**Адресация на канальном уровне. MAC-адрес.**

На канальном уровне используется "плоская" схема адресации, основанная на физических (уникальных) адресах интерфейсов отдельных сетевых устройств (MAC- адресах).

Существует 3 типа MAC-адресов:

1)индивидуальный(unicast) - физический

2)групповой(multicast) | - логические

3) широковещательный |

Назначение MAC-адресов:

1)централизованно (записывается производителем сетевого оборудования)

2)локально(назначается админом сети, mac адрес должен быть уникальным)

1C:75:FD : D2:45:11

Производитель | Серия

**Формат Ethernet-кадра.**

6 байт | 6 байт |2 байта|46-1500 байт| 4 байта

--------------------------------------------------------------------------------------

Адрес | Адрес | Тип |Данные |Контрольная

получателя | отправителя| | | сумма

**Технология коммутируемого Ethernet. Таблица коммутации.**

Суть коммутируемого Ethernet в том, что вместо хаба используется свич (коммутатор) – устройство, которое работает на канальном уровне и обладает полносвязной топологией, что обеспечивает соединение всех портов друг с другом напрямую по технологии точка-точка. Коммутатор принимает кадр, анализирует заголовок, извлекает из него адрес получателя и сопоставляет его с таблицей коммутации, определяя порт, к которому подключено устройство. Таким образом, кадр передается на конкретный порт получателя, а не на все порты, как в случае с концентратором. Если же адрес не найден в таблице, коммутатор работает так же, как и хаб(отправка на все порты).

Порт коммутатора Мак - адрес

1 1С-75-08-D2-49-45

2 13-54-08-54-49-46

3 00-31-08-D2-49-47

**Классический Ethernet** - это технология локальных сетей, основанная на стандарте IEEE 802.3. Физический уровень включает в себя 3 варианта работы Ethernet, которые зависят от сред передачи данных. : коаксиальный кабель, витая пара, оптоволокно

*MAC-адреса* позволяют идентифицировать устройства, подключенные к сети Ethernet, и идентичных при этом быть не должно, в противном случае из нескольких устройств с одинаковыми адресами будет работать только одно.

Адреса могут назначаться как производителем оборудования (централизованно), так и администратором сети (локально).

Также не стоит забывать о коллизиях(накладывании друг на друга сигналов). Если сигнал, который принят, отличается от переданного, это означает, что произошла коллизия.

CSMA/CD :Механизм доступа к среде передачи данных, который обеспечивает устройствам возможность проверить, свободен ли канал для передачи данных, и в случае обнаружения коллизии – принимать меры для ее разрешения.

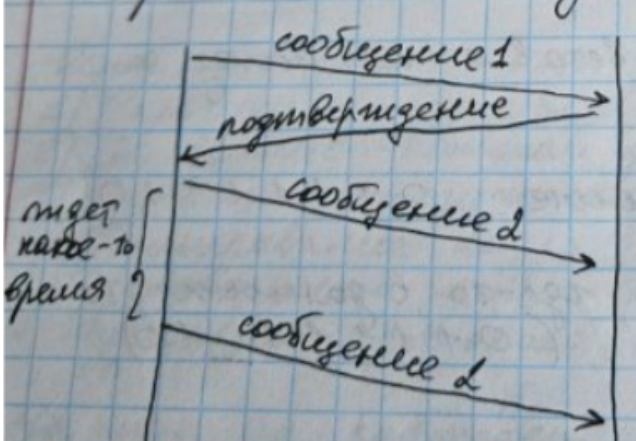
Обнаружение и исправление ошибок на канальном уровне.

**а)Обнаружение ошибок**

Если обнаружена ошибка то кадр отбразывается

**б)Исправление ошибок**

Необходимо добавить в кадр дополнительную информацию для восстановления в случае ошибки

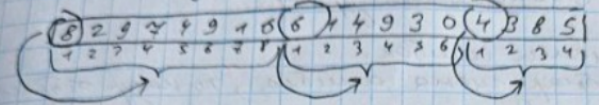
**в)Повторная передача данных**

В средах где ошибки редки используется метод A

В средах типа Wi-Fi используют метод Б

**Канальный уровень: методы выделения кадров.**

*Указатель количества байт* - в начало кадра добавляется длина кадра



*Вставка байт* - в начало и конец кадра вставляется специальная последовательность байт

StartOfText



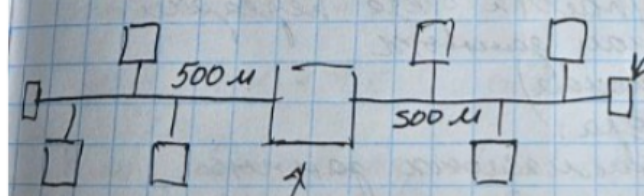
*Вставка бит* - перед каждым кадром вставляется последовательность и заканчивается ею. 01111110…данные... 01111110

