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

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

Сеть часто классифицируется по территориальному признаку.

* Локальные — несколько близко расположенных зданий.
* Региональные — в пределах конкретной области.
* Городские/муниципальные — в пределах небольшого района/города.
* Глобальные.

Но ключевой характеристикой является скорость доступа к информации. В связи с данной характеристикой сети подразделяются на локальные и глобальные (с временной задержкой).

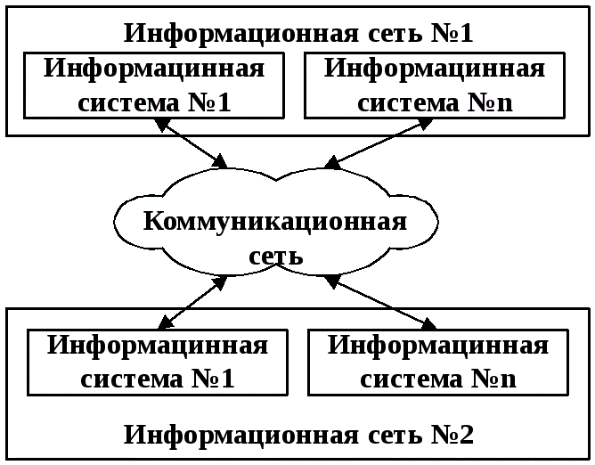
В состав сети в общем случае включается следующие элементы:

* сетевые компьютеры (оснащенные сетевым адаптером);
* каналы связи (кабельные, спутниковые, телефонные, цифровые, волоконно-оптические, радиоканалы и др.);
* различного рода преобразователи сигналов;
* сетевое (коммуникационное) 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, способна осуществлять хранение, обработку или передачу информации. В состав информационной системы входят: компьютеры, программы, пользователи и др.

Вычислительная сеть — одна из разновидностей распр. Систем, предназначенных для распараллеливания вычислений, за счет чего может быть достигнуто повышение производительности и отказоустойчивости системы.

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. 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 каналможно охарактеризовать, как маршрут, проложенный через физические каналы и узлы коммутации.

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

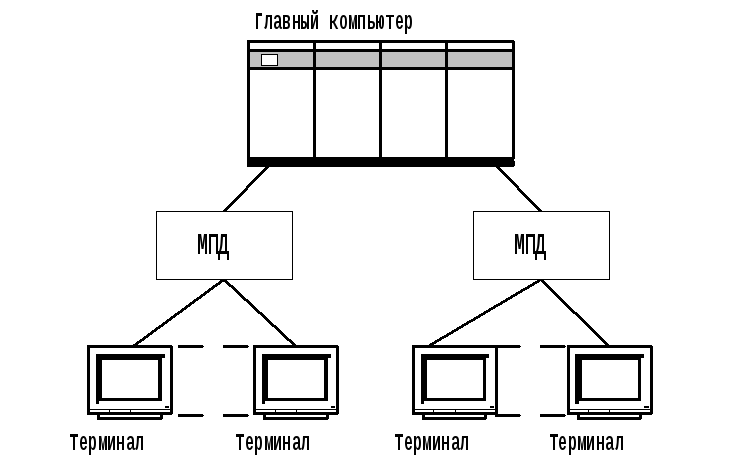
Трафик (traffic) – это поток сообщений в сети передачи данных. Под ним понимают количественное измерение в выбранных точках сети числа проходящихблоков данныхи их длины, выраженное в битах в секунду.

1. **Архитектура терминал – главный компьютер.**

Существует 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.

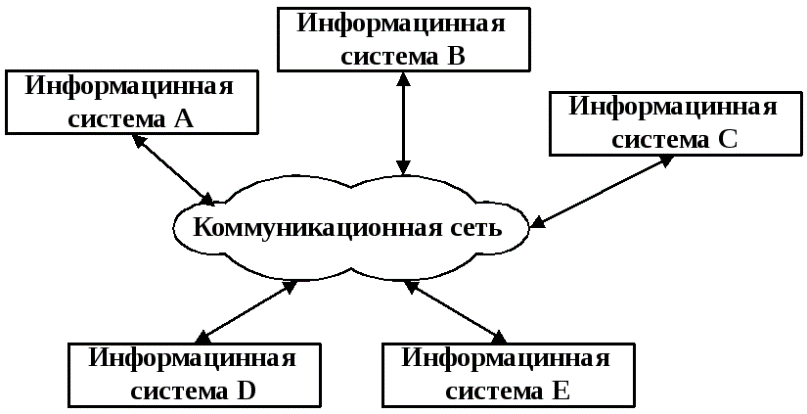
Рассматриваемая архитектура предполагает два типа оборудования:

* Главный компьютер, где осуществляется управление сетью, хранение и обработка данных (может быть не один).
* 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, как представлено. Классический пример архитектуры сети с главными компьютерами – системная сетевая архитектура (SystemNetworkArchitecture– SNA).

1. **Одноранговая архитектура. Архитектура клиент – сервер.**

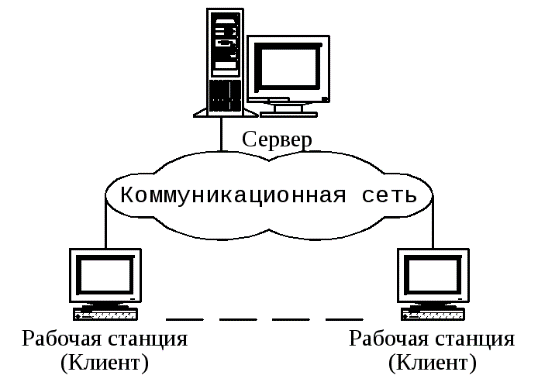
Одноранговая архитектура – это концепция информационной сети, в которой ее ресурсы рассредоточены по всем системам. Данная архитектура характеризуется тем, что в ней все системы равноправны. К одноранговым сетям относятся малые сети, где любая рабочая станция может выполнять одновременно функции файлового сервера и рабочей станции.

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

Преимущества:

* они легки в установке и настройке;
* отдельн. ПК не завис. от выдел сервера;
* пользователи в состоянии контролировать свои ресурсы;
* малая стоимость и легкая эксплуатация;
* мин. оборудования и ПО;
* нет необходимости в администраторе;
* хорошо подходят для сетей с кол-вом пользователей, не > 10.

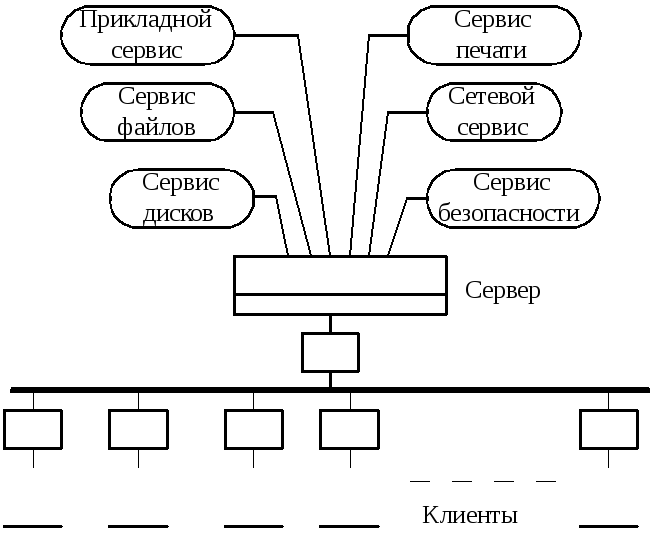
Проблемой одноранговой архитектуры является ситуация, когда компьютеры отключаются от сети. В этих случаях из сети исчезают виды сервиса, которые они предоставляли. Сетевую безопасность одновременно можно применить только к одному ресурсу, и пользователь должен помнить столько паролей, сколько сетевых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

**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.

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

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

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

Сети на базе серверов имеют лучшие характеристики и повышенную надежность.

В современной клиент – серверной архитектуре выделяется четыре группы объектов: клиенты, серверы, данные и сетевые службы.

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.

Недостатки:

* 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 – 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. Выделяют два основных класса 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.

Строго говоря, при упоминании о топологии сети, могут подразумеваться четыре совершенно разных понятия, относящихся к различным уровням сетевой архитектуры.

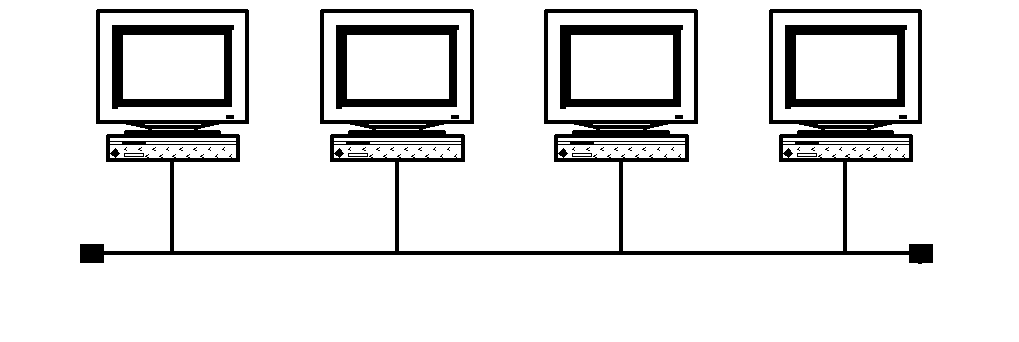
*Физическая топология* – географическая схема расположения компьютеров и прокладки кабелей. В этом смысле, например, «пассивная звезда» ничем не отличается от «активной», поэтому ее нередко называют просто «звездой».

*Логическая топология* – структура связей, характер распространения сигналов по сети. Это наиболее правильное определение топологии.

*Топология управления обменом* – принцип и последовательность передачи права на захват сети между отдельными компьютерами.

*Информационная топология* – направление потоков информации, передаваемой по сети.

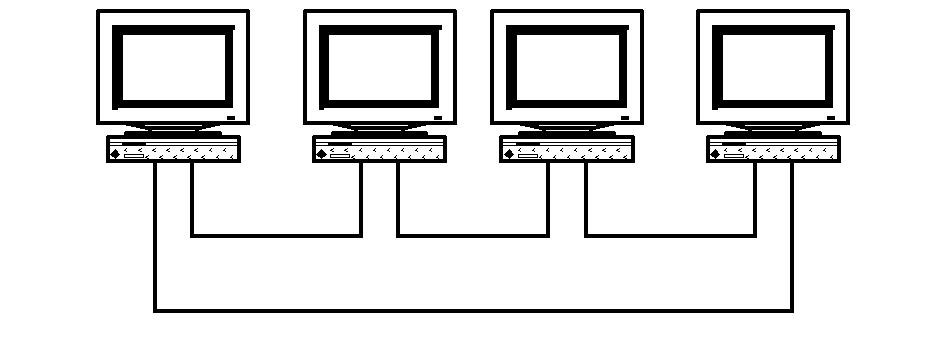
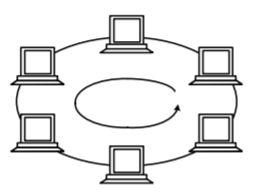
**Общая шина** - это тип сетевой топологии, в которой рабочие станции расположены вдоль одного участка кабеля, называемого сегментом.

Общая шина предполагает использование одного кабеля, к которому подключаются все компьютеры сети. В случае данной топологиикабель 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 станцияотбирает адресованные ей сообщения, пользуясьадреснойинформацией. 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 (дешёвая) и наиболее распространенная топология сети.

Примерами использования топологии общая шина является сеть 10Base–5 (соединение ПК толстым коаксиальным кабелем) и 10Base–2 (соединение ПК тонким коаксиальным кабелем). Без терминатора сеть работать не будет. «Врезаться» в шину нельзя!

1. **Топология кольцо. Топология цепочка.**

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

Данные передаются от одной рабочей станции к другой в одном направлении. 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. Очень просто делается запрос на все станции одновременно.

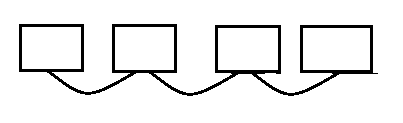
Чистая кольцевая топология используется редко. Вместо этого кольцевая топология играет транспортную роль в схеме метода доступа. Кольцо описывает логический маршрут, а пакет передается от одной станции к другой, совершая в итоге полный круг.

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.

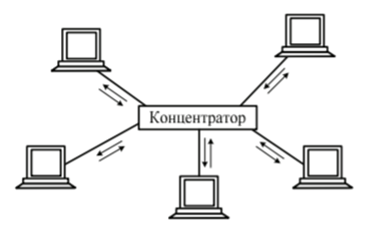
Проблемы:

* В случае выхода из строя хотя бы одного компа, вся сеть накрылась.
* Подключение новой рабочей станции требует временного прекращения работы и изменения маршрута
* Кольцо не любит трансформаций. Кольцо ретранслируемо.
* Дорого, но надёжно.
* Кольцо имеет предсказуемое время отклика, определяемое числом рабочих станций, (работает маркерный доступ).

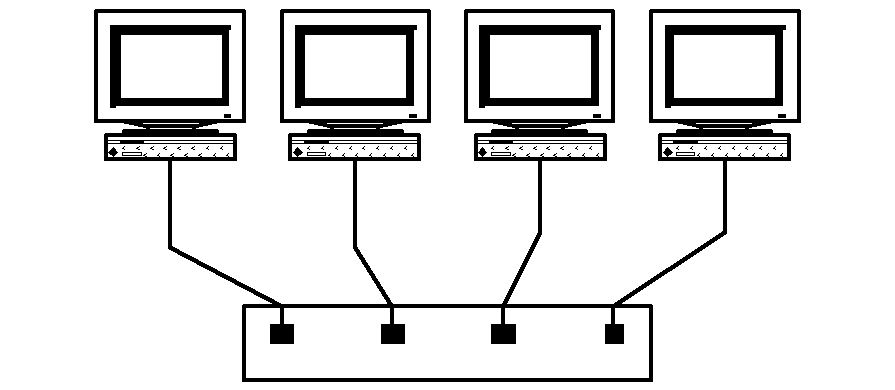
Топология «**цепочка**» работает по логике кольца, но её нельзя замкнуть. Используется тогда, когда интенсивность трафика в сети не так велика и существует необходимость ответвления в ряде точек на линии, где могут вводиться и выводиться каналы доступа.



1. **Звездообразные топологии.**

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

Преимуществом такой топологии является возможность простого исключения неисправного узла. Однако, если неисправен центральный узел, вся сеть выходит из строя. Максимум 48 компов.

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).

Легко диагностировать неисправность. Если центральное устройство концентратор, то сеть становится малоуправляемой широковещательной.

Примером звездообразной топологии является топология Ethernetс кабелем типаВитая пара10BASE-T, центромЗвездыобычно являетсяHub.

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.

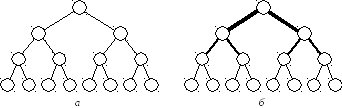
Недостатки:

* Расход кабеля большой.
* Концентраторы не дорогие, коммутаторы дороже.
* Кабельные концентраторы при большом количестве кабеля трудно обслуживать.

Однако в большинстве случаев в такой топологии используется недорогой кабель типа витая пара. В некоторых случаях можно даже использовать существующие телефонные кабели. Кроме того, для диагностики и тестирования выгодно собирать все кабельные концы в одном месте. По сравнению с концентраторами ArcNet концентраторы Ethernet и MAU Token Ring достаточно дороги. Новые подобные концентраторы включают в себя средства тестирования и диагностики, что делает их еще более дорогими.

1. **Древовидные топологии.**

Дерево рассматривают как комбинацию нескольких звёзд, может быть активными или пассивными. Выделяют также утолщённое дерево. В активном дереве в центре объединения нескольких линий находят центральный компьютер.

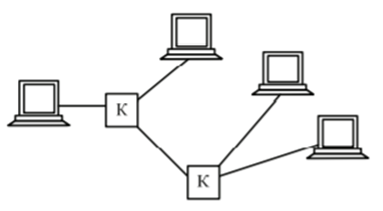
а – стандартное дерево

б – утолщённое дерево (дешёвый способ построения)

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.

В пассивном дереве в центре находятся концентраторы (хабы). Концентратор не может быть вершиной т.к. он тупой.

 - активное.

 - пассивное

Преимущества:

* Если дерево активное, дополнить устройствами проблемно.
* Если пассивное, быстро.
* В глубь дерево не наращивается, только в ширину.

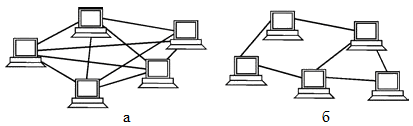
У суперкомпьютера наращивается пропускная способность, все вычисления происходят на листьях. Делается на оптике. Цена увеличения работает на вычислительную мощность.

1. **Ячеистые топологии.**

Ячеистая или сеточная топология — это топология, в которой компьютеры связаны между собой не одной, а несколькими линиями связи. Выделяют 2 типа топологии: полную и частичную.

В полной каждый ПК связан напрямую со всеми остальными ПК сети. 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 предполагает наличие связей между самыми активными узлами сети (передающие большие объёмы информации), с другими ПК связь через промежуточные узлы.

Характеристика:

Наличие альтернативных путей передачи информации.

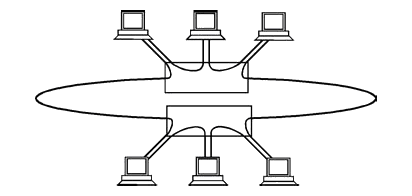
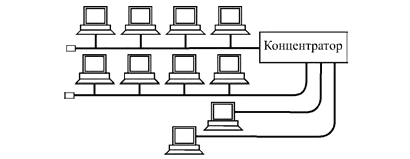
Логика последовательной топологии.

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.

1. **Комбинированные топологии.**

Используются для устранения недостатка одиночных топологий.

Довольно часто применяются комбинированные топологии, среди которых наиболее распространены *звездно-шинная* (star-bus) и *звездно-кольцевая* (star-ring):



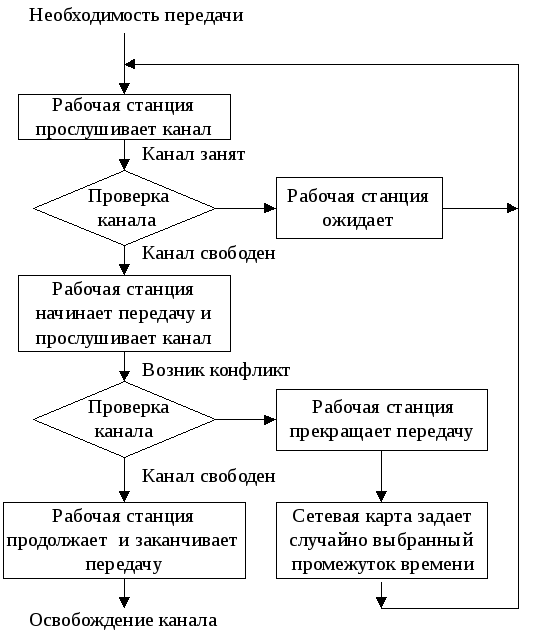
В «звездно-шинной» топологии используется комбинация «шины» и «пассивной звезды». В звездно-шинной топологии к концентратору подключаются как отдельные компьютеры, так и целые шинные сегменты. На самом деле реализуется физическая топология шина, включающая все компьютеры сети. В данной топологии может использоваться и несколько концентраторов, соединенных между собой и образующих так называемую магистральную, опорную шину. 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, 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. Примерами методов доступа являются:

* множественный доступ с прослушиванием несущей и разрешением коллизий (CarrierSenseMultipleAccesswithCollisionDetection– CSMA/CD);
* множественный доступ с передачей полномочия (TokenPassingMultipleAccess– TPMA) или метод с передачей маркера;
* множественный доступ с разделением во времени (TimeDivisionMultipleAccess– TDMA);
* множественный доступ с разделением частоты (FrequencyDivisionMultipleAccess– FDMA) или множественный доступ с разделением длины волны (WavelengthDivisionMultipleAccess– WDMA).

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

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

Возможна повторная коллизия при похожих промежутках времени. В этом случае промежутки «молчания» увеличиваются.

Данный метод доступа предполагает использование арбитражного элемента именно он в таком случае принимает от рабочей станции заявку на передачу и выдаёт разрешение.

Протокол CSMA/CD работает на [канальном уровне](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) в модели [OSI](https://ru.wikipedia.org/wiki/Open_Systems_Interconnection).

Данная группа методов является самой распространенной.

