**Вопрос 9**.

1. Формат IP-датаграммы. Назначение полей.
2. <https://studfile.net/preview/9080827/page:4/>

Формат ip-дейтаграммы. Структура пакета

Пакет IP содержит **14 полей**, из которых 13 являются обязательными. Четырнадцатое поле предназначено для необязательных опций. Поля используют порядок байтов от старшего к младшему, старшие биты идут первыми. Первый бит имеет номер 0. Таким образом, например, поле с версией находится в четырех старших битах первого байта.

**1. Версия**

Первым полем пакета является версия протокола размером в четыре бита. Для IPv4 это 4.

**2. Размер заголовка**

Следующие четыре бита содержат размер заголовка пакета в 32-х битных словах. Поскольку число опций не постоянно, указание размера важно для отделения заголовка от данных. Минимальное значения равно 5 (5×32=160 бит, 20 байт), максимальное — 15 (60 байт).

**3. Differentiated Services Code Point (DSCP)**

Изначально называлось «тип обслуживания» (Type of Service, ToS), в настоящее время определяется RFC2474 как «Differentiated Services». Используется для разделения трафика на классы обслуживания, например для установки чувствительному к задержкам трафику, такому как VoIP большего приоритета.

**4. Указатель перегрузки (Explicit Congestion Notification, ECN)**

Предупреждение о перегрузке сети без потери пакетов. Является необязательной функцией и используется только если оба хоста ее поддерживают.

**5. Размер пакета**

16-битный полный размер пакета в байтах, включая заголовок и данные. Минимальный размер равен 20 байтам (заголовок без данных), максимальный — 65535 байт. Хосты обязаны поддерживать передачу пакетов размером не менее 576 байт, но современные реализации обычно поддерживают гораздо больший размер. Пакеты большего размера, чем поддерживает канал связи, фрагментируются.

**6. Идентификатор**

Преимущественно используется для идентификации фрагментов пакета, если он был фрагментирован. Существуют эксперименты по его использованию для других целей, таких как добавление информации о трассировке пакета для упрощения отслеживания пути пакета с подделанным адресом источника.[8]

**7. Флаги**

Поле размером три бита содержащее флаги контроля над фрагментацией. Биты, от старшего к младшему, означают:

* 0: Зарезервирован, должен быть равен 0[9].
* 1: Не фрагментировать
* 2: У пакета еще есть фрагменты

Если установлен флаг «не фрагментировать», то в случае необходимости фрагментации такой пакет будет уничтожен. Может использоваться для передачи данных хостам, не имеющим достаточных ресурсов для обработки фрагментированных пакетов.

Флаг «есть фрагменты» должен быть установлен в 1 у всех фрагментов пакета, кроме последнего. У нефрагментированных устанавливается в 0 — такой пакет считается собственным последним фрагментом.

**8. Смещение фрагмента**

Поле размером в 13 бит, указывает смещение текущего фрагмента от начала передачи фрагментированного пакета в блоках по 8 байт. Позволяет (213-1)×8=65528 байт смещения, что превышает максимальный размер пакета. Первый фрагмент в последовательности имеет нулевое смещение.

**9. «Время жизни» (Time to Live, TTL) пакета.**

Позволяет предотвратить закольцовывание пакетов в сети путем уничтожения пакетов, превысивших время жизни. Указывается в секундах, интервалы менее секунды округляются до одной секунды. На практике каждый маршрутизатор уменьшает время жизни пакетов на единицу (что справедливо при существующих типичных задержках в сети). Пакеты, время жизни которых стало равно нулю уничтожаются, а отправившему посылается сообщение ICMP Time Exceeded. На отправке пакетов с разным временем жизни основана трассировка их пути прохождения (traceroute).

**10. Протокол**Указывает, данные какого протокола содержит пакет (например, TCP или ICMP). Присвоенные номера протоколов можно найти на сайте IANA[10].

**11. Контрольная сумма заголовка**

16-битная контрольная сумма, используемая для проверки целостности заголовка. Каждый хост или маршрутизатор сравнивает контрольную сумму заголовка со значением этого поля и отбрасывает пакет, если они не совпадают. Целостность данных IP не проверяет — она проверяется протоколами более высоких уровней (такими, как TCP или UDP), которые тоже используют контрольные суммы.

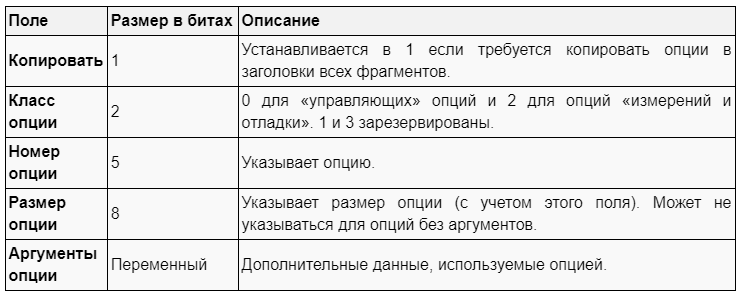
+Поскольку TTL уменьшается на каждом шаге прохождения пакета, сумма тоже должна вычисляться на каждом шаге. Метод пересчета контрольной суммы определен в RFC1071[11].

**12. Адрес источника**

32-х битный адрес отправителя пакета. Может не совпадать с настоящим адресом отправителя из-за трансляции адресов.

**13. Адрес назначения**

32-х битный адрес получателя пакета.



**14. Опции**

+За адресом назначения может следовать поле дополнительных опций, но оно используется редко. Размер заголовка в этом случае должен быть достаточным чтобы вместить все опции (с учетом дополнения до целого числа 32-х битных слов).

Если список опций не является концом заголовка, он должен оканчиваться опцией 0x00. Опции имеют следующий формат:

* Замечание: Размер заголовка более 5 указывается на присутствие опций и необходимость их обработки.
* Замечание: Поля «копировать», «класс опции» и «номер опции» иногда называют одним восьмибитным полем «тип опции»