Роль и назначение протокола IP в модели TCP/IP

Internet Protocol или IP— маршрутизируемый протокол сетевого уровня [модели стека протоколов TCP/IP](https://zametkinapolyah.ru/kompyuternye-seti/stek-protokolov-tcp-ip.html). Благодаря протоколу IP существует нынешняя сеть Интернет, поскольку именно этот протокол стал связующей нитью между разрозненными компьютерными сетями во всем мире. На данный момент нам нужно выделить два ключевых понятия в протоколе IP: минимально единицей измерения данных здесь является IP-пакет ([о единицах измерения в компьютерных сетях](https://zametkinapolyah.ru/kompyuternye-seti/korotko-o-edinicax-izmereniya.html)), который чаще всего [инкапсулируется](https://zametkinapolyah.ru/kompyuternye-seti/inkapsulyaciya-dannyx.html) в Ethernet кадр, а также каждый узел на сетевом уровне в модели TCP/IP должен иметь IP-адрес.

Мы уже не раз говорили, что протокол IP относится к сетевому уровню модели TCP/IP, это также справедливо и для [эталонной модели OSI 7](https://zametkinapolyah.ru/kompyuternye-seti/osi-7-i-ee-urovni.html). Также мы уже не раз применяли этот протокол на практике, а значит косвенно касались вопроса о значении протокола IP [в компьютерных сетях или сетях передачи данных](https://zametkinapolyah.ru/kompyuternye-seti/kurs-po-osnovam-kompyuternyx-setej.html). Если говорить коротко, то протокол IP нужен для логической адресации устройств в компьютерной сети или сети передачи данных.

Тут стоит сразу заметить, что IP-адреса делятся на две большие группы: публичные IP-адреса, которые должны быть уникальными во всем мире и частные IP-адреса, которые могут использоваться в любых частных/локальных сетях. Так, например, каждый в мире знает, что IP-адрес 8.8.8.8 принадлежит компании Google и это адрес их публичного DNS-сервера.

Вторая функция протокола IP заключается в том, чтобы предоставить услугу вышестоящему уровню, то есть транспортному уровню. Тут нужно заметить, что модель TCP/IP не предполагает [взаимодействие с установлением соединения](https://zametkinapolyah.ru/kompyuternye-seti/sluzhby-protokolov.html) на сетевом уровне, [вид взаимодействия](https://zametkinapolyah.ru/kompyuternye-seti/sovmestnye-resursy.html) определяется транспортным уровнем (при помощи выбора одного из двух протоколов: TCP или UDP), следовательно сам протокол IP работает без установления соединения и как бы это странно не прозвучала, но услугой протокола IP для транспортного уровня является передача данных между сетями или же транспортировка. То есть протоколы TCP и UDP рассматривают IP как рабочую лошадку, которая таскает пакеты из точки А в точку Б, минуя множество различных подсетей, если мы говорим о сети Интернет.

Как мы знаем, протокол IP связан с [канальным уровнем](https://zametkinapolyah.ru/servera-i-protokoly/kanalnyj-uroven-modeli-osi-vtoroj-uroven-etalonnoj-modeli-setevogo-vzaimodejstviya.html) при помощи протокола ARP. Сейчас мы этот факт просто для себя отмечаем и запоминаем, в дальнейшем пригодится. Также на сетевом уровне работают протоколы динамической маршрутизации, такие как OSPF, IS-IS, RIP, EIGRP, в английской литературе эти протоколы объединены общим словом Routing, то есть те, кто маршрутизирует, сам же IP именуется Routed, то есть тот, кого маршрутизируют. Internet Control Message Protocol или просто ICMP также относится к сетевому уровню.

Собственно, на этом можно завершить разговор о назначении протокола IP, у которого мы выделили две важные функции: **первая заключается в логическом именовании узлов сети передачи данных на сетевом уровня, вторая заключается в том, чтобы доставить пакет из точки А в точку Б через множество промежуточных сетей**. При этом IP-пакеты при передаче данных могут быть изменены (иногда это не стороннее вмешательство с целью взлома, а необходимость), потеряны, повреждены, пакеты могут прийти получателю не в той последовательности, в которой они были отправлены, обо всем этом протокол IP не заботится, его задача организовать маршрут между точкой А находящейся в одной сети и точкой Б, находящей в другой сети. Задачи, описанные выше, решают другие протоколы.

