроводных сетей.Стандарт IEEE 802.12 описывает рекомендации по использованию сетей 100VG – AnyLAN со скоростью100 Мб/с и методом доступа по очереди запросов и по приоритету (Demand Priority Queuing – DPQ, Demand Priority Access – DPA).

Стандарт IEEE 802.14 определяет функционирование кабельных модемов.Стандарт IEEE 802.15 (PAN – Personal Area Network, персональные сети) рассматривает вопросы организации персональных сетей. В настоящее время уже существует несколько спецификаций данного стандарта.Стандарт IEEE 802.16 предназначен для реализации широкополосных каналов в городских сетях (MAN). В отличии от 802.11 он ориентирован для соединения стационарных, а не мобильных объектов. Его задачей является обеспечения сетевого уровня между локальными сетями (IEEE 802.11) и региональными сетями (WAN), где планируется применение разрабатываемого стандарта IEEE802.20. Эти стандарты совместно со стандартом IEEE 802.15 и 802.17 образуют взаимосогласованную иерархию протоколов беспроводной связи.

Стандарт IEEE 802.17 называется RPR (Resilient Packet Ring –адаптивное кольцо для пакетов), и в отличие от FDDI (а также Token Ring или DQDB) пакеты удаляются из кольца узлом-адресатом, что позволяет осуществлять несколько обменов одновременно.Стандарт IEEE 802.18  представляет собой требования и рекомендации технической консультативной группы по радиочастотному регулированию – RTAG (Radio Regulatory Technical Advisory Group).Стандарт IEEE 802.19 представляет собой  требования и рекомендации технической консультативной группы по сосуществованию – CTAG (Coexistence Technical Advisory Group).

Стандарт IEEE 802.20 описывает правила беспроводного мобильного широкополосного доступа MBWA (Mobile Broadband Wireless Access) для пакетного интерфейса в беспроводных городских сетях WMAN. Этот стандарт должен поддерживать услуги по передаче данных с IP в качестве транспортного протокола и дополнять стандарт IEEE 802.16 в масштабе WiMAX. Стандарт IEEE 802.21 – это стандарт независимой от среды эстафетной передаче соединений – MIHS (Media Independent Handover Services).Стандарт IEEE 802.22 – определяет функционирование беспроводных региональных сетей WRAN (Wireless Regional Area Network), использующих для передачи данных телевизионные частотные диапазоны.

1. Понятия протоколов и стеков протоколов. Сетевые протоколы. Транспортные протоколы. Прикладные протоколы.

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

Примерами популярных стеков протоколов могут служить стек IPX/SPX фирмы Novell, стек TCP/IP.

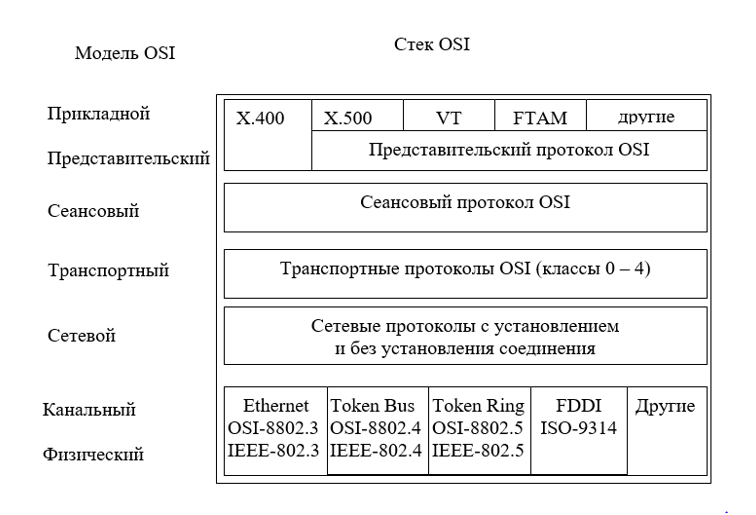
В общем случае можно выделить три укрупненных уровня протоколов, характерных в той или иной степени для любых стеков:сетевые;транспортные; прикладные.

