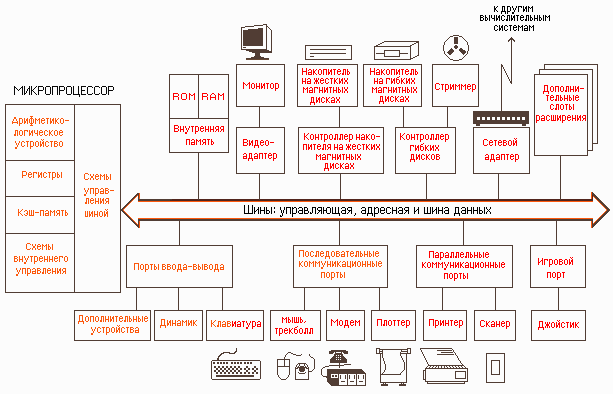
### 1.Структура ПК



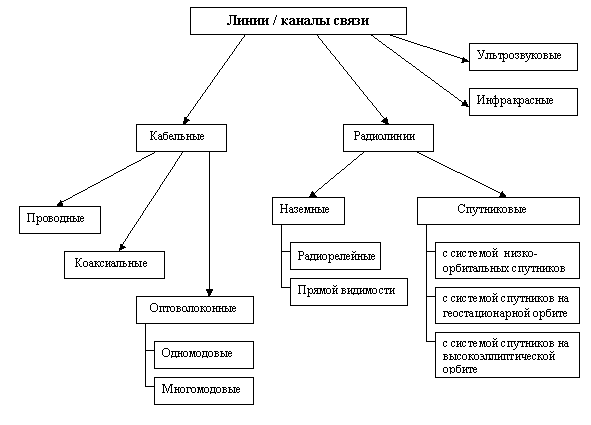
### 2.Методы и средства защиты информации в КС

Локальные сети предприятий очень часто подключаются к сети Интернет. Для защиты локальных сетей компаний, как правило, применяются межсетевые экраны - брандмауэры (firewalls). Экран (firewall) - это средство разграничения доступа, которое позволяет разделить сеть на две части (граница проходит между локальной сетью и сетью Интернет) и сформировать набор правил, определяющих условия прохождения пакетов из одной части в другую. Экраны могут быть реализованы как аппаратными средствами, так и программными.

К средствам защиты информации ИС от действий субъектов относятся:

* средства защита информации от несанкционированного доступа;
* защита информации в компьютерных сетях;
* криптографическая защита информации;
* [электронная цифровая подпись](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C);
* защита информации от компьютерных вирусов.

### 3.Типы линий связи ЛВС



### 4.Пакеты,протоколы и методы управления информационным обменом между

**Пакет** — это определённым образом оформленный блок [данных](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5), передаваемый по сети в пакетном режиме. При разбиении данных на пакеты скорость их передачи возрастает настолько, что каждый компьютер в сети получает возможность принимать и передавать данные практически одновременно с остальными компьютерами.

Методы управления обменом в локальных сетях делятся на две группы:

* ***Централизованные методы***, в которых все управление обменом сосредоточено в одном месте. Недостатки таких методов: неустойчивость к отказам центра, малая гибкость управления (центр обычно не может оперативно реагировать на все события в сети). Достоинство *централизованных методов* – отсутствие конфликтов, так как центр всегда предоставляет право на передачу только одному абоненту, и ему не с кем конфликтовать.
* **Децентрализованные методы**, в которых отсутствует центр управления. Всеми вопросами управления, в том числе предотвращением, обнаружением и разрешением конфликтов, занимаются все абоненты сети. Главные достоинства децентрализованных методов: высокая *устойчивость к отказам* и большая гибкость. Однако в данном случае возможны конфликты, которые надо разрешать.

[TCP/IP](https://ru.wikipedia.org/wiki/TCP/IP) — набор протоколов передачи данных, получивший название от двух принадлежащих ему протоколов. *Наиболее известные протоколы, используемые в сети Интернет:*

* [HTTP](https://ru.wikipedia.org/wiki/HTTP) — это протокол передачи [гипертекста](https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%BF%D0%B5%D1%80%D1%82%D0%B5%D0%BA%D1%81%D1%82). Протокол HTTP используется при пересылке Web-страниц с одного компьютера на другой.
* [FTP](https://ru.wikipedia.org/wiki/FTP) — это протокол передачи файлов со специального файлового сервера на компьютер пользователя. FTP дает возможность абоненту обмениваться двоичными и текстовыми файлами с любым компьютером сети. Установив связь с удаленным компьютером, пользователь может скопировать файл с удаленного компьютера на свой или скопировать файл со своего компьютера на удаленный.
* [POP](https://ru.wikipedia.org/wiki/POP) — это стандартный прот. почтового соединения. Серверы POP обраб-ют вход. почту, а прот. POP предназначен для обработки запросов на получение почты от клиентских почтовых программ.
* [SMTP](https://ru.wikipedia.org/wiki/SMTP) — протокол, который задает набор правил для передачи почты. Сервер SMTP возвр-ет либо подтверждение о приеме, либо сообщение об ошибке, либо запрашивает дополнительную инф-цию.
* [TELNET](https://ru.wikipedia.org/wiki/TELNET) — это протокол удаленного доступа. TELNET дает возможность абоненту работать на любой ЭВМ сети Интернет, как на своей собственной, то есть запускать программы, менять режим работы и так далее. На практике возможности ограничиваются тем уровнем доступа, который задан администратором удаленной машины.

### 5.Беспроводные сети Wi-Fi

**Wi-Fi** — торговая марка [Wi-Fi Alliance](http://alliance) для беспроводных сетей на базе стандарта [IEEE 802.11](https://ru.wikipedia.org/wiki/IEEE_802.11). Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity[[1]](https://ru.wikipedia.org/wiki/Wi-Fi" \l "cite_note-1), которое можно дословно перевести как «беспроводное качество» или «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

Любое оборудование, соответствующее стандарту [IEEE 802.11](https://ru.wikipedia.org/wiki/IEEE_802.11), может быть протестировано в [Wi-Fi Alliance](http://alliance) и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.

По способу объединения точек доступа в единую систему можно выделить:

* Автономные точки доступа (называются также самостоятельные, децентрализованные, умные)
* Точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные)
* Бесконтроллерные, но не автономные (управляемые без контроллера)

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

* Со статическими настройками радиоканалов
* С динамическими (адаптивными) настройками радиоканалов
* Со «слоистой» или многослойной структурой радиоканалов

**Преимущества Wi-Fi**

* позволяет развернуть сеть без прокладки [кабеля](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C), что может уменьшить стоимость развёртывания и/или расширения сети.
* позволяет иметь доступ к сети мобильным устройствам.
* гарантируется совместимость оборудования благодаря обязательной сертификации оборудования с логотипом wi-fi.
* мобильность.
* в пределах wi-fi зоны в сеть интернет могут выходить несколько пользователей с компьютеров, ноутбуков, телефонов и т. д.
* излучение от wi-fi устройств в момент передачи данных на порядок (в 10 раз) меньше, чем у сотового телефона

### 6.Выбор конфигурации сетей Ethernet и Fast Ethernet

**Ethernet: Модель 1**

Первая модель формулирует набор простых правил, которые необходимо соблюдать проектировщику сети при соединении отдельных компьютеров и сегментов.

1. Репитер или концентратор, подключенный к сегменту, снижает на единицу максимально допустимое число абонентов, подключаемых к сегменту.

2. Полный путь между двумя любыми абонентами должен включать в себя не более пяти сегментов, четырех концентраторов (репитеров) и двух трансиверов (MAU) для сегментов 10 BASES.

З.Если путь между абонентами состоит из пяти сегментов и четырех концентраторов (репитеров), то количество сегментов, к которым подключены компьютеры, не должно превышать трех, а остальные сегменты должны просто связывать между собой концентраторы (репитеры). Это так называемое «правило 5-4-3».

4. Если путь между абонентами состоит из четырех сегментов и трех концентраторов (репитеров), то должны выполняться следующие условия:

* максимальная длина оптоволоконного кабеля сегмента 10BASE-FL, соединяющего между собой концентраторы (репитеры), не должна превышать 1000 м;
* максимальная длина оптоволоконного кабеля сегмента 10BASE-FL, соединяющего концентраторы (репитеры) с компьютерами, не должна превышать 400 м;
* ко всем сегментам могут подключаться компьютеры.

**Ethernet: Модель 2**

В модели 2 используются две системы расчетов:

* первая система предполагает вычисление двойного (кругового) времени прохождения сигнала по сети и сравнение его с максимально допустимой величиной;
* вторая система проверяет допустимость величины получаемого межкадрового временного интервала, межпакетной щели (IPG - InterPacket Gap) в сети.

При этом вычисления в обеих системах расчетов ведутся для наихудшего случая, для пути максимальной длины, то есть для такого пути передаваемого по сети пакета, который требует для своего прохождения максимального времени. При первой системе расчетов выделяются три типа сегментов:

* начальный сегмент — это сегмент, соответствующий началу пути максимальной длины;
* конечный сегмент — это сегмент, расположенный в конце пути максимальной длины;
* промежуточный сегмент - это сегмент, входящий в путь максимальной длины, но не являющийся ни начальным, ни конечным.

Промежуточных сегментов в выбранном пути может быть несколько, а начальный и конечный сегменты при разных расчетах могут меняться местами друг с другом. Выделение трех типов сегментов позволяет автоматически учитывать задержки сигнала на всех концентраторах, входящих в путь максимальной длины, а также в приемопередающих узлах адаптеров.

Для расчетов используются величины задержек. Методика расчета сводится к следующему.

1. В сети выделяется путь максимальной длины. Все дальнейшие расчеты ведутся для него. Если этот путь не очевиден, то расчеты ведутся для всех возможных путей, и на основании этих расчетов выбирается путь максимальной длины.

2. Если длина сегмента, входящего в выбранный путь, не максимальна, то рассчитывается двойное (круговое) время прохождения в каждом сегменте выделенного пути по формуле: ts = LtL + to, где L — длина сегмента в метрах (при этом надо учитывать тип сегмента: начальный, промежуточный или конечный).

3. Если длина сегмента равна максимально допустимой, то из таблицы для него берется величина максимальной задержт ки t .

4. Суммарная величина задержек всех сегментов выделенного пути не должна превышать предельной величины 512 битовых интервалов (51,2 мкс).

5. Выполняются те же действия для обратного направления выбранного пути (то есть конечный сегмент считается начальным, и наоборот). Из-за разных задержек передающих и принимающих узлов концентраторов величины задержек в разных направлениях могут отличаться (правда, не слишком сильно).

6. Если задержки в обоих случаях не превышают величины 512 битовых интервалов, то сеть считается работоспособной.

**Fast Ethernet: Модель 1**

* В соответствии с первой моделью, при выборе конфигурации в любом случае надо руководствоваться следующими принципами:
* Сегменты, выполненные на электрических кабелях (витых парах) не должны быть длиннее 100 м. Это относится к кабелям всех возможных категорий - 3, 4 и 5, к сегментам 100BASE-T4 и 100BASE-TX.
* Сегменты, выполненные на оптоволоконных кабелях, не должны быть длиннее 412м.
* Если используются адаптеры с внешними (выносными) трансиверами, то трансиверные кабели (МП) не должны быть длиннее 50 см.

Модель 1 выделяет три возможных конфигурации сети Fast Ethernet:

1. Соединение двух абонентов (узлов) сети напрямую, без репитера или концентратора (рис. 10.4). Абонентами при этом могут выступать не только компьютеры, но и сетевой принтер, порт коммутатора, моста или маршрутизатора. Это соединение называется соединением DTE—DTE или двухточечным.

2. Соединение двух абонентов сети с помощью одного репитер-ного концентратора класса I или класса II.

3. Соединение двух абонентов сети с помощью двух репитер-ных концентраторов класса II (рис. 10.6). При этом предполагается, что для связи концентраторов всегда используется электрический кабель длиной не более 5 м. Концентраторы класса II имеют меньшую задержку, поэтому их может быть два. Использование трех концентраторов не допускается в соответствии с моделью 1 ни в коем случае.

**Fast Ethernet: Модель 2**

Вторая модель для сети Fast Ethernet, как и в случае Ethernet, основана на вычислении суммарного двойного времени прохождения сигнала по сети.

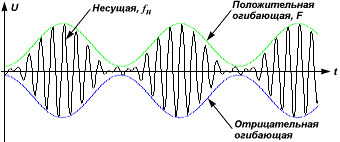
Для расчетов в соответствии со второй моделью сначала надо выделить в сети путь с максимальным двойным временем прохождения и максимальным числом репитеров (концентраторов) между компьютерами, то есть путь максимальной длины. Если таких путей несколько, то расчет должен производиться для каждого из них

### 7.Методы модуляции сигналов

Модуляция – это процесс изменения каких-либо параметров несущего сигнала под действием информационного потока.

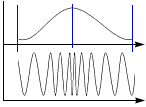
Амплитудная модуляция

В радиовещании в длинно- и средневолновом диапазоне радиоволн широко используется амплитудная модуляция сигнала. На вход модулятора подаются опорный сигнал и передаваемый (модулирующий), а на выходе получаем смодулированный сигнал, положительная огибающая которого и есть исходный сигнал. Для корректного преобразования необходимо, чтобы несущая частота должна была быть, по крайней мере, в два раза выше, чем верхняя граница полосы модулирующего сигнала.



Частотная модуляция

При частотной модуляции модулирующий сигнал модулирует не мощность опорного сигнала, а его частоту. То есть, если уровень сигнала увеличивается, то частота растет, и наоборот. Из-за этого спектр частотно-модулированного сигнала значительно шире исходного сигнала. Соответственно, частотная модуляция обладает высокой помехоустойчивостью, но для ее применения необходимо занимать высокочастотные диапазоны вещания.



Фазовая модуляция

При фазовой модуляции модулирующий сигнал модулирует фазу опорного сигнала. При модулировании цифровым (дискретным) сигналом получается сигнал с очень широким спектром, так как фаза резко поворачивается (двоичный сигнал — на 180 градусов). Поэтому фазовую модуляцию с успехом применяют для обеспечения помехозащищенной цифровой связи в микроволновых диапазонах.

### 8.Режим мультиплексирования передачи данных в КС

**Мультиплексирование** (англ. multiplexing, muxing)— это процесс уплотнение канала связи, другими словами, передача нескольких потоков (каналов) данных с меньшей скоростью (пропускной способностью) по одному каналу связи, с использованием специального устройства, называемого мультиплексором.

В настоящее время, для уплотнения канала связи, в основном используют:

* Временное мультиплексирование (Time Division Multiplexing, TDM)
* Частотное мультиплексирование (Frequency Division Multiplexing, FDM)
* Волновое мультиплексирование (Wave Division Multiplexing, WDM)
* Множественный доступ с кодовым разделением (CodeDivisionMultipleAccess, CDMA) - каждый канал имеет свой код наложение которого на групповой сигнал позволяет выделить информацию конкретного канала

### 9.Беспроводные каналы связи в КС

**Беспроводные компьютерные сети** — это технология, позволяющая создавать вычислительные [сети](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), полностью соответствующие стандартам для обычных проводных сетей (например, [Ethernet](https://ru.wikipedia.org/wiki/Ethernet)), без использования кабельной проводки. В качестве носителя информации в таких сетях выступают радиоволны СВЧ-диапазона.

Существует два основных направления применения беспроводных компьютерных сетей:

* Работа в замкнутом объеме (офис, выставочный зал и т. п.);
* Соединение удаленных [локальных сетей](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) (или удаленных сегментов локальной сети).

Для организации беспроводной сети в замкнутом пространстве применяются передатчики со всенаправленными антеннами. Стандарт [IEEE 802.11](https://ru.wikipedia.org/wiki/IEEE_802.11) определяет два режима работы сети — [Ad-hoc](https://ru.wikipedia.org/wiki/Ad-hoc) и [клиент-сервер](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B8%D0%B5%D0%BD%D1%82-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80). Режим Ad-hoc (иначе называемый «[точка-точка](https://ru.wikipedia.org/wiki/%D0%A2%D0%BE%D1%87%D0%BA%D0%B0-%D1%82%D0%BE%D1%87%D0%BA%D0%B0)») — это простая сеть, в которой связь между станциями (клиентами) устанавливается напрямую, без использования специальной [точки доступа](https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D1%81%D0%BF%D1%80%D0%BE%D0%B2%D0%BE%D0%B4%D0%BD%D0%B0%D1%8F_%D1%82%D0%BE%D1%87%D0%BA%D0%B0_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0). В режиме клиент-сервер беспроводная сеть состоит, как минимум, из одной точки доступа, подключенной к проводной сети, и некоторого набора беспроводных клиентских станций. Поскольку в большинстве сетей необходимо обеспечить доступ к файловым серверам, принтерам и другим устройствам, подключенным к проводной локальной сети, чаще всего используется режим клиент-сервер. Без подключения дополнительной антенны устойчивая связь для оборудования IEEE 802.11b достигается в среднем на следующих расстояниях: открытое пространство — 500 м, комната, разделенная перегородками из неметаллического материала — 100 м, офис из нескольких комнат — 30 м.