Протоколу IP не важно [какими характеристиками обладает компьютерная сеть](https://zametkinapolyah.ru/kompyuternye-seti/osnovnye-xarakteristiki-kompyuternoj-seti.html), какая [топология у сети передачи данных](https://zametkinapolyah.ru/kompyuternye-seti/topologii-kompyuternoj-seti.html), протоколу IP даже не важно поверх какого протокола канального уровня работать, протокол IP будет точно будет работать, если между устройствами будет один из следующих каналов: Ethernet, ATM, линки типа точка-точка, и это далеко не полный список. Протоколу IP не важен даже [размер компьютерной сети](https://zametkinapolyah.ru/kompyuternye-seti/tipy-kompyuternyx-setej.html), его можно использовать как в сетях BAN, так и в сетях WAN.

Типы адресов в модели TCP/IP

Теперь стоит поговорить не конкретно о видах IP-адресов, а о видах адресов в сети, построенной по архитектуре TCP/IP, тут для нас будут важны четыре вида адресов:

* локальные адреса, для нас это будут MAC-адреса;
* сетевые адреса, естественно, в нашем случае это IP-адреса;
* адреса транспортного уровня;
* символьные адреса или доменные имена.

Начнем двигаться снизу-вверх по иерархии модели TCP/IP.

4.1.2.3 Адреса транспортного уровня

На транспортном уровне тоже есть свои адреса, эти адреса называются сокетами, которые представляют собой пару IP-адрес + номер TCP/UDP порта. Так, например, чтобы попасть на сайт по [протоколу HTTP](https://zametkinapolyah.ru/servera-i-protokoly/chto-nuzhno-znat-pro-http-protokol-veb-razrabotchiku-pravila-http-protokola.html), наш компьютер будет посылать запрос удаленному [серверу](https://zametkinapolyah.ru/servera-i-protokoly/chto-takoe-server-servernyj-kompyuter-i-servernoe-prilozhenie.html) на 80-ый TCP порт, выглядеть это будет примерно так 192.168.1.1:80. Но это еще не все, дело в том, что серверу надо как-то ответить своему [клиенту](https://zametkinapolyah.ru/servera-i-protokoly/chto-takoe-klient-klientskij-kompyuter-i-klientskoe-prilozhenie.html), для этого он тоже будет использовать TCP. А это означает, что клиент должен заранее позаботиться о том, чтобы сервер знал – на какой TCP порт нужно отвечать, поэтому в TCP-сегменте (так называются сообщения в протоколе TCP) указывается два порта: порт источника, чаще всего это случайно сгенерированное число и порт назначения (чаще всего этот порт относится к хорошо известным и закреплен за каким-нибудь протоколом), в нашем случае порт является хорошо известным (80 порт закреплен за HTTP).

Для примера, у нас есть компьютер с IP-адресом 10.10.10.25 и где-то в нашей сети есть [веб-сервер](https://zametkinapolyah.ru/servera-i-protokoly/chto-takoe-http-server-apache-ustanovka-veb-servera-apache-2-4-na-windows-gde-skachat-apache-2-4-dlya-windows.html), доступ к которому осуществляется по HTTPs, пусть у этого сервера будет IP-адрес 192.168.1.67. Тогда наш клиент сформирует TCP сообщение, в котором будет два сокета, сокет источника 10.10.10.25:45678 (в данном случае число 45678 является случайно сгенерированным), этим сокетом воспользуется сервер, чтобы ответить клиенту; а также у нас будет сокет назначения: 192.168.1.67:443, в данном случае число 443 означает, что мы обращаемся к серверу по протоколу HTTPs, TCP порт 443 является хорошо известным. Разобраться со [схемой взаимодействия клиент-сервер](https://zametkinapolyah.ru/servera-i-protokoly/o-modeli-vzaimodejstviya-klient-server-prostymi-slovami-arxitektura-klient-server-s-primerami.html), вам поможет эта публикация.

Какие выводы можно сделать? Да все очень просто! Адресация на транспортном уровне нужна и важна для конечных устройств. Именно благодаря ей конечные узлы понимают: для какого приложения приходят данные. Здесь мы поговорили очень сжато и скомкано, поскольку у нас будет отдельная тема по транспортному уровню, где мы все расставим по своим местам.

Версии протокола IP: IPv4 и IPv6

Версий протокола IP на данный момент две: IPv4 и IPv6. Сделаем поверхностный разбор каждой из представленных версий протокола IP.

Начнем с IPv4, цифра четыре здесь не означает четыре октета в IP-адресе, просто так случайно вышло. Больше всего нас интересует IP-адрес, под него в IPv4 выделено четыре байта или октета, как известно, в байте 8 бит, то есть восемь двоичных значений (0 или 1), следовательно, максимально возможное десятичное число равно 255, минимально допустимое 0. Думаю, приводить примеры IP-адресов для IPv4 не нужно, вам они уже знакомы. Более детальное описание у нас будет в отдельной теме.

Обмен информацией в IPv4 происходит при помощи IP-пакетов, у данной версии протокола этот пакет делится на два больших поля: поле данