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

*Сеть* – это совокупность объектов, образуемых устройствами передачи и обработки данных.

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

Локальные вычислительные сети (ЛВС), расположенные в одном или нескольких близко расположенных зданиях. ЛВС обычно размещаются в рамках какой-либо организации, поэтому их называют корпоративными.

Распределенные компьютерные сети, глобальные, 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 состав сети в общем случае включается следующие элементы:

* сетевые компьютеры;
* каналы связи;
* различного рода преобразователи сигналов;
* сетевое оборудование.

Различают два понятия сети: *коммуникационная сеть* и *информационная сеть*.

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

На базе коммуникационной сети может быть построена группа информационных сетей:

Под *информационной системой* следует понимать систему, которая является поставщиком или потребителем информации. Компьютерная сеть состоит из *информационных систем* и *каналов связи*.

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

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

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

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

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

Загрузка сети характеризуется параметром, называемым *трафиком*.

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

Существенное влияние на характеристику сети оказывает *метод доступа*.

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

В сети все рабочие станции физически соединены между собою каналами связи по определенной структуре, называемой *топологией*.

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

Состав основных элементов в сети зависит от ее архитектуры.

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

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

Компьютерные сети представляют собой вариант сотрудничества людей и компьютеров, обеспечивающего ускорение доставки и обработки информации. С помощью сетей можно разделять ресурсы и информацию. Компьютерная сеть позволяет работать с многопользовательскими программами, обеспечивающими одновременный доступ всех пользователей к общим базам данных с блокировкой файлов и записей, обеспечивающей целостность данных.

1. Архитектура терминал – главный компьютер.

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

В данном курсе будет рассмотрено три вида архитектур:

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

Архитектура терминал – главный компьютер – это концепция информационной сети, в которой вся обработка данных осуществляется одним или группой главных компьютеров.

Рассматриваемая архитектура предполагает два типа оборудования:

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

*Главный компьютер* через мультиплексоры передачи данных (МПД) взаимодействуют с терминалами.

Классический пример архитектуры сети с главными компьютерами – системная сетевая архитектура.

1. Одноранговая архитектура.

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

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

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

Одноранговые сети имеют следующие преимущества:

они легки в установке и настройке;

отдельные ПК не зависят от выделенного сервера;

пользователи в состоянии контролировать свои ресурсы;

малая стоимость и легкая эксплуатация;

минимум оборудования и программного обеспечения;

нет необходимости в администраторе;

хорошо подходят для сетей с количеством пользователей, не превышающим десяти.

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

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

1. Архитектура клиент – сервер.

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

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

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.

*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 NT фирмы Microsoft;

Linux.

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

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

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

Сети клиент – серверной архитектуры имеют следующие преимущества:

позволяют организовывать сети с большим количеством рабочих станций;

обеспечивают централизованное управление учетными записями пользователей, безопасностью и доступом, что упрощает сетевое администрирование;

эффективный доступ к сетевым ресурсам;

пользователю нужен один пароль для входа в сеть и для получения доступа ко всем ресурсам, на которые распространяются права пользователя.

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

неисправность сервера может сделать сеть неработоспособной, как минимум потерю сетевых ресурсов;

требуют квалифицированного персонала для администрирования;

имеют более высокую стоимость сетей и сетевого оборудования.

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;

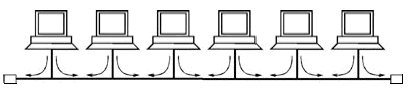
выбор оптимального маршрута передачи блоков данных;

предоставление приемлемого времени ответа и нужной пропускной способности.

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

Общая шина

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. 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.

1. Топология кольцо. Топология цепочка.

*Кольцо –* это топология ЛВС, в которой каждая станция соединена с двумя другими станциями, образуя кольцо (рис.2.3).

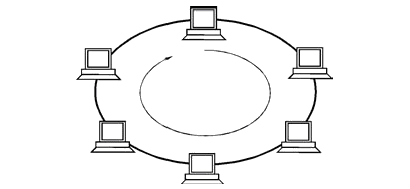


Рис. 2.3. Топология «*Кольцо*»

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

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

Также стоит упомянуть в качестве отдельной топологию «цепочка», представляющую «разомкнутое» кольцо (рис. 2.4).



Рис. 2.4. Топология «*Цепочка*»

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

1. Звездообразные топологии.

*Звезда –* это топология ЛВС (рис. 2.5), в которой все *рабочие станции* присоединены к центральному узлу (устройству), например, к концентратору или коммутатору, который устанавливает, поддерживает и разрывает связи между рабочими станциями. Преимуществом такой топологии является возможность простого исключения неисправного *узла*. Однако, если неисправен центральный узел, вся сеть выходит из строя.

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

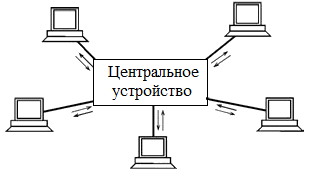


Рис. 2.5. Топология «*Звезда*»

Центром *Звезды* обычно является концентратор(hub).

Если в качестве центрального устройства в топологии «звезда» выступает коммутатор или компьютер, то ее называют «активной звездой», если же используется устройство типа концентратов, то «пассивной звездой».

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

Однако звездообразная топология имеет и недостатки. Во-первых, она требует много кабеля. Во-вторых, центральные устройства в случае использования коммутатора будут довольно дороги. В-третьих, кабельные концентраторы и коммутаторы при большом количестве кабеля трудно обслуживать. Однако в большинстве случаев в такой топологии используется недорогой кабель типа *витая пара*. В некоторых случаях можно даже использовать существующие телефонные кабели. Кроме того, для диагностики и тестирования выгодно собирать все кабельные концы в одном месте.

Еще одним недостатком можно выделить ограниченность расширения сети на основе топологии «звезда», так как и концентраторы, и коммутаторы в определенной степени ограничены по числу портов. Возможно последовательное соединение нескольких «звезд» через центральные устройства, но при большом числе соединенных «звезд» могут возникнуть сложности с передачей между удаленными узлами.

1. Древовидные топологии.

Топологию «**дерево**» (tree) в общем случае можно рассматривать как комбинацию нескольких звезд. Причем, как и в случае «звезды», «дерево» может быть активным или истинным (рис. 2.6).

