# 0) Базовые понятия

**Вычислительная система** (ВС) – это совокупность ап­паратных и программных средств, предназначенных для обработки информации.

**Компьютерная сеть** – это совокупность компьютеров и сетевого оборудования, соединенных каналами связи.

**Вычислительная сеть (network) -** распределенная в пространстве система программных и аппаратных компонентов, связанных линиями компьютерной связи.

Физической основой вычислительной сети является **распределенная вычислительная среда.**

**Декомпозиция** - разбиение одной сложной задачи на несколько более простых задач-модулей.

В результате иерархической декомпозиции достигается:

* логическое упрощение задачи,
* относительная независимость уровней,
* возможность модификации отдельных модулей без изменения остальной части системы

При рассмотрении работы компьютера в сети можно выделить две основные подзадачи:

* взаимодействие программного обеспечения пользователя с физическим каналом связи в пределах одного компьютера,
* взаимодействие компьютера через канал связи с другим компьютером.

**Протокол** - правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты в разных узлах одного уровня.

**Интерфейс** - правила, с которыми взаимодействуют модули, реализующие протоколы соседних уровней и находящиеся в одном узле.

**Стек коммуникационных протоколов** - иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети.

# 1) Семиуровневая модель взаимодействия открытых систем

**Открытая система** – система, взаимодействующая с другими системами в соответствии с принятыми стандартами.

Сетевая модель OSI (The Open Systems Interconnection model) — сетевая модель посредством которой различные сетевые устройства могут взаимодействовать друг с другом.

Запрос, вырабатываемый на каком-либо уровне, передается на исполнение нижележащему уровню. Результаты обработки запроса передаются на вышележащий уровень.

Принято начинать описание уровней модели OSI с 7-го уровня, прикладного, на котором пользовательские приложения обращаются к сети.

7. Прикладной — решение функциональных задач

6. Представительный — преобразует данные в форму, понятную абонентам

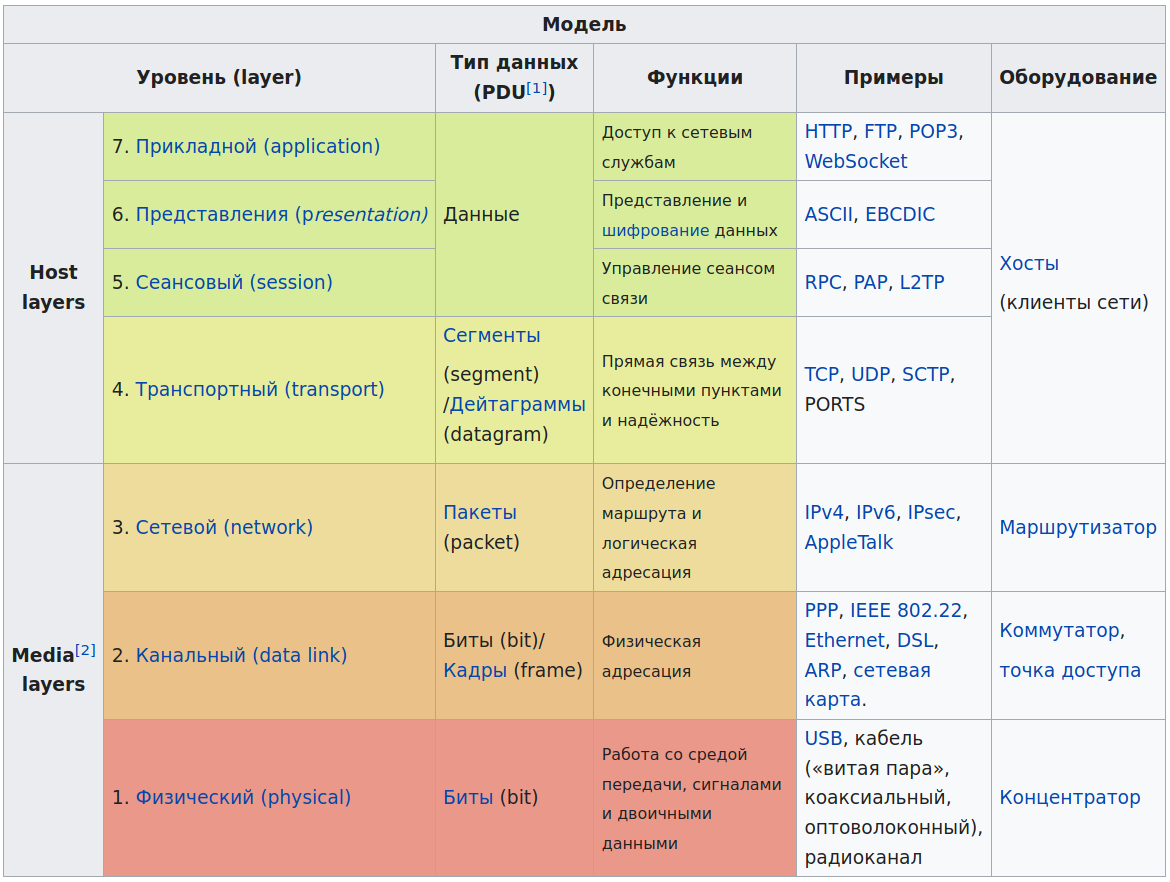
5. Сеансовый — организация диалога между прикладными процессами (управляет проведением сеансов связи)

4. Транспортный — сквозная передача абонентских сообщений, разбивает данные на множество сегментов

3. Сетевой уровень — выбор маршрута и передача данных(пакеты) от отправителя до адресата

2. Канальный уровень — передача между соседними узлами блоков данных (кадры/фреймы): определение доступности среды передачи данных и определение механизма обнаружения и коррекции ошибок

1. Физический уровень — передача потока бит между соседними узлами (отвечает за кодирование передаваемой информации в уровни сигналов, принятые в среде передачи, и обратное декодирование)



Архитектура Internet (4 уровня)

4. Прикладной (5-7)

3. Транспортный (4)

2. Сетевой (3)

1. Уровень сетевого доступа (1+2)

**Инкапсуляци**я

При отправке данных пакет проходит последовательно через все уровни программного обеспечения. На каждом уровне к пакету добавляется управляющая информация данного уровня (заголовок и концевик), которая необходима для успешной передачи данных по сети, как это показано на рис. 4, где Заг – заголовок пакета, Кон – конец пакета.

Каждый уровень модели взаимодействия открытых систем реагирует только на свой заголовок. Заголовки вышележащих уровней воспринимаются нижележащими уровнями как данные блока информации.

Преобразование форматов данных при приеме-передаче:

7-5) Сообщение, снабжаемое заголовком сеансового и представительного уровня.

4) Все разбивается на сегменты и добавляются у каждого сегмента свой заголовок транспортного уровня со служебной информацией.

3) Добавляются заголовки сетевого уровня и получаются пакеты (каждый пакет содержит один заголовок)

2) Добавляются заголовки канального уровня и получаются кадры

1) Добавляются флаги потока бит, которые позволяют выделить отдельный элемент в потоке бит.

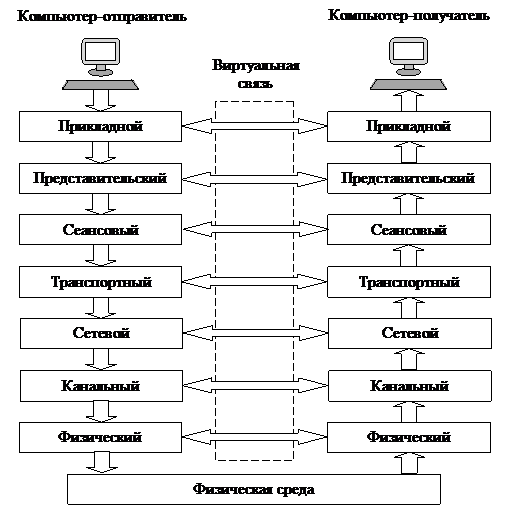
Вся эта процедура называется инкапсуляцией

# 

# 2) Взаимодействие уровневых протоколов

Каждый уровень компьютера-отправителя взаимодействует с таким же уровнем компьютера-получателя, как будто он связан напрямую. Такая связь называется логической или виртуальной связью. В действительности взаимодействие осуществляется между смежными уровнями одного компьютера.

Эта модель (OSI) содержит в себе, по сути, 2 различных модели – **вертикальную** и **горизонтальную.**



**По вертикали** данная среда представляется рядом логических уровней, на каждый из которых возложена одна из задач сети.

Вертикальная модель построена на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине. Соседние уровни обмениваются данными с использованием интерфейсов API.

**По горизонтали** информационно-вычислительная среда делится на локальные части (открытые системы), отвечающие требованиям и стандартам структуры открытых систем.

В горизонтальной модели двум программам требуется общий протокол для обмена данными (механизм взаимодействия программ и процессов на различных машинах).

* спецификацию услуг - что делает уровень
* спецификацию протокола - как он это делает

Итак, информация на компьютере-отправителе должна пройти через все уровни. Затем она передается по физической среде до компьютера-получателя и опять проходит сквозь все слои, пока не доходит до того же уровня, с которого она была послана на компьютере-отправителе.

Модель OSI описывает системные средства взаимодействия, реализуемые операционной системой, системными утилитами, системными аппаратными средствами. Модель не описывает взаимодействия приложений с конечным пользователем.

Любой протокол модели OSI должен взаимодействовать либо с протоколами своего уровня, либо с протоколами на единицу выше и/или ниже своего уровня. Взаимодействия с протоколами своего уровня называются горизонтальными, а с уровнями на единицу выше или ниже — вертикальными. Любой протокол модели OSI может выполнять только функции своего уровня и не может выполнять функций другого уровня

# 3) Требования предъявляемые к компьютерным сетям

1. Сеть должна быть системой открытой для расширения (новые узлы должны гармонично интегрироваться в сеть и не препятствовать работе уже существующий)
2. Сеть должна быть неоднородной (гетерогенной). Причем неоднородность должна быть и технической, и программной (в т.ч. разные ОС). Это необходимо для того, чтобы возможности подключения к сети не были ограничены платформой или архитектурой.
3. Сеть должна допускать функциональное расширение подсистемы. Чтобы ее можно было легко и без особых затрат модифицировать
4. Сеть должна быть надежной системой. Часто между узлами есть несколько путей (если сеть представлена в виде графа). Также встречается дублирование функциональности
5. Удобство сетевых служб. Работа на локальном компьютере не должна сильно отличаться от работы в сети
6. Сеть должна быть экономически эффективной системой. Инвестиции вложенные в создание сети должны сохраняться максимально долго

# 4) Классификация вычислительных сетей по протяженности

1. **Персональные** (Personal Area Network, **PAN**) позволяют общаться устройствам вблизи человека. PAN могут быть созданы на основе различных технологий.

Типичный пример — сеть, соединяющая компьютер с его периферийными устройствами. Присоединение монитора, клавиатуры, мыши, принтера и других устройств может быть основано как на использовании кабелей, так и быть беспроводным.

1. **Локальные** (ЛВС (LAN - Local Area Network)) - охватывающие ограниченную территорию (обычно в пределах удаленности станций не более чем на несколько десятков или сотен метров друг от друга, реже на 1...2 км);
2. **Корпоративные** (масштаба предприятия) - совокупность связанных между собой ЛВС, охватывающих территорию, на которой размещено одно предприятие или учреждение в одном или нескольких близко расположенных зданиях. Локальные и корпоративные вычислительные сети - основной вид вычислительных сетей, используемых в системах автоматизированного проектирования (САПР).
3. **Глобальные сети (**Wide Area Networks - WAN) — объединяют территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах, на различных континентах.

Территориальные - охватывающие значительное географическое пространство:

* сети региональные MAN (Metropolitan Area Network)
* сети глобальные WAN (Wide Area Network - общее англоязычное название для территориальных сетей)

Особо выделяют единственную в своем роде глобальную **сеть Internet** (реализованная в ней информационная служба World Wide Web (WWW) переводится на русский язык как всемирная паутина); это сеть сетей со своей технологией. В Internet существует понятие интрасетей (Intranet) - корпоративных сетей в рамках Internet.

# 5) Виды сигналов и способы представления информации

Сигнал формируется путём изменения тех или иных параметров физического носителя в соответствии с передаваемым сообщением и является функцией времени.

Все сигналы, применяемые в телекоммуникациях, можно разделить на 2 основных вида: аналоговые и цифровые. Основной признак такого разделения - способ представления информации: аналоговый или цифровой.

Изначально в природе вся информация возникает и воспринимается в аналоговом виде, т.е. непрерывно и определена для любого момента времени.

**Аналоговые сигналы -**функция от времени, применялись долгое время во всех видах связи: телефонной сети, телевизионного радиовещания, военной связи и т.п. Для борьбы с помехами при передаче данного вида сигнала обычно используется увеличение мощности, т.к. чем выше мешающее воздействие, тем выше должна быть мощность сигнала, чтобы он мог быть принят без искажения. При этом данный метод борьбы будет давать результаты до тех пор, пока усиливаемый сигнал не начнет оказывать влияние на другие каналы связи. Кроме того этот способ борьбы очень энергетически не эффективен, потому как очень большая энергия сигнала рассеивается на тепло.

Однако аналоговые сигналы имеют и преимущества. В частности если аналоговый сигнал (например, речь) передавать по цифровому каналу, то необходимо будет провести аналого-цифровое преобразование, в результате которого качество сигнала будет снижено. На приемном конце потребуется обратная процедура (цифро-аналоговое преобразование) которое также немного снизит качество сигнала. Если передавать аналоговую информацию по аналоговому каналу, то этого удастся избежать.

