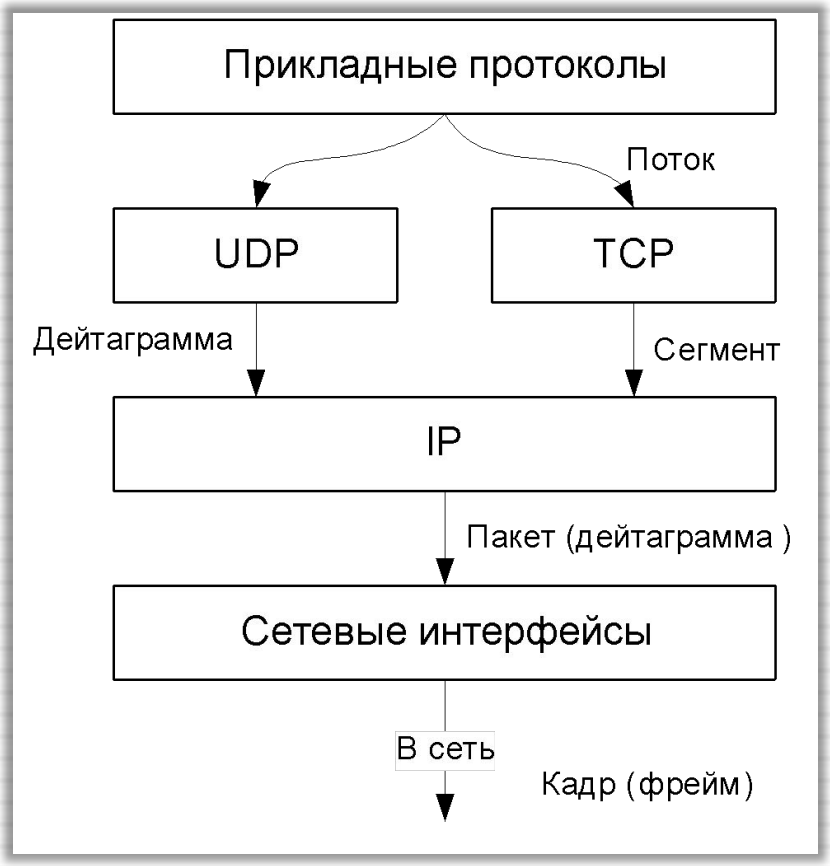
СТЕК ПРОТОКОЛОВ TCP/IP

Составляющие модели TCP/IP

Уровни OSI	Уровни стека TCP/IP	Протоколы
Прикладной (Application)	Прикладной (Application)	FTP, HTTP, SMTP, DNS
Представительный (Presentation)		
Сеансовый (Session)		
Транспортный (Transport)	Транспортный (Transport)	TCP, UDP
Сетевой (Network)	Сетевой (Network)	IP, ICMP
Канальный (Link)	Уровень сетевых интерфейсов (Network Interface)	Протоколы инкапсуляции и преобразования адресов
Физический (Physical)		

Название единиц данных, используемых в TCP/IP



- Потоком называют данные, поступающие от приложений на вход протоколов транспортного уровня TCP и UDP.
- Протокол TCP «нарезает» из потока данных сегменты.
- Единицу данных протокола UDP часто называют дейтаграммой (или датаграммой).
- **Дейтаграмма** – это общее название для единиц данных, которыми оперируют протоколы без установления соединений. К таким протоколам относится и протокол межсетевого взаимодействия IP.
- Дейтаграмму протокола IP называют также пакетом.
- В стеке TCP/IP принято называть кадрами (фреймами) единицы данных протоколов, на основе которых IP-пакеты переносятся через подсети составной сети. При этом не имеет значения, какое название используется для этой единицы данных в локальной технологии

Сетезависимые и сетенезависимые уровни TCP/IP

- Можно выделить уровни, функции которых зависит от конкретной технической реализации сети, и уровни, функции которых ориентированы на работ с приложениями.
- Сетенезависимые:
  - Прикладной
  - Транспортный
- Сетезависимые:
  - Сетевого взаимодействия
  - Сетевых интерфейсов

Типы адресов TCP/IP

- **Локальный адрес-** такой тип адреса, который используется для доставки данных в пределах подсети, являющейся элементом составной интерсети.
  - Если подсетью интерсети является локальная сеть, то локальный адрес – это MAC-адрес.
  - MAC-адрес назначается сетевым адаптерам и сетевым интерфейсам маршрутизаторов. MAC-адреса назначаются производителями оборудования и являются уникальными, так как управляются централизованно.
- **IP-адрес** - основной тип адресов, на основании которых сетевой уровень передает пакеты между сетями.
  - IP-адрес назначается администратором во время конфигурирования компьютеров и маршрутизаторов.
- **Символьные имена** (доменные имена).
  - Составляющие полного символьного имени в IP-сетях разделяются точкой и перечисляются в следующем порядке: сначала простое имя конечного узла, затем имя группы узлов (например, имя организации), затем имя более крупной группы (поддомена) и так до имени домена самого высокого уровня (например, домена объединяющего организации по географическому принципу: RU – Россия, UK – Великобритания, SU – США).
  - В сетях TCP/IP используется специальная распределенная служба DNS (*Domain Name System*), которая устанавливает это соответствие на основании создаваемых администраторами сети таблиц соответствия. Поэтому доменные имена называют также DNS-именами.

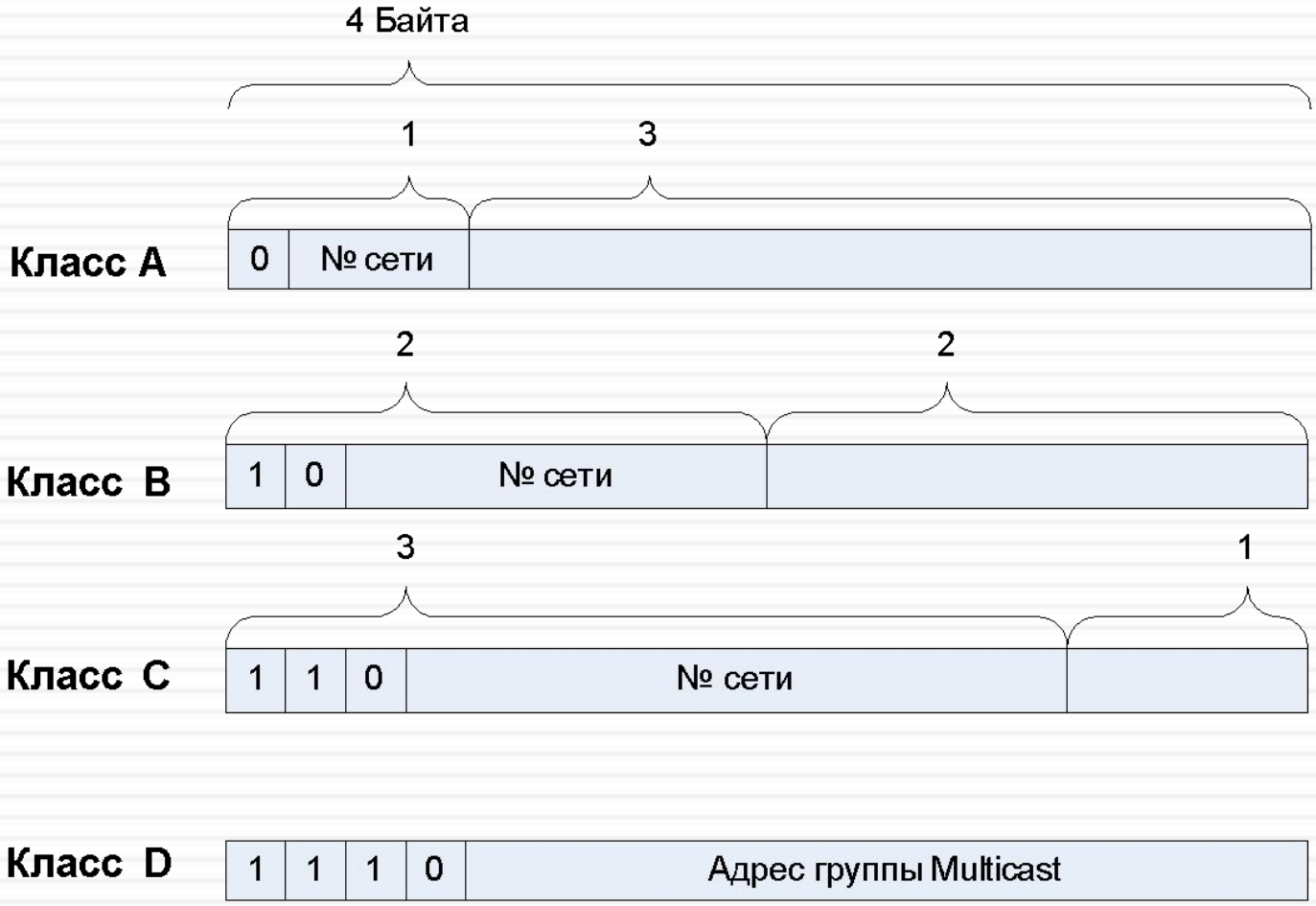
1. Сетевой уровень.