Для соединения удаленных локальных сетей (или удаленных сегментов локальной сети) используется оборудование с направленными [антеннами](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B5%D0%BD%D0%BD%D0%B0), что позволяет увеличить дальность связи до 20 км (а при использовании специальных усилителей и большой высоте размещения антенн — до 50 км). Причем в качестве подобного оборудования могут выступать и устройства [Wi-Fi](https://ru.wikipedia.org/wiki/Wi-Fi), нужно лишь добавить к ним специальные антенны (конечно, если это допускается конструкцией).

### 10.Манчестерский код передачи данных в КС

В локальных сетях до недавнего времени самым распространенным методом кодирования был так называемый *манчестерский код* (рис. 2.16, г). Он применяется в технологиях Ethernet и Token Ring.

В манчестерском коде для кодирования единиц и нулей используется перепад потенциала, то есть фронт импульса. При манчестерском кодировании каждый такт делится на две части. Информация кодируется перепадами потенциала, происходящими в середине каждого такта. Единица кодируется перепадом от низкого уровня сигнала к высокому, а ноль - обратным перепадом. В начале каждого такта может происходить служебный перепад сигнала, если нужно представить несколько единиц или нулей подряд. Так как сигнал изменяется по крайней мере один раз за такт передачи одного бита данных, то манчестерский код обладает хорошими самосинхронизирующими свойствами. Полоса пропускания манчестерского кода уже, чем у биполярного импульсного. У него также нет постоянной составляющей, а основная гармоника в худшем случае (при передаче последовательности единиц или нулей) имеет частоту N Гц, а в лучшем (при передаче чередующихся единиц и нулей) она равна N/2 Гц, как и у кодов AMI или NRZ. В среднем ширина полосы манчестерского кода в полтора раза уже, чем у биполярного импульсного кода, а основная гармоника колеблется вблизи значения 3N/4. Манчестерский код имеет еще одно преимущество перед биполярным импульсным кодом. В последнем для передачи данных используются три уровня сигнала, а в манчестерском - два.

### 11.Коммутация пакетов в КС

*Коммутация сообщений* производится путем передачи сообщения, содержащего заголовок и данные, по маршруту, определяемому узлами сети. В заголовке сообщения указывается адрес абонента *а,* — получателя сообщения. Сообщение, генерируемое отправителем — абонентом *а* принимается узлом *А* и хранится в памяти узла. Узел *А* обрабатывает заголовок сообщения и определяет маршрут передачи сообщения, ведущий к узлу *В.* Узел *В* принимает сообщение, размещая его в памяти, а по окончании приема обрабатывает заголовок и выводит сообщение из памяти на линию связи, ведущую к следующему узлу. Процесс приема, обработки и передачи сообщения повторяется последовательно всеми узлами на маршруте от абонента *щ* до абонента *а^* Значение С/г определяет время доставки данных при коммутации сообщений.

*Коммутация пакетов* производится путем разбивки сообщения на пакеты — элементы сообщения, снабженные заголовком, имеющие фиксированную максимальную длину, и последующей передачи пакетов по маршруту, определяемому узлами сети. Передача данных при коммутации пакетов происходит так же, как и при коммутации сообщений, но данные разделяются на последовательность пакетов 1, 2, ..., длина которых ограничена предельным значением, например 1024 бит.

Во-первых, способ коммутации каналов требует, чтобы все соединительные линии, из которых формируется канал, имели одинаковую пропускную способность.

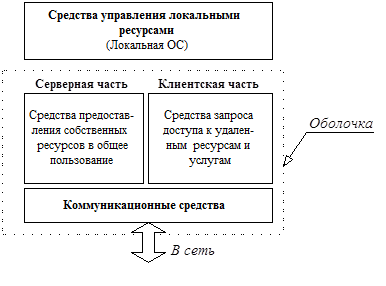
Во-вторых, представление данных пакетами создает наилучшие условия для мультиплексирования потоков данных — разделения времени работы канала для одновременной передачи нескольких потоков данных.

В-третьих, малая длина пакетов позволяет выделять для промежуточного хранения передаваемых данных меньшую емкость памяти, чем требуется для сообщений.

В-четвертых, пакеты, имея незначительную длину, в большей степени гарантированы от искажений, чем сообщения.

### 12.Структура сетевой операционной системы

Сетевая операционная система составляет основу любой вычислительной сети. Каждый компьютер в сети автономен, поэтому под сетевой операционной системой в широком смысле понимается совокупность операционных систем отдельных компьютеров, взаимодействующих с целью обмена сообщениями и разделения ресурсов по единым правилам – протоколам. В узком смысле сетевая ОС – это операционная система отдельного компьютера, обеспечивающая ему возможность работать в сети.



1.    Средства управления локальными ресурсами компьютера: функции распределения оперативной памяти между процессами, планирования и диспетчеризации процессов, управления процессорами, управления периферийными устройствами и другие функции управления ресурсами локальных ОС.

2.    Средства предоставления собственных ресурсов и услуг в общее пользование – серверная часть ОС (сервер). Эти средства обеспечивают, например, блокировку файлов и записей, ведение справочников имен сетевых ресурсов; обработку запросов удаленного доступа к собственной файловой системе и базе данных; управление очередями запросов удаленных пользователей к своим периферийным устройствам.

3.    Средства запроса доступа к удаленным ресурсам и услугам – клиентская часть ОС (редиректор). Эта часть выполняет распознавание и перенаправление в сеть запросов к удаленным ресурсам от приложений и пользователей. Клиентская часть также осуществляет прием ответов от серверов и преобразование их в локальный формат, так что для приложения выполнение локальных и удаленных запросов неразличимо.

4.    Коммуникационные средства ОС, с помощью которых происходит обмен сообщениями в сети. Эта часть обеспечивает адресацию и буферизацию сообщений, выбор маршрута передачи сообщения по сети, надежность передачи и т.п., т. е. является средством транспортировки сообщений.

### 13. Сеть Token Ring и ее возможности

**Token Ring** — технология [локальной вычислительной сети](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) (LAN) кольца с «маркерным доступом» — протокол локальной сети, который находится 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) (DLL) [модели OSI](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI). Он использует специальный трёхбайтовый фрейм, названный маркером, который перемещается вокруг кольца. Владение маркером предоставляет его обладателю право передавать информацию на носителе. Кадры кольцевой сети с маркерным доступом перемещаются в цикле.

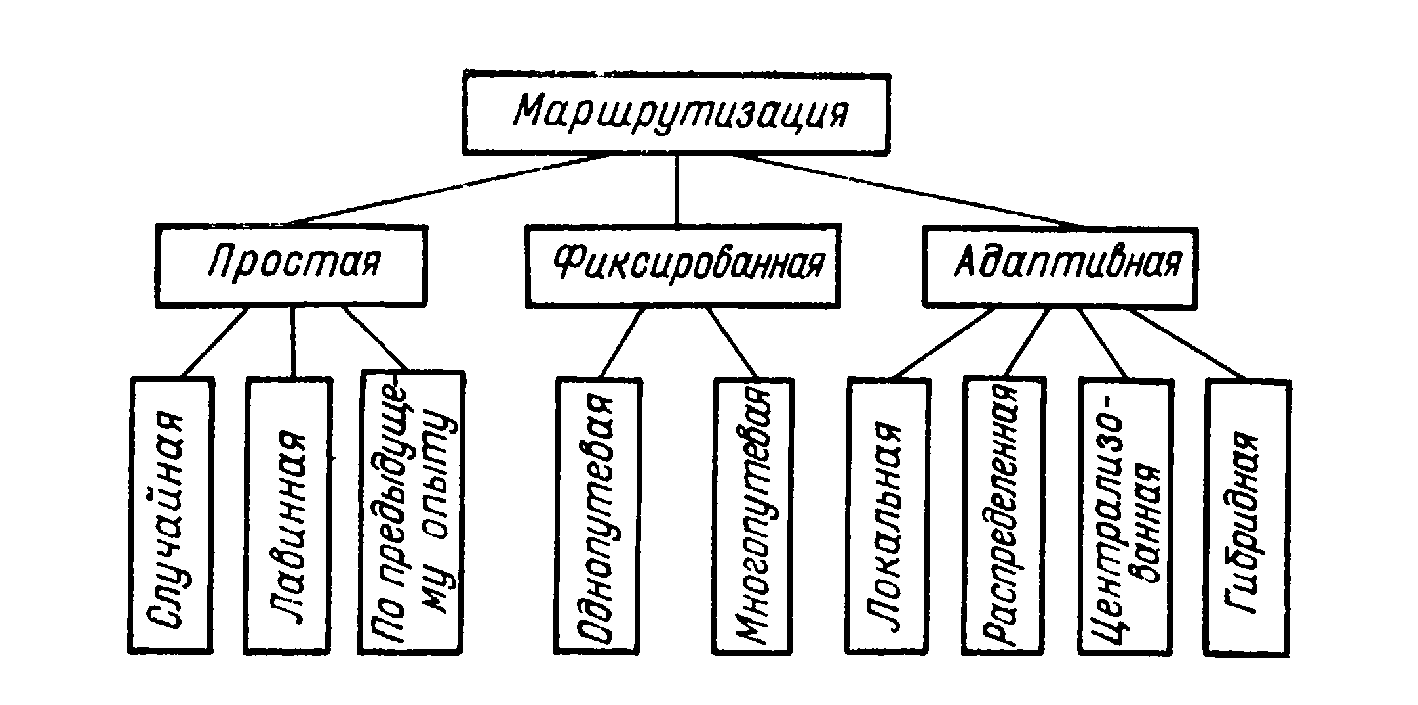
Token Ring и IEEE 802.5 являются главными примерами сетей с передачей маркера. Сети с передачей маркера перемещают по сети небольшой блок данных, называемый маркером. Владение этим маркером гарантирует право передачи. Если узел, принимающий маркер, не имеет информации для отправки, он просто переправляет маркер к следующей конечной станции. Каждая станция может удерживать маркер в течение определенного максимального времени (по умолчанию — 10 мс).

Данная технология предлагает вариант решения проблемы коллизий, которая возникает при работе локальной сети. В технологии Ethernet такие коллизии возникают при одновременной передаче информации несколькими рабочими станциями, находящимися в пределах одного [сегмента](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D0%B3%D0%BC%D0%B5%D0%BD%D1%82_%D1%81%D0%B5%D1%82%D0%B8), то есть использующих общий [физический канал](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%B7%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB) данных.

Если у станции, владеющей маркером, имеется информация для передачи, она захватывает маркер, изменяет у него один бит (в результате чего маркер превращается в последовательность «начало блока данных»), дополняет информацией, которую он хочет передать, и отсылает эту информацию к следующей станции кольцевой сети. Когда информационный блок циркулирует по кольцу, маркер в сети отсутствует (если только кольцо не обеспечивает «раннего освобождения маркера» — early token release), поэтому другие станции, желающие передать информацию, вынуждены ожидать. Следовательно, в сетях Token Ring не может быть коллизий. Если обеспечивается раннее высвобождение маркера, то новый маркер может быть выпущен после завершения передачи блока данных.

Информационный блок циркулирует по кольцу, пока не достигнет предполагаемой станции назначения, которая копирует информацию для дальнейшей обработки. Информационный блок продолжает циркулировать по кольцу; он окончательно удаляется после достижения станции, отославшей этот блок. Станция отправки может проверить вернувшийся блок, чтобы убедиться, что он был просмотрен и затем скопирован станцией назначения.

### 14.Алгоритмы маршрутизации пакетов в КС



*Простая маршрутизация* — способ маршрутизации, не изменяющийся при изменении топологии и состояния СПД.

*Случайная маршрутизация* — передача пакета из узла в любом, случайным образом выбранном направлении, кроме направления, по которому пакет поступил в узел. Пакет, совершая «блуждания» по сети, с конечной вероятностью когда-либо достигает адресата. Очевидно, что случайная маршрутизация неэффективна ни по времени доставки пакетов, ни по использованию пропускной способности сети.

*Лавинная маршрутизация* — передача пакета из узла во всех направлениях, кроме того, по которому поступил пакет. При этом, если узел связан с *п* другими узлами СПД, пакет передается в я—1 направлениях, т. е. размножается. Очевидно, что хотя бы одно направление обеспечит доставку пакета за минимальное время, т. е. лавинная маршрутизация гарантирует малое время доставки, однако это достигается за счет резкого ухудшения использования пропускной способности сети.

*Фиксированная маршрутизация* — способ выбора направления передачи по таблице маршрутизации, устанавливающей направление передачи для каждого узла назначения. Таблицы маршрутизации определяют кратчайшие пути от узлов к адресатам и вводятся в узлы связи.

*Адаптивная маршрутизация* — способ выбора направления передачи, учитывающий изменение состояния СПД. При адаптивной маршрутизации узлы СПД принимают решение о выборе маршрутов, реагируя на разного рода данные об изменении топологии и нагрузки.

*Локальная адаптивная маршрутизация* основана на использовании информации, имеющейся в отдельном узле СПД.

*Распределенная адаптивная маршрутизация* основана на использовании информации, получаемой от соседних узлов сети.

***Централизованная адаптивная маршрутизация* основана на использовании** информации, получаемой от центра маршрутизации.

***Гибридная адаптивная маршрутизация* основана на использовании таблиц,** периодически рассылаемых центром маршрутизации, в сочетании с анализом длины очередей в узлах.

### 15.Сеть FDDI и ее возможности

**FDDI** ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Fiber Distributed Data Interface* — Волоконно-оптический интерфейс передачи данных) — стандарт передачи данных в [локальной сети](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), протянутой на расстоянии до 200 [километров](https://ru.wikipedia.org/wiki/%D0%9A%D0%B8%D0%BB%D0%BE%D0%BC%D0%B5%D1%82%D1%80). Стандарт основан на [протоколе](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) [Token Ring](https://ru.wikipedia.org/wiki/Token_Ring). Кроме большой территории, сеть FDDI способна поддерживать несколько тысяч пользователей.

В качестве среды передачи данных в FDDI рекомендуется использовать [волоконно-оптический кабель](https://ru.wikipedia.org/wiki/%D0%92%D0%BE%D0%BB%D0%BE%D0%BA%D0%BE%D0%BD%D0%BD%D0%BE-%D0%BE%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C), однако можно использовать и медный кабель, в таком случае используется сокращение CDDI (Copper Distributed Data Interface). В качестве[топологии](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D1%82%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F) используется схема [двойного кольца](https://ru.wikipedia.org/wiki/%D0%94%D0%B2%D0%BE%D0%B9%D0%BD%D0%BE%D0%B5_%D0%BA%D0%BE%D0%BB%D1%8C%D1%86%D0%BE_(%D1%82%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D1%81%D0%B5%D1%82%D0%B8)), при этом данные в кольцах циркулируют в разных направлениях. Одно кольцо считается основным, по нему передаётся информация в обычном состоянии; второе — вспомогательным, по нему данные передаются в случае обрыва на первом кольце. Для контроля за состоянием кольца используется сетевой маркер, как и в технологии Token Ring.

Поскольку такое дублирование повышает надёжность системы, данный стандарт с успехом применяется в магистральных каналах связи.

### 16.Методы шифрования данных в КС

Для обеспечения секретности данных используются методы *криптографии* — преобразования данных из общепринятой формы в кодированную (шифрования) и обратного преобразования (дешифрования) на основе правил, известных только взаимодействующим пользователям. Криптография применяется для защиты

передаваемых данных, а также данных, хранимых на сменных томах — пакетах дисков, гибких дисках и лентах. Для защиты вычислительной сети от несанкционированного доступа применяется *идентификация пользователей* (сообщений), позволяющая

устанавливать конкретного пользователя, работающего за терминалом и отправляющего сообщения.

**Шифрование данных.** Шифрование данных производится по алгоритму, определяющему порядок преобразования исходного текста в шифрованный текст, а дешифрование — по алгоритму, реализующему обратное преобразование. К криптографическим средствам предъявляются требования сохранения секретности, даже когда известна сущность алгоритмов шифрования — дешифрования. Секретность обеспечивается введением в алгоритмы ключей — последовательностей символов. Зашифрованный текст превращается в исходный только в том случае, если в каждом из процессов использовался один и тот же ключ. Область значений ключа выбирается столь большой, что практически исключается возможность идентификации ключа путем перебора его значений.

