

# **Протоколы семейства TCP/IP**

# Компьютерная сеть

Компьютерная сеть — это множество вычислительных устройств, взаимодействующих между собой и совместно использующих ресурсы. Понятие сеть близко по смыслу к понятию графа.

# **Локальные и глобальные компьютерные сети**

**Personal Area Network (PAN).**

**Local Area Network (LAN).**

**Metropolitan Area Network (MAN).**

**Wide Area Network (WAN).**

# Сетевые модели

Под сетевой моделью понимаются концептуальные основы, которые стандартизируют сетевое взаимодействие. Это основные термины, а также назначение и функции сетевых компонентов. Сетевая модель разделяет сетевые компоненты и их функции на уровни. Каждый слой сетевой модели имеет определённое назначение и функции.

# Модель TCP/IP

- это базовый набор сетевых протоколов и правил, определяющий, как данные разбиваются, упаковываются, передаются, маршрутизируются и принимаются в интернете и компьютерных сетях.

# Модель TCP/IP: Базовые понятия

- хост (host);
- сообщение;
- IP-датаграмма;
- пакет;
- фрейм;
- IP-адрес;
- MAC-адрес;
- TCP-сегмент;
- UDP-датаграмма;
- MTU.

# Модель TCP/IP: Единицы данных

**Сообщение (Message):** Данные в чистом виде на уровне приложения (например, текст письма или запрос браузера).

**TCP-сегмент:** Часть сообщения, к которой добавлен заголовок протокола TCP. TCP гарантирует доставку и правильный порядок частей, «нумеруя» их.

**UDP-датаграмма:** Аналог сегмента, но для протокола UDP. Здесь нет гарантии доставки и проверки очереди (используется для видеосвязи или игр, где важна скорость, а не точность).

# Модель TCP/IP: Единицы данных

Р-датаграмма (Пакет): Сегмент, упакованный в заголовок протокола IP. Здесь добавляются IP-адреса отправителя и получателя. На этом этапе данные готовы к путешествию между сетями через роутеры.

Фрейм (Кадр): Пакет, упакованный для передачи по физическому проводу или радиоэфиру. К нему добавляются MAC-адреса.

# Технические ограничения

**MTU (Maximum Transmission Unit):** Максимальный размер «посылки» (обычно фрейма), который может быть передан через сетевой интерфейс за один раз.

- Стандартное значение для Ethernet — 1500 байт.
- Если IP-пакет больше, чем MTU, его приходится делить на части (фрагментация).

# Как работает TCP/IP сеть

IP-сеть представляет собой множество связанных между собой хостов. Хосты связаны непосредственно или косвенно при помощи ретранслирующих устройств (маршрутизаторов и коммутаторов).

# Как работает TCP/IP сеть

Для приёма сообщений из сети и отправку их в сеть хост использует интерфейсы. Физический интерфейс отправляет и принимает фреймы, а логический интерфейс отправляет и принимает IP-пакеты. Физический интерфейс идентифицируется MAC-адресом, логический интерфейс – IP-адресом.

# Как работает TCP/IP сеть

Передаваемое сообщение представляет собой UDP-датаграмму или TCP-сегмент. Сообщение содержит заголовок и полезные данные. Чтобы передать сообщение внутри IP-сети оно помещается в IP-датаграмму. Конкретный физический интерфейс позволяет передавать данные порциями, которые имеют определённый максимально допустимый размер (MTU). Если размер IP-датаграммы превышает MTU, выполняется её фрагментация и создаётся несколько IP-пакетов, иначе создаётся только один IP-пакет для всей IP-датаграммы.

# Как работает TCP/IP сеть

IP-пакет в соответствии с таблицей маршрутизации хоста передаётся на выбранный логический интерфейс.

# Как работает TCP/IP сеть

Логический интерфейс сам непосредственно не может передать IP-пакет, он использует физический интерфейс. Физический интерфейс передаёт данные фреймами. Фрейм имеет заголовок и полезные данные (payload). В заголовке фрейма указывается MAC-адрес получателя, MAC-адрес отправителя и какому протоколу принадлежат данные в payload (Ethertype). Адрес отправителя известен, это MAC-адрес интерфейса отправляющего хоста. Для протокола IPv4 Ethertype=0x0800.

# Как работает TCP/IP сеть

Адрес физического интерфейса определяется путём посылки ARP-сообщения в широковещательный домен. ARP-сообщение инкапсулируется во фрейм, у которого EtherType = 0x0806 (ARP). В сообщении указывается MAC-адрес отправителя, широковещательный MAC-адрес получателя и интересующий IP-адрес. Хост с физическим интерфейсом, которому назначен этот IP-адрес в ответном сообщении, указывает MAC-адрес этого физического интерфейса. Чтобы не отсыпать ARP-сообщение каждый раз, соответствие IP-адреса MAC-адресу сохраняется в кеше хоста.

# Как работает TCP/IP сеть

После передачи фрейма на другой сетевой интерфейс из него извлекается содержимое IP-пакета, и, если IP-адрес логического интерфейса хоста соответствует IP-адресу получателя, он собирается в IP-датаграмму. Из IP-датаграммы извлекается TCP-сегмент или UDP-датаграмма. Из них извлекаются сами данные и передаются процессу операционной системы, который уже понимает, что с ними делать дальше.

# Как работает TCP/IP сеть

Иначе IP-пакет или отвергается или пересылается далее в соответствии с таблицей маршрутизации хоста. При отсылке он опять передаётся на логический интерфейс. Там упаковывается во фрейм и отсылается.

# Адресация

Адресация позволяет указать источника и получателя данных. Для слоя L2 получатель и отправитель идентифицируются MAC-адресами, для L3 — IP-адресами, для L4 — портами.

# Адресация

физический интерфейс имеет уникальный МАС-адрес, состоящий из 6 байт.

# Адресация

Всего возможно  $2^{32}$  IP-адресов, но количество допустимых IP-адресов хостов меньше, а глобальных (IP-адресов, видимых в интернете) ещё меньше.

# Адресация

Каждый IP-адрес — это последовательность из 32 бит. Первые n-бит в IP-адресе несут информацию о том, к какой сети принадлежит IP-адрес, оставшиеся биты — это уникальный адрес внутри этой сети.

# Адресация

Если выполнить побитовое “И” IP-адреса с маской сети, то получится идентификатор сети. Если выполнить побитовое “И” с инвертированной маской сети, то мы получим уникальный адрес внутри сети. Чтобы можно было проще представить информацию об IP-адресе, и какая его часть используется для идентификации сети, используется CIDR-нотация.

Писать маску вроде 255.255.255.0 долго. Поэтому используется /24 просто говорит: «Первые 24 бита из 32 – это адрес сети». Оставшиеся 8 бит ( $32 - 24 = 8$ ) отданы под устройства.

# Адресация

В 8 битах можно зашифровать 256 комбинаций (от 0 до 255). Но использовать для устройств можно только 254:

- Все нули в конце (напр., .0): Это «имя» самой сети. Его нельзя присвоить компьютеру.
- Все единицы в конце (напр., .255): Сообщение, отправленное на этот адрес, получат сразу все устройства в этой сети.

# Адресация

Например, запись 192.168.0.0/24 означает: сеть имеет идентификатор 192.168.0.0, 24 первых бита используются для идентификации сети. Для кодирования хостов используется 8 последних бит. Максимальное количество хостов в сети – 254 (0 – сеть, 255 – широковещательный адрес).

# Адресация

Не все сети могут быть видимыми в сети и некоторые из них используются для специальных целей.  
(серые/частные IP, напр 192.168.x.x)

# Виды адресов

**Индивидуальный адрес** (unicast address) — это уникальный адрес в сегменте сети, или локальной (глобальной) сети.

**Широковещательный адрес** (broadcast address) — общий для всех сетевых устройств, имеющих MAC-адрес или для всех хостов подсети. Сообщения, посылаемые на широковещательный адрес, будут получены всеми узлами.

# Виды адресов

Можно сделать так, чтобы сообщения отсылались только тем узлам, которые в них заинтересованы. Для этого используются групповые адреса(multicast address).

# Маршрутизация в IP-сетях

Если необходимо отправить IP-пакет по определённому адресу, то каждый раз просматривается таблица маршрутизации хоста, и на основании её определяется, нужно его отправлять на хост внутри сети, которой принадлежит отправляющий хост, или нужно его перенаправить на особый хост (маршрутизатор, шлюз), который решит, что делать с ним дальше. (Что за шлюз такой?)

