1. Назначение сетей. Основные определения и термины. Преимущества использования сетей.
2. Архитектура терминал – главный компьютер.
3. Одноранговая архитектура. Архитектура клиент – сервер.
4. Топология вычислительной сети. Виды топологий. Топология общая шина.
5. Топология кольцо.
6. Топология звезда.
7. Древовидные топологии.
8. Ячеистые топологии.
9. Комбинированные топологии.
10. Метод доступа CSMA/CD.
11. Метод доступа TPMA.
12. Метод доступа TDMA.
13. Метод доступа FDMA.
14. Назначение пакетов и их структура. Адресация пакетов.
15. MAC-адреса и их структура.
16. Семиуровневая модель OSI . Назначение. Взаимодействие уровней модели OSI.
17. Уровни модели OSI: прикладной уровень (Application layer)
18. Уровни модели OSI: уровень представления данных (Presentation layer)
19. Уровни модели OSI: сеансовый уровень (Session layer).
20. Уровни модели OSI: транспортный уровень (Transport Layer)
21. Уровни модели OSI: сетевой уровень (Network Layer).
22. Уровни модели OSI: канальный уровень (Data Link)
23. Уровни модели OSI: физический уровень (Physical Layer).
24. Спецификации стандартов 802.1 – 802.7
25. Спецификации стандартов 802.8 - 802.12.
26. Спецификации стандартов 802.14 - 802.22.
27. Понятия протоколов и стеков протоколов. Сетевые протоколы. Транспортные протоколы. Прикладные протоколы.
28. Архитектура стека протоколов Microsoft TCP/IP.
29. Стек TCP/IP: уровень Приложения, уровень транспорта
30. Стек TCP/IP: межсетевой уровень, уровень сетевого интерфейса.
31. Типы адресаций в сетях. Символьная адресация. Протоколы сопоставления адреса ARP и RARP.
32. Структура IPv4. Классы IP-адресов.
33. Понятие маски. Правила использование масок. Определение NetworkID и HostID с использованием масок.
34. Структурирование сетей с помощью масок.
35. Особые IP-адреса. Понятие частных сетей. Диапазоны частных адресов.
36. Адресация IPv6. Особенности. Текстовое представление адреса. Типы IPv6 адресов
37. Кабель типа «витая пара» (twisted pair). Схемы разводки. Кабельные системы Ethernet.
38. Кабели и структурированные кабельные системы. Коаксиальные кабели.
39. Сетевые адаптеры (Network Interface Card). Назначение. Функции сетевых адаптеров. Типы сетевых адаптеров.
40. Повторители и концентраторы. Назначение. Особенности использования.
41. Мосты. Назначение. Особенности использования.
42. Коммутаторы. Назначение. Особенности использования.
43. Различие между мостом и коммутатором.
44. Маршрутизаторы. Назначение. Особенности использования. Различия между маршрутизаторами и мостами.
45. Шлюзы. Назначение. Особенности использования.
46. Беспроводные технологии: радиосвязь, инфракрасная, связь в микроволновом диапазоне.
47. Сети Wi-Fi. Стандарт IEEE802.11a.
48. Сети Wi-Fi. Стандарт IEEE802.11b.
49. Сети Wi-Fi. Стандарт IEEE802.11g.
50. Сети Wi-Fi. Стандарт IEEE802.11n.
51. Оборудование для сетей Wi-Fi.
52. Особенности оптических систем связи (физические, технические).
53. Оптический кабель: его разновидности и характеристики.
54. Достоинства и недостатки оптических систем связи.
55. Защита информации. Основные понятия. Виды основных сетевых атак.
56. Классификация средств защиты информации.
57. Понятие шифрования. Классические алгоритмы шифрования данных.
58. Стандартные методы шифрования и криптографические системы.
59. **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.*

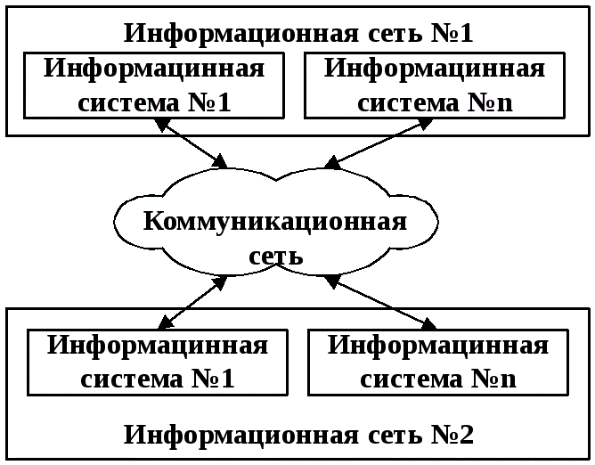
В состав сети в общем случае включается следующие элементы:

* сетевые компьютеры (оснащенные сетевым адаптером);
* каналы связи (кабельные, спутниковые, телефонные, цифровые, волоконно-оптические, радиоканалы и др.);
* различного рода преобразователи сигналов;
* сетевое оборудование.

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.

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 канал можно 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.

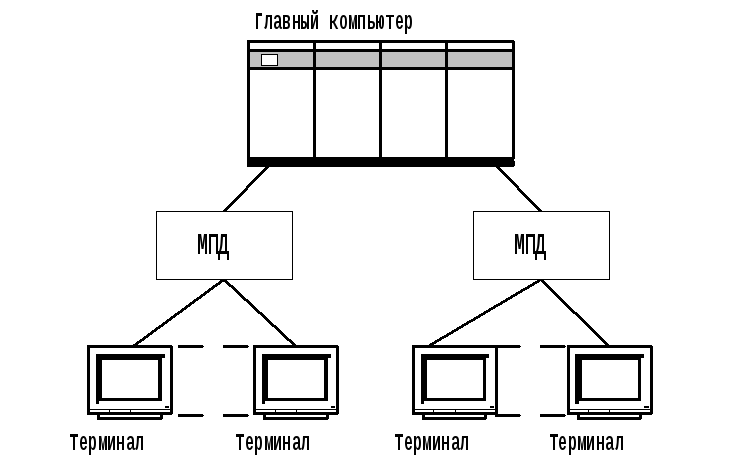
Трафик (traffic) – это поток сообщений в сети передачи данных. Под ним понимают количественное измерение в выбранных точках сети числа проходящих блоков данных и их длины, выраженное в битах в секунду.

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.

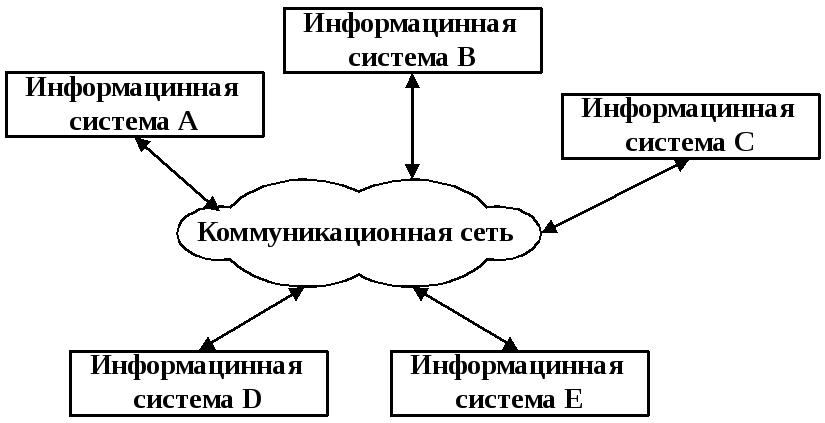
Рассматриваемая архитектура предполагает два типа оборудования:

* Главный компьютер, где осуществляется управление сетью, хранение и обработка данных.
* 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 (System Network Architecture– 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.

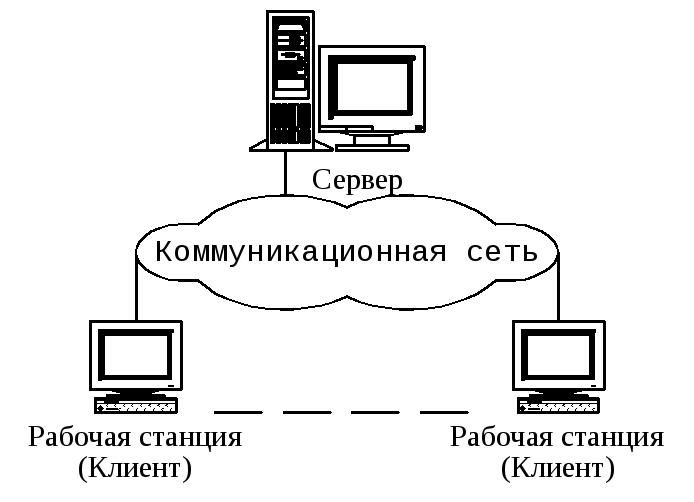
Одноранговые сети имеют следующие преимущества:

* они легки в установке и настройке;
* отдельные ПК не зависят от выделенного сервера;
* пользователи в состоянии контролировать свои ресурсы;
* малая стоимость и легкая эксплуатация;
* минимум оборудования и программного обеспечения;
* нет необходимости в администраторе;
* хорошо подходят для сетей с 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.