*Средство физического уровня преамбула* - последовательность данных перед началом каждого кадра, состоит из 8 байт, первые 7 байт - 10101010 последний байт 10101011 (указывает на начало кадра)

**Физический уровень модели взаимодействия открытых систем (ISO OSI): среды передач.**

*Телефонный кабель* (500 - 200 м)

*Коаксиальный кабель* (толстый тонкий) - используется в технологии “Общая шина”



Повторитель(соединяет два сегмента сети)

Терминатор на концах кабеля для гашения сигнала

*Витая пара (скрученная пара проводов)* - скручивание снижает количество помех

*Оптический кабель* - для передачи используется свет

*Провода электропитания 220В*

*Беспроводные технологии* (Wi-Fi и инфракрасное излучение)

Спутниковая связь

Беспроводная оптика (лазеры)

**Физический уровень модели ISO: Характеристики линии связи.** *Затухание* - показывает уменьшение мощности эталонного синусоидального сигнала на выходе линии связи по отклонению мощности сигнала на выходе линии связи. A = 10\*lg(Pout/Pin) дб.

*Полоса пропускания* - непрерывный диапазон частот для которых затухание не превышает некоторой заранее заданной величины.

*Помехи -* нежелательное воздействие на сигнал ухудшающее возможность его распознавания при приеме.

*Пропускная способность* - максимальная скорость линии связи при передаче данных

*Количество ошибок* - характеристика канала показывающая частоту появления ошибок.

**Стек протоколов  TCP/IP** - это набор правил, определяющих формат и порядок передачи данных в сети. Он лежит в основе интернет-протоколов и используется в большинстве современных сетей

Прикладной  (HTTP, SMTP, FTP, DNS)

Транспортный (ТСP/UDP)

Интернет (IP, ARP, DHCP, ICMP)

Сетевые интерфейсы (Ethernet, WiFi)

**Модель OSI:**

*7)Прикладной(Application layer)* - доступ к сетевым службам

*6)Представительный(Presentation)* - представление данных.

*5)Сеансовый(Session)* - определение очередности сообщений. решение задачи одновременного доступа к  критическим операциям.

*4)Транспортный(Transport)* - организует передачу данных между процессами. организует гарантию доставки сообщений.

*3)Сетевой(Network)* - предназначен для построения сложный сетей с разными технологиями. Обеспечивает: 1.Согласование технологий канального уровня (Ethernet, WIFI..) 2.Обеспечение адресации с помощью IP адресов 3.Маршрутизация.

*2) Канальный(Data Link)* - передача сообщений из битов. Предлагаемые сетевому уровню услуги: 1.Установление логического соединения между узлами 2. Согласование скоростей передачи и приема информации 3. Обнаружение и коррекция ошибок  4. Управление доступом к разделяемой среде передачи

*1) Физический(Physical)* - передача сигналов по каналу связи

|-  Среда передачи  -|

**Физическая топология** – это физическое соединение устройств в сети.

**Логическая топология** – правило распространения сигнала в сети.

a)Общая шина –  все компы подключены к одной среде передачи данных

б)Звезда– подключены друг к другу через центральное сетевое устройство

в)Кольцо– каждый комп соединен с двумя соседними, данные передаются по кольцу.

г)Полносвязное соединение– все со всеми

д)Ячеистая– неполное полносвязное (без некоторых связей).

е)Дерево ё)Смешанная

**Стандартизация** определяет правила взаимодействия оборудования от разных производителей в сети.

IEEE – разрабатывает множество стандартов компьютерных сетей, включая Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), bluetooth 802.15).

IAB – совет по архитектуре интернета. 2 отдела: группа исследования инт. (IRTF)

группа проектирования (IETF, развивают RFC (документ со стандартами))

ISO – разрабатывает стандарт ISO/OSI, который определяет модель взаимодействия сетевых протоколов.

W3C – HTML и иные стандарты

**Основы организации компьютерных** *сетей. Архитектура компьютерной сети.*

**Для организации сети** используется методика декомпозиции. Задача разбивается на мелкие задачи. Уровень ниже предоставляет интерфейс для уровня выше

Комп 1 Комп 2

Уровень 3 Уровень 3

       | |

Уровень 2 Уровень 2

       | |

Уровень 1 Уровень 1

       | - Среда передачи - |

Сервис - функции реализующие уровень.

Интерфейс - набор предоставляемых операций.

Протокол - правила для связи N - го уровня с N - уровнем другого компа.

Инкапсуляция - включение сообщения вышестоящего уровня в сообщение нижестоящего.

**Компьютерная сеть** – это система из нескольких компьютеров и других устройств для обмена данными.

**Классификация:**

1. По типу коммутации:

 а)к. каналов – устанавливается соединение между отправителем и получателем, по которому идут сообщения. При разрыве соединения передача останавливается

б)к. пакетов - данные делятся на части, передаются независимо друг от друга.