# Маршрутизация в IP-сетях

WiFi-роутер обладает рядом функций и фактически состоит из нескольких устройств. Одной из важных функций WiFi-роутера является функция трансляции сетевых устройств (Network Address Translation — NAT), позволяющая устройствам из локальной сети получить доступ в интернет.

# Расчёт контрольной суммы

При передаче данных по сети могут происходить различные ситуации, когда принятые данные могут отличаться от тех, которые были переданы. Чтобы определить такие случаи, с данными передаётся контрольная сумма, вычислив которую на принимающей стороне и сравнив с принятой, можно дать ответ, передались ли данные верно, или где-то произошла ошибка передачи данных. Как правило, сообщения с неверной контрольной суммой отвергаются, и сообщение считается потерявшимся. (контрольные суммы вычисляются сетевым адаптером.)

# Стек протоколов TCP/IP

Ethernet II;

IP – Internet Protocol;

ICMP – Internet Control Management Protocol;

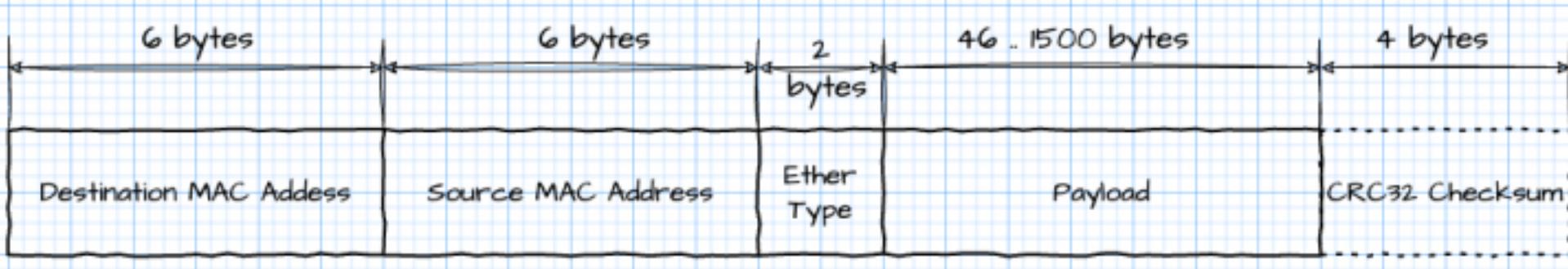
UDP – User Datagram Protocol;

TCP – Transmission Control Protocol;