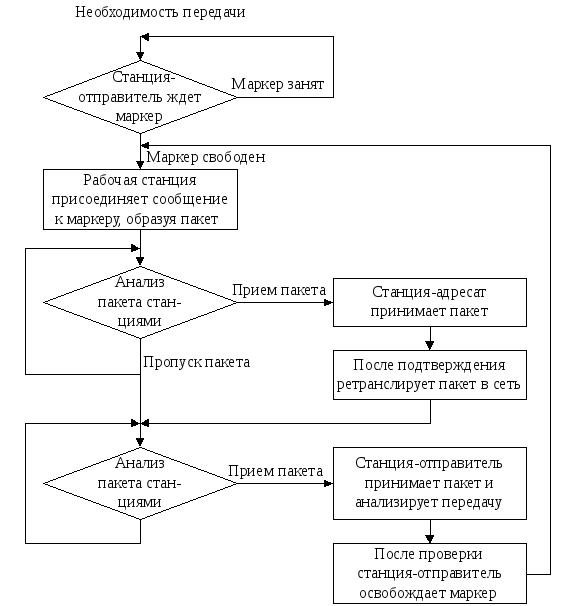
1. **Метод доступа TPMA.**

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.

Алгоритм множественного доступа с передачей полномочия, или маркера:

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

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

Пакет распространяется по ЛВС от адаптера к адаптеру, пока не найдет своего адресата, который установит в нем определенные биты для подтверждения того, что данные достигли адресата, и ретранслирует его вновь вЛВС. После чего пакет возвращается в узел из которого был отправлен. Здесь после проверки безошибочной передачи пакета, узел освобождаетЛВС, выпуская новый маркер. Таким образом, вЛВСс 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.

Это связано с тем, что получив сообщение с маркером, адресат сначала проверяет сообщение на корректность. В случае, если оно валидно, то к маркеру присоединяется еще специальное сообщение и отправляется отправителю. Иначе происходит повтор передачи.

Решение заключается в организации последовательного числа передач между 2 узлами.

Возможно расставление приоритетов.

1. **Метод доступа TDMA.**

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.

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

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.

R20

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.

Если ПК нечего передавать, то её ячейка может быть предоставлена для передачи другому ПК.

Плюсы:

Возможность обеспечить одинаковые промежутки времени между передачами.

Часто используется при передаче голосом/речи.

1. **Метод доступа FDMA и WDMA.**

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.

Множественный доступ с разделением частоты – **FDMA.**

Множественный доступ с разделением длины волны – **WDMA.**

Множественный доступ с разделением частоты основан на разделении полосы пропускания канала на группу полос частот, образующих логические каналы.

R21Широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. Размеры узких полос могут быть различными в зависимости от требований, оборудования и т.д.

Защитные полосы необходимы для предотвращения наложения сигналов, передающихся по соседним узким полосам.

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.

Метод применяется для беспроводных сетей (сотовая связь).

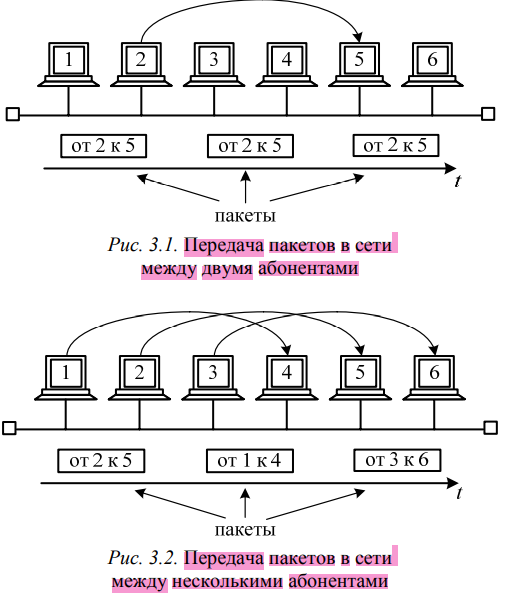
В оптических каналах разделение частоты осуществляется направлением в каждый из них лучей света с различными частотами. Благодаря этому пропускная способность физического канала увеличивается в несколько раз. При осуществлении этого мультиплексирования в один световод излучает свет большое число лазеров (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.**

Вся информация, передаваемая по сетям, передается отдельными частями, которые могут называться пакеты/кадры/фреймы/блоки.

При этом длина пакета ограничена сверху и снизу.

Выбор длины пакета с точки зрения пользователя зависит от времени доступа. Это временной интервал между моментом готовности абонента передачи и моментом передачи.

Ожидание начала передачи связано с тем, что в сети не может происходить несколько передач одновременно (во всяком случае, при топологиях шина и кольцо). Всегда есть только один передатчик и один приемник (реже – несколько приемников). В противном случае информация от разных передатчиков смешивается и искажается. В связи с этим абоненты передают свою информацию по очереди. И каждому абоненту, прежде чем начать передачу, надо дождаться своей очереди. Вот это время ожидания своей очереди и есть время доступа.

Если бы вся требуемая информация передавалась каким-то абонентом сразу, непрерывно, без разделения на пакеты, то это привело бы к монопольному захвату сети этим абонентом на довольно продолжительное время. Все остальные абоненты вынуждены были бы ждать окончания передачи всей информации, что в ряде случаев могло бы потребовать десятков секунд и даже минут. С тем, чтобы уравнять в правах всех абонентов, а также сделать примерно одинаковой величину времени доступа к сети и интегральную скорость передачи информации, как раз и применяются пакеты (кадры) ограниченной длины.

Важно также и то, что при передаче больших массивов информации вероятность ошибки (передана «1» – принимается «0», или наоборот) из-за помех и сбоев довольно высока. Например, при характерной для локальных сетей величине вероятности одиночной ошибки в 10–8 (в среднем одна ошибка приходится на 100 Мбайт переданных двоичных символов) пакет длиной 10 Кбит будет искажен с вероятностью 10–4, а массив длиной 10 Мбит – уже с вероятностью 10–1. К тому же выявить ошибку в массиве из нескольких мегабайт намного сложнее, чем в пакете из нескольких килобайт, а при обнаружении ошибки придется повторить передачу всего большого массива. Но и при повторной передаче большого массива снова высока вероятность ошибки, и процесс этот при слишком большом массиве может повторяться до бесконечности.

С другой стороны, сравнительно большие пакеты имеют преимущества перед очень маленькими пакетами, например, перед побайтовой (8 бит) или пословной (16 бит или 32 бита) передачей информации.

Дело в том, что каждый пакет помимо собственно данных, которые требуется передать, должен содержать некоторое количество служебной информации. Прежде всего, это адресная информация, которая определяет, от кого и кому передается данный пакет (как на почтовом конверте – адреса получателя и отправителя).

Если порция передаваемых данных будет очень маленькой (например, несколько байт), то доля служебной информации станет непозволительно высокой, что резко снизит интегральную скорость обмена информацией по сети.

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.

Таким образом, процесс информационного обмена в сети представляет собой чередование пакетов, каждый из которых содержит информацию, передаваемую от абонента к абоненту.

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.

Все пакеты более высоких уровней последовательно вкладываются в передаваемый пакет, точнее, в поле данных передаваемого пакета. Этот процесс последовательной упаковки данных для передачи называется также **инкапсуляцией** пакетов.

Каждый следующий вкладываемый пакет может содержать собственную служебную информацию, располагающуюся как до данных (заголовок), так и после них (трейлер), причем ее назначение может быть различным. Безусловно, доля вспомогательной информации в пакетах при этом возрастает с каждым следующим уровнем, что снижает эффективную скорость передачи данных. Для увеличения этой скорости предпочтительнее, чтобы протоколы обмена были проще и уровней этих протоколов было меньше. Иначе никакая скорость передачи битов не поможет, и быстрая сеть может передавать файл дольше, чем медленная сеть, которая пользуется более простым протоколом. Обратный процесс последовательной распаковки данных приемником называется **декапсуляцией** пакетов.\

Сетевой протокол — это набор программно реализованных правил общения компьютеров, подключенных к сети. Практически это "язык", на котором компьютеры разговаривают друг с другом. Сетево́й протоко́л — набор правил и действий (очерёдности действий), позволяющий осуществлять соединение и обмен данными между двумя и более включёнными в сеть устройствами.

Разные протоколы зачастую описывают лишь разные стороны одного типа связи. Названия «протокол» и «стек протоколов» также указывают на программное обеспечение, которым реализуется протокол.

Поскольку каждый из уровней модели ISO/OSI обладает своими особенностями, реализация всех этих особенностей невозможна в рамках одного протокола. Мало того, она даже невыгодна, так как значительную часть логики можно создавать на уровне аппаратного обеспечения, что приводит к ускорению обработки данных. Исходя из этих соображений было разработано множество узконаправленных протоколов, каждый из которых выполняет свою задачу и делает это с максимальной отдачей и быстродействием.

1. **Назначение пакетов и их структура. Адресация пакетов.**

Информация по сети как правило передаётся порциями (пакетами, фреймами, кадрами). Придельная длина пакета строга ограничена как сверху, так и снизу. Сверху по объёму, снизу по служебной информации. Слишком длинные пакеты отправлять нельзя так как будет высока вероятность появления ошибок, которые не будут исправлены на принимающем приложении, соответственно потребуется повтор передачи, что является нежелательным вариантом. Слишком маленькими пакеты тоже отправлять нельзя так как в нём возрастёт доля служебной информации, которые необходимы принимающей стороне для обработки информации. (не более 10%).

Существует некоторая оптимальная длина пакета (диапазон), при которой итегр. Скорость передачи информации по сети будет максимальная.

Длина пакета не является величиной постоянной она зависит от уровня помех, от количества объектов сети, от методов доступа, от характера передаваемое информации (мультимедиа, голос и др.) и т. д.

Процесс обмена должен предполагать обязательное чередование пакетов между различными парами узлов для оптимизации времени доступа.

Структура может завесить от типа сети и используемой аппаратурой, и в целом определяется стандартом на сеть. Чаще всего пакет содержит следующие поля:

***Стартовая комбинация битов*** или ***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.

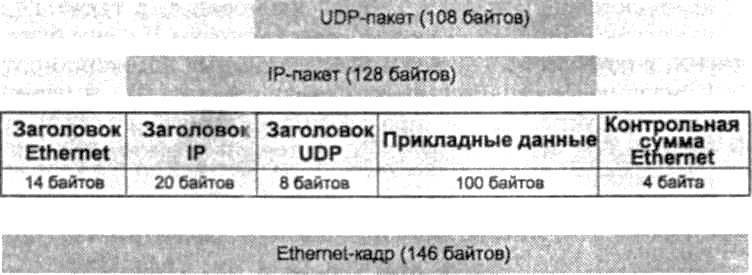
***Сетевой адрес****(****идентификатор****)* ***приёмника***, индивидуальный или групповой адрес, присвоенный каждому принимающему абоненту в сети.

***Сетевой адрес*** *(****идентификатор****)* ***передатчика***, индивидуальный номер, присвоенный каждому передающему абоненту. Этот адрес информирует принимающего абонента, откуда пришел данный пакет.

***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***– 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.

***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 запрашивает его повторную передачу.

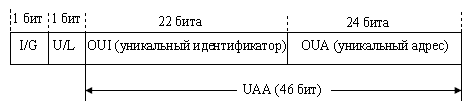
***Стоповая комбинация*** служит для информирования аппаратуры принимающего абонента об окончании пакета, обеспечивает выход аппаратуры приемника из состояния приема. Это поле может отсутствовать, если используется самосинхронизирующийся код, позволяющий определять момент окончания передачи пакета.

Кадр вложен в пакет (все поля кроме преамбулы и стоповой комбинации).

1. **MAC-адреса и их структура.**

Международная организация IEEE предложила присваивать уникальный адрес каждому сетевому адаптеру еще на стадии производства.

Физический, или локальный, адрес узла определяется технологией, с помощью которой построена сеть, в которую входит узел. Для узлов, входящих в локальные сети, это МАС-адрес сетевого адаптера или порта маршрутизатора. В качестве стандартного выбран 48-битный формат адреса, что соответствует примерно 280 триллионам различных адресов. Для распределения диапазонов адресов между многочисленными изготовителями сетевых адаптеров, есть следующая структура адреса.

Младшие 24 разряда кода адреса называются OUA – организационно уникальный адрес. Именно их присваивает каждый из зарегистрированных производителей сетевых адаптеров. Всего возможно свыше 16 миллионов комбинаций, это значит, что каждый изготовитель может выпустить 16 миллионов сетевых адаптеров. С

Следующие 22 разряда кода называются OUI – организационно 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 –универсально управляемый (административный) 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.

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.

Существует широковещательный Mac-адрес (48 единиц).

1. **7 - ая модель OSI. Назначение. Взаимодействие уровней модели OSI. Понятие горизонтальной и вертикальной модели.**

Для единого представления данных в сетях с неоднородными устройствами и программным обеспечением международная организация по стандартам ISO разработала **базовую модель связи открытых систем** OSI. 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.

Каждый уровень модели OSI выполняет определенную задачу в процессе передачи данных по сети. Базовая модель является основой для разработки сетевых протоколов. OSI разделяет коммуникационные функции в сети на семь уровней, каждый из которых обслуживает различные части процесса взаимодействия открытых систем

Есть 2 вида: горизонтальная и вертикальная.

-  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.

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

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

На принимающей стороне пакет проходит через все уровни в обратном порядке. На каждом уровне протокол этого уровня читает информацию пакета, затем удаляет информацию, добавленную к пакету на этом же уровне отправляющей стороной, и передает пакет следующему уровню.

Каждый уровень обеспечивает сервис для вышестоящего уровня, запрашивая сервис у нижестоящего. Верхние три уровня запрашивают сервис одинаково: требование маршрутизации данных из одной сети в другую.

Каждый уровень компьютера-отправителя взаимодействует с таким же уровнем компьютера-получателя, будто связан напрямую = логическая/виртуальная связь.

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

-  взаимодействию прикладных процессов;

-  формам представления данных;

-  единообразному хранению данных;

-  управлению сетевыми ресурсами;

-  безопасности данных и защите информации;

-  диагностике программ и технических средств.

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

Прикладной уровень является верхним (седьмым) уровнем и непосредственно примыкает к прикладным процессам.

В действительности прикладной уровень – это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы.

Обеспечивает процессам средства доступа к области взаимодействия.

Одна из основных задач этого уровня – определить, как следует обрабатывать запрос прикладной программы или какой вид должен принять данный запрос. Единица данных прикладного уровня, называется сообщением.

Главная задача: согласование достоверности различных форм взаимодействий.

Прикладной уровень выполняет следующие функции:

1.       Выполнение различных видов работ.

-         передача файлов;

-         управление заданиями, системой и т. д;

2.       Идентификация пользователей по их паролям, адресам, электронным подписям;

3.       Определение работающих абонентов и возможности доступа к новым прикладным процессам;

4.       Определение достаточности имеющихся ресурсов;

5.       Определение качества обслуживания (t доставки блоков данных, допустимой v ошибок);

6.   Соглашение об исправлении ошибок и определении достоверности данных;

7.   Согласование ограничений, накладываемых на синтаксис.

8. Выбор процедур

Указанные функции определяют виды сервиса, которые прикладной уроыень предоставляет прикладным процессам. Он передает этим процессам сервис, предоставл. Физическим, канальным, сетевым, транспортным, сеансовым, представительским уровнями.

К числу наиболее распространенных протоколов верхних трех уровней относятся:

-  FTP протокол передачи файлов;

-  TFTP простейший протокол пересылки файлов;

-  X.400 электронная почта;

-  Telnet работа с удаленным терминалом;

-  SMTP простой протокол почтового обмена;

-  CMIP общий протокол управления информацией;

-  SLIP протокол последовательной посимвольной передачи данных;

-  SNMP простой протокол сетевого управления;

-  FTAM протокол передачи, доступа и управления файлами.

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

Функции данного уровня – представление данных, передаваемых между прикладными процессами, в нужной форме.

Этот уровень обеспечивает то, что информация, передаваемая прикладным уровнем, будет понятна прикладному уровню в другой системе.

Уровень преобразовывает данные в единый формат ASN.1 — служит для описания структуры файлов и позволяет решить проблемы шифрования данных.

На нём может выполняться шифрование и дешифрование данных, благодаря которым секретность обмена данными обеспечивается сразу для всех прикладных сервисов. Примером такого протокола является Secure Socket Layer (SSL). Этот уровень обеспечивает преобразование данных прикладного уровня в поток информации для транспортного уровня.

Могут выполняться: компрессия (сжатие данных), преобразование кодировок и т. д.

Представительный уровень выполняет следующие основные функции:

1.       Генерация запросов на установление сеансов взаимодействия прикладных процессов.

2.       Согласование представления данных между прикладными процессами.

3.       Реализация форм представления данных.

4.       Представление графического материала (чертежей, рисунков, схем).

5.       Засекречивание данных.

6.       Передача запросов на прекращение сеансов.

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

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

Сеансовый уровень содержит дополнительно функции управления паролями, управления диалогом, синхронизации и отмены связи в сеансе передачи после сбоя вследствие ошибок в нижерасположенных уровнях. Функции этого уровня состоят в координации связи между двумя прикладными программами, работающими на разных рабочих станциях. 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).

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

Функции:

* Установка и завершение соединения
* Выполнение нормального и срочного обмена данными
* Управление взаимодействием прикладных процессов
* Синхронизация сеансовых соединений
* Извещение прикладных процессов об исключительных ситуациях
* установление меток
* Прерывание сеанса
* Прекращение без потери данных
* Передача особых сообщение о ходе проведения сеанса

Отвечает за организацию сеансов обмена данными между оконченными машинами. Протокол этого уровня — составная часть протоколов трех верхних уровней модели.

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

Транспортный уровень предназначен для передачи пакетов через коммуникационную сеть.

На транспортном уровне пакеты разбиваются на блоки. На пути от отправителя к получателю пакеты могут быть искажены или утеряны. Работа транспортного уровня заключается в том, чтобы обеспечить приложениям или верхним уровням модели передачу данных с той степенью надежности, которая им требуется. Виды сервиса предоставляемые уровнем отличаются качеством предоставляемых услуг (5 классов сервиса): срочностью, возможностью восстановления прерванной связи, способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов, предоставление приоритетов при передаче блоков данных, наличием средств [мультиплексирования](http://scask.ru/book_r_cos.php?id=179) нескольких соединений между различными прикладными протоколами через общий [транспортный протокол](http://sernam.ru/book_icn.php?id=9).

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. Начиная с транспортного уровня, протоколы реализуются средствами, сетевой ОС:

-  TCP (TransmissionControlProtocol) протокол управления передачей стека TCP/IP;

-  UDP (User DatagramProtocol) пользовательский протокол дейтаграмм стека TCP/IP;

-  NCP (NetWareCoreProtocol) базовый протокол сетей NetWare;

-  SPX (SequencedPacketeXchange) упорядоченный обмен пакетами стека Novell;

-  TP4 протокол передачи класса 4;

Функции:

* Управление передачей по сети и обеспечение целостности пакетов
* Обнаружение ошибок, частичная их ликвидация, сообщение о неисправных ошибках
* Восстановление передачи после отказов, неисправностей
* Укрупнение или разделение пакетов
* Предоставление приоритетов
* Подтверждение передачи
* Ликвидация пакетов при тупиковых ситуациях в сети.

Начиная с транспортного уровня задачи реализуются программными свойствами, включенные в ОС = системная часть.

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

Сетевой уровень устанавливает связь в сети между 2 системами и обеспечивает прокладку виртуальных каналов между ними. Сетевой уровень сообщает транспортному уровню о появляющихся ошибках, эти сообщения принято называть пакетами. Уровень отвечает завершает формирование, а также отвечает за их адресацию и доставку.

Фактически основной задачей является прокладка наилучшего пути для передачи данных -маршрутизация, и ее решение. Часто критерием при выборе маршрута является время передачи данных по этому маршруту; оно зависит от пропускной способности [каналов связи](http://sernam.ru/book_p_net.php?id=5) и интенсивности трафика, которая может изменяться с течением времени. Выбор маршрута может осуществляться и по другим критериям, например, надежности передачи. Внутри сети доставка данных регулируется канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень. Внутри сети маршрут не нужен.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. Маршрутизатор – это устройство, которое собирает информацию о [топологии](http://sernam.ru/book_e_math.php?id=135) межсетевых соединений и на ее основании пересылает пакеты в сеть назначения. Для того чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач (hops) между сетями, каждый раз, выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, по которым проходит пакет.

Сетевой уровень выполняет функции:

1.       Создание сетевых соединений и идентификация их портов.

2.        Обнаружение и исправление ошибок, возникающих при передаче через коммуникационную сеть.

3.       Управление потоками пакетов, организация последовательностей пакетов.

4.       Маршрутизация и коммутации, сегментирование и объединение пакетов.

Протоколы:

1) определение правил передачи пакетов и данных конечных узлов от узла к маршрутизатору и между маршрутизаторами – сетевого уровня

2) протоколы общения маршрутизаторов – сбор актуальной информации о состоянии сети.

Протоколы сетевого уровня реализуются программными модулями ОС, программными и аппаратными средствами маршрутизаторов.

Наиболее часто на сетевом уровне используются протоколы:

-  IP (Internet Protocol) протокол Internet, [сетевой протокол](http://sernam.ru/book_icn.php?id=9) стека TCP/IP, который предоставляет адресную и маршрутную информацию;

-  IPX (InternetworkPacketExchange) 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 уровне 2);

-  CLNP (ConnectionLessNetworkProtocol) сетевой протокол без организации соединений.