Протокол IP и IP-адресация

IP адрес (v4)

- Имеет размер 4 Байта (32 бита) и состоит из двух частей – номера сети и номера узла в сети.
- Наиболее часто встречается форма записи в виде 4 десятичных чисел (октетов), разделенных точкой.

Классы IP-адресов



Характеристики адресов

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Max число узлов в сети
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^{8}
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервирован

Групповой адрес (класс D) идентифицирует группу узлов, которые в общем случае могут принадлежать разным сетям. Интерфейс, входящий в группу, получает, вместе с индивидуальным IP адресом еще и групповой.
При отправке пакета с адресом класса D в качестве адреса получателя, он будет доставлен всем узлам, входящим в группу

Использование масок при IP-адресации

Пример:
Сеть класса C – 194.149.115.0
Последний байт сетевой маски:
- в двоичной записи – .11110000
- в десятичной записи – .240

Количество подсетей = количество узлов в подсети = $2^4-2 = 14$

№	Подсеть (последний байт)	Адрес подсети (десятичный)	Max число хостов
1	00000000 – 00001111	194.149.115.0	0
2	00010000 – 00011111	194.149.115.16	14
3	00110000 – 00111111	194.149.115.32	14
4	01000000 – 01001111	194.149.115.48	14
…	…	…	…
16	11110000 – 11111111	194.149.115.240	0

Частные адреса

Определены и зарезервированы три диапазона адресов, которые могли использоваться только для внутренних целей, по одному от каждого из классов IPv4 A, B и C:

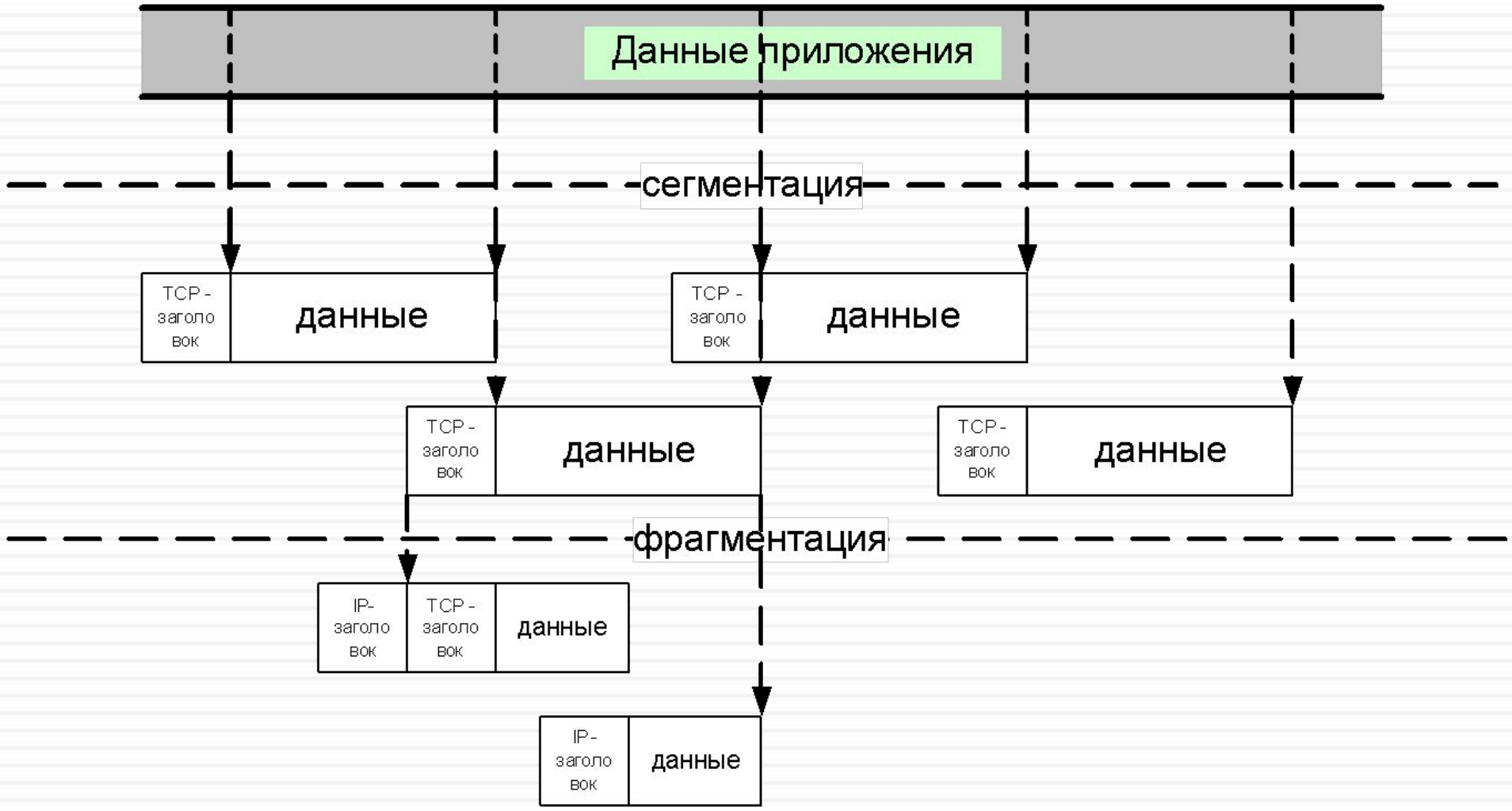
```
10.0.0.0    -  10.255.255.255.
172.16.0.0  -  172.31.255.255.
192.168.0.0 -  192.168.255.255.
```

Эти диапазоны были зарезервированы для частных сетей.

Устройство IP-дейтаграммы

<table>
<tr><td>Версия IP
4 бита</td><td>Длина
заголовка</td><td>Тип обслуживания
8 бит</td><td colspan="2">Общая длина IP пакета
16 бит</td></tr>
<tr><td colspan="3">Идентификатор IP пакета
16 бит</td><td>Флаги</td><td>Смещение фрагмента</td></tr>
<tr><td colspan="2">Время жизни (TTL)
8 бит</td><td>Протокол высшего
уровня, 8 бит</td><td colspan="2">Контрольная сумма IP заголовка
16 бит</td></tr>
<tr><td colspan="5">IP адрес отправителя</td></tr>
<tr><td colspan="5">IP адрес получателя</td></tr>
<tr><td colspan="5">Опции заголовка
(если есть)</td></tr>
<tr><td colspan="5">Данные</td></tr>
</table>