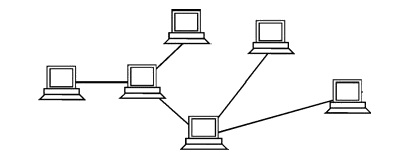


Рис. 2.6. Топология «активное дерево»

Также «дерево» может быть пассивным (рис. 2.7). При ***«активном дереве»*** в центрах объединения нескольких линий связи находятся центральные компьютеры или коммутаторы, а при «***пассивном»*** – концентраторы (хабы).

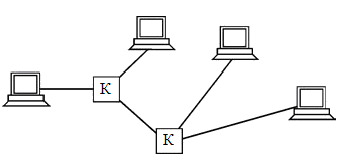


Рис. 2.7. Топология «пассивное дерево» (К – концентраторы)

Однако в отличии от вариаций звездообразной топологии, все древовидные топологии предполагают иерархическую структуру со строго выделенной вершиной дерева. При этом надо отметить, что использовать древовидную топологию, как активную, так и пассивную, целесообразно при большом числе узлов (при малом числе узлов эффективна будет топология «звезда»). Так, например, «активное» и «пассивное» дерево в таком случае может выглядеть следующим образом (рис. 2.8 и 2.9 соответственно).

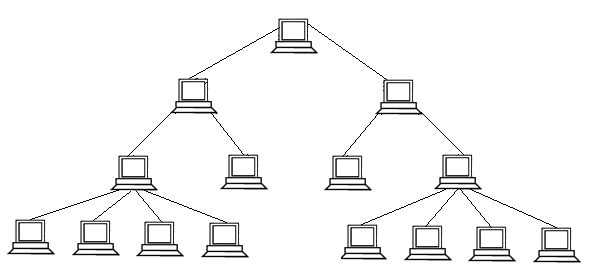


Рис. 2.8. Топология «активное» дерево с большим числом узлов

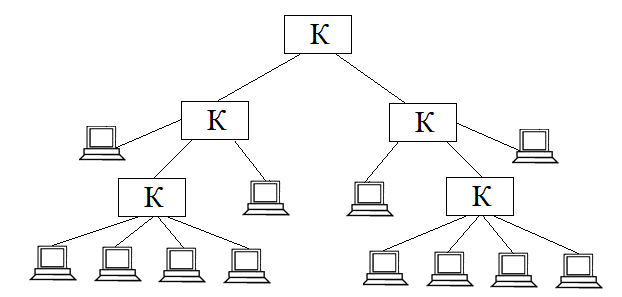


Рис. 2.9. Топология «пассивное» дерево с большим числом узлов

Также отметим, что на практике эффективно исполнять роль вершины дерева в пассивном варианте топологии устройство типа «концентратор» не может – целесообразно использовать «коммутатор».

Еще одной разновидностью древовидных сетевых топология является топология «***fat tree»*** (утолщенное дерево), изобретенная Чарльзом Лейзорсоном. НА практике она является дешевой и эффективной основой для построения суперкомпьютеров (рис. 2.10).

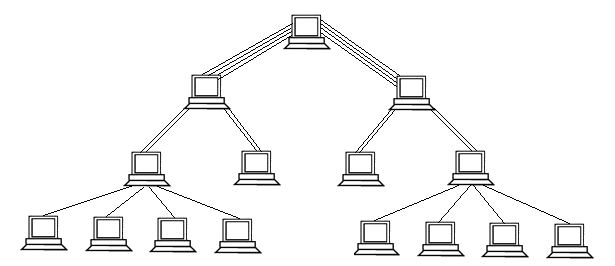


Рис. 2.10. Топология «fat tree»

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. Сети с топологией «fat tree» являются предпочтительными для построения кластерных межсоединений.

1. Ячеистые топологии.

В *сеточной* (**ячеистой**) (mesh) топологии компьютеры связываются между собой не одной, а многими линиями связи, образующими сетку (рис. 2.11).

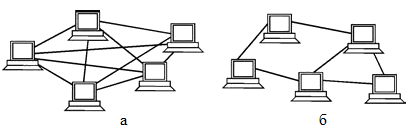


Рис. 2.11. Сеточная топология: полная (а) и частичная (б)

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.

В заключение несколько слов о ***решетчетой*** топологии, 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.

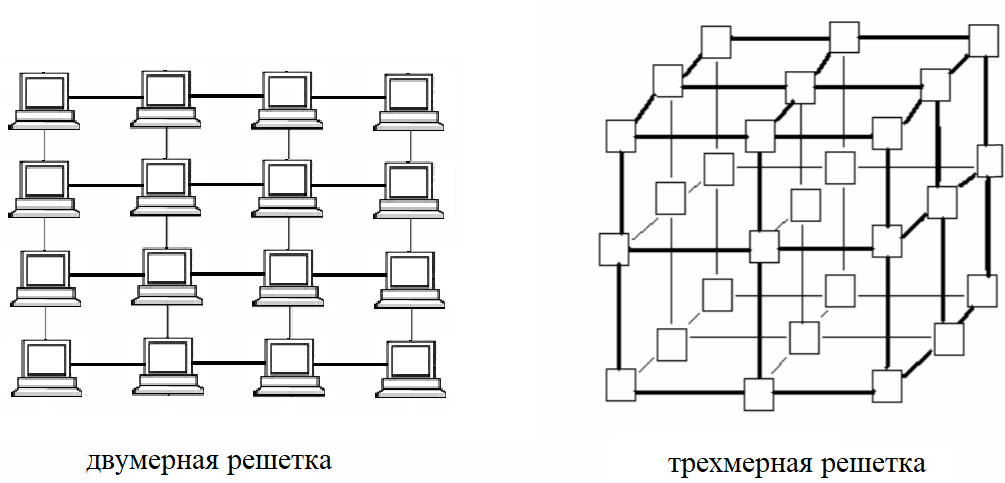


Рис. 2.12 Пример сетевых топологий типа двумерная и трехмерная решетка

Многомерная решетка, соединенная циклически в более чем одном измерении, называется «тор».

Основным достоинством топологии «решетка» является высокая надежность, а недостатком – сложность реализации.

1. Комбинированные топологии.

Довольно часто применяются комбинированные топологии, среди которых наиболее распространены «*звездно-шинная»* (star – bus) (рис. 2.13) и «*звездно-кольцевая»* (star – ring) (рис. 2.14).