2. По технологии передачи:

а)широковещательные сети - данные, переданные в сеть, доступны всем устройствам этой сети;

б)точка-точка - передача от одного устройства к другому, иногда с наличием промежуточных узлов.

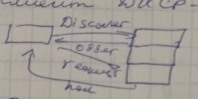
3.Протяженность:

а) Персональные (распространенные до 1м, bluetooth)  
б) Локальные (Внутри одного / нескольких зданий, до 1км)  
в) Муниципальные (масштаб города)

г) Глобальные (масштаб страны / континента)

д) Объединение сетей (Ethernet)

**Протокол DHCP** – это протокол, используемый в сетях TCP/IP для автоматической настройки сетевых параметров устройств, таких как IP-адреса, маски подсети, шлюзы и DNS-серверы. Протокол работает по технологии клиент-сервер. Клиент получает Ip - адрес, сервер назначает адрес. Протокол работает в режиме вопрос-ответ.



Discover запрос отправляет клиент в формате широковещательного формата. DHCP-сервер в ответ отправляет offer, предлагая ip-адрес. После клиент отправляет request, с выбраным ip-адресом, на который сервер отвечает подтверждением (ACK)

**Алгоритм определение адреса сети, широковещательного адреса по ip-адресу хоста и маске сети.**

*Адрес сети* - Делаем операцию логического И с маской подсети и IP адресом хоста

*Широковещательный адрес* - делаем операцию логического ИЛИ с ИНВЕРТИРОВАННОЙ маской подсети и IP адресом хоста

**Адресация на сетевом уровне. IP-адрес.**

IP-адрес — это адрес, используемый узлом на сетевом уровне. имеет длину 4 байта и обычно записывается в виде четырех чисел: 192.168.41.101

**Сетевой уровень: назначение, задачи.**

Сетевой уровень используется для создания крупной составной сети на основе разных технологий.

Задачи сетевого уровня:

1. Объединение сети разных технологий
2. Адресация адресов
3. Пакет отбрасывается, если нельзя его отправить
4. маршрутизация ( поиск оптимального пути для отправки пакета )

Нормальным языком

\* Обеспечение логической связи:  Сетевой уровень  предоставляет  логический  адрес  (IP-адрес)  для  каждого  устройства  в  сети  и  создает  маршруты  между  ними.

\* Управление  маршрутизацией:  Сетевой уровень  отвечает  за  определение  лучшего  пути  для  передачи  данных  между  двумя  устройствами  в  сети.

\* Разделение  сети  на  подсети:  Сетевой уровень  позволяет  разделить  большую  сеть  на  несколько  меньших  подсетей.  Это  позволяет  упростить  администрирование  сети  и  повысить  ее  безопасность.

\* Управление  заторами  и  конфликтами:  Сетевой уровень  обеспечивает  управление  заторами  и  конфликтами  в  сети.

**Сервисы технологии Wi-Fi.**

1.Базовый набор сервисов:   
 а. аутентификация ( запрос на подключение)

3 режима:

1) открытая аутентификация ( шифрование не выполнена, пароля нет)  
 2) персональная аутентификация ( все подключ. ус-ва используют один пароль )

3)prise aут. ( все имеют разные пароли, которые хранятся на серверах)

б. доп. аутентификация ( клиенту нужно пройти доп. аутент)

в. ассоциация ( клиент высылает свои параметры, если они подходят к точке доступа то все нормально )

г. отключение сети

2.Расширенный набор сервисов ( роуминг - переход от одной точки доступа к другой, сканирование - поиск точек доступа)

а. Пассивное - точки доступа рассылают инфу о себе и клиент может подключится

б. активное - клиент посылает широковещательный запрос точкам доступа, получив запрос они отправляются инфу о своих сетях

в. шифрование

**Технология Wi-Fi: управление доступом к разделяемой среде.**

1. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

\* Carrier Sense:  Устройства слушают канал связи, чтобы проверить, есть ли в нем сигнал от других устройств.

\* Multiple Access:  Несколько устройств могут пытаться передать данные одновременно.

\* Collision Avoidance:  Если устройство обнаруживает сигнал от другого устройства, оно откладывает передачу данных, чтобы избежать коллизии.

2. Как работает

шаг 1: Первый комп передает, а сет. слушает несущую частоту

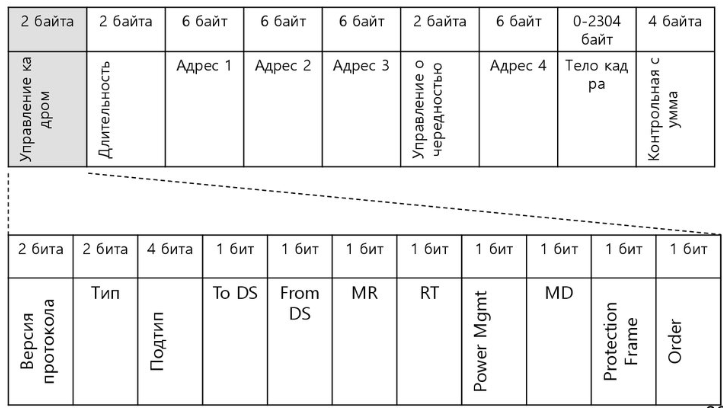
шаг 2: Передается подтверждение МКИ (временной)

шаг 2: Период молчания ( компы выбирают слуш. кол-во слотов ожид. )

Слот ожидания - промежуток времени, пока устройство ожидаем входящий сигнал. Размер слота зависит от времени распространения сигналов между любыми 2-мя устройствами.