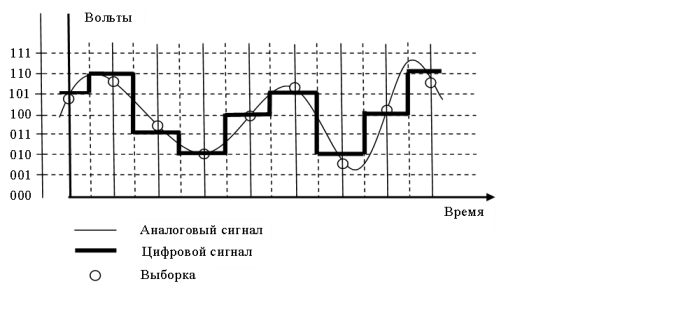
**Цифровой сигнал**

Цифровая информация – это набор конечных значений, т..е. она дискретна. Соответственно, цифровой сигнал определен только для отдельных моментов времени. Цифровую информацию принято кодировать двоичным кодом. Соответственно и цифровой сигнал, как правило, принимает одно из двух возможных значений (реже используется 3 и более значения, например, для увеличения помехозащищенности или информационной емкости элементов сигнала). Таким образом, цифровой сигнал, представляет собой последовательность резко сменяющих друг друга значений.

Цифровой сигнал имеет достаточно много преимуществ. Во-первых, он более помехоустойчив. Для защиты от ошибок в цифровой поток обычно вводится некоторая избыточность. Кроме того, цифровой сигнал энергетически эффективен, т.к. вводимая избыточность позволяет использовать меньшую мощность источника при передаче, чем при передаче аналогового сигнала. Также цифровой сигнал более эффективно использует выделяемые для передачи ресурсы связи.

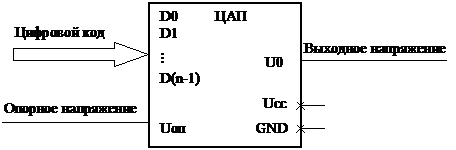
# 6) ЦАП и АЦП

Аналого-цифровой преобразователь **(АЦП)** — устройство, преобразующее входной аналоговый сигнал в цифровой сигнал. На вход подается аналоговый сигнал в виде тока или напряжения, происходит измерение соответствующей величины во многих точках оси времени.

На схеме амплитуда (вертикальная линия) разбита на 8 отрезков. На оси времени откладывается 8 интервалов. В построении ломаной линии участвуют промежутки между соседними временными отметками.

Цифро-аналоговый преобразователь **(ЦАП)** — устройство для преобразования цифрового (обычно двоичного) кода в аналоговый сигнал.

В общем случае микросхему ЦАП можно представить в виде блока, имеющего несколько цифровых входов и один аналоговый вход, а также аналоговый выход. Построение функции выходного напряжения производится с помощью процесса интерполяции по входным значениям.



# 7) Характеристики аналоговых сигналов. Гармонизация

Периодическим сигналом (например, ток или напряжение) называют такой вид воздействия, когда форма сигнала повторяется через некоторый интервал времени T, который называется периодом.

Простейшей формой периодического сигнала является **гармонический** сигнал или синусоида, все остальные сигналы являются негармоническими или несинусоидальными.

Основными характеристиками периодических аналоговых сигналов являются: **амплитуда**, **частота** и **фаза**

**Амплитуда** сигнала – это измерение, относящееся к величине напряжения сигнала, которое может быть положительным, нулевым или отрицательным.

Полное колебание сигнала называется циклом.

**Частота** – количество полных циклов в секунду. Частота измеряется в герцах (Гц).

**Фаза** сигнала представляет точку, которую достиг сигнал в цикле.

# 8) Принцип коммутации каналов и принцип коммутации пакетов(11.3 11.4)

Сравнительные показатели

a. Скорость передачи данных и задержка данных

b. Эффективность использования средств связи

c. Надежность

d. Реакция на перегрузку

Два вида трафика:

1) Компьютерные данные - лучше применять коммутацию пакетов. Необходимо поставлять без искажений, а скорость вторична.

2) Мультимедийный трафик (голос, видео...) - лучше применять коммутацию каналов. Главное - постоянная скорость, потери вторичны. Потери можно восстановить.

**Коммутация каналов**

Коммутация каналов – технология, при которой соединение устанавливается перед началом передачи данных (выделение линий).

Чтобы узел смог передать данные другому узлу, ему необходимо предварительно передать специальный запрос на установление соединения близлежащему коммутатору, этот коммутатор - следующему и т.д.

Таким образом при коммутации каналов коммутационная сеть образует между конечными узлами непрерывный составной физический канал из последовательно соединенных коммутаторами промежуточных канальных участков. Условием того, что несколько физических каналов при последовательном соединении образуют единый физический канал, является равенство скоростей передачи данных в каждом из составляющих физических каналов. Равенство скоростей означает, что коммутаторы такой сети не должны буферизовать передаваемые данные.

Достоинства технологии коммутации каналов:

1. Уменьшенное количество служебной информации (не передается адрес источника и назначения, ибо нет необходимости в этом при двухточечных каналах).
2. Коммутация каналов может использоваться на базе как цифровых, так и аналоговых.
3. Постоянная скорость передачи и высокая стабильность канала.

Недостатки технологии коммутации каналов:

1. Нерациональное использование пропускной способности канала (пропускной способности канала могло бы хватить больше, чем на двух абонентов). Невозможность динамического перераспределения пропускной способности представляет собой принципиальное ограничение сети с коммутацией каналов, так как единицей коммутации здесь является информационный поток в целом.
2. Возможен отказ в установлении соединения.

Перед тем как начать передачу сначала устанавливается соединение с абонентом. Проходит все через транзитные узлы. Затем когда соединение установлено отправляется обратный сигнал. Разумеется существует незначительная задержка между временем отправки и временем приема сигнала, чем больше расстояние между узлами, тем эта задержка существеннее.

1) Задержка и скорость передачи данных - постоянные величины (const)

2) Эффективность использования линий связи низкая при спорадическом трафике

3) Происходит накопление ошибок и как следствие падает надежность

4) Отказ в услуге в случае перегрузки

**Коммутация пакетов**

Коммутация пакетов – технология, при которой данные разбиваются на пакеты определенного размера, которые содержат в себе адрес источника и адрес назначения. В отличие от технологии коммутации каналов, коммутация пакетов осуществляет динамическую передачу данных абонентам, адреса которых берутся с полученных коммутационным оборудованием пакетов.

Таким образом, коммутация пакетов – технология доступа нескольких абонентов к общей сети. По одной физической линии данные могут передаваться многими узлами единовременно.

*Сообщение* - это логически завершенная порция данных — запрос на передачу файла, ответ на этот запрос, содержащий весь файл и т.д.

Пакет - сравнительно небольшая часть сообщения.

Пакеты обычно тоже могут иметь переменную длину, но в узких пределах, например от 46 до 1500 байт. Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета на узел назначения, а также номер пакета, который будет использоваться узлом назначения для сборки сообщения. Пакеты транспортируются по сети как независимые информационные блоки. Коммутаторы сети принимают пакеты от конечных узлов и на основании адресной информации передают их друг другу, а в конечном итоге — узлу назначения.

Такая схема передачи данных позволяет сглаживать пульсацию трафика на магистральных связях между коммутаторами и тем самым наиболее эффективно использовать их для повышения пропускной способности сети в целом.

Достоинства коммутации пакетов:

1. Высокая общая пропускная способность сети при передаче пульсирующего трафика.
2. Возможность динамически перераспределять пропускную способность физических каналов связи между абонентами в соответствии с реальными потребностями их трафика. Эффективность использования полосы пропускания (абонент, который не использует полосу, отдает ее другим).
3. При большом количестве абонентов не бывает отказа в обслуживании сети (типа, линия «занята»)
4. Данные передаются сразу, без установления соединения (пакеты передаются на коммутационное оборудование сразу после их формирования).

Особенности и недостатки коммутации пакетов:

1. Много служебной информации в пакетах (включая адресацию).
2. Сложность коммутационного оборудования (микропроцессорные устройства).
3. Работает только в цифровых сетях.
4. Неопределенность скорости передачи данных между абонентами сети, обусловленная тем, что задержки в очередях буферов коммутаторов сети зависят от общей загрузки сети.
5. Переменная величина задержки пакетов данных, которая может быть достаточно продолжительной в моменты мгновенных перегрузок сети.
6. Возможные потери данных из-за переполнения буферов.

Имеют место различные протоколы и процедуры. Есть процедуры с установлением связи и без. Сообщения разбиваются на пакеты, которые передаются отдельно друг от друга. Временная задержка также имеет место, но тут действует эффект параллелизма при конвейерной обработке из-за чего задержка существенно снижается.

1) Задержка и скорость являются функциями, зависящими от нагрузки

2) Высокая эффективность использования линий связи

3) Высокая надежность связи за счет использования алгоритмов с решающей обратной связью (на каждом участке переприема). Отправляется сообщение успешно прошел прием или нет, если нет, то отправка повторяется. Разумеется накопление ошибок отсутствует. Решающая обратная связь используется дважды (один раз в сумме отправитель-получатель).

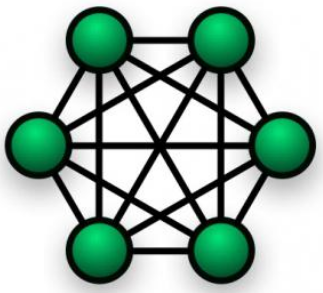
4) Реакция на перегрузки - ухудшение качества (характеристик) связи. Увеличивается задержка, снижается скорость передачи данных

# 9) Классификация вычислительных сетей по топологии(6)

**Под топологией** компьютерной сети обычно понимается физическое расположение компьютеров сети один относительно одного и способ соединения их линиями связи.

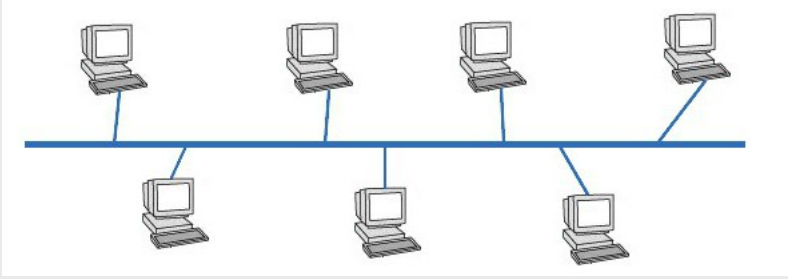
*Сетевая тополо́гия* — это конфигурация графа, вершинам которого соответствуют конечные узлы сети (компьютеры) и коммуникационное оборудование (маршрутизаторы), а рёбрам — физические или информационные связи между вершинами.

1) Полносвязная

Сеть, в которой каждый компьютер непосредственно связан со всеми остальными. Однако этот вариант громоздкий и неэффективный, потому что каждый компьютер в сети должен иметь большое количество коммуникационных портов, достаточное для связи с каждым из остальных компьютеров.

2) Неполносвязные

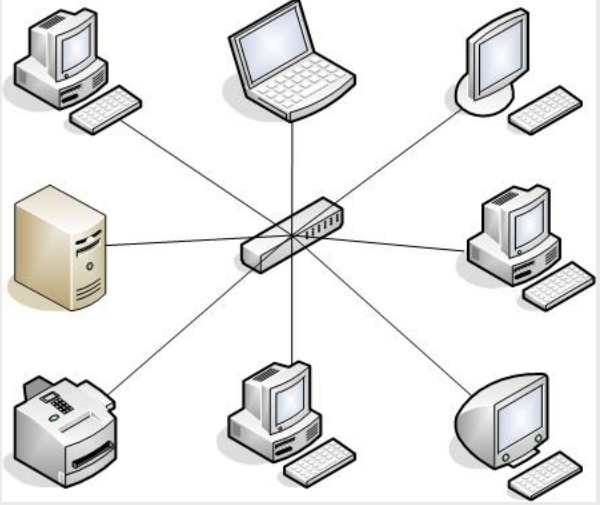
**Шина**

Топология данного типа представляет собой общий кабель (линия связи, шина или магистраль), к которому подсоединены все рабочие станции. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала.

При таком соединении компьютеры могут вести передачу только по очереди, потому что линия связи единственная.

**Звезда**

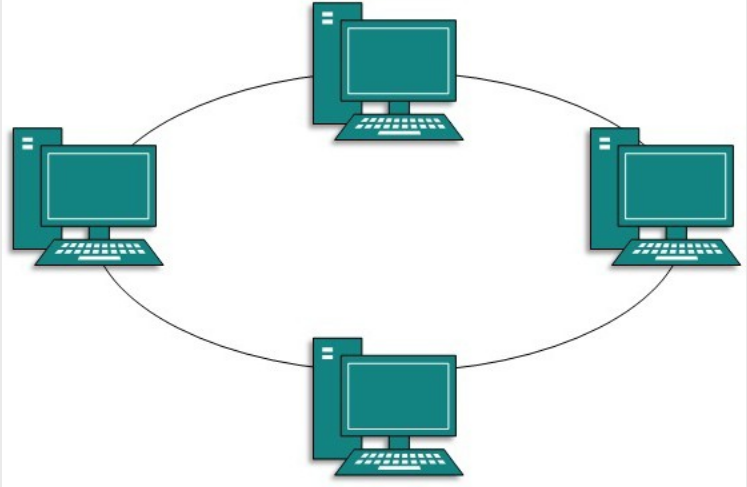
В сети, построенной по топологии типа «звезда», каждая рабочая станция подсоединяется кабелем к концентратору, или хабу. Концентратор обеспечивает параллельное соединение ПК и, таким образом, все компьютеры, подключенные к сети, могут общаться друг с другом.

Данные от передающей станции сети передаются через хаб по всем линиям связи всем ПК. Информация поступает на все рабочие станции, но принимается только теми станциями, которым она предназначается.

**Кольцо**

В сети с топологией типа «кольцо» все узлы соединены каналами связи в неразрывное кольцо, по которому передаются данные. Выход одного ПК соединяется со входом другого ПК. Начав движение из одной точки, данные, в конечном счете, попадают на его начало. Данные в кольце всегда движутся в одном и том же направлении.

Принимающая рабочая станция распознает и получает только адресованное ей сообщение.



# 10) Метод управления обменом(7)

[Сайт с инфой](https://sdo.nsuem.ru/mod/book/view.php?id=7617)

Сеть объединяет несколько абонентов, каждый из которых имеет право передавать свои пакеты. Однако одновременно по одному кабелю передавать несколько пакетов нельзя, иначе может возникнуть коллизия (конфликт), который приведет к искажению либо потере этих пакетов. Необходимо установить очередность доступа к сети (захвата сети) всеми абонентами, желающими передавать свои данные. Это относится, главным образом, к сетям с топологиями кольцо и шина.

В любой сети обязательно применяется тот или иной метод управления обменом (метод доступа, метод арбитража), предотвращающий или разрешающий конфликты между абонентами.

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 не может оперативно реагировать на все события в сети). Достоинство централизованных методов – отсутствие конфликтов.

**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 возможны конфликты, которые надо разрешать.

Децентрализованные методы управления сетевым обменом, в свою очередь, делят:

* *Детерминированные методы*, которые определяют четкие правила и порядок использования сети абонентами. Абоненты имеют определенную систему приоритетов, причем эти приоритеты различны для всех участников сетевого обмена. При этом конфликты полностью исключены (или маловероятны), однако некоторые абоненты могут дожидаться своей очереди на передачу определенное, но достаточно продолжительное время. К детерминированным методам относится, например, маркерный доступ (сети Token-Ring, FDDI), при котором право передачи передается по эстафете от предыдущего абонента к следующему.
* *Случайные методы*, которые подразумевают случайное (псевдослучайное) чередование абонентов, использующих сеть для передачи своих данных. При этом возможность конфликтов (коллизий) подразумевается, но предлагаются способы их разрешения. Случайные методы значительно хуже (по сравнению с детерминированными) работают при больших информационных нагрузках в сети (при большом сетевом трафик) и не гарантируют абоненту величину времени доступа. В то же время они, как правило, устойчивее к отказам сетевого оборудования и более эффективно используют сеть при невысокой интенсивности обмена. Характерным примером случайного метода служит – CSMA/CD.

**Управление обменом в сети с топологией звезда**

В топологии звезда чаще всего используют централизованный метод управления обменом. Это связано с тем, что все информационные потоки проходят через центр, и именно этому центру логично выполнять управление обменом в сети.

**Управление обменом в сети с топологией шина**

При топологии шина также возможно централизованное управление. Значительно чаще в шине используется децентрализованное случайное управление, так как сетевые адаптеры всех абонентов одинаковы, и именно этот метод наиболее органично подходит шинной топологии. При децентрализованном управлении все абоненты имеют равные права доступа к сети, а значит особенности топологии в большой степени совпадают с особенностями метода управления. Решение о возможности передавать свой пакет, принимается каждым абонентом, исходя из анализа состояния сети.

**Управление обменом в сети с топологией кольцо**

Самыми популярными методами управления в кольцевых сетях являются маркерные (эстафетные) которые используют небольшой управляющий пакет специального вида. Эстафетная передача маркера по кольцу позволяет передавать право на использования сети от одного абонента к другому. Маркерные методы относятся к децентрализованным и детерминированным методам управления сетевым обменом. В них отсутствует явно выраженный центр, но существует четкая система приоритетов, которая позволяет полностью избежать конфликтов.

# 11) Основные характеристики линии связи

[Сайт с инфой](http://ingraf.ru/kompus/setevik213.htm)

К основным характеристикам линий связи относятся:

* амплитудно-частотная характеристика;
* полоса пропускания;
* затухание;
* помехоустойчивость; Ethernet Локальные сети Глобальные сети
* перекрестные наводки на ближнем конце линии;
* пропускная способность;
* достоверность передачи данных;
* удельная стоимость.

В первую очередь разработчика вычислительной сети интересуют пропускная способность и достоверность передачи данных, поскольку эти характеристики прямо влияют на производительность и надежность создаваемой сети. Пропускная способность и достоверность - это характеристики как линии связи, так и способа передачи данных. Поэтому если способ передачи (протокол) уже определен, то известны и эти характеристики. Например, пропускная способность цифровой линии всегда известна, так как на ней определен протокол физического уровня, который задает битовую скорость передачи данных - 64 Кбит/с, 2 Мбит/с и т. п.

Однако нельзя говорить о пропускной способности линии связи, до того как для нее определен протокол физического уровня.

**Амплитудно-частотная характеристика** показывает, как затухает амплитуда синусоиды на выходе линии связи по сравнению с амплитудой на ее входе для всех возможных частот передаваемого сигнала.

**Полоса пропускания** - это непрерывный диапазон частот, для которого отношение амплитуды выходного сигнала ко входному превышает некоторый заранее заданный предел, обычно 0,5. То есть полоса пропускания определяет диапазон частот синусоидального сигнала, при которых этот сигнал передается по линии связи без значительных искажений.

**Затухание** определяется как относительное уменьшение амплитуды или мощности сигнала при передаче по линии сигнала определенной частоты. Таким образом, затухание представляет собой одну точку из амплитудно-частотной характеристики линии. Часто при эксплуатации линии заранее известна основная частота передаваемого сигнала, то есть та частота, гармоника которой имеет наибольшую амплитуду и мощность. Поэтому достаточно знать затухание на этой частоте, чтобы приблизительно оценить искажения передаваемых по линии сигналов.

Затухание А обычно измеряется в децибелах (дБ) и вычисляется по следующей формуле:

А = 10 log10 Рвых /Рвх,

где Рвых ~ мощность сигнала на выходе линии, Рвх - мощность сигнала на входе линии.

**Пропускная способность** (throughput) линии характеризует максимально возможную скорость передачи данных по линии связи. Пропускная способность измеряется в битах в секунду - бит/с, Кбит/с, Мбит/с, Гбит/с.

Пропускная способность линии связи зависит не только от ее характеристик, таких как амплитудно-частотная характеристика, но и от спектра передаваемых сигналов.

**Помехоустойчивость** линии определяет ее способность уменьшать уровень помех, создаваемых во внешней среде, на внутренних проводниках. Помехоустойчивость линии зависит от типа используемой физической среды, а также от экранирующих и подавляющих помехи средств самой линии. Наименее помехоустойчивыми являются радиолинии.

**Перекрестные наводки на ближнем конце** **(Near End Cross Talk - NEXT)** определяют помехоустойчивость кабеля к внутренним источникам помех, когда электромагнитное поле сигнала, передаваемого выходом передатчика по одной паре проводников, наводит на другую пару проводников сигнал помехи. Если ко второй паре будет подключен приемник, то он может принять наведенную внутреннюю помеху за полезный сигнал. Показатель NEXT, выраженный в децибелах, равен 10 log Рвых/Рнав, где Рвых - мощность выходного сигнала, Рнав - мощность наведенного сигнала.

**Достоверность передачи данных** характеризует вероятность искажения для каждого передаваемого бита данных. Иногда этот же показатель называют интенсивностью битовых ошибок (Bit Error Rate, BER).

# 12) Структура стандарта IEEE 802.x (7.5)

Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI.

*IEEE 802* — группа стандартов семейства IEEE (*Institute of Electrical and Electronics Engineers)*, касающихся локальных вычислительных сетей (LAN) и сетей мегаполисов (MAN)

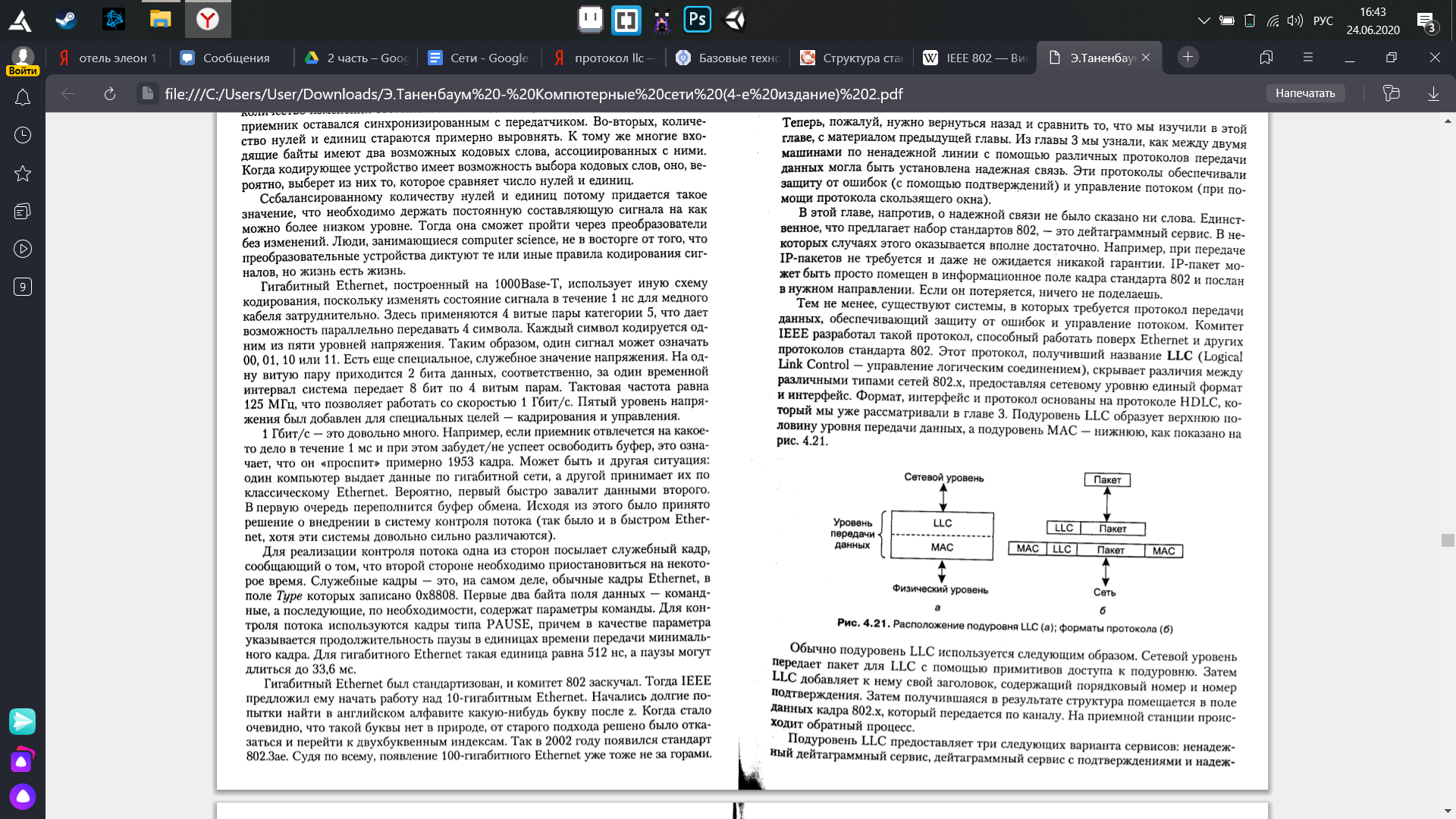
Службы и протоколы, указанные в IEEE 802, находятся на двух нижних уровнях (канальный и физический) семиуровневой сетевой модели OSI. Фактически IEEE 802 разделяет канальный уровень OSI на два подуровня — Media Access Control (MAC) и Logical Link Control (LLC).

Уровень LLC, действующий над уровнем МАС, отвечает за установление канала связи и за безошибочную посылку и прием сообщений с данными, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем.

Уровень МАС обеспечивает совместный доступ к физическому уровню, определение границ кадров, распознавание адресов назначения кадров. Этот уровень обеспечивает совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети. После того как доступ к среде получен, ею может пользоваться более высокий уровень – уровень LLC, организующий передачу логических единиц данных, кадров информации, с различным уровнем качества транспортных услуг. Через уровень LLC сетевой протокол запрашивает у канального уровня нужную ему транспортную операцию с нужным качеством.

# 13) Протокол LLC(11.1)

Существуют системы, в которых требуется протокол передачи данных, обеспечивающий защиту от ошибок и управление потоком. Комитет IEEE разработал такой протокол, способный работать поверх Ethernet и других протоколов стандарта 802. Этот протокол, получивший название LLC (Logical Link Control - управление логическим соединением), скрывает различия между различными типами сетей 802.x, предоставляя сетевому уровню единый формат и интерфейс. Формат, интерфейс и протокол основаны на протоколе HDLC. Подуровень LLC образует верхнюю половину уровня передачи данных, а подуровень MAC - нижнюю, как показано на рисунке.



Обычно подуровень LLC используется следующим образом: сетевой уровень передает пакет для LLC с помощью примитивов доступа к подуровню. Затем LLC добавляет к нему свой заголовок, содержащий порядковый номер и номер подтверждения. Затем получившаяся в результате структура помещается в поле данных кадра 802.x, который передается по каналу. На приемной станции происходит обратный процесс.

Подуровень LLC предоставляет три следующих варианта сервисов:

* ненадежный дейтаграммный сервис
* дейтаграммный сервис с подтверждениями
* надежный, ориентированный на соединение, сервис

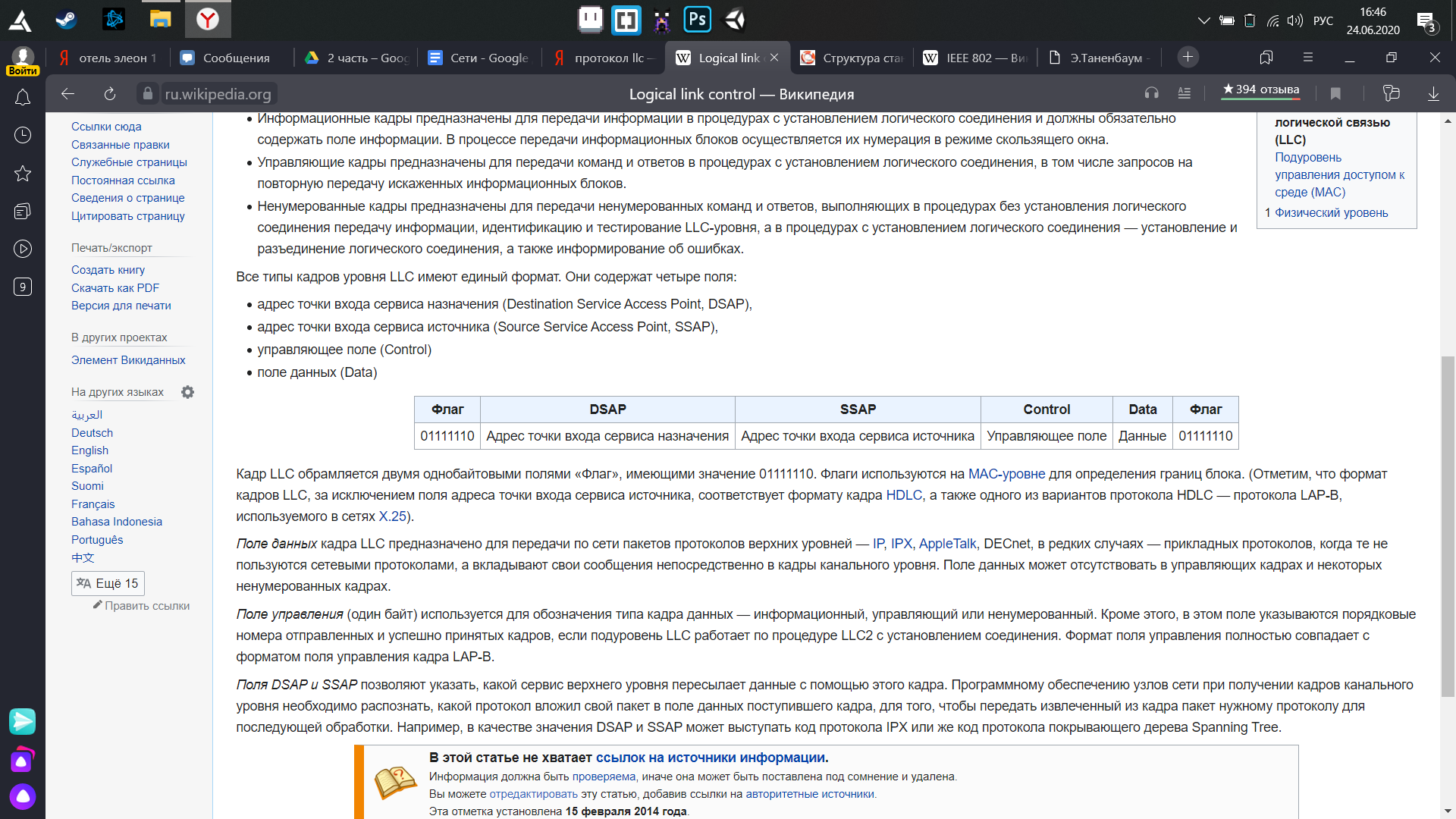
В заголовке LLC имеются три поля: целевая точка доступа, исходная точка доступа и контрольное поле. Точки доступа определяют, с какого процесса пришел кадр и какому процессу его нужно представить. Это аналог поля Type кадра DIX. Контрольное поле содержит порядковые номера и номера подтверждений, что также очень сильно напоминает стиль HDLC, однако форматы все-таки немного различаются. Эти поля используются в основном тогда, когда требуется надежное соединение на уровне передачи данных. Для передачи через Интернет IP-пакетов подтверждения на уровне LLC не требуется.

По своему назначению все кадры уровня LLC (называемые в стандарте [IEEE 802.2](https://ru.wikipedia.org/wiki/IEEE_802.2) блоками данных — Protocol Data Unit, PDU) подразделяются на три типа:

* *Информационные* кадры предназначены для передачи информации в процедурах с установлением логического соединения и должны обязательно содержать поле информации. В процессе передачи информационных блоков осуществляется их нумерация в режиме скользящего окна.
* *Управляющие* кадры предназначены для передачи команд и ответов в процедурах с установлением логического соединения, в том числе запросов на повторную передачу искаженных информационных блоков.
* *Ненумерованные* кадры предназначены для передачи ненумерованных команд и ответов, выполняющих в процедурах без установления логического соединения передачу информации, идентификацию и тестирование LLC-уровня, а в процедурах с установлением логического соединения — установление и разъединение логического соединения, а также информирование об ошибках.

Все типы кадров уровня LLC имеют единый формат. Они содержат четыре поля:

* адрес точки входа сервиса назначения (Destination Service Access Point, DSAP),
* адрес точки входа сервиса источника (Source Service Access Point, SSAP),
* управляющее поле (Control)
* поле данных (Data)



Кадр LLC обрамляется двумя однобайтовыми полями «Флаг», имеющими значение 01111110. Флаги используются на MAC-уровне для определения границ блока.

**Поле данных** кадра LLC предназначено для передачи по сети пакетов протоколов верхних уровней — IP, IPX, AppleTalk, DECnet, в редких случаях — прикладных протоколов, когда те не пользуются сетевыми протоколами, а вкладывают свои сообщения непосредственно в кадры канального уровня. Поле данных может отсутствовать в управляющих кадрах и некоторых ненумерованных кадрах.

**Поле управления** (один байт) используется для обозначения типа кадра данных — информационный, управляющий или ненумерованный. Формат поля управления полностью совпадает с форматом поля управления кадра LAP-B.

**Поля DSAP и SSAP** позволяют указать, какой сервис верхнего уровня пересылает данные с помощью этого кадра. Программному обеспечению узлов сети при получении кадров канального уровня необходимо распознать, какой протокол вложил свой пакет в поле данных поступившего кадра, для того, чтобы передать извлеченный из кадра пакет нужному протоколу для последующей обработки. Например, в качестве значения DSAP и SSAP может выступать код протокола IPX или же код протокола покрывающего дерева Spanning Tree.

# 14) Аппаратура физического и канального уровня(8.1 8.2)

**Канальный уровень:**

1. Отметим, что хотя драйверы сетевых карт не являются аппаратной частью, но они работают именно на втором уровне модели OSI.
2. [Коммутаторы](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) доступа, которые есть в каждом многоквартирном доме крупного города.

**Коммутатор** - устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети.

Коммутатор хранит в памяти (т.н. ассоциативной памяти) таблицу коммутации, в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует фреймы (кадры) и, определив MAC-адрес хоста-отправителя, заносит его в таблицу на некоторое время. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если MAC-адрес хоста-получателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты, за исключением того порта, с которого он был получен. Со временем коммутатор строит таблицу для всех активных MAC-адресов, в результате трафик локализуется.

**Физический уровень:**

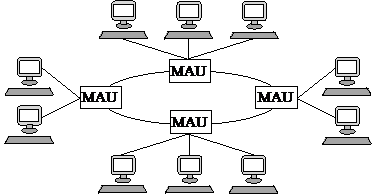
1. Медиаконвертер, который преобразует электрический сигнал в оптический и наоборот.
2. SFP (Small Form-factor Pluggable) модуль выполняется те же самые функции, что и медиаконвертер.
3. Концентратор. Концентратор – типичное устройство первого уровня модели OSI, которое на данный момент практически везде вытеснено коммутаторами. Принцип действия концентраторам очень прост: сигнал, приходящий на один из портов концентратора, ретранслируется на все порты, кроме того порта, откуда пришел сигнал.
4. Повторитель (усилитель сигнала). При передаче данных могут возникать всевозможные помехи (внутренние и внешние), которые уменьшают дальность передачи сигналов. Повторители увеличивают дальность передачи физического сигнала.
5. Всевозможные разъемы, коннекторы, розетки и делители сигнала.

# 15) Сеть TokenRing. Концентратор MAU. Схема управления сетью(9.1 9.2)

[TokenRing](https://www.sites.google.com/site/websitecomputernetworks/home/lection/2/2-7/2-7-1) — протокол передачи данных в локальной вычислительной сети (LAN) с топологией кольца и «маркерным доступом». Находится на канальном уровне (DLL - data link level) модели OSI.

Станции в локальной вычислительной сети Token Ring логически организованы в кольцевую топологию с данными, передаваемыми последовательно от одной станции в кольце к другой. Token Ring использует специальный трёхбайтовый блок данных, называемый **маркером**, который также перемещается по кольцу. Владение маркером предоставляет его обладателю право передавать данные.

Сеть Token-Ring имеет топологию кольцо, хотя внешне она больше напоминает звезду. Это связано с тем, что отдельные абоненты (компьютеры) присоединяются к сети не напрямую, а через специальные концентраторы или многостанционные устройства доступа (MSAU или MAU – Multistation Access Unit). Физически сеть образует звездно-кольцевую топологию. В действительности же абоненты объединяются все-таки в кольцо, то есть каждый из них передает информацию одному соседнему абоненту, а принимает информацию от другого.

Концентратор (MAU) при этом позволяет централизовать задание конфигурации, отключение неисправных абонентов, контроль работы сети и т.д. Никакой обработки информации он не производит.

Для каждого абонента в составе концентратора применяется специальный блок подключения к магистрали (TCU – Trunk Coupling Unit), который обеспечивает автоматическое включение абонента в кольцо, если он подключен к концентратору и исправен. Если абонент отключается от концентратора или же он неисправен, то блок TCU автоматически восстанавливает целостность кольца без участия данного абонента. Срабатывает TCU по сигналу постоянного тока (так называемый «фантомный» ток), который приходит от абонента, желающего включиться в кольцо. Абонент может также отключиться от кольца и провести процедуру самотестирования. «Фантомный» ток никак не влияет на информационный сигнал, так как сигнал в кольце не имеет постоянной составляющей

Концентратор в сети может быть единственным, в этом случае в кольцо замыкаются только абоненты, подключенные к нему. Внешне такая топология выглядит, как звезда. Если же нужно подключить к сети большое число абонентов, несколько концентраторов соединяют магистральными кабелями и образуют звездно-кольцевую топологию.

Существуют как пассивные, так и активные концентраторы MAU. Активный концентратор восстанавливает сигнал, приходящий от абонента (то есть работает, как концентратор Ethernet). Пассивный концентратор не выполняет восстановление сигнала, только перекоммутирует линии связи.

Активный концентратор восстанавливает сигнал, приходящий от абонента.

Активный концентратор (active hub) регенерирует, синхронизирует и усиливает сигналы при каждом их перемещении к следующему узлу. В результате удаленные узлы получают более мощный сигнал, что более чем в два раза. Увеличивает количество поддерживаемых узлов; при этом активный концентратор работает как повторитель.

Пассивный концентратор не выполняет восстановление сигнала и только перекоммутирует линии связи.

Пассивный концентратор (passive hub) лишь передает сигнал от станции к станции. Сигнал частично ослабляется при каждом прохождении через модуль MAU, что уменьшает максимальную пропускную способность сети.

Модули MAU используются исключительно в сетях с маркерным кольцом, где они могут выполнять следующие функции:

* соединять рабочие станции в логическое кольцо в рамках физической звездообразной топологии;
* передавать по кольцу маркер и фреймы;
* усиливать информационные сигналы;
* соединяться в последовательные цепочки для расширения маркерного кольца;
* обеспечивать правильное перемещение данных;
* отключать порты, связанные с неисправными узлами.

**Схема управления сетью**

Технология Token Ring является сложной технологией. Она обладает свойствами отказоустойчивости.

В сети Token Ring определены процедуры контроля работы сети, которые используют обратную связь кольцеобразной структуры — посланный кадр всегда возвращается в станцию-отправитель.

В некоторых случаях обнаруженные ошибки в работе сети устраняются автоматически, например, может быть восстановлен потерянный маркер. В других случаях ошибки только фиксируются, а их устранение выполняется вручную обслуживающим персоналом.

Для контроля сети одна из станций выполняет роль, так называемого, активного монитора.

Аппаратура активного монитора ничем не отличается от остальных, но его программные средства следят за временными соотношениями в сети и формируют в случае необходимости новый маркер.

Для различных видов сообщений, передаваемым кадрам, могут назначаться различные приоритеты: от 0 (низший) до 7 (высший). Решение о приоритете конкретного кадра принимает передающая станция (протокол Token Ring получает этот параметр через межуровневые интерфейсы от протоколов верхнего уровня, например прикладного). Маркер также всегда имеет некоторый уровень текущего приоритета. Станция имеет право захватить переданный ей маркер только в том случае, если приоритет кадра, который она хочет передать, выше (или равен) приоритета маркера. В противном случае станция обязана передать маркер следующей по кольцу станции.

За наличие в сети маркера, причем единственной его копии, отвечает активный монитор. Если активный монитор не получает маркер в течение установленного времени, он порождает новый маркер.

# 16) Технология Ethernet. Доступ к среде. Спецификации физической среды. Формат кадров. Использование коммутаторов (10)

Ethernet — это самый распространенный на сегодняшний день стандарт локальных сетей.

Одновременно все компьютеры сети имеют возможность немедленно (с учетом задержки распространения сигнала по физической среде) получить данные, которые любой из компьютеров начал передавать на общую шину.

Простота схемы подключения — это один из факторов, определивших успех стандарта Ethernet. Говорят, что кабель, к которому подключены все станции, работает в режиме коллективного доступа.

*Этапы доступа к среде.* Чтобы получить возможность передавать кадр, станция должна убедиться, что разделяемая среда свободна. Это достигается прослушиванием основной гармоники сигнала, которая также называется **несущей частотой**. Признаком незанятости среды является отсутствие на ней несущей частоты.