- ARP и RARP –MACIP (по известному) и наоборот.

- ICMP протокол межсетевых управляющих сообщений

- IGMP протокол управления группами Интернета

- IPsec часть IPv6 + занимается шифрованием.

1. **Уровни модели OSI: канальный уровень (DataLink)**

Единицей информации канального уровня являются кадры (frame). Кадры – это логически организованная структура, в которую можно помещать данные (пакет с сетевого уровня).

1) задача формирование кадра и передача его на физический уровень.

2) задача является проверка доступности среды передачи.

3) задача реализация механизмов обнаружения и коррекции ошибок.

Обладает механизмом исправления ошибок типа инверсия.

Занимается контролем над доступностью передач, передачей информации об ошибках вверх.

Канальный уровень также вычисляет контрольную сумму, суммируя все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит, получатель снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется ошибка.

Спецификации IEEE 802.Х делят канальный уровень на два подуровня:

-  LLC (LogicalLinkControl) управление логическим каналом осуществляет логический контроль связи. Подуровень LLC обеспечивает обслуживание сетевого уровня и связан с передачей и приемом пользовательских сообщений.

-  MAC (MediaAssessControl) контроль доступа к среде. Подуровень MAC регулирует доступ к разделяемой физической среде (передача маркера или обнаружение коллизий или столкновений) и управляет доступом к [каналу связи](http://sernam.ru/book_p_net.php?id=5). Подуровень LLC находится выше подуровня МАC.

Канальный уровень может выполнять следующие виды функций:

1.       Организация (установление, управление, расторжение) канальных соединений и идентификация их портов.

2.       Организация и передача кадров.

3.       Обнаружение и исправление ошибок.

4.       Управление потоками данных.

Наиболее часто используемые протоколы на канальном уровне включают:

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

-  Ethernet сетевая технология по стандарту IEEE 802.3 для сетей, использующая шинную [топологию](http://sernam.ru/book_e_math.php?id=135) и коллективный доступ с прослушиванием несущей частоты и обнаружением конфликтов;

-  Tokenring сетевая технология по стандарту IEEE 802.5, использующая кольцевую топологию и метод доступа к кольцу с передачей маркера;

-  FDDI (FiberDistributedDateInterfaceStation) сетевая технология по стандарту IEEE 802.6, использующая оптоволоконный носитель;

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

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

Физический уровень предназначен для сопряжения с физическими средствами соединения. Физические средства соединения – это совокупность аппаратных и программных средств, обеспечивающая передачу сигналов между системами + кодирование сигналов. Физический уровень состоит из *Подуровня стыковки со средой* и *Подуровня преобразования передачи*.

Первый из них обеспечивает сопряжение потока данных с используемым физическим [каналом связи](http://sernam.ru/book_p_net.php?id=5). Второй осуществляет преобразования, связанные с применяемыми протоколами.

Манчестерское кодирование решает задачу преобразования 0 и 1 в сигналы соответсвующего типа.

На физическом уровне определяются следующие свойства среды:

* Тип используемых кабелей, разъемов, сопряженных со средой
* Правило разборки контактов в этих разъемах
* Схема кодировки

Физический уровень выполняет следующие функции:

1.  Установление и разъединение физических соединений.

2.  Передача сигналов в последовательном коде и прием.

3.  Прослушивание, в нужных случаях, каналов.

4.  Идентификация каналов.

5.  Оповещение о появлении неисправностей и отказов.

6. Обнаружение механического контакта.

Реализует синхронную/асинхронную передачу.

Физический уровень получает кадры данных от канального уровня и преобразует их в оптические или электрические сигналы, соответствующие 0 и 1 бинарного потока.

Физический уровень может обеспечивать как асинхронную (последовательную) так и синхронную (параллельную) передачу, которая применяется для некоторых мэйнфреймов и мини-компьютеров.

К числу наиболее распространенных спецификаций физического уровня относятся:

-  Ethernet – сетевая технология по стандарту IEEE 802.3 для сетей, использующая шинную [топологию](http://sernam.ru/book_e_math.php?id=135) и метод доступаCSMA/CD;

-  Tokenring – сетевая технология по стандарту IEEE 802.5, использующая кольцевую топологию и метод доступа TPMA.

1. **Спецификации стандартов 802.1 – 802.11**

**Стандартные стеки протоколов.**

**Стандарт IEEE 802.1** (объединение сетей) задает механизмы управления сетью на MAC-уровне.

**Стандарт IEEE 802.2** (управление логической связью) определяет функционирование подуровня LLC на канальном уровне [модели OSI](http://sernam.ru/book_icn.php?id=6).

**Стандарт IEEE 802.3** описывает физический уровень и подуровень MAC для сетей, использующих шинную [топологию](http://sernam.ru/book_e_math.php?id=135) и метод доступаCSMA/CD. Прототипом этого метода является метод доступа стандарта Ethernet (10BaseT, 10Base2, 10Base5). Метод доступа CSMA/CD. 802.3 также включает технологии FastEthernet (100BaseTx, 100BaseFx).

**Стандарт IEEE 802.4** определяет метод доступа к шине с передачей маркера, прототип – ArcNet.Этот метод предусматривает следующие правила:

-  все устройства, подключенные к сети, могут передавать данные, только получив разрешение на передачу (маркер);

-  в любой момент времени только одна станция в сети обладает таким правом;

-  кадр, передаваемый одной станцией, одновременно анализируется всеми остальными станциями сети.

**Стандарт IEEE 802.5** описывает метод доступа к кольцу с передачей маркера, прототип – TokenRing.

**Стандарт IEEE 802.6** (MetropolitanAreaNetwork – городские сети) описывает рекомендации для региональных сетей.

**Стандарт IEEE 802.7** описывает рекомендации по широкополосным сетевым технологиям, носителям, интерфейсу и оборудованию.

**Стандарт IEEE 802.8** содержит обсуждение использования оптических кабелей в сетях 802.3 – 802.6, а также рекомендации по оптоволоконным сетевым технологиям, носителям, интерфейсу и оборудованию, прототип – сеть FDDI (FiberDistributedDataInterface). Скорость сети до 100 Мб/с. Данная технология позволяет включать до 500 узлов на расстоянии 100 км.

**Стандарт IEEE 802.9** 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** рассмотрены вопросы обмена данными, шифрования, управления сетями и безопасности в сетевых архитектурах, совместимых с [моделью OSI](http://sernam.ru/book_icn.php?id=6).

**Стандарт IEEE 802.11** рекомендации по использованию беспроводных

1. **Спецификации стандартов 802.12 - 802.22.**

**Стандарт 802.12** описывает рекомендации по использованию сетей 100VG – AnyLAN со скоростью 100Мб/с и методом доступа по очереди запросов и по приоритету (DPQ, DPA). Технология 100VG – это комбинация Ethernet и Token-Ring со скоростью передачи 100 Мбит/c, работающая на неэкранированных витых парах. Имеется два уровня приоритетов – высокий и низкий.

**Стандарт IEEE 802.14** определяет функционирование кабельных модемов.

**Стандарт IEEE 802.15** рассматривает вопросы организации персональных сетей. В настоящее время уже существует несколько спецификаций данного стандарта.

*Стандарт IEEE 802.15.1* базируется на спецификациях Bluetooth v1.x. и предназначен для построения персональных беспроводных сетей (WPAN). Для работы радиоинтерфейса Bluetooth используется нижний (2,45 ГГц) диапазон, предназначенный для работы промышленных, научных и медицинских приборов.

*Стандарт IEEE 802.15.3* предназначен для беспроводных частных сетей и является прямым наследником Bluetooth (частота 2,4 ГГц). Шифрование данных в этой сети может осуществляться по стандарту AES 128.

*Стандарт IEEE 802.15.4* (ZigBee) ориентирован на использование в качестве средства связи между автономными приборами и оборудованием.

*Стандарт IEEE 802.15.4a* (UltraWideband, UWB) базируется на технологии сверхширокополосной связи (UWB).

**Стандарт IEEE 802.16** предназначен для реализации широкополосных каналов в городских сетях (MAN). Он ориентирован на соединение стационарных, а не мобильных объектов.

**Стандарт IEEE 802.17** называется RPR (адаптивное кольцо для пакетов), пакеты удаляются из кольца узлом-адресатом, что позволяет осуществлять несколько обменов одновременно.

**Стандарт IEEE 802.18** требования и рекомендации по радиочастотному регулированию.

**Стандарт IEEE 802.19** требования и рекомендации по сосуществованию.

**Стандарт IEEE 802.20** описывает правила беспроводного мобильного широкополосного доступа MBWA для пакетного интерфейса в беспроводных городских сетях WMAN.

**Стандарт IEEE 802.21** – это стандарт независимой от среды эстафетной передачи соединений.

**Стандарт IEEE 802.22** определяет функционирование беспроводных региональных сетей WRAN, использующих для передачи данных телевизионные частотные диапазоны.

1. **Понятия протоколов и стеков. Сетевые, транспортные, прикладные протоколы.**

Стеки протоколов — согласованный набор протоколов разных уровней, дост. Для организации межсетевого взаимодействия. Они разбиваются на три условных уровня: сетевые; транспортные; прикладные.

Для каждого уровня определен набор функций-запросов для взаимодействия с вышележащим уровнем, который называется интерфейсом.

Правила взаимодействия 2-х узлов могут быть описаны в виде процедур для каждого из уровней — протокол.

* TCP/IP
* IPX/SPX

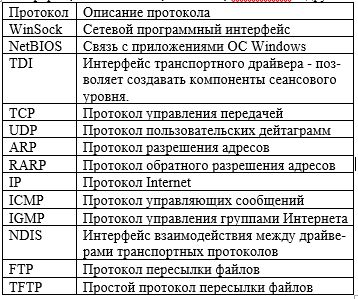
**Сетевые протоколы** предоставляют следующие услуги: адресацию и маршрутизацию информации, проверку на наличие ошибок, запрос повторной передачи и установление правил взаимодействия в конкретной сетевой среде.

* IP (Internet Protocol – Протокол Internet). Протокол стека TCP/IP, обеспечивающий адресную информацию и информацию о маршрутизации.
* IPX (Межсетевой обмен пакетами) в NWLink. Протокол NovelNetWare, используемый для маршрутизации и направления пакетов.
* DDP – используется в Apple Talk.
* NetBEUI – пользовательский интерфейс баз. Системой ввода/вывода. Транспортные услуги для NetBIOS.

**Транспортные протоколы** предоставляют следующие услуги надежной транспортировки данных между компьютерами.

* NetBIOS (Базовая сетевая система ввода вывода). NetBIOS устанавливает соединение между компьютерами, а NetBEUI предоставляет услуги передачи данных для этого соединения.
* SPX (Последовательный обмен пакетами) в NWLink. Протокол NovelNetWare, используемый для обеспечения доставки данных.
* TCP (Протокол управления передачей). Протокол стека TCP/IP, отвечающий за надежную доставку данных.
* АTP – сеансовый и транспортный протокол Apple Talk.

**Прикладные протоколы** отвечают за взаимодействие приложений.

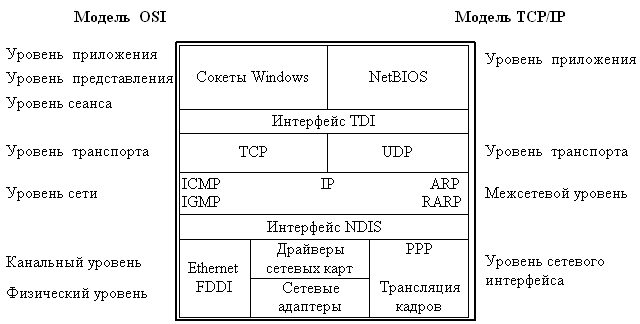
* FTP (File Transfer Protocol – Протокол передачи файлов). Протокол стека TCP/IP, используемый для обеспечения услуг по передачи файлов.
* SNMP (Простой протокол управления сетью). Протокол стека TCP/IP, используемый для управления и наблюдения за сетевыми устройствами.
* HTTP(Hyper Text Transfer Protocol) – протокол передачи гипертекста и другие протоколы.
* AFP – удаленное управление файлами «Макинтош».
* NCP – оболочка и редиректоры клиента NovelNetWare.

1. **Архитектура стека протоколов Microsoft TCP/IP.**

Набор многоуровневых протоколов, или как называют стек TCP/IP предназначен для использования в различных вариантах сетевого окружения. Модель TCP/IP включает большее число функций на один уровень, что приводит к уменьшению числа уровней.

Соответствует модели OSI с разницей, что верхние 3 уровня объединены в 1 уровень — уровень приложения.

Задачи физического и большей части канального уровня объединены в уровень сетевого интерфейса.



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

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

-  Сокеты Windows;

-  NetBIOS.

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

Интерфейс NetBIOS используется для связи между процессами (IPC – Interposes Communications) служб и приложений ОС Windows. NetBIOS выполняет три основных функции: определение имен NetBIOS; служба дейтаграмм NetBIOS; служба сеанса NetBIOS.

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

-  подтверждение получения информации;

-  управление потоком данных;

-  упорядочение и ретрансляция пакетов.

Алгоритм установки соединения:

Клиент запрашивает соединение. Отправляет серверу пакет, указывающий номер порта, который используется для передачи и свой ISM-код – число.

Сервер в случае согласия отвечает пакетом, который содержит имя сервера и … . Код клиента увеличивается на 1.

Клиент подтверждает соединение. При необходимости количество промежуточных шагов может быть увеличено.

При этом пакет будет содержать номер DSP-порта отправителя/получателя, номер фрагмента пакета, контрольную сумму, чтобы убедиться, что ошибок не произошло.

Конфликтов не возникает (могут совпадать по номеру, но они разные0.

В зависимости от типа службы могут быть использованы два протокола:

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

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

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

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

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

***Протокол IP*** обеспечивает обмен дейтаграммами между узлами сети и является протоколом, не устанавливающим соединения и использующим дейтаграммы для отправки данных из одной сети в другую.

Данный протокол не устанавливает соединения, исп. Дейтаграммы для отправки данных из одной сети в другую или внутри сети, не имеет отношения к вопросам корректности.

Функции: межсетевая адресация, при необходимости – запрос данных процесса.

В рамках сетей выделяют 3 вида адресов: физический, сетевой и символьный.

Для сопоставления сетевых адресов используется 2 протокола **ARP** и **RARP**.

ARP определяет физический адрес по сетевому.

Узел, которому нужно выполнить данное преобразование, формирует ARP-запрос, указывает в нем известный сетевой адрес, всё это вкладывает в кадр канального уровня и отправляет по сети широковещательно. Все узлы получают данный, но один, чей сетевой адрес имеется в запросе, формирует ARP-ответ, в котором указывает свой сетевой и физический адрес. Ответ отправляет направленно. ARP-запрос и ответ в одном и том же формате.

Обратное преобразование выполняет протокол RARP.

(Для определения локального адреса по IP-адресу используется протокол разрешения адреса **AddressResolutionProtocol** (ARP). ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети – протокол локальной сети (Ethernet, TokenRing, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети, или же протокол глобальной сети (X.25, framerelay), как правило, не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу – нахождение IP-адреса по известному локальному адресу. Он называется **реверсивный ARP** – RARP и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего [сетевого адаптера](http://sernam.ru/book_icn.php?id=29).)

Протокол **ICMP** управления сообщениями интернета используется IP и другими протоколами высокого уровня для отправки и получения отчетов о состоянии передаваемой информации.

Маршрутизатор используется для обмена информацией о состоянии сети, а также для управления скоростью передачи.

Если маршрутизатор перегружен трафиком, он может отправить специальное сообщение ICMP-ошибку для уменьшения скорости отправки сообщений.

**IGMP**. Узлы локальной сети используют этот протокол чтобы зарегистрировать себя в группе. Маршрутизатор использует эту информацию для передачи групповых сообщений.

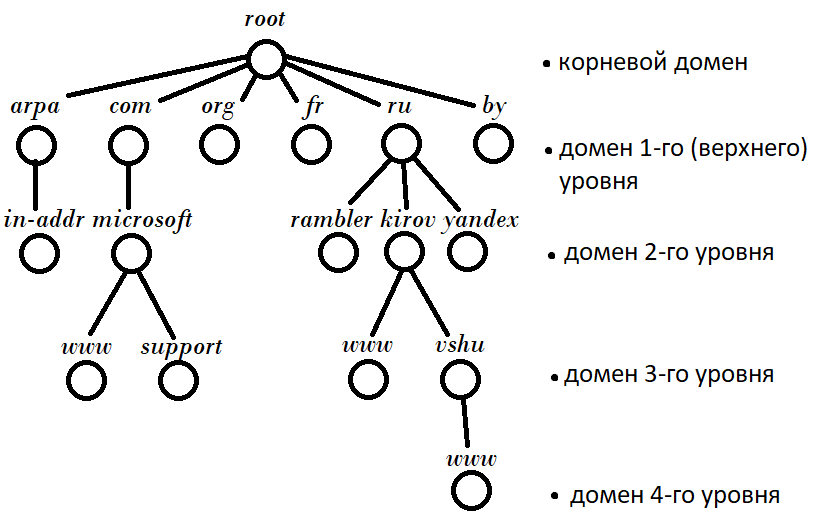
**Интерфейс** **NDIS**. – Спецификация интерфейса сетевого устройства, программный интерфейс, обеспечивающий взаимодействие между драйверами транспортных протоколов и соотв. Протоколов сетевых интерфейсов. Позволяет использовать несколько протоколов, даже если одна сетевая карта. (односторонний сетевой адаптер).

***Уровень сетевого интерфейса*** 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, TokenRing, затем IP-дейтаграмма помещается в область данных этого кадра, и он отправляется в сеть.

1. **Символьная адресация. Отличие DNS-имени от NetBIOS-имен. Структура DNS-имени.**

Символьный адрес, или **DNS-имя**, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес используется на прикладном уровне, например, в протоколах FTP или telnet. Для облегчения взаимодействия вначале применялись таблицы соответствия числовых адресов именам машин. По мере роста сети была разработана система доменных имен – DNS (DomainNameSystem), которая позволяет присваивать компьютерам легко запоминаемые имена и отвечает за перевод этих имен обратно в IP-адреса. DNS строится по иерархическому принципу, однако эта иерархия не является строгой. Фактически нет единого корня всех доменов Internet.

Компьютерное имя имеет по меньшей мере два уровня доменов, отделяемых друг от друга точкой (.). Идущие после доменов верхнего уровня домены обычно определяют либо регионы (ru), либо организации (belstu). Например, в имени somesite.spbgu.ru, somesite является поддоменом spbgu, который в свою очередь является поддоменом ru.

Корневой домен как реальный узел не существует. Он исполняет роль вершины дерева.

Его потомки – домены 1-го уровня. Они делятся на:

* .arpa – особый домен, который исп. Для преобразования IP-адресов в доменные;
* Домены организаций;
* Географические домены (стран).

Полностью определенное имя домена – FQDN записывается след. образом:

Имя хоста – через точку DNS-суффикс, последовательность доменных имен всех уровней – запись завершается точкой, после которой подразумевается корневой домен. Например, www.vshu.kirov.ru. WWW-имя хоста, остальное – суффикс. Точку в конце можно не ставить.

DNS – служба доменных имен, которая занимается переводом доменного имени в IP-адрес и обратно.

Главная задача поддержание ИЕРАРХИЧЕСКОГО пространства имен.

Пространство имен **NetBIOS**. — линейный список имен.

15 вид. символов, 16 – служебный. Если вид. < 15, оставшие места заполняются нулями.

- широковещательный запрос

- обращается к локальной БД NetBIOS-имен, хран. в файле LMHOSTS

- к центральной БД имен на сервере WINS

В зависимости от типа узла разрешение имени осуществляется с помощью различных комбинаций способов:

B-узел – широковещ.

P-узел – с помощью WINS сервера.

M-узел – комбинация p + b узлов.

H-узел – комбинация b + p узлов (сначала к серверу, в случае необходимости – широковещательно).

1. **Принципы разрешения DNS-имени.**

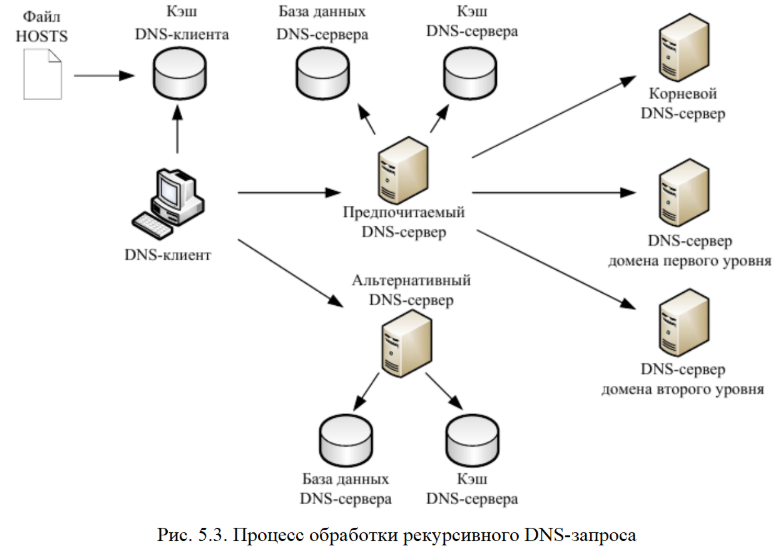
Процесс преобразования имени в IP-адрес называется разрешением доменного имени.