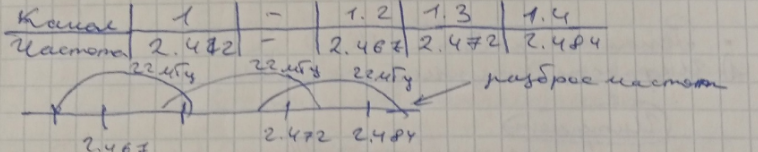
шаг 4. Если устройство успешно передает данные, оно ждет подтверждения от получателя

  Формат Wi-Fi-кадра.

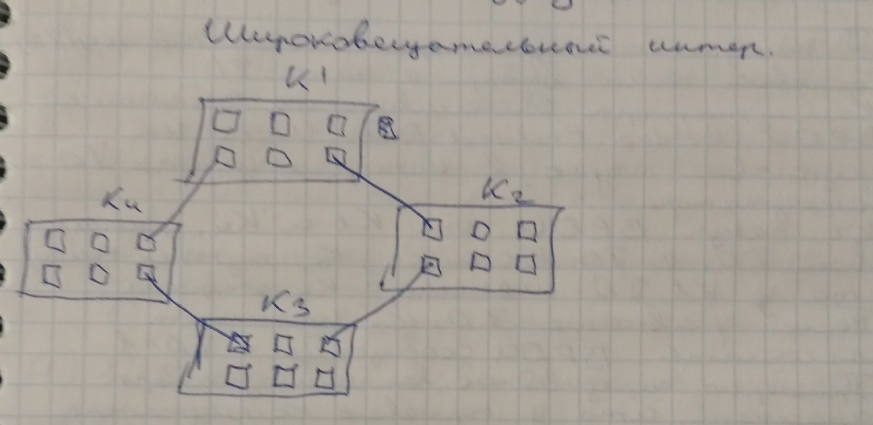


**Технология Wi-Fi: мультиплексирование с ортогональным частотным разделением**

Современные стандарты используют OFMD( Мультиплексирование с ортодоксальным разделением ). Данные разбиваются на части и передаются на разных частотах. Если сигнал на одной из частот исказится то его можно восстановить по сигналам из других частот.



**Протокол остовного дерева STP.**



Для ликвидации кольца применим протокол STP (SPanning Track Protocol) (протокол связующего дерева). Этот протокол описан в стандарте IEEE 802.1D. Протокол STP блокирует один из путей.

Алгоритм STP работы  STP:

1) Выбор корневого коммутатора. Выбранный по ID коммутаторы обменивается сообщениями BPDU на групповой адрес, в котором указан его ID.

После выбирается коммутаторы выбирают коммутатор с наименьшим ID.

2) Рассчитать кратчайший путь. Из двух путей блокируется тот чей путь наибольшей длины, длина зависит от количества промежуточных коммутаторов и скорости соединения

**Тегирование в виртуальной локальной сети (VLAN).**

При использовании VLAN каждый кадр данных, передаваемый по сети, помечается специальным идентификатором VLAN, называемым тегом. Этот тег содержит информацию о принадлежности к определенной VLAN.

1) Сетевой интерфейс отправляет кадр стандартного вида:

[mac Получателя][mac Отправителя][Тип][Пакет][КС]