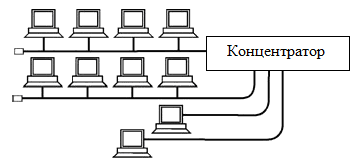


Рис. 2.13. Пример «звездно-шинной» топологии

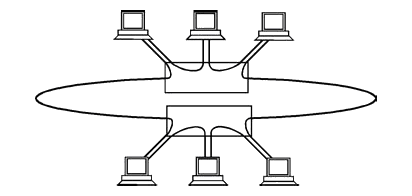


Рис. 2.14. Пример «звездно-кольцевой» топологии

В «звездно – шинной» топологии используется комбинация шины и «пассивной звезды». К концентратору подключаются как отдельные компьютеры, так и целые шинные сегменты. На самом деле реализуется физическая топология шина, включающая все компьютеры сети. 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». Таким образом, пользователь может гибко комбинировать преимущества шинной и звездной топологий, а также легко изменять количество компьютеров, подключенных к сети. С точки зрения распространения информации данная топология равноценна классической шине.

В случае звездно – кольцевой топологии в кольцо объединяются не сами компьютеры, а специальные концентраторы (прямоугольник на рис. 2.14), 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. Например, концентраторы позволяют собрать в одно место все точки подключения кабелей сети. Если говорить о распространении информации, данная топология равноценна классическому кольцу.

1. Метод доступа CSMA/CD.

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.

В современных сетях в основном используются следующие методы доступа:

* *множественный доступ с прослушиванием несущей* (Carrier Sense Multiple Access),который будет рассмотрен в двух вариантах: *множественный доступ с прослушиванием несущей и разрешением коллизий* (Carrier Sense Multiple Access with Collision Detection –CSMA/CD) и *множественный доступ с прослушиванием несущей и предотвращением коллизий* (Carrier Sense Multiple Access with With Collision Avoidance – CSMA/CA);
* *централизованный метод доступа* (Demand Priority, DP);
* *множественный доступ с передачей полномочия* (Token Passing Multiple Access – TPMA), или метод с передачей *маркера*;
* *множественный доступ с разделением во времени* (Time Division Multiple Access – TDMA);
* *множественный доступ с разделением частоты* (Frequency Division Multiple Access – FDMA), или *множественный доступ с разделением длины волны* (Wavelength Division Multiple Access – WDMA).

В компьютерных сетях могут быть использованы различные варианты реализации метода множественного доступа с прослушиванием несущей (CSMA). Первый из них − CSMA/CD.

***Метод множественного доступа* *с прослушиванием несущей*** ***и* *разрешением коллизий*** (***CSMA/CD***) основан на следующих правилах определени права на передачу: если рабочая станция «хочет» воспользоваться сетью для передачи данных, она сначала должна проверить состояние канала, начинать передачу рабочая станция может, если канал свободен.

В процессе передачи рабочая станция продолжает прослушивание сети для обнаружения возможных конфликтов (коллизий). Если возникает конфликт из-за того, что два узла попытаются занять канал, то обнаружившая конфликт интерфейсная плата соответствующего компьютера выдает в сеть специальный сигнал и обе станции одновременно прекращают передачу. Принимающая рабочая станция отбрасывает частично принятое сообщение, а все рабочие станции, желающие передать сообщение, в течение некоторого случайно выбранного промежутка времени выжидают, прежде чем начать сообщение.

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

***Метод*** ***множественного доступа* *с прослушиванием несущей*** **и *предотвращением коллизий*** ***(CSMA/CA)*** в отличии от CSMA/CD характеризуется следующими основновными особенностями:

* станция, которая собирается начать передачу, посылает jam signal (сигнал затора);
* после продолжительного ожидания всех станций, которые могут послать jam signal, станция начинает передачу;
* если во время передачи станция обнаруживает jam signal от другой станции, она останавливает передачу на отрезок времени случайной длины и затем повторяет попытку.

В сущности, CSMA/CA отличается от CSMA/CD тем, что узлы сообщают о намерении передать данные по сети до фактической их передачи. Узлы постоянно «прослушивают» объявления других узлов и при обнаружении объявления отменяют передачу своих данных.

В таком случае при использовании CSMA/CA коллизиям подвержены не пакеты данных, а только jam-сигналы. Избегание коллизий используется для того, чтобы улучшить производительность CSMA. Улучшение производительности достигается за счет снижения вероятности коллизий и повторных попыток передачи. Но ожидание jam signal создает дополнительные задержки, поэтому другие методы доступа позволяют достичь лучших результатов. Избегание коллизий полезно на практике в тех ситуациях, когда своевременное обнаружение коллизии невозможно.

*Централизованный метод доступа Demand Priority*

Развитием метода CSMA/CD является *централизованный метод доступа* (Demand Priority, DP), в котором концентратор выступает в роли «арбитра» − проблема доступа к разделяемой среде решается через передачу запросов концентратору, который циклически прослушивает всех абонентов по очереди и дает право передачи абоненту, следующему по порядку за тем, который закончил передачу. В данном методе доступа реализованы два уровня приоритетов: низкий − для обычных приложений и высокий − для мультимедийных.

1. Метод доступа TPMA.

**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.

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.

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 *сети*.

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*. После чего 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. Таким образом, в *сети* с передачей маркера невозможны коллизии (конфликты). Метод с передачей маркера в основном используется в кольцевой топологии.

Данный метод характеризуется следующими достоинствами:

гарантирует определенное время доставки блоков данных в сети;

дает возможность предоставления различных приоритетов передачи данных.

Вместе с тем он имеет существенные недостатки:

в сети возможны потеря маркера, а также появление нескольких маркеров, при этом сеть прекращает работу;

включение новой рабочей станции и отключение связаны с изменением адресов всей системы.

1. Метод доступа TDMA.

Множественный доступ с разделением во времени основан на распределении времени работы канала между системами (рис. 2.17).

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

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

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

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

1. Метод доступа FDMA и WDMA.

Доступ *FDMA* основан на разделении полосы пропускания канала на группу полос частот (рис. 2.18), 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.

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.

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

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. Это время ожидания абонентом начала своей передачи.

В процессе сеанса обмена информацией по сети между передающим и принимающим абонентами происходит обмен информационными и управляющими пакетами по установленным правилам, называемым *протоколом обмена*. Это позволяет обеспечить надежную передачу информации при любой интенсивности обмена по сети.