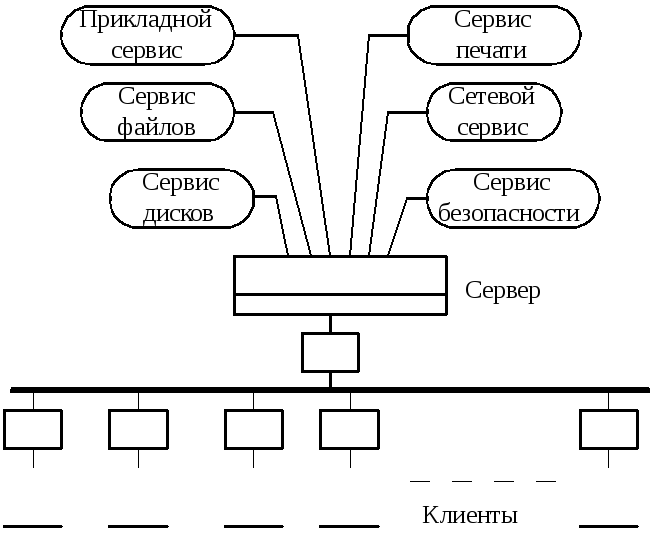
**Архитектура клиент – сервер** – это концепция информационной сети, в которой основная часть ее ресурсов сосредоточена в серверах, обслуживающих своих клиентов. Рассматриваемая архитектура определяет два типа компонентов: серверы и клиенты.

***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.

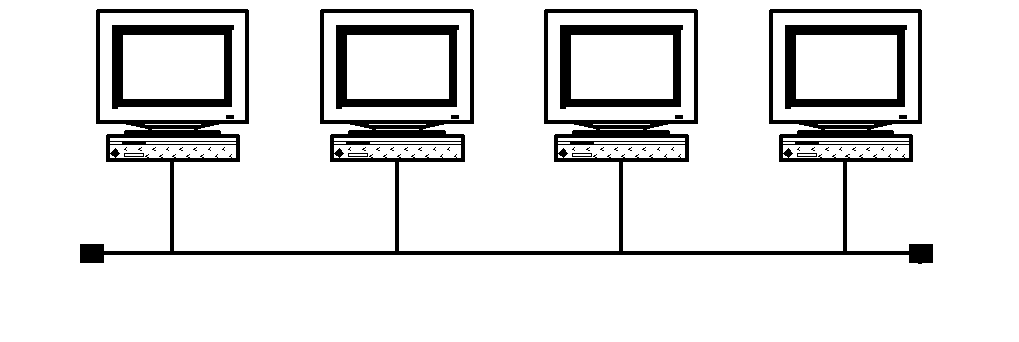
В *широковещательных* топологиях ПК передает сигналы, которые могут быть восприняты остальными ПК. К таким топологиям относятся топологии: общая шина, дерево, звезда.

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.

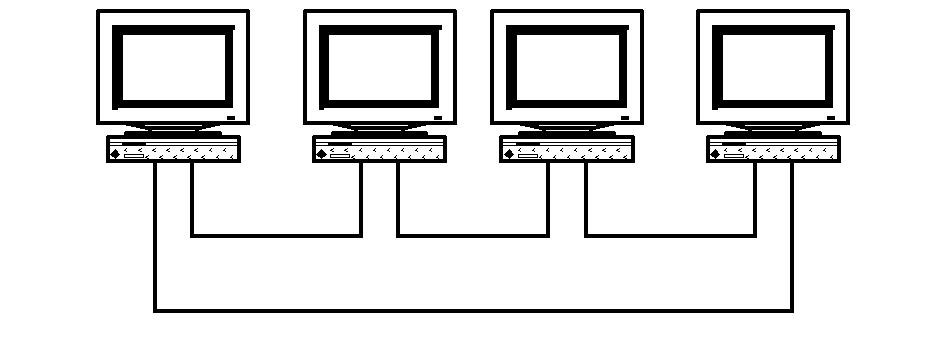
**Общая шина** - это тип сетевой топологии, в которой рабочие станции расположены вдоль одного участка кабеля, называемого сегментом.

Общая шина предполагает использование одного кабеля, к которому подключаются все компьютеры сети. В случае данной топологии кабель используется всеми станциями по очереди. Принимаются специальные меры для того, чтобы при работе с общим кабелем компьютеры не мешали друг другу передавать и принимать данные. Все сообщения, посылаемые отдельными компьютерами, принимаются и прослушиваются всеми остальными компьютерами, подключенными к сети. Рабочая станция отбирает адресованные ей сообщения, пользуясь адресной информацией. Надежность здесь выше, так как выход из строя отдельных компьютеров не нарушит работоспособность сети в целом. Поиск неисправности в сети затруднен. Кроме того, так как используется только один кабель, в случае обрыва нарушается работа всей сети. Шинная топология - это наиболее простая (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.**

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.

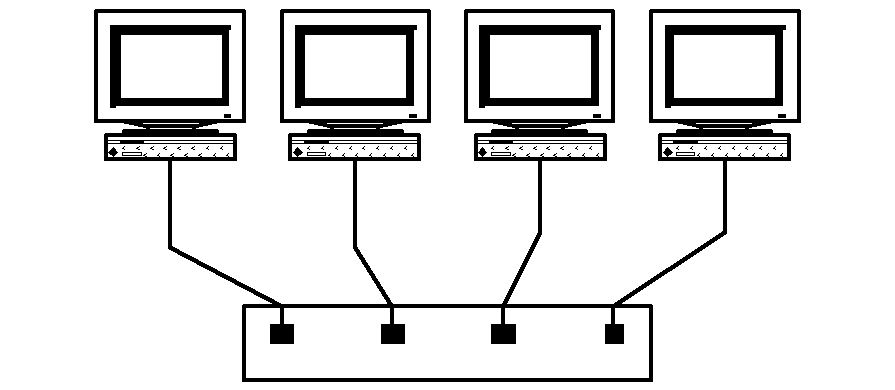
Проблемы:

* 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).

1. **Топология звезда.**

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.

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

Примером звездообразной топологии является топология Ethernet с кабелем типа Витая пара 10BASE-T, центром Звезды обычно является Hub.

Звездообразная топология обеспечивает защиту от разрыва кабеля. Если кабель рабочей станции будет поврежден, это не приведет к выходу из строя всего сегмента сети. Она позволяет также легко диагностировать проблемы подключения, 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.

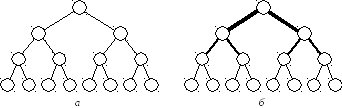
Недостатки:

* 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.

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

Преимущество:

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

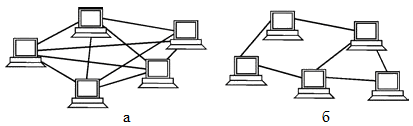
У суперкомпьютера наращивается пропускная способность, все вычисления происходят на листьях. Делается на оптике. Цена увеличения работает на вычислительную мощность.

1. **Ячеистые топологии.**

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 на прямую со всеми остальными ПК сети.

Частичная сеточная предполагает наличие связей между самыми активными узлами сети (передающие большие объёмы информации), с другими ПК связь через промежуточные узлы.

Характеристика:

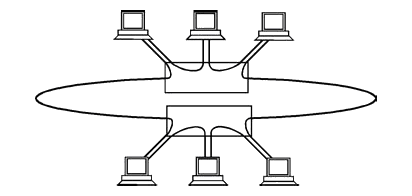
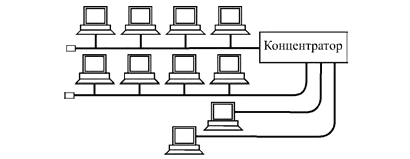
Наличие альтернативных путей передачи информации.

Логика последовательной топологии.