Сегментация и фрагментация

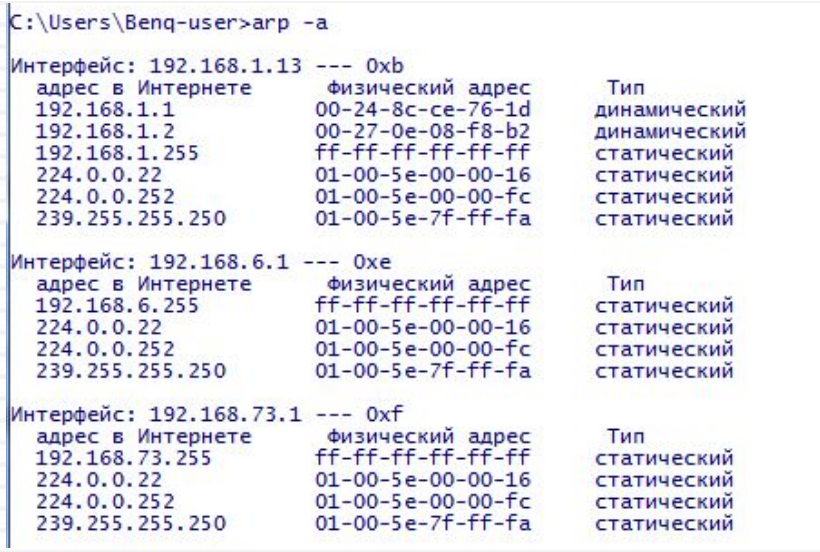


Автоматизация процесса назначения IP-адресов

- Назначение IP-адресов узлам сети даже при не очень большом размере сети может представлять для администратора утомительную процедуру. Протокол *Dynamic Host Configuration Protocol (DHCP)* освобождает администратора от этих проблем, автоматизируя процесс назначения IP-адресов.
- Протокол DHCP работает в соответствии с моделью клиент-сервер. Во время старта системы компьютер, являющийся DHCP-клиентом, посылает в сеть широковещательный запрос на получение IP-адреса. DHCP-сервер откликается и посылает сообщение-ответ, содержащее IP-адрес. Предполагается, что DHCP-клиент и DHCP-сервер находятся в одной IP-сети.

Отображение IP-адресов на локальные адреса

- Для определения локального адреса по IP-адресу используется *протокол разрешения адреса (Address Resolution Protocol, ARP)*.
- Протокол, решающий обратную задачу называется реверсивным ARP (Reverse Address Resolution Protocol, RARP) и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.
- Работа протокола ARP начинается с просмотра так называемой *ARP-таблицы*. Каждая строка таблицы устанавливает соответствие между IP-адресом и MAC-адресом. Для каждой сети, подключенной к сетевому адаптеру компьютера или к порту маршрутизатора, строится отдельная ARP-таблица.



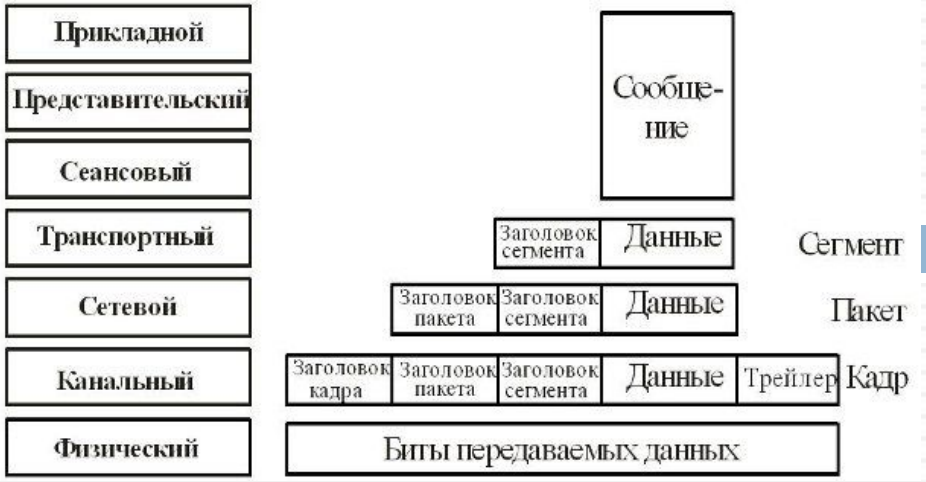
```
C:\Users\Benq-user>arp -a

Интерфейс: 192.168.1.13 --- 0xb
  адрес в Интернете      Физический адрес      Тип
  192.168.1.1           00-24-8c-ce-76-1d     динамический
  192.168.1.2           00-27-0e-08-f8-b2     динамический
  192.168.1.255         ff-ff-ff-ff-ff-ff     статический
  224.0.0.22            01-00-5e-00-00-16     статический
  224.0.0.252           01-00-5e-00-00-fc     статический
  239.255.255.250       01-00-5e-7f-ff-fa     статический

Интерфейс: 192.168.6.1 --- 0xe
  адрес в Интернете      Физический адрес      Тип
  192.168.6.255         ff-ff-ff-ff-ff-ff     статический
  224.0.0.22            01-00-5e-00-00-16     статический
  224.0.0.252           01-00-5e-00-00-fc     статический
  239.255.255.250       01-00-5e-7f-ff-fa     статический

Интерфейс: 192.168.73.1 --- 0xf
  адрес в Интернете      Физический адрес      Тип
  192.168.73.255        ff-ff-ff-ff-ff-ff     статический
  224.0.0.22            01-00-5e-00-00-16     статический
  224.0.0.252           01-00-5e-00-00-fc     статический
  239.255.255.250       01-00-5e-7f-ff-fa     статический
```