**Идентификация пользователей.** Право доступа к определенным информационным

ресурсам — программам и наборам данных — и вычислительной сети в целом предоставляется ограниченному контингенту лиц, и система должна идентифицировать пользователей, работающих за терминалами. Идентификация пользователей чаще всего производится с помощью паролей. Пароль — совокупность символов, известных подключенному абоненту, вводится абонентом в начале сеанса взаимодействия с сетью. Сеть определяет подлинность пароля и тем самым пользователя. Для идентификации пользователей могут использоваться физические ключи, например, карточки с магнитной полоской, на которой записывается персональный идентификатор пользователя. Для уменьшения риска злоупотреблений карточки используются совместно с каким-либо другим способом идентификации пользователя, например с коротким паролем.

Для защиты средств идентификации пользователей от неправомочных вмешательств пароли передаются и сравниваются только в зашифрованном виде и таблицы паролей хранятся также в зашифрованном виде, что исключает возможность прочтения паролей без знания ключей.

### 17.Сеть Ethernet и ее возможности

**Ethernet**  — семейство технологий [пакетной](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D0%BA%D0%B5%D1%82_(%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D1%8B%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8)) передачи данных для [компьютерных сетей](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C).

Стандарты Ethernet определяют проводные соединения и электрические сигналы на [физическом уровне](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%B7%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D1%81%D0%BB%D0%BE%D0%B9), формат [кадров](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%B4%D1%80_(%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8)) и протоколы управления доступом к среде — 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) [модели OSI](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI). Ethernet в основном описывается стандартами [IEEE](https://ru.wikipedia.org/wiki/IEEE) [группы 802.3](https://ru.wikipedia.org/wiki/IEEE_802.3). Ethernet стал самой распространённой технологией [ЛВС](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) в середине [1990-х годов](https://ru.wikipedia.org/wiki/1990-%D0%B5), вытеснив такие устаревшие технологии, как [Arcnet](https://ru.wikipedia.org/wiki/Arcnet) и [Token ring](https://ru.wikipedia.org/wiki/Token_ring).

Название «Ethernet» (буквально «эфирная сеть») отражает первоначальный принцип работы этой технологии: всё, передаваемое одним узлом, одновременно принимается всеми остальными (то есть имеется некое сходство с [радиовещанием](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D0%B8%D0%BE%D0%B2%D0%B5%D1%89%D0%B0%D0%BD%D0%B8%D0%B5)). В настоящее время практически всегда подключение происходит через [коммутаторы (switch)](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%82%D0%BE%D1%80), так что кадры, отправляемые одним узлом, доходят лишь до адресата (исключение составляют передачи на [широковещательный адрес](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%80%D0%BE%D0%BA%D0%BE%D0%B2%D0%B5%D1%89%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B0%D0%B4%D1%80%D0%B5%D1%81)) — это повышает скорость работы и безопасность сети.

Преимущества использования витой пары по сравнению с коаксиальным кабелем:

* возможность работы в [дуплексном](https://ru.wikipedia.org/wiki/%D0%94%D1%83%D0%BF%D0%BB%D0%B5%D0%BA%D1%81_(%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8)) режиме;
* низкая стоимость кабеля витой пары;
* более высокая надёжность сетей: при использовании витой пары сеть строится по топологии «звезда», поэтому обрыв кабеля приводит лишь к нарушению связи между двумя объектами сети, соединёнными этим кабелем (при использовании коаксиального кабеля сеть строится по топологии «общая шина», для которой требуется наличие терминальных резисторов на концах кабеля, поэтому обрыв кабеля приводит к неисправности сегмента сети);
* уменьшен минимально допустимый радиус изгиба кабеля;
* большая помехоустойчивость из-за использования дифференциального сигнала;
* возможность питания по кабелю маломощных узлов, например IP-телефонов (стандарт [Power over Ethernet](https://ru.wikipedia.org/wiki/Power_over_Ethernet), PoE);
* гальваническая развязка трансформаторного типа. В условиях СНГ, где, как правило, отсутствует заземление компьютеров, применение коаксиального кабеля часто приводило к выходу из строя сетевых карт в результате электрического пробоя.

Причиной перехода на оптический кабель была необходимость увеличить длину сегмента без повторителей.

### 18.Метод доступа к физической среде в сети Token Ring

В сетях Token Ring 16 Мб/с используется  алгоритм доступа к кольцу, называемый алгоритмом *раннего освобождения маркера (Early Token Release).* В соответствии с ним станция передает маркер доступа следующей станции сразу же после окончания передачи последнего бита кадра, не дожидаясь возвращения по кольцу этого кадра с битом подтверждения приема. В этом случае пропускная способность кольца используется более эффективно и приближается к 80 % от номинальной.

Для различных видов сообщений передаваемым данным могут назначаться различные *приоритеты.*

Каждая станция имеет механизмы обнаружения и устранения неисправностей сети, возникающих в результате ошибок передачи или переходных явлений (например, при подключении и отключении станции).

Не все станции в кольце равны. Одна из станций обозначается как *активный монитор,*что означает дополнительную ответственность по управлению кольцом. Активный монитор осуществляет управление тайм-аутом в кольце, порождает новые маркеры (если необходимо), чтобы сохранить рабочее состояние, и генерирует диагностические кадры при определенных обстоятельствах. Активный монитор выбирается, когда кольцо инициализируется, и в этом качестве может выступить любая станция сети. Если монитор отказал по какой-либо причине, существует механизм, с помощью которого другие станции (резервные мониторы) могут договориться, какая из них будет новым активным монитором.

### 19.Метод доступа к физической среде в сети Ethernet

В сетях Ethernet используется метод доступа к среде передачи данных, называемый *методом коллективного доступа с опознаванием несущей и обнаружением коллизий (carrier-sense-multiply-access with collision detection, CSMA/CD)*.

Этот метод используется исключительно в сетях с общей шиной (к которым относятся и радиосети, породившие этот метод). Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Простота схемы подключения - это один из факторов, определивших успех стандарта Ethernet. Говорят, что кабель, к которому подключены все станции, работает в режиме *коллективного доступа (multiply-access,MA).*

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения. Затем кадр передается по кабелю. Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ. Адрес станции-источника также включен в исходный кадр, поэтому станция-получатель знает, кому нужно послать ответ.

Метод CSMA/CD определяет основные временные и логические соотношения, гарантирующие корректную работу всех станций в сети:

* Между двумя последовательно передаваемыми по общей шине кадрами информации должна выдерживаться пауза в 9.6 мкс; эта пауза нужна для приведения в исходное состояние сетевых адаптеров узлов, а также для предотвращения монопольного захвата среды передачи данных одной станцией.
* При обнаружении коллизии (условия ее обнаружения зависят от применяемой физической среды) станция выдает в среду специальную 32-х битную последовательность (jam-последовательность), усиливающую явление коллизии для более надежного распознавания ее всеми узлами сети.
* После обнаружения коллизии каждый узел, который передавал кадр и столкнулся с коллизией, после некоторой задержки пытается повторно передать свой кадр. Узел делает максимально 16 попыток передачи этого кадра информации, после чего отказывается от его передачи. Величина задержки выбирается как равномерно распределенное случайное число из интервала, длина которого экспоненциально увеличивается с каждой попыткой. Такой алгоритм выбора величины задержки снижает вероятность коллизий и уменьшает интенсивность выдачи кадров в сеть при ее высокой загрузке.

### 20.Скоростные версии сети Ethernet Fast Ethernet Gigabit Ethernet,10G Ethernet

*10-гигабитный Ethernet (Ethernet 10G, 10 Гбит/с)*

Новый стандарт 10-гигабитного Ethernet включает в себя семь стандартов физической среды для [LAN](https://ru.wikipedia.org/wiki/LAN), [MAN](https://ru.wikipedia.org/wiki/Metropolitan_area_network) и [WAN](https://ru.wikipedia.org/wiki/Wide_area_network). В настоящее время он описывается поправкой [IEEE 802.3ae](https://ru.wikipedia.org/w/index.php?title=IEEE_802.3ae&action=edit&redlink=1) и должен войти в следующую ревизию стандарта [IEEE 802.3](https://ru.wikipedia.org/wiki/IEEE_802.3).

* [**10GBASE-CX4**](https://ru.wikipedia.org/w/index.php?title=10GBASE-CX4&action=edit&redlink=1) — технология 10-гигабитного Ethernet для коротких расстояний (до 15 [метров](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D1%80)), используется медный кабель CX4 и коннекторы [InfiniBand](https://ru.wikipedia.org/wiki/InfiniBand).
* [**10GBASE-SR**](https://ru.wikipedia.org/w/index.php?title=10GBASE-SR&action=edit&redlink=1) — технология 10-гигабитного Ethernet для коротких расстояний (до 26 или 82 [метров](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D1%80), в зависимости от типа кабеля), используется многомодовое волокно. Он также поддерживает расстояния до 300 метров с использованием нового многомодового волокна (2000 МГц/км).
* [**10GBASE-LX4**](https://ru.wikipedia.org/w/index.php?title=10GBASE-LX4&action=edit&redlink=1) — использует [уплотнение по длине волны](https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B5%D0%BA%D1%82%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D1%83%D0%BF%D0%BB%D0%BE%D1%82%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2) для поддержки расстояний от 240 до 300 [метров](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D1%80) по многомодовому волокну. Также поддерживает расстояния до 10 [километров](https://ru.wikipedia.org/wiki/%D0%9A%D0%B8%D0%BB%D0%BE%D0%BC%D0%B5%D1%82%D1%80) при использовании одномодового волокна.
* [**10GBASE-LR**](https://ru.wikipedia.org/w/index.php?title=10GBASE-LR&action=edit&redlink=1) и [**10GBASE-ER**](https://ru.wikipedia.org/w/index.php?title=10GBASE-ER&action=edit&redlink=1) — эти стандарты поддерживают расстояния до 10 и 40 [километров](https://ru.wikipedia.org/wiki/%D0%9A%D0%B8%D0%BB%D0%BE%D0%BC%D0%B5%D1%82%D1%80) соответственно.
* [**10GBASE-SW**](https://ru.wikipedia.org/w/index.php?title=10GBASE-SW&action=edit&redlink=1), [**10GBASE-LW**](https://ru.wikipedia.org/w/index.php?title=10GBASE-LW&action=edit&redlink=1) и [**10GBASE-EW**](https://ru.wikipedia.org/w/index.php?title=10GBASE-EW&action=edit&redlink=1) — эти стандарты используют физический интерфейс, совместимый по скорости и формату данных с интерфейсом [OC-192](https://ru.wikipedia.org/w/index.php?title=OC-192&action=edit&redlink=1) / [STM-64](https://ru.wikipedia.org/w/index.php?title=STM-64&action=edit&redlink=1) [SONET](https://ru.wikipedia.org/wiki/SONET)/[SDH](https://ru.wikipedia.org/wiki/SDH). Они подобны стандартам [10GBASE-SR](https://ru.wikipedia.org/w/index.php?title=10GBASE-SR&action=edit&redlink=1), [10GBASE-LR](https://ru.wikipedia.org/w/index.php?title=10GBASE-LR&action=edit&redlink=1) и[10GBASE-ER](https://ru.wikipedia.org/w/index.php?title=10GBASE-ER&action=edit&redlink=1) соответственно, так как используют те же самые типы кабелей и расстояния передачи.
* [**10GBASE-T**](https://ru.wikipedia.org/w/index.php?title=10GBASE-T&action=edit&redlink=1), [IEEE 802.3an-2006](https://ru.wikipedia.org/w/index.php?title=IEEE_802.3an-2006&action=edit&redlink=1) — принят в июне 2006 года после 4 лет разработки. Использует витую пару категории 6 (максимальное расстояние 55 метров)[[16]](https://ru.wikipedia.org/wiki/Ethernet#cite_note-Olifer-16) и 6а (максимальное расстояние 100 метров)[[16]](https://ru.wikipedia.org/wiki/Ethernet#cite_note-Olifer-16).
* [**10GBASE-KR**](https://ru.wikipedia.org/w/index.php?title=10GBASE-KR&action=edit&redlink=1) — технология 10-гигабитного Ethernet для кросс-плат (backplane/midplane) модульных коммутаторов/маршрутизаторов и серверов (Modular/Blade).

Компания Harting заявила о создании первого в мире 10-гигабитного соединителя RJ-45, не требующего инструментов для монтажа — [HARTING RJ Industrial 10G](https://ru.wikipedia.org/w/index.php?title=%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D1%81%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D0%B8%D1%82%D0%B5%D0%BB%D0%B8_Harting&action=edit&redlink=1)[[17]](https://ru.wikipedia.org/wiki/Ethernet#cite_note-17)[[18]](https://ru.wikipedia.org/wiki/Ethernet#cite_note-18).

*Быстрый Ethernet (*[*Fast Ethernet*](https://ru.wikipedia.org/wiki/Fast_Ethernet)*, 100 Мбит/с)*

* [**100BASE-T**](https://ru.wikipedia.org/wiki/100BASE-T) — общий термин для обозначения стандартов, использующих в качестве среды передачи данных витую пару. Длина сегмента до 100 метров. Включает в себя стандарты [100BASE-TX](https://ru.wikipedia.org/wiki/100BASE-TX), [100BASE-T4](https://ru.wikipedia.org/wiki/100BASE-T4) и [100BASE-T2](https://ru.wikipedia.org/w/index.php?title=100BASE-T2&action=edit&redlink=1).
* [**100BASE-TX**](https://ru.wikipedia.org/wiki/100BASE-TX), [IEEE 802.3u](https://ru.wikipedia.org/w/index.php?title=IEEE_802.3u&action=edit&redlink=1) — развитие стандарта 10BASE-T для использования в сетях топологии «звезда». Задействована витая пара категории 5, фактически используются только две неэкранированные пары проводников, поддерживается дуплексная передача данных, расстояние до 100 м.
* [**100BASE-T4**](https://ru.wikipedia.org/wiki/100BASE-T4) — стандарт, использующий витую пару категории 3. Задействованы все четыре пары проводников, передача данных идёт в полудуплексе. Практически не используется.
* [**100BASE-T2**](https://ru.wikipedia.org/w/index.php?title=100BASE-T2&action=edit&redlink=1) — стандарт, использующий витую пару категории 3. Задействованы только две пары проводников. Поддерживается полный дуплекс, когда сигналы распространяются в противоположных направлениях по каждой паре. Скорость передачи в одном направлении — 50 Мбит/с. Практически не используется.
* [**100BASE-FX**](https://ru.wikipedia.org/w/index.php?title=100BASE-FX&action=edit&redlink=1) — стандарт, использующий многомодовое волокно. Максимальная длина сегмента 400 метров в полудуплексе (для гарантированного обнаружения коллизий) или 2 километра в полном дуплексе.
* [**100BASE-SX**](https://ru.wikipedia.org/w/index.php?title=100BASE-SX&action=edit&redlink=1) — стандарт, использующий многомодовое волокно. Максимальная длина ограничена только величиной затухания в оптическом кабеле и мощностью передатчиков, по разным материалам от 2 до 10 километров.
* [**100BASE-FX WDM**](https://ru.wikipedia.org/w/index.php?title=100BASE-FX_WDM&action=edit&redlink=1) — стандарт, использующий одномодовое волокно. Максимальная длина ограничена только величиной затухания в волоконно-оптическом кабеле и мощностью передатчиков. Интерфейсы бывают двух видов, отличаются длиной волны передатчика и маркируются либо цифрами (длина волны) либо одной латинской буквой A(1310) или B(1550). В паре могут работать только парные интерфейсы: с одной стороны передатчик на 1310 нм, а с другой — на 1550 нм.