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):



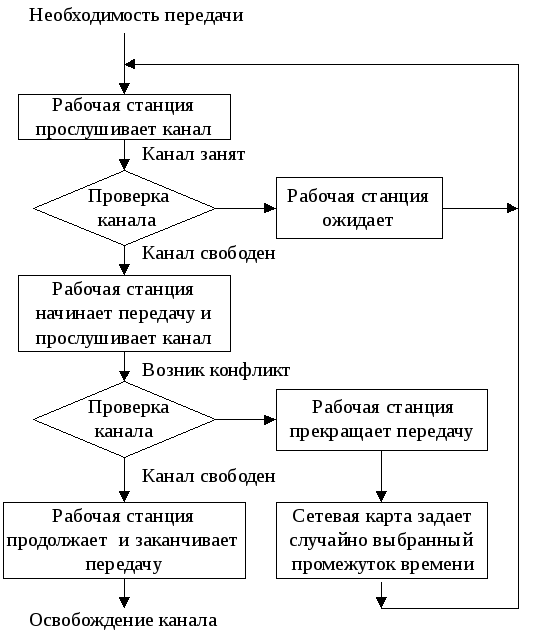
В звездно-шинной топологии к концентратору подключаются как отдельные компьютеры, так и целые шинные сегменты. На самом деле реализуется физическая топология шина, включающая все компьютеры сети. В данной топологии может использоваться и несколько концентраторов, соединенных между собой и образующих так называемую магистральную, опорную шину.

В 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.

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 (Carrier Sense Multiple Access with Collision Detection– CSMA/CD);
* множественный доступ с передачей полномочия (Token Passing Multiple Access – TPMA) или метод с передачей маркера;
* множественный доступ с разделением во времени (Time Division Multiple Access – TDMA);
* множественный доступ с разделением частоты (Frequency Division Multiple Access – FDMA) или множественный доступ с разделением длины волны (Wave length Division Multiple Access– 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.

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

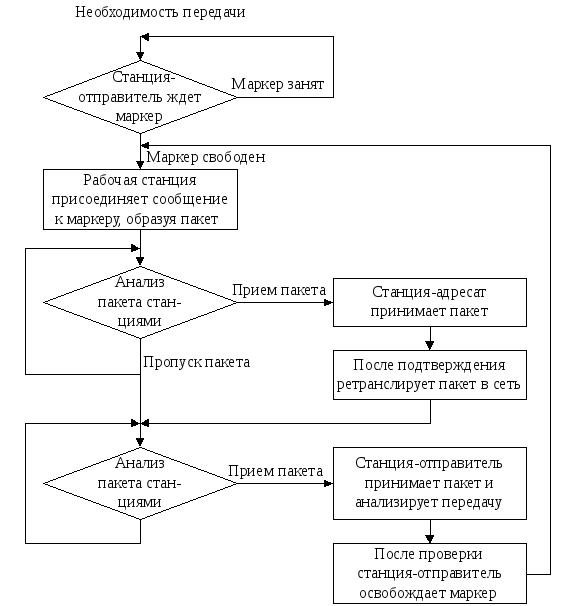
Протокол CSMA/CD работает на [канальном уровне](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) в модели [OSI](https://ru.wikipedia.org/wiki/Open_Systems_Interconnection).

1. **Метод доступа TPMA.**

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 в ЛВС. После чего пакет возвращается в узел из которого был отправлен. Здесь после проверки безошибочной передачи пакета, узел освобождает ЛВС, выпуская новый маркер. Таким образом, в ЛВС с передачей маркера невозможны коллизии (конфликты). Метод с передачей маркера в основном используется в кольцевой топологии.

Данный метод характеризуется следующими достоинствами:

* гарантирует определенное время доставки блоков данных в сети;
* дает возможность предоставления различных приоритетов передачи данных.

Вместе с тем он имеет существенные недостатки:

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

1. **Метод доступа TDMA.**

Множественный доступ с разделением во времени основан на распределении времени работы канала между системами (рис.4.7).

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.

1. **Метод доступа FDMA.**

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.

При использовании FDMA, именуемого также множественным доступом с разделением волны WDMA, широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. В каждой узкой полосе создается логический канал. Размеры узких полос могут быть различными. Передаваемые по логическим каналам сигналы накладываются на разные несущие и поэтому в частотной области не должны пересекаться. Вместе с этим, иногда, несмотря на наличие защитных полос, спектральные составляющие сигнала могут выходить за границы логического канала и вызывать шум в соседнем логическом канале.

В оптических каналах разделение частоты осуществляется направлением в каждый из них лучей света с различными частотами. Благодаря этому пропускная способность физического канала увеличивается в несколько раз. При осуществлении этого мультиплексирования в один световод излучает свет большое число лазеров (на различных частотах). Через световод излучение каждого из них проходит независимо от другого. На приемном конце разделение частот сигналов, прошедших физический канал, осуществляется путем фильтрации выходных сигналов. Метод доступа FDMA относительно прост, но для его реализации необходимы передатчики и приемники, работающие на различных частотах.

1. **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%).

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 тд. 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.

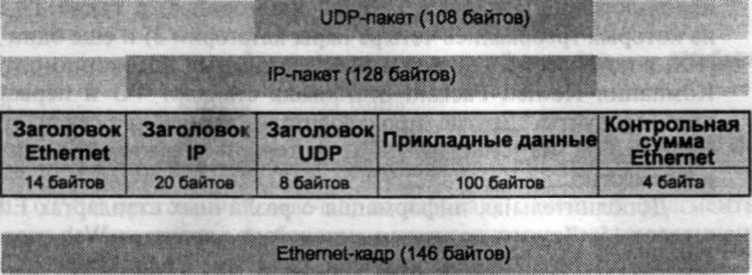
***Сетевой адрес*** *(****идентификатор****)* ***приёмника***, индивидуальный или групповой адрес, присвоенный каждому принимающему абоненту в сети.

***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.

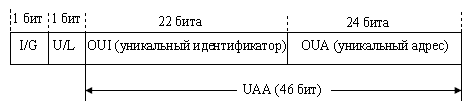
***Контрольная сумма пакета*** – это числовой код, формируемый передатчиком по определенным правилам и содержащий в свернутом виде информацию обо всем пакете. Приемник, повторяя вычисления, сделанные передатчиком, с принятым пакетом, сравнивает их результат с контрольной суммой и делает вывод о правильности 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.

Пакет от индификаторов до конца, кадр – всё.

1. **MAC-адреса и их структура.**

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.

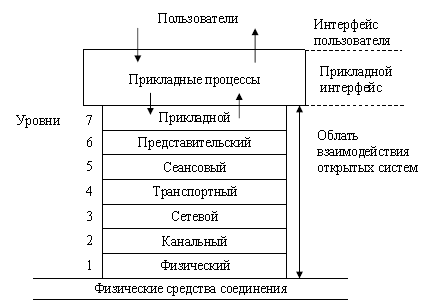
Младшие 24 разряда кода адреса называются OUA – организационно уникальный адрес. Именно их присваивает каждый из зарегистрированных производителей сетевых адаптеров. Всего возможно свыше 16 миллионов комбинаций, это значит, что каждый изготовитель может выпустить 16 миллионов сетевых адаптеров. С

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.

1. **7 - ая модель OSI. Назначение. Взаимодействие уровней модели OSI.**

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.

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. 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. 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.

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. 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.

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.

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: срочностью, возможностью восстановления прерванной связи, 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), способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

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 (Transmission Control Protocol) протокол управления передачей стека TCP/IP;

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

-  NCP (NetWare Core Protocol) базовый протокол сетей NetWare;

-  SPX (Sequenced Packet eXchange) упорядоченный обмен пакетами стека Novell;

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.

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.

5.       Маршрутизация и коммутации, сегментирование и объединение пакетов.

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 (Internetwork Packet Exchange) протокол межсетевого обмена пакетами, предназначенный для адресации и маршрутизации пакетов в сетях Novell;

-  X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов (частично этот протокол реализован на уровне 2);

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

- ARP и RARP – MAC  IP (по известному) и наоборот.

- ICMP протокол межсетевых управляющих сообщений

- IGMP протокол управления группами Интернета

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

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.

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

-  MAC (Media Assess Control) контроль доступа к среде. Подуровень MAC регулирует доступ к разделяемой физической среде (передача маркера или обнаружение коллизий или столкновений) и управляет доступом к [каналу связи](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;

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

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

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

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. 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.

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.

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 доступа CSMA/CD;

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

1. **Спецификации стандартов 802.1 – 802.7**

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

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

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

**Стандарт 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 802.5** описывает метод доступа к кольцу с передачей маркера, прототип – Token Ring.

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

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

1. **Спецификации стандартов 802.8 - 802.12.**

**Стандарт 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 (Fiber Distributed Data Interface). Скорость сети до 100 Мб/с. Данная технология позволяет включать до 500 узлов на расстоянии 100 км.

