1. **История развития инфо-коммуникационных систем.**

История развития инфо-коммуникационных систем начинается с изобретения телефона Александром Грэхэмом Беллом в 1876 году. Это было первое устройство, которое позволяло передавать голосовые сообщения на расстояние.

В 20-х годах прошлого века, была создана первая радиосвязь, которая позволила передавать сообщения без проводов. Это привело к возникновению радиостанций и трансляций радиопередач.

В 1950-х годах, была создана первая телевизионная сеть, которая позволила передавать видео-сигналы на большие расстояния. Это привело к возникновению телевизионных каналов и трансляций телепередач.

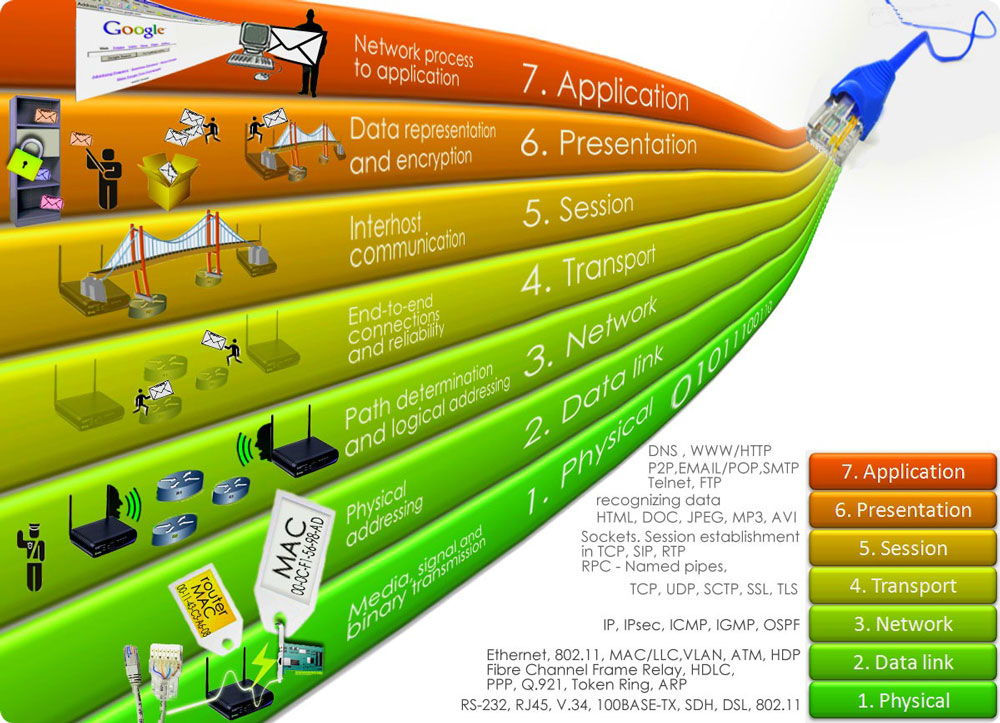
В 1960-х годах, была создана первая компьютерная сеть ARPANET, которая позволила компьютерам обмениваться информацией между собой. Это привело к возникновению интернета и возможности передачи данных по всему миру.

С 1980-х годов, началось широкое распространение персональных компьютеров и возникновение локальных сетей. Это привело к возможности обмена информацией между компьютерами внутри офисов и предприятий

В 1990-х годах, началось широкое распространение мобильных телефонов и возникновение беспроводной связи. Это привело к возможности общаться и передавать данные на расстоянии без использования проводов.

Сегодня инфо-коммуникационные системы продолжают развиваться и улучшаться. Это приводит к возможности передавать данные с еще большей скоростью и точностью, а также обеспечивает доступ к информации в любом месте и в любое время.

1. **Сетевая модель OSI/ISO. Общее представление.**





1. **Уровень L1. Физический. Общие сведения.**

Физический уровень ([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) physical layer) — нижний уровень модели, который определяет метод передачи данных, представленных в двоичном виде, от одного устройства (компьютера) к другому.

1. **Уровень L2. Канальный. Общие сведения. Протоколы.**

Канальный уровень ([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) data link layer) предназначен для обеспечения взаимодействия сетей на физическом уровне и контроля ошибок, которые могут возникнуть. Полученные с физического уровня данные, представленные в битах, он упаковывает в [кадры](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)), проверяет их на целостность и, если нужно, исправляет ошибки (либо формирует повторный запрос повреждённого кадра) и отправляет на сетевой уровень. Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.