*Гигабитный Ethernet (Gigabit Ethernet, 1 Гбит/с)*

* **1000BASE-T**, [IEEE 802.3ab](https://ru.wikipedia.org/w/index.php?title=IEEE_802.3ab&action=edit&redlink=1) — основной гигабитный стандарт, опубликованный в 1999 году[[4]](https://ru.wikipedia.org/wiki/Ethernet#cite_note-gbe-t-vs-tx2002-4), использует [витую пару](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D1%82%D0%B0%D1%8F_%D0%BF%D0%B0%D1%80%D0%B0) категории 5e. В передаче данных участвуют 4 пары, каждая пара используется одновременно для передачи по обоим направлениям со скоростью — 250 Мбит/с. Используется метод кодирования PAM5 (*5-level Phase Amplitude Modulation*, 5тиуровневая фазоамплитудная модуляция)[[5]](https://ru.wikipedia.org/wiki/Ethernet#cite_note-5) с 4 линиями (4D-PAM5) и 4-х мерной [Треллис-модуляцией](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B5%D0%BB%D0%BB%D0%B8%D1%81-%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8F%D1%86%D0%B8%D1%8F) (TCM)[[6]](https://ru.wikipedia.org/wiki/Ethernet#cite_note-6), частота основной гармоники 62,5 МГц. Расстояние до 100 метров.
* **1000BASE-TX** был создан Ассоциацией Телекоммуникационной Промышленности (англ. *Telecommunications Industry Association, TIA*) и опубликован в марте 2001 года как «Спецификация физического уровня дуплексного Ethernet 1000 Мб/с (1000BASE-TX) симметричных кабельных систем категории 6 (ANSI/TIA/EIA-854-2001)». Распространения не получил из-за высокой стоимости кабелей[[8]](https://ru.wikipedia.org/wiki/Ethernet#cite_note-8), фактически устарел. Стандарт разделяет принимаемые и посылаемые сигналы по парам (две пары передают данные, каждая на 500 Мбит/с и две пары принимают) что упрощало бы конструкцию приёмопередающих устройств. Ещё одним существенным отличием 1000BASE-TX являлось отсутствие схемы цифровой компенсации наводок и возвратных помех, в результате чего сложность, уровень энергопотребления и цена реализаций должна становится ниже, чем у стандарта 1000BASE-T. Для работы технологии требуется кабельная система 6 категории.
* [**1000BASE-X**](https://ru.wikipedia.org/w/index.php?title=1000BASE-X&action=edit&redlink=1) — общий термин для обозначения стандартов со сменными приёмопередатчиками в форм-факторах [GBIC](https://ru.wikipedia.org/wiki/GBIC) или [SFP](https://ru.wikipedia.org/wiki/SFP).
* [**1000BASE-SX**](https://ru.wikipedia.org/w/index.php?title=1000BASE-SX&action=edit&redlink=1), [IEEE 802.3z](https://ru.wikipedia.org/w/index.php?title=IEEE_802.3z&action=edit&redlink=1) — стандарт, использующий многомодовое волокно в первом окне прозрачности с длиной волны равной 850 нм. Дальность прохождения сигнала составляет до 550 метров.
* [**1000BASE-LX**](https://ru.wikipedia.org/w/index.php?title=1000BASE-LX&action=edit&redlink=1), [IEEE 802.3z](https://ru.wikipedia.org/w/index.php?title=IEEE_802.3z&action=edit&redlink=1) — стандарт, использующий одномодовое или многомодовое оптическое волокно во втором окне прозрачности с длиной волны равной 1310 нм. Дальность прохождения сигнала зависит только от типа используемых приемопередатчиков и, как правило, составляет для одномодового оптического волокна до 5 км и для многомодового оптического волокна до 550 метров.
* [**1000BASE-CX**](https://ru.wikipedia.org/w/index.php?title=1000BASE-CX&action=edit&redlink=1) — стандарт для коротких расстояний (до 25 метров), использующий [экранированную витую пару](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D1%82%D0%B0%D1%8F_%D0%BF%D0%B0%D1%80%D0%B0), используются 2 пары из 4. Заменён стандартом 1000BASE-T и сейчас не используется.
* [**1000BASE-LH**](https://ru.wikipedia.org/w/index.php?title=1000BASE-LH&action=edit&redlink=1) (Long Haul) — стандарт, использующий одномодовое волокно. Дальность прохождения сигнала без повторителя до 100 километров[[10]](https://ru.wikipedia.org/wiki/Ethernet#cite_note-10).

### 21.Сеть Gigabit Ethernet и ее возможности

Вопрос «Gigabit Ethernet - это Ethernet или нет?» отнюдь не праздный, и, хотя Gigabit Ethernet Alliance отвечает на него утвердительно на том основании, что эта технология использует тот же формат кадров, тот же метод доступа к среде передачи CSMA/CD, те же механизмы контроля потоков и те же управляющие объекты, все же Gigabit Ethernet отличается от Fast Ethernet больше, чем Fast Ethernet от Ethernet. (К тому же, например, Hewlett-Packard полагает, что он имеет больше сходства со 100VG-AnyLAN, чем с Fast Ethernet.) В частности, если для Ethernet было характерно разнообразие поддерживаемых сред передачи, что давало повод говорить о том, что он может работать хоть по колючей проволоке, то в Gigabit Ethernet волоконно-оптические кабели становятся доминирующей средой передачи (это, конечно, далеко не единственное отличие, но с остальными мы подробнее познакомимся ниже). Кроме того, Gigabit Ethernet ставит несравнимо более сложные технические задачи и предъявляет гораздо более высокие требования к качеству проводки. Иными словами, он гораздо менее универсален, чем его предшественники.

Основные трудности при использовании Gigabit Ethernet связаны с возникновением дифференциальной задержки сигналов (differential mode delay, DMD) в многомодовых волоконных кабелях. Эта задержка появляется при использовании некоторых комбинаций многомодового волокна и лазерных диодов, применяемых для ускорения передачи данных по волоконному кабелю. В результате возникают нарушения синхронизации (своего рода дрожание) сигнала, ограничивающие максимальное расстояние, на которое могут передаваться данные по Gigabit Ethernet.

Компания Cisco Systems намерена решить вопросы физического уровня путем замены в своих недавно анонсированных аппаратных системах преобразователей гигабитного интерфейса. Таким образом, для настройки аппаратуры на спецификации окончательного стандарта не потребуется вносить никаких внутренних изменений. «В худшем случае изменения коснутся только реализации физического уровня, - заявляет Джеф Моссман, системный инженер Cisco. - Для этого будет достаточно замены конвертера гигабитного интерфейса».

Спецификация Gigabit Ethernet изначально предусматривала три среды передачи: одномодовый и многомодовый оптический кабель с длинноволновыми лазерами 1000BaseLX для длинных магистралей для зданий и комплексов зданий, многомодовый оптический кабель с коротковолновыми лазерами 1000BaseSX для недорогих коротких магистралей, симметричный экранированный короткий 150-омный медный кабель 1000BaseCX для межсоединения оборудования в аппаратных и серверных.

### 22.Оценка производительности КС

Потенциально высокая производительность - это одно из основных свойств распределенных систем, к которым относятся компьютерные сети. Это свойство обеспечивается возможностью распараллеливания работ между несколькими компьютерами сети. К сожалению, эту возможность не всегда удается реализовать. Существует несколько основных характеристик производительности сети:

* время реакции;
* пропускная способность;
* задержка передачи и вариация задержки передачи.

*Время реакции* сети является интегральной характеристикой производительности сети с точки зрения пользователя. Именно эту характеристику имеет в виду пользователь, когда говорит: «Сегодня сеть работает медленно».

В общем случае время реакции определяется как интервал времени между возникновением запроса пользователя к какой-либо сетевой службе и получением ответа на этот запрос.

Очевидно, что значение этого показателя зависит от типа службы, к которой обращается пользователь, от того, какой пользователь и к какому серверу обращается, а также от текущего состояния элементов сети - загруженности сегментов, коммутаторов и маршрутизаторов, через которые проходит запрос, загруженности сервера и т. п.

Поэтому имеет смысл использовать также и средневзвешенную оценку времени реакции сети, усредняя этот показатель по пользователям, серверам и времени дня (от которого в значительной степени зависит загрузка сети).

*Пропускная способность* отражает объем данных, переданных сетью или ее частью в единицу времени. Пропускная способность уже не является пользовательской характеристикой, так как она говорит о скорости выполнения внутренних операций сети - передачи пакетов данных между узлами сети через различные коммуникационные устройства. Зато она непосредственно характеризует качество выполнения основной функции сети - транспортировки сообщений - и поэтому чаще используется при анализе производительности сети, чем время реакции. Пропускная способность измеряется либо в битах в секунду, либо в пакетах в секунду. Пропускная способность может быть мгновенной, максимальной и средней.

*Средняя пропускная способность* вычисляется путем деления общего объема переданных данных на время их передачи, причем выбирается достаточно длительный промежуток времени - час, день или неделя.

*Мгновенная пропускная способность* отличается от средней тем, что для усреднения выбирается очень маленький промежуток времени - например, 10 мс или 1 с.

*Максимальная пропускная способность* - это наибольшая мгновенная пропускная способность, зафиксированная в течение периода наблюдения.

### 23.Сеть 10 Gigabit Ethernet,ее достоинства и недостатки

Протоколы 10 GigaBit Ethernet получают все большее распространие в локальных сетях передачи данных. По опубликованным данным, в 44% сетей скорости 10 Гбит/с потребуются уже в ближайшие 5 лет, в основном, в магистралях и хранилищах данных.

Cтандарт на приложения 10 GigaBit Ethernet по оптическому волокну IEEE 802.3ae (10GBASE-F) был принят в 2002 г. Тогда же были опубликованы стандартные спецификации на соответствующие волоконно-оптические кабельные тракты. Наиболее экономичной реализацией 10 GigaBit Ethernet является протокол 10GBASE-SR, т. е. комбиниция лазерного светоизлучателя VCSEL (Vertical cavity surface emitting laser ) и многомодового волокна класса ОМ3, оптимизированного для работы с таким лазером.

Следующим этапом будет принятие стандарта 10 GigaBit Ethernet по витой паре IEEE 802.3an (10GBASE-T). Он послужит основой для реализации высокоскоростных соединений серверов друг с другом и с рабочими местами. Принятие стандарта 10GBASE-T планируется на 2006 г.

Потребность в пропускной способности кабельных каналов постоянно растет, к тому же сети 10 GigaBit Ethernet имеют экономические преимущества перед менее скоростными решениями. Поэтому уже сегодня приходится их учитывать при планировании новых или модернизации существующих кабельных сетей. AMP NETCONNECT предлагает полный набор волоконно-оптических и медных кабельных решений для сетей 10 GigaBit Ethernet.

### 24.Составные сети,пример составной сети

Internet Две или более сети, в которых используются различные сетевые протоколы, соединенные с помощью маршрутизаторов (router). Пользователи составной сети имеют доступ к ресурсам всех входящих в нее сетей.

Практически все сети (пожалуй, кроме самых небольших, состоящих из нескольких компьютеров) являются сегодня составными, т. е. состоящими из нескольких сетей, каждая из которых может работать на основе собственной технологии канального уровня (хотя это и не обязательно). Такое положение дел складывается по разным причинам: историческим - общая сеть создавалась постепенно, объединяя все большее число изолированных до этого сетей; техническим - разделенной на части сетью легче управлять и т. п. С развитием Internet количество сетей, не относящихся к составным, резко уменьшилось. Даже сети небольших офисов или домашние сети все чаще становятся постоянными или временными (на время подключения по телефонной сети) членами этой самой большой в мире составной сети. В данном уроке рассматриваются принципы и средства, с помощью которых составную сеть можно превратить из набора разрозненных сетей в единое целое.

### 25.Полоса пропускания и пропускная способность канала связи

Пропускная способность — метрическая характеристика, показывающая соотношение предельного количества проходящих единиц (информации, предметов, объёма) в единицу времени через канал, систему, узел.

В информатике определение пропускной способности обычно применяется к каналу связи и определяется максимальным количеством переданной или полученной информации за единицу времени.  
Пропускная способность — один из важнейших с точки зрения пользователей факторов. Она оценивается количеством данных, которые сеть в пределе может передать за единицу времени от одного подсоединенного к ней устройства к другому.

**Пропускная способность канала**

Наибольшая возможная в данном канале скорость передачи информации называется его пропускной способностью. Пропускная способность канала есть скорость передачи информации при использовании «наилучших» (оптимальных) для данного канала источника, кодера и декодера, поэтому она характеризует только канал.

Номинальная скорость — битовая скорость передачи данных без различия служебных и пользовательских данных.  
Эффективная скорость — скорость передачи пользовательских данных (нагрузки). Этот параметр зависит от соотношения накладных расходов и полезных данных.

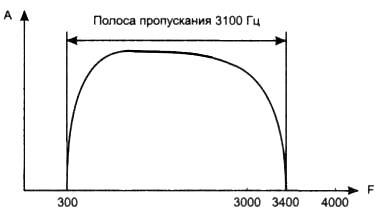
**Пропускная способность дискретного (цифрового) канала без помех**

*C* = log *m* × Vт,

где *m* — основание кода сигнала, используемого в канале. [Скорость передачи информации](https://ru.wikipedia.org/wiki/%D0%A1%D0%BA%D0%BE%D1%80%D0%BE%D1%81%D1%82%D1%8C_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) в дискретном канале без шумов (идеальном канале) равна его пропускной способности, когда символы в канале независимы, а все *m* символов алфавита равновероятны (используются одинаково часто). Vт - символьная скорость передачи.

### 26.Модуляция при передаче аналоговых и дискретных сигналов

При передаче дискретной информации посредством модуляции единицы и нули кодируются изменением амплитуды, частоты или фазы несущего синусоидального сигнала. В случае, когда модулированные сигналы передают дискретную информацию, вместо термина «модуляция» иногда используется термин «манипуляция»: амплитудная манипуляция (Amplitude Shift Keying, ASK), частотная манипуляция (Frequency Shift Keying, FSK), фазовая манипуляция (Phase Shift Keying, PSK). Пожалуй, самый известный пример применения модуляции при передаче дискретной информации — это передача компьютерных данных по телефонным каналам. Типичная амплитудно-частотная характеристика стандартного абонентского канала, называемого также каналом тональной частоты, представлена на рис. 1. Этот составной канал проходит через коммутаторы телефонной сети и соединяет телефоны абонентов. Канал тональной частоты передает частоты в диапазоне от 300 до 3400 Гц, таким образом, его полоса пропускания равна 3100 Гц. Такая узкая полоса пропускания вполне достаточна для качественной передачи голоса, однако она недостаточно широка для передачи компьютерных данных в виде прямоугольных импульсов. Решение проблемы было найдено благодаря аналоговой модуляции. Устройство, которое выполняет функцию модуляции несущей синусоиды на передающей стороне и обратную функцию демодуляции на приемной стороне, носит названце модема (модулятор-демодулятор).



При амплитудной модуляции для логической единицы выбирается один уровень амплитуды синусоиды несущей частоты, а для логического нуля — другой (рис. 2, б). Этот способ редко используется в чистом виде на практике из-за низкой помехоустойчивости, но часто применяется в сочетании с другим видом модуляции — фазовой модуляцией.

### 27.Методы кодирования сигналов в сети и их сравнительный анализ

Форматы кодов:

Каждый бит кодового слова передается или записывается с помощью дискретных сигналов, например, импульсов. Способ представления исходного кода определенными сигналами определяется форматом кода. Известно большое количество форматов, каждый из которых имеет свои достоинства и недостатки и предназначен для использования в определенной аппаратуре.

1. Формат БВН (без возвращения к нулю) естественным образом соответствует режиму работы логических схем. Единичный бит передается в пределах такта уровень не меняется. Положительный перепад означает переход из 0 к 1 в исходном коде, отрицательный — от 1 к 0. Отсутствие перепадов показывает, что значения предыдущего и последующего битов равны. Для декодирования кодов в формате БВН необходимы тактовые импульсы, так как в его спектре не содержится тактовая частота. Соответствующий коду формата БВН сигнал содержит низкочастотные компоненты (при передаче длинных серий нулей или единиц перепады не возникают).
2. Формат БВН-1 (без возвращения к нулю с перепадом при передаче 1) является разновидностью формата БВН. В отличие от последнего в БВН-1 уровень не передает данные, так как и положительные и отрицательные перепады соответствуют единичным битам. Перепады сигнала формируются при передаче 1. При передаче 0 уровень не меняется. Для декодирования требуются тактовые импульсы.
3. Формат БВН −0 (без возвращения к нулю с перепадом при передаче 0) является дополнительным к БВН-1 (перепады соответствуют нулевым битам исходного кода). В многодорожечных системах записи цифровых сигналов вместе с кодом в формате БВН надо записывать тактовые импульсы. Возможным вариантом является запись двух дополнительных сигналов, соответствующих кодам в форматах БВН-1 и БВН-0. В одном из двух сигналов перепады происходят в каждом такте, что позволяет получить импульсы тактовой частоты.
4. Формат ВН (с возвращением к нулю) требует передачи импульса, занимающего только часть тактового интервала (например, половину), при одиночном бите. При нулевом бите импульс не формируется.
5. Формат ВН-П (с активной паузой) означает передачу импульса положительной полярности при единичном бите и отрицательной — при нулевом бите. Сигнал этого формата имеет в спектре компоненты тактовой частоты. Он применяется в ряде случаев для передачи данных по линиям связи.
6. Формат ДФ-0 (двухфазный со скачком фазы при передаче 0) соответствует способу представления, при котором перепады формируются в начале каждого такта. При единичных битах сигнал в этом формате меняется с тактовой частотой, то есть в середине каждого такта происходит перепад уровня. При передаче нулевого бита перепад в середине такта не формируется, то есть имеет место скачок фазы. Код в данном формате обладает возможностью самосинхронизации и не требует передачи тактовых сигналов.

