**IPv4**

**Internet Protocol (IP)** — маршрутизируемый протокол сетевого уровня стека TCP/IP.

IP объединяет сегменты сети в единую сеть, обеспечивая доставку пакетов данных между любыми узлами сети через произвольное число промежуточных узлов (маршрутизаторов). Он классифицируется как протокол сетевого уровня по сетевой модели OSI. IP не гарантирует надёжной доставки пакета до адресата — в частности, пакеты могут прийти не в том порядке, в котором были отправлены, продублироваться (приходят две копии одного пакета), оказаться повреждёнными (обычно повреждённые пакеты уничтожаются) или не прийти вовсе. Гарантию безошибочной доставки пакетов дают некоторые протоколы более высокого уровня — транспортного уровня сетевой модели OSI, — например, TCP, которые используют IP в качестве транспорта.

**Фрагментация IP-пакетов**

При доставке IP-пакета он проходит через разные каналы доставки. Возможно возникновение ситуации, когда размер пакета превысит возможности узла системы связи. В этом случае протокол предусматривает возможность дробления пакета на уровне IP в процессе доставки. Соответственно, к конечному получателю пакет придет в виде нескольких пакетов, которые необходимо собрать в один перед дальнейшим анализом. Возможность дробления пакета с последующей сборкой называется IP-фрагментацией.

В протоколе предусмотрена возможность запрета фрагментации конкретного пакета. Если такой пакет нельзя передать через сегмент связи целиком, то он уничтожается, а отправителю направляется ICMP-сообщение о проблеме.

IPv4 использует 32-битные (четырёхбайтные) адреса, ограничивающие адресное пространство 4 294 967 296 (232) возможными уникальными адресами.

Традиционной формой записи IPv4 адреса является запись в виде четырёх десятичных чисел (от 0 до 255), разделённых точками. Через дробь указывается длина маски подсети.

**Классовая адресация**

Адресное пространство разделено на несколько логических групп и в каждой группе отводилось разное соотношение хостов и подсетей. Эти группы носят названия классов сетей и пронумерованы латинскими буквами: A, B, C, D и E. Деление основывается на старших битах адреса. Подробно адресация рассматривается в RFC 790.

Класс А: 0.XXX.XXX.XXX — 127.XXX.XXX.XXX

Класс B: 128.0.XXX.XXX — 191.255.XXX.XXX

Класс C: 192.0.0.XXX — 223.255.255.XXX

Класс D: 224.XXX.XXX.XXX — 239.XXX.XXX.XXX

Класс Е: 240.XXX.XXX.XXX — 255.XXX.XXX.XXX.

**Бесклассовая адресация**

С ростом сети Интернет эта система оказалась неэффективной и была дополнена бесклассовой адресацией (CIDR). Была введена дополнительная метрика — маска подсети, определяющая сколько бит адреса отводится на адрес сети, а сколько — на адрес узла.

**Структура заголовка пакета**

Заголовок пакета 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 четырёх старших битах первого байта. При передаче многооктетных значений старший октет передаётся первым.



**Версия**

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

**Размер заголовка (Internet Header Length)**

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

**Differentiated Services Code Point (DSCP)**

Изначально называлось «тип обслуживания» (Type of Service, ToS), в настоящее время определяется RFC 2474 как «Differentiated Services». Используется для разделения трафика на классы обслуживания, например, для установки чувствительному к задержкам трафику, такому как VoIP, большего приоритета.

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

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

**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 должны поддерживать передачу пакетов размером до 576 байт, но современные реализации обычно поддерживают гораздо больший размер. Пакеты большего размера, чем поддерживает канал связи, фрагментируются.

**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.

**Флаги**

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

* 0: Зарезервирован, должен быть равен 0.[13]
* 1: Не фрагментировать
* 2: У пакета ещё 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.

**Смещение фрагмента**

Поле размером в 13 бит, указывает смещение поля данных текущего фрагмента относительно начала поля данных первого фрагментированного пакета в блоках по 8 байт. Позволяет (213−1)×8=65528 байт смещения. При учёте размера заголовка итоговое смещение может превысить максимальный размер пакета (65528 + 20 = 65548 байт). Первый фрагмент в последовательности имеет нулевое смещение.

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

Определяет максимальное количество маршрутизаторов на пути следования пакета. Наличие этого параметра не позволяет пакету бесконечно ходить по сети. Каждый маршрутизатор при обработке пакета должен уменьшить значение TTL на единицу. Пакеты, время жизни которых стало равно нулю, уничтожаются, а отправителю посылается сообщение ICMP Time Exceeded. На отправке пакетов с разным временем жизни основана трассировка их пути прохождения (traceroute). Максимальное значение TTL=255. Обычное начальное значение TTL=64 (зависит от ОС).

**Протокол**

Указывает, данные какого протокола IP содержит пакет (например, TCP или ICMP). Присвоенные номера протоколов можно найти на сайте IANA.[14]

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 пересчёта контрольной суммы определён в RFC 1071.[15]

**Адрес источника**

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

**Адрес назначения**

32-битный адрес получателя пакета. Также может меняться при трансляции адресов.

**Опции**

За адресом назначения может следовать поле дополнительных опций, но оно используется редко.