Если среда свободна, то узел имеет право начать передачу кадра. Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес пункта назначения в заголовке кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ. Адрес станции источника содержится в исходном кадре, поэтому станция-получатель знает, кому нужно послать ответ.

Если узел, готовый к передаче кадра, обнаруживает, что среда занята — на ней присутствует несущая частота, то он вынужден ждать, пока не прекратится передача кадра активным узлом.

После окончания передачи кадра все узлы сети обязаны выдержать технологическую паузу. Эта пауза, называемая также межкадровым интервалом, нужна для приведения сетевых адаптеров в исходное состояние, а также для предотвращения монопольного захвата среды одной станцией. После окончания технологической паузы узлы имеют право начать передачу своего кадра, так как среда свободна.

**Возникновение коллизии.** Механизм прослушивания среды и пауза между кадрами не гарантируют отсутствие возникновения коллизии - столкновении содержимого двух и более кадров и искажение информации при одновременной передаче кадров несколькими хостами.

Коллизия — это нормальная ситуация в работе сетей Ethernet и являются следствием распределенного характера сети.

Коллизия фиксируется передающей станцией, если обнаруживается, что передаваемые и наблюдаемые сигналы отличаются.

Обнаружившая коллизию передающая станция обязана прекратить передачу и сделать паузу в течение короткого случайного интервала времени. Затем она может снова предпринять попытку захвата среды и передачи кадра.

Очевидно, что вероятность успешного получения в свое распоряжение общей среды зависит от загруженности сети. При значительной интенсивности коллизий, например, работе приложений в реальном масштабе времени с мультимедийной информацией, полезная пропускная способность сети Ethernet резко падает, так как сеть почти постоянно занята повторными попытками передачи кадров.

Следует отметить, что метод доступа вообще не гарантирует станции, что она когда-либо сможет получить доступ к среде.

Этот недостаток метода случайного доступа — плата за его чрезвычайную простоту, которая сделала технологию Ethernet самой недорогой.

## Спецификации физической среды

**Физическая среда – коаксиальный кабель (стандарты 10Base-5 и 10Base-2). Классический Ethernet.**

Станция подключается к коаксиальному кабелю путем врезки приемопередатчика — трансивера. **Трансивер** — это часть сетевого адаптера, которая выполняет следующие функции:

* прием и передача данных с кабеля на кабель;
* определение коллизий на кабеле;
* электрическая развязка между кабелем и остальной частью адаптера;
* защита кабеля от некорректной работы адаптера.

Таким образом, коаксиальный кабель – это кабель многоточечный.

Стандарты

Физическая среда:

* 10Base-2 – тонкий коаксиал,
* 10Base-5 – толстый коаксиал.

Эти стандарты определяют возможность увеличения длины сети путем использования повторителя.

В классическом случае допускается установка четырех повторителей, что позволяет увеличить максимальную длину кабеля с 500 до 2500 м.

**Физическая среда - две неэкранированные витые пары**. **(Стандарт 10Base-T).**

Этот кабель предназначен для передачи голоса и используется для подключения телефонных аппаратов внутри зданий.

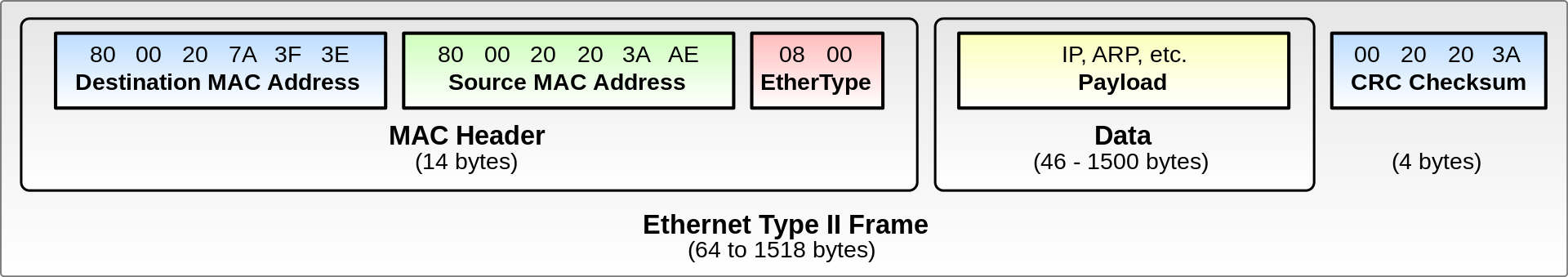
Очевидно, что использование технологии многоточечного кабеля в такой физической среде невозможно. Поэтому конечные узлы соединяются по топологии «точка-точка» многопортовым повторителем или концентратором

**Физическая среда - оптоволокно**

Функционально сеть Ethernet на оптическом кабеле состоит из тех же элементов, что и сеть стандарта 10Base-T — сетевых адаптеров, концентраторов и отрезков кабеля, соединяющих адаптер с портом повторителя.

Сети, построенные на основе стандарта 10Base-T, обладают по сравнению с коаксиальными вариантами Ethernet многими преимуществами. Эти преимущества связаны с разделением общего физического кабеля на отдельные кабельные отрезки, подключенные к центральному коммуникационному устройству. И хотя логически эти отрезки по-прежнему образуют общую разделяемую среду, их физическое разделение позволяет контролировать их состояние и отключать в случае обрыва, короткого замыкания или неисправности сетевого адаптера на индивидуальной основе.

## Форматы кадров технологии Ethernet



DA - адрес назначения, может быть индивидуальным или групповым.

* индивидуальный - это MAC-адрес узла-получателя.
* групповой адрес может предназначаться всем узлам сети (широковещательный адрес) или определенной группе узлов сети.

Несколько узлов могут быть (например, вручную) сконфигурированы как члены группы, номер которой указан в групповом адресе.

SA - адрес источника, узла - отправителя кадра.

L - длина поля данных в кадре (EtherType **?**).

Data - поле данных, может содержать от 0 до 1500 байт.

FCS - поле контрольной суммы.

Поскольку данный кадр является кадром МАС-подуровня, в соответствии со стандартом 802.2 в его поле данных Data вкладывается кадр подуровня LLC (DSAP : SSAP : Control) с удаленными флагами начала и конца кадра.

## Использование коммутаторов

Использование концентраторов и коммуникаторов позволило в рамках Ethernet достаточно просто реализовать и виртуальную ЛВС.

# 17) Сетевой уровень. Назначение и задачи. Дейтаграммная передача. Виртуальные каналы(12 13.1)

Доставкой данных между сетями занимается сетевой уровень, а внутри сети доставка данных регулируется канальным уровнем.

Сетевой уровень выполняет *функции*:

1. Создание сетевых соединений и идентификация их портов.
2. Обнаружение и исправление ошибок, возникающих при передаче через коммуникационную сеть.
3. Управление потоками пакетов.
4. Организация (упорядочение) последовательностей пакетов.
5. Маршрутизация и коммутация.
6. Сегментирование и объединение пакетов.

При организации доставки пакетов на сетевом уровне используется понятие номер сети. То есть, адрес получателя состоит из номера сети и номера компьютера в этой сети.

Сети соединяются между собой специальными устройствами, называемыми *маршрутизаторами*. Маршрутизатор собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения. Для того чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями, каждый раз выбирая подходящий маршрут.

Таким образом, маршрут представляет собой последовательность маршрутизаторов, по которым проходит пакет.

## Дейтаграммная передача

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 (транзитного или конечного) происходит только на основании адреса узла назначения, содержащегося в заголовке пакета.

Решение о том, какому узлу передать пришедший пакет, принимается на основе таблицы маршрутизации

## Виртуальные каналы

Механизм виртуальных каналов создает в сети устойчивые пути следования трафика через сеть с коммутацией пакетов.

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.

Маршрут от отправляющей до получающей машины прописывается в настройках системы и хранится в таблицах коммутации. Один и тот же маршрут используется для всего трафика, проходящего через данное соединение (именно так работает телефонная станция).

# 18) Протокол IP и IP-адресация(13.2)

IP (Internet Protocol — протокол сети Интернет) - сетевой протокол стека TCP/IP, который предоставляет адресную и маршрутную информацию; Его работа заключается в приложении максимума усилий (тем не менее, без всяких гарантий) по транспортировке дейтаграмм от отправителя к получателю, независимо от того, находятся эти машины в одной и той же сети или нет.

IP-адрес – 32 бита

У каждого хоста и маршрутизатора в Интернете есть IP-адрес, который может использоваться в полях Адрес отправителя и Адрес получателя IP-пакетов.

**Префиксы.** IP-адреса имеют иерархическую организацию. Первая часть 32-битного адреса имеет переменную длину и задает сеть, а последняя часть указывает на хост (получатель, принимающее устройство). Для всех хостов одной сети (например, ЛВС Ethernet) сетевая часть совпадает. Сети соответствует непрерывный блок пространства IP-адресов. Этот блок называется префиксом (prefix).

IP-адреса обычно записываются в виде четырех десятичных чисел (которые соответствуют отдельным байтам), разделенных точками. Например, шестнадцатеричный адрес 80D00297 записывается как 128.208.2.151 (151 – номер хоста).

По традиции размер префикса задается после префикса IP-адреса в виде слэша и длины сетевой части в битах, например, 128.208.2.0/24 (24 – длина префикса в битах).

Длина префикса соответствует двоичной маске, в которой единицы указывают на сетевую часть. Такая маска называется маской подсети (subnet mask).

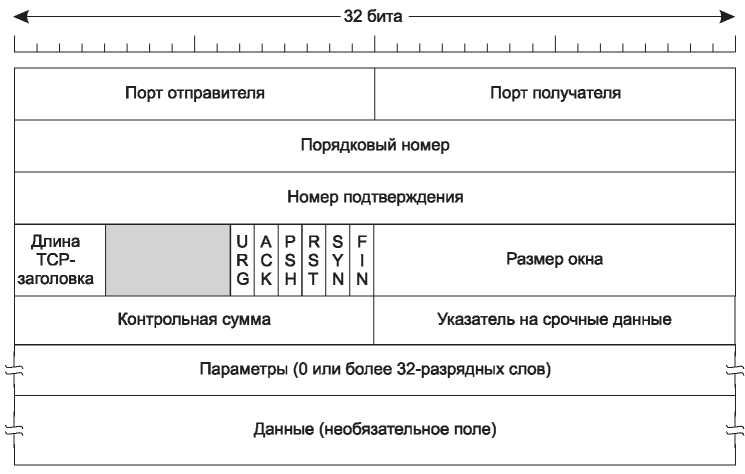
Выполнение операции И между маской и IP-адресом позволяет выделить сетевую часть.



# 19) Транспортный уровень. Назначение. Протокол TCP. Понятие скользящего окна(14)

Конечная цель транспортного уровня заключается в предоставлении эффективных, надежных и экономичных услуг (сервисов) передачи данных своим пользователям, которыми обычно являются процессы прикладного уровня. Для достижения этой цели транспортный уровень пользуется услугами, предоставляемыми сетевым уровнем. Программа и/или аппаратура, выполняющая работу транспортного уровня, называется **транспортной подсистемой** или **транспортным объектом**. Транспортная подсистема может располагаться в ядре операционной системы, в библиотечном модуле, загруженном сетевым приложением, в отдельном пользовательском процессе или даже в сетевой интерфейсной плате. Первые два варианта чаще всего встречаются в сети Интернет.

## TCP



Ключевым свойством TCP, определяющим всю структуру протокола, является то, что в TCP-соединении у каждого байта есть свой 32-разрядный порядковый номер. Отдельные 32-разрядные порядковые номера используются для указания позиции скользящего окна в одном направлении и подтверждений в обратном направлении.

Поля “Порт получателя” и “Порт отправителя” являются идентификаторами локальных конечных точек соединения. Этот идентификатор соединения включает пять инфо

рмационных составляющих: протокол (TCP), IP-адрес источника, порт источника, IP-адрес получателя и порт получателя.

Поля “Порядковый номер” и “Номер подтверждения” выполняют свою обычную функцию. Поле “Номер подтверждения” относится к следующему по порядку ожидаемому байту, а не к последнему полученному, таким образом, один номер объединяет в себе информацию обо всех полученных данных. Сфера его применения не выходит за рамки потерянных данных.

Поле Длина TCP-заголовка содержит размер TCP-заголовка, выраженный в 32-разрядных словах.

Далее 1-битовые флаги:

URG – срочное сообщение,

ACK – квитанция на принятый сегмент,

PSH – запрос на передачу сообщения без ожидания заполнения буфера,

RST – запрос на восстановление соединения,

SYN – сообщение, используемое для синхронизации счетчиков переданных данных при установлении соединения,

FIN – признак достижения передающей стороной последнего байта в потоке передаваемых байтов.

Управление потоком в протоколе TCP осуществляется при помощи скользящего окна переменного размера

## Скользящее окно

Для регулирования потока данных между устройствами в протоколе TCP используется механизм управления потоком. Принимающий протокол TCP сообщает посылающему протоколу TCP размер окна. Этот размер задает количество байтов, начиная с номера подтверждения, которое принимающий TCP готов принять на текущий момент.

В протоколе TCP используются “ожидательные” подтверждения, означающие, что номер подтверждения соответствует ожидаемому следующим байту.. Слово "скользящее" в термине скользящее окно отражает тот факт, что размер окна согласуется динамически во время TCP-сеанса. Использование скользящего окна приводит к более эффективному использованию хост-машиной полосы пропускания, поскольку больший размер окна позволяет передавать больший объем данных, откладывая момент получения подтверждения. ([доп. статья](https://zvondozvon.ru/tehnologii/protokoli/tcp))

# 20) Задачи сеансового и представительного уровня(15.1)

## Сеансовый уровень OSI

Основные задачи сеансового уровня:

1. установление способа обмена сообщениями (дуплексный или полудуплексный);
2. синхронизация обмена сообщениями;
3. организация "контрольных точек" диалога.