**Стандарт 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 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 802.11** рекомендации по использованию беспроводных сетей.

**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.

1. **Спецификации стандартов 802.14 - 802.22.**

**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 радио интерфейса 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* (Ultra Wideband, 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 протоколов. Сетевые протоколы. Транспортные протоколы. Прикладные протоколы.**

Стеки протоколов разбиваются на три уровня: сетевые; транспортные; прикладные.

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

* 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.

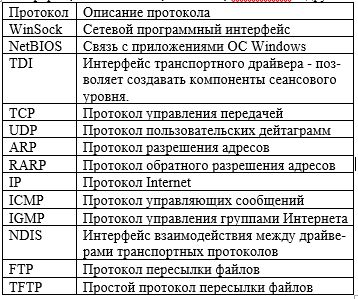
**Транспортные протоколы** предоставляют следующие услуги надежной транспортировки данных между компьютерами.

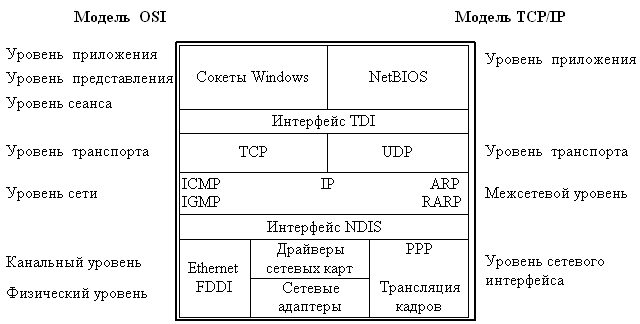
* NetBIOS (Базовая сетевая система ввода вывода). NetBIOS устанавливает соединение между компьютерами, а NetBEUI предоставляет услуги передачи данных для этого соединения.
* SPX (Последовательный обмен пакетами) в NWLink. Протокол NovelNetWare, используемый для обеспечения доставки данных.
* TCP (Протокол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

**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(HyperText Transfer Protocol) – протокол передачи гипертекста и другие протоколы.

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.



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.

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.

***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, Token Ring, затем IP-дейтаграмма помещается в область данных этого кадра, и он отправляется в сеть.

1. **Типы адресаций в сетях. Символьная адресация. Протоколы сопоставления адреса ARP и RARP.**

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

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 (Domain Name System), 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.

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

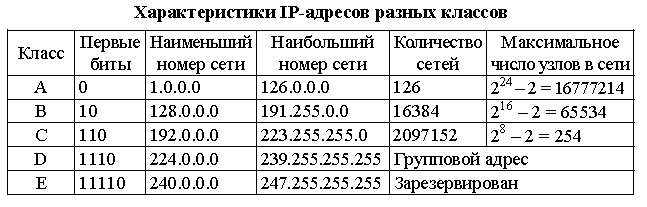
1. **Структура IPv4. Классы IP-адресов.**

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 равно 111111112 (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 подсети 172.16.0.0; 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.

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

К Кириллу**.**

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 не 256, а 254 узлов.

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 – индификаторов одиночного интерфейса маршрутизатора.
* Anycast – индификаторов набора интерфейсов принадлежащих различным узлам.
* Multicast – индификаторов набора интерфейсов принадлежащих разным узлам.

Интерфейс – средство подключения узла к каналу.

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

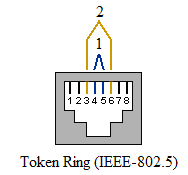
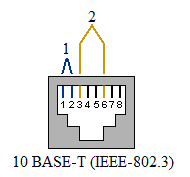
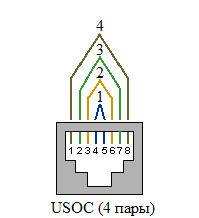
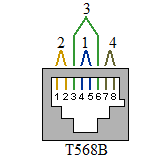
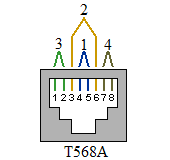
Если две и более групп подряд равны 0000, то они могут быть опущены и заменены на двойное двоеточие (::). Сокращению не могут быть подвергнуты 2 разделённые нулевые группы из-за возникновения неоднозначности.

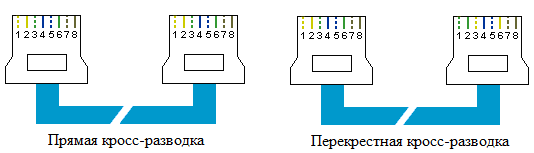
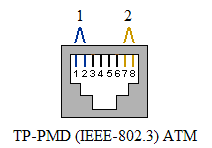
1. **Кабель типа «витая пара» (twisted pair). Схемы разводки. Кабельные системы Ethernet.**

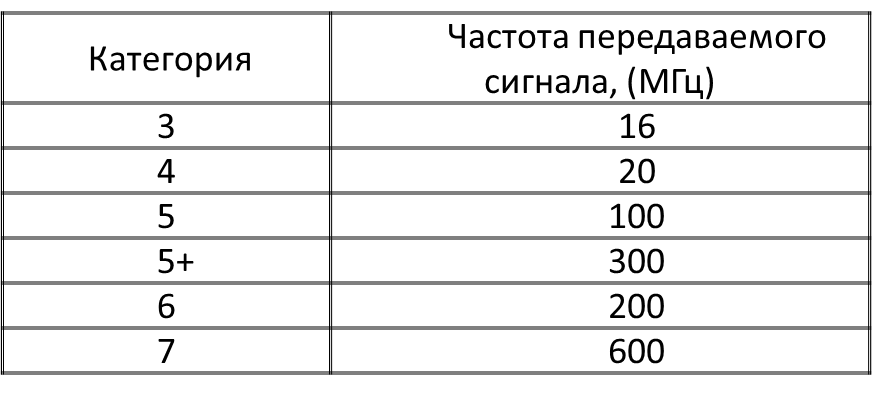
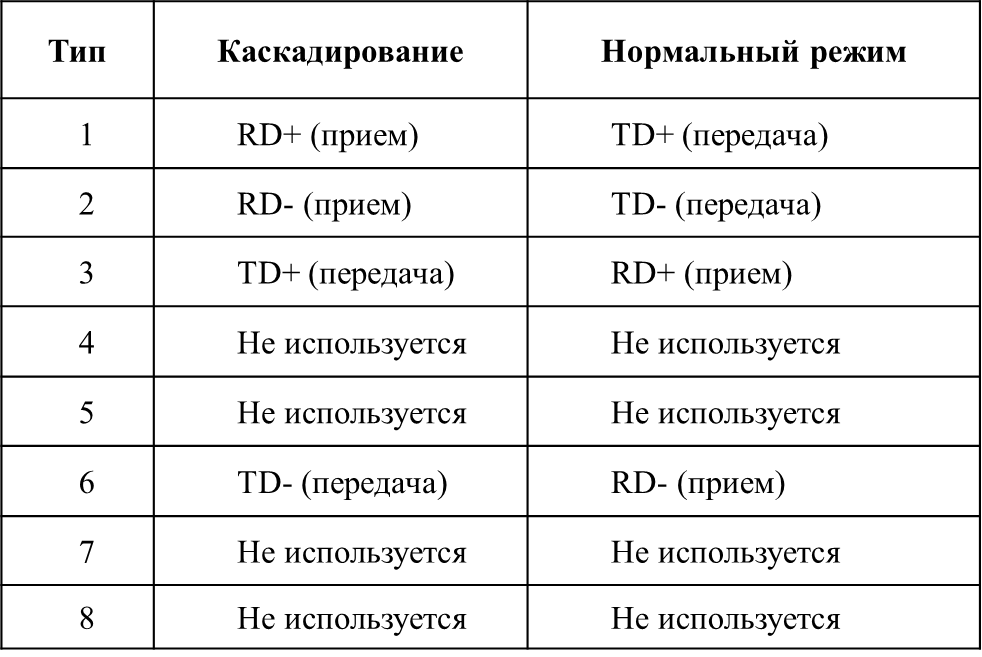
Выделяют два больших класса кабелей: электрические и оптические, которые принципиально различаются по способу передачи по ним сигнала. Из кабелей связи и других элементов (монтаж, крепеж, кожухи и т. д.) строят линии связи между узлами сети.

Витой парой называется кабель, в котором изолированная пара проводников скручена с небольшим числом витков на единицу длины. Скручивание проводов уменьшает электрические помехи извне при распространении сигналов по кабелю, а экранированные витые пары еще более увеличивают степень помехозащищенности сигналов.