Протоколы канального уровня: [ARCnet](https://ru.wikipedia.org/wiki/ARCnet" \o "ARCnet), [ATM](https://ru.wikipedia.org/wiki/Asynchronous_Transfer_Mode), [Controller Area Network](https://ru.wikipedia.org/wiki/Controller_Area_Network) (CAN), [Econet](https://ru.wikipedia.org/wiki/Econet" \o "Econet), [IEEE 802.3](https://ru.wikipedia.org/wiki/IEEE_802.3) ([Ethernet](https://ru.wikipedia.org/wiki/Ethernet)), [Ethernet Automatic Protection Switching](https://ru.wikipedia.org/wiki/Ethernet_Automatic_Protection_Switching) (EAPS), [Fiber Distributed Data Interface](https://ru.wikipedia.org/wiki/Fiber_Distributed_Data_Interface) (FDDI), [Frame Relay](https://ru.wikipedia.org/wiki/Frame_Relay), [High-Level Data Link Control](https://ru.wikipedia.org/wiki/High-Level_Data_Link_Control) (HDLC), [IEEE 802.2](https://ru.wikipedia.org/wiki/IEEE_802.2) (предоставляет функции LLC для подуровня IEEE 802 MAC), [Link Access Procedures, D channel](https://ru.wikipedia.org/w/index.php?title=Link_Access_Procedures,_D_channel&action=edit&redlink=1) (LAPD), [IEEE 802.11](https://ru.wikipedia.org/wiki/IEEE_802.11) [wireless LAN](https://ru.wikipedia.org/wiki/Wireless_LAN), [LocalTalk](https://ru.wikipedia.org/wiki/LocalTalk" \o "LocalTalk), [Multiprotocol Label Switching](https://ru.wikipedia.org/wiki/Multiprotocol_Label_Switching) (MPLS), [Point-to-Point Protocol](https://ru.wikipedia.org/wiki/Point-to-Point_Protocol) (PPP), [Point-to-Point Protocol over Ethernet](https://ru.wikipedia.org/wiki/PPPoE) (PPPoE), [Serial Line Internet Protocol](https://ru.wikipedia.org/wiki/SLIP) (SLIP, устарел), [StarLan](https://ru.wikipedia.org/wiki/StarLan" \o "StarLan), [Token ring](https://ru.wikipedia.org/wiki/Token_ring), [Unidirectional Link Detection](https://ru.wikipedia.org/w/index.php?title=Unidirectional_Link_Detection&action=edit&redlink=1)[[en]](https://en.wikipedia.org/wiki/Unidirectional_Link_Detection) (UDLD), [x.25](https://ru.wikipedia.org/wiki/X.25), [ARP](https://ru.wikipedia.org/wiki/ARP).

1. **Определение коллизии. Описание процесса и методология устранения**

Коллизия ([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) collision — ошибка наложения, столкновения) — в терминологии компьютерных и [сетевых](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) технологий наложение двух и более кадров от станций, пытающихся передать кадр в один и тот же момент времени в среде передачи коллективного доступа.

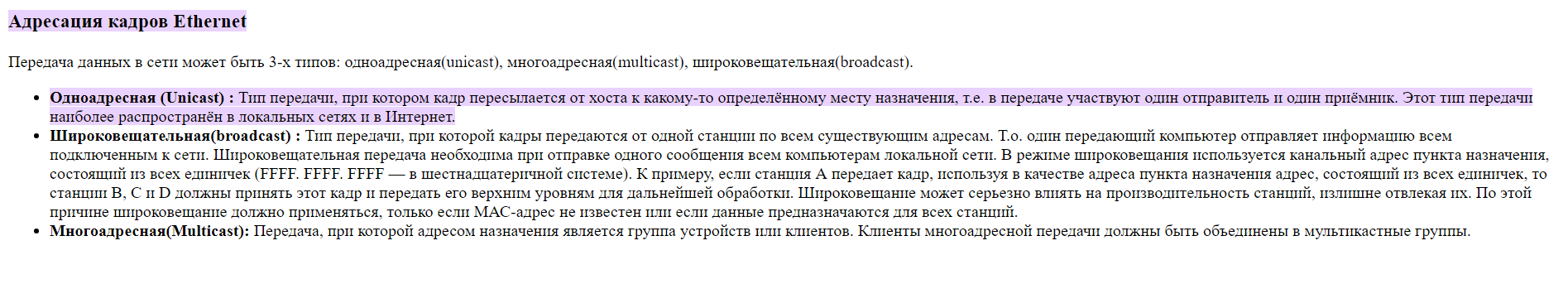
Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется обнаружение коллизии (collision detection, CD).

1. **Определение домена коллизии. Адресация в Ethernet**

### Доме́н колли́зий (англ. Collision domain) — часть сети Ethernet, все узлы которой конкурируют за общую разделяемую среду передачи и, следовательно, каждый узел которой может создать коллизию с любым другим узлом этой части сети. Адресация кадров Ethernet

Передача данных в сети может быть 3-х типов: одноадресная(unicast), многоадресная(multicast), широковещательная(broadcast).

* Одноадресная (Unicast) : Тип передачи, при котором кадр пересылается от хоста к какому-то определённому месту назначения, т.е. в передаче участвуют один отправитель и один приёмник. Этот тип передачи наиболее распространён в локальных сетях и в Интернет.
* Широковещательная(broadcast) : Тип передачи, при которой кадры передаются от одной станции по всем существующим адресам. Т.о. один передающий компьютер отправляет информацию всем подключенным к сети. Широковещательная передача необходима при отправке одного сообщения всем компьютерам локальной сети. В режиме широковещания используется канальный адрес пункта назначения, состоящий из всех единичек (FFFF. FFFF. FFFF — в шестнадцатеричной системе). К примеру, если станция А передает кадр, используя в качестве адреса пункта назначения адрес, состоящий из всех единичек, то станции В, С и D должны принять этот кадр и передать его верхним уровням для дальнейшей обработки. Широковещание может серьезно влиять на производительность станций, излишне отвлекая их. По этой причине широковещание должно применяться, только если МАС-адрес не известен или если данные предназначаются для всех станций.
* Многоадресная(Multicast): Передача, при которой адресом назначения является группа устройств или клиентов. Клиенты многоадресной передачи должны быть объединены в мультикастные группы.



1. **Поддерживаемые и неподдерживаемые Ethernet топологии сети**

Стандарт Ethernet поддерживает топологию вида «кольцо», «шина», «звезда» и т.д., но не поддерживает топологию дерева(и полностью дублирующую).

1. **Эволюция стандарта Ethernet и расширение пропускной способности канала**

Ethernet - это стандарт передачи данных в локальных сетях. С течением времени, этот стандарт эволюционировал и улучшался.