При реальном обмене по сети применяются многоуровневые протоколы, каждый из уровней которых предполагает свою структуру пакета. Ведь протоколы высоких уровней имеют дело с такими понятиями, как файл-сервер или приложение, запрашивающее данные у другого приложения, и вполне могут не иметь представления ни о типе аппаратуры сети, ни о методе управления обменом. Все пакеты более высоких уровней последовательно вкладываются в передаваемый пакет, точнее, в поле данных передаваемого пакета (рис. 6). Этот процесс последовательной упаковки данных для передачи называется также инкапсуляцией пакетов**.**

Обратный процесс последовательной распаковки данных приемником называется *декапсуляцией* пакетов*.*

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.

Чаще всего пакет содержит в себе следующие основные поля или части.

1. MAC-адреса и их структура.

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

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

Базовая 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. OSI разделяет коммуникационные функции в сети на семь уровней, каждый из которых обслуживает различные части процесса области взаимодействия открытых систем.

Модель OSI можно разделить на две различных модели:

* 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 действительности взаимодействие осуществляется между смежными уровнями одного компьютера.

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

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

Прикладной уровень обеспечивает прикладным процессам средства доступа к области взаимодействия, является верхним (седьмым) уровнем и непосредственно примыкает к прикладным процессам. 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:

1. Описание форм и методов взаимодействия прикладных процессов.
2. Согласование требований к различным видам работ (например, передача файлов, управление заданиями, управление системой и т.д.) и управление ими.
3. Идентификация пользователей по их паролям, адресам, электронным подписям;
4. Определение функционирующих абонентов и возможности доступа к новым прикладным процессам;
5. Определение достаточности имеющихся ресурсов;
6. Организация запросов на соединение с другими прикладными процессами;
7. Передача заявок представительскому уровню на необходимые методы описания информации;
8. Выбор процедур планируемого диалога процессов;
9. Управление данными, которыми обмениваются прикладные процессы и синхронизация взаимодействия прикладных процессов;
10. Определение качества обслуживания (время доставки блоков данных, допустимой частоты ошибок);
11. Соглашение об исправлении ошибок и определении достоверности данных;
12. Согласование ограничений, накладываемых на синтаксис (наборы символов, структура данных).

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

1. Уровни модели OSI: 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.

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.

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

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

## 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. На практике немногие приложения используют сеансовый уровень, и он редко реализуется.

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

*полудуплексной* (процессы будут передавать и принимать данные по очереди)

*дуплексной* (процессы будут передавать данные, и принимать их одновременно).

Сеансовый уровень обеспечивает выполнение следующих функций:

1. Установление и завершение на сеансовом уровне соединения между взаимодействующими системами.
2. Управление выполнением нормального и срочного обмена данными между прикладными процессами.
3. Управление взаимодействием прикладных процессов.
4. Синхронизация сеансовых соединений.
5. Извещение прикладных процессов об исключительных ситуациях, касающихся сеанса связи.
6. Установление в прикладном процессе меток, позволяющих после отказа либо ошибки восстановить его выполнение от ближайшей метки.
7. Прерывание в нужных случаях прикладного процесса и его корректное возобновление.
8. Прекращение сеанса без потери данных.
9. Передача особых сообщений о ходе проведения сеанса.
10. Уровни модели OSI: транспортный уровень (Transport Layer)

Транспортный уровень предназначен для управления передачей пакетов через коммуникационную сеть. На транспортном уровне сообщение (message), приходящее с вышележащих уровней, разбивается на блоки. Фактически это является началом формирования пакета.

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 данных;

1. Обнаружение ошибок, частичная их ликвидация (за счет использование избыточных кодов) и сообщение о неисправленных ошибках.
2. Восстановление передачи после отказов и неисправностей.
3. Укрупнение блоков или разделение данных на блоки.
4. Предоставление приоритетов при передаче (нормальная или срочная).
5. Подтверждение передачи.
6. Ликвидация передаваемых структур при тупиковых ситуациях в сети.
7. Уровни модели OSI: сетевой уровень (Network Layer).

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

*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, связанных с адресацией и маршрутизацией.

Сообщения сетевого уровня принято называть *пакетами* (packet). В них помещаются фрагменты данных. Сетевой уровень отвечает за их адресацию и маршрутизацию.

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.

Сетевой уровень также отвечает за деление пользователей на группы. 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 (связанных с адресацией и маршрутизацией), возникающих при передаче через коммуникационную 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.

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

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.

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

Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок.

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 802.Х делят канальный уровень на два подуровня:

*LLC* (*Logical Link Control*) управление логическим каналом осуществляет логический контроль связи.

*MAC* (*Media Assess Control)* контроль доступа к среде.

Канальный уровень может выполнять следующие виды функций:

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

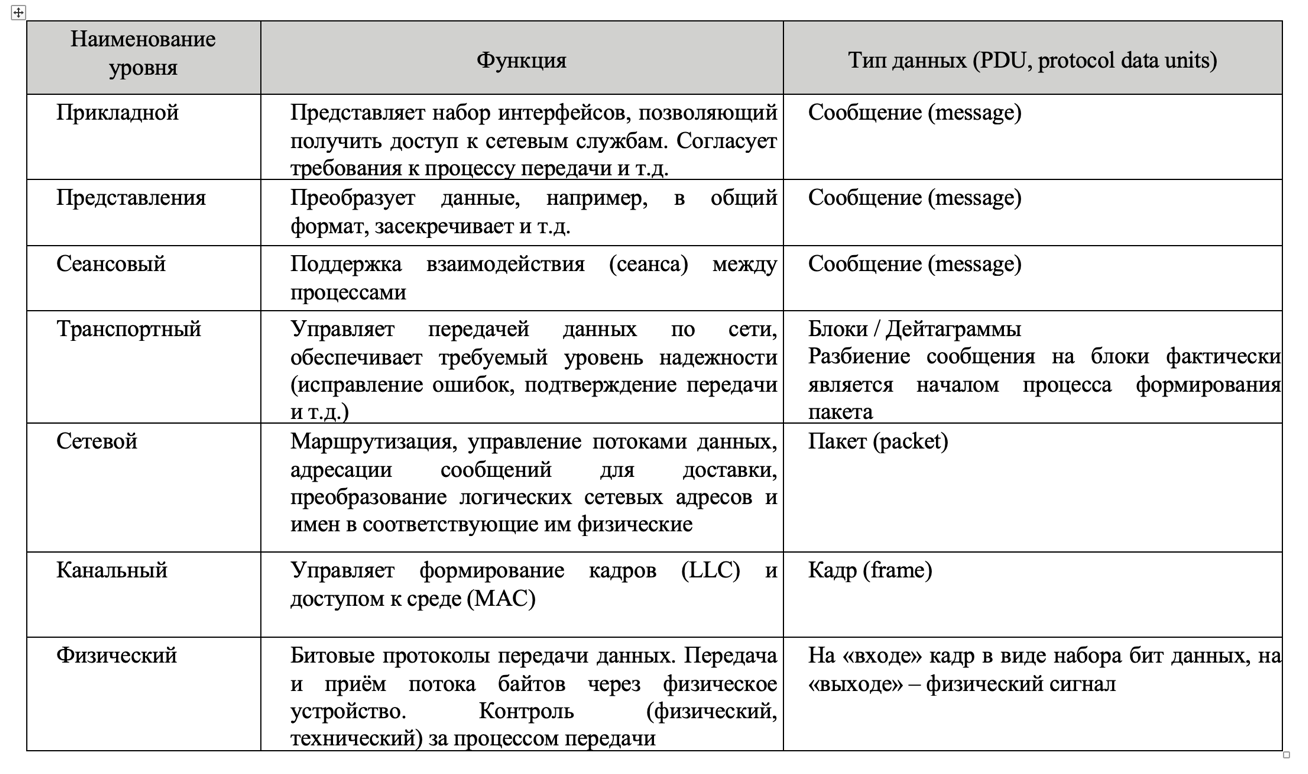
В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

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

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.

Можно считать этот уровень, отвечающим за аппаратное обеспечение.

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



1. Спецификации стандартов 802.1 – 802.11

Спецификации IEEE 802 (Institute of Electrical and Electronics Engineers) 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.

Существует более двадцати спецификаций IEEE 802.

Стандарты IEEE 802 подразделяют канальный уровень на два подуровня:

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

***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 (конфликтов).

***Стандарт IEEE 802.4*** (Token Bus LAN – *локальные сети Token Bus*) определяет метод доступа к шине с передачей маркера, прототип – 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.

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

1. Спецификации стандартов 802.12 – 802.22.

Спецификации IEEE 802 (Institute of Electrical and Electronics Engineers) 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.

Существует более двадцати спецификаций IEEE 802.

***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.

***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.

Правила взаимодействия двух машин могут быть описаны в виде набора процедур для каждого из уровней, которые называются **протоколами**.

Согласованный набор протоколов разных уровней, достаточный для организации межсетевого взаимодействия, называется **стеком протоколов**.

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

* сетевые;
* транспортные;
* прикладные.

*Протоколы сетевого уровня*

* 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
* IP
* IPX
* NetBEUI

*Протоколы транспортного уровня*

* Транспортные протоколы предоставляют услуги надежной транспортировки данных между компьютерами. Ниже приведены наиболее популярные транспортные протоколы:
* ATP
* NetBIOS
* SPX

*Протоколы прикладного уровня*

* Прикладные протоколы отвечают за взаимодействие приложений. Ниже приведены наиболее популярные прикладные протоколы:
* AFP
* FTP
* NCP
* SNMP

1. 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 позволяет обмениваться данными по сети приложениям и службам, работающим практически на любой платформе, включая Unix, Windows, Macintosh и другие.

**Назначение протоколов TCP/IP**

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

1. Стек TCP/IP: уровень приложения, уровень транспорта

***Уровень Приложения***

Через уровень *Приложения* модели TCP/IP приложения и службы получают доступ к сети. Доступ к протоколам TCP/IP осуществляется посредством двух программных интерфейсов API: сокеты Windows и NetBIOS.

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

**NetBIOS –** это протокол для работы в локальных сетях на персональных компьютеров типа IBM/PC, разработан в виде интерфейса, который не зависит от фирмы-производителя. В целом NetBIOS обеспечивает:

* регистрацию и проверку сетевых имен;
* установление и разрыв соединений;
* связь с подтверждением доставки информации;
* связь без подтверждения доставки информации;
* поддержку управления и мониторинга драйвера и сетевой карты.

***Транспортный уровень***

Транспортный уровень TCP/IP отвечает за установление и поддержание соединения между двумя узлами, а также за обеспечение, при необходимости, надежности передачи.

Основные функции уровня:

* подтверждение получения информации и обеспечение надежности передачи;
* управление потоком данных;
* упорядочение и ретрансляция пакетов.

В зависимости от типа службы могут быть использованы два протокола:

TCP (Transmission Control Protocol – *протокол управления передачей*);

UDP (User Datagram Protocol – *пользовательский протокол дейтаграмм*).

TCP обычно используют в тех случаях, когда приложению требуется передать большой объем информации и убедиться, что данные получены адресатом в неизменном виде. Приложения и службы, отправляющие небольшие объемы данных и не нуждающиеся в получении подтверждения, используют протокол UDP, который является протоколом без установления соединения. На практике протокол UDP логично использовать для передачи служебных сообщений.

1. Стек TCP/IP: межсетевой уровень, уровень сетевого интерфейса.

***Межсетевой уровень***

Межсетевой уровень отвечает за маршрутизацию данных внутри сети и между различными сетями, решая при этом функции сетевого и частично канального уровней модели OSI. 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 протоколы IP, ARP, RARP, ICMP, IGMP.

Процесс получения по известному IP-адресу МАС-адреса называется **разрешением IP-адреса**.

Удаление происходит для того, чтобы при перемещении в другую подсеть компьютера с МАС-адресом, занесенным в таблицу, кадры не отправлялись бесполезно в сеть.

**Протокол управления сообщениями Интернета** (Internet Control Message Protocol, ICMP) используется IP и другими протоколами высокого уровня для отправки и получения отчетов о состоянии переданной информации.

Узлы локальной сети используют **протокол управления группами Интернета** (Internet Group Management Protocol, IGMP), чтобы зарегистрировать себя в группе.