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





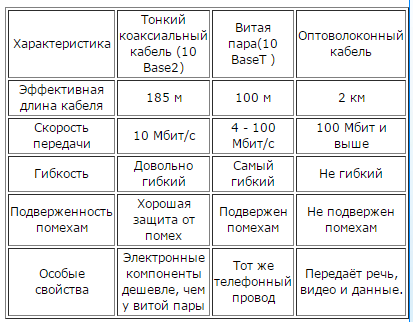


1. **Кабели и структурированные кабельные системы. Коаксиальные кабели.**

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.

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

Сетевые адаптеры – это сетевое оборудование, обеспечивающее функционирование сети на физическом и канальном уровнях, относится к периферийному устройству компьютера, непосредственно взаимодействующему со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами. Это устройство решает задачи надежного обмена двоичными данными, представленными соответствующими электромагнитными сигналами, по внешним линиям связи. Как и любой контроллер компьютера, сетевой адаптер работает под управлением драйвера операционной системы. Сетевые адаптеры должны быть совместимы с кабельной системой сети, внутренней информационной шиной ПК и сетевой операционной системой.

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.

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. **Мосты. Назначение. Особенности использования.**

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. Что касается канального процесса, то он объединяет разнотипные каналы передачи данных в один общий. Мост, а также его быстродействующий аналог –коммутатор (switchinghub), 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 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).

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

Коммутатор (switch) – устройство, осуществляющее выбор одного из возможных вариантов направления передачи данных. 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 при использовании коммутатора скорости передачи сигналов в соединяемых каналах передачи данных должны быть одинаковыми. Канальные процессы, реализуемые коммутатором, выполняются специальными интегральными схемами. В отличие от других видов ретрансляционных систем, здесь, как правило, не используется программное обеспечение. Вначале коммутаторы использовались лишь в территориальных сетях. Затем они появились и в локальных сетях, например, частные учрежденческие коммутаторы. Позже появились коммутируемые локальные сети. Их ядром стали коммутаторы локальных сетей.

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

1. **Различие между мостом и коммутатором.**

Разница между мостом и коммутатором состоит в том, что мост в каждый момент времени может осуществлять передачу кадров только между одной парой портов, а коммутатор одновременно поддерживает потоки данных между всеми своими портами. Другими словами, мост передает кадры последовательно, а коммутатор параллельно. Мосты используются только для связи локальных сетей с глобальными, то есть как средства удаленного доступа, поскольку в этом случае необходимость в параллельной передаче между несколькими парами портов просто не возникает.

1. **Маршрутизаторы. Назначение. Особенности использования. Различия между маршрутизаторами и мостами.**

Маршрутизатор (router) – ретрансляционная система, соединяющая две коммуникационные сети либо их части, реализует протоколы физического, канального уровней. Специальные сетевые процессы соединяют части коммутатора в единое целое. 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 обеспечивают также соединение административно независимых коммуникационных сетей. Для работы маршрутизаторов требуется один и тот же протокол во всех сегментах, с которыми он связан.

Маршрутизаторы не обладают такой способностью к анализу сообщений как мосты, но зато могут принимать решение о выборе оптимального пути для данных между двумя сетевыми сегментами. Мосты принимают решение по поводу адресации каждого из поступивших пакетов данных, переправлять его через мост или нет в зависимости от адреса назначения. Маршрутизаторы же выбирают из таблицы маршрутов наилучший для данного пакета. При связывании сетей с различными протоколами лучше использовать мосты.

1. **Шлюзы. Назначение. Особенности использования.**

**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.

1. **Беспроводные технологии: радиосвязь, инфракрасная, связь в микроволновом диапазоне.**

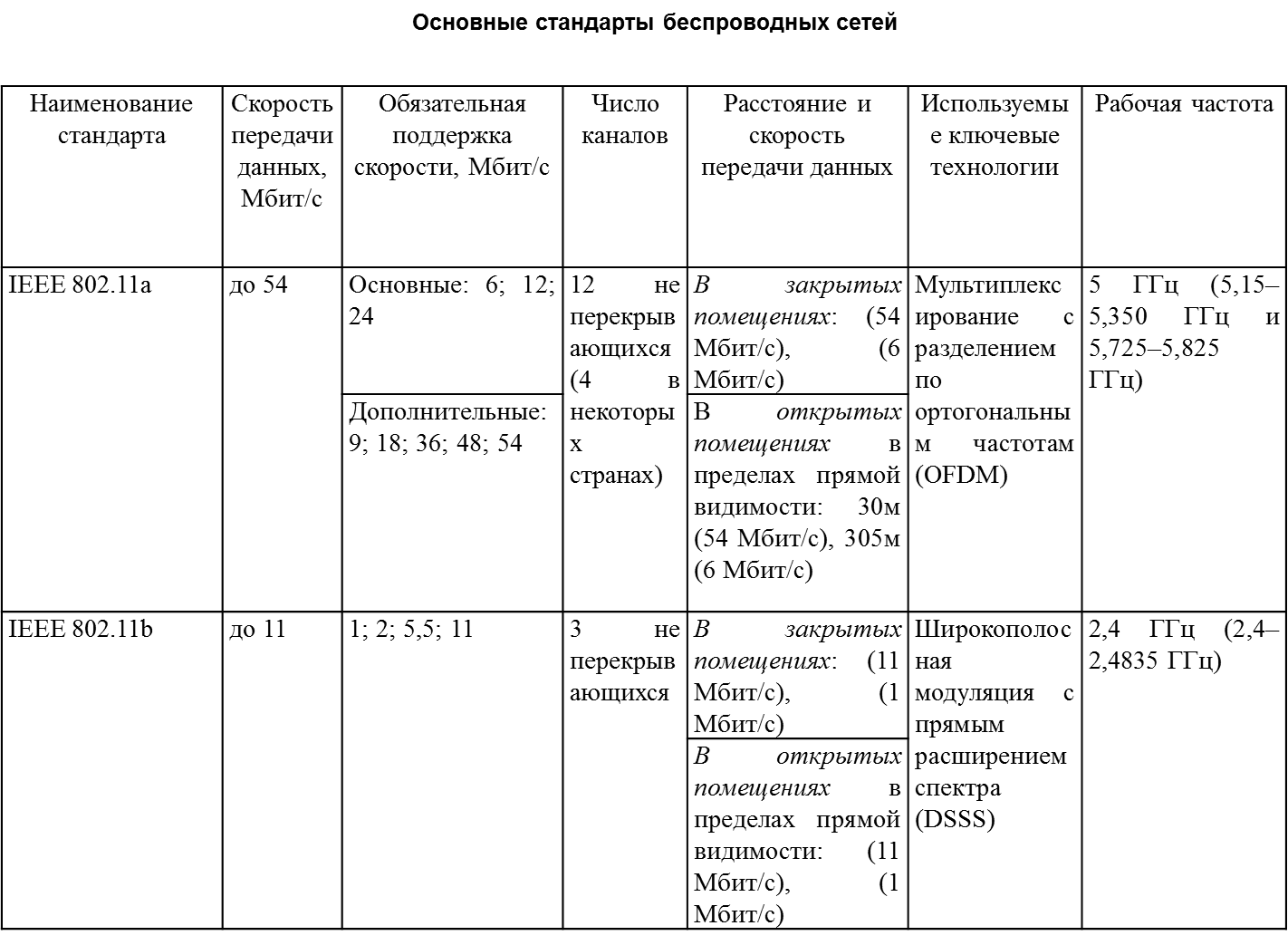
Методы беспроводной технологии (wireless) передачи данных являются удобным, а иногда незаменимым средством связи. Беспроводные технологии различаются по типам сигнала, частоте и расстоянию передачи. Большое значение имеют помехи и стоимость. Можно выделить три основных типа беспроводной технологии: радиосвязь;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