Первоначальный стандарт Ethernet был разработан в 1973 году в компании Xerox. Он был основан на технологии передачи данных по коаксиальному кабелю и имел скорость передачи 10 Мбит/с.

В 1980-х годах, стандарт Ethernet был усовершенствован, и был создан новый стандарт Ethernet II. Он использовал другой формат заголовка и добавил возможность передачи данных по твистедной паре кабеля. Это позволило увеличить скорость передачи данных3.

В 1995 году, был создан новый стандарт Fast Ethernet, который позволил увеличить скорость передачи данных до 100 Мбит/с. Это было достигнуто за счет использования оптимизированных протоколов и улучшенных технологий передачи данных.

В 1998 году, был создан стандарт Gigabit Ethernet, который позволяет передавать данные со скоростью до 1 Гбит/с. Это было достигнуто за счет использования оптимизированных протоколов и новых технологий передачи данных.

В 2006 году, был создан стандарт 10 Gigabit Ethernet, который позволяет передавать данные со скоростью до 10 Гбит/с. Это было достигнуто за счет использования новых технологий передачи данных и оптимизированных протоколов.

Сегодня Ethernet является наиболее распространенным стандартом для передачи данных в локальных сетях и продолжает развиваться и улучшаться.

1. **Режим автоматического согласования типа передачи и скорости канала**

Автосогласование ([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) autonegotiation) - это [механизм](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%85%D0%B0%D0%BD%D0%B8%D0%B7%D0%BC) и [процедура](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D0%B4%D1%83%D1%80%D0%B0) сигнализации, используемая в семействе технологий [Ethernet](https://ru.wikipedia.org/wiki/Ethernet" \o "Ethernet) при передаче данных по [витой паре](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D1%82%D0%B0%D1%8F_%D0%BF%D0%B0%D1%80%D0%B0), посредством которой два подключенных устройства выбирают общие параметры передачи, такие как скорость, [дуплексный](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)) режим и [управление потоком](https://ru.wikipedia.org/wiki/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BC) . В этом процессе подключенные устройства сначала обмениваются своими возможностями в отношении этих параметров, а затем выбирают режим передачи с наивысшей [производительностью](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%BE%D0%B4%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C), который они оба поддерживают.

1. **Структура Ethernet фрейма и определение MTU. ARP**

В компьютерных сетях термин maximum transmission unit означает максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации.

ARP — протокол в компьютерных сетях, предназначенный для определения MAC-адреса другого компьютера по известному IP-адресу.

1. **Основы коммутации и биение домена коллизий на широковещательные домены**

Широковеща́тельный доме́н (сегме́нт) ([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) broadcast domain) — группа [доменов коллизий](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B5%D0%BD_%D0%BA%D0%BE%D0%BB%D0%BB%D0%B8%D0%B7%D0%B8%D0%B9), соединенных с помощью устройств [второго уровня](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)[[1]](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%B4%D0%BE%D0%BC%D0%B5%D0%BD#cite_note-1). Иными словами логический участок [компьютерной 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), в котором все узлы могут передавать данные друг другу с помощью [широковещания](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%BA%D0%B0%D0%BD%D0%B0%D0%BB) 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) [сетевой модели OSI](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI).[[2]](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%B4%D0%BE%D0%BC%D0%B5%D0%BD#cite_note-2)[[3]](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%B4%D0%BE%D0%BC%D0%B5%D0%BD#cite_note-3)

Коммутация сообщений (КС, message switching) — разбиение информации на сообщения, которые передаются последовательно к ближайшему транзитному узлу, который, приняв сообщение, запоминает его и передаёт далее сам таким же образом. Получается нечто вроде конвейера.

1. **Основы сетевой схемотехники. Обозначения ключевых сетевых устройств.**

Сетевая схемотехника - это процесс проектирования и создания схем, которые используются для соединения различных устройств и компонентов в сети. Она включает в себя следующие основы:

1. Топология сети - это физическая структура сети, определяющая способ соединения устройств и передачи данных между ними. Существуют различные типы топологий, такие как звезда, шина, кольцо и др.

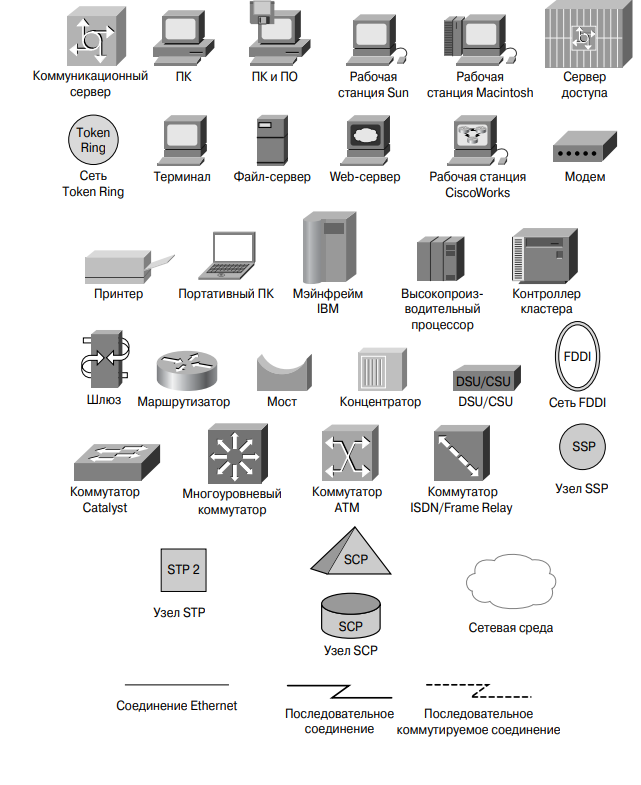
2. Устройства сети - это компоненты, используемые для создания сети, такие как маршрутизаторы, коммутаторы, мосты, хабы и др. Они обеспечивают передачу данных между устройствами в сети.

