### Протоколы

Протоколы - набор правил и соглашений по которым происходит передачи данных между узлами в сети

Стек протоколов TCP/IP - четырехуровневая модель, разработанная по инициативе Министерства обороны США. Используется сейчас как основной стек протоколов в сетях

##### Internet Protocol IPv4: (сетевой уровень)

Интернет протокол (ИП, Интернет протокол или межсетевой протокол) является маршрутизируемым протоколом сетевого уровня. На основе протокола IP работает большинство современных сетей



##### Стек TCP/IP:

4. Application layer(прикладной уровень) - потоки данных - HTTP, SSH, DNS

3.Transport layer(транспортный уровень) - сегменты - TCP, UDP

2. Internet layer(сетевой уровень) - пакеты - IP

1. Link layer(канальный уровень) - фреймы - Enhernet

Браузер отправляет запрос веб серверу, вышестоящий уровень обращается к нижестоящему уровню, сервер отправляет страничку обратно, размер которой превышает в 15-40 раз максимально допустимый. Страница разбивается на много частей, нумеруется и собирается обратно воедино. Браузер этим не занимается как и сам веб сервер (сложно, не унифицированно). Сборкой страницы будет заниматься нижестоящий уровень протокол - TCP (транспортный уровень). Если кто то потерялся, идет повторный запрос этого пакета, части

Межсетевой уровень позволяет пересылать сообщения между сетями (от нас до вайфай роутера, роутер до провайдера, через провайдера в дата центр и тд) - IP

Полученные данные кодируются, чтобы полученные данные получили именно мы в нашем канале

HTTP - TCP - IP - Ethernet - IP - TCP - HTTP

Соответствие уровней модели OSI и стека TCP/IP

4.Прикладной - (7.Прикладной 6.Представления 5.Сеансовый)

3.Транспортный - (4.Транспортный)

2. Сетевой - (3.Сетевой)

1. Канальный - (2.Канальный 1.Физический)

##### ICMP: (сетевой уровень)

Протокол служебных сообщений (ping), для проверкии удаленных хостов

Тип=8 - Эхо запрос

Тип=0 - Эхо ответ

Тип=3 Код=0 - Сеть недостижима

Тип=3 Код=1 - Узел недостижим

Тип=3 Код-3 - Порт недостижим

Тип=3 Код=4 - Необходима фрагментация, но установлен флаг ее запрета (DF)

Тип=11 - TTL истекло



##### ARP: (канальный уровень)

Основной протокол для диагностики сети, связывает канальный и сетевой уровень

Протокол позволяет узнать неизвестный МАК адрес по известному ИП адресу устройства в пределах локальной сети

Протокол связи ИП адреса и МАК адреса

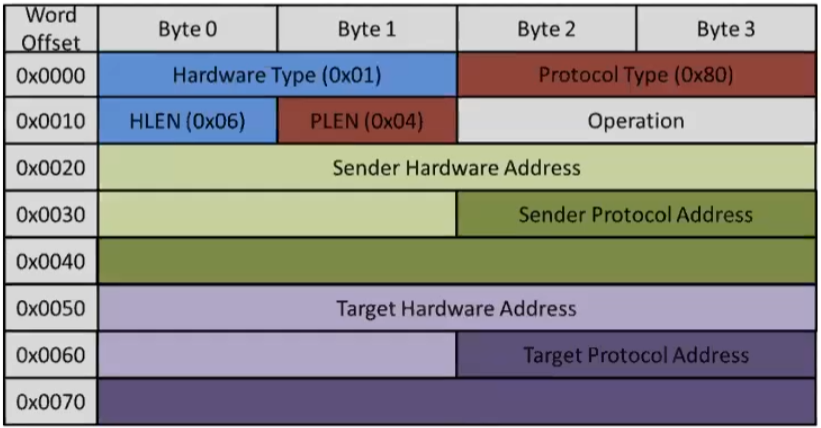
Протокол, какой МАК адрес соответствует ИП адресу

АРП таблица - АРП кэш. Связка ИП адреса с МАК адресом. Хранится в оперативной памяти (динамическая запись) в локальной сети

АРП запрос не проходит через устройства 3 уровня, поэтому в АРП кэш сохранится ИП шлюза и МАК адрес конечного броадкастного домена (роутера)

Если нужно передать АРП запрос в другую сеть, тогда в настройки МАК адреса получателя нужно указать МАК адрес шлюза (IP адрес шлюза в настройках сетевой карты)