Служба поддерживающая распределяющую базу данных, которая хранится на специальных компьютерах — специальных DNS-серверах.

Информация не хранится в одном месте, ее части распределены по отдельным серверам (безопасность и нагрузка).

Например, за домены 1-го уровня отвечают 13 корневых серверов с именами от A.ROOT-SERVERS.NET до М.ROOT-SERVERS.NET, расположенных по всему миру.

Зоны. Исходя из удобства администрирования, 1 зона может содержать несколько доменов или 1 домен может быть рассредоточен по нескольким зонам.

Когда распространен по нескольким зонам: основная копия – primary zone, остальные дополнительные содержат вспомогательные копии – secondary zone.

Зоны обратного преобразования – для преобразования IP-адресов в доменные имена.

Процесс:

Служба построена по модели «клиент-сервер», то есть в процессе разрешения имен учавствуют DNS-клиенты и DNS-серверы.

Системные компоненты клиента, называемые DNS-распознавателями, отправляют запрос на сервер.

Виды запросов:

Итеративные — просьба разрешить имя без обращения к другим серверам (только к конкретному).

Рекурсивные — клиент перекладывает всю работу по разрешению имени на сервер. Если запрашиваемое имя отсутствует в базе данных и в кэше сервера, он отправляет итеративные запросы на другие сервера.

Сначала DNS-клиент осуществляет поиск в собственном локальном кэше DNS-имен. Это память для временного хранения ранее разрешенных запросов. В эту же память переносится содержимое файла HOSTS (каталог windows/system32/drivers/etc). Утилита IPconfig с ключом /displaydns отображает содержимое DNS-кэша. Если кэш не содержит требуемой информации, DNS-клиент обращается с рекурсивным запросом к предпочитаемому DNS-серверу (Preferred DNS server), адрес которого указывается при настройке стека TCP/IP. DNS-сервер просматривает собственную базу данных, а также кэш-память, в которой хранятся ответы на предыдущие запросы, отсутствующие в базе данных. В том случае, если запрашиваемое доменное имя не найдено, DNS-сервер осуществляет итеративные запросы к DNS-серверам верхних уровней, начиная с корневого DNS-сервера.

Рассмотрим процесс разрешения доменного имени на примере. Пусть, требуется разрешить имя www.microsoft.com. Корневой домен содержит информацию о DNS-сервере, содержащем зону .com. Следующий запрос происходит к этому серверу, на котором хранятся данные о всех поддоменах зоны .com, в том числе о домене microsoft и его DNS-сервере. Сервер зоны microsoft.com может непосредственно разрешить имя www.microsoft.com в IP-адрес.

Иногда оказывается, что предпочитаемый DNS-сервер недоступен. Тогда происходит запрос по той же схеме к альтернативному DNS-серверу, если, конечно, при настройке стека TCP/IP был указан его адрес.

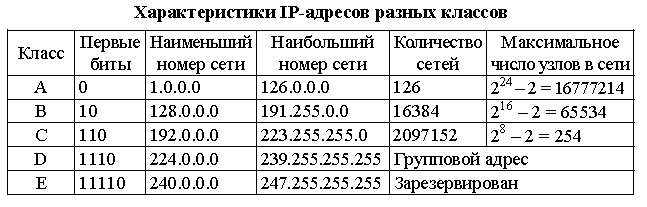
1. **Структура IPv4. Классы IP-адресов.**

IP-адрес представляет собой 32-разрядное двоичное число, разделенное на группы по 8 бит, называемые октетами. Например, 00010001.11101111.00101111.01011110.

Обычно IP-адреса записываются в виде четырех десятичных октетов и разделяются точками. Таким образом, приведенный выше IP-адрес можно записать в следующей форме: 17.239.47.94. Следует заметить, что максимальное значение октета равно111111112 (двоичная система счисления), что соответствует в десятичной системе 25510. Поэтому IP-адреса, в которых хотя бы один октет превышает это число, являются недействительными.

IP-адрес состоит из двух логических частей – номера подсети (ID подсети) и номера узла (ID хоста) в этой подсети. При передаче пакета из одной подсети в другую используется ID подсети. Когда пакет попал в подсеть назначения, ID хоста указывает на конкретный узел в рамках этой подсети.

Чтобы записать ID подсети, в поле номера узла в IP-адресе ставят нули. Чтобы записать ID хоста, в поле номера подсети ставят нули. Например, если в IP-адресе 172.16.123.1 первые два байта отводятся под номер подсети, остальные два байта – под номер узла, то номера записываются следующим образом: ID подсети172.16.0.0; ID хоста 0.0.123.1.По числу разрядов, отводимых для представления номера узла(или номера подсети), можно определить общее количество узлов(или подсетей) по простому правилу: если число разрядов для представления номера узла равно N, то общее количество узлов равно 2N – 2. Два узла вычитаются вследствие того, что адреса со всеми разрядами, равными нулям или единицам, являются особыми и используются в специальных целях. Для определения того, какая часть IP-адреса отвечает за ID подсети, а какая за ID хоста, применяются два способа: с помощью классов и с помощью масок.



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).

Маска подсети записывается либо в виде, аналогичном записи IP-адреса, например, 255.255.255.0, либо совместно с IP-адресом с помощью указания числа единичных разрядов в записи маски, например, 192.168.1.1/24, т. е. в маске содержится 24 единицы (255.255.255.0). При использовании масок можно вообще отказаться от понятия классов.

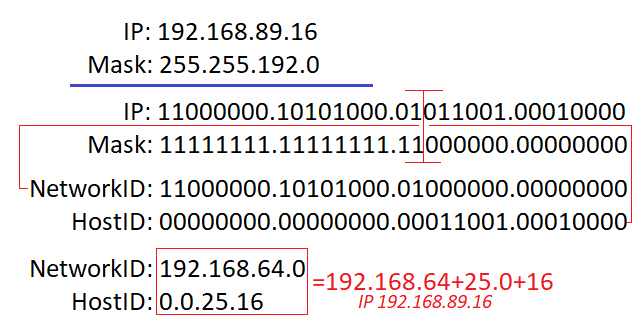
Маска должна советовать правилам корректности:

* Начинаться с 1 в двоичном виде
* Последовательность 1 должна быть непрерывной.

Для корректности маска может начинаться с 255, 254, 252, 248, 240, 224, 192, 128. Если стоит 255, то за ним может следовать ещё одно из приведенных чисел, так как октет оканчивается на 1. Если октет заканчивается 0, за ним могут стоять только 0.

Всего может быть составлена 31 маска!

Пример определения NetworkID и HostID с использованием масок:



1. **Структурирование сетей с помощью масок.**

Часто администраторы сетей испытывают неудобства, из-за того, что количество централизовано выделенных им номеров сетей недостаточно для того, чтобы структурировать сеть надлежащим образом, например, разместить все слабо взаимодействующие компьютеры по разным сетям.

В такой ситуации возможны два пути. Первый из них связан с получением от NIC дополнительных номеров сетей. Второй способ, употребляющийся более часто, связан с использованием так называемых*масок*, которые позволяют разделять одну сеть на несколько сетей.

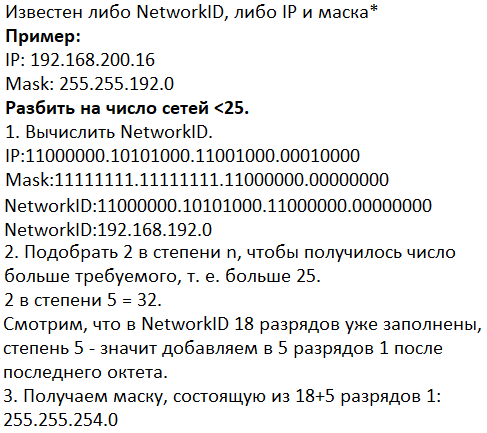
Маска — это число, двоичная запись которого содержит единицы в тех разрядах, которые должны интерпретироваться как номер сети.

Например, для стандартных классов сетей маски имеют следующие значения:

255.0.0.0 - маска для сети класса А,

255.255.0.0 - маска для сети класса В,

255.255.255.0 - маска для сети класса С.

В масках, которые использует администратор для увеличения числа сетей, количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты.

Пусть, например, маска имеет значение 255.255.192.0 (11111111 11111111 11000000 00000000). И пусть сеть имеет номер 129.44.0.0 (10000001 00101100 00000000 00000000), из которого видно, что она относится к классу В. После наложения маски на этот адрес число разрядов, интерпретируемых как номер сети, увеличилось с 16 до 18, то есть администратор получил возможность использовать вместо одного, централизованно заданного ему номера сети, четыре:

129.44.0.0 (10000001 00101100 00000000 00000000)

129.44.64.0 (10000001 00101100 01000000 00000000)

129.44.128.0 (10000001 00101100 10000000 00000000)

129.44.192.0 (10000001 00101100 11000000 00000000)

Например, IP-адрес 129.44.141.15 (10000001 00101100 10001101 00001111), который по стандартам IP задает номер сети 129.44.0.0 и номер узла 0.0.141.15, теперь, при использовании маски, будет интерпретироваться как пара:

129.44.128.0 - номер сети, 0.0. 13.15 - номер узла.

Таким образом, установив новое значение маски, можно заставить маршрутизатор по-другому интерпретировать IP-адрес. При этом два дополнительных последних бита номера сети часто интерпретируются как номера подсетей.

Еще один пример. Пусть некоторая сеть относится к классу В и имеет адрес 128.10.0.0 (рисунок 4.4).Этот адрес используется маршрутизатором, соединяющим сеть с остальной частью интерсети. И пусть среди всех станций сети есть станции, слабо взаимодействующие между собой. Их желательно было бы изолировать в разных сетях. Для этого сеть можно разделить на две сети, подключив их к соответствующим портам маршрутизатора, и задать для этих портов в качестве маски, например, число 255.255.255.0, то есть организовать внутри исходной сети с централизовано заданным номером две подсети класса C (можно было бы выбрать и другой размер для поля адреса подсети). Извне сеть по-прежнему будет выглядеть, как единая сеть класса В, а на местном уровне это будут две отдельные сети класса С. Приходящий общий трафик будет разделяться местным маршрутизатором между подсетями.

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 (петля, замыкание на себя) 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 1, адрес называется ограниченным широковещательным (limited broadcast). Пакеты, направленные по такому адресу, рассылаются всем узлам той подсети, в которой находится отправитель пакета.

4. Если все биты ID хоста равны 1, адрес -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 не256, а 254 узлов.

Служба распределения номеров IANA зарезервировала для частных адресов 3 блока:

1 сеть класса А – 10.0.0.0 – 10.255.255.255. Диапазон) 10.0.0.1 – 10.255.255.254

16 сетей класса В – 172.16.0.0 – 172.31.255.255. Диапазон) 172.16.0.0 – 172.31.0.0 (NW), 172.16.0.1 – 172.31.255.254 (IP).

256 сетей класса С – 192.168.0.0 – 192.168.255.255.

Любая организация может использовать эти адреса из данных блоков. Но они предназначены только для внутреннего использования.

К частным относится 1 сеть класса В с NW ID 169.254.0.0, который используется Виндовс для автоматического предоставления IP адреса при отсутствии DNS-сервера.

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

Длина 128 бит, автоматическая конфигурация (динамическая настройка без использования DHCP), встроенная безопасность.

Существует 3 типа адресов:

* Unicast – идентификатор одиночного интерфейса маршрутизатора.
* Anycast – идентификатор набора интерфейсов принадлежащих различным узлам. Пакет доставляется одному из интерфейсов, указанном в адресе (ближайшему, в соответствии с мерой, определенной протоколом маршрутизации).
* Multicast – идентификатор набора интерфейсов принадлежащих разным узлам. Пакет доставляется всем указанным интерфейсам.

Интерфейс – средство подключения узла к каналу.

Модель адресации:

Адреса всех типов ассоциированы с интерфейсами, а не с узлами. Так как каждый интерфейс принадлежит только одному узлу, уникастный адрес интерфейса может идентифицировать узел.

Соотносится только с 1 интерфейсом!

* Одиночный адрес может быть присвоен нескольким физическим интерфейсам – если приложение рассматривается как единое целое в интернете.
* Маршрутизаторы могут изменять нумерацию интерфейсов – исключение – необходимость вручную объявлять адрес.

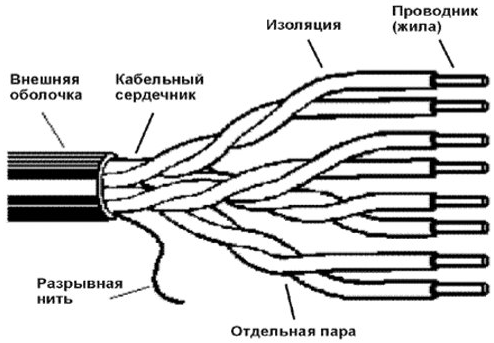
IPv6 соответствует модели IPv4, где подсеть ассоциируется с каналом. 1 канал — 1+ подсетей.

В IPv6 не существует широковещательных адресов их функции принадлежат multicast адресам. Основная форма записи IPv6: X:X:X:X:X:X:X:X – ‘X’ – Адреса IPv6 отображаются как восемь четырёхзначных [шестнадцатеричных чисел](https://ru.wikipedia.org/wiki/%D0%A8%D0%B5%D1%81%D1%82%D0%BD%D0%B0%D0%B4%D1%86%D0%B0%D1%82%D0%B5%D1%80%D0%B8%D1%87%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F) (то есть групп по четыре символа), разделённых двоеточием. 2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d. В каждом поле должна быть по крайней мере 1 цифра.

Если две и более групп подряд равны 0000, то они могут быть опущены и заменены на двойное двоеточие (::). Сокращению не могут быть подвергнуты 2 разделённые нулевые группы из-за возникновения неоднозначности.

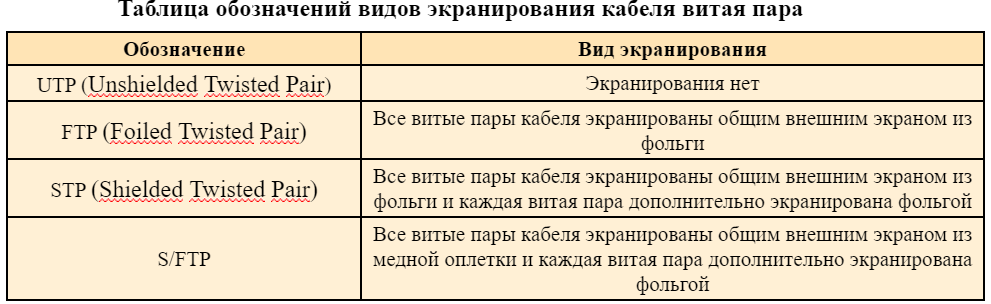
Существует альтернативная форма записи. 0:0:0:0:0:0:13.1.68.3 — ::13.1.68.3. С IPv6 и IPv4.

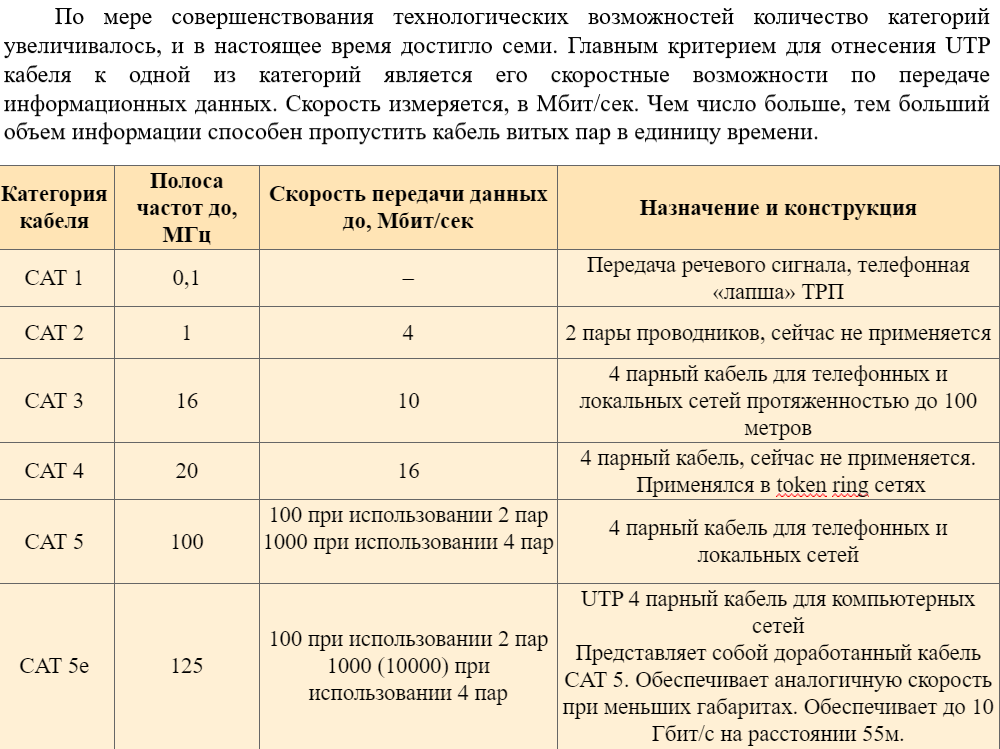
1. **Кабель типа «витая пара» (twisted pair). Схемы разводки. Кабельные системы Ethernet.**

Выделяют два больших класса кабелей: электрические и оптические, которые принципиально различаются по способу передачи по ним сигнала. Из кабелей связи и других элементов (монтаж, крепеж, кожухи и т. д.) строят линии связи между узлами сети.

Витая пара представляет собой одну или несколько **пар** изолированных проводников, скрученных между собой. Скручивание проводов уменьшает электрические помехи извне при распространении сигналов по кабелю, а экранированные витые пары еще более увеличивают степень помехозащищенности сигналов.