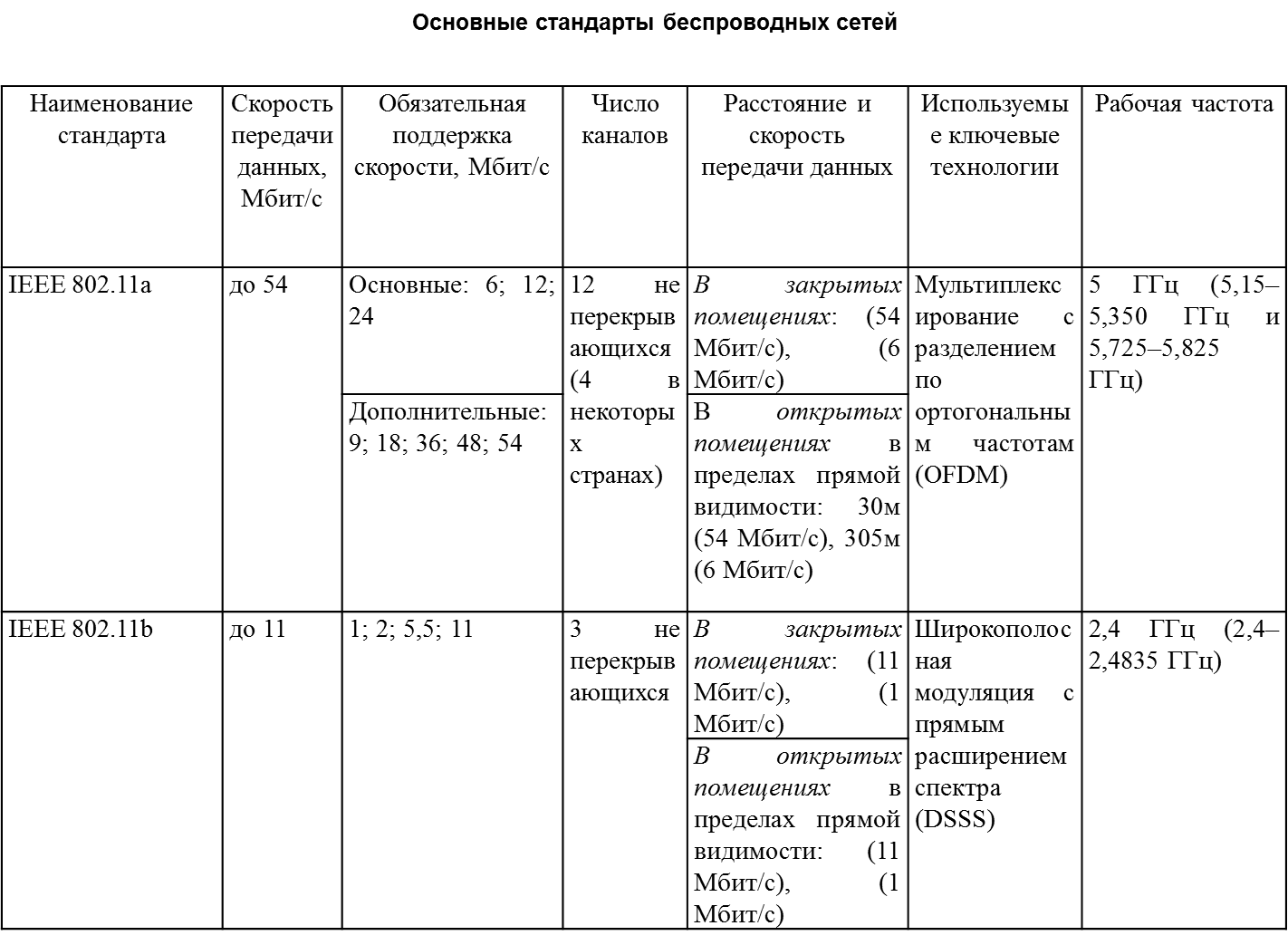
**Инфракрасные технологии** (Infrared transmission), функционируют на очень высоких частотах, приближающихся к частотам видимого света. Они могут быть использованы для установления двусторонней или широковещательной передачи на близких расстояниях. При инфракрасной связи обычно используют светодиоды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

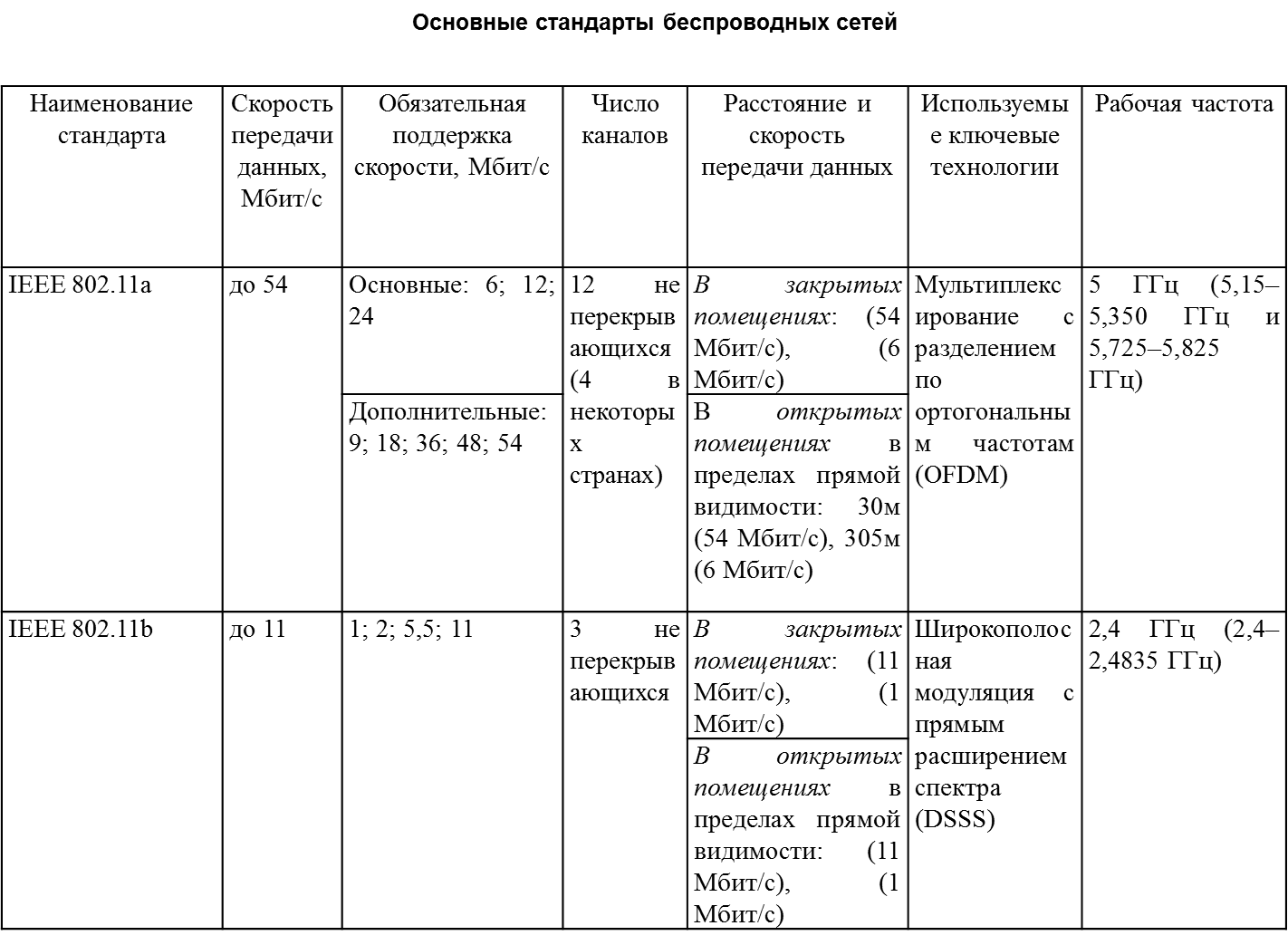
Технологии **радиосвязи** пересылают данные на радиочастотах и практически не имеют ограничений по дальности. Она используется для соединения локальных сетей на больших географических расстояниях. Радиопередача в целом имеет высокую стоимость и чувствительна к электронному и атмосферному наложению, а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