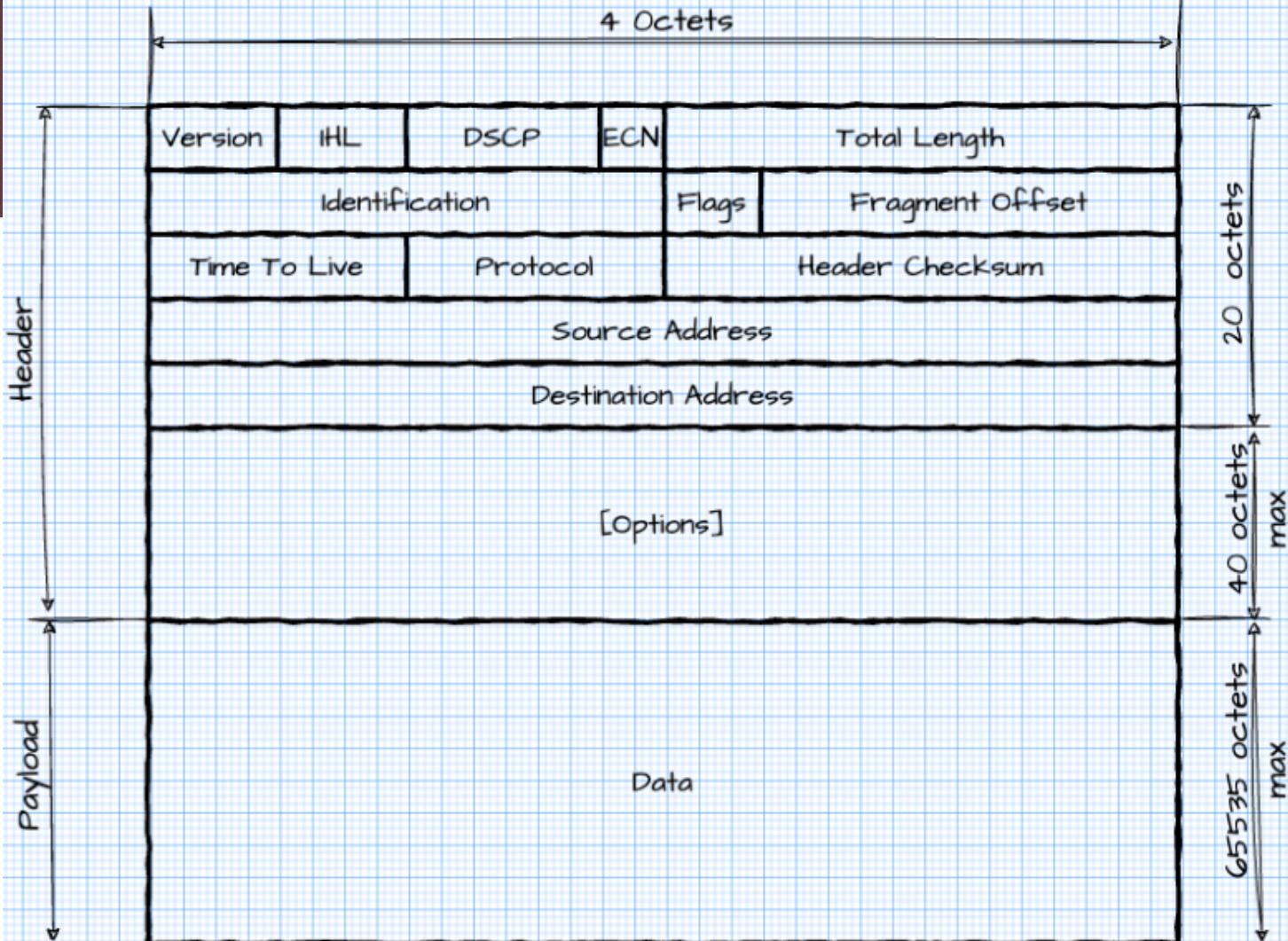
DHCP – Dynamic Host Configuration Protocol;

DNS – Domain Name Service.