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







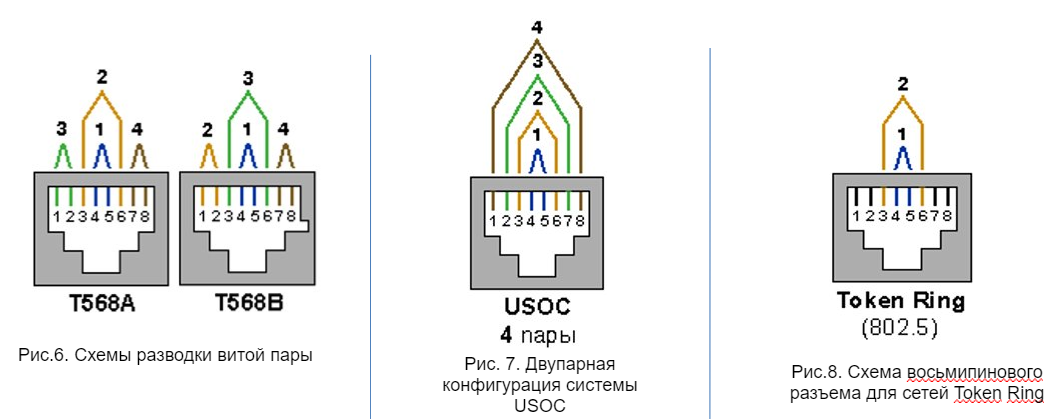
Экранированная витая пара STP хорошо защищает передаваемые сигналы от внешних помех, а также меньше излучает электромагнитных колебаний вовне, что защищает, в свою очередь, пользователей сетей от вредного для здоровья излучения. Наличие заземляемого экрана удорожает кабель и усложняет его прокладку, так как требует выполнения качественного заземления. Экранированный кабель применяется только для передачи данных, а голос по нему не передают.​

Основным стандартом, определяющим параметры экранированной витой пары, является фирменный стандарт IBM. В этом стандарте кабели делятся не на категории, а на типы: Туре 1, Туре 2, ..., Туре 9.​

Электрические параметры кабеля Туре 1 примерно соответствуют параметрам кабеля UTP категории 5. Некоторые стандарты поддерживают кабель STP Туре 1 –например, 100VG-AnyLAN, а также Fast Ethernet (хотя основным типом кабеля для Fast Ethernet является UTP CAT 5).​

Характеристики неэкранированной витой пары:​

* диаметр проводников 0.4–0.6 мм (22~26 AWG), 4 скрученных пары (8 проводников, из которых для 10Base-T, 100Base-TX 1000Base-TX используются одну, две или четыре пары (кабель должен иметь категорию 3, 5 или 6 и качество data grade или выше);​
* максимальная длина сегмента 100 м;​
* разъемы восьмиконтактные RJ-45. ​

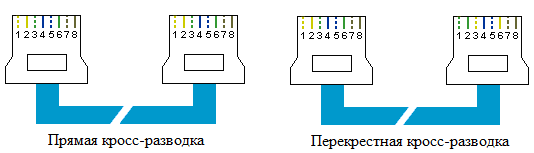
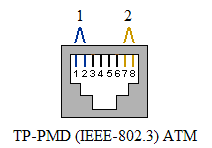
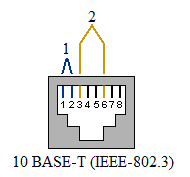


Схемы:

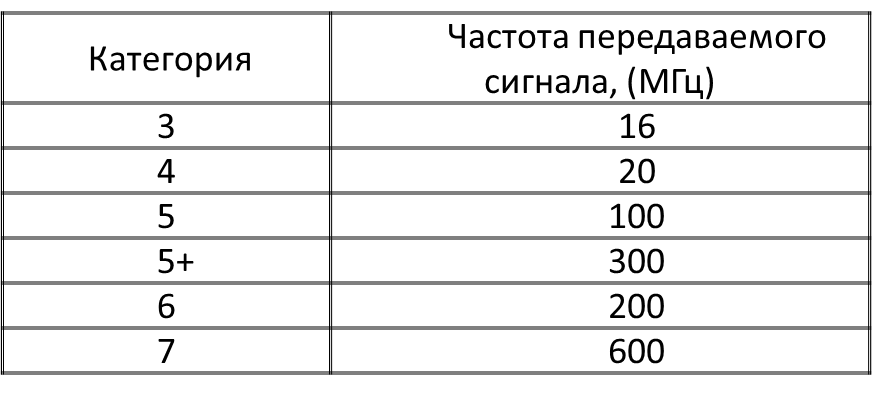
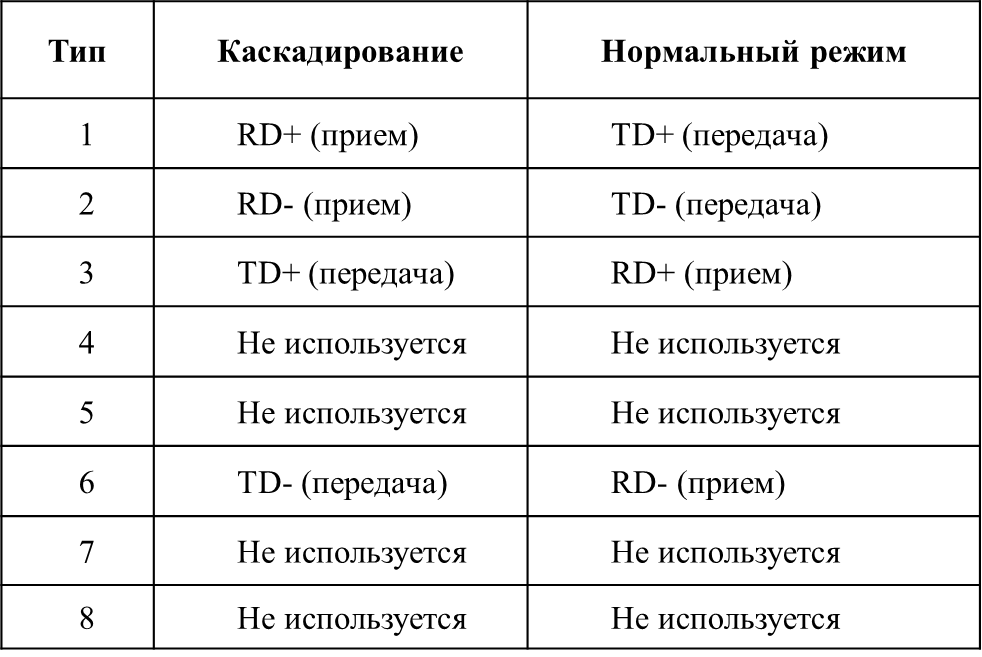
Т 568В — БЖ Ж БЗ С БС З БК К

Т 568А — БЗ З БЖ С БС Ж БК К

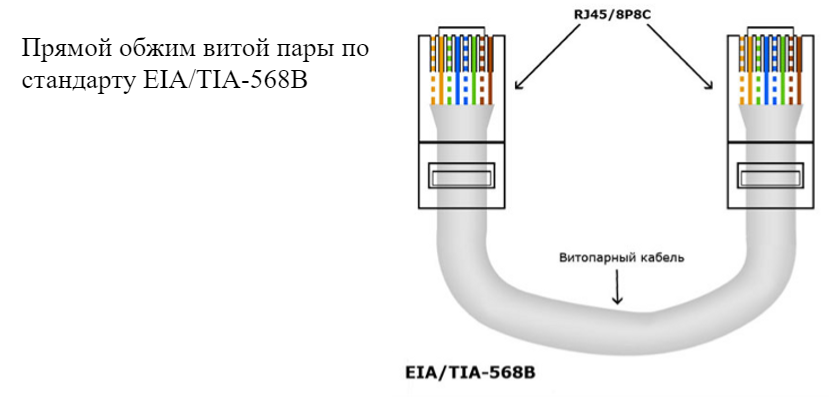
Кабельные системы: Неэкранированная витая пара (**10Base-T, 100Base-TX)**,Тонкий коаксиальный кабель(**10Base2),** Толстый коаксиальный кабель **(10Base5)**

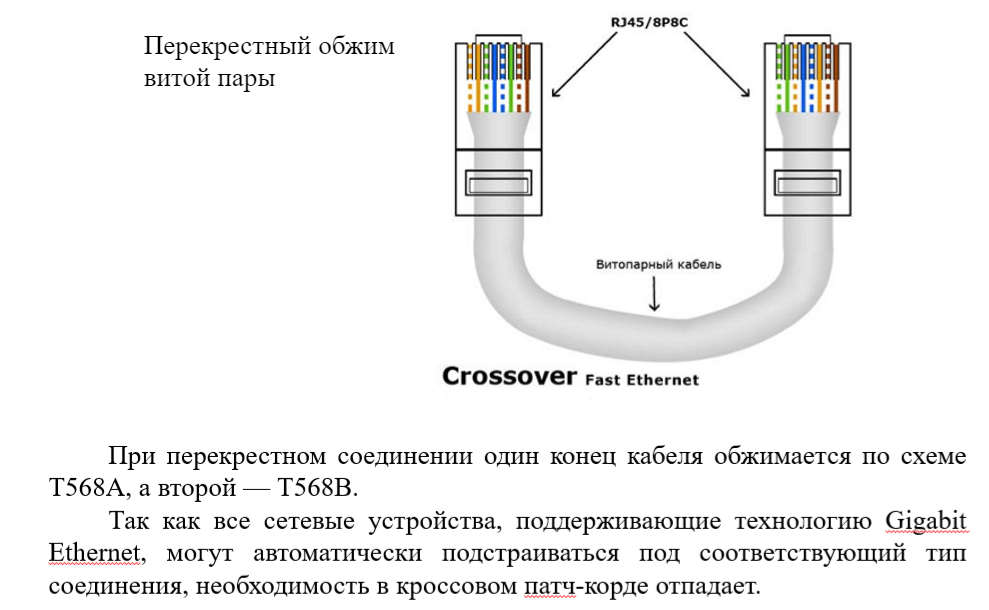


При передаче сигнала со скоростью 1Гбит/с задействованы все 4 пары проводников. Для 100 мегабитного соединения необходимы только 2 пары — зеленая и оранжевая. В этом случае для передачи сигнала используются контакты 1 и 2 коннектора, а для приема — 3 и 6. Синяя и коричневая пары остаются свободными.​

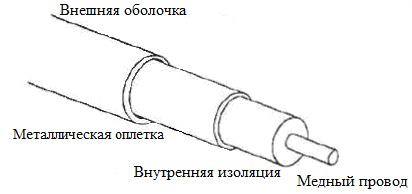






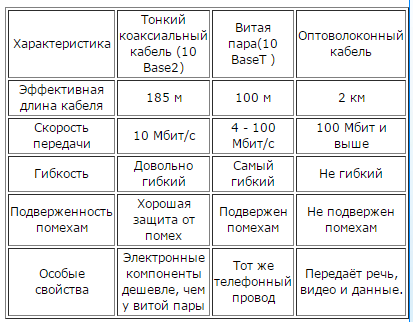


1. **Кабели и структурированные кабельные системы. Коаксиальные кабели.**

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

Характеристики спецификации 10Base2:

* тонкий коаксиальный кабель;
* максимальная длина сегмента – 185 м;
* минимальное расстояние между узлами – 0,5 м;
* максимальное число узлов в сегменте – 30.



Характеристики спецификации 10Base5:

* толстый коаксиальный кабель;
* максимальная длина сегмента – 500 метров;
* минимальное расстояние между узлами – 2,5 м;
* максимальное число узлов в сегменте – 100.

Физическая среда является основой, на которой строятся физические средства соединения. Сопряжение с физическими средствами соединения посредством физической среды обеспечивает физический уровень. ​

В качестве физической среды широко используются эфир, металлы, оптическое стекло и кварц. Среда передачи данных может включать как кабельные, так и беспроводные технологии. Хотя физические кабели являются наиболее распространенными носителями для сетевых коммуникаций, беспроводные технологии все более внедряются благодаря их способности связывать глобальные сети.​

Механические и электрические (оптические) свойства среды передачи включают:​

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

В качестве среды передачи данных используются различные виды кабелей: ​

* коаксиальный;​
* кабель на основе экранированной и неэкранированной витой пары;​
* оптоволоконный кабель. ​

Фундаментом сети является **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 компьютерных сетях.​

**Преимущества** структурированной кабельной системы​

\*Универсальность.​ Структурированная кабельная система при продуманной организации может стать единой средой для передачи любых компьютерных данных в компьютерной сети.​

​\*Увеличение срока службы. ​Срок старения хорошо структурированной кабельной системы может составлять 8–10 лет или даже более.​

\*Уменьшение стоимости добавления новых пользователей и изменения их мест размещения. Стоимость кабельной системы в основном определяется не стоимостью кабеля, а стоимостью работ по его прокладке.​

\*Возможность легкого расширения сети. Структурированная кабельная система является модульной, поэтому ее легко наращивать, позволяя легко и ценой малых затрат переходить на более совершенное оборудование, удовлетворяющее растущим требованиям к системам коммуникаций.​

​\*Обеспечение более эффективного обслуживания. ​Структурированная кабельная система облегчает обслуживание и поиск неисправностей.​

\*Надежность.​ Структурированная кабельная система имеет повышенную надежность, поскольку обычно производство всех ее компонентов и техническое сопровождение осуществляется одной фирмой-производителем.​

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

Обычно кабели присоединяются к оборудованию с помощью разъемов. Кроме этого, для обеспечения быстрой перекоммутации кабелей и оборудования используются различные электромеханические устройства, называемые кроссовыми секциями, кроссовыми коробками, или шкафами.​

​Наиболее важные характеристики кабелей:​

* Затухание (Attenuation). Затухание измеряется в децибелах на метр для определенной частоты или диапазона частот сигнала.​
* Перекрестные наводки на ближнем конце (Near End Cross Talk, NEСT). Измеряются в децибелах для определенной частоты сигнала.​
* Импеданс (impedance, волновое сопротивление) – это полное (активное и реактивное) сопротивление в электрической цепи. ​
* Активное сопротивление – это сопротивление постоянному току в электрической цепи. В отличие от импеданса активное сопротивление не зависит от частоты и возрастает с увеличением длины кабеля.​
* Емкость – это свойство металлических проводников накапливать энергию.​
* Уровень внешнего электромагнитного излучения, или электрический шум. Электрический шум – это нежелательное переменное напряжение в проводнике. Электрический шум бывает двух типов: фоновый и импульсный. ​
* Диаметр, или площадь сечения проводника. Для медных проводников достаточно употребительной является американская система AWG (American Wire Gauge), которая вводит некоторые условные типы проводников, например 22 AWG, 24 AWG, 26 AWG. Чем больше номер типа проводника, тем меньше его диаметр.​

1. **Сетевые адаптеры (Network Interface Card). Назначение. Функции. Типы.**

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

Сетевой адаптер относится к периферийному устройству компьютера, непосредственно взаимодействующему со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами. Это устройство решает задачи надежного обмена двоичными данными, представленными соответствующими сигналами (электрическими, оптическими и др.), по внешним линиям связи. ​

Как и любой контроллер компьютера, сетевой адаптер работает под управлением драйвера операционной системы, и распределение функций между сетевым адаптером и драйвером может изменяться от реализации к реализации. ​

Это устройство решает задачи **надежного обмена двоичными данными**, представленными соответствующими электромагнитными сигналами, по внешним линиям связи.

Для работы ПК в сети надо правильно установить и настроить сетевой адаптер. 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). ​

Обычно сетевая карта обнаруживает конфликт, если двум устройствам назначен один и тот же ресурс (запрос на прерывание или адрес ввода/вывода). Сетевые карты поддерживают различные типы сетевых соединений. ​

​Физический интерфейс между самой сетевой картой и сетью называют трансивером (transceiver) – это устройство, которое как получает, так и посылает данные. Трансиверы на сетевых картах могут получать и посылать цифровые и аналоговые сигналы.​

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

1. Гальваническая развязка с коаксиальным кабелем или витой парой.

2. Прием (передача) данных.

3. Буферизация. Во время обработки в сетевом адаптере, данные хранятся в буфере.

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

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

6. Идентификация своего адреса в принимаемом пакете.

7. Преобразование параллельного кода в последовательный код при передаче данных, и наоборот при приеме.

8. Кодирование и декодирование данных.

9. Передача или прием импульсов. В режиме передачи закодированные электрические импульсы данных передаются в кабель.

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

Все современные сетевые адаптеры поддерживают технологию Plug and Play. Если сетевую карту установить в компьютер, то при первой загрузке система определит тип адаптера и запросит для него драйверы (либо установит их автоматически). ​

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

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

Различные типы сетевых адаптеров отличаются следующими параметрами:​

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

1. **Повторители и концентраторы. Назначение. Особенности использования.**

Основная функция *повторителя* это – повторение сигналов, поступающих 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 или хабом, что отражает тот факт, что данное устройство реализует не только функцию повторения сигналов, но и концентрирует в одном центральном устройстве функции объединения компьютеров в сеть.

*Концентратор* – устройство, у которого суммарная пропускная способность входных каналов выше пропускной способности выходного канала. Так как потоки входных данных в концентраторе больше выходного потока, то главной его задачей является концентрация данных. При этом возможны ситуации, когда число блоков данных, поступающее на входы концентратора, превышает его возможности. Тогда концентратор ликвидирует часть этих блоков. Ядром концентратора является процессор. Для объединения входной информации чаще всего используется множественный доступ с разделением времени. Концентратор является активным оборудованием, служит центром звездообразной конфигурации сети и обеспечивает подключение сетевых устройств.

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

Отрезки кабеля, соединяющие два компьютера или какие-либо два других сетевых устройства, называются физическими сегментами, поэтому концентраторы и повторители, которые используются для добавления новых физических сегментов, являются средством физической (но не логической) структуризации сети. ​

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

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

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

-объединение сегментов с различными физическими средами (например, коаксиал, витая пара и оптоволокно) в единый логический сегмент;​

-автосегментация портов – автоматическое отключение порта при его некорректном поведении (повреждение кабеля, интенсивная генерация пакетов ошибочной длины и т. п.);​

-поддержка между концентраторами резервных связей, которые используются при отказе основных;​

-защита передаваемых по сети данных от несанкционированного доступа (например, путем искажения поля данных в кадрах, повторяемых на портах, не содержащих компьютера с адресом назначения);​

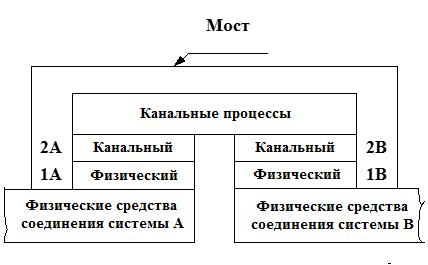
-поддержка средств управления сетями – протокола SNMP, баз управляющей информации MIB. ​

Многосегментные концентраторы нужны для создания разделяемых сегментов, состав которых может легко изменяться. ​

В таких концентраторах имеется несколько несвязанных внутренних шин, которые предназначены для создания нескольких разделяемых сред. Например, концентратор имеет три внутренние шины Ethernet. Если в таком концентраторе 72 порта, то каждый из этих портов может быть связан с любой из трех внутренних шин. Между собой компьютеры, подключенные к разным сегментам, общаться через концентратор не могут, так как шины внутри концентратора никак не связаны.​

​Большинство многосегментных концентраторов позволяют выполнять операцию соединения порта с одной из внутренних шин чисто программным способом, например, с помощью локального конфигурирования через консольный порт.​

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

Мост – ретрансляционная система, соединяющая каналы передачи данных.

В соответствии с базовой эталонной моделью взаимодействия открытых систем мост описывается протоколами физического и канального уровней, над которыми располагаются канальные процессы. Мост опирается на пару связываемых им физических средств соединения, которые в этой модели представляют физические каналы. ​

Мост преобразует физический (1A, 1B) и канальный (2A, 2B) уровни различных типов.​

 Мост, а также его быстродействующий аналог коммутатор (switching hub), делят общую среду передачи данных на логические сегменты. ​

Логический сегмент образуется путем объединения нескольких физических сегментов (отрезков кабеля) с помощью одного или нескольких концентраторов. Каждый логический сегмент подключается к отдельному порту моста/коммутатора. При поступлении кадра на какой-либо из портов мост/коммутатор повторяет этот кадр, но не на всех портах, как это делает концентратор, а только на том порту, к которому подключен сегмент, содержащий компьютер-адресат. ​

Мосты могут соединять сегменты, использующие разные типы носителей, например, 10BaseT и 10Base2. Они могут соединять сети с разными методами доступа к каналу, например, сети Ethernet (CSMA/CD) и TokenRing (TPMA).

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

    Часто мосты наделяются дополнительными функциями. Такие мосты обладают определенным интеллектом (интеллектом в сетях называют действия, выполняемые устройствами) и фильтруют сквозь себя блоки данных, адресованные абонентским системам, расположенным в той же сети. ​

Блоки, проходящие через интеллектуальный мост, дважды проверяются, на входе и выходе. Это позволяет предотвращать появление ошибок внутри моста.​

Мосты не имеют механизмов управления потоками блоков данных. Поэтому может оказаться, что входной поток блоков окажется большим, чем выходной. В этом случае мост не справится с обработкой входного потока, и его буферы могут переполняться. Чтобы этого не произошло, избыточные блоки выбрасываются. ​

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

В итоге, наиболее частое использование мостов – соединение глобальной сети с локальной.​

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

**Разница между мостом и маршрутизатором**. Мосты способны к анализу сообщений. они принимают решение по поводу адресации каждого из поступивших пакетов данных, переправлять его через мост или нет в зависимости от адреса назначения. Маршрутизаторы же выбирают из таблицы маршрутов наилучший для данного пакета. При связывании сетей с различными протоколами лучше использовать мосты.

1. **Коммутаторы. Назначение. Особенности использования.**

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

Общая структура коммутатора аналогична структуре моста, т.е. современные коммутаторы оперируют не только на физическом, но и на канальном уровне модели OSI.​

В коммуникационной сети коммутатор является ретрансляционной системой, обладающей свойством прозрачности (т.е. коммутация осуществляется здесь без какой-либо обработки данных). Коммутатор не имеет буферов и не может накапливать данные. Поэтому скорости передачи сигналов в соединяемых каналах должны быть одинаковыми. Канальные процессы, выполняются интегральными схемами. не используется программное обеспечение.

Коммутатор (Switch) может соединять серверы в кластер и служить основой для объединения нескольких рабочих групп. Он направляет пакеты данных между узлами ЛВС.

Коммутатор не имеет буферов и не может накапливать данные. Поэтому при использовании коммутатора скорости передачи сигналов в соединяемых каналах передачи данных должны быть одинаковыми. Канальные процессы, реализуемые коммутатором, выполняются специальными интегральными схемами.​

Коммутатор может соединять серверы в кластер и служить основой для объединения нескольких рабочих групп (разных логических сегментов сети). Он направляет пакеты данных между узлами сети. ​

Каждый коммутируемый сегмент получает доступ к каналу передачи данных без конкуренции и видит только тот трафик, который направляется в его сегмент. Коммутатор должен предоставлять каждому порту возможность соединения с максимальной скоростью без конкуренции со стороны других портов (в отличие от совместно используемого концентратора). ​

Обычно в коммутаторах имеются один или два высокоскоростных порта, а также хорошие инструментальные средства управления. ​

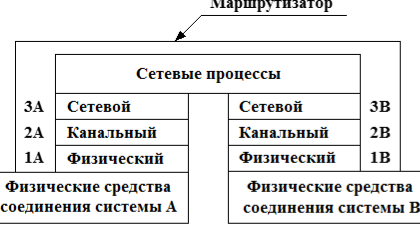
Коммутатор локальной сети (local area network switch) – устройство, обеспечивающее взаимодействие сегментов одной либо группы локальных сетей.​

Коммутатор локальной сети, как и обычный коммутатор, обеспечивает взаимодействие подключенных к нему локальных сетей ​



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

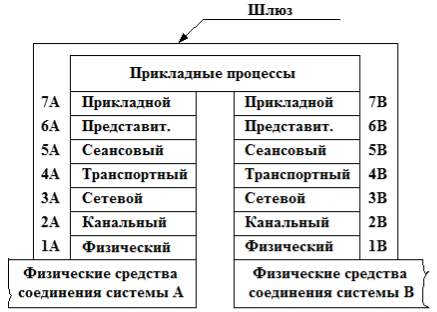
Маршрутизатор (router) – ретрансляционная система, соединяющая две коммуникационные сети либо их части, реализует протоколы физического, канального уровней.