Статические АРП записи нужно заносить руками (будут сохраняться после перезагрузки)



##### Протоколы маршрутизации:

Динамическая маршрутизация:

Позволяет роутерам обмениваться с такими же соседями

AS - автономной системой называют область IP сетей и роутеров, управляемых одним или несколькими операторами (RFC 1930)

**Автономная система** - группа роутеров, которые работают под управлением одного администратора или одной группы администраторов и используют общую стратегию маршрутизации

**Interior Routing Protocols (внутри AS):**

RIP, RIP2 (Routing Information Protocol (15 маршрутизаторв максимум)

OSPF (Open Shortest Path First)

IS-IS, IGRP, EIGRP и др.

**Exterior Routing Protocols (между AS):**

EGP (Exterior Gateway Protocol)

BGP (Border Gateway Protocol)

**Классификация протоколов маршрутизации:**



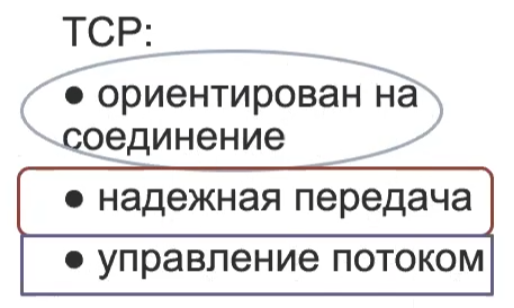
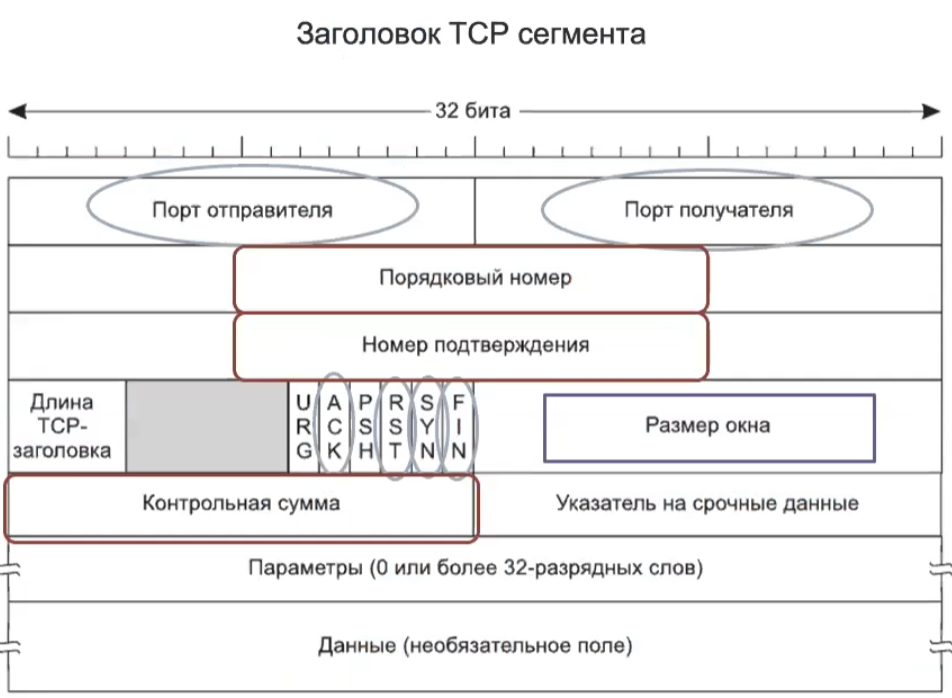
Дистанционно-векторные протоколы - оценивают расстояние, промежуточные маршрутизации

Протоколы маршрутизации по состоянию канала - оценивают качество, пропускную способность, задержку и тд

Протокол РИП выбирает дистанцию некст хопа по метрике (количеству маршрутизаторов до нужного узла, чем меньше тем лучше)

##### Протокол TCP:

TCP ориентирован на соединение, надежную передачу, управление потоком. Надежный протокол передачи данных транспортного уровня



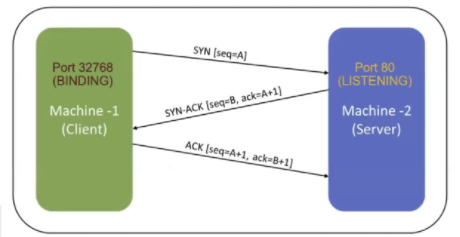
**Установка TCP соединения (сессии):**

Тройное рукопожатие, трехстороннее квитирование:

Клиент и сервер 3 раза жмут друг другу руки и начинается передача данных

Клиент инициатор стучится на сервер, отправляет служебный СИН сегмент. Если сервер принимает СИН сегмент и если сервер готов установить соединение с этим клиентом, он отправит СИНАГ (сегмент с флагами СИН и АК), будет свой номер последовательности и подтверждение сегмента. Клиент получает СИНАГ от сервера и отправляет финальный АК сегмент

Передача данных возможно только после установления соединения между клиентом и сервером



**Управление потоком:**

Методы управления потоком:

Буферизация - поток данных буферизируется в ожидание паузы

Останавливающее сообщение - передача источником сообщения о снижение скорости передачи с помощю ICMP

Метод скользящего окна - управление количеством передаваемых данных в единицу времени

**Сокет (программный интерфейс):**

Интерфейс сокета Беркли используется для взаимодействия между компьютерами в сети или процессами запущенными на компьютере.

Сокеты - это стандарт интерфейсов для транспортных подсистем.

Различные варианты сокетов могут быть реализованы в разных ОС и языках программирования

Операция SOCKET создает новый сокет и записывает его в таблицу транспортной подсистемы. Параметры вызова задают тип используемого формата адресации, тип применяемого сервиса (например,, надежный поток байтов) и протокол.

Например, при обращении к серверу geekbrains.ru на HTTP порт сокет будет выглядеть так: 5.61.239.21:80, а ответ будет поступать на mmm.nnn.ppp.qqq:xxxxx

**Базовые операции сокетов для TCP:**

SOCKET (Сокет) - Создание нового сокета

BIND (Связать) - Привязать локальный адрес и сокет

LISTEN (Ожидать) - Слушать входящие соединения, указав номер очереди

ACCEPT (Принять) - Подтвердить установление входящих соединений

CONNECT (Соединить) - Инициировать процесс установления соединения

SEND (Послать) - Передать информацию по установленному соединению

RECEIVE (Получить) - Принять информацию по установленному соединению

CLOSE (Закрыть) - Закрыть сеанс связи и отправить сообщение о завершение соединения

**Флаги:**

SYN - рукопожатие

SYN, ACK - второе рукопожатие

ACK - финальное подтверждение

FIN, ACK - закрытие соединения

##### SCTP:

Транспортные протоколы развиваются и встают новые задачи обработки групповых связанных потоков. Например, браузер может запрашивать с сервера несколько страниц, в этом случае создаются отдельные сокеты для каждого соединения

SCTP (Stream Control Transmission Protocol - протокол передачи с управлением потоками), описанный в RFC 4960.

Протокол работает по аналогии с TCP. Из нововведений нужно выделить использование многопоточности и встроенную защиту от DDoS атак, в отличии от TCP

Протокол может использовать синхронное соединение хостов по нескольким независимым физическим каналам (multi-homing) например безспроводную и проводную сеть одновременно

Используется ЧЕТВЕРНОЕ рукопожатие

##### UDP:

User Datagram Protocol (UDP) - протокол передачи дейтаграмм пользователя

Ненадежный протокол, не требует предварительной установки соединения между отправителем и получателем, не нужно иметь огромный заголовок и содержать в нем огромное количество полей

Не контролирует соединение, не управляет потоком, не гарантирует доставку всех переданных сегментов

UDP гораздо быстрее, заголовок легче

Протокол используется в потоковой передаче видео и аудио, где более критична задержка нежели гарантированные переданные сегменты (важна скорость передачи данных и задержки)

Заголовок UDP сегмента состоит из 32 битов (4 поля):

Порт отправителя Порт получателя

Длина UDP Контрольная сумма UDP

UDP:

Без установления соединения

Ненадежная передачи

Используется служебными протоколами в локальных сетях RIP, SNMP, DHCP, TFTP и потоковыми приложениями

**Модификации протокола:**

**DCCP: (Гибрид между TCP и UDP)**

Является усовершенствованным протоколом UDP, в который добавили механизм управления перегрузкой. Более подробную информацию можно посмотреть в RFC 4340

DCCP отличается следующими пунктами:

Поток дейтаграмм реализован с механизмом подтверждения получения данных, но без повторной отправки в случае потери данных

Ненадежный алгоритм установления и закрытия соединения

Согласование параметров передачи даных при установлении соединения