### 28.Сетевые устройства: повторители, мосты, коммутаторы, маршрутизаторы, шлюзы

Повторитель (репи́тер, от англ. repeater) — сетевое оборудование, предназначенное для увеличения расстояния сетевого соединения путём повторения электрического сигнала «один в один». Бывают однопортовые повторители и многопортовые. В терминах модели OSI работает на физическом уровне. Одной из первых задач, которая стоит перед любой технологией транспортировки данных, является возможность их передачи на максимально большое расстояние. Физическая среда накладывает на этот процесс своё ограничение — рано или поздно мощность сигнала падает, и приём становится невозможным. Но ещё большее значение имеет то, что искажается «форма сигнала» — закономерность, в соответствии с которой мгновенное значение уровня сигнала изменяется во времени. Это происходит в результате того, что провода, по которым передаётся сигнал, имеют собственную ёмкость и индуктивность. Электрические и магнитные поля одного проводника наводят ЭДС в других проводниках (длинная линия).

Сетевой мост, бридж (с англ. bridge) — сетевое устройство второго уровня модели OSI, предназначенное для объединения сегментов (подсети) компьютерной сети в единую сеть.

Сетевой мост работает на канальном уровне сетевой модели OSI, при получении кадра из сети, сверяет MAC-адрес последнего и если он не принадлежит данной подсети передаёт (транслирует) кадр дальше в тот сегмент, которому предназначался данный кадр. Если кадр принадлежит данной подсети, мост ничего не делает.

Сетевой коммутатор (жарг. свич от англ. switch — переключатель) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы (3 уровень OSI).

Маршрутиза́тор или ро́утер (транслитерация английского слова)) — специализированный сетевой компьютер, имеющий два или более сетевых интерфейса[2] и пересылающий пакеты данных между различными сегментами сети. Маршрутизатор может связывать разнородные сети различных архитектур. Для принятия решений о пересылке пакетов используется информация о топологии сети и определённые правила, заданные администратором.

Сетевой шлюз (англ. gateway) — аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы (например, локальной и глобальной).

### 29.Дейтаграммный и виртуальный способы передачи пакетов и их сравнительный анализ

***Дейтаграммный способ передачи*** данных основан на том, что все передаваемые пакеты обрабатываются независимо друг от друга, пакет за пакетом. Принадлежность пакета к определенному *потоку* между двумя конечными узлами и двумя приложениями, работающими на этих узлах, никак не учитывается.

Выбор следующего узла — например, коммутатора *Ethernet* или маршрутизатора *IP*/*IPX* — происходит только на основании адреса узла назначения, содержащегося в заголовке пакета. Решение о том, какому узлу передать пришедший пакет, принимается на основе таблицы, содержащей набор адресов назначения и адресную информацию, однозначно определяющую следующий (транзитный или конечный) узел. Такие таблицы имеют разные названия — например, для сетей*Ethernet* они обычно называются таблицей продвижения (forwarding *table*), а для сетевых протоколов, таких как *IP* и *IPX*, — таблицами маршрутизации (*routing table*). Далее для простоты будем пользоваться термином "*таблица* маршрутизации" в качестве обобщенного названия такого рода таблиц, используемых для дейтаграммной передачи на основании только адреса назначения конечного узла.

Механизм ***виртуальных каналов*** ( *virtual circuit* или *virtual channel* ) создает в сети устойчивые *пути* следования трафика через *сеть с коммутацией пакетов*. Этот механизм учитывает существование в сети *потоков* данных.

Если целью является прокладка для всех пакетов *потока* единого *пути* через *сеть*, то необходимым (но не всегда единственным) признаком такого *потока* должно быть наличие для всех его пакетов общих точек входа и выхода из сети. Именно для передачи таких *потоков* в сети создаются *виртуальные каналы*.

*Сеть* только обеспечивает возможность передачи трафика вдоль *виртуального канала*, а какие именно *потоки* будут передаваться по этим каналам, решают сами *конечные* узлы. Узел может использовать один и тот же *виртуальный канал* для передачи всех *потоков*, которые имеют общие с данным *виртуальным каналом* *конечные* точки, или же только части из них. Например, для *потока* реального времени можно использовать один *виртуальный канал*, а для трафика электронной почты — другой. В последнем случае разные *виртуальные каналы* будут предъявлять разные требования к качеству обслуживания, и удовлетворить их будет проще, чем в том случае, когда по одному *виртуальному каналу* передается трафик с разными требованиями к параметрам QoS.

### 30.Выбор размера и структуры сети

Под размером сети в данном случае понимается как количество объединяемых в *сеть* компьютеров, так и расстояния между ними. Надо четко представлять себе, сколько компьютеров (минимально и максимально) нуждается в подключении к сети. При этом необходимо оставлять возможность для дальнейшего роста количества компьютеров в сети, хотя бы процентов на 20–50.

Кстати, совсем не обязательно раз и навсегда включать в *сеть* все компьютеры предприятия. Иногда имеет смысл оставить некоторые из них автономными, например, из соображений безопасности информации на их дисках. Количество подключенных к сети компьютеров сильно влияет как на *производительность*, так и на сложность ее обслуживания. Оно также определяет *стоимость* требуемых программных средств, поэтому просчеты могут иметь довольно серьезные последствия.

Требуемая *длина линий связи* сети также играет не малую роль в проектировании сети. Например, если расстояния очень большие, может понадобиться использование дорогого оборудования. К тому же с увеличением расстояния резко возрастает*значимость* защиты линий связи от внешних электромагнитных помех. От расстояния зависит и *скорость передачи*информации *по* сети (выбор между *Ethernet* и *Fast* *Ethernet*). Целесообразно при выборе расстояний закладывать небольшой запас (хотя бы процентов 10) для учета непредвиденных обстоятельств. Преодолеть ограничения *по* длине иногда можно путем выбора *структуры сети*, разбиения ее на отдельные части.

Под *структурой сети* понимается способ разделения сети на части (*сегменты*), а также способ соединения этих сегментов между собой. *Сеть* предприятия может включать в себя рабочие группы компьютеров, сети подразделений, опорные сети, средства связи с другими сетями. Для объединения частей сети могут использоваться репитеры, репитерные *концентраторы*, коммутаторы, мосты и маршрутизаторы. Причем в ряде случаев *стоимость* этого объединительного оборудования может даже превысить *стоимость* компьютеров, сетевых адаптеров и кабеля, поэтому выбор *структуры сети* исключительно важен.

В идеале *структура сети* должна соответствовать структуре здания или комплекса зданий предприятия. Рабочие места группы сотрудников, занимающихся одной задачей (например, бухгалтерия, отдел продаж, инженерная *группа*), должны размещаться в одной или рядом расположенных комнатах. Тогда можно компьютеры этих сотрудников объединить в один сегмент, в единую рабочую группу и установить вблизи их комнат *сервер*, с которым они будут работать, а также концентратор или *коммутатор*, связывающий все их машины. Точно так же рабочие места сотрудников *подразделения*, занимающихся комплексом близких задач, лучше расположить на одном этаже здания, что существенно упростит их*объединение* в сегмент и дальнейшее его *администрирование*. На этом же этаже удобно расположить коммутаторы, маршрутизаторы и серверы, с которыми работает данное подразделение.

Как и в других случаях, при выборе *структуры* разумно оставлять возможности для дальнейшего развития сети. Например, лучше приобретать коммутаторы или маршрутизаторы с количеством портов, несколько большим, чем требуется в настоящий момент (хотя бы на 10—20 процентов). Это позволит при необходимости легко включить в *сеть* один или несколько сегментов. Ведь любое предприятие всегда стремится к росту (порой совершенно напрасно), и этот рост не должен каждый раз приводить к необходимости проектировать *сеть* предприятия заново.

### 31.Беспроводные компьютерные сети,их достоинства и недостатки

Беспроводные локальные сети Wi-Fi позволят повысить мобильность сотрудников в офисных или производственных помещениях, избавиться от кучи проводов в офисе или дома, вдобавок исключив затраты на монтаж и обслуживание проводной сети.  
Wi-Fi имеет смысл использовать в компаниях с небольшим количеством рабочих мест или при наличии большого количества беспроводных устройств (ноутбуков, нетбуков, коммуникаторов и т. д.). Чаще всего используются оба типа сетей одновременно: проводные сети и беспроводные сети Wi-Fi.

Простота и скорость развертывания сети;

Низкая стоимость развертывания;

Отсутствие проводов на рабочем месте (хотя бы части проводов).

Скорость передачи делится между всеми устройствами Wi-Fi в пределах обслуживания их одной и той же точкой доступа. Это значит, что если точка доступа предоставляет скорость передачи данных 300 мбит/с и к ней будет одновременно подключено, например 5 ноутбуков, то скорость передачи данных для каждого ноутбука составит 300 / 5 = 60 мбит/с. А в реальности и того меньше, поскольку объем передаваемой служебной информации может достигать 30-40%. В итоге скорость передачи составляет около 36 мбит/с на устройство;

Влияние окружающей среды (деревья, стены зданий);

Сравнительно низкая надежность;

Низкая устойчивость к взлому при неправильной настройке.

Минусы частично можно закрыть более качественным оборудованием и добавлением в состав беспроводной сети большего количества точек доступа Wi-Fi.

По моему скромному мнению, в большинстве случаев, для бизнеса предпочтительно использовать структурированные кабельные системы (СКС) - они дадут Вам большую надежность, отличную пропускную способность и гарантию защиты от простоев. Беспроводные сети на предприятии следует использовать там, где этого требует специфика бизнеса, например, большие складские площади с небольшим количеством используемого компьютерного оборудования. В любом случае, необходимо тщательно взвесить все за и против перед началом [построения локальной сети компании](http://www.it-lines.ru/services/s-business/proektirovaninie-montazh-nastroika-localnoy-seti).

Для домашней сети из 2-3 ноутбуков, компьютера и пары любых гаджетов беспроводная сеть (Wi-Fi) будет идеальным вариантом. Не забывайте про настройку защиты точки доступа в целях предотвращения кражи Ваших личных данных и интернет трафика.

### 32.Протокол Telnet

TELNET (англ.  TErminaL NETwork) — сетевой протокол для реализации текстового интерфейса по сети (в современной форме — при помощи транспорта TCP). Название «telnet» имеют также некоторые утилиты, реализующие клиентскую часть протокола. Современный стандарт протокола описан в RFC 854.

Выполняет функции протокола прикладного уровня модели OSI.

Назначение протокола TELNET в предоставлении достаточно общего, двунаправленного, восьмибитного байт-ориентированного средства связи. Его основная задача заключается в том, чтобы позволить терминальным устройствам и терминальным процессам взаимодействовать друг с другом. Предполагается, что этот протокол может быть использован для связи вида терминал-терминал («связывание») или для связи процесс-процесс («распределенные вычисления»).

Исторически Telnet служил для удалённого доступа к интерфейсу командной строки операционных систем. Теоретически, даже обе стороны протокола могут являться не только людьми, но и программами.

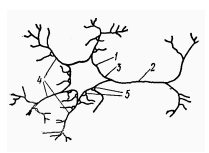
Иногда клиенты telnet используются для доступа к другим протоколам на основе транспорта TCP,

Протокол telnet используется в управляющем соединении FTP.

В протоколе не предусмотрено использование ни шифрования, ни проверки подлинности данных. Поэтому он уязвим для любого вида атак, к которым уязвим его транспорт, то есть протокол TCP.

Каждая команда TELNET является многобайтовой последовательностью, начинающейся с кода \377 (десятичное: 255) «Interpret as Command» (IAC) и кода команды.

### 33.Схема нейрона и его модель

Нервные клетки, или нейроны, представляют собой особый вид клеток в живых организмах, обладающих электрической активностью, основное назначение которых заключается в оперативном управлении организмом. Схематическое изображение нейрона приведено на рисунке.

Нейрон имеет тело (сому) 1, дерево входов (дендриты) 4 и выходов (аксон и его окончания) 2. Сома, как правило, имеет поперечный размер в несколько десятков микрон. Длина дендритов может достигать 1 мм, дендриты сильно ветвятся, пронизывая сравнительно большое пространство в окрестности нейрона. Длина аксона может достигать сотен миллиметров. Начальный сегмент аксона 3, прилегающий к телу клетки, утолщен. Иногда этот сегмент называют аксонным холмиком. По мере удаления от клетки он постепенно сужается и на расстоянии нескольких десятков микрон на нем появляется миэлиновая оболочка, имеющая высокое электрическое сопротивление. На соме и на дендритах располагаются окончания (коллатерали) аксонов, идущих от других нервных клеток. Каждое такое окончание J имеет вид утолщения, называемого синаптической бляшкой, или синапсом. Поперечные размеры синапса, как правило, не превышают нескольких микрон, чаще всего эти размеры составляют около 1 мкм.

Входные сигналы дендритного дерева (постсинаптические потенциалы) взвешиваются и суммируются на пути к аксонному холмику, где генерируется выходной импульс (спайк) или пачка импульсов. Его наличие (или интенсивность), следовательно, является функцией взвешенной суммы входных сигналов. Выходной сигнал проходит по ветвям аксона и достигает синапсов, которые соединяют аксоны с дендритными деревьями других нейронов. Через синапсы сигнал трансформируется в новый входной сигнал для смежных нейронов. Этот входной сигнал может быть положительным и отрицательным (возбуждающим или тормозящим) в зависимости от вида синапсов. Величина входного сигнала, генерируемого синапсом, может быть различной даже при одинаковой величине сигнала, приходящего в синапс. Эти различия определяются эффективностью или весом синапса. Синаптический вес может изменяться в процессе функционирования синапса. Многие ученые считают такое изменение нейрофизиологическим коррелятом (следом) памяти. При этом роль механизмов молекулярной памяти заключается в долговременном закреплении этих следов.

Нейроны можно разбить на три большие группы: рецепторные, промежуточные и эффекторные. Рецепторные нейроны обеспечивают ввод в мозг сенсорной информации. Они трансформируют сигналы, поступающие на органы чувств (оптические сигналы в сетчатке глаза, акустические в ушной улитке или обонятельные в хеморецепторах носа), в электрическую импульсацию своих аксонов. Эффекторные нейроны передают приходящие на них сигналы исполнительным органам. На конце их аксонов имеются специальные синаптические соединения с исполнительными органами, например мышцами, где возбуждение нейронов трансформируется в сокращения мышц. Промежуточные нейроны осуществляют обработку информации, получаемой от рецепторов, и формируют управляющие сигналы для эффекторов. Они образуют центральную нервную систему.

«нейроподобные сети» или просто «нейронные сети». Модель нейрона принято называть также «нейроподобный элемент», «искусственный нейрон», «блок», «узел» или просто «нейрон»

### 34.Протокол FTP

**FTP** (англ. *File Transfer Protocol* — протокол передачи файлов) — стандартный протокол, предназначенный для передачи файлов по TCP-сетям (например, Интернет). Использует 21й порт. FTP часто используется для загрузки сетевых страниц и других документов с частного устройства разработки на открытые сервера хостинга

Протокол построен на архитектуре «клиент-сервер» и использует разные сетевые соединения для передачи команд и данных между клиентом и сервером. Пользователи FTP могут пройти аутентификацию, передавая логин и пароль открытым текстом, или же, если это разрешено на сервере, они могут подключиться анонимно. Можно использовать протокол SSH для безопасной передачи, скрывающей (шифрующей) логин и пароль, а также шифрующей содержимое.

FTP может работать в активном или пассивном режиме, от выбора которого зависит способ установки соединения. В активном режиме клиент создаёт управляющее TCP-соединение с сервером и отправляет серверу свой IP-адрес и произвольный номер клиентского порта, после чего ждёт, пока сервер запустит TCP-соединение с этим адресом и номером порта. В случае, если клиент находится за [брандмауэром](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD) и не может принять входящее TCP-соединение, может быть использован пассивный режим. В этом режиме клиент использует поток управления, чтобы послать серверу команду PASV, и затем получает от сервера его IP-адрес и номер порта, которые затем используются клиентом для открытия потока данных с произвольного клиентского порта к полученному адресу и порту.

Передача данных может осуществляться в любом из трёх режимов:

Поточный режим — данные посылаются в виде непрерывного потока, освобождая FTP от выполнения какой бы то ни было обработки. Вместо этого, вся обработка выполняется TCP. Индикатор конца файла не нужен, за исключением разделения данных на записи.

Блочный режим — FTP разбивает данные на несколько блоков (блок заголовка, количество байт, поле данных) и затем передаёт их TCP.

Режим сжатия — данные сжимаются единым алгоритмом (обычно, кодированием длин серий).

### 35.Нейроподобные сети и математическое правило их обучения

Нейроподобная сеть представляет собой совокупность нейроподобных элементов, определенным образом соединенных друг с другом и с внешней средой. Входной вектор (кодирующий входное воздействие или образ внешней среды) подается на сеть путем активации входных нейроподобных элементов. Множество выходных сигналов нейронов сети *y1*…*ум* называют вектором выходной активности, или паттерном активности нейронной сети. Веса связей нейронов сети удобно представлять в виде матрицы *W,*где *Wij -* вес связи между *i*- и *j*-м нейронами. В процессе функционирования (эволюции состояния) сети осуществляется преобразование входного вектора в выходной, т. е. некоторая переработка информации, которую можно интерпретировать, например, как функцию гетеро- или авто- ассоциативной памяти. Конкретный вид выполняемого сетью преобразования информации обусловливается не только характеристиками нейроподобных элементов, но и особенностями ее архитектуры, т. е. той или иной топологией межнейронных связей, выбором определенных подмножеств нейроподобных элементов для ввода и вывода информации, наличием или отсутствием конкуренции, направлением и способами управления и синхронизации информационных потоков между нейронами и т. д.