3. Протоколы - это наборы правил и процедур, которые определяют способы передачи данных между устройствами в сети. Некоторые известные протоколы включают TCP/IP, HTTP, FTP, SMTP и др.

4. Адресация - это процесс присвоения уникальных адресов устройствам в сети для их идентификации и обмена данными. Например, IP-адреса используются для идентификации устройств в сети TCP/IP.

5. Безопасность - это важный аспект сетевой схемотехники, который обеспечивает защиту сети от несанкционированного доступа и вредоносных атак. Он включает в себя использование паролей, шифрования данных, брандмауэров и других мер защиты.

6. Масштабируемость - это способность сети увеличивать свою емкость и расширяться по мере необходимости. Это важно для обеспечения эффективной работы сети при увеличении количества устройств и объема передаваемых данных.



1. **Иерархическая модель сети**

Иерархическая модель сети - это структура, которая используется для организации сети в виде иерархии уровней. Каждый уровень выполняет определенную функцию и имеет свои характеристики. Такая модель обеспечивает более эффективное управление и масштабирование сети.

Иерархическая модель сети состоит из трех уровней:

1. Уровень доступа - это первый уровень, который включает в себя устройства, подключенные к сети, такие как компьютеры, принтеры, телефоны и др. Он обеспечивает доступ к сети и контролирует доступ пользователей к ресурсам.

2. Уровень распределения - это второй уровень, который обеспечивает маршрутизацию и фильтрацию трафика между устройствами на уровне доступа и ядре сети. Он также выполняет функции управления полосой пропускания и обеспечивает безопасность сети.

3. Уровень ядра - это последний уровень, который обеспечивает высокую скорость передачи данных между различными сегментами сети. Он также обеспечивает надежность и доступность сети.

Иерархическая модель сети позволяет более эффективно управлять сетью, уменьшить нагрузку на устройства и повысить ее масштабируемость. Она также обеспечивает более высокую производительность и безопасность сети.

1. **MAC Address Table. Типы передаваемых фреймов и обработка их коммутатором**

Таблица MAC - это таблица соответствий между MAC-адресами устройств назначения и портами коммутатора. MAC-адреса могут быть статические и динамические. Статические MAC-адреса настраиваются пользователем вручную, имеют наивысший приоритет, хранятся постоянно и не могут быть перезаписаны динамическими MAC-адресами.

1. **Широковещательный шторм (Broadcast Storm)**

Широковещательный шторм — лавина широковещательных пакетов. Размножение широковещательных сообщений активным сетевым оборудованием приводит к экспоненциальному росту их числа и парализует работу сети. Такие пакеты, в частности, используются сетевыми сервисами для оповещения станций о своём присутствии.

1. **Перегрузка коммутаторов и Poison Frame**

Перегрузка сети в компьютерных сетях и [теории очередей](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BE%D1%80%D0%B8%D1%8F_%D0%BC%D0%B0%D1%81%D1%81%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE_%D0%BE%D0%B1%D1%81%D0%BB%D1%83%D0%B6%D0%B8%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F) — это снижение [качества обслуживания](https://ru.wikipedia.org/wiki/QoS), которое возникает, когда сетевой узел или линия связи переносит больше данных, чем может обрабатывать. Типичные эффекты включают задержку в очереди, потерю [пакетов](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)) или блокировку новых соединений. Последствием перегрузки является то, что постепенное увеличение предлагаемой нагрузки приводит либо к небольшому увеличению, либо даже к снижению [пропускной способности](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BF%D1%83%D1%81%D0%BA%D0%BD%D0%B0%D1%8F_%D1%81%D0%BF%D0%BE%D1%81%D0%BE%D0%B1%D0%BD%D0%BE%D1%81%D1%82%D1%8C) сети.

Poison frame это вид фрейма, который коммутатор отправляет через свои интерфейсы, когда перегружен. Другие устройства, получив такой фрейм, на некоторое время перестают вещать в сеть.

1. **Протокол связующего дерева STP. Принцип работы**

Spanning Tree Protocol (STP, протокол [остовного дерева](https://ru.wikipedia.org/wiki/%D0%9E%D1%81%D1%82%D0%BE%D0%B2%D0%BD%D0%BE%D0%B5_%D0%B4%D0%B5%D1%80%D0%B5%D0%B2%D0%BE" \o "Остовное дерево)) — канальный протокол. Основной задачей STP является устранение [петель](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%82%D0%BB%D1%8F_(%D1%82%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F)) в топологии произвольной сети [Ethernet](https://ru.wikipedia.org/wiki/Ethernet" \o "Ethernet), в которой есть один или более [сетевых мостов](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BC%D0%BE%D1%81%D1%82), связанных избыточными соединениями.

Выбирается кратчайший путь между узлами, а остальные пути блокируются

1. **Эволюция STP. Различие состояний портов STP и RSTP.**

Rapid STP (RSTP) является значительным усовершенствованием STP. В первую очередь необходимо отметить уменьшение времени сходимости и более высокую устойчивость.

RSTP отличается от STP тем, что состояние порта отвязали от его роли. Это позволило описать роль порта в топологии сети без оглядки на его состояние. А значит, обладать лучшим видение топологии сети и возможностью оперативно реагировать на изменения в ней.