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

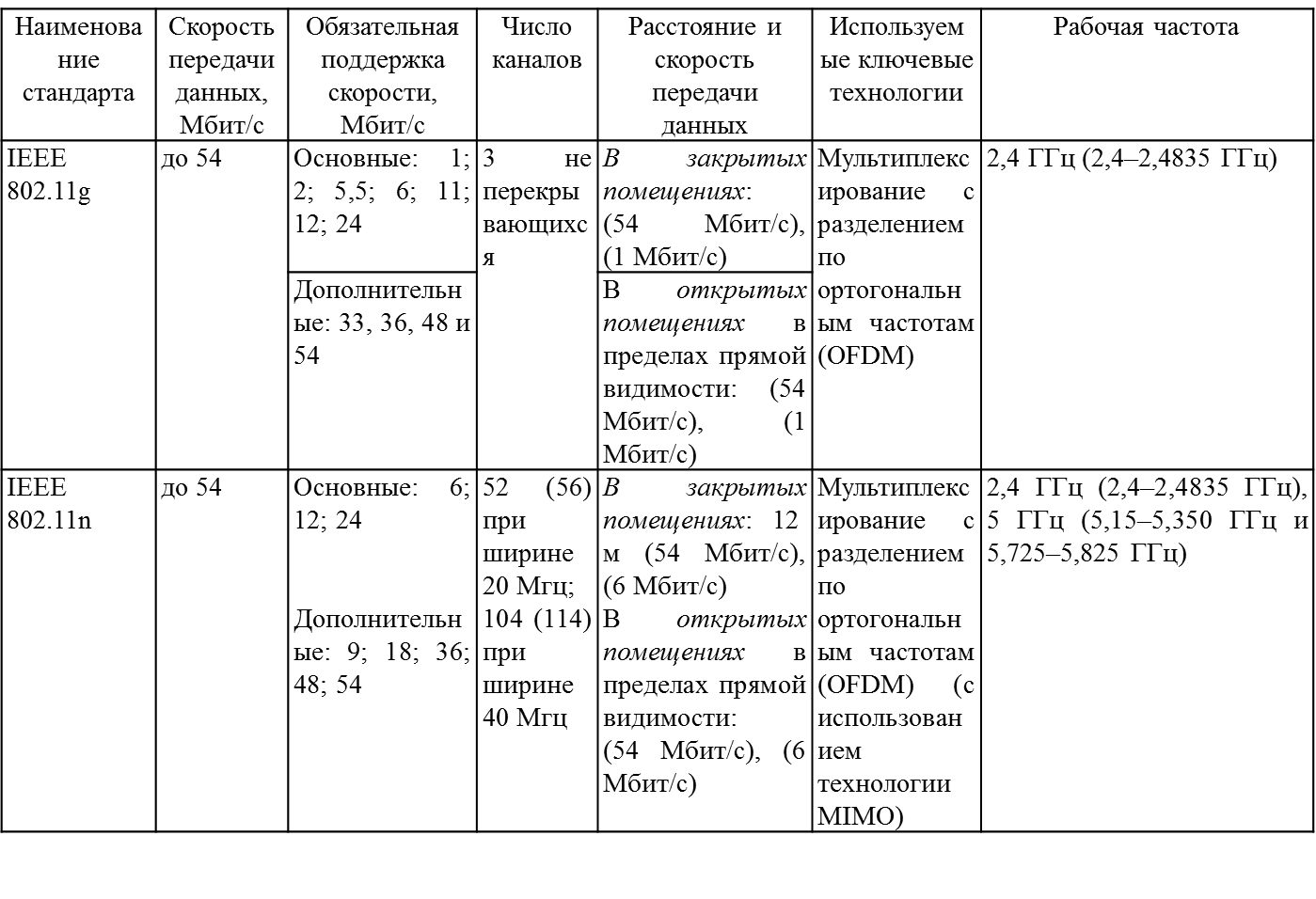
******

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

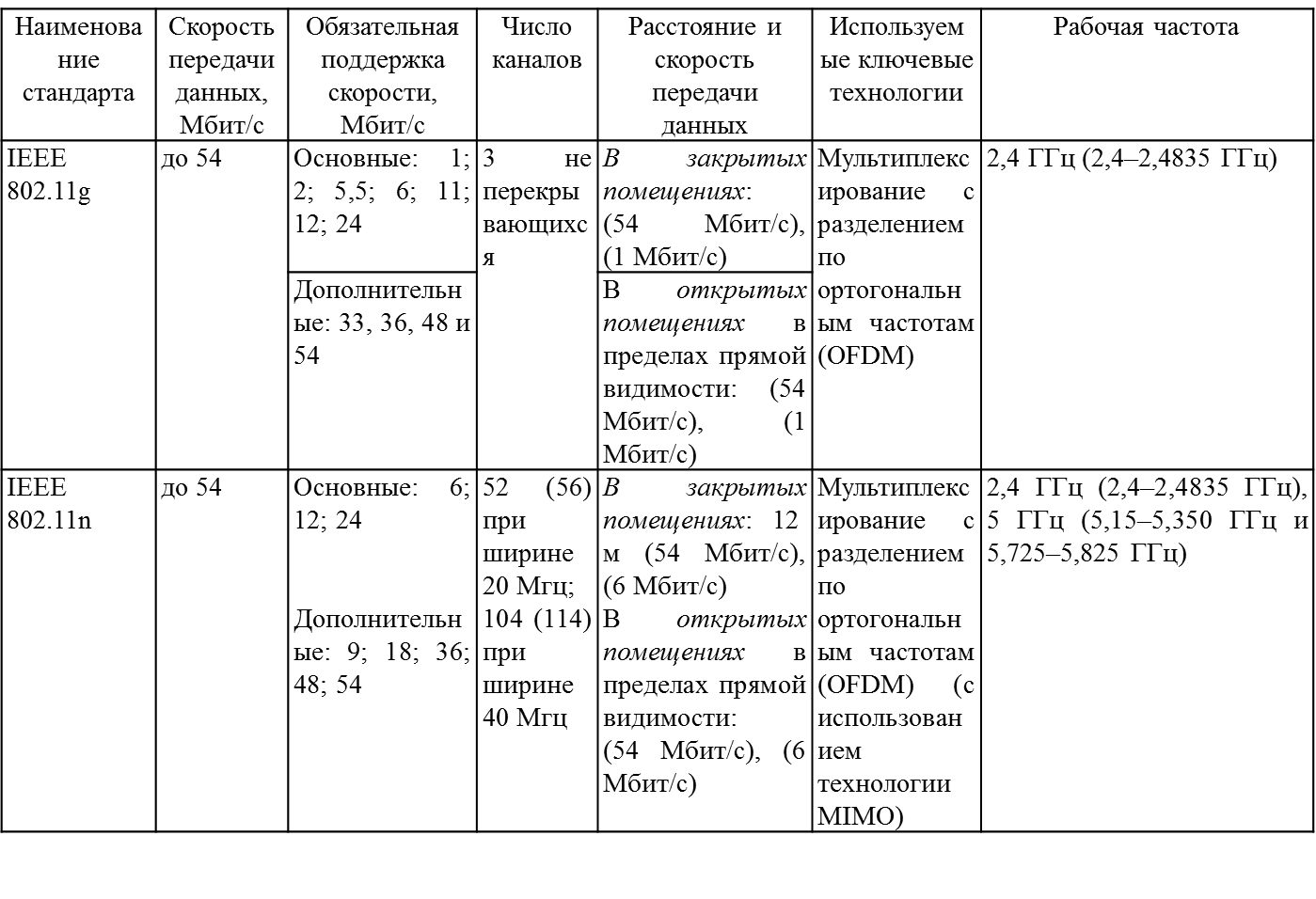
******

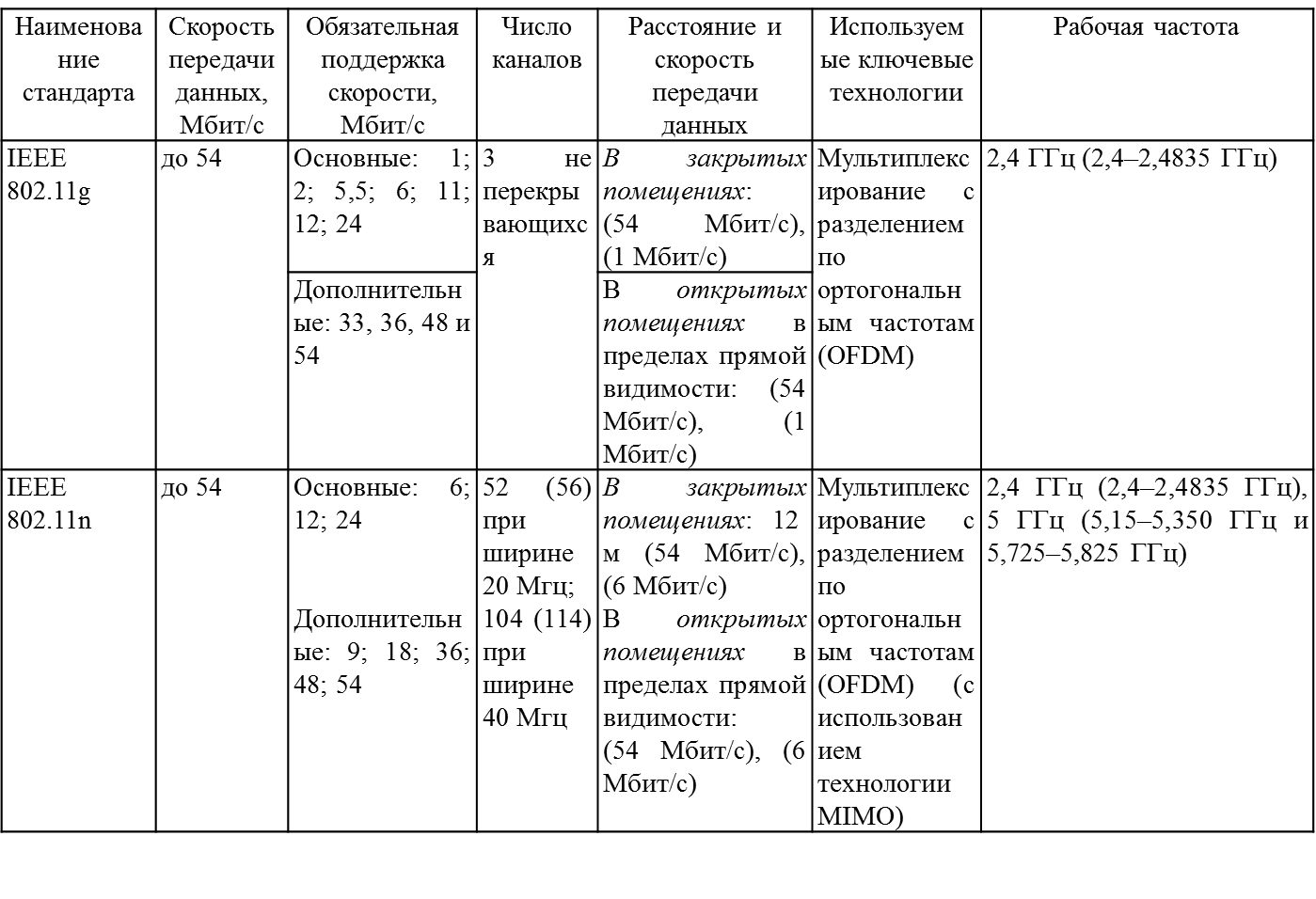
******

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

******

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

******

******

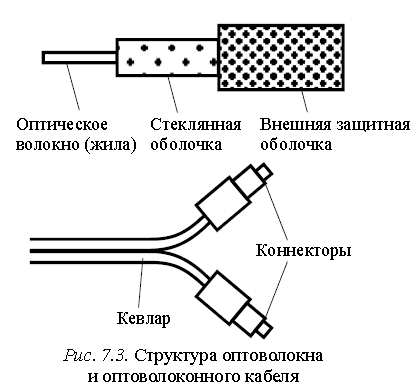
1. **Оборудование для сетей Wi-Fi.**

Сети Wi-Fi отождествляются  с аббревиатурей *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.

1. **Особенности оптических систем связи (физические, технические).**

 ***Физические особенности.***

Широкополосность оптических сигналов обусловлена чрезвычайно высокой частотой несущей (Fo == 1014 Гц). Это означает, что по оптической линии связи можно передавать информацию со скоростью порядка 1000 Мбит/с. Говоря другими словами, по одному волокну можно передать одновременно 10 миллионов телефонных разговоров и миллион видеосигналов.

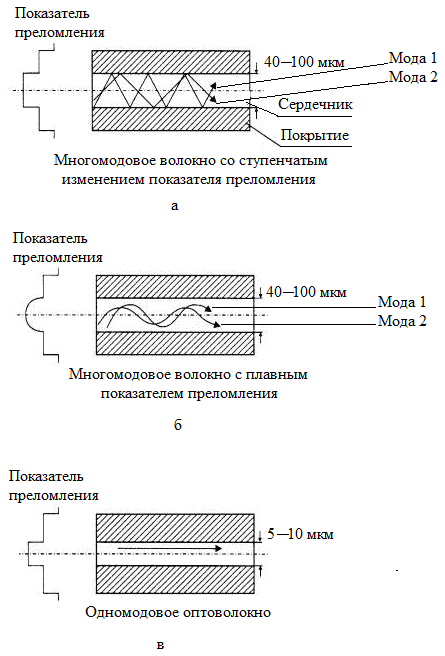
Скорость передачи данных может быть увеличена за счет передачи информации сразу в двух направлениях, так как световые волны могут распространяться в одном волокне независимо друг от друга. На сегодняшний день предел по плотности передаваемой информации по оптическому волокну не достигнут. Очень малое (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 длиной до 100 км 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. Применяя особо прочный пластик, на кабельных заводах изготавливают самонесущие подвесные кабели, не содержащие металла и тем самым безопасные в электрическом отношении. Такие кабели можно монтировать на мачтах существующих линий электропередач, как отдельно, так и встроенными в фазовый провод, экономя значительные средства на прокладку кабеля через реки и другие преграды.

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.

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

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

− многомодовое волокно со ступенчатым изменением показателя преломления (рис. 7.4, а);

− многомодовое волокно с плавным изменением показателя

преломления (рис. 7.4, б);

− одномодовое волокно (рис. 7.4, в).

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

В **одномодовом** кабеле (Single Mode Fiber, SMF) используется центральный проводник очень малого диаметра, соизмеримого с длиной волны света – от 5 до 10 мкм. При этом практически все лучи света распространяются вдоль оптической оси световода, не отражаясь от внешнего проводника.

В **многомодовых** кабелях (Multi Mode Fiber, 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, где 62,5 мкм или 50 мкм – это диаметр центрального проводника, а 125 мкм – диаметр внешнего проводника. В многомодовых кабелях во внутреннем проводнике одновременно существует несколько световых лучей, отражающихся от внешнего проводника под разными углами. Угол отражения луча называется модой луча.

1. **Достоинства и недостатки оптических систем связи.**

**Недостатки волоконной технологии.** 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. Другой недостаток заключается в том, что 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** (ВОЛС) настолько значительны, что, несмотря на перечисленные недостатки оптического волокна, эти линии связи все шире используются для передачи информации.

1. **Защита информации. Основные понятия. Виды основных сетевых атак.**