Маршрутизатор работает с несколькими каналами, направляя в какой-нибудь из них очередной блок данных. Для этого он по адресу пришедшего блока и таблице маршрутизации определяет имя канала, в который этот блок должен быть передан. Маршрутизаторы обмениваются информацией об изменениях структуры сетей, трафике и их состоянии. Благодаря этому, выбирается оптимальный маршрут следования блока данных в разных сетях от абонентской системы-отправителя к системе-получателю.

Маршрутизаторы могут принимать решение о выборе оптимального пути для данных между двумя сетевыми сегментами, не анализируя их.

Необходимо отметить, что для работы маршрутизаторов требуется один и тот же протокол во всех сегментах, с которыми он связан.

**Шлюз** является наиболее сложной ретрансляционной системой, обеспечивающей взаимодействие сетей с различными наборами протоколов всех семи уровней.

***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.

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

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

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

Шлюзы оперируют на верхних уровнях модели OSI (сеансовом, представительском и прикладном) и представляют наиболее развитый метод подсоединения сетевых сегментов и компьютерных сетей. Необходимость в сетевых шлюзах возникает при объединении двух систем, имеющих различную архитектуру. ​

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 и расстоянию передачи. Большое значение имеют помехи и стоимость. Можно выделить три основных типа беспроводной технологии: радиосвязь; связь в микроволновом диапазоне; инфракрасная связь.

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

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

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

Wi-Fi-сети (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.​

Достоинства беспроводных сетей:

a) мобильность пользователей.

б) отсутствие необходимости монтажа кабельной системы.

в) простота подключения пользовательских устройств.

Недостатки беспроводных сетей:

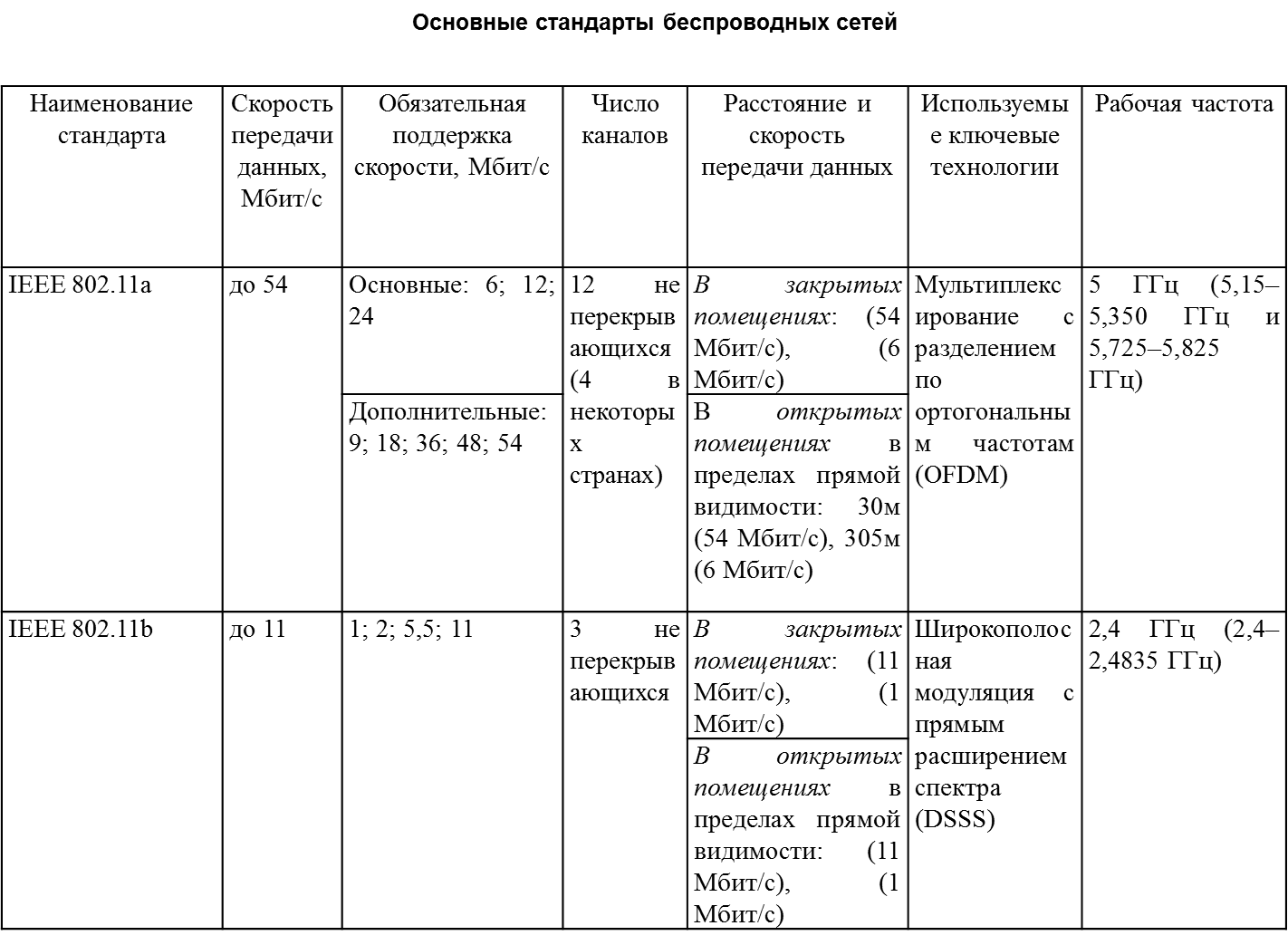
a) Низкая скорость передачи данных по сравнению с кабельными сетями аналогичного поколения.

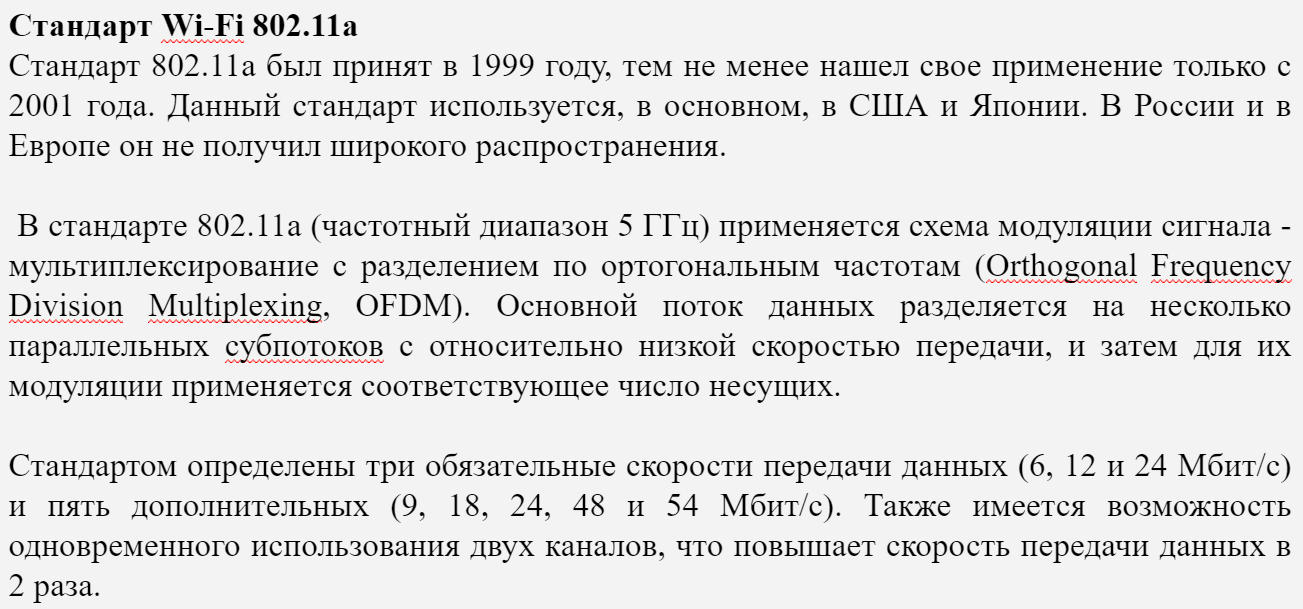
б) высокая уязвимость сети в плане обеспечения безопасности.

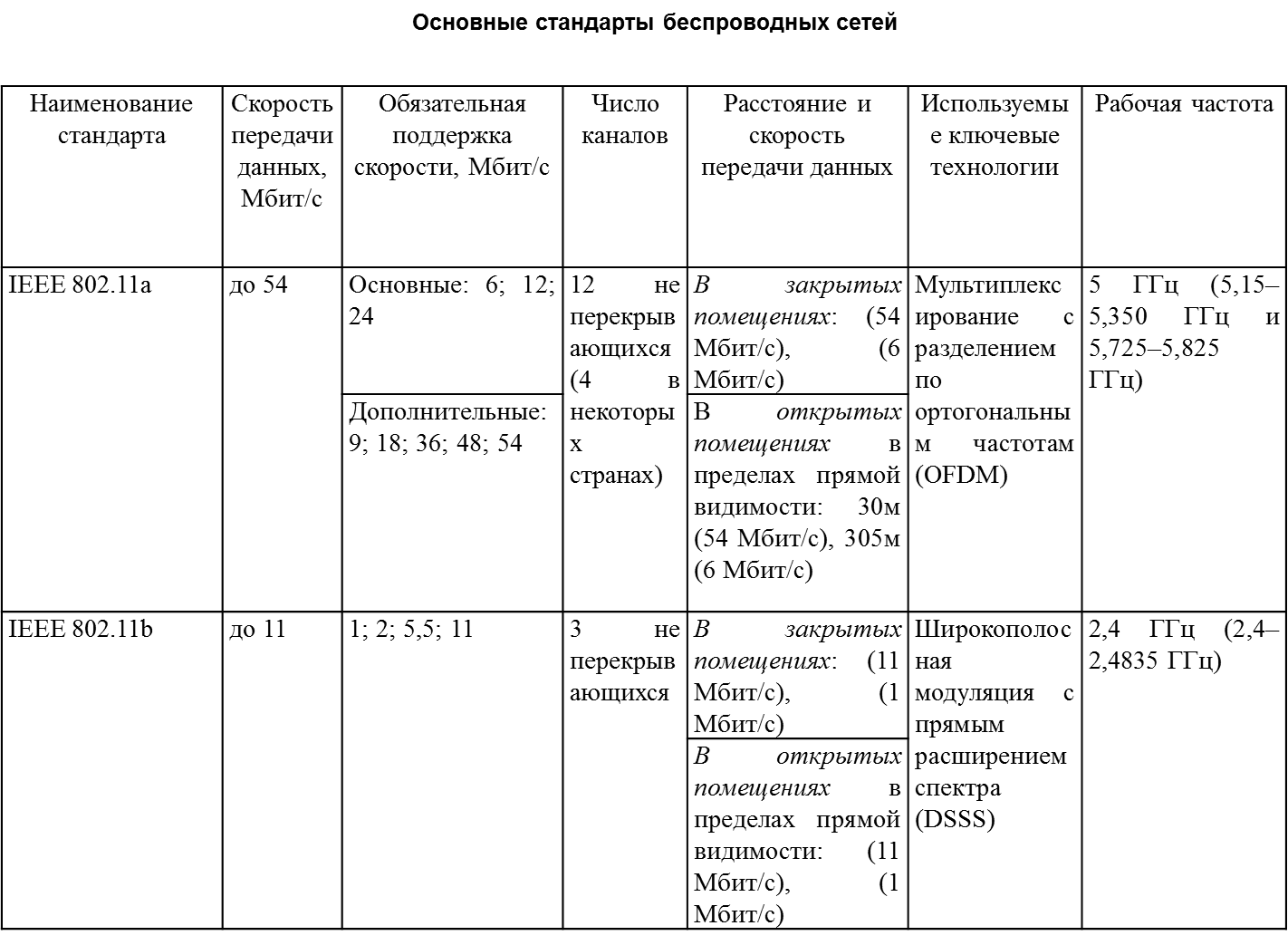
в) низкая предсказуемость зоны покрытия сети.

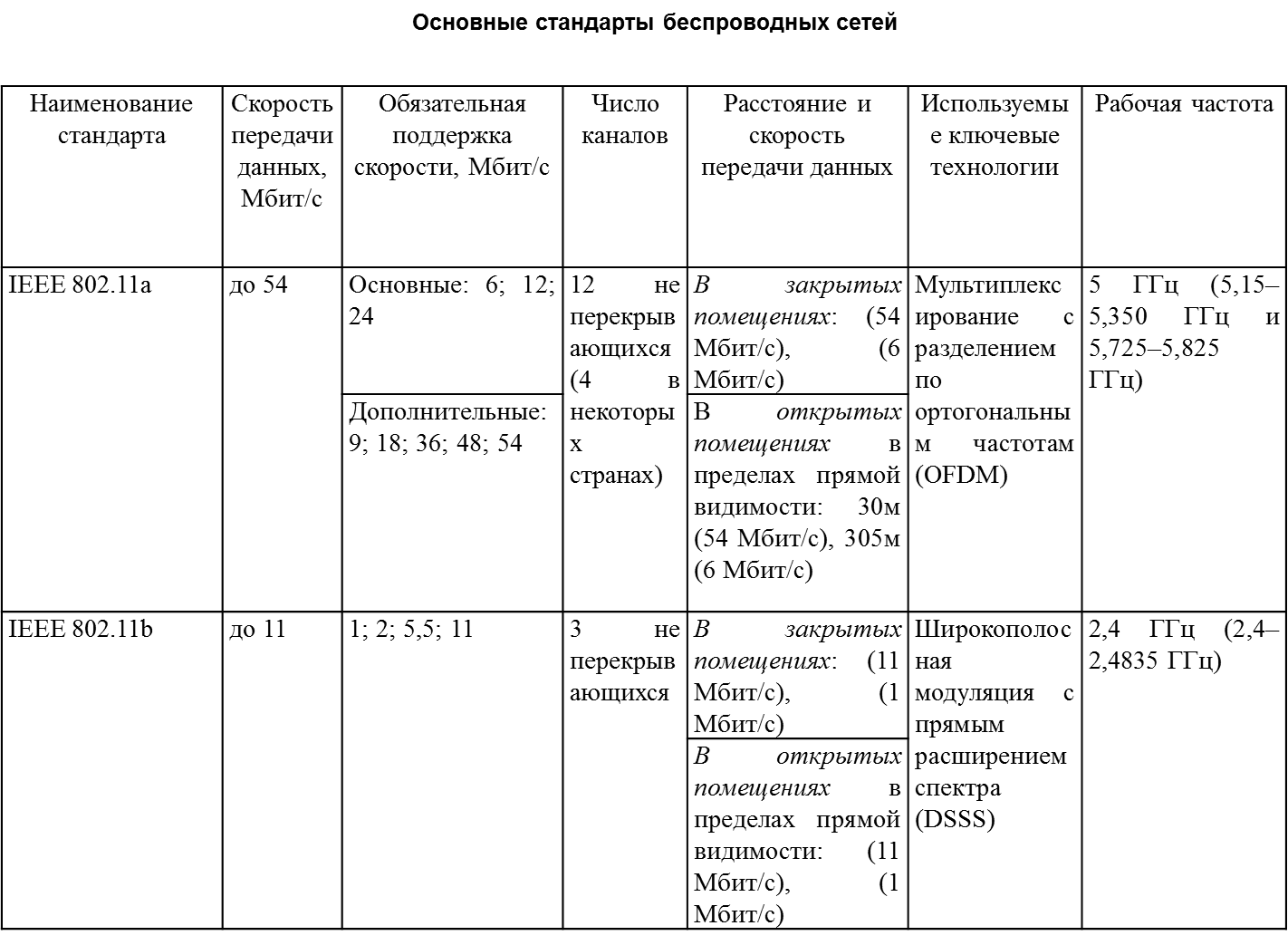
г) создание помех другим устройствам и сетям передачи данных.

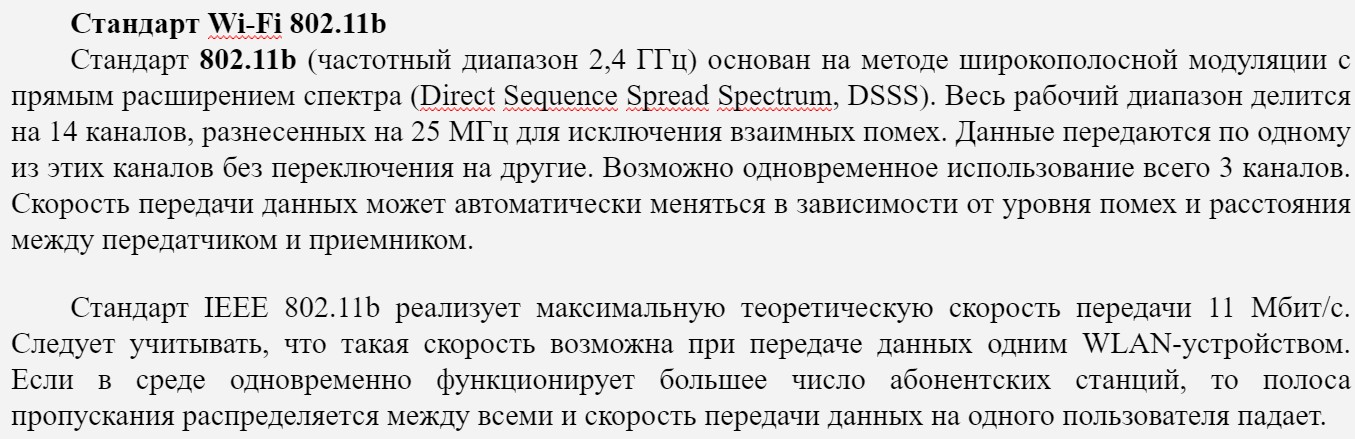
1. **Сети Wi-Fi. Стандарт IEEE802.11a. Стандарт IEEE802.11b.**