1. **Общие сведения о MSTP. Отличие от RSTP**

В один экземпляр MSTP могут входить несколько виртуальных сетей при условии, что их топология одинакова (в смысле входящих в VLAN коммутаторов и соединений между ними).

1. **BPDU Guard - назначение технологии. Режим PortFast**

BPDU — фрейм протокола управления сетевыми мостами. BPDU Guard — функция, которая позволяет выключать порт при получении BPDU. PortFast является функцией протокола spanning-tree, которая переводит порт в состояние пересылки сразу после его включения.

1. **Методология привязки сетевых устройств к портам коммутатора**

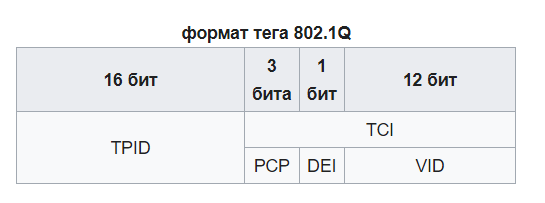
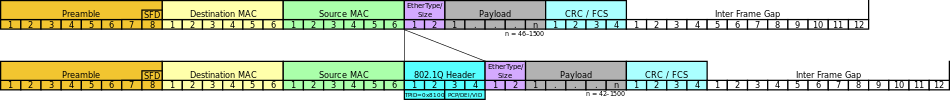
Методология привязки сетевых устройств к портам коммутатора называется порт-связывание (port mapping). Это процесс определения, какой порт коммутатора соответствует какому устройству в сети.

1. **Агрегация портов сетевых устройств. Зеркалирование портов**

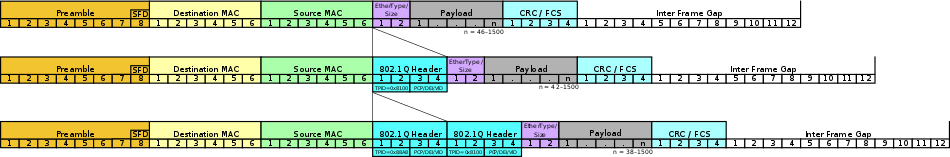
Агрегирование каналов связи (Link Aggregation) — это объединение нескольких физических портов в одну логическую магистраль на канальном уровне модели OSI с целью образования высокоскоростного канала передачи данных и повышения отказоустойчивости.

Зеркали́рование — дублирование пакетов одного порта сетевого коммутатора на другом.

1. **Стандарт 802.1Q. Структура фрема. Структура тега. (VLAN)**

IEEE 802.1Q — открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN по сетям стандарта IEEE 802.3 Ethernet.  

1. **Стандарт 802.1ad. Структура фрема. Структура тега.(Q&Q vlan)**

IEEE 802.1ad — это поправка к [сетевому стандарту](https://en.wikipedia.org/wiki/Computer_network)[IEEE 802.1Q-1998](https://en.wikipedia.org/wiki/IEEE_802.1Q) , которая добавляет поддержку мостов провайдеров . 

1. **Приоритеризация сетевого трафика на L2-уровне**

Приоритизация сетевого трафика на L2-уровне осуществляется с помощью технологии Quality of Service (QoS). QoS позволяет управлять и контролировать трафик в сети, определяя приоритеты для различных типов трафика.

1. **Виртуальные сети организации и методы их коммутации с помощью IEEE 802.1Q (vlan)**

Виртуальные сети организации (VLAN) - это метод разделения физической сети на несколько логических сегментов с помощью коммутаторов. Каждая VLAN является отдельной логической сетью, которая может иметь свои правила безопасности и настройки.

IEEE 802.1Q - это стандарт, который определяет методы коммутации VLAN на уровне 2 OSI-модели. Он позволяет передавать трафик нескольких VLAN через один физический порт коммутатора.

1. **Роли портов коммутатора в расширении IEEE 802.1Q. VLAN по умолчанию**

позволяет передавать трафик нескольких VLAN через один физический порт коммутатора.

Для стандарта 802.1Q используется понятие native VLAN. Информационный трафик для этого VLAN будет передаваться нетегированным.

1. **IEEE 802.1Q Tag. PCP. DEI. VID**

EEE 802.1Q Tag - это заголовок, который добавляется к кадрам Ethernet для идентификации VLAN. Он состоит из 4 байтов, включающих в себя идентификатор VLAN (VID) и дополнительные поля, такие как приоритет класса (PCP) и индикатор отметки отбрасывания (DEI).

VID (VLAN ID) - это 12-битное поле, которое определяет идентификатор VLAN. Оно может принимать значения от 1 до 4094, где значения 0 и 4095 зарезервированы. Каждая VLAN должна иметь уникальный VID.

PCP (Priority Code Point) - это 3-битное поле, которое указывает приоритет кадра внутри VLAN. Он используется для определения приоритета передачи трафика в сети. Значения PCP могут быть от 0 до 7, где значение 0 означает наивысший приоритет.

DEI (Drop Eligible Indicator) - это 1-битное поле, которое указывает, может ли кадр быть отброшен в случае перегрузки сети. Если DEI установлен в 1, то кадр может быть отброшен.

IEEE 802.1Q Tag позволяет коммутаторам разделять трафик на разные VLAN и обеспечивает эффективную передачу данных в сети. Он также позволяет настраивать приоритеты трафика и управлять его потоком в сети.

1. **Уровень L3. Сетевой. Общие сведения. Протоколы.**

Сетевой уровень ([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) network layer) модели предназначен для определения пути передачи данных. Отвечает за трансляцию логических адресов и имён в физические, определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и «заторов» в сети.