# Протокол Ethernet



# Структура IP-пакета



\* IHL - Internet Header Length in 32 bit words

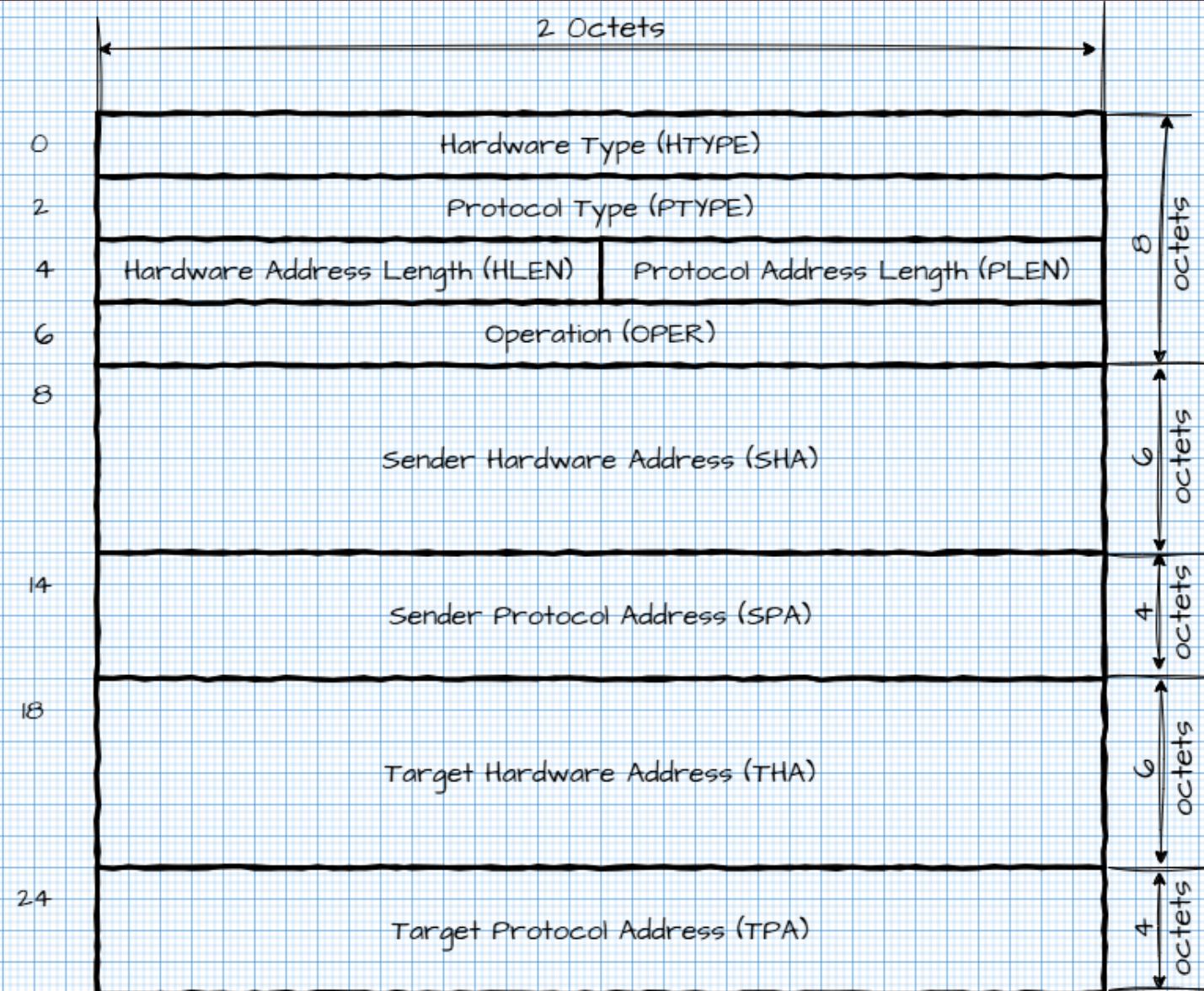
# MTU

Размер IP-пакета ограничивается MTU (Maximum Transmission Unit) — максимально возможное количество данных, которые могут быть переданы одним фреймом на канальном уровне. Чтобы передать IP-датаграмму, которая содержит полезных данных больше, чем может поместиться в один IP-пакет, используется фрагментация.