******



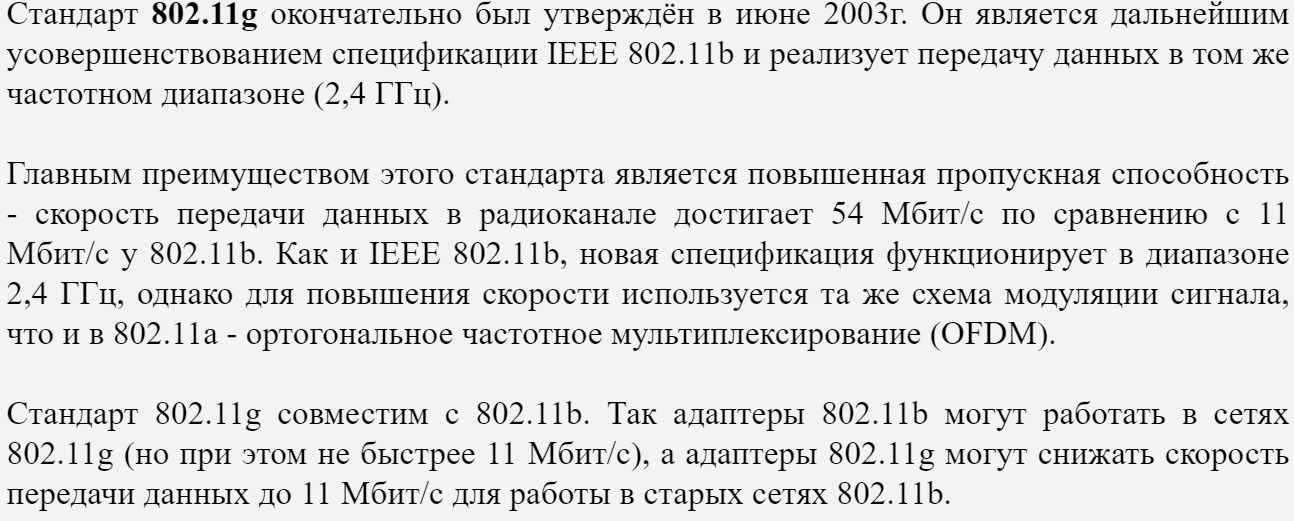
******

******



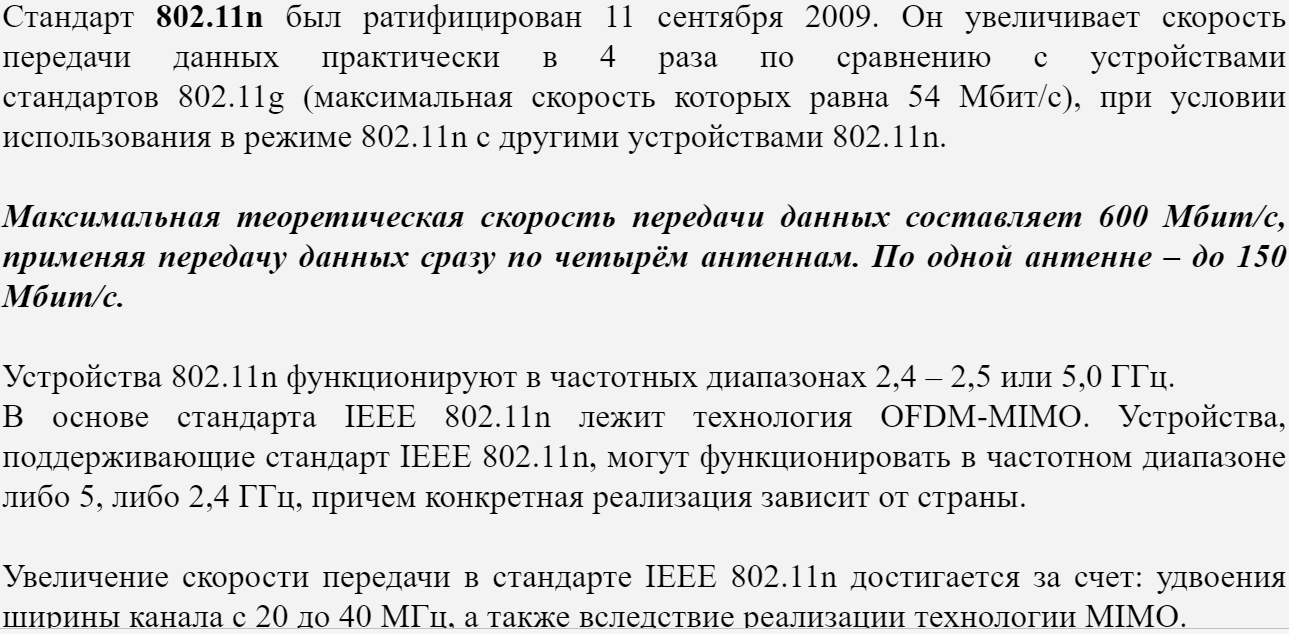
1. **Сети Wi-Fi. Стандарт IEEE802.11g. Стандарт IEEE802.11n.**

******

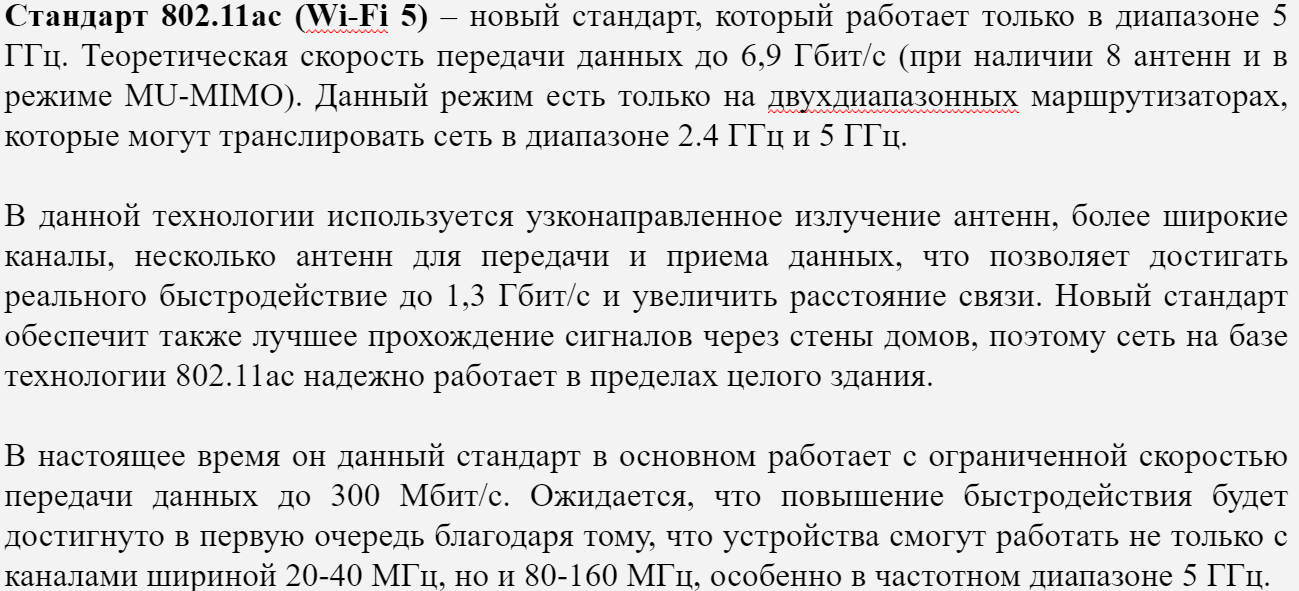


******

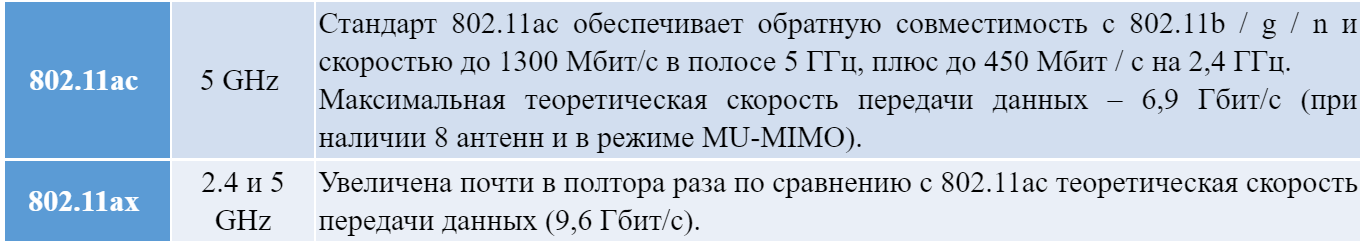
******



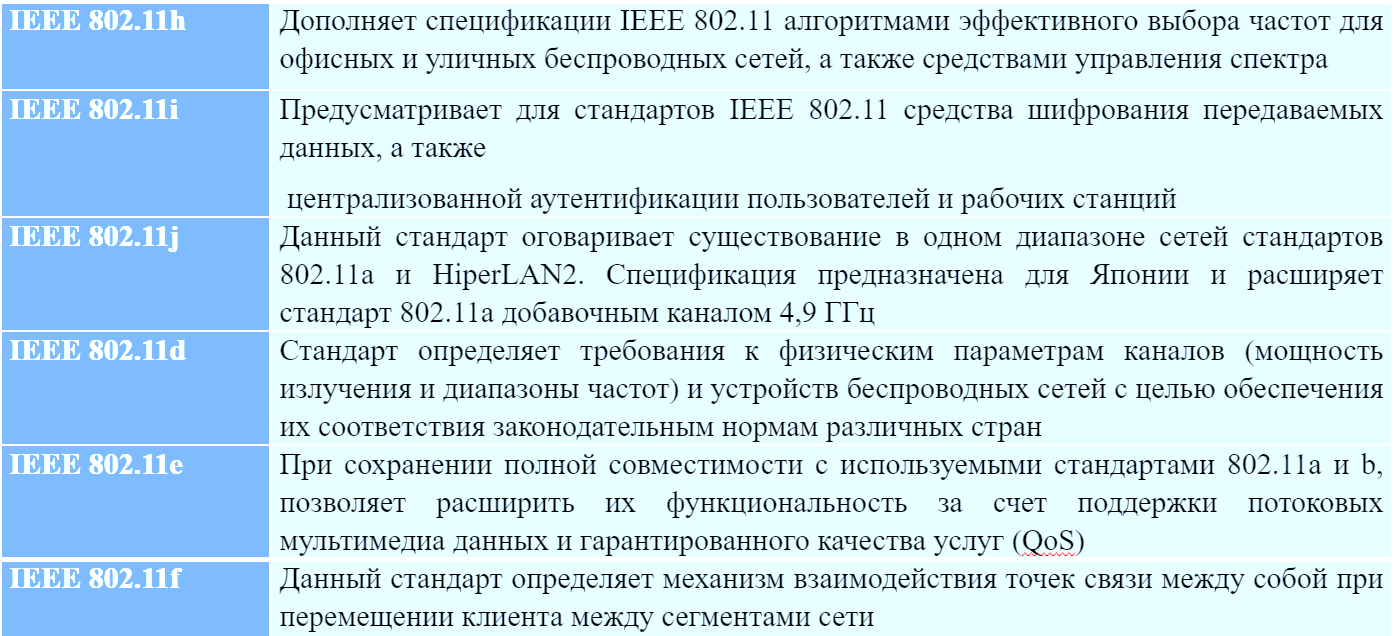
1. **Сети Wi-Fi. Стандарт IEEE802.11ac. Стандарт IEEE802.11ax.**







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



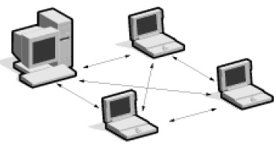
1. **Оборудование для сетей Wi-Fi. Формы организации Wi-Fi сетей.**

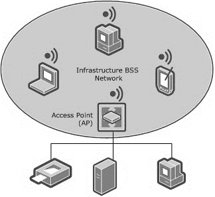
Сети Wi-Fi отождествляются с аббревиатурой *WLAN* (Wireless Local Area Network). Для организации *сетей Wi-Fi* (Wireless Fidelity, беспроводное соответствие) **необходимы Wi-Fi сетевые карты, точки доступа и антенны.** Необходимость в использовании точек доступа отпадает, когда мы говорим об очень малых сетях, размещенных в одном помещении. Использование точек доступа позволяет более гибко настроить сеть, объединить клиентов проводных и беспроводных сетей, а также установить связь с удаленными объектами (внешнее исполнение).

*Wi-Fi сетевые карты* по сути мало чем отличаются от обычных сетевых карт, за исключением некоторых особенностей настройки.  Wi-Fi сетевые карты представлены в трех основных вариантах исполнения – внутренние PCI карты, CARDBUS и USB адаптеры. Также существуют адаптеры в COMPACT FLASH форм-факторе.

Адаптеры различаются по платформе, в которой они используются: PCI – настольный компьютер, CARDBUS – ноутбук, Compact Flash – карманный компьютер, USB – универсален. Принцип построения и настройки сетей – един и не зависит от форм-фактора Wi-Fi адаптера. Необходимо отметить, что тип адаптера влияет лишь на излучаемую мощность передатчика и чувствительность приемника, а также возможность использования внешней антенны.

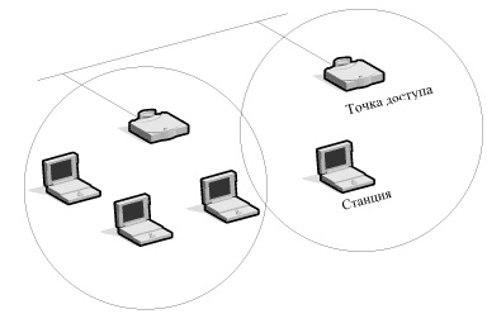
Выделяют три режима организации беспроводных сетей WiFi:​

* Эпизодическая сеть (Ad-Hoc или IBSS – Independent Basic Service Set).​
* Основная зона обслуживания Basic Service Set (BSS) или Infrastructure Mode.​
* ​Расширенная зона обслуживания ESS – Extended Service Set.​

Режим **Ad-Hoc** представляет собой простейшую структуру локальной сети, когда абонентские станции (ноутбуки или компьютеры) взаимодействуют непосредственно друг с другом. Такая структура удобна для срочного развертывания сетей.

 В режиме **BSS** узлы сети взаимодействуют друг с другом не напрямую, а через точку доступа (Access Point, AP).​

В режиме BSS все узлы взаимодействуют между собой через одну AP, которая может играть роль моста для подключения к внешней кабельной сети.​

 Режим **ESS** позволяет объединить несколько точек доступа, т.е. объединяет несколько сетей BSS. В данном случае точки доступа могут взаимодействовать и друг с другом. Расширенный режим удобно применять тогда, когда необходимо объединить в одну сеть несколько пользователей или подключить несколько проводных или беспроводных сетей.​

**Wi-Fi точки доступа** – устройства, позволяющие объединять клиентов сети (как проводной, так и беспроводной) в единую сеть. Другими словами – для Wi-Fi клиентов, точка доступа – это своеобразный хаб (концентратор). ​

Wi-Fi точки доступа представлены в двух основных вариантах исполнения – для использования внутри помещений и для внешнего использования. ​

Внутриофисные точки доступа служат для объединения Wi-Fi клиентов внутри помещений. Они оснащены функциями фильтров, создания виртуальных сетей и т. д. Но зачастую используются точки доступа с более широкими возможностями – WAN-порт, firewall, Ftp-сервер и т.д. ​

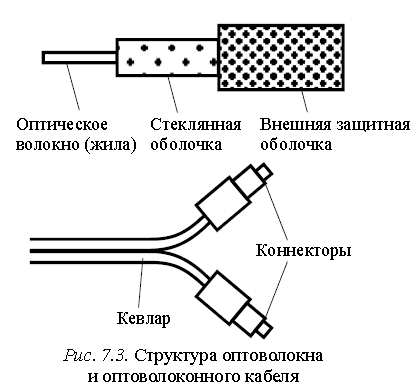
Внешние Wi-Fi точки доступа служат для объединения Wi-Fi клиентов вне помещений, имеют защищенное исполнение, более жесткие эксплуатационные характеристики и т.д. При применении нескольких внешних точек доступа можно соединить достаточно удаленные объекты. Внешние Wi-Fi точки доступа отличаются и большей излучаемой мощностью. Ко всем внешним точкам доступа можно подключить дополнительные антенны, что позволяет расширить зону покрытия Wi-Fi сети. ​

**Внешние Wi-Fi антенны** служат для передачи и приема сигнала, усиление которого в режиме передачи позволяет увеличить зону покрытия Wi-Fi сетей. ​

В основном распространены пассивные антенны – круговые, или всенаправленные и направленные. ​

Основное различие – характер распространения волн антенной. Круговая антенна излучает сигнал по кругу 360º (горизонталь), а направленная лишь на определенный сектор.​

1. **Особенности оптических систем связи (физ., техн.). Их достоинства и недостатки.**

 Волоконно-оптические линии связи – это вид связи, при котором информация передается по оптическим диэлектрическим волноводам, известным под названием «оптическое волокно».​

Оптическое волокно в настоящее время считается самой совершенной физической средой для передачи информации, а также самой перспективной средой для передачи больших потоков информации на значительные расстояния. Основания так считать вытекают из ряда особенностей, присущих оптическим волноводам. ​

***Физические особенности.***

по оптической линии связи можно передавать информацию со скоростью порядка 1000 Мбит/с.

На сегодняшний день предел по плотности передаваемой информации по оптическому волокну не достигнут. Очень малое (по сравнению с другими средами) затухание светового сигнала в волокне.

Высокую пропускную способность за счёт высокой несущей частоты. Потенциальная возможность одного оптического волокна – несколько терабит информации за 1 секунду. Говоря другими словами, по одному волокну можно передать одновременно десятки миллионов телефонных разговоров и миллион видеосигналов.​

Волоконно-оптический кабель отличается низким уровнем шума, что положительно сказывается на его пропускной способности и возможности передавать сигналы различной модуляции.​

Скорость передачи данных может быть увеличена за счет передачи информации сразу в двух направлениях, так как световые волны могут распространяться в одном волокне независимо друг от друга. На сегодняшний день предел по плотности передаваемой информации по оптическому волокну не достигнут.​

Очень малое (по сравнению с другими средами) затухание светового сигнала в волокне. Лучшие образцы российского волокна имеют затухание 0.22 дБ/км на длине волны 1.55 мкм, что позволяет строить линии связи на сотни километров без регенерации сигналов (промежуточного усиления). Для сравнения, лучшее волокно Sumitomo на длине волны 1.55 мкм имеет затухание 0.154 дБ/км. В лабораториях разрабатываются еще более «прозрачные», так называемые фторцирконатные волокна с теоретическим пределом порядка 0,02 дБ/км на длине волны 2.5 мкм. Лабораторные исследования показали, что на основе таких волокон могут быть созданы линии связи с регенерационными участками через 4600 км при скорости передачи порядка 1 Гбит/с.​

***Технические особенности и преимущества оптических волокон.***

Волокно изготовлено из кварца, основу которого составляет двуокись кремния, широко распространенного, а потому недорогого материала, в отличие от меди. Оптические волокна имеют **диаметр около 100 мкм**, то есть очень компактны и легки, что делает их перспективными для использования в авиации, приборостроении, в кабельной технике.

Системы связи на основе оптических волокон **устойчивы к электромагнитным помехам**, а передаваемая по световодам информация защищена от несанкционированного доступа. Волоконно-оптические **линии связи нельзя прослушать, не разрушив поверхность канала**. Всякие воздействия на волокно могут быть зарегистрированы методом мониторинга (непрерывного контроля) целостности линии. Важное **свойство оптического волокна – долговечность. Время жизни волокна, то есть сохранение им своих свойств в определенных пределах, превышает 25 лет**, что позволяет проложить оптико-волоконный кабель один раз и по мере необходимости наращивать пропускную способность канала путем замены приемников и передатчиков на более быстродействующие.

Недостатки: при создании линии связи требуются высоконадежные активные элементы, преобразующие электрические сигналы в свет и свет в электрические сигналы. Необходимы также оптические коннекторы (соединители) с малыми оптическими потерями и большим ресурсом на подключение-отключение. ​

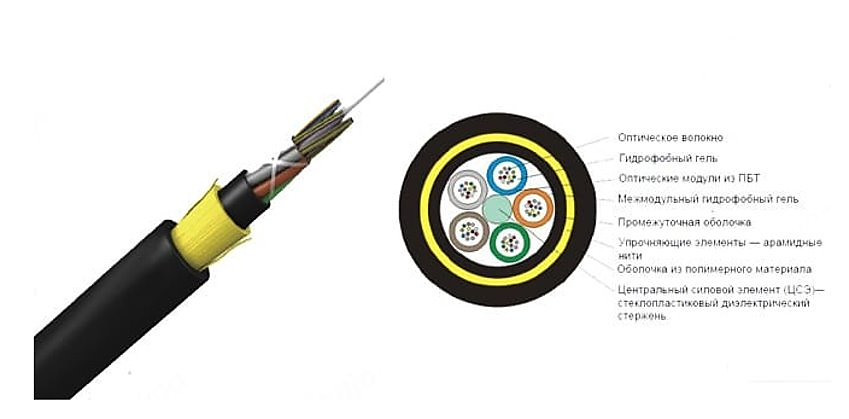
Точность изготовления таких элементов линии связи должна соответствовать длине волны излучения, то есть погрешности должны быть порядка доли микрона. Поэтому производство таких компонентов оптических линий связи очень дорогостоящее. ​

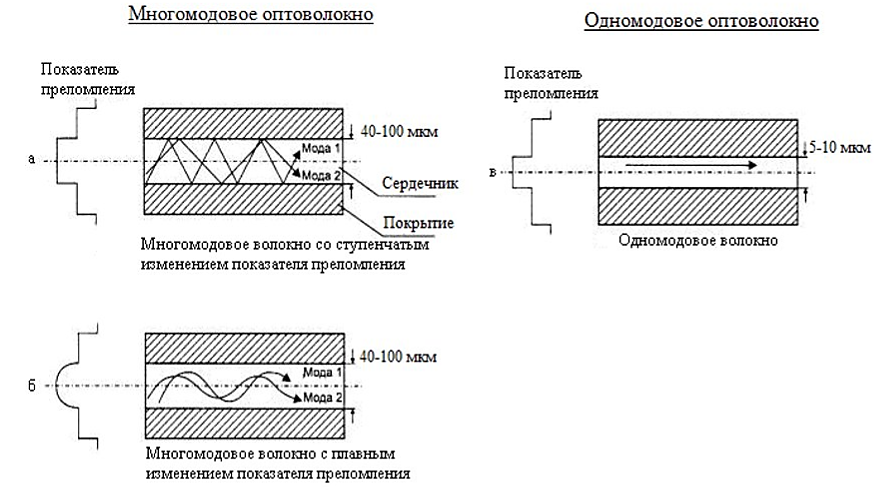
Для монтажа оптических волокон требуется прецизионное (высокоточное), а потому дорогое, технологическое оборудование. Как следствие, при аварии (обрыве) оптического кабеля затраты на восстановление выше, чем при работе с медными кабелями.​

*Преимущества от применения волоконно-оптических линий связи настолько значительны, что, несмотря на перечисленные недостатки оптического волокна, эти линии связи все шире используются для передачи информации.*

1. **Оптический кабель: его разновидности и характеристики.**

Волоконно-оптические линии связи – это вид связи, при котором информация передается по оптическим диэлектрическим волноводам, известным под названием «оптическое волокно».​



 В зависимости от распределения показателя преломления и от величины диаметра сердечника различают:

− многомодовое волокно со ступенчатым изменением показателя преломления;

− многомодовое волокно с плавным изменением показателя

преломления;

− одномодовое волокно.