**Обучение нейроподобной сети**

Одно из важнейших свойств нейроподобной сети - способность к самоорганизации, самоадаптации с целью улучшения качества функционирования. Это достигается обучением сети, алгоритм которого задается набором обучающих правил. Обучающие правила определяют, каким образом изменяются связи в ответ на входное воздействие. Многие из них являются развитием высказанной Д. О. Хеббом идеи о том, что обучение основано на увеличении силы связи (синаптического веса) между одновременно активными нейронами. Таким образом, часто используемые в сети связи усиливаются, что объясняет феномен обучения путем повторения и привыкания. Математически это правило можно записать следующим образом:

image021.gif (540 bytes)  
где *wij (t)* и *wij(t + 1)* - значение веса связи от *i*-го к *j*-му нейрону соответственно до и после его изменения, *б -* скорость обучения. В настоящее время существует множество разнообразных обучающих правил (алгоритмов обучения). Некоторые из них будут представлены в параграфах, посвященных рассмотрению конкретных нейросетевых моделей.

### 36.Протокол TFTP

TFTP (англ. Trivial File Transfer Protocol — простой протокол передачи файлов) используется главным образом для первоначальной загрузки бездисковых рабочих станций. TFTP, в отличие от FTP, не содержит возможностей аутентификации(хотя возможна фильтрация по IP-адресу) и основан на транспортном протоколе UDP.

Основное назначение TFTP — обеспечение простоты реализации клиента. В связи с этим он используется для загрузки бездисковых рабочих станций, загрузки обновлений и конфигураций в «умные» сетевые устройства, записи статистики с мини-АТС (CDR) и аппаратных [маршрутизаторов](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80)/[файрволов](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D1%80%D0%B2%D0%BE%D0%BB).

Сначала в TFTP-пакете идет поле размером в 2 [байта](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D0%B9%D1%82), определяющее тип пакета:

Read Request (RRQ, #1) — запрос на чтение файла.    Write Request (WRQ, #2) — запрос на запись файла.

Data (DATA, #3) — данные, передаваемые через TFTP.   Acknowledgment (ACK, #4) — подтверждение пакета.  Error (ERR, #5) — ошибка.   Error2 (ERR2, #6) — ошибка2.

В TFTP существует 2 режима передачи (режим Mail, определенный в IEN 133, признан устаревшим):

**netascii** — файл перед передачей перекодируется в ASCII.

**octet** — файл передается без изменений.

После получения RRQ-пакета сервером, он сразу начинает передачу данных. В случае с WRQ-запросом — сервер должен прислать ACK-пакет c номером пакета 0.

Обмен между клиентом и сервером начинается с того, что клиент запрашивает сервер либо прочитать, либо записать файл для клиента. В стандартном варианте загрузки бездисковой системы первый запрос - это запрос на чтение (RRQ).

Чтобы позволить нескольким клиентам загружаться одновременно, TFTP сервер предоставляет несколько форм одновременной работы. Так как UDP не предоставляет уникального соединения между клиентом и сервером (как это делает TCP), TFTP сервер создает новый UDP порт для каждого клиента. Это позволяет разным клиентам выдавать датаграммы, которые будут демультиплексированы UDP модулем сервера, на основе номеров портов назначения, вместо того чтобы это делал сам сервер.

Протокол TFTP не предоставляет средства безопасности. Большинство реализаций позволяет доступ по протоколу TFTP только к файлам, которые необходимы при загрузке.

### 37.Навигационные системы GPS и Глонасс

Система ГЛОНАСС (Глобальная навигационная спутниковая система) предназначена для определения местоположения, скорости движения и точного времени морских, воздушных, сухопутных транспортных средств и других видов потребителей. Она разрабатывалась и внедрялась как система двойного назначения, в первую очередь, для обеспечения национальной безопасности России, а также для решения гражданских научных и производственных задач. Система ГЛОНАСС создавалась с начала 70-х годов большой кооперацией научных гражданских и военных организаций. Первые космические аппараты серии ГЛОНАСС («Космос-1413», «Космос-1414», «Космос-1415») были выведены на орбиты 12 октября 1982 года.

Задачи, возложенные на систему ГЛОНАСС: 1. создание (задание) общеземной геодезической и геоцентрической систем координат; 2. распространение единой глобальной высокоточной шкалы времени; 3. создание общеземной сети слежения за современными движениями земной коры; 4. координатно-временное обеспечение o операций в космическом пространстве; o международной службы вращения Земли; o процесса дистанционного зондирования Земли, осуществляемого в интересах картографирования планеты, мониторинга экологического состояния её поверхности и атмосферы; o работ, реализуемых методом спутниковой альтиметрии с целью слежения за уровнем мирового океана, изучения его физической поверхности, в частности морской топографической поверхности и её отличий от поверхности геоида (квазигеоида), а также изучения закономерностей глобальной циркуляции водных масс. Основу системы ГЛОНАСС составляют три сегмента: • космический сегмент; • сегмент управления; • сегмент потребителей.

Космический сегмент включает 24 спутника, излучающих непрерывные радионавигационные сигналы, которые формируют сплошное радионавигационное поле на поверхности Земли и околоземном пространстве.

Сегмент управления — наземная система управления, предназначенная для контроля функционирования, непосредственно управления и информационного обеспечения сети спутников.

Сегмент потребителя обеспечивает определение пространственных координат, вектора скорости, текущего времени и других навигационных параметров в результате приёма и обработки радиосигналов, принимаемых от спутников.

Американская система позиционирования GPS по своим функциональным возможностям аналогична российской системе ГЛОНАСС. Её основное назначение — высокоточное определение координат потребителя, составляющих вектора скорости и привязка к системной шкале времени. Аналогично отечественной, система GPS разработана для Министерства обороны США и находится под его управлением. Как и система ГЛОНАСС, GPS состоит из космического сегмента, наземного командно-измерительного комплекса и сегмента потребителей.

Орбитальная группировка GPS состоит из 28 навигационных космических аппаратов. Все они находятся на круговых орбитах с периодом обращения вокруг Земли равным 12 часам. Высота орбиты каждого спутника примерно равна 20 тыс. км.

### 38.Сетевая файловая служба NFS

**Network file system** (**NFS**) — протокол сетевого доступа к файловым системам, первоначально разработан Sun Microsystems в 1984 году. Основан на протоколе вызова удалённых процедур (ONC RPC). Позволяет подключать (монтировать) удалённые файловые системы через сеть.

NFS абстрагирован от типов файловых систем как сервера, так и клиента, существует множество реализаций NFS-серверов и клиентов для различных операционных систем и аппаратных архитектур. Наиболее зрелая версия NFS — v.4, поддерживающая различные средства аутентификации (в частности, Kerberos и LIPKEY с использованием протокола RPCSEC GSS) и списков контроля доступа (как POSIX, так и Windows-типов).

NFS предоставляет клиентам прозрачный доступ к файлам и файловой системе сервера. В отличие от FTP, протокол NFS осуществляет доступ только к тем частям файла, к которым обратился процесс, и основное достоинство его в том, что он делает этот доступ прозрачным. Это означает, что любое приложение клиента, которое может работать с локальным файлом, с таким же успехом может работать и с NFS файлом, без каких-либо модификаций самой программы.

NFS-клиенты получают доступ к файлам на NFS-сервере путём отправки RPC-запросов на сервер. Это может быть реализовано с использованием обычных пользовательских процессов — а именно, NFS-клиент может быть пользовательским процессом, который осуществляет конкретные RPC-вызовы на сервер, который так же может быть пользовательским процессом.

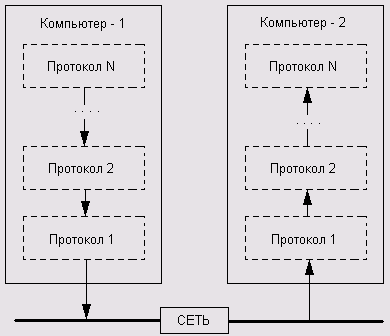
Реализация NFS состоит из нескольких компонентов. Некоторые из них локализованы либо на сервере, либо на клиенте, а некоторые используются и на обеих сторонах соединения. Некоторые компоненты не требуются для обеспечения основных функциональных возможностей, но составляют часть расширенного интерфейса NFS.

Протокол NFS определяет набор запросов (операций), которые могут быть направлены клиентом к серверу, а также набор аргументов и возвращаемые значения для каждого из этих запросов. Версия 1 этого протокола существовала только в недрах Sun Microsystems и никогда не была выпущена. Все реализации NFS (в том числе NFSv3) поддерживают версию 2 NFS (NFSv2), которая впервые была выпущена в 1985 году в [SunOS](https://ru.wikipedia.org/wiki/SunOS) 2.0. Версия 3 протокола была опубликована в 1993 году и реализована некоторыми фирмами-поставщиками.

### 39.Концептуальная модель многоуровневой системы протоколов

Вместе с тем передача информации между несколькими сетевыми компьютерами — не такая уж простая задача, как это может показаться на первый взгляд. Для того чтобы понять это, достаточно представить себе тот круг проблем, который может возникнуть в процессе приема или трансляции каких-либо данных. Отсюда следует, что в локальной сети необходимо обеспечить жесткий контроль для отслеживания всех этих ошибок, и более того, организовать четкую работу как аппаратных, так и программных компонентов сети.   
Выход нашелся в разделении протоколов на ряд концептуальных уровней, каждый из которых обеспечивает интерфейс между различными модулями программного обеспечения, установленного на работающих в сети компьютерах. Таким образом, механизм передачи какого-либо пакета информации через сеть от клиентской программы, работающей на общем компьютере, клиентской программе, работающей на другом компьютере, можно условно представить в виде последовательной пересылки этого пакета сверху вниз от некоего протокола верхнего уровня, обеспечивающего взаимодействие с пользовательским приложением, протоколу нижнего уровня, организующему интерфейс с сетью, его трансляции на компьютер-получатель и обратной передачи протоколу верхнего уровня уже на удаленной машине (Рисунок 2.1).

Рисунок 2.1. Концептуальная модель многоуровневой системы протоколов

  
Согласно такой схеме, каждый из уровней подобной системы обеспечивает собственный набор функций при передаче информации по локальной сети.  
Например, можно предположить, что протокол верхнего уровня, осуществляющий непосредственное взаимодействие с клиентскими программами, транслирует данные протоколу более низкого уровня, «отвечающему» за работу с аппаратными устройствами сети, преобразовывая их в «понятную» для него форму. Тот, в свою очередь, передает их протоколу, осуществляющему непосредственно пересылку информации на другой компьютер. На удаленном компьютере прием данных осуществляет аналогичный протокол «нижнего» уровня и контролирует корректность принятых данных, то есть определяет, следует ли транслировать их протоколу, расположенному выше в иерархической структуре, либо запросить повторную передачу. В этом случае взаимодействие осуществляется только между протоколами нижнего уровня, верхние уровни иерархии в данном процессе не задействованы. В случае если информация была передана без искажений, она транслируется вверх через соседние уровни протоколов до тех пор, пока не достигнет программы-получателя. При этом каждый из уровней не только контролирует правильность трансляции данных на основе анализа содержимого пакета информации, но и определяет дальнейшие действия исходя из сведений о его назначении. Например, один из уровней «отвечает» за выбор устройства, с которого осуществляется получение и через которое передаются данные в сеть, другой «решает», передавать ли информацию дальше по сети, или она предназначена именно этому компьютеру, третий «выбирает» программу, которой адресована принятая информация. Подобный иерархический подход позволяет не только разделить функции между различными модулями сетевого программного обеспечения, что значительно облегчает контроль работы всей системы в целом, но и дает возможность производить коррекцию ошибок на том уровне иерархии, на котором они возникли. Каждую из подобных иерархических систем, включающих определенный набор протоколов различного уровня, принято называть стеком протоколов.

### 40.Протокол SMTP

**SMTP** (англ. *Simple Mail Transfer Protocol* — простой протокол передачи почты) — это широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.

SMTP впервые был описан в RFC 821 (1982 год); последнее обновление в RFC 5321 (2008) включает масштабируемое расширение — **ESMTP** (англ.  *Extended SMTP*). В настоящее время под «протоколом SMTP», как правило, подразумевают и его расширения. Протокол SMTP предназначен для передачи исходящей почты с использованием порта TCP 25.

В то время, как электронные почтовые серверы и другие агенты пересылки сообщений используют SMTP для отправки и получения почтовых сообщений, работающие на пользовательском уровне клиентские почтовые приложения обычно используют SMTP только для отправки сообщений на почтовый сервер для ретрансляции.

SMTP — требующий соединения текстовый протокол, по которому отправитель сообщения связывается с получателем посредством выдачи командных строк и получения необходимых данных через надёжный канал, в роли которого обычно выступает TCP-соединение (Transmission Control Protocol — протокол управления передачей). SMTP-сессия состоит из команд, посылаемых SMTP-[клиентом](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B8%D0%B5%D0%BD%D1%82_(%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)), и соответствующих ответов SMTP-[сервера](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80_(%D0%B0%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5)). Когда сессия открыта, сервер и клиент обмениваются её параметрами. Сессия может включать ноль и более SMTP-операций (транзакций).

SMTP-операция состоит из трёх последовательностей команда/ответ (см. пример ниже). Описание последовательностей:

MAIL FROM — устанавливает обратный адрес (т. е. Return-Path, 5321.From, mfrom). Это адрес для [возвращённых писем](https://ru.wikipedia.org/wiki/%D0%92%D0%BE%D0%B7%D0%B2%D1%80%D0%B0%D1%89%D1%91%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BF%D0%B8%D1%81%D1%8C%D0%BC%D0%BE).

RCPT TO — устанавливает получателя данного сообщения. Эта команда может быть дана несколько раз, по одному на каждого получателя. Эти адреса также являются частью оболочки.

DATA — для отправки текста сообщения. Это само содержимое письма, в противоположность его оболочке. Он состоит из заголовка сообщения и тела сообщения, разделенных пустой строкой. DATA, по сути, является группой команд, а сервер отвечает дважды: первый раз на саму команду DATA, для уведомления о готовности принять текст; и второй раз после конца последовательности данных, чтобы принять или отклонить всё письмо.

SMTP — всего лишь протокол доставки. Он не может по требованию взять сообщения с удаленного сервера.

### 41.Протокол SNMP

SNMP ( Simple Network Management Protocol - 1988г. )

Протокол SNMP был разработан с целью проверки функционирования сетевых маршрутизаторов и мостов. Впоследствии сфера действия протокола охватила и другие сетевые устройства, такие как хабы, шлюзы, терминальные сервера, LAN Manager сервера , машины под управлением Windows NT и т.д. Кроме того, протокол допускает возможность внесения изменений в функционирование указанных устройств.

Протокол SNMP работает на базе протокола UDP и предназначен для использования сетевыми управляющими станциями. Он позволяет управляющим станциям собирать информацию о положении в сети Internet. Протокол определяет формат данных, их обработка и интерпретация остаются на усмотрение управляющих станций или менеджера сети. SNMP-сообщения не имеют фиксированного формата и фиксированных полей. При работе протокол SNMPиспользует управляющую базу данных (MIB — Management Information Base, RFC-1213,-1212).

### 42.Сетезависимые и сетенезависимые уровни протоколов модели OSI

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

Три верхних уровня — прикладной, представительный и сеансовый — ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют какие бы то ни было изменения в топологии сети, замена оборудования или переход на другую сетевую технологию. Так, переход от Ethernet на высокоскоростную технологию lOOVG-AnyLAN не потребует никаких изменений в программных средствах, реализующих функции прикладного, представительного и сеансового уровней.

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

### 43.Выбор оборудования КС

*Сетевое оборудование* – устройства, из которых состоит компьютерная сеть. Условно выделяют два вида сетевого оборудования:

* Активное сетевое оборудование – оборудование, которое способно обрабатывать или преобразовывать передаваемую по сети информацию. К такому оборудованию относятся сетевые карты, маршрутизаторы, принт-серверы.
* Пассивное сетевое оборудование – оборудование, служащее для простой передачи сигнала на физическом уровне. Это сетевые кабели, коннекторы и сетевые розетки, повторители и усилители сигнала.