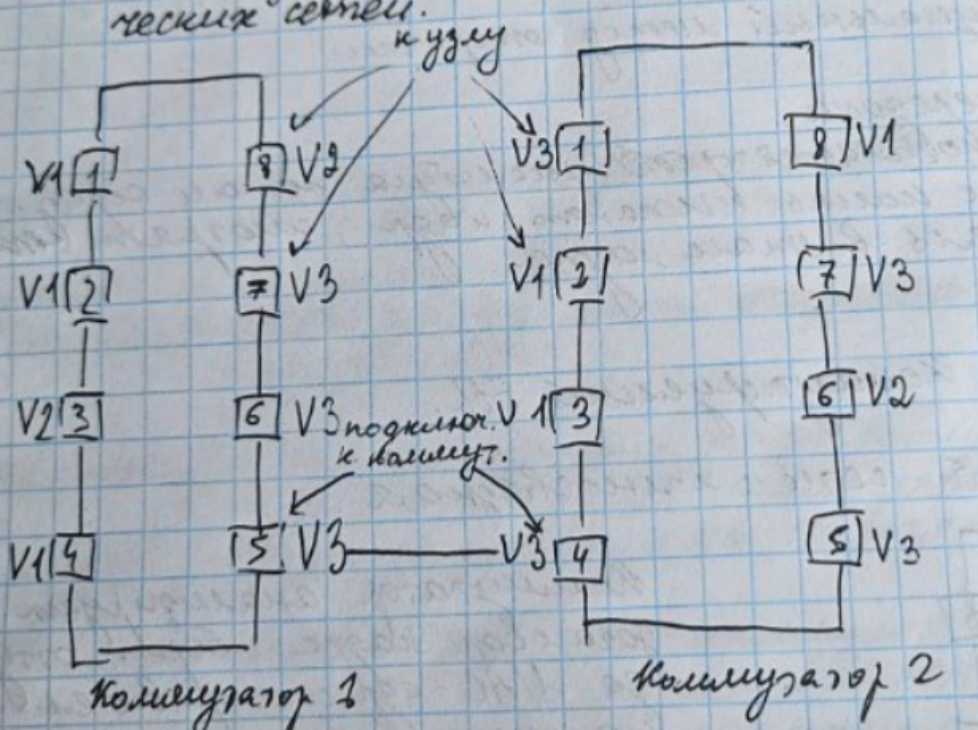
2) Этот пакет доходит до коммутатора, который изменяет кадр (увеличивает его на 4 байта)

[mac Получателя][mac Отправителя][0x800][3 (номер Vlan)][0x800][Тип][Пакет][КС]

3)После коммутатор удаляет эту инфу и передает пакет узлу

**Виртуальная локальная сеть VLAN.**

Технология позволяющая разделить одну физическую сеть на несколько логических сетей



**Метод доступа к разделяемой среде CSMA/CD.**

Множественный доступ к прослушиванию несущей частоты с предотвращением коллизии

*Прослушивание носителя (Carrier Sense):* Устройство, желающее отправить данные, сначала слушает среду (кабель) на предмет активности перед тем, как начать передачу. Если среда свободна, устройство может начать отправку.

*Множественный доступ (Multiple Access):* Множество устройств имеет доступ к тому же кабелю (или среде передачи данных) для передачи информации.

*Обнаружение коллизий (Collision Detection):* Если два устройства начинают передавать данные одновременно (то есть происходит коллизия), они обнаруживают эту ситуацию и прекращают передачу. После этого они ждут случайный промежуток времени перед новой попыткой передачи.

*Резервирование (Backoff):* После обнаружения коллизии устройства ждут некоторое случайное время перед тем, как повторно пытаться передать данные. Это снижает вероятность повторных коллизий.

**Сетевой уровень: фрагментация.**

Фрагментация - разделение передаваемых по сети пакетов трафика на отдельные части ( фрагменты), каждая из которых не превышает размер сети- маршрута.   
Каждый фрагмент будет обладать IP- заголовком не более 20 байт

Идентификатор пакета 16 бит|Флаги 3 бита| Смещение фрагмента 13 бит

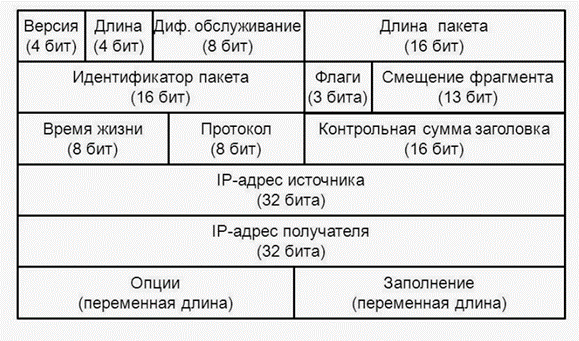
**Флаги:**

**1 бит – резерв, всегда 0**

2 бит -DonotFragments, запрещает фрагментацию

3 бит – MoreFragments, указывает на не фрагментированный или последний пакет в серии

**Формат IP-пакета.**



**Статическая маршрутизация. Таблица маршрутизации.**

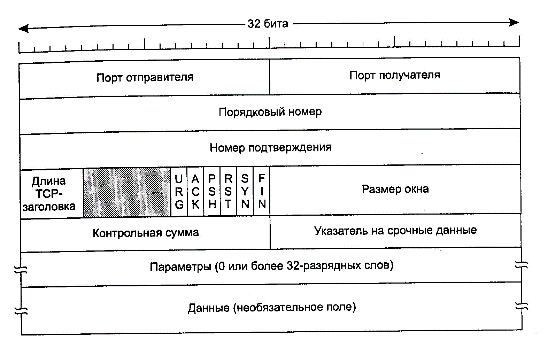
Статическая маршрутизация - это способ управления маршрутизацией в сети, при котором администратор вручную настраивает маршруты для каждого сетевого устройства. Маршруты вводятся в таблицу маршрутизации вручную, и эти маршруты не меняются автоматически, пока не будут вручную изменены администратором.