Протокол сеансового уровня обеспечивает управление диалогом: фиксирует, какая из сторон является активной в данный момент, предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться обратно к последней контрольной точке, а не начинать все сначала. На практике некоторые дополнения используют сеансовый уровень, и он редко реализуется в виде отдельных протоколов, хотя функции этого уровня часто совмещают с функциями прикладного уровня и реализуют в одном протоколе.

## Представительный уровень OSI

Основные задачи представительского уровня:

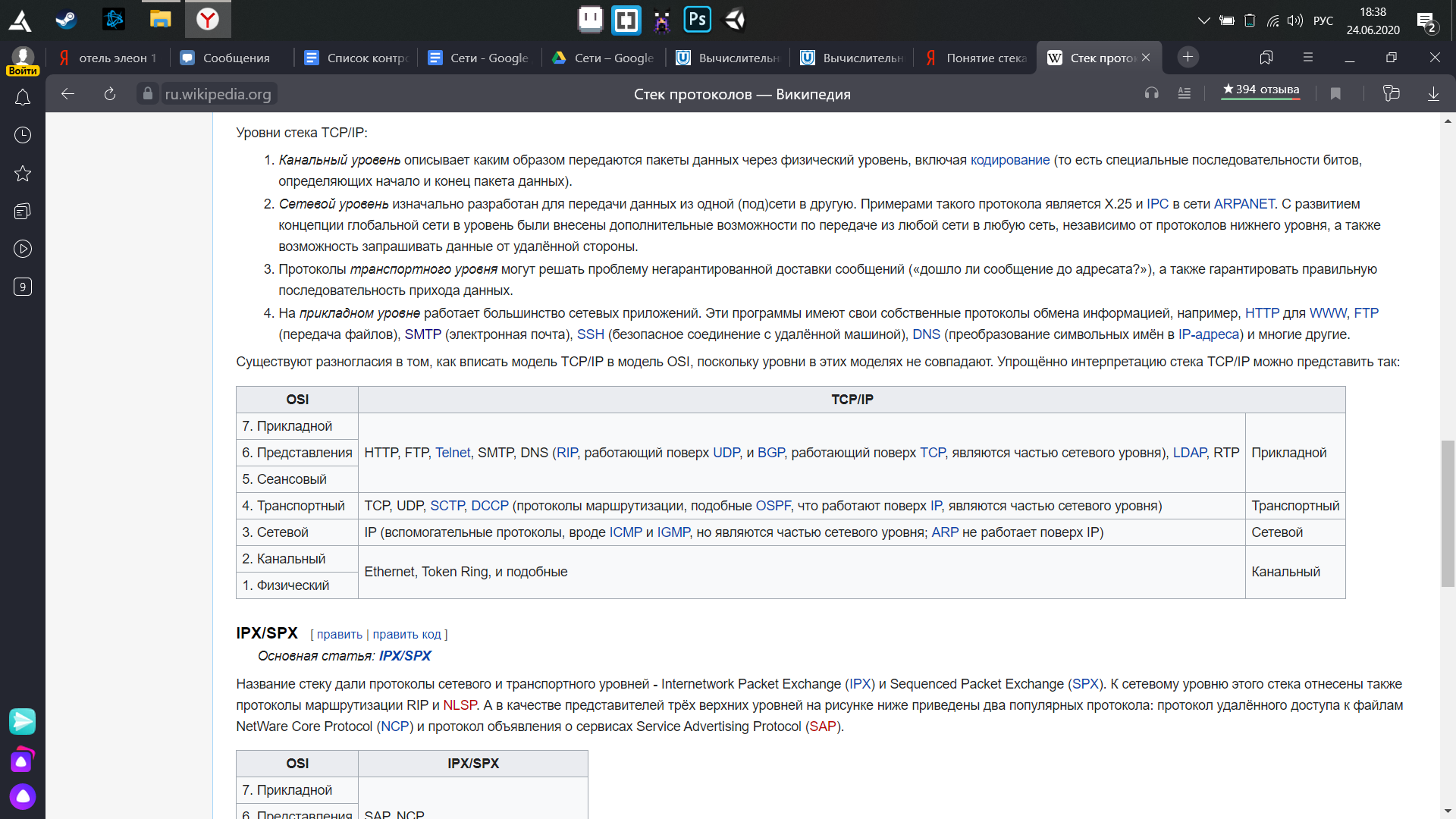
1. превращение данных из внешнего формата во внутренний;
2. шифровка и расшифровка данных;

Представительный уровень имеет дело с формой представления переданной по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, переданная прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут перебороть синтаксические расхождения в представлении данных или же расхождения в кодах символов, например кодов ASCII и EBCDIC. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которой секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является протокол Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

# 21) Понятие стека протоколов. Иерархия протоколов TCP/IP

Стек протоколов — это иерархически организованный набор сетевых протоколов, достаточный для организации взаимодействия узлов в сети.

Стек протоколов TCP/IP — набор сетевых протоколов, на которых базируется Интернет. Обычно в стеке TCP/IP верхние 3 уровня (прикладной, представления и сеансовый) модели OSI объединяют в один — прикладной.



# 22) Служба имен доменов DNS. Пространство имен DNS(15.2)

Хотя программы теоретически могут обращаться к веб-страницам, почтовым ящикам и другим ресурсам по сетевым адресам компьютеров (например, IP-адрес 128.111.24.41), такое обращение обладает недостатками;

* пользователям тяжело запоминать такие адреса;
* в случае переезда сервера компании на новую машину новый IP будет необходимо сообщить всем заинтересованным лицам.

Для отделения имён машин от их адресов было решено использовать понятные имена высокого уровня.

Суть системы DNS (Domain Name System) заключается в иерархической схеме имён, основанной на доменах, и распределенной базе данных, реализующей эту схему имён.

В общих чертах система DNS применяется следующим образом. Для преобразования имени в IP-адрес прикладная программа обращается к библиотечной процедуре, называющейся распознавателем, передавая ей имя в качестве параметра. Распознаватель посылает запрос, содержащий имя, локальному DNS-серверу, который ищет имя в БД и возвращает соответствующий IP-адрес распознавателю, который, в свою очередь, передает этот адрес вызвавшей его прикладной программе. Запрос и ответ передаются как UDP-пакеты. Имея IP-адрес, программа может установить TCP-соединение с адресатом или послать ему UDP-пакеты (при дейтаграммной передаче).

Пространство имён DNS

Домен (в Интернете) - имя множества хостов, объединенных в логическую группу. То есть, иерархия имен хостов – это иерархия имен доменов.

За каждым государством в соответствии с международным стандартом ISO 3166 закреплен один домен государства.

# 23) Система именования интернет ресурсов (URI)(15.2)

С каждым ресурсом, размещенным в Интернете (документом, рисунком, архивным файлом и т.д.) сопоставляется значение (гиперссылка), по которому можно однозначно определить его расположение -- универсальный идентификатор ресурса URI (Uniform Resource Identifier).

URI включает три компоненты: протокол (который также называют схемой), DNS-имя машины, на котором расположен ресурс, и путь, уникально определяющий ресурс (веб-страницу, файл для чтения, программу, предназначенную для запуска на машине).

В общем случае путь представляется иерархическим именем, которое моделирует структуру каталогов файлов.

Существует две разновидности URI:

* URL - это URI, указывающее, как определить местонахождение ресурса, то есть «где» и «как» (каким методом, протоколом) найти.
* URN - унифицированное имя ресурса (Uniform Resource Name ); указывает имя ресурса, то есть, «что требуется найти», но не место его нахождения.

# 24) Протокол HTTP. Сторона клиента. Сторона сервера(15.4)

Самым распространенным протоколом прикладного уровня в настоящее время является протокол передачи гипертекстовой информации (Hypertext Transfer Protocol – HTTP),

Его основным приложением является веб-браузер, который отображает данные веб-страниц, используя текст, графику, звук и видео.

HTTP — простой протокол, работающий по принципу запрос-ответ, который обычно запускается через TCP. Он определяет, какие сообщения клиент может отсылать на серверы и какие получать ответы.

[Клиент-сервер](http://falbar.ru/article/frontend-ili-bekend-klientskaya-ili-servernaya-storona)

## Сторона клиента

По сути дела, браузер — это программа, которая может отображать веб-страницы и распознавать щелчки мыши на элементах активной страницы - гиперссылках. При выборе элемента браузер следует по гиперссылке и получает с сервера запрашиваемую страницу.

Клиент – это программное обеспечение, которое работает на компьютере пользователя (ноутбуке, iPad, смартфоне) и может взаимодействовать с сервером.

## Сторона сервера

В основном цикле сервер выполняет следующие действия:

1. Принимает входящее TCP-соединение от клиента (браузера).

2. Получает путь к странице, являющийся именем запрашиваемого файла.

3. Получает файл (с диска).

4. Высылает содержимое файла клиенту.

5. Разрывает TCP-соединение.

В случае, если контент является динамическим, третий шаг может быть заменен запуском программы (определенной по пути), возвращающей контент.

Сервер принимает данные от пользователя (его имя, адрес электронной почты и т. д.) и сохраняет их для дальнейшего использования.

# 25) Протоколы передачи файлов(16.1)

Протокол передачи файлов (File Transfer Protocol – FTP) – служба, ориентированная на предварительное соединение (connection-oriented), которая взаимодействует с протоколом транспортного уровня TCP.

Главная цель протокола FTP состоит в том, чтобы передавать файлы от одного компьютера другому или копировать и перемещать файлы от серверов клиентам и от клиентов серверам. Это является главным отличием от протокола HTTP, который позволяет клиенту "скачивать" файлы с сервера, но не позволяет пересылать файлы на сервер.

Шаги протокола.

1. Протокол передачи файлов FTP сначала устанавливает соединение между клиентом и сервером, используя команды запроса клиента и ответы сервера (номер порта – 21).
2. Производится обмен данными (номер порта – 20). Передача данных может производиться в режиме кода ASCII или в двоичном коде. Эти режимы определяют кодирование, используемое для файла данных, которое в модели OSI является задачей представительского уровня.
3. После завершения передачи файла соединение для передачи данных заканчивается автоматически.

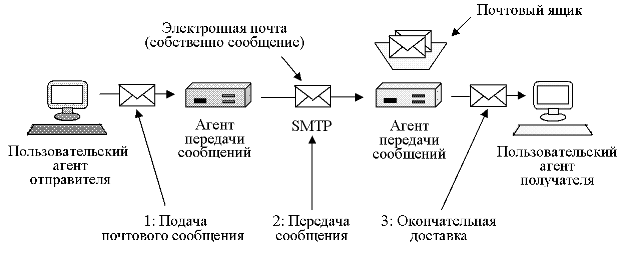
Управление сеансом связи происходит на сеансовом (Session) уровне.

Простой протокол передачи файлов (Trivial File Transfer Protocol – TFTP) – служба без установления соединения.

Протокол TFTP характеризует простота и малый объем программного обеспечения. Он может читать или записывать файлы при соединении с сервером, но не ведет списки и каталоги. Поэтому протокол TFTP работает быстрее, чем протокол FTP.

<https://ru.wikipedia.org/wiki/FTP>

# 26) Протоколы передачи почты(16.2)



Система электронной почты состоит из двух подсистем: пользовательских агентов, позволяющих пользователям читать и отправлять электронную почту, и агентов передачи сообщений, пересылающих сообщения от отправителя к получателю.

Почтовые серверы, как правило, являются системными процессами. Они работают в фоновом режиме на машинах почтовых серверов и всегда должны быть доступными. Они должны автоматически перемещать почтовые сообщения по системе от отправителя получателю при помощи SMTP (Simple Mail Transfer Protocol — простого протокола передачи почтовых сообщений).

SMTP отсылает сообщения по соединениям и высылает обратно отчёты о статусе доставки и любых возникших ошибках.

За связь пользовательских агентов и почтовых серверов отвечают почтовые ящики и стандартный формат почтовых сообщений.

**Простая передача сообщений между почтовыми серверами, их доставляющими.**

Установив TCP-соединение с портом 25, передающая машина, выступающая в роли клиента, ждет запроса принимающей машины, работающей в режиме сервера.

Сервер начинает диалог с того, что посылает текстовую строку, содержащую его идентификатор и сообщающую о его готовности (или неготовности) к приему почты. Если сервер не готов, клиент разрывает соединение и повторяет попытку позднее.

Если сервер готов принимать почту, клиент объявляет, от кого поступила почта и кому она предназначается. Если получатель почты существует, сервер дает клиенту добро на пересылку сообщения. Затем клиент посылает сообщение, а сервер подтверждает его получение.

<https://ru.wikipedia.org/wiki/SMTP>

<https://ru.wikipedia.org/wiki/POP3>

<https://ru.wikipedia.org/wiki/IMAP>

# 

# Всякое

Соседние уровни обмениваются данными с использованием интерфейсов API

Протоколы сетевого уровня:

* IP (Internet Protocol) протокол Internet, сетевой протокол стека TCP/IP, который предоставляет адресную и маршрутную информацию
* IPX (Internetwork Packet Exchange) протокол межсетевого обмена пакетами, предназначенный для адресации и маршрутизации пакетов в сетях Novell
* X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов (частично этот протокол реализован на уровне 2)  
  CLNP (Connection Less Network Protocol) сетевой протокол без организации соединений

На практике большинство хостов подключены к одной сети, следовательно, имеют один адрес, а маршрутизаторы обычно имеют несколько интерфейсов и, следовательно, несколько IP-адресов

Порты файлов 20 21

Порты почты 143 25

http 80

**Для чего используется логическое кодирование?**

Используется для уменьшения длинных последовательностей одинаковых бит, приводящие к неизменному потенциалу(потому что спектр уже, следовательно выше скорость), вставками бинарных единиц.