Понятие «мода» описывает режим распространения световыхлучей во внутреннем сердечнике кабеля.

В **одномодовом** кабеле (SingleModeFiber, SMF) используетсяцентральный проводник очень малого диаметра, соизмеримого сдлиной волны света – от 5 до 10 мкм. При этом практически вселучи света распространяются вдоль оптической оси световода, неотражаясь от внешнего проводника.

В **многомодовых** кабелях (MultiModeFiber, MMF) используются более широкие внутренние сердечники, которые легче изготовить технологически. В стандартах определены два наиболее употребительных многомодовых кабеля: 62,5/125 мкм и 50/125 мкм, где62,5 мкм или 50 мкм – это диаметр центрального проводника, а125 мкм – диаметр внешнего проводника.В многомодовых кабеляхво внутреннем проводнике одновременно существует несколькосветовых лучей, отражающихся от внешнего проводника под разными углами. Угол отражения луча называется модой луча.

Можно выделить следующие основные виды оптоволоконных кабелей для передачи данных исходя из области применения: ​

* для прокладки внутри зданий;​
* для кабельной канализации небронированный;​
* для кабельной канализации бронированный;​
* для укладки в грунт;​
* подвесной самонесущий;​
* с тросом;​
* подводный.​

**Для прокладки внутри зданий.** Конструкция оптоволоконных кабелей для прокладки в зданиях включает в себя оптическое волокно, защитное покрытие и центральный силовой элемент, например, пучок арамидных нитей. К оптике, прокладываемой в помещениях, есть особые требования по противопожарной безопасности, такие как нераспространение горения и низкое дымовыделение, поэтому в качестве оболочки для них используется не полиэтилен, а полиуретан. Другие требования — это низкая масса кабеля, гибкость и небольшой размер. ​

**Для кабельной канализации небронированный.** Небронированная оптика используется для укладки в канализации, при условии, что на нее не будет внешних механических воздействий. Также подобный кабель прокладывается в тоннелях, коллекторах и зданиях. ​

Характерной особенностью данного типа оптоволоконного кабеля можно назвать наличие гидрофобного наполнителя (компаунда), который гарантирует возможность эксплуатации в условиях канализации и дает некоторую защиту от влаги. ​

**Для кабельной канализации бронированный.** Бронированные оптоволоконные кабели используются при наличии больших внешних нагрузок, в особенности, на растяжение. Бронирование может быть различным, ленточным или проволочным. ​

Кабели с ленточным бронированием используются в менее агрессивных условиях, например, при прокладке в кабельной канализации, трубах, тоннелях, на мостах. Ленточное бронирование представляет собой стальную гладкую или гофрированную трубку толщиной в 0,15-0,25 мм. При более суровых условиях эксплуатации, например, при закладке в грунт или на дно рек используются кабели с проволочной броней. ​

**Для прокладки в грунт** используют оптические кабели с проволочной одноповивной или двухповивиной броней. Также применяются и усиленные кабели с ленточным бронированием, но значительно реже. ​

В условиях влажного грунта используется модель кабеля, оптоволоконная часть которого заключена в герметичную металлическую трубку, а бронеповивы проволоки пропитаны специальным водоотталкивающим компаундом.​

**Подвесные самонесущие кабели** монтируются на уже существующих опорах воздушных линий связи и высоковольтных ЛЭП. В конструкции самонесущих подвесных оптических кабелей обязательно присутствует ЦСЭ — центральный силовой элемент, изготовленный из стеклопластика или арамидных нитей.​

В зависимости от строения сердечника различают несколько типов подвесного кабеля: ​

* Кабель с профилированным сердечником — содержит оптические волокна или модули с этими волокнами – кабель устойчив к растяжению и сдавливанию;​
* Кабель со скрученными модулями — содержит оптические волокна, свободно уложенные, кабель устойчив к растяжениям;​
* Кабель с одним оптическим модулем – сердечник данного типа кабеля не имеет силовых элементов, поскольку они находятся в оболочке. Такие кабели обладают недостатком, связанным с неудобством идентификации волокон. Тем не менее, они обладают меньшим диаметром и более доступной ценой.​

**Оптические кабеля с тросом** — это разновидность самонесущих кабелей, которые также используются для воздушной прокладки. В таком изделии трос может быть несущим и навивным. Еще существуют модели, в которых оптика встроена в грозозащитный трос. ​

**Подводный оптический кабель.** Данный тип оптических кабелей стоит в сторонке от всех остальных, так как прокладывается в принципиально иных условиях. Почти все типы подводных кабелей, так или иначе, бронированы, а степень бронирования уже зависит от рельефа дна и глубины залегания. ​

Различают следующие основные типы подводных кабелей (по типу бронирования): ​

* Не бронирован;​
* Одинарное (одноповивное) бронирование;​
* Усиленное (одноповивное) бронирование;​
* Усиленное скальное (двухповивное) бронирование;​

1. **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.

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.​

Переход от работы на персональных компьютерах к работе в сети усложняет защиту информации по следующим причинам:​

1. Большое число пользователей в сети и их переменный состав. Защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц; ​
2. Значительная протяженность сети и наличие многих потенциальных каналов проникновения в сеть; ​
3. Недостатки в аппаратном и программном обеспечении, которые зачастую обнаруживаются не на предпродажном этапе, называемом бета- тестированием, а в процессе эксплуатации. В том числе неидеальны встроенные средства защиты информации.​

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

**Авторизация** – предоставление субъектам доступ к объектам системы. Доступ к объекту означает доступ к содержащейся в нем информации.

**Аутентификация** – проверка идентификации пользователя, устройства или другого компонента в системе (обычно для принятия решения о разрешении доступа к ресурсам системы). Частным вариантом аутентификации является установление принадлежности сообщения конкретному автору.

**Удаленная атака** – информационное разрушающее воздействие на распределенную компьютерную сеть, программно-осуществленное по каналам связи.

**Отказоустойчивость** – это такое свойство вычислительной системы, которое обеспечивает ей как логической машине возможность продолжения действий, заданных программой, после возникновения неисправностей. Введение отказоустойчивости требует избыточного аппаратного и программного обеспечения.

**Виды атак:**

**Сниффер пакетов** (sniffer – в данном случае фильтрация) –прикладная программа, которая использует сетевую карту, работающую в режиме (promiscuous(«не делающий различия») mode),в котором все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки.Сниффер перехватывает все сетевые пакеты, которые передаются через атакуемый домен.

**Социальная инженерия** – это использование хакером психологических приемов «работы» с пользователем. В самом худшемслучае хакер, перехватив пароль, получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает нового пользователя, которого можно в любой момент использовать для доступа в сеть и к ее ресурсам.

**IP-спуфинг** – это вид атаки, при которой хакер, находящийсявнутри организации или за ее пределами, выдает себя за санкционированного пользователя.Это можно сделать двумя способами. Во-первых, хакер можетвоспользоваться IP-адресом, находящимся в пределах диапазонасанкционированных IP-адресов, или авторизованным внешнимадресом, которому разрешается доступ к определенным сетевымресурсам. Атаки IP-спуфинга часто являются отправной точкойдля прочих атак. Классический пример – атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера.

**Отказ в обслуживании (Denial of Service, DoS). Атака DoS**делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.

Атаки DoS, без всякого сомнения, являются наиболее известной формой хакерских атак и одной из самых молодых технологий. Против атак такого типа труднее всего создать стопроцентную защиту. Атаки DoS считаются тривиальными, а от хакера длясвоей организации они требуют минимум знаний и умений: всенеобходимое программное обеспечение вместе с описаниями самой технологии совершенно свободно доступно в Интернете.Именно простота реализации и огромный причиняемый вред привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность.

**Атаки типа Man-in-the-Middle** – непосредственный доступ кпакетам, передаваемым по сети.Такой доступ ко всем пакетам, передаваемым от провайдера влюбую другую сеть, может, к примеру, получить сотрудник этогопровайдера. Для атак этого типа часто используются снифферыпакетов, транспортные протоколы и протоколы маршрутизации.Атаки проводятся с целью кражи информации, перехвата текущейсессии и получения доступа к частным сетевым ресурсам, дляанализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

**DDoS** означает **Distributed Denial of Service**: распределённая атака типа «отказ в обслуживании». В этом случае речь идёт об огромной массе злонамеренных запросов, поступающих на атакуемый сервер из множества разных мест. Обычно такие атаки организуются посредством бот-сетей.​

**Парольные атаки** – их целью является завладение паролем и логином законного пользователя. Злоумышленники могут проводить парольные атаки, используя следующие методы: подмена IP-адреса (IР-спуфинг); прослушивание (сниффинг); простой перебор; использование метода «троянского коня».​

Парольные атаки часто проводятся с помощью методов социальной инженерии. Данная тактика основана на анализе общедоступной информации о пользователе (место проживания, учёбы, дата рождения, кличка любимого питомца и многое другое) и может нанести большой урон, т.к. обычно используются одни и те же учётные данные в разных сервисах. Получение общедоступной информации уменьшает трудозатраты злоумышленника.

**Сетевая разведка** – получение и обработка данных об информационной системе клиента, ресурсов информационной системы, используемых устройств и программного обеспечения и их уязвимостях, средств защиты, а также о границе проникновения в информационную систему.​

Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (ping sweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. И, наконец, хакер анализирует характеристики приложений, работающих на хостах. В результате добывается информация, которую можно использовать для взлома.​

**Атаки на уровне приложений**. В данном случае злоумышленники получают прямой доступ к приложениям корпоративной сети. Отдельный интерес для них представляют сервисы HTTP (TCP порт 80) и HTTPS (TCP порт 443), которые во многих сетях открыты именно на уровне приложений модели OSI (Open Systems Interconnection). В то же время устройства контроля доступа не могут эффективно идентифицировать злонамеренные действия, направленные на эти сервисы. К данной категории атак относят, например, запуск сценария на стороне клиента, инжекции кода SQL и т.д.​

**Вредоносное ПО типа «вирусы» или «черви».** Компьютерный вирус и компьютерный червь — это вредоносные программы, которые способны воспроизводить себя на компьютерах или через компьютерные сети. При этом пользователь не подозревает о заражении своего компьютера. Так как каждая последующая копия вируса или компьютерного червя также способна к самовоспроизведению, заражение распространяется очень быстро. Существует очень много различных типов компьютерных вирусов и компьютерных червей, большинство которых обладают высокой способностью к разрушению.​

1. **Классификация средств защиты информации.**

Защита информации в сети может быть улучшена за счет использования специальных генераторов шума, маскирующих побочные электромагнитные излучения и наводки, помехоподавляющих сетевых фильтров, устройств зашумления сети питания, скремблеров (шифраторов телефонных переговоров), подавителей работы сотовых телефонов и т.д. ​

Кардинальным решением является переход к соединениям на основе оптоволокна, свободным от влияния электромагнитных полей и позволяющим обнаружить факт несанкционированного подключения.​

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

* Технические

Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. (Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др. Вторую – упоминавшиеся выше генераторы шума, сетевые фильтры). Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны – недостаточная гибкость, относительно большие объем и масса, высокая стоимость. ​

* Программные

(включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов). 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). ​

* Смешанные аппаратно-программные средства

(реализуют те же функции, что аппаратные и программные средства в отдельности) и имеют промежуточные свойства.

* Организационные средства

(подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней). 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.​

1) Различаются по типу устройства, по требованиям. Аппаратные средства рассматривают вопрос защиты информации, они либо препятствуют проникновению, либо если проникновение состоялось, то выполняют маскировку передаваемых данных, например, через искажение.

+ надёжность, независимость от субъективных факторов. Высокая устойчивость к модификации.

2) Различный софт по аунтефикации, индификации, контроль доступа на разных языках программирования.

3) Разрабатываются определённые требования, по которым должны проводится работы в сети, политика правил поведения пользователя.

1. **Понятие шифрования. Стандартные методы шифрования (подстановка, перестановка, гаммирование) и криптографические системы.**

**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.​

Понятие «шифрование» часто употребляется в связи с понятием «криптография».

**Криптография** изучает методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность.

**Аутентичность** информации состоит в подлинности авторства и целостности.

**Конфиденциальность** информации – свойство информации быть известной только допущенным и прошедшим авторизацию субъектам системы (пользователям, программам, процессам и др.); статус, предоставленный информации и определяющий требуемую степень ее защиты.

Все современные алгоритмы шифрования представлю собой комбинацию 3 основных классов алгоритмов:

* Подстановка (простая – одноалфавитная, многоалфавитная однопетлевая, многоалфавитная многопетлевая); ​
* Перестановка (простая, усложненная)
* Гаммирование (смешивание с маской, основано на сложении по модулю 2, побитовое «или»)

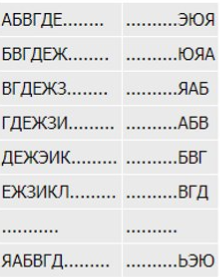
**Подстановка**. Подстановка предполагает использование альтернативного алфавита (или нескольких) вместо исходного. В случае простой подстановки для символов английского алфавита можно предложить, например, следующую замену. ​



Тогда слово "cache" в зашифрованном виде представляется как "usuxk". ​

Однако, существует, возможность дешифрования сообщения с помощью известной статистической частоты повторяемости символов в произвольном, достаточно длинном тексте. Символ E встречается чаще всего – в среднем 123 раза на каждые 1000 символов или в 12,3% случаев, далее следуют символы T – 9,6%, A – 8,1%, O – 7,9%, N – 7,2%, I – 7,2%, S – 6,6%, R – 6,0%, H – 5,1%, L – 4,0% и т.д. ​

Использование многоалфавитной подстановки, при которой можно добиться того, что в зашифрованном тексте все символы будут встречаться примерно с одинаковой частотой, что существенно затруднит дешифрование.

**Многоалфавитная подстановка.** В многоалфавитных подстановках для замены символов исходного текста используется не один, а несколько алфавитов. Обычно алфавиты для замены образованы из символов исходного алфавита, записанных в другом порядке. Примером многоалфавитной подстановки может служить схема, основанная на использовании таблицы Вижинера.​

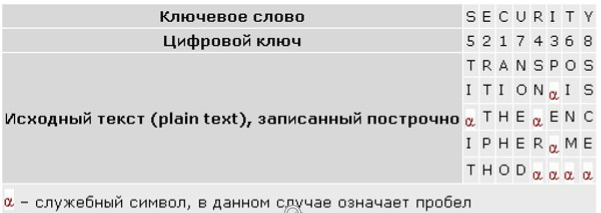
В этом методе для шифрования используется таблица, представляющая собой квадратную матрицу с числом элементов NxN, где N — количество символов в алфавите. ​

В первой строке матрицы записывают буквы в порядке очередности их в исходном алфавите, во второй — ту же последовательность букв, но с циклическим сдвигом влево на одну позицию, в третьей — со сдвигом на две позиции и т. д.​

Для шифрования текста выбирают ключ, представляющий собой некоторое слово или набор символов исходного алфавита. Далее из полной матрицы выписывают подматрицу шифрования, включающую первую строку и строки матрицы, начальными буквами которых являются последовательно буквы ключа (например, если выбрать ключ "весна", то таблица шифрования будет следующей).

В процессе шифрования под каждой буквой шифруемого текста записывают буквы ключа, повторяющие ключ требуемое число раз, затем шифруемый текст по таблице шифрования заменяют буквами, расположенными на пересечениях линий, соединяющих буквы текста первой строки таблицы и буквы ключа, находящейся под ней .

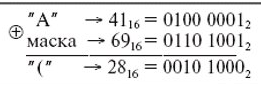
**Перестановка**. Потенциально обеспечивает большую по сравнению с подстановкой устойчивость к дешифрованию и выполняется с использованием цифрового ключа или эквивалентного ключевого слова​



Для рассматриваемого примера зашифрованное сообщение будет выглядеть следующим образом:​

AIHHORTTPHPαEααα…SSCEα. ​

**Гаммирование** (смешивание с маской) основано на побитном сложении по модулю 2 (в соответствии с логикой ИСКЛЮЧАЮЩЕЕ ИЛИ) исходного сообщения с заранее выбранной двоичной последовательностью (маской). Компактным представлением маски могут служить числа в десятичной (шестнациричной) системе счисления или некоторый текст (в данном случае рассматривается внутренние коды символов – для английского текста таблица ASCII). ​



Операция суммирования по модулю 2 (ИСКЛЮЧАЮЩЕЕ ИЛИ) является обратимой, так что при сложении с той же маской (ключом) зашифрованного сообщения получается исходный текст (происходит дешифрование). ​

Наибольшую устойчивость к дешифрованию может обеспечить применение маски с бесконечной длиной, которая образована генератором случайных (точнее, псевдослучайных) последовательностей. ​

Такой генератор легко реализуется аппаратными или программными средствами, например, с помощью сдвигового регистра с обратными связями, который используется при вычислении помехоустойчивого циклического кода. Точное воспроизведение псевдослучайной последовательности в генераторе на приемном конце линии обеспечивается при установке такого же исходного состояния (содержимого сдвигового регистра) и той же структуры обратных связей, что и в генераторе на передающем конце.​

Перечисленные "классические" методы шифрования (подстановка, перестановка и гаммирование) являются линейными в том смысле, что длина зашифрованного сообщения равна длине исходного текста. ​

Возможно нелинейное преобразование типа подстановки вместо исходных символов (или целых слов, фраз, предложений) заранее выбранных комбинаций символов другой длины, что позволит повысить защищенность. ​

Эффективна также защита информации методом рассечения-разнесения, когда исходные данные разбиваются на блоки, каждый из которых не несет полезной информации, и эти блоки хранятся и передаются независимо друг от друга. ​

**Криптографическая система** - набор криптографических преобразований или алгоритмов, предназначенных для работы в единой технологической цепочке с целью решения определенной задачи защиты информационного процесса.

В настоящие время выделяют 2 вида шифрования:

* Асинхронное
* Синхронное

В симметричных криптосистемах для зашифрования и для расшифрования используется один и тот же ключ. В ассиметричных криптосистемах используются два ключа –открытый (публичный) и закрытый (секретный, тайный), которые математически связаны друг с другом.

1. **Классические алгоритмы шифрования данных (симметричные и ассиметричные системы).**

Существуют две принципиально различные группы стандартных методов шифрования:​

шифрование с применением одних и тех же ключей (шифров) при шифровании и дешифровании (**симметричное** шифрование или системы с закрытыми ключами – private-key systems); ​

шифрование с использованием открытых ключей для шифрования и закрытых – для дешифрования (**несимметричное** шифрование или системы с открытыми ключами – public-key systems).

Стандарт шифрования США DES (Data Encryption Standard – стандарт шифрования данных) относится к группе методов симметричного шифрования и действует с 1976 г. Число шагов – 16. Длина ключа – 56 бит, из которых 8 бит – проверочные разряды четности/нечетности. ​

Долгое время степень устойчивости к дешифрованию этого метода считалась достаточной, однако в настоящее время он устарел. Вместо DES предлагается "тройной DES" – 3DES, в котором алгоритм DES используется 3 раза, обычно в последовательности "шифрование – дешифрование – шифрование" с тремя разными ключами на каждом этапе.​

Надежным считается алгоритм IDEA (International Data Encryption Algorithm), разработанный в Швейцарии и имеющий длину ключа 128 бит.​

Отечественный ГОСТ28147-89 – это аналог DES, но с длиной ключа 256 бит, так что его степень устойчивости к дешифрованию изначально существенно выше. ​

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

Довольно популярны, особенно при использовании электронной почты в Интернет, несимметричные (асимметричные) методы шифрования или системы с открытыми ключами – public-key systems.​

К этой группе методов относится, в частности, PGP (Pretty Good Privacy – достаточно хорошая секретность). Каждый пользователь имеет пару ключей. Открытые ключи предназначены для шифрования и свободно рассылаются по сети, но не позволяют произвести дешифрование. Для этого нужны секретные (закрытые) ключи. ​

Другая известная система с открытыми ключами – RSA.​

Несимметричные методы шифрования имеют преимущества и недостатки, обратные тем, которыми обладают симметричные методы. В частности, в несимметричных методах с помощью посылки и анализа специальных служебных сообщений может быть реализована процедура аутентификации (проверки легальности источника информации) и целостности (отсутствия подмены) данных. ​

В отличие от симметричных методов шифрования, проблема рассылки ключей в несимметричных методах решается проще – пары ключей (открытый и закрытый) генерируются "на месте" с помощью специальных программ. Для рассылки открытых ключей используются такие технологии как LDAP (Lightweight Directory Access Protocol – протокол облегченного доступа к справочнику). Рассылаемые ключи могут быть предварительно зашифрованы с помощью одного из симметричных методов шифрования. ​