Для монтажа проводной локальной сети нам в первую очередь понадобятся:

* сетевой кабель и разъемы (называемые коннекторами);
* сетевые карты – по одной в каждом ПК сети, и две на компьютере, служащем сервером для выхода в интернет;
* устройство или устройства, обеспечивающие передачу пакетов между компьютерами сети. Для сетей из трех и более компьютеров нужно специальное устройство –коммутатор, который объединяет все компьютеры сети;
* дополнительные сетевые устройства. Простейшая сеть строится и без такого оборудования, однако при организации общего выхода в интернет, использовании общих сетевых принтеров дополнительные устройства могут облегчить решение подобных задач.

сетевые кабели (витая пара, коаксиальный кабель, оптоволокно).

* *Коаксиальный кабель* – это первый кабель, который применялся для создания сетей. От его использования при построении локальных компьютерных сетей уже давно отказались.
* *Оптоволоконный кабель* – наиболее перспективный в плане скоростных показателей, но и более дорогой по сравнению с коаксиальным кабелем или витой парой. К тому же монтаж оптоволоконных сетей требует высокой квалификации, а для оконцовки кабеля необходимо дорогостоящее оборудование. По этим причинам широкого распространения данный вид кабеля пока не получил.
* *Витая пара* – самый распространенный на сегодняшний день вид кабеля, применяемый для построения локальных сетей. Кабель состоит из попарно перевитых медных изолированных проводников. Типичный кабель несет в себе 8 проводников (4 пары), хотя выпускается и кабель с 4 проводниками (2 пары). Цвета внутренней изоляции проводников строго стандартны. Расстояние между устройствами, соединенными витой парой, не должно превышать 100 метров.  
  Существует несколько категорий кабелей типа витая пара, которые маркируются от CAT1 до CAT7. В локальных сетях стандарта Ethernet используется витая пара категории CAT5.
* Для работы с кабелем витая пара применяются коннекторы RJ-45.

### 44.Протокол IPX

IPX/SPX (от англ. Internetwork Packet eXchange/Sequenced Packet eXchange) — стек протоколов, используемый в сетях Novell NetWare. Протокол IPX обеспечивает сетевой уровень (доставку пакетов, аналог IP), SPX — транспортный и сеансовый уровень (аналог [TCP](http://wiki.mvtom.ru/index.php/TCP)).

Этот стек является оригинальным стеком протоколов фирмы Novell, который она разработала для своей сетевой операционной системы NetWare еще в начале 80-х годов. Протоколы Internetwork Packet Exchange (IPX) и Sequenced Packet Exchange (SPX), которые дали имя стеку, являются прямой адаптацией протоколов XNS фирмы Xerox, распространенных в гораздо меньше степени, чем IPX/SPX.

Протокол IPX предназначен для передачи дейтограмм в системах, неориентированных на соединение (также как и IP или NETBIOS, разработанный IBM и эмулируемый в Novell), он обеспечивает связь между NetWare серверами и конечными станциями. Максимальный размер IPX-дейтограммы составляет 576 байт, из них 30 байта занимает заголовок. Предполагается, что сеть, через которую транспортируются эти дейтограммы, способна пересылать пакеты соответствующей длины. IPX-пакеты могут рассылаться широковещательно, для этого поле типа должно принять значение 0x14, адрес сети назначения должен соответствовать локальной сети, адрес узла назначения при этом принимает значение 0xFFFFFF.

### 45.Структура пакета

Пакеты могут содержать несколько типов данных:

* информацию (например, сообщения или файлы);
* определенные виды данных и команд, управляющих компьютером (например, запросы к службам);
* коды управления сеансом (например, запрос на повторную передачу для исправления ошибок).

Некоторые компоненты являются обязательными для всех типов пакетов:

* адрес источника (source), идентифицирующий компьютер-отправитель;
* передаваемые данные;
* адрес местоназначения (destination), идентифицирующий компьютер-получатель;
* инструкции сетевым компонентам о дальнейшем маршруте данных;
* информация компьютеру-получателю о том, как объединить передаваемый пакет с остальными, чтобы получить данные в исходном виде;
* информация для проверки ошибок, обеспечивающая корректность передачи.

Компоненты пакета группируются в три раздела: заголовок, данные и трейлер.  
**Заголовок**

Заголовок включает:

* сигнал, ©говорящий© о том, что передается пакет;
* адрес источника;
* адрес местоназначения;
* информацию, синхронизирующую передачу.  
  Данные

Эта часть пакета - собственно передаваемые данные. В зависимости от типа сети её размер может меняться. Но для большинства сетей он составляет от 512 байтов (0,5 Кб) до 4 Кб. Так как обычно размер исходных данных гораздо больше 4 Кб, для помещения в пакет их необходимо разбивать на меньшие блоки. При передаче объемного файла может потребоваться много пакетов.  
**Трейлер** (концевик, терминатор)

Содержимое трейлера зависит от метода связи, или протокола. Чаще всего трейлер содержит информацию для проверки ошибок, называемую циклическим избыточным кодом (Cyclical Redundancy Check, CRC). CRC - это число, получаемое в результате математических преобразований над пакетом и исходной информацией. Когда пакет достигает местоназначения, эти преобразования повторяются. Если результат совпадает с CRC, с высокой вероятностью можно считать, что пакет принят без ошибок.

### 46.Управление потоком данных в сети

Управление потоком передачи данных ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Flow Control*) — в компьютерных сетях, механизм, который притормаживает передатчик данных при неготовности приёмника.

Различают три основных способа:

* аппаратный, при котором сигналы «готов/занят» передаются по отдельным физическим линиям связи. Наиболее известна такая реализация в интерфейсе [RS-232](https://ru.wikipedia.org/wiki/RS-232).
* программный, при котором программный флажок «готов/занят» взводится и сбрасывается вставкой в поток данных специальной уникальной последовательности (XOn/XOff). Применяется в программных драйверах интерфейса RS-232 как альтернатива аппаратному контролю потока в случаях неполного соединительного кабеля.
* протокольный, при котором программный флажок «готов/занят» взводится и сбрасывается специальными соглашениями в рамках протокола обмена данными. На сегодня является практически единственным применяемым способом контроля потока. Наиболее известный пример — реализация контроля потока в протоколе[TCP](https://ru.wikipedia.org/wiki/TCP) методом скользящего окна.

### 47.Протокол маршрутной информации RIP

Протокол маршрутной информации ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA)  *Routing Information Protocol*) — один из самых простых [протоколов](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8) [маршрутизации](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F). Применяется в небольших[компьютерных сетях](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), позволяет [маршрутизаторам](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80) динамически обновлять маршрутную информацию (направление и дальность в [хопах](http://участок)), получая ее от соседних маршрутизаторов.

Характеристики:

– является дистанционно-векторным протоколом маршрутизации;

– в качестве метрики при выборе маршрута используется количество переходов (хопов);

– если количество переходов становится дольше 15 – пакет отбрасывается;

– по умолчанию обновления маршрутизации рассылаются широковещательно каждые 30 секунд.

Протокол RIP предотвращает появление петель в маршрутизации, по которым пакеты могли бы циркулировать неопределенно долго, устанавливая максимально допустимое количество переходов на маршруте от отправителя к получателю. Стандартное максимальное значение количества переходов равно 15.При получении маршрутизатором обновление маршрутов, содержащего новую или измененную запись, он увеличивает значение метрики на единицу.

Если при этом значение метрики превышает 15, то считается бесконечно большим, и сеть-получатель считается недостижимой.Протокол RIP обладает рядом функций, которые являются общими для него и других протоколов маршрутизации.Например, он позволяет использовать механизмы расщепления горизонта и таймеры удержания информации для предотвращения распространения некорректных сведений о маршрутах, но об этом я напишу в следующих статьях.

### 48.Стек протоколов TCP/IP

Стек протоколов TCP/IP — набор [сетевых протоколов](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) передачи данных, используемых в сетях, включая сеть[Интернет](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82). Название TCP/IP происходит из двух наиважнейших протоколов семейства — [Transmission Control Protocol](http://protocol)(TCP) и [Internet Protocol](http://protocol) (IP), которые были разработаны и описаны первыми в данном стандарте. Также изредка упоминается как [модель DOD](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_DOD) в связи с историческим происхождением от сети [ARPANET](https://ru.wikipedia.org/wiki/ARPANET) из 1970 годов (под управлением [DARPA](https://ru.wikipedia.org/wiki/DARPA), [Министерства обороны США](https://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D0%B5%D1%80%D1%81%D1%82%D0%B2%D0%BE_%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D1%8B_%D0%A1%D0%A8%D0%90)).

Протоколы работают друг с другом в [стеке](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%BA) ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *stack*, стопка) — это означает, что протокол, располагающийся на уровне выше, работает «поверх» нижнего, используя механизмы [инкапсуляции](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D0%BA%D0%B0%D0%BF%D1%81%D1%83%D0%BB%D1%8F%D1%86%D0%B8%D1%8F_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8)). Например, протокол [TCP](https://ru.wikipedia.org/wiki/TCP) работает поверх протокола [IP](https://ru.wikipedia.org/wiki/IP).

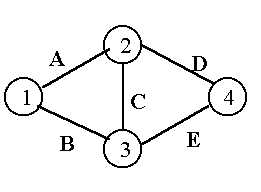
Стек протоколов TCP/IP включает в себя четыре уровня:

* [прикладной уровень](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%BE%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) (application layer),
* [транспортный уровень](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B0%D0%BD%D1%81%D0%BF%D0%BE%D1%80%D1%82%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) (transport layer),
* [сетевой уровень](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) (network layer),
* [канальный уровень](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) (link layer).

Протоколы этих уровней полностью реализуют функциональные возможности [модели OSI](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI). На стеке протоколов TCP/IP построено всё взаимодействие пользователей в IP-сетях. Стек является независимым от физической среды передачи данных.

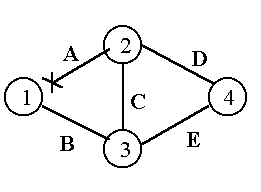
### 49.Пример RIP-системы

Протокол RIP является дистанционно-векторным протоколом внутренней маршрутизации. Процесс работы протокола состоит в рассылке, получении и обработке векторов расстояний до IP-сетей, находящихся в области действия протокола, то есть в данной RIP-системе. Результатом работы протокола на конкретном маршрутизаторе является таблица, где для каждой сети данной RIP-системы указано расстояние до этой сети (в *хопах*) и адрес *следующего маршрутизатора*. Информация о номере сети и адресе следующего маршрутизатора из этой таблицы вносится в таблицу маршрутов, информация о расстоянии до сети используется при обработке векторов расстояний.



Здесь  , ‚ , ƒ , „  - маршрутизаторы, A, B, C, D, E - сети.

Следовательно, узел  рассылает в сети А и В вектор расстояний (А=1,В=1).



Узел  обнаруживает свое отсоединение от сети А и меняет таблицу маршрутов, устанавливая бесконечное расстояние до всех сетей, ранее достижимых через маршрутизаторы, подключенные к сети А (то есть ‚ ). В протоколе RIP значение бесконечности равно 16.

### 50.Формат сообщения протокола RIP

RIP работает на основе UDP-протокола и использует порт 520. На каждом хосте, использующем RIP, должно быть установлено программное обеспечение, обрабатывающее RIP-пакеты.

Полное сообщение протокола RIP IP, включая заголовок и данные, инкапсулируется в порцию данных дейтаграммы протокола UDP, которая, в свою очередь, инкапсули- руется в IP дейтаграмму.

Все сообщения протокола RIP состоят из заголовка фиксированной длины и следующего за ним списка сетей, которые могут быть достижимы с использованием данного передающего маршрутизатора.

* 0-7 биты – Command
* 8-15 биты – Version
* 16-31 биты – Routing Domain
* 0-31 биты – RIP Entry

Command — команда, определяет назначение датаграммы (1 — request; 2 — response).

Version — номер версии, в зависимости от версии, определяется формат пакета

Routing Domain — идентификатор RIP-системы, к которой принадлежит данное сообщение; часто — номер автономной системы. Используется, когда к одному физическому каналу подключены маршрутизаторы из нескольких автономных систем, в каждой автономной системе поддерживается своя таблица маршрутов.

RIP Entry (RTE) — запись маршрутной информации RIP. RIP пакет может содержать от 1 до 25 записей RIP Entry.

### 51.Схема защиты локальной сети с помощью сетевого фильтра

Сетевые фильтры работают на сетевом уровне иерархии OSI. Сетевой фильтр представляет собой маршрутизатор, обрабатывающий пакеты на основании информации, содержащейся в заголовках пакетов. Сетевые фильтры существуют для сетей TCP/IP и IPX/SPX, но последние применяют в локальных сетях, поэтому мы их рассматривать не будем.

При обработке пакетов ими учитывается следующая информация:

* IP-адрес отправителя;
* IP-адрес получателя;
* протокол (TCP, UDP, ICMP);
* номер программного порта отправителя;
* номер программного порта получателя.

Администратор на основе этой информации задает правила, в соответствии с которыми пакеты будут либо пропускаться через фильтр, либо отбрасываться им. Например, сетевой фильтр позволяет реализовать следующую схему обмена данными между компьютерами корпоративной сети и Internet:

1. все компьютеры корпоративной сети имеют возможность общаться с внешними серверами Web и ftp, но не с telnet, NNTP и т. д.;
2. доступ извне запрещен ко всем компьютерам корпоративной сети, кроме доступа к серверу A по протоколу HTTP и к серверу B по протоколу ftp; кроме того, внешнему компьютеру Z разрешается доступ к внутреннему серверу C и к любым службам TCP и UDP, но не ICMP.

Сетевые фильтры очень легко реализовать, поэтому они получили повсеместное распространение и представлены программно-аппаратными и чисто программными реализациями.

В сетевых фильтрах в основном используется статическая фильтрация, когда администратору приходится создавать свой фильтр для каждого уникального типа пакета, требующего обработки. Поясним это на примере. Допустим, всем компьютерам по умолчанию запрещен доступ в Internet.

### 52.Протокол OSPF

OSPF — это открытый протокол маршрутизации, базирующийся на алгоритме поиска наикратчайшего пути (Open Shortest Path First — OSPF). OSPF имеет две основные характеристики: протокол является открытым, т. е. его спецификация является общественным достоянием, он базируется на алгоритме SPF. Алгоритм SPF иногда называют алгоритмом *Dijkstra* по имени его автора.

OSPF является иерархическим протоколом маршрутизации с объявлением состояния о канале соединения (link-state). Он был спроектирован как протокол работы внутри сетевой области — AS (Autonomous System), которая представляет собой группу маршрутизаторов и сетей, объединенных по иерархическому принципу и находящихся под единым управлением и совместно использующих общую стратегию маршрутизации. В качестве транспортного протокола для маршрутизации внутри AS OSPF использует IP-протокол.

Обмен информацией о маршрутах внутри AS протокол OSPF осуществляет посредством обмена сообщениями о состояниях канала соединений между маршрутизаторами и сетями области (link-state advertisement — LSA). Эти сообщения передаются между объектами сети, находящимися в пределах одной и той же иерархической области — это может быть как вся AS, так и некоторая группа сетей внутри данной AS. В LSA-сообщения протокола OSPF включается информация о подключенных интерфейсах, о параметрах маршрутов и других переменных. По мере накопления роутерами OSPF информации о состоянии маршрутов области, они рассчитывают наикратчайший путь к каждому узлу, используя алгоритм SPF. Причем расчет оптимального маршрута осуществляется динамически в соответствии с изменениями топологии сети.

### 53.Прокси-сервер и его функции

**Прокси-сервер** — это особый тип приложения, которое выполняет функции посредника между клиентскими и серверными частями распределенных сетевых приложений, причем предполагается, что клиенты принадлежат внутренней (защищаемой) сети, а серверы — внешней (потенциально опасной) сети.

Роль транзитного узла позволяет прокси-серверу логически разорвать прямое соединение между клиентом и сервером с целью контроля процесса обмена сообщениями между ними.

Подобно сетевому экрану, прокси-сервер может эффективно выполнять свои функции только при условии, что контролируемый им трафик не пойдет обходным путем.

Прокси-сервер может быть установлен не только на платформе, где работают все остальные модули сетевого экрана, но и на любом другом узле внутренней сети или сети периметра. В последнем случае программное обеспечение клиента должно быть сконфигурировано таким образом, чтобы у него не было возможности установить прямое соединение с ресурсным сервером, минуя прокси-сервер.

Когда клиенту необходимо получить ресурс от какого-либо сервера (файл, веб-страницу, почтовое сообщение), он посылает свой запрос прокси-серверу. Прокси-сервер анализирует этот запрос на основании заданных ему администратором правил и решает, каким образом он должен быть обработан (отброшен, передан без изменения ресурсному серверу, модифицирован тем или иным способом перед передачей, немедленно обработан силами самого прокси-сервера).

Прокси-сервер, выступая посредником между клиентом и сервером, взаимодействующими между собой по совершенно определенному протоколу, не может не учитывать специфику этого протокола. Так, для каждого из протоколов HTTP, HTTPS, SMTP/POP, FTP, telnet существует особый прокси-сервер, ориентированный на использование соответствующими приложениями: веб-браузером, электронной почтой, FTP-клиентом, клиентом telnet. Каждый из этих посредников принимает и обрабатывает пакеты только того типа приложений, для обслуживания которого он был создан.