[статья по логическому кодированию](http://just-networks.ru/tekhnologii-fizicheskogo-urovnya/logicheskoe-kodirovanie)

**Логическое кодирование** повышает надежность синхронизации устройств, подключенных к линии связи (обеспечивает надежное выделение тактовой частоты непосредственно из принимаемого сигнала), и уменьшает уровень помех, излучаемых на соседние линии многожильного кабеля.

Другая область применения скремблеров — защита передаваемой информации от несанкционированного доступа. Повышает надежность синхронизации устройств, подключенных к линии связи (обеспечивает надежное выделение тактовой частоты непосредственно из принимаемого сигнала), и уменьшает уровень помех, излучаемых на соседние линии многожильного кабеля.

Скремблер - шифровальное устройство; устройство, выполняющее скремблирование (обратимое преобразование цифрового потока с целью получения свойств случайной последовательности).

Скрэмблирование (перемешивание данных скремблером) это второй способ логического кодирования. Методы скремблирования заключаются в побитном вычислении результирующего кода на основании бит исходного кода и полученных в предыдущих тактах бит результирующего кода.Скрэмблирование (перемешивание данных скремблером) это второй способ логического кодирования. Методы скремблирования заключаются в побитном вычислении результирующего кода на основании бит исходного кода и полученных в предыдущих тактах бит результирующего кода.

Физическое кодирование - представление дискретных сигналов, передаваемых по цифровому каналу связи, с целью передачи данных, представленных в цифровом виде, на расстояние по физическому каналу связи.

Механизм виртуальных каналов создает в сети устойчивые пути следования трафика через сеть с коммутацией пакетов.

[Сети с виртуальными каналами — Компьютерные сети](http://conlex.kz/seti-s-virtualnymi-kanalami/)

[Дейтаграммные сети — Компьютерные сети](http://conlex.kz/dejtagrammnye-seti/)

PAT [https://ru.wikipedia.org/wiki/Трансляция\_порт-адрес](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B0%D0%BD%D1%81%D0%BB%D1%8F%D1%86%D0%B8%D1%8F_%D0%BF%D0%BE%D1%80%D1%82-%D0%B0%D0%B4%D1%80%D0%B5%D1%81)

Инкапсуляция [https://ru.wikipedia.org/wiki/Инкапсуляция\_(компьютерные\_сети)](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))

Про ЦАП и АЦП <https://principraboty.ru/cap-princip-raboty/>

**Через какой параметр осуществляется управление передачей между конечными пользователями?** (окно)

**Через какой параметр осуществляется передача данных программам?** (порт)

**За счёт чего происходит экономия IP адресов?** (за счёт повторного использования адресов благодаря технологии NAT (а точнее, по его словам, PAT), локальные адреса преобразуются в один глобальный, но с уникальными портами, а с глобального по портам уже получаются локальные адреса)

**PAT:** IP-пакеты, поступающие на маршрутизатор, в зависимости от адреса порта получателя транслируются с различными адресами — порты 80 и 443 направляются на один сервер (10.0.0.2), порты 25 и 110 - на второй (10.0.0.3), 53 - на третий (10.0.0.4), 53 на четвертый (10.0.0.5). Соответствующим же образом производится и трансляция ответов серверов (в этом случае заменяется адрес отправителя). В соответствии с этим есть два типа сети: внутренняя (nat inside) и внешняя (nat outside). У пакетов, приходящих из наружной сети, меняется адрес получателя, у пакетов из внутренней — отправителя. Для обеспечения распределения нагрузки пакеты могут направляться на различные сервера для одного и того же порта поочередно (это работает только для протоколов, не требующих установления соединения и не имеющих понятия «текущее состояние»

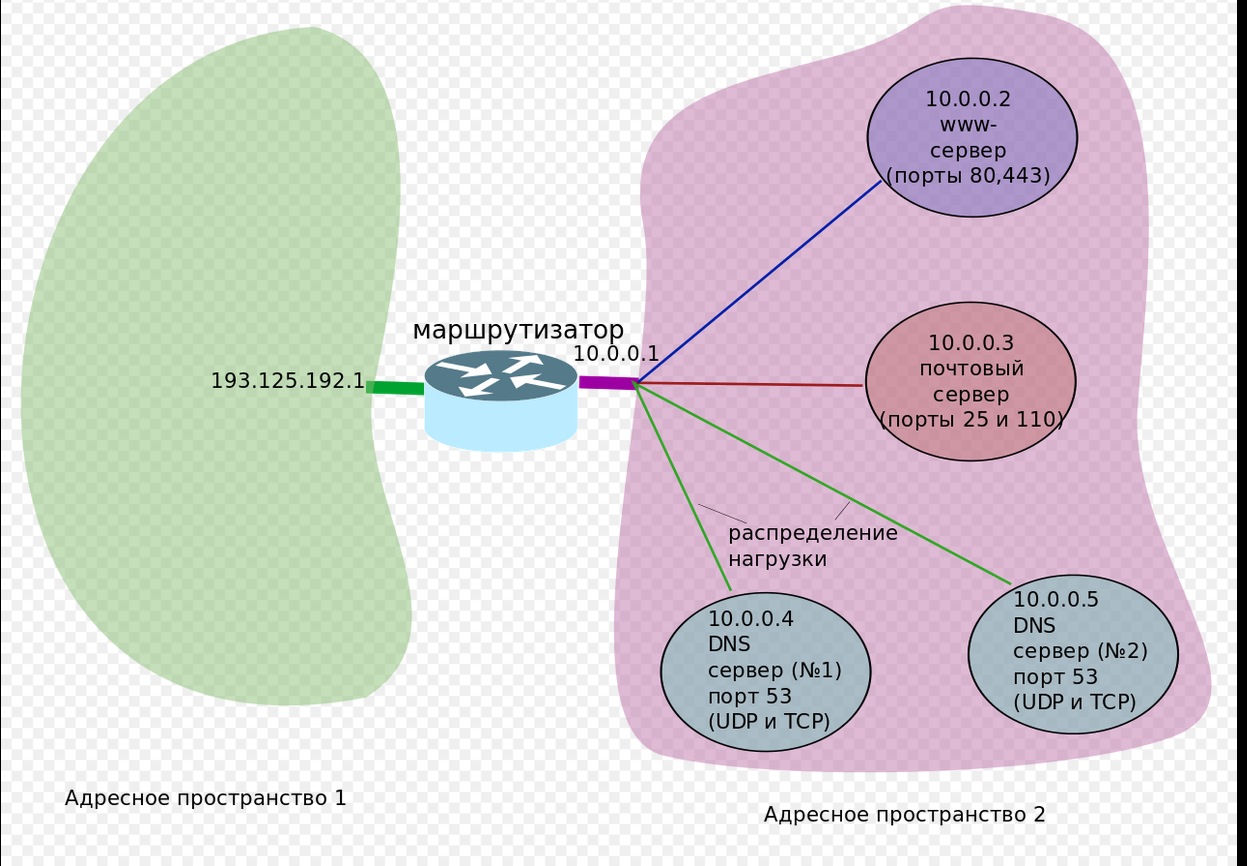
**Почему маршрутизаторы имеют несколько ip адресов**

**Сколько адресов имеет маршрутизатор?**

[Принцип работы маршрутизации](https://zvondozvon.ru/tehnologii/kompyuternye-seti/marshrutizatsiya)

[Маршрутизатор](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) (для примера ниже) имеет два интерфейса (например, адрес 193.125.192.1, на который поступают запросы и для которого производится трансляция, и адрес 10.0.0.1, который обращен в сторону сети с серверами).

На практике большинство хостов подключены к одной сети, следовательно, имеют один адрес, а маршрутизаторы обычно имеют несколько интерфейсов и, следовательно, несколько IP-адресов



**Ты маршрутизатор и к тебе пришёл пакет данных, как ты с помощью таблицы маршрутизации его отправишь дальше?** **А что кроме адреса понадобится?** (ответ - порт)

Я пакет - я пришел, а я маршрутизатор.

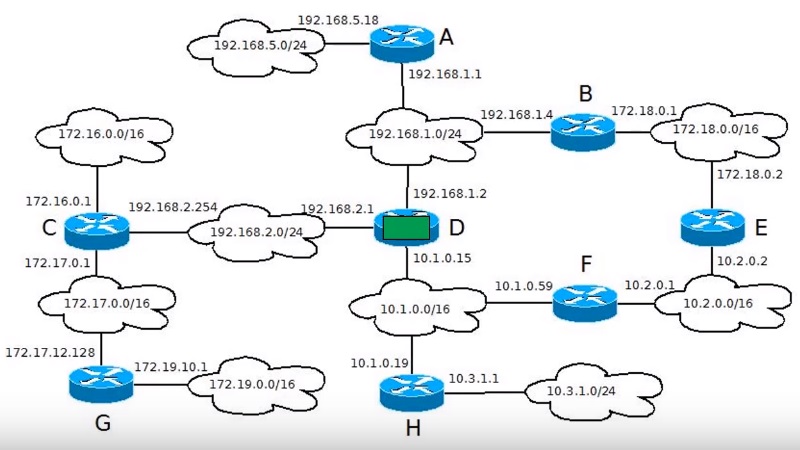
Пришел адрес, смотрим подключение сети. Если в этой сети, то находим по арп запросу мак-адрес компьютера

Если не в этой не сети, то находим следующий маршрутизатор.

В пакете достаем сначала адрес узла назначения, из первой строки таблицы выбираем маску, накладываем на адрес выбранный из пакета, получили адрес подсети получателя. Смотрим по таблице подключения к маршрутизатору. Поле подсеть назначения в таблице, с ним сравниваем. Если совпали находим, если нет к следующей строке

---

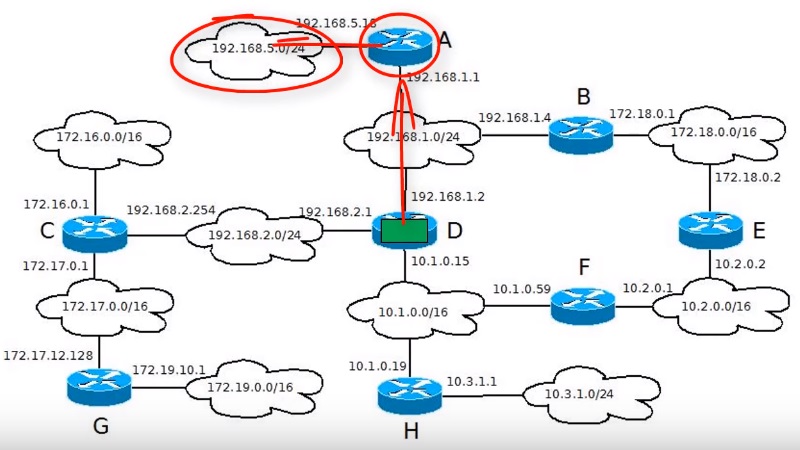
В качестве примера, рассмотрим схему составной сети, здесь показаны отдельные подсети, для каждой подсети есть ее адрес и маска, а также маршрутизаторы, которые объединяют эти сети.



Рассмотрим маршрутизатор D, на него пришел пакет, и маршрутизатор должен решить, что ему делать с этим пакетом. Начнем с того, какие вообще возможны варианты действий у маршрутизатора. Первый вариант: сеть, которой предназначен пакет, подключена непосредственно к маршрутизатору. У маршрутизатора D таких сетей 3, в этом случае маршрутизатор передает пакет непосредственно в эту сеть.



Второй вариант, нужная сеть подключена к другому маршрутизатору (А), и известно, какой маршрутизатор нужен. В этом случае, маршрутизатор D передает пакет на следующий маршрутизатор, который может передать пакет в нужную сеть, такой маршрутизатор называется шлюзом.



Третий вариант, пришел пакет для сети, маршрут которой неизвестен, в этом случае маршрутизатор отбрасывает пакет. В этом отличие работы маршрутизатора от [коммутатора](https://zvondozvon.ru/tehnologii/kompyuternye-seti/ethernet-tipy), коммутатор отправляет кадр который он не знает куда доставить на все порты, маршрутизатор так не делает. В противном случае составная сеть очень быстро может переполнится мусорными пакетами для которых не известен маршрут доставки.

Что нужно знать маршрутизатору для того чтобы решить куда отправить пакет?

* Во-первых у маршрутизатора есть несколько интерфейсов, к которым подключены сети. Нужно определить в какой из этих интерфейсов отправлять пакет.
* Затем нужно определить, что именно делать с этим пакетом. Есть 2 варианта, можно передать пакет в сеть (192.168.1.0/24), либо можно передать его на один из маршрутизаторов подключенные к этой сети. Если передавать пакет на маршрутизатор, то нужно знать, какой именно из маршрутизаторов подключенных к этой сети, выбрать для передачи пакета.

Эту информацию маршрутизатор хранит в таблице маршрутизации



**Пакет распаковывается в кадр, что он содержит, чтобы добраться до отправителя?**

**Что такое ip адрес?** (уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP)

Не знаю, меняет ли это что-то, но ещё Сущенко спрашивал, **какой протокол отвечает за отображение ip адреса на физический** (ответ - [ARP](https://ru.wikipedia.org/wiki/ARP)(Address Resolution Protocol))

Если спросит **что именует IP адрес**, не отвечайте host (его слова: Мы же не в Гарварде молодой человек) отвечайте, машина.

**Какие адреса ты знаешь?**

- IP адрес, MAC адрес, Доменный адрес....

**Для чего нужен IP адрес и что он именует и на каком он уровне?**

- Он именует физическое устройство в сети и нужен для его идентификации. Он на сетевом уровне.

**Скремблеры, скремблирование**

**Прикладной процесс**

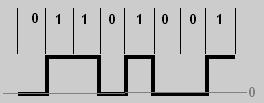
**Почему маршрутизатор имеет несколько портов?**

Маршрутизатор - это устройство которое соединяет несколько компьютеров между собой, поэтому он имеет несколько портов. Если маршрутизатор это вершина графа, то количество адресов определяется количеством дуг которыми он соединен с другими вершинами - компьютерами.