Протоколы сетевого уровня: IP/IPv4/IPv6

1. **Классовая и бесклассовая IP адресация**

Классовая адресация сетей — метод [IP](https://ru.wikipedia.org/wiki/IP)-адресации. Применение этого метода не позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку невозможно применение масок к различным подсетям.

Бесклассовая адресация — метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации. Использование этого метода позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку возможно применение различных масок подсетей к различным подсетям.

1. **Расчет количества хостов, вычисление широковещательных IP и IP подсетей**

Количество хостов в подсети = 2n-2, где n – это количество свободных бит (нулей) в порции хоста, а «-2» - это вычет адреса сети (в порции хоста все нули) и широковещательного адреса (в порции хоста все единицы).

Широковещательный – max на конце.

Подсеть – 0 на конце

1. **Принцип работы утилиты tracert (traceroute)**

Tracert отправляет эхо-запрос ICMP (ICMP Echo Request) с TTL=1. Первый маршрутизатор проверяет адрес назначения, чтобы выяснить был ли отправлен запрос именно ему. Узнав, что цель пакета – другой хост, маршрутизатор отбрасывает его, и TTL становится равным 0.

1. **Фрагментация пакетов на уровне L3.**

Фрагментация пакета — генерация двух сетевых пакетов из одного. Происходит при превышении длины кадра MTU интерфейса, через который он в данный момент проходит. Фрагментация (и её запрещение) поддерживается IP-протоколом и не предусмотрена в большинстве других протоколов.

1. **Маршрутизация и виды маршрутов. Алгоритм выбора маршрута**

В TCP/IP предусмотрено два типа маршрутизации: статическая и динамическая. Выбирается самый быстрый маршрут(опционально).

1. **Маршрут по умолчанию. Суммаризация маршрутов. Обратные маски.**

Ip route 0.0.0.0 0.0.0.0

Суммирование маршрутов используется, чтобы уменьшить размер таблицы маршрутизации.  
Если один статический маршрут может использоваться вместо нескольких статических маршрутов, размер таблицы маршрутизации будет уменьшен. Во многих случаях единственный статический маршрут может использоваться, чтобы представить десятки, сотни или даже тысячи маршрутов.

Обратная маска: (255.255.255.255)xor(ip\_address) используется в динамических протоколах(OSPf)

1. **Протоколы динамической маршрутизации и их классификация**

Протоколы маршрутизации делятся на внешние и внутренние. Внешние протоколы (EGP, BGP) переносят маршрутную информацию между автономными системами, а внутренние (RIP, OSPF) применяются только в пределах определенной автономной системы.

1. **Определение автономной системы, регионального и локального интернет регистратора**

Автономная система - это набор сетей и шлюзов, которые находятся под единым управлением. Если шлюз расположен в той же самой автономной системе, то он называется внутренним соседом, а если в другой автономной системе, то внешним соседом.

Локальный интернет-регистратор ([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) Local Internet registry, LIR) — организация, занимающаяся распределением адресного пространства пользователям сетей (сервис-провайдерам и их абонентам) и оказанием сопутствующих регистрационных услуг.

Региональный интернет-регистратор ([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) Regional Internet Registry) — организация, занимающаяся вопросами адресации и [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) в сети [Интернет](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82).

1. **Метрика протокола и алгоритмы расчета для RIP и OSPF**

RIP — так называемый протокол [дистанционно-векторной маршрутизации](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE-%D0%B2%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%BD%D0%B0%D1%8F_%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F), который оперирует [транзитными участками](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B0%D0%BD%D0%B7%D0%B8%D1%82%D0%BD%D1%8B%D0%B9_%D1%83%D1%87%D0%B0%D1%81%D1%82%D0%BE%D0%BA) (хоп, hop) в качестве метрики маршрутизации. Максимальное количество транзитных участков, разрешенное в RIP — 15 (метрика 16 означает «бесконечно большую метрику»). Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд, довольно сильно нагружая низкоскоростные линии связи. RIP работает в сетях [TCP/IP](https://ru.wikipedia.org/wiki/TCP/IP), используя [UDP](https://ru.wikipedia.org/wiki/UDP) порт 520.

OSPF ([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) Open Shortest Path First) — протокол динамической [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), основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути [алгоритм Дейкстры](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%94%D0%B5%D0%B9%D0%BA%D1%81%D1%82%D1%80%D1%8B). Протокол OSPF использует стоимость в качестве метрики.

1. **RIP. Общие сведения**

RIP — так называемый протокол [дистанционно-векторной маршрутизации](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE-%D0%B2%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%BD%D0%B0%D1%8F_%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F), который оперирует [транзитными участками](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B0%D0%BD%D0%B7%D0%B8%D1%82%D0%BD%D1%8B%D0%B9_%D1%83%D1%87%D0%B0%D1%81%D1%82%D0%BE%D0%BA) (хоп, hop) в качестве метрики маршрутизации. Максимальное количество транзитных участков, разрешенное в RIP — 15 (метрика 16 означает «бесконечно большую метрику»). Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд, довольно сильно нагружая низкоскоростные линии связи. RIP работает в сетях [TCP/IP](https://ru.wikipedia.org/wiki/TCP/IP), используя [UDP](https://ru.wikipedia.org/wiki/UDP) порт 520.

1. **RIP. Анонсируемая подсеть. Максимально достижимая подсеть**

Анонсируемая сеть – сеть, достижимая в рипе. Максимально достижимая подсеть - 15

1. **OSPF. Задача коммивояжера. Алгоритм Дейкстры**

OSPF ([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) Open Shortest Path First) — протокол динамической [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), основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути [алгоритм Дейкстры](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%94%D0%B5%D0%B9%D0%BA%D1%81%D1%82%D1%80%D1%8B).