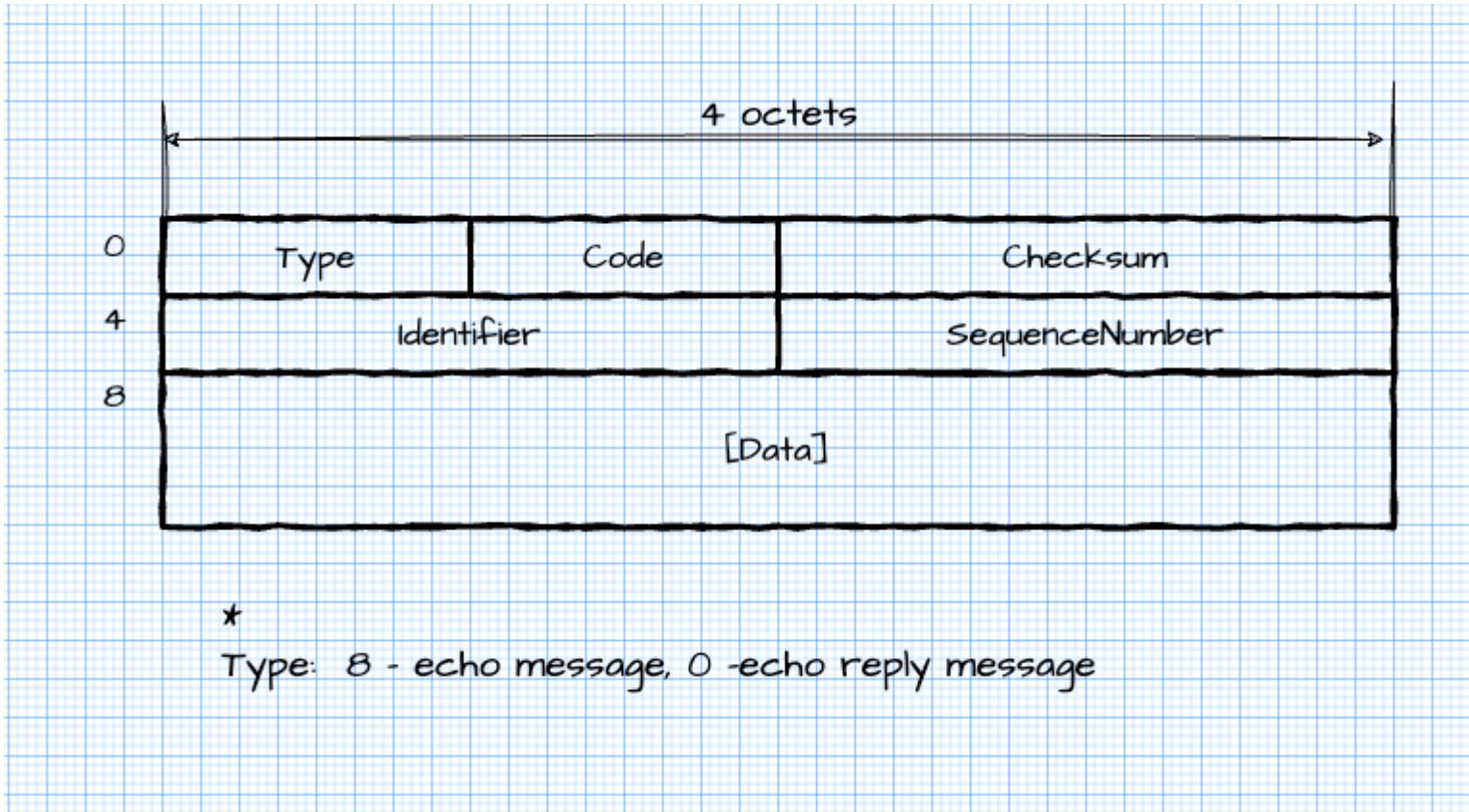
# Протокол ARP

Протокол ARP используется для определения МАС-адреса физического интерфейса хоста по его IP-адресу.

# ARP



# ICMP сообщение



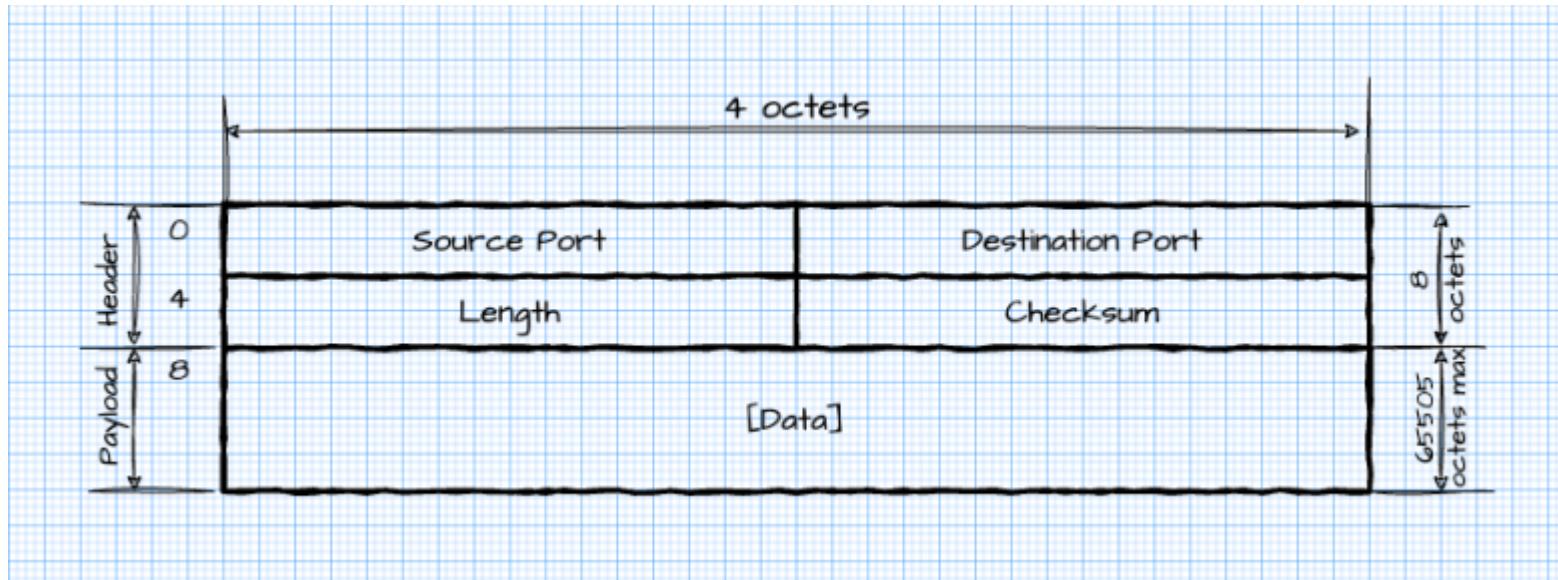
# Протокол UDP

Протокол позволяет двум процессам обмениваться UDP-датаграммами.