Сеть |Маска |Шлюз |Интерфейс

192.168.42.0 | 24 |192.168.42.1|192.168.42.2

Куда хотим | | Как попасть| Откуда

Если интерфейс имеет прямой выход в целевую сеть, то шлюзу присваевается значение On-Link



**Протокол TCP: управление потоком.**

Управление потоком TCP — это определение количества данных, которое может послать источник, прежде чем получить подтверждение от пункта назначения.

Для достижения управления потоком TCP использует протокол «скользящего окна». При таком методе оба хоста используют окно для каждого соединения. Окно выделяет небольшую часть буфера, содержащую байты, которые буфер может передать, прежде чем беспокоиться о подтверждении от другого хоста.

Окно называется «скользящим окном», потому что оно может скользить как по буферу данных, так и по буферу подтверждения, изменяя при этом величину байтов, которые можно посылать и принимать без принятия или посылки сигнала подтверждения.

**Формат TCP-сегмента.**

**Установка и разрыв соединения на транспортном уровне.**

*Установка соединения:*

1) Узел отправитель инициализирует установление связи путём посылки узлу получателю запроса синхронизации SYN.

2) Узел получатель подтверждает запрос синхронизации и задаёт свои параметры синхронизации ACK.

3) Узлу получателю посылается подтверждение, что обе стороны готовы для передачи данных.  
*Разрыв соединения*:

Для разрыва соединения TCP клиент генерирует команду закрытия соединения, которая приводит к отправке специального сегмента с флагом FIN=1.

Получив данный сегмент, сервер подтверждает его, а затем отсылает клиенту завершающий сегмент с флагом FIN=1. Получение этого сегмента подтверждается клиентом.

**Метод передачи данных «Скользящее окно».**

Вся суть метода заключается в том что отправитель посылает разом несколько пакетов данных не дожидаясь подтверждения, после чего получатель отправляет одно подтверждение, называемое кумулятивным.

Если какой то сегмент не был доставлен, то оправка всех сегментов повторяется снова.

При выборочном подтверждении при потере одного из нескольких сегментов будет отправлен только один.

**Протокол TCP: порядок следования сообщений.**

Однако гарантия доставки защищает только от потери сегментов, но не сохранение порядка следования сообщений.

Механизм очень простой, все сообщения нумеруются. При передачи отправитель включает в сегмент номер первого байта данных, который в нем содержится

**Протокол TCP: гарантия доставки данных.**

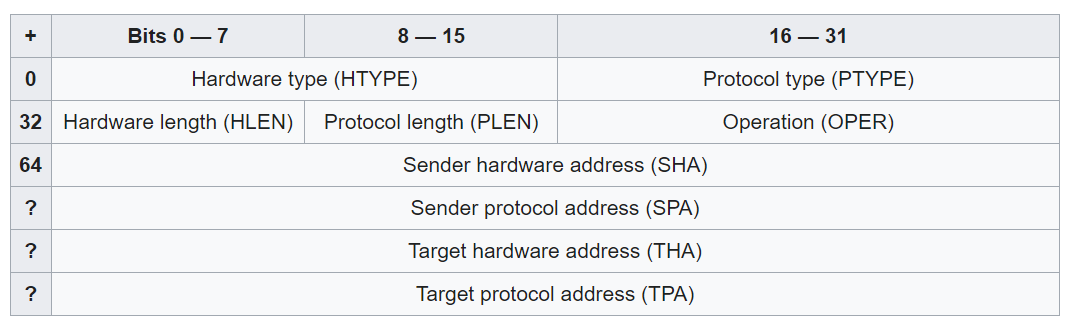
Для реализации гарантии доставки сообщений TCP использует подтверждение сообщений.

Отправитель посылает сегмент данных, после принятия получатель отправляет подтверждение (ACK). Затем отправляется следующий сегмент и снова подтверждение. Если произошла потеря сегмента данных то если по истечению времени ожидания подтверждения сегмент будет отправлен повторно.

**Протокол ARP.**

Протокол ARP позволяет автоматически определить MАК-адрес компьютера по его IP- адресу. Протокол работает в режиме запрос-ответ.

Компьютер, который хочет узнать МАК-адрес по известному IP-адресу, направляет ARP запрос "У кого IP 192.168.10.43?" Запрос отправляется на широковещательный MAK-адрес (FF:FF:FF:FF:FF:FF).



*HTYPE*Каждый канальный протокол передачи данных имеет свой номер, который хранится в этом поле.

*PTYPE*Код сетевого протокола. Например, для [IPv4](https://ru.wikipedia.org/wiki/IPv4) будет записано 0x0800.

*HLEN*Длина физического адреса в байтах. Адреса Ethernet имеют длину 6 байт (0x06).