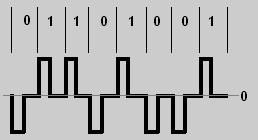
**Какие цифровые коды, с помощью которых данные передаются в линию связи, вам известны?**

- потенциальные и импульсные коды. ([мануалка](https://pykhtina.files.wordpress.com/2016/03/l14_method.pdf))

Потенциальный способ кодирования заключается в выставлении уровня сигнала в соответствии с поступающим на вход кодирующего устройства двух битов. Каждой паре битов соответствует потенциальный уровень сигнала, всего таких уровней четыре. Для потенциального кода главным параметром будет уровень напряжения (потенциал сигнала)



В импульсных кодах главным фактором, естественно, является полярность импульса или перепад напряжения:



**Почему не пользуются импульсными кодами, а берут и исправляют потенциальные?**

Потомушто потенциальные коды имеют меньший спектр частот, чем импульсные, и это позволяет достичь бОльших скоростей при передаче данных???????????????????(вроде ответ правильный но какой свой спектр я хз)

**Таблица коммутации**: каждому порту соответствует МАС адрес

Коммутаторы пакетной сети отличаются от коммутаторов каналов тем, что они имеют внутреннюю буферную память для временного хранения пакетов, если выходной порт коммутатора в момент принятия пакета занят передачей другого пакета

**Сравнение подсетей виртуальных каналов и дейтаграммных подсетей**

1. Обычно в крупной сети количество проложенных через узел виртуальных каналов существенно меньше количества узлов и подсетей, поэтому по размерам таблица коммутации намного меньше таблицы маршрутизации, и, следовательно, просмотр занимает гораздо меньше времени и не требует от коммутатора большой вычислительной мощности.

2. Идентификатор виртуального канала (соединения) намного короче адреса конечного узла, поэтому размер заголовка пакета, не содержащего длинный адрес, существенно меньше.

3. Виртуальный канал требует определенных затрат времени на его установку, однако последующая обработка пакетов для маршрутизации проще и быстрее, чем в дейтаграммной подсети.

4. Во время установки соединения ресурсы могут быть зарезервированы заранее, поэтому виртуальные каналы:

* предоставляют гарантированное качество обслуживания,
* позволяют избежать заторов в подсети.

В дейтаграммной подсети сложно:

* обеспечить необходимое качество обслуживания для всех пакетов одного потока,
* реализовать предотвращение заторов.

5 В системах обработки транзакций накладные расходы на установку соединения и удаление виртуального канала по окончании связи могут значительно снизить потребительские свойства сети. Более того, если объем передаваемой информации невелик, нет смысла устанавливать соединение.

6. В случае выхода из строя маршрутизатора все виртуальные каналы, проходившие через него, будут прерваны, и потеряны все, находившиеся на прерванной линии, пакеты.

Выход из строя маршрутизатора дейтаграммной подсети приводит к потере только пакетов, находившихся на нем.

То есть, обрыв связи в виртуальной сети является фатальным, а в дейтаграммной остается незамеченным.

7. Размытость путей следования трафика через дейтаграммную подсеть позволяет повысить производительность и надежность сети путем возможности сбалансирования нагрузки на отдельные узлы.

**Взаимодействие уровней -** [**2)Взаимодействие уровней**](#_wjq9y097oqgb)

**Установление связи на транспортном уровне**

1. Узел-отправитель (А) инициализирует установление связи, посылая узлу-получателю (В) запрос синхронизации (сегмент SYN), в котором указывает номер своей последовательности, например SECА = 101.

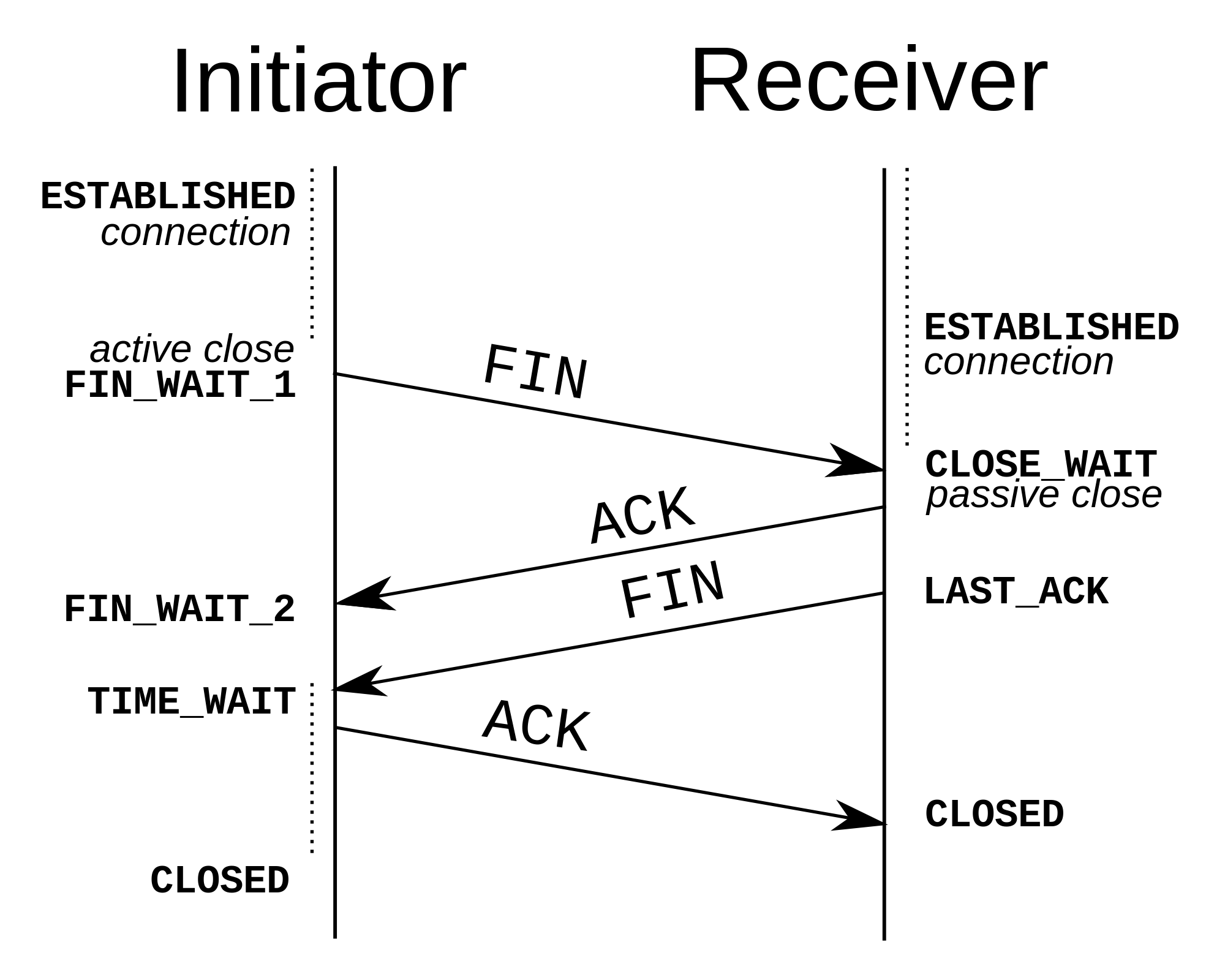
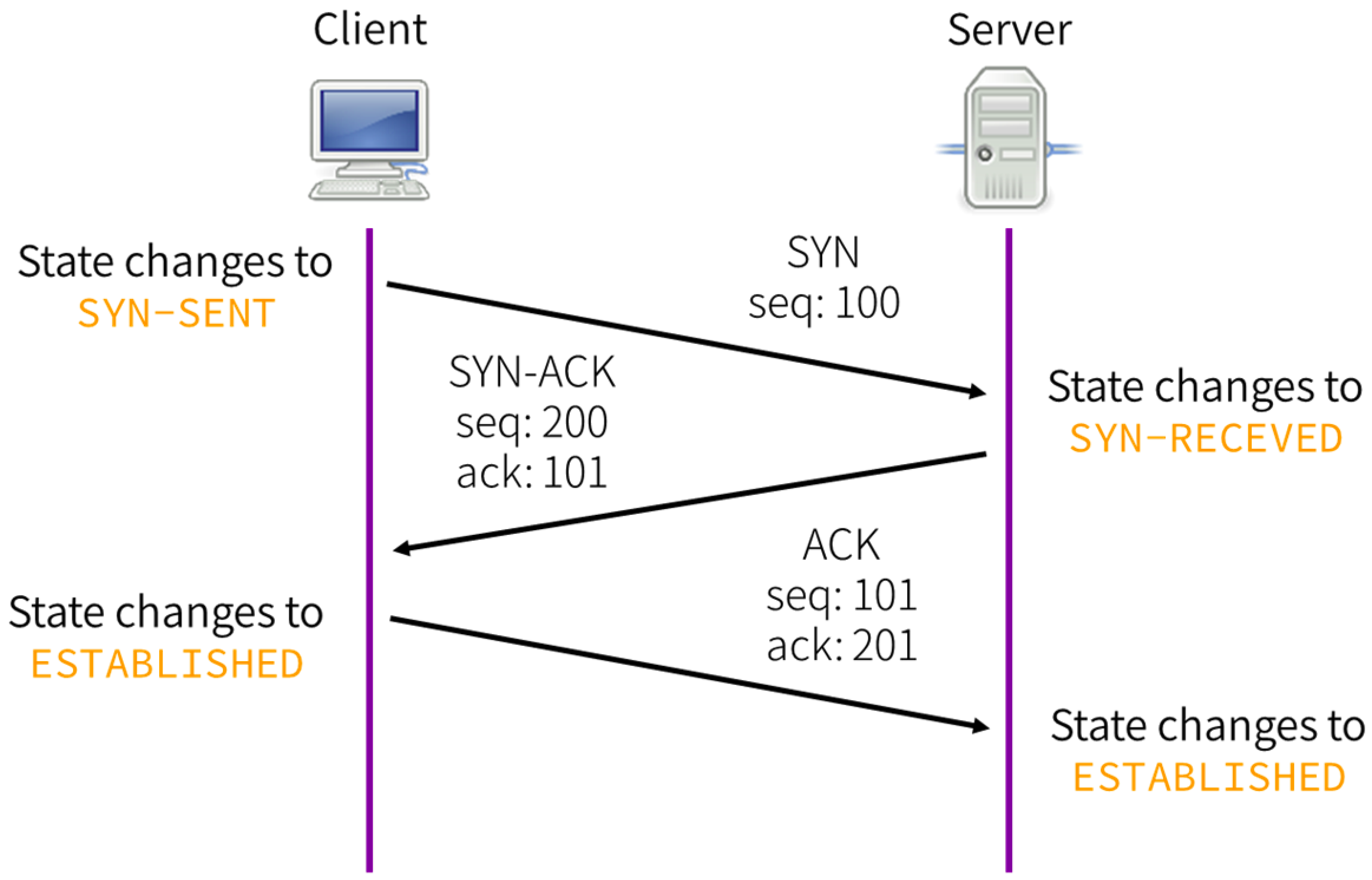
2. Получив сегмент инициализации соединения, узел-получатель В делает запись принятого номера последовательности 101, подтверждает запрос синхронизации и формирует ответ в виде сегмента ACK со своим параметром синхронизации ACK В = 101 + 1 = 102.

Ответ ACKВ = 102 означает, что хост B получил сегмент данных, включая байт с номером 101, и ожидает следующий байт с номером 102.

Одновременно хост B формирует начальный номер своей последовательности данных, например SECВ = 51.

3. Узел A, получив сегмент от B со значениями ACKВ = 102, SECВ = 51, формирует ответ ACKА = 52, SECА = 102, который завершает процесс соединения, то есть, подтверждение, что обе стороны готовы к тому, чтобы соединение было установлен.

Таким образом, синхронизация требует, чтобы каждая сторона послала собственный начальный номер последовательности и получила подтверждение от другой стороны. Каждая сторона, получив начальный номер последовательности от другой стороны, отвечает подтверждением ACK.



**Протокол маршрутизации** — это сетевой протокол (3 уровень модели OSI), который используется маршрутизаторами (роутерами) с целью определения маршрутов передачи данных в составной вычислительной сети (интрасеть). В частности, во избежание ручного ввода всех допустимых маршрутов в маршрутизаторы, используются протоколы маршрутизации, что экономит труд системных администраторов и снижает количество ошибок в настройке маршрутизаторов.

Протоколы маршрутизации делятся на два вида, зависящие от типов алгоритмов, на которых они основаны:

* **Дистанционно-векторные протоколы**, основаны на Distance Vector Algorithm (**DVA**);
* **Протоколы состояния каналов связи**, основаны на Link State Algorithm (**LSA**).

В **дистанционно-векторном алгоритме** (DVA) основная идея заключается в рассылке маршрутизаторов друг другу так называемого вектора расстояний. В векторе расстояний содержится информация (расстояние) от передающего маршрутизатора до всех соседних (известных) ему сетей.

Самым распространенным представителем дистанционно-векторного алгоритма является протокол **RIP**

**Алгоритм состояния связей (LSA)** снабжает все маршрутизации информацией, необходимой для построения подробного графа связей составной вычислительной сети.

протокол **OSPF**(Open Shortest Path First, алгоритм кратчайшего пути) стека TCP/IP;

Я пакет - я пришел, а я маршрутизатор. Пришел адрес, смотрим подключение сети. Если в этой сети, то находим по арп запросу мак-адрес компьютера Если не в этой не сети, то находим следующий маршрутизатор. В пакете достаем сначала адрес узла назначения, из первой строки таблицы выбираем маску, накладываем на адрес выбранный из пакета, получили адрес подсети получателя. Смотрим по таблице подключения к маршрутизатору. Поле подсеть назначения в таблице, с ним сравниваем. Если совпали находим, если нет к следующей строке