Протокол используется в качестве транспортного протокола там, где на транспортном уровне допускается дублирование получаемых данных, пропуск данных или не важен порядок, в котором данные будут доставлены.

Например, в потоковом видео или аудио данные пропускаются, так как повторная передача данных является в этом случае бессмысленной.

# Структура сообщений UDP

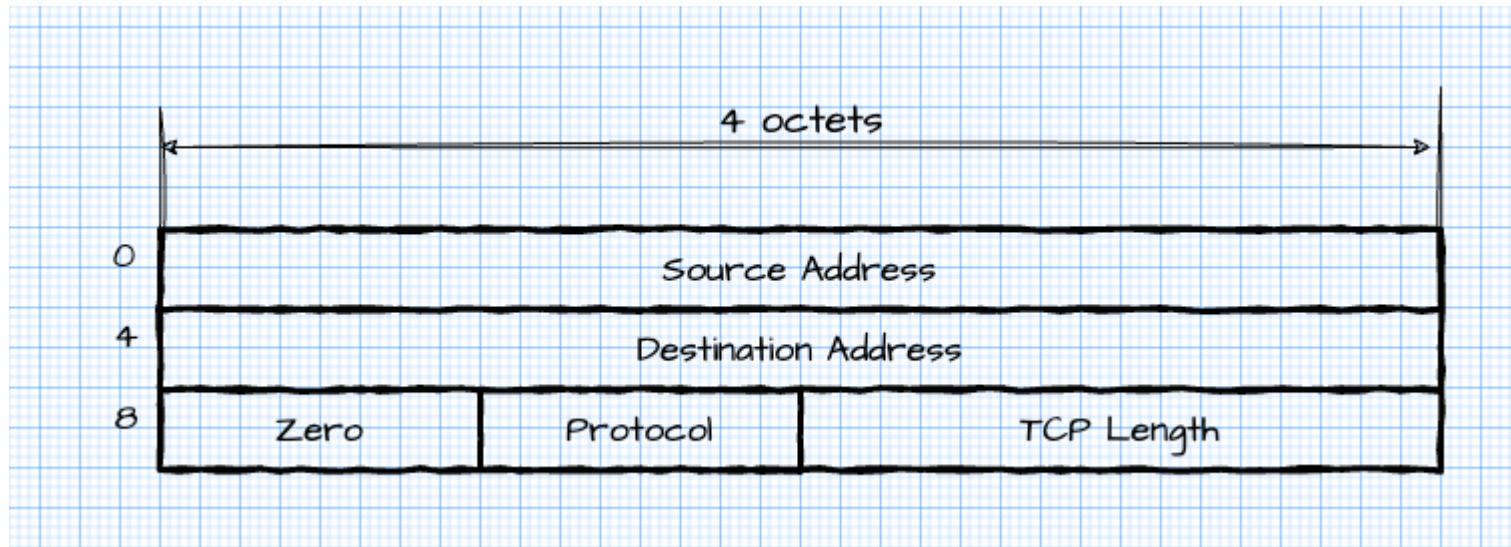


# Протокол TCP

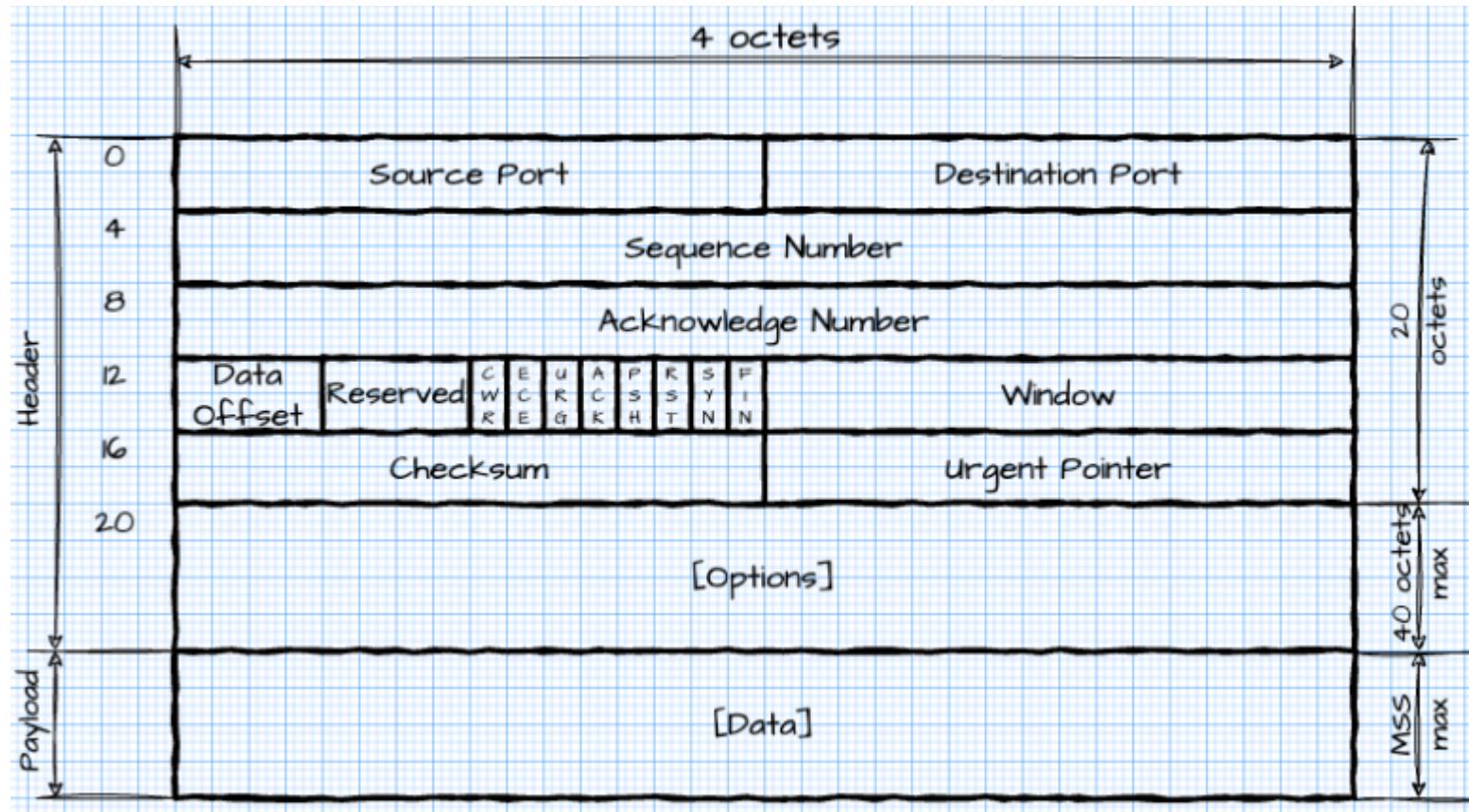
Назначение протокола TCP — создать надёжное виртуальное полнодуплексное соединение между процессами.

Сообщения, используемые в протоколе TCP, называются TCP-сегментами.

# Протокол TCP



# Протокол TCP



IDE/ATAPI CD-ROM Device Driver Version 2.14 10:48:22 02/17/98  
CD-ROM drive #0 found on 1F0h port slave device, v1.04

Killer v1.0 Copyright 1995 Vincent Penquerc'h. All Rights Reserved.  
Killer installed in memory.  
DOSKEY installed.  
DOSLFN 0.32o: high loaded consuming 11840 bytes.  
MSCDEX Version 2.25

Copyright (C) Microsoft Corp. 1986-1995. All rights reserved.

Drive D: = Driver IDE-CD uni

SHARE v7.10 (Revision 4.11.1492)

Copyright (c) 1989-2003 Datalight,

installed.

CuteMouse v1.9.1 [DOS]

Installed at PS/2 port

Locking volumes...

Now you are in MS-DOS 7.10 prompt.

C:>\_