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

**Протоколы обмена маршрутной информацией стека TCP/IP** относятся к классу адаптивных протоколов, которые в свою очередь делятся на две группы, каждая из которых связана с одним из следующих типов алгоритмов:

* дистанционно-векторный алгоритм (Distance Vector Algorithms, DVA),
* алгоритм состояния связей (Link State Algorithms, LSA).

***Уровень сетевого интерфейса***

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. Кадр преобразуется в сигналы требуемого вида и отправляется в сеть.

1. Символьная адресация в сетях. Отличие DNS-имени от NetBios имен. Структура DNS-имени.
2. Принципы разрешения DNS-имени.

Служба DNS построена по модели «клиент-сервер», т. е. в процессе разрешения имен участвуют DNS-клиент и DNS-серверы. Системный компонент DNS-клиента, называемый DNS-распознавателем, отправляет запросы на DNS-серверы. Запросы бывают двух видов:

– итеративные – DNS-клиент обращается к DNS-серверу с просьбой разрешить имя без обращения к другим DNS-серверам;

– рекурсивные – DNS-клиент перекладывает всю работу по разрешению имени на DNS-сервер. Если запрашиваемое имя отсутствует в базе данных и в кэше сервера, он отправляет итеративные запросы на другие DNS-серверы.

В основном DNS-клиентами используются рекурсивные запросы. На следующем рисунке проиллюстрирован процесс разрешения доменного имени с помощью рекурсивного запроса.

1. Структура IPv4. Классы IP-адресов.

Адрес IP представляет собой 32-разрядное двоичное число, разделенное на группы по 8 бит, называемые октетами.

IP-адрес состоит из двух логических частей – номера подсети (ID подсети) и номера узла (ID хоста) в этой подсети.

Существует пять классов IP-адресов: A, B, C, D и E.

За принадлежность к тому или иному классу отвечают первые биты IP-адреса.

1. Понятие маски. Правила использование масок. Определение NetworkID и HostID с использованием масок.

Маска подсети (subnet mask) – это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети.

Для стандартных классов сетей маски имеют следующие значения:

класс А – 11111111. 00000000. 00000000. 00000000 (255.0.0.0);

класс В – 11111111. 11111111. 00000000. 00000000 (255.255.0.0);

класс С – 11111111. 11111111. 11111111. 00000000 (255.255.255.0)

1. Структурирование сетей с помощью масок.

С помощью масок администратор может структурировать сеть, не требуя от поставщика услуг дополнительных номеров сетей.

1. Особые IP-адреса. Понятие частных сетей. Диапазоны частных адресов.

Некоторые IP-адреса являются особыми, они не должны применяться для идентификации обычных сетей.

1. Если первый октет ID сети начинается с 127, такой адрес считается адресом машины-источника пакета. В этом случае пакет не выходит в сеть, а возвращается на компьютер-отправитель. Такие адреса называются **loopback** и используются для проверки функционирования стека TCP/IP.
2. Если все биты IP-адреса равны нулю, адрес обозначает узел-отправитель и используется в некоторых сообщениях ICMP.
3. Если все биты ID сети равны 0, а все биты ID хоста равны 1, тоадрес называется ***ограниченным широковещательным***(limited broadcast).Пакеты, направленные по такому адресу рассылаются всем узлам той подсети, в которой находится отправитель пакета. К данному же типу адреса можно относить и IP-адрес, в котором 32 разряда заполнены 1, т.к. пакет с таким адресом устройством, связующим сети, например, коммутатром или маршрутизатором, не будет «выпущен» за пределы сети отправителя.
4. Если все биты ID хоста равны 1, а биты ID сети не равны 0, т.е. однозначно идентифицируют адрес подсети, то адрес называется ***широковещательным***(broadcast);пакеты, имеющие широковещательный адрес, доставляются всем узлам подсети назначения.
5. Если все биты ID хоста равны 0, адрес считается **идентификатором подсети** (subnet ID).

Наличие особых IP-адресов объясняет, почему из диапазона доступных адресов исключаются два адреса – это случаи, когда все биты ID хоста равны 1 или 0. Например, в сети *класса* *С* не 256, а 254 узлов.

Служба распределения номеров IANA (Internet Assigned Numbers Authority) зарезервировала для частных сетей три блока адресов:

10.0.0.0 – 10.255.255.255 (1 сеть класса А);

172.16.0.0 – 172.31.255.255 (16 сетей класса B);

192.168.0.0 – 192.168.255.255 (256 сетей класса С).

Также в качестве частной можно выделить еще одну сеть класса B – 169.254.0.0, адреса которой используются для автоматической конфигурации сетевых адаптеров операционной системой Windows при отсутствии либо не работающем DHCP-сервере.

1. Адресация IPv6. Особенности. Текстовое представление адреса. Типы IPv6 адресов.

Для преодоления ограничений IPv4 был разработан **протокол IP 6-й версии** – **IPv6.**

Протокол IPv6 имеет следующие основные особенности:

* длина адреса 128 бит – такая длина обеспечивает примерно 3,4×1038 адресов; такое количество адресов позволит присваивать в обозримом будущем уникальные IP-адреса любым устройствам;
* автоматическая конфигурация – протокол IPv6 предоставляет средства автоматической настройки IP-адреса и других сетевых параметров даже при отсутствии таких служб, как DHCP;
* встроенная безопасность – для передачи данных является обязательным использование *протокола защищенной передачи* IPsec (протокол IPv4 также может использовать IPsec, но не обязан этого делать).

Существует три типа адресов:

* *unicast*: идентификатор одиночного интерфейса. Пакет, посланный по unicast-адресу, доставляется интерфейсу, указанному в адресе. Под интерфейсом в контексте Ipv6 следует понимать это средство подключения узла к каналу.
* *anycast*: идентификатор набора интерфейсов (принадлежащих разным узлам). Пакет, посланный по anycast-адресу, доставляется одному из интерфейсов, указанному в адресе (ближайший, в соответствии с мерой, определенной протоколом маршрутизации).
* *multicast*: идентификатор набора интерфейсов (обычно принадлежащих разным узлам). Пакет, посланный по multicast-адресу, доставляется всем интерфейсам, заданным этим адресом.

1. Unicast и Anycast IPv6 адреса.

*Unicast-адрес* служит для определения интерфейса устройства под управлением протокола IPv6. Пакет, который отправляется на unicast-адрес, будет получен интерфейсом, присвоенным для этого адреса. Как и в случае с протоколом IPv4, IPv6-адрес должен быть индивидуальным.