**Сетевые протоколы** предоставляют следующие услуги: адресацию и маршрутизацию информации, проверку на наличие ошибок, запрос повторной передачи и установление правил взаимодействия в конкретной сетевой среде. DDP (Datagram Delivery Protocol – Протокол доставки дейтаграмм). Протокол передачи данных Apple, используемый в Apple Talk. IP (Internet Protocol – Протокол Internet). Протокол стека TCP/IP, обеспечивающий адресную информацию и информацию о маршрутизации. IPX (Internetwork Packet eXchange – Межсетевой обмен пакетами) в NWLink. Протокол Novel NetWare, используемый для маршрутизации и направления пакетов. NetBEUI (NetBIOS Extended User Interface – расширенный пользовательский интерфейс базовой сетевой системы ввода вывода). Разработанный совместно IBM и Microsoft, этот протокол обеспечивает транспортные услуги для NetBIOS.

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

**Прикладные протоколы** отвечают за взаимодействие приложений.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.

Стек OSI – это набор вполне конкретных спецификаций протоколов, образующих согласованный стек протоколов. Этот стек протоколов поддерживает правительство США в своей программе GOSIP.



1. Архитектура стека протоколов Microsoft TCP/IP.
2. Стек TCP/IP: уровень приложения, уровень транспорта
3. Стек TCP/IP: межсетевой уровень, уровень сетевого интерфейса.
4. Символьная адресация в сетях. Отличие DNS-имени от NetBios имен. Структура DNS-имени.
5. Принципы разрешения DNS-имени.
6. Структура IPv4. Классы IP-адресов.
7. Понятие маски. Правила использование масок. Определение NetworkID и HostID с использованием масок.
8. Структурирование сетей с помощью масок.
9. Особые IP-адреса. Понятие частных сетей. Диапазоны частных адресов.
10. Адресация IPv6. Особенности. Текстовое представление адреса. Типы IPv6 адресов.
11. Unicast и Anycast IPv6 адреса.
12. Multicast IPv6 адреса.
13. Кабель типа «витая пара» (twisted pair). Схемы разводки. Кабельные системы Ethernet.
14. Кабели и структурированные кабельные системы. Коаксиальные кабели.
15. Сетевые адаптеры (Network Interface Card). Назначение и функции сетевых адаптеров. Типы сетевых адаптеров.
16. Повторители и концентраторы. Назначение и особенности использования.
17. Мосты. Назначение и особенности использования. Различие между мостом и коммутатором. Различия между маршрутизаторами и мостами.
18. Коммутаторы. Назначение и особенности использования.
19. Маршрутизаторы. Назначение. Особенности использования. Шлюзы. Назначение и особенности использования.
20. Беспроводные технологии: радиосвязь, инфракрасная, связь в микроволновом диапазоне. Достоинства и недостатки беспроводных сетей wi-fi.
21. Сети Wi-Fi стандарта IEEE802.11a и IEEE802.11b.
22. Сети Wi-Fi стандарта IEEE802.11g и IEEE802.11n.
23. Сети cтандарта IEEE802.11ac. Сети стандарта IEEE802.11ax.
24. Сети Wi-Fi. Стандарты IEEE802.11h, IEEE802.11i, IEEE802.11j, IEEE802.11d, IEEE802.11e, IEEE802.11f.
25. Оборудование для сетей Wi-Fi.
26. Особенности оптических систем связи (физические, технические). Достоинства и недостатки оптических систем связи.
27. Оптический кабель: его разновидности и характеристики.
28. Защита информации. Основные понятия. Виды основных сетевых атак.
29. Классификация средств защиты информации.
30. Понятие шифрования. Классические алгоритмы шифрования данных (подстановка, перестановка, гаммирование).
31. Стандартные методы шифрования и криптографические системы.