Вспомогательные протоколы и средства стека TCP/IP

- Протокол межсетевых управляющих сообщений (Internet Control Message Protocol, ICMP) является вспомогательным протоколом, используемым для диагностики и мониторинга сети.
- Предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом-источником пакета. С помощью специальных пакетов ICMP сообщает о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т. п.
- Утилиты, использующие ICMP-сообщения:
  - **Ping – использует эхо-запросы для проверки доступности узла назначения.**
  - Tracerote – осуществляет трассировку маршрута, посылая серию IP-пакетов в конечную точку изучаемого маршрута.
    - TTL перового пакета = 1

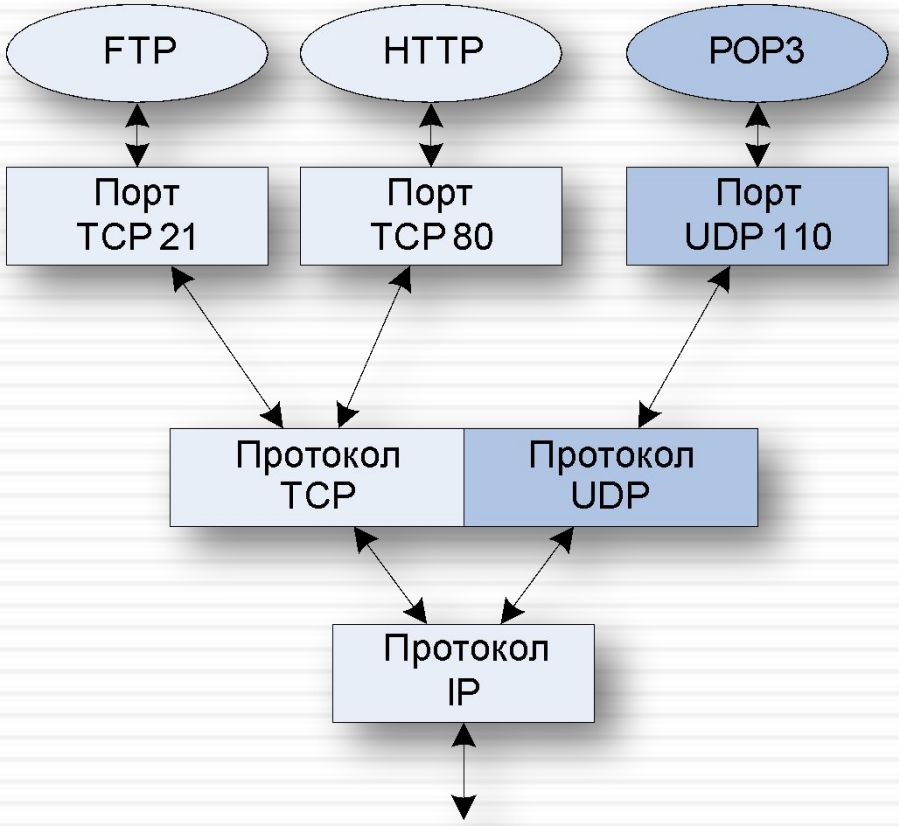
2. Транспортный уровень

Протоколы TCP и UDP



- Функция транспортного уровня - транспортировка сообщений и управление потоком информации от источника до устройства назначения с обеспечением надежности доставки.
- Контроль доставки обеспечены:
  - номерами последовательности передаваемых сегментов данных;
  - размером так называемого скользящего окна;
  - квитированием, т. е. подтверждением приема сообщения.
- Уровень устанавливает логическое соединение между двумя конечными точками сети.
- Протоколы транспортного уровня сегментируют данные, посланные приложениями верхнего уровня на передающей стороне, и повторно собирают из полученных сегментов целое сообщение на приемной стороне