*PLEN*Длина логического адреса в байтах. IPv4 адреса имеют длину 4 байта (0x04).

*Operation* Код операции отправителя: 0x0001 в случае запроса и 0x0002 в случае ответа.

*SHA*Физический адрес отправителя.

SPA Логический адрес отправителя.

THA Физический адрес получателя. Не требуется при запросе.

*TPA*Логический адрес получателя.

**Протокол UDP**

User Datagram Protocol - протокол дейтаграмм пользователя. не дает гарантий доставки пакетов, нет соединения, нет сохранения порядка сообщений. Но быстрее и менее затратен чем TCP

Формат заголовка

16 бит Порт отправителя |  16 бит Порт получателя

----------------------------------------------------------------------------------

16 бит Длина UDP | 16 бит Контрольная сумма UDP.

—------------------------------------------------------------------------------

Даннные

Минимальная длина UDP сообщения - 8 байт.

Максимальная длина -65535-8 = 65527-20 = 65507

**Адресация на транспортном уровне. Порты.**

Для адресации на транспортном уровне используются порты. Это просто число от 1 до 65 535. Номера у процессов на одном хосте не должны повторяться, иначе мы не сможем понять к какому конкретно процессу отправить пришедший пакет.

Записываются порты, следующим образом **192.168.1.3**:80. Выделенные жирным это IP-адрес, а 80 — это порт. Чтобы в интернете подключиться к какому-нибудь сервису и к службе необходимо указать ip адрес и соответствующий порт.

Зарезервированные порты: 1-1024

• 80 - HTTP (Web) •25 - SMTP (Электронная почта)

• 53 – DNS • 67,68 – DHCP • 443 - HTTPS

• Использовать может только root/Администратор

Зарегистрированные порты: 1025-49151

•Регистрация в Internet Assigned Numbers Authority (IANA)

Динамические порты: 49151-65535

Автоматически назначаются операционной системой сетевым приложениям

**Транспортный уровень: назначение, задачи.**

Транспортный уровень используется для передачи данных. Он отвечает не просто за передачу данных, но и за надежность, точность и эффективность этой операции.

Задачи:

1)передача данных меж. процессами на разных ПК

2)адресация процесса

3) предоставление нужного уровня надежности

**Взаимодействие сетевого и канального уровня.**

Канальный уровень получает данные от сетевого уровня, добавляет информацию к кадру и передает на физический уровень для отправки по среде передачи.

Сетевой уровень направляет данные на канальный уровень для дальнейшей передачи и обеспечивает маршрутизацию пакетов по сети.

**Протокол ICMP.**

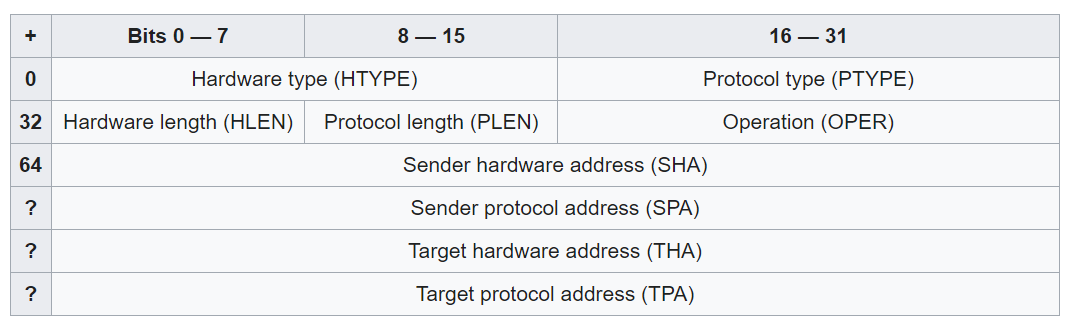
ICMP (Internet Control Message Protocol) - это протокол сетевого уровня модели OSI, который используется для передачи управленческих сообщений между устройствами в сети интернет. Он работает поверх протокола IP и позволяет устройствам сообщать друг другу о проблемах, возникающих во время передачи данных.



**Протокол ARP.**

Протокол ARP позволяет автоматически определить MАК-адрес компьютера по его IP- адресу. Протокол работает в режиме запрос-ответ.

Компьютер, который хочет узнать МАК-адрес по известному IP-адресу, направляет ARP запрос "У кого IP 192.168.10.43?" Запрос отправляется на широковещательный MAK-адрес (FF:FF:FF:FF:FF:FF).



*HTYPE*Каждый канальный протокол передачи данных имеет свой номер, который хранится в этом поле.

*PTYPE*Код сетевого протокола. Например, для [IPv4](https://ru.wikipedia.org/wiki/IPv4) будет записано 0x0800.

*HLEN*Длина физического адреса в байтах. Адреса Ethernet имеют длину 6 байт (0x06).

*PLEN*Длина логического адреса в байтах. IPv4 адреса имеют длину 4 байта (0x04).