### 54.Брандмауэр и его функции

Брандмауэр представляет собой программное приложение, или же специальное устройство, основной задачей которого является контроль над трафиком между компьютерными сетями с различными уровнями безопасности, разделяя, например, меньшую домашнюю или офисную сети от остальной части Интернета. Если задача брандмауэра в здании - предотвращение распространения сигнала из одной части здания в другую, то в компьютерных сетях, задачей межсетевого экрана является предотвращение распространения вредоносных атак из менее защищенной внешней сети во внутреннюю сеть или в конкретный компьютер.  
Для разделения внутренней сети от внешней сети обычно используют буфер или скрытие адресов внутренней сети. Буфер или **прокси** анализирует входящие запросы и, если на запрос уже давали ответ, и ответы уже находятся в буферной памяти, внутренняя сеть не передает его повторно для обработки, а отвечает сам. **NAT** (**Network Address Translation**) или переименование сетевых адресов означает то, что у локальной сети в Интернете есть свой IP-адрес; устройство NAT заботится о том, чтобы данные приходящие из интернета на этот адрес были пересланы на правильные адреса. Злоумышленники, которые хотят из внешней сети атаковать внутреннюю сеть, не находят компьютеры внутренней сети, т.к. во внешней сети адреса этих компьютеров не видны.

### 55.Основные функции элементов сетевого управления

**Система управления элементами сети** (англ. *Element management system*, сокр. EMS) — программное обеспечение предназначенное для управления и контроля отдельного сетевого элемента группы однотипных элементов.

Состоит из систем и приложений, которые связаны с управлением (СЭ) на сетевом уровне управления элементом (УСЭ) модели управления телекоммуникационной сетью.

EMS управляет одним или более специфичным типом телекоммуникационных сетевых элементов. Как правило, EMS управляет функциями и возможностями в рамках каждого СЭ, но не управляет трафиком между различными СЭ в сети. Для поддержки управления трафиком между собой и другими СЭ, EMS обращается выше, к системам управления сетью (NMS) более высокого уровня, как описано в многоуровневой модели управления телекоммуникационной сетью (TMN). EMS обеспечивает основу для реализации архитектуры многоуровневых TMN систем поддержки операций (OSS), которая позволит поставщикам услуг удовлетворить потребности клиента для быстрого развертывания новых услуг, а также отвечают строгим качества обслуживания (QoS) требований.

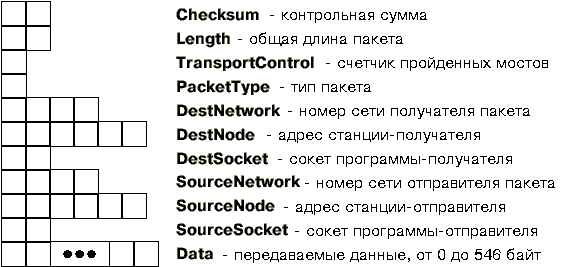
В соответствии с рекомендациями ITU-T, основные функции управления элементами сети делится на пять основных областей: управление отказами, управление конфигурацией, учёт, управление производительностью и безопасностью (FCAPS). Все части FCAPS укладываются в модель TMN.

NMS предоставляет единую систему обмена информацией через управляющие приложения, автоматизацию задач управления устройствами, обзор состояния и производительности сети, а также выявление и определение сетевых неисправностей. С помощью единой централизованной системы и знания инвентаризации сети, NMS обеспечивает уникальную платформу межфункциональных возможности управления, что снижает накладные расходы сетевого администрирования.

NMS это решение для управления уровня оператора. Она способна расширятся по мере роста сети, сохраняя высокие уровни производительности, в соответствие с ростом числа сетевых событий, и предоставлять возможность упрощенной интеграции с системами сторонних производителей. Это соответствует ожиданиям поставщиков услуг по системам OSS.

### 56.Формат пакета IPX

Формат передаваемых по сети пакетов:



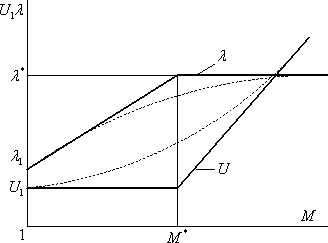
Пакет можно разделить на две части - заголовок и передаваемые данные. Все поля, представленные на рис. 2, кроме последнего (Data), представляют собой заголовок пакета. Заголовок пакета выполняет ту же роль, что и конверт обычного письма - там располагается адрес назначения, обратный адрес и некоторая служебная информация.

Особенностью формата пакета является то, что все поля заголовка содержат значения в перевернутом формате, т. е. по младшему адресу записывается старший байт данных, а не младший, как это принято в процессорах фирмы Intel. Поэтому перед записью значений в многобайтовые поля заголовка необходимо выполнить соответствующее преобразование. Представление данных в заголовке пакета соответствует, например, формату целых чисел в компьютере IBM-370 (серия ЕС ЭВМ).

### 57.Мультипрограммный режим работы СОД. Формула, отражающая основной закон теории массового обслуживания

Это способ выполнения задания, характеризующийся порядком распределения ресурсов системы между заданиями. Требуемый режим обработки данных обеспечивается ОС, которое выделяет заданию необходимые системные ресурсы в соответствующем порядке, с учетом приоритетов, сложности задач и другого.

**Мультипрограммная обработка.**Режим обработки, в котором в системе обрабатывается сразу одновременно несколько задач, называется мультипрограммным или мультипрограммированием. При этом процессорные обработки, относящиеся к разным задачам, одновременно выполняются различными устройствами системы способными работать параллельно. Цель мультипрограммирования: увеличение производительности системы.

Число задач находящихся в системе называются уровнем мультипрограммирования, рассмотрим его влияние на производительности время ответа.

На графике штриховыми кривыми показаны зависимость производительность системы ʎ и времени ответа U от уровня мультипрограммирования М. При изучении этих зависимостей удобно эти кривые представлять ломанными линиями, состоящими из 2-х асимптот, характеризующие верхнюю и нижнюю оценку данных показателей. В однопрограммном режиме: (М=1)=˃ U = U1 = V. Производительность системы: ʎ=ʎ1= 1/U1

C увеличением М увеличивается вероятность того, что большее число устройств одновременно занято выполнением задач, но вместе с тем вероятность того что несколько задач одновременно обращаются к одному устройству достаточно мала, поэтому время ожидания оказывается незначительным, однако при М= М\*возникает ситуация, когда по крайней мере одно устройство оказывается полностью загруженным. Дальнейшее увеличение числа задач не приводит к росту производительности ʎ, а ʎ определяется производительностью ʎ\* этого устройства.

Производительность λ и среднее время ответа U связаны между собой зависимостью ʎ=М/U которая называется формулой Литтла и является фундаментальным законом теории массового обслуживания.

В системе, состоящей из N устройств, загрузка которых равна , среднее число задач m, выполняемых одновременно в мультипрограммном режиме, равно суммарной загрузке устройств: http://konspekta.net/lektsiinetimg/baza3/2216022071773.files/image002.png ; http://konspekta.net/lektsiinetimg/baza3/2216022071773.files/image003.png ;

Таким образом, коэффициент мультипрограммирования m является показателем увеличения производительности системы за счет мультипрограммирования.

**Теория массового обслуживания** (теория очередей) — раздел теории вероятностей, целью исследований которого является рациональный выбор структуры системы обслуживания и процесса обслуживания на основе изучения потоков требований на обслуживание, поступающих в систему и выходящие из неё, длительности ожидания и длины очередей. В теории массового обслуживания используются методы теории вероятностей и математической статистики.

### 58.Открытая модель OSI и ее общая характеристика

***Модель взаимодействия открытых систем*** ( ***Open System Interconnection, OSI*** ) определяет различные уровни взаимодействия систем в *сетях с коммутацией пакетов*, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень.

В *модели OSI*  средства взаимодействия делятся на семь уровней: прикладной, *представительный*, *сеансовый*,транспортный,  *сетевой*,  *канальный* и *физический.*  Каждый уровень имеет дело с определенным аспектом взаимодействия сетевых устройств.

*Модель OSI* описывает только системные средства взаимодействия, реализуемые операционной системой, *системными утилитами* и аппаратными средствами. Модель не включает средства взаимодействия приложений конечных пользователей. Собственные протоколы взаимодействия приложения реализуют, обращаясь к системным средствам. Поэтому необходимо различать уровень взаимодействия приложений и *прикладной уровень*.

Итак, пусть приложение обращается с запросом к прикладному уровню, например к *файловой службе*. На основании этого запроса программное обеспечение прикладного уровня формирует *сообщение* стандартного формата. Обычное *сообщение* состоит из заголовка и поля данных.

После формирования сообщения *прикладной уровень* направляет его вниз по *стеку* *представительному уровню*. Протокол *представительного уровня* на основании информации, полученной из заголовка прикладного уровня, выполняет требуемые действия и добавляет к сообщению собственную служебную информацию — заголовок *представительного уровня*, в котором содержатся указания для протокола *представительного уровня* машины-адресата. Полученное в результате *сообщение* передается вниз*сеансовому уровню*, который в свою очередь добавляет свой заголовок, и т. д. (Некоторые протоколы помещают служебную информацию не только в начале сообщения в виде заголовка, но и в конце, в виде так называемого "концевика".) Наконец,*сообщение* достигает нижнего, *физического уровня*, который, собственно, и передает его по линиям связи машине-адресату. К этому моменту *сообщение* "обрастает" заголовками всех уровней.

Когда *сообщение* по сети поступает на машину-адресат, оно принимается ее *физическим уровнем* и последовательно перемещается вверх с уровня на уровень. Каждый уровень анализирует и обрабатывает заголовок своего уровня, выполняя соответствующие данному уровню функции, а затем удаляет этот заголовок и передает *сообщение* вышележащему уровню.

### 59.Выбор сетевых и программных средств

При выборе сетевого программного обеспечения (*ПО*) надо, в первую *очередь*, учитывать следующие факторы:

* Какую сеть поддерживает сетевое ПО: *одноранговую*, сеть на основе сервера или оба этих типа;
* Максимальное количество пользователей (лучше брать с запасом не менее 20%);
* Количество серверов и возможные их типы;
* Совместимость с разными операционными системами и компьютерами, а также с другими сетевыми средствами;
* Уровень производительности программных средств в различных режимах работы;
* Степень надежности работы, разрешенные режимы доступа и степень защиты данных;
* Какие сетевые службы поддерживаются;
* И, возможно, главное – стоимость программного обеспечения, его эксплуатации и модернизации.

Всегда есть соблазн использовать самый совершенный продукт, ведь он популярен и, следовательно, оптимален. Тем не менее, лучше устоять, так как с ним, возможно, сложнее обращаться, да и цена у него выше. Вполне вероятно, что для задач предприятия может подойти простая *одноранговая сеть*, не требующая специального администрирования и покупки дорогого сервера.

Наконец, еще до установки сети необходимо решить вопрос об управлении сетью. Даже в случае *одноранговой сети* лучше выделить для этого отдельного специалиста (*администратора*), который будет иметь всю информацию о конфигурации сети и распределении ресурсов и следить за корректным использованием сети всеми пользователями. Если *сеть* большая, то одним*сетевым администратором* уже не обойтись, нужна *группа*, возглавляемая системным администратором. После установки и запуска сети решать эти вопросы, как правило, слишком поздно.

Только после всего перечисленного можно переходить к установке выбранного программного обеспечения, если, конечно, таковая требуется. Следует заметить, что в большинстве случаев непосредственно установкой программных средств занимаются работники специализированных компьютерных фирм. Но принимать решение, о том, что нужно конкретному предприятию, должны все-таки те, кто будет с этой сетью работать в дальнейшем.

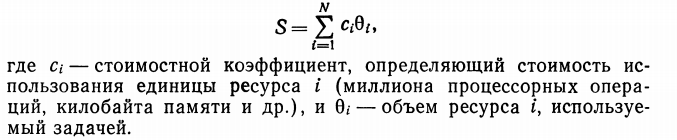
Затем необходимо провести *конфигурирование* сети, то есть задать ее логическую конфигурацию, настроить на работу в конкретных условиях. В обязанности *системного администратора сети*, который осуществляет *контроль* и управление входит:

* Создание групп пользователей различного назначения;
* Определение прав доступа пользователей;
* Обучение новых пользователей и оперативная помощь в случае необходимости;
* Контроль дискового пространства всех серверов сети;
* Защита и резервное копирование данных, борьба с компьютерными вирусами;
* Модернизация программного обеспечения и сетевой аппаратуры;
* Настройка сети для получения максимальной производительности.

### 60.Оценка стоимости КС

Стоимость КС — это суммарная стоимость технических средств и программного обеспечения. Стоимость технических средств определяется их составом и техническими характеристиками. Устройства с более высокими техническими характеристиками — быстродействием, емкостью, надежностью — имеют более высокую стоимость. Стоимость программного обеспечения определяется в основном затратами на разработку программ и тиражируемостью программ — числом систем, в которых используются программы. Затраты на разработку программ наиболее существенно зависят от сложности программ.

Стоимость КС влияет на стоимость решения задачи, которая определяется стоимостью ресурсов, используемых задачей:



### 61.Проектирование кабельной системы КС

Структурированная кабельная система (СКС) — законченная совокупность кабелей связи и коммутационного оборудования, отвечающая требованиям соответствующих нормативных документов[[](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0#cite_note-.D0.93.D0.9E.D0.A1.D0.A2_.D0.A0_53246-2008-1). Включает набор кабелей и коммутационных элементов, и методику их совместного использования, позволяющую создавать регулярные расширяемые структуры связей в локальных сетях различного назначения. СКС — физическая основа инфраструктуры здания, позволяющая свести в единую систему множество сетевых информационных сервисов разного назначения: [локальные вычислительные сети](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) и [телефонные сети](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BB%D0%B5%D1%84%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C_%D0%BE%D0%B1%D1%89%D0%B5%D0%B3%D0%BE_%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F), системы безопасности, [видеонаблюдения](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%B4%D0%B5%D0%BE%D0%BD%D0%B0%D0%B1%D0%BB%D1%8E%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5) и т. д.

Кабельная система — это [система](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0), элементами которой являются кабели и компоненты, которые связаны с кабелем. К кабельным компонентам относится все пассивное коммутационное оборудование, служащее для соединения или физического окончания (терминирования) кабеля — телекоммуникационные розетки на рабочих местах, кроссовые и[коммутационные панели](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%B0%D0%BD%D0%B5%D0%BB%D1%8C) (жаргон: «патч-панели») в телекоммуникационных помещениях, муфты и сплайсы;

Любая СКС состоит из трёх иерархически организованных подсистем:

* магистральной кабельной подсистемы первого уровня;
* магистральной кабельной подсистемы второго уровня;
* горизонтальной кабельной подсистемы.

Кабельные кроссы служат интерфейсом между этими подсистемами, при этом подсистемы могут иметь различную топологию, например: «шина», «звезда» или «кольцо». Выделяется также кабельная подсистема рабочего места, часто непосредственно не относящаяся к СКС. Для построения структурированных кабельных систем используются кабели 5 и 6 категории, многопарные медные или волоконно-оптические. Наборы элементов и устройств для СКС состоят из разнообразных типов стоек и коммутационных шкафов, которые также делятся по типу формы и конструкции, напольного или настенного исполнения.

### 62.Логическое кодирование.Избыточные коды.Скремблирование

Логическое кодирование выполняется передатчиком до физического кодирования средствами физического уровня. На этапе логического кодирования борются с недостатками методов физического цифрового кодирования - отсутствие синхронизации, наличие постоянной составляющей. Сформированные исправленные последовательности данных затем с помощью методов физического кодирования передаются по линиям связи.

Логическое кодирование подразумевает замену бит исходной информационной последовательности новой последовательностью бит, несущей ту же информацию, но обладающей, кроме этого, дополнительными свойствами.

Различают два метода логического кодирования:

* избыточные коды;
* скремблирование.

*Избыточные коды* основаны на разбиении исходной последовательности бит на группы и замене каждой исходной группы в соответствии с заданной таблицей кодовым словом, которое содержит большее количество бит.

*Скремблирование* представляет собой "перемешивание" исходной последовательности данных таким образом, чтобы вероятность появления единиц и нулей на линии становилась близкой 0,5. Устройства (или программные модули), выполняющие такую операцию, называются скремблерами (scramble - свалка, беспорядочная сборка).

Скремблер в передатчике выполняет преобразование структуры исходного цифрового потока. Дескремблер в приемнике восстанавливает исходную последовательность бит. Практически единственной операцией, используемой в скремблерах и дескремблерах, является XOR - "побитное исключающее ИЛИ" (сложение по модулю 2).