Порты и сокеты



- Пакеты, поступающие на транспортный уровень, организуются операционной системой в виде множества очередей к точкам входа различных прикладных процессов. Такие системные очереди называются *портами*.
- Номер порта в совокупности с номером сети и номером конечного узла однозначно определяют прикладной процесс в сети. Этот набор идентифицирующих параметров имеет название *сокет* (*socket*).

Протокол UDP

Порт отправителя	Порт получателя
Длина UDP-дейтаграммы	Контрольная сумма UDP

- Протокол UDP – дейтаграммный протокол, реализующий ненадежный сервис *по возможности*, который не гарантирует доставку сообщений адресату.
- На хосте-отправителе: из поступающих данных формируются UDP-дейтаграммы, к ним добавляется 8-байтный заголовок, и они передаются на сетевой уровень – **мультиплексирование.**
- Если контрольная сумма показывает, что в поле данных ошибка, протокол UDP отбрасывает поврежденную дейтаграмму.

Протокол TCP

- Протокол основан на *логическом* соединении, что позволяет ему обеспечивать гарантированную доставку данных.

Формат заголовка TCP-сегмента

<table>
<tr><td colspan="8">Порт источника</td><td colspan="2">Порт приемника</td></tr>
<tr><td colspan="10">Последовательный номер – номер первого байта данных в сегменте, определяет смещение сегмента относительно потока отправляемых данных</td></tr>
<tr><td colspan="10">Подтвержденный номер – максимальный номер байта в полученном сегменте, увеличенный на единицу.</td></tr>
<tr><td>Длина заголовка</td><td>Резерв</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="2">Окно – количество байт, которое в настоящий момент готов принять модуль TCP на стороне получателя, начиная с байта, номер которого указан в поле подтвержденного номера</td></tr>
<tr><td colspan="8">Контрольная сумма</td><td colspan="2">Указатель срочности – указывает на конец данных, которые необходимо срочно принять, несмотря на переполнение буфера.</td></tr>
<tr><td colspan="8"></td><td colspan="2"></td></tr>
<tr><td colspan="8"></td><td colspan="2"></td></tr>
<tr><td colspan="8"></td><td colspan="2"></td></tr>
</table>