Задача коммивояжера – цикл минимального веса, проходящий через все вершины.

Алгори́тм Де́йкстры — Находит кратчайшие пути от одной из вершин графа до всех остальных.

1. **Зональное биение в OSPF. Магистральная OSPF зона**

Зона (area) — совокупность сетей и маршрутизаторов, имеющих один и тот же идентификатор зоны. В OSPF взаимодействия между зонами возможно только через зону 0.

Магистральная зона (известная также как нулевая зона или зона 0.0.0.0) формирует ядро сети OSPF. Все остальные зоны соединены с ней, и межзональная маршрутизация происходит через маршрутизатор, соединенный с магистральной зоной.

1. **Inter Vlan routing (CrossVLAN routing)**

Когда узлам в одной VLAN нужно связаться с узлами в другой VLAN, между ними нужна маршрутизация трафика. Это называется маршрутизацией между VLAN(InterVlan Routing).

1. **DHCP. Клиент серверная архитектура.**

DHCP – это стандартный протокол в сети с архитектурой «клиент-сервер», который динамически назначает IP-адреса и другую необходимую информацию конфигурации для новых устройств в сети. Каждое сетевое устройство должно иметь собственный, уникальный IP-адрес, чтобы в сети не возникали конфликты.

1. **DHCP. Формат запросов и ответов до получения IP**

1. Клиент отправляет широковещательный запрос DHCP Discover с помощью UDP-пакета.

2. Сервер DHCP, получает запрос и отправляет в ответ DHCP Offer, содержащий предложение IP-адреса клиенту.

3. Клиент получает DHCP Offer и отправляет запрос DHCP Request, запрашивая выделенный ему IP-адрес.

4. Сервер DHCP получает запрос DHCP Request и отправляет в ответ DHCP Ack, подтверждая выделение IP-адреса клиенту.

1. **DHCP Pools. Борьба с конфликтами при раздаче IP**

DHCP pool – создание пула адресов, которые будут выдаваться автоматически клиентам DHCP.

DHCP-сервер не может дважды выдать один и тот же адрес. Однако в сети вполне может оказаться устройство со статическим адресом, входящим в пул адресов DHCP-сервера, поэтому для избежания конфликта DHCP-сервер перед выдачей адреса должен проверять, не используется ли этот адрес.

1. **Уровень L4. Транспортный. Общие сведения. Протоколы.**

Транспортный уровень ([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) transport layer) модели предназначен для обеспечения надёжной передачи данных от отправителя к получателю. При этом уровень надёжности может варьироваться в широких пределах.

Протоколы транспортного уровня: ATP, TCP, UDP

1. **Абстракция порта. UDP - формат, минусы**

Абстракция порта - это концепция, используемая в сетевых протоколах для идентификации конечных точек связи в сети.

UDP — один из ключевых элементов набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных. Минусы – недостаток надёжности.

1. **TCP - формат. Принцип тройного рукопожатия. Определение сессии и ее состояния**

TCP  — один из основных [протоколов передачи данных](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%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) интернета. Предназначен для управления [передачей данных интернета](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B0_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85).

Принцип тройного рукопожатия - В процессе передачи данных клиент и сервер обмениваются сегментами, поочередно подтверждая число полученных пакетов путем увеличения счетчиков порядкового номера.

Сессия – промежуток времени, в который устройство внутри сети включено и активно.

1. **Сетевая модель TCP/IP. Общее представление.**

TCP/IP — [сетевая модель](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C) [передачи данных](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B0_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85), представленных в цифровом виде. Модель описывает способ передачи данных от источника информации к получателю. В модели предполагается прохождение информации через четыре уровня, каждый из которых описывается протоколом передачи.(прикладной, транспортный, межсетевой, канальный)

1. **TCP/IP. Канальный уровень (Network Access Layer).**

Канальный уровень ([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) Link layer) описывает способ кодирования данных для передачи [пакета данных](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D0%BA%D0%B5%D1%82_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) на физическом уровне. [Ethernet](https://ru.wikipedia.org/wiki/Ethernet), например, в полях [заголовка пакета](https://ru.wikipedia.org/w/index.php?title=%D0%97%D0%B0%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BE%D0%BA_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%B0&action=edit&redlink=1) содержит указание того, какой машине или машинам в сети предназначен этот пакет.

1. **TCP/IP. Межсетевой уровень (Сетевой уровень) (Internet Layer).**

[Межсетевой уровень](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B_%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B3%D0%BE_%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D1%8F) (Network layer) изначально разработан для передачи данных из одной сети в другую. На этом уровне работают [маршрутизаторы](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), которые перенаправляют пакеты в нужную сеть путём расчёта адреса сети по [маске сети](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%81%D0%BA%D0%B0_%D0%BF%D0%BE%D0%B4%D1%81%D0%B5%D1%82%D0%B8).

1. **TCP/IP. Транспортный уровень (Transport Layer).**

Протоколы [транспортного уровня](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) могут решать проблему негарантированной доставки сообщений («дошло ли сообщение до адресата?»), а также гарантировать правильную последовательность прихода данных. В стеке TCP/IP транспортные протоколы определяют, для какого именно приложения предназначены эти данные.

1. **Проприетарные протоколы Cisco. Vlan Trunking Protocol. Принцип работы.**

Vlan Trunking Protocol - это собственный протокол Cisco, который распространяет определение виртуальных локальных сетей (VLAN) на всю локальную сеть. Для этого VTP передает информацию о VLAN всем коммутаторам в домене VTP. Объявления VTP можно отправлять по магистральным каналам 802.1Q и ISL.