*Operation* Код операции отправителя: 0x0001 в случае запроса и 0x0002 в случае ответа.

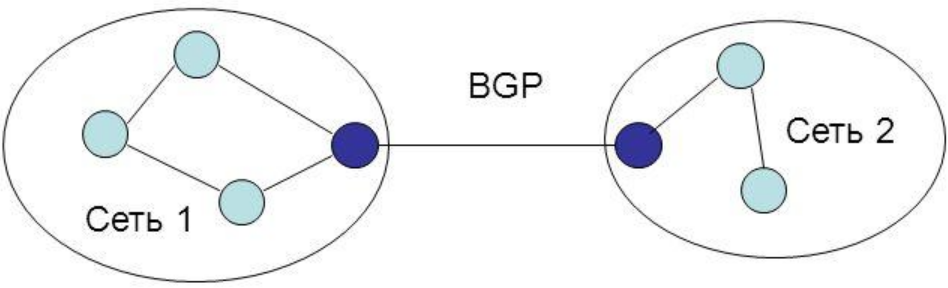
*SHA*Физический адрес отправителя.

SPA Логический адрес отправителя.

THA Физический адрес получателя. Не требуется при запросе.

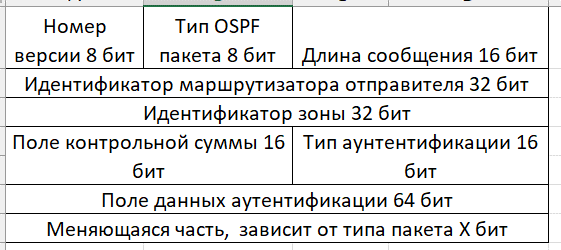
*TPA*Логический адрес получателя.

**Протокол внешней маршрутизации BGP.**

Border Gateway Protocol. Обеспечивает взаимосвязь между независимыми сетями. Использует рассылку только обновлений. Содержит ряд функций, повышающий безопасность (например, аутентификацию пользователя). Обеспечивает контроль за правильностью работы маршрутизаторов и сетевых соединений. В качестве протокола транспортного уровня использует ТСР. Обновления

**Протокол OSPF.**

OSPF — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути алгоритм Дейкстры.



**Динамическая маршрутизация** - это способ управления маршрутизацией в сети, при котором маршруты автоматически обновляются с помощью  протоколов динамической маршрутизации.  Эти протоколы позволяют устройствам  обмениваться информацией о маршрутах  между собой и автоматически  обновлять таблицу маршрутизации.  
**Протоколы** динамической маршрутизации:

К внешним протоколам относятся EGP :

EGP предназначен для анонсирования сетей, которые доступны для автономных систем за пределами данной автономной системы. По данному протоколу шлюз одной AS передает шлюзу другой AS информацию о сетях из которых состоит его AS.

BGP - В своих сообщениях он уже позволяет указать различные веса для маршрутов, и, таким образом, способствовать выбору наилучшего маршрута.

К внутренним протоколам относятся протоколы IGP:

RIP - предназначен для автоматического обновления таблицы маршрутов и использует алгоритм Белмана-Форда. Выбирается самый короткий маршрут (distance-vector).

OSPF — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

**Система доменных имен DNS.Типы записей DNS.**

DNS (Domain Name System - система доменных имен) представляет собой распределенную систему хранения и обработки информации о доменных зонах. Она необходима, в первую очередь, для соотнесения IP-адресов устройств в сети и более адаптированных для человеческого восприятия символьных имен.

Домен представляет собой именованную ветвь в дереве имен, включающую в себя сам узел (напр.,домен нулевого -., домен первого уровня ".com"), а также подчиненные ему узлы (напр., домен второго уровня "example.com", домен третьего уровня "mail.example.com" и т.д.). Для обозначения иерархической принадлежности доменных имен принято использовать понятие "уровень" - показатель положения узла в дереве доменов. Чем ниже значение уровня, тем выше иерархическое положение домена.

**45.  Трансляция сетевых адресов (NAT).**

Трансляция сетевых адресов по английский Network Address Translation (NAT) это технология замены ip адресов и портов в заголовке ip пакета. Чаще всего nat используется, чтобы заменить ip адрес внутренней сети на ip адрес из внешней сети. Это делается, чтобы преодолеть нехватку адресов IPv4.

Как работает технология NAT для преобразования внутренних адресов во внешние? Предположим, у нас есть сеть организации в которой используются внутренние адреса из диапазона 192.168.1.0. Есть Интернет в котором такие адреса использовать нельзя и внутренняя сеть подключаемая к интернет через устройство NAT.  Устройство NAT имеет один внешний ipv4 адрес 184.86.48.128 и когда компьютеры из внутренней сети хотят подключиться к интернету, устройство NAT преобразует ip адреса из внутренней сети в ip адрес внешней сети.

Есть три типа статический, динамический, один ко многим