**Защита информации** – это комплекс мероприятий, проводмых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования 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 худшем случае 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, находящийся внутри организации или за ее пределами, выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, хакер может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для 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 для своей организации они требуют минимум знаний и умений: все необходимое 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 к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера. Для атак этого типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации. Атаки проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

1. **Классификация средств защиты информации.**

* Технические
* Программные
* Смешанные аппаратно-программные средства
* Организационные средства

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. Классические алгоритмы шифрования данных.**

**Шифрование** данных представляет собой разновидность программных средств защиты информациии имеет особое значение на практике как единственная надежная защита информации, передаваемой по протяженным последовательным линиям, от утечки. 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 (уязвимость - статистика появления различных символов)
* Перестановка
* Гамирование (смешивание с маской, основано на сложении по модулю 2, побитовое «или»)

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. **Стандартные методы шифрования и криптографические системы.**

**SKIP-технология** (Secure Key Internet Protocol) – стандарт защиты трафика IP-пакетов, позволяющий на сетевом уровне обеспечить защиту соединения и передаваемых данных.

Возможны два способа реализации SKIP-защиты трафика IP-пакетов:

– шифрование блока данных IP-пакета;

– инкапсуляция IP-пакета в SKIP-пакет.

SKIP-пакет похож на обычный IP-пакет. В поле данных SKIP- пакета полностью размещается в зашифрованном виде исходный IP- пакет. В этом случае в новом заголовке вместо истинных адресов могут быть помещены некоторые другие адреса. Такая структура SKIP-пакета позволяет беспрепятственно направлять его любому хост-компьютеру в сети Интернет, при этом межсетевая адресация осуществляется по обычному IP-заголовку в SKIP-пакете. Конечный получатель SKIP-пакета по заранее определенному разработчиками алгоритму расшифровывает криптограмму и формирует обычный TCP- или UDP-пакет, который и передает соответствующему модулю (TCP или UDP) ядра операционной системы.

**SSL** (Secure Sockets Layer, протокол защищенных сокетов) создает защищенное соединение между двумя сокетами, позволяющее:

* клиенту и серверу договориться об используемых параметрах;
* клиенту и серверу произвести взаимную аутентификацию;
* организовать тайное общение; обеспечить защиту целостности данных.

К специализированным программным средствам защиты информации от несанкционированного доступа в компьютерных сетях относятся и **proxy-серверы** (proxy – доверенное лицо, доверенность). Идея использования **proxy-сервера** заключается в том, что весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью – маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники.

Синхронные:

* DES (используется 3DES, 56 байт)
* Алгоритм IDEA (128 байт)
* ГОСТ 28147-89 (256 байт)

Асинхронные:

* PGA
* RSA

+ электронные цифровые подписи.