1. **Проприетарные протоколы Cisco. Cisco Discover protocol (CDP). В качестве бонуса – LLDP**

CDP ([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) Cisco Discovery Protocol) — проприетарный протокол [второго уровня](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI), разработанный компанией [Cisco Systems](https://ru.wikipedia.org/wiki/Cisco_Systems" \o "Cisco Systems), позволяющий обнаруживать подключённое (напрямую или через устройства первого уровня) сетевое оборудование Cisco, его название, версию [IOS](https://ru.wikipedia.org/wiki/Cisco_IOS) и IP-адреса. Поддерживается многими устройствами компании, почти не поддерживается сторонними производителями.

Link Layer Discovery Protocol — протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.

1. **Статическая маршрутизация. Принцип работы. Таблица маршрутизации.**

Стати́ческая маршрутиза́ция — вид [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), при котором маршруты указываются в явном виде при конфигурации [маршрутизатора](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). Вся маршрутизация при этом происходит без участия каких-либо [протоколов маршрутизации](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).

При установке статического маршрута указывается:

* [Адрес сети](https://ru.wikipedia.org/w/index.php?title=%D0%90%D0%B4%D1%80%D0%B5%D1%81_%D1%81%D0%B5%D1%82%D0%B8&action=edit&redlink=1)(на которую маршрутизируется трафик), [маска сети](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%81%D0%BA%D0%B0_%D1%81%D0%B5%D1%82%D0%B8)
* Адрес [шлюза](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%88%D0%BB%D1%8E%D0%B7) (узла), который способствует дальнейшей маршрутизации (или подключен к маршрутизируемой сети напрямую)
* (опционально) [метрика](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D1%80%D0%B8%D0%BA%D0%B0) (иногда именуется также «ценой») маршрута. При наличии нескольких маршрутов на одну и ту же сеть некоторые маршрутизаторы выбирают маршрут с минимальной метрикой

Таблица маршрутизации — это конечный итог, куда заносится маршрут.

1. **Тайминги перестроения маршрутов при работе протокола RIP. Объяснить принцип построения маршрута**

Update timer — частота отправки обновлений протокола, по истечению таймера отправляется обновление. По умолчанию равен 30 секундам.

Invalid timer — Если обновление о маршруте не будет получено до истечения данного таймера, маршрут будет помечен как Invalid, то есть с метрикой 16. По умолчанию таймер равен 180 секундам.

Flush timer (garbage collection timer) — По умолчанию таймер равен 240 секундам, на 60 больше чем invalid timer. Если данный таймер истечет до прихода обновлений о маршруте, маршрут будет исключен из таблицы маршрутизации. Если маршрут удален из таблицы маршрутизации то, соответственно, удаляются и остальные таймеры, которые ему соответствовали.

Holddown timer — Запуск таймера произойдет после того, как маршрут был помечен как не достижимый. До истечения данного таймера маршрут будет находиться в памяти для предотвращения образования маршрутной петли и по этому маршруту передается трафик. По умолчанию равен 180 секундам. Таймер не является стандартным, добавлен в реализации Cisco.

Когда маршрутизатор отправляет обновление RIP, он добавляет к метрике маршрута, которую он использует, 1 и отправляет соседу. Сосед получает обновление, в котором указано какую метрику для полученного маршрута ему использовать.

Маршрутизатор отправляет каждые 30 секунд все известные ему маршруты соседним маршрутизаторам.

1. **Тайминги перестроения маршрутов при работе протокола OSPF. Объяснить принцип построения маршрута**

* HelloInterval — Интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет с интерфейса. Для широковещательных сетей и сетей точка-точка значение по умолчанию, как правило, равно 10 секундам.
* RouterDeadInterval — Интервал времени в секундах, по истечении которого сосед будет считаться "мертвым" (dead). Этот интервал должен быть кратным значению HelloInterval. Как правило, RouterDeadInterval равен 4 интервалам отправки hello-пакетов, то есть 40 секундам.
* Wait Timer — Интервал времени в секундах, по истечении которого маршрутизатор выберет DR в сети. Его значение равно значению интервала RouterDeadInterval.
* RxmtInterval — Интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, на который не получил подтверждения о получении (например, Database Description пакет или Link State Request пакеты). Это интервал называется также Retransmit interval. Значение интервала — 5 секунд.

Работает по алгоритму Дейкстры.

1. **Протокол динамической маршрутизации BGP. Различия iBGP и eBGP**

BGP (Border Gateway Protocol) — это основной протокол динамической маршрутизации, который используется в Интернете.

Маршрутизаторы, использующие протокол BGP, обмениваются информацией о доступности сетей. Вместе с информацией о сетях передаются различные атрибуты этих сетей, с помощью которых BGP выбирает лучший маршрут и настраиваются политики маршрутизации.

Один из основных атрибутов, который передается с информацией о маршруте — это список автономных систем, через которые прошла эта информация. Эта информация позволяет BGP определять где находится сеть относительно автономных систем, исключать петли маршрутизации, а также может быть использована при настройке политик.

Маршрутизация осуществляется пошагово от одной автономной системы к другой. Все политики BGP настраиваются, в основном, по отношению к внешним/соседним автономным системам. То есть, описываются правила взаимодействия с ними.

Ibgp – маршрутизация внтури зоны bgp, ebgp – маршрутизация между зонами bgp.

1. **Автономная система BGP. Пограничные маршрутизаторы**

Автономная система (autonomous system, AS) — набор маршрутизаторов, имеющих единые правила маршрутизации, управляемых одной технической администрацией и работающих на протоколе BGP. Автономные системы соединяются при помощи пограничнызх маршру тизаторов.