Поля TCP-сегмента

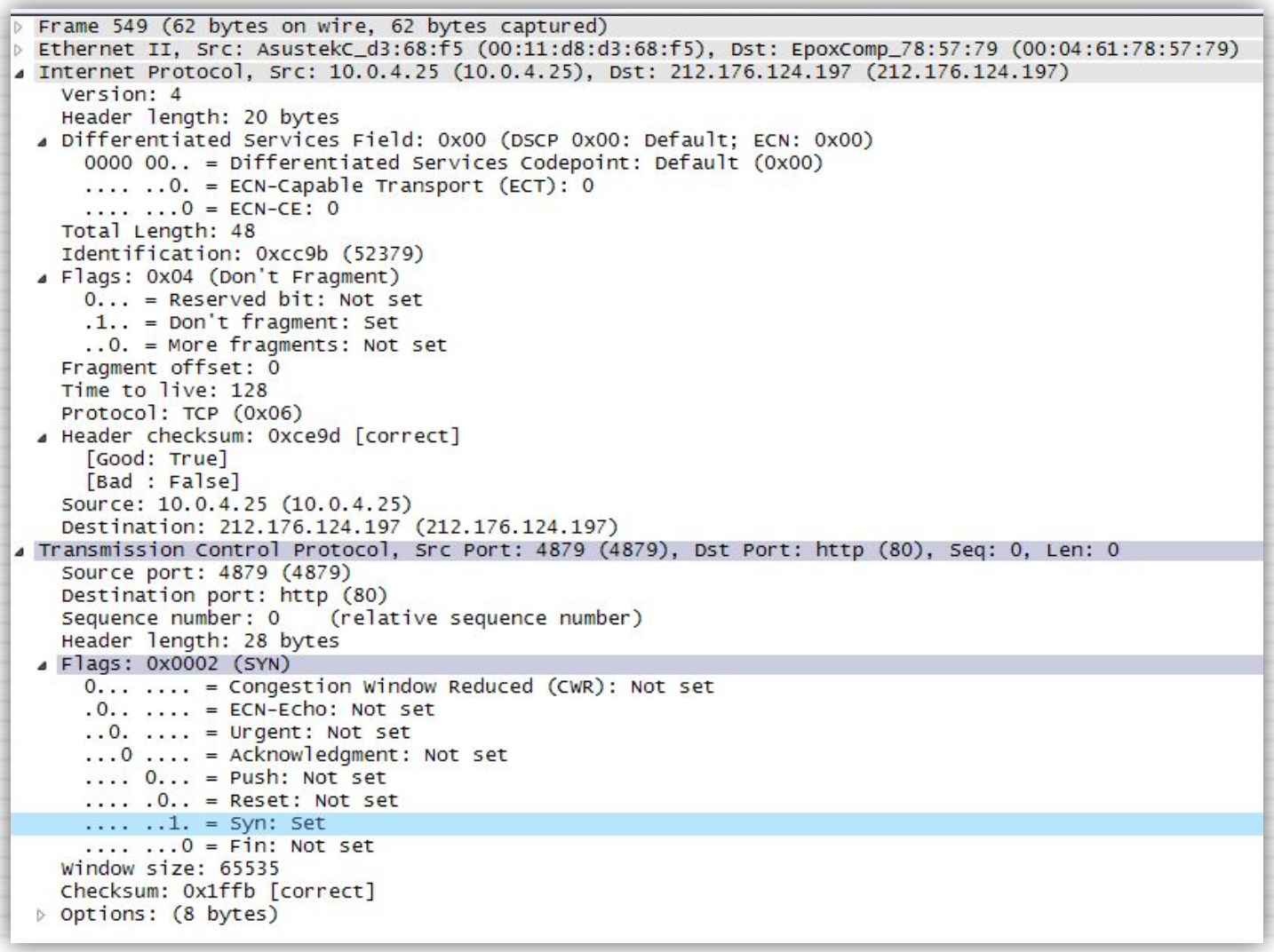
- Порядковый номер - номер байта TCP сегмента в потоке данных.
- Номер подтверждения - отображает номер следующего байта, который адресат готов принять.
- Размер окна - количество байтов которое можно принять.
- Указатель срочности – когда отправляются срочные данные, это поле содержит конечную границу срочных данных в сегменте. Используется вместе с указателем срочности URG
- Флаги:
  - URG – сегмент содержит срочные данные
  - ACK – TCP сегмент с действительным номером подтверждения (во всех сегментах, кроме первого)
  - PSH – сегмент содержит данные приложения, и оправка этих данных должна быть предусмотрена так быстро, насколько это возможно.
  - RST – сброс соединения
  - SYN – отправитель сбрасывает счетчик переданных байтов (новое соединение)
  - FIN – флаг закрытия соединения

Процедура соединения через TCP

При открытии соединений TCP используется процедура согласования, основанная на обмене тремя пакетами со следующими значениями флагов SYN и ACK:

1. Узел-инициатор посылает узлу-получателю служебный пакет с предложением установить соединение.
   - SYN=1 и ACK=0 — открытие соединения
2. Если узел-получатель согласен с этим, то он посылает в ответ другой служебный пакет, подтверждающий установление соединения
   - SYN=1 и ACK=1 — подтверждение открытия соединения
3. SYN=0 и ACK=1 — пакет данных или пакет ACK

Пример содержания пакета TCP/IP



Использованный инструментарий: сетевой монитор Ethereal.