Существует шесть типов Unicast адресов:

1. *Global unicast-адрес.*
2. *Link-local адреса.*
3. *Loopback-адрес.*
4. *Unspecified-адрес.*
5. *Unique local адрес.*
6. *IPv4 embedded адрес.*
7. Multicast IPv6 адреса.

*Мультикаст-адрес IPv6* является идентификатором для группы узлов. Узел может принадлежать к любому числу мультикаст групп.



Структура multicast-адреса

Поле *scope* представляет собой 4-битовый код, предназначенный для определения предельной области действия multicastг-группы.

Multicast адреса не должны использоваться в качестве адреса отправителя в IPv6 пакетах или встречаться в любых заголовках маршрутизации.

1. Кабель типа «витая пара» (twisted pair). Схемы разводки. Кабельные системы Ethernet.

Витой парой (twisted pair) называется кабель, в котором изолированная пара проводников скручена с небольшим числом витков на единицу длины.

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)

1. Кабели и структурированные кабельные системы. Коаксиальные кабели.

**Кабель** – это достаточно сложное изделие, состоящее из проводников, слоев экрана и изоляции.

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

1. *Универсальность*.
2. *Увеличение срока службы*.
3. *Уменьшение стоимости добавления новых пользователей и изменения их мест размещения*.
4. *Возможность легкого расширения сети*.
5. *Обеспечение более эффективного обслуживания*.
6. *Надежность*.

Коаксиальные кабели используются в радио и телевизионной аппаратуре

1. Сетевые адаптеры (Network Interface Card). Назначение и функции сетевых адаптеров. Типы сетевых адаптеров.

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

Для адаптеров, отвечающих *стандарту PnP* (plug and play), настройка производится автоматически. В ином случае необходимо настроить линию *запроса на прерывание, IRQ* (Interrupt Request Line) и *адрес ввода/вывода* (Input/Output address).

Современные сетевые адаптеры как правило поддерживают следующие функции.

1. PCI BUS-Mastering. Данная функция означает возможность пересылки данных устройством без участия центрального процессора.
2. BootRom. Возможность загрузки системы по сети заложена в виде BootRom сетевой карты.
3. Wake-on-Lan. Данная технология представляет собой включение удаленной системы через сеть.

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

*Сетевые адаптеры различаются* также по типу принятой в сетитехнологии– Ethernet, Token Ring, FDDI и т. п.

1. Повторители и концентраторы. Назначение и особенности использования.

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

*Многопортовый повторитель* часто называют *концентратором* (concentrator) или *хабом* (hub),

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

*Концентратор* – устройство, у которого суммарная пропускная способность входных каналов выше пропускной способности выходного канала.

*Концентратор является активным оборудованием. Он служит центром (шиной) звездообразной конфигурации сети и обеспечивает подключение сетевых устройств*.

Концентраторы образуют из отдельных физических отрезков кабеля общую среду передачи данных – **логический сегмент**.

1. Мосты. Назначение и особенности использования. Различие между мостом и коммутатором. Различия между маршрутизаторами и мостами.

**Мост**(bridge) – ретрансляционная система, соединяющая каналы передачи данных (рис. 16.2). Мост, а также его быстродействующий аналог  *коммутатор* (switching hub), делят общую среду передачи данных на логические сегменты.

Основное различие между коммутатором и мостом 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.

*Маршрутизаторы превосходят мосты своей способностью фильтровать и направлять пакеты данных на сети*.

1. Коммутаторы. Назначение и особенности использования.

**Коммутатор** (switch) – устройство, осуществляющее выбор одного из возможных вариантов направления передачи данных. Общая структура коммутатора аналогична стуктуре моста, т.е. современные коммутаторы оперируют не только на физическом, но и на канальном уровне модели OSI.

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

В перечень функций, выполняемых коммутатором локальной сети, входят:

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

1. Маршрутизаторы. Назначение. Особенности использования. Шлюзы. Назначение и особенности использования.

**Маршрутизатор** (router) – ретрансляционная система, соединяющая две коммуникационные сети либо их части. Маршрутизаторы обмениваются информацией об изменениях структуры сетей, трафике. 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.

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

1. Беспроводные технологии: радиосвязь, инфракрасная, связь в микроволновом диапазоне. Достоинства и недостатки беспроводных сетей wi-fi.

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

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

Wi-Fi сеть (Wireless Local Area Network – WLAN) – это радиосеть, позволяющая передавать информацию между объектами по радиоволнам (без проводов). Разработкой стандартов в этой области занимается Wi-Fi Alliance.

WLAN-сети имеют ряд преимуществ перед обычными кабельными сетями:

* + WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса;
  + пользователи мобильных устройств, при подключении к локальным беспроводным сетям, могут легко перемещаться в рамках действующих зон сети;
  + скорости современных сетей довольно высоки (до 300 Мб/с), что позволяет их использовать для очень широкого спектра задач;
  + с помощью дополнительного оборудования беспроводная сеть может быть успешно соединена с кабельными сетями;
  + WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Несмотря на все достоинства, WLAN-сети обладают рядом недостатков, главный из которых – возможность легкого перехвата данных и взлома сети.

1. Сети Wi-Fi стандарта IEEE802.11a и IEEE802.11b.

|  |  |  |
| --- | --- | --- |
| **Название** | **Частота** | **Комментарий** |
| **802.11a** | 5 GHz | Не совместим с сетями b или g. Это один из самых старых стандартов, но сегодня он используется многими устройствами. Максимальная скорость передачи – 54 Mбит/с, но обычно от 6 до 24 Mбит/с. |
| **802.11b** | 2.4 GHz | Совместим с g сетями. В реальности, g была сделана обратно совместимой с b для поддержки большего количества устройств.  Максимальная скорость передачи – 11 Mбит/с |
| **802.11g** | 2.4 GHz | Самый популярный тип сети. Сочетание скорости и обратной совместимости делает его подходящим для современных сетей.  Максимальная скорость передачи – 54 Mбит/с |
| **802.11n** | 2.4 и 5 GHz | Максимальная теоретическая скорость передачи данных составляет 600 Мбит/с, применяя передачу данных сразу по четырём антеннам. По одной антенне – до 150 Мбит/с. |

1. Сети Wi-Fi стандарта IEEE802.11g и IEEE802.11n.

|  |  |  |
| --- | --- | --- |
| **Название** | **Частота** | **Комментарий** |
| **802.11a** | 5 GHz | Не совместим с сетями b или g. Это один из самых старых стандартов, но сегодня он используется многими устройствами. Максимальная скорость передачи – 54 Mбит/с, но обычно от 6 до 24 Mбит/с. |
| **802.11b** | 2.4 GHz | Совместим с g сетями. В реальности, g была сделана обратно совместимой с b для поддержки большего количества устройств.  Максимальная скорость передачи – 11 Mбит/с |
| **802.11g** | 2.4 GHz | Самый популярный тип сети. Сочетание скорости и обратной совместимости делает его подходящим для современных сетей.  Максимальная скорость передачи – 54 Mбит/с |
| **802.11n** | 2.4 и 5 GHz | Максимальная теоретическая скорость передачи данных составляет 600 Мбит/с, применяя передачу данных сразу по четырём антеннам. По одной антенне – до 150 Мбит/с. |

1. Сети cтандарта IEEE802.11ac. Сети стандарта IEEE802.11ax.

|  |  |  |
| --- | --- | --- |
| **Название** | **Частота** | **Комментарий** |
| **802.11ac** | 5 GHz | Стандарт 802.11ac обеспечивает обратную совместимость с 802.11b / g / n и скоростью до 1300 Мбит/с в полосе 5 ГГц, плюс до 450 Мбит / с на 2,4 ГГц.  Максимальная теоретическая скорость передачи данных – 6,9 Гбит/с (при наличии 8 антенн и в режиме MU-MIMO). |
| **802.11aх** | 2.4 и 5 GHz  (до 6 GHz для WI-FI 6) | Для Wi-Fi 6 увеличена почти в полтора раза по сравнению с 802.11ac теоретическая скорость передачи данных (9,6 Гбит/с).  В случае с Wi-Fi 6Е увеличение частоты с 5ГГц до 6 ГГц, а также увеличение числа каналов (добавилось 14 новых 80 МГц и 7 160 МГц каналов) должно приводить к увеличению пропускной способности по сравнению с базовым Wi-Fi 6. |

1. Сети Wi-Fi. Стандарты IEEE802.11h, IEEE802.11i, IEEE802.11j, IEEE802.11d, IEEE802.11e, IEEE802.11f.

|  |  |
| --- | --- |
| **Наименование стандарта** | **Назначение** |
| **IEEE 802.11h** | Дополняет спецификации IEEE 802.11 алгоритмами эффективного выбора частот для офисных и уличных беспроводных сетей, а также средствами управления спектра |
| **IEEE 802.11i** | Предусматривает для стандартов IEEE 802.11 средства шифрования передаваемых данных, а также   централизованной аутентификации пользователей и рабочих станций |
| **IEEE 802.11j** | Данный стандарт оговаривает существование в одном диапазоне сетей стандартов 802.11a и HiperLAN2. Спецификация предназначена для Японии и расширяет стандарт 802.11а добавочным каналом 4,9 ГГц |
| **Наименование стандарта** | Назначение |
| **IEEE 802.11d** | Стандарт определяет требования к физическим параметрам каналов (мощность излучения и диапазоны частот) и устройств беспроводных сетей с целью обеспечения их соответствия законодательным нормам различных стран |
| **IEEE 802.11e** | При сохранении полной совместимости с используемыми стандартами 802.11а и b, позволяет расширить их функциональность за счет поддержки потоковых мультимедиа данных и гарантированного качества услуг (QoS) |
| **IEEE 802.11f** | Данный стандарт определяет механизм взаимодействия точек связи между собой при перемещении клиента между сегментами сети |

1. Оборудование для сетей Wi-Fi. Формы организации Wi-Fi сетей.
2. Особенности оптических систем связи (физические, технические). Достоинства и недостатки оптических систем связи.
3. Оптический кабель: его разновидности и характеристики.
4. Защита информации. Основные понятия. Виды основных сетевых атак.

Защита информации – это комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

Поскольку утрата информации может происходить по сугубо техническим, объективным и неумышленным причинам, под это определение подпадают также и мероприятия, связанные с повышением надежности сервера из-за отказов или сбоев в работе винчестеров, недостатков в используемом программном обеспечении и т.д.

Сетевые атаки через Интернет могут быть классифицированы следующим образом:

1. Сниффер пакетов

2. IP-спуфинг– происходит, когда хакер, находящийся внутри корпорации (сети) или вне ее, выдает себя за санкционированного пользователя.

3. Отказ в обслуживании

5. Парольные атаки – их целью является завладение паролем и логином законного пользователя.

6. Атаки типа MITM – вид атаки, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.

8. Атаки на уровне приложений. В данном случае злоумышленники получают прямой доступ к приложениям корпоративной сети.

1. Классификация средств защиты информации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

1. Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации.
2. Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств – универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки – ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).
3. Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.
4. Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки – высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.
5. Понятие шифрования. Классические алгоритмы шифрования данных (подстановка, перестановка, гаммирование).

**Шифрование** данных представляет собой разновидность программных средств защиты информации и имеет особое значение на практике как единственная надежная защита информации, передаваемой по протяженным последовательным линиям, от утечки.

Шифрование - это обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней.

Имеются следующие "классические" методы шифрования:

* подстановка (простая – одноалфавитная, многоалфавитная однопетлевая, многоалфавитная многопетлевая);
* перестановка (простая, усложненная);
* гаммирование (смешивание с короткой, длинной или неограниченной маской).

1. Стандартные методы шифрования и криптографические системы.

Стандартные методы шифрования (национальные или международные) для повышения степени устойчивости к дешифрованию реализуют несколько этапов (шагов) шифрования, на каждом из которых используются различные "классические" методы шифрования в соответствии с выбранным ключом (или ключами).

Существуют две принципиально различные группы стандартных методов шифрования:

1. Шифрование с применением одних и тех же ключей (шифров) при шифровании и дешифровании

2. Шифрование с использованием открытых ключей для шифрования и закрытых – для дешифрования

К достоинствам симметричных методов шифрования относится высокая скорость шифрования и дешифрования, к недостаткам – малая степень защиты в случае, если ключ стал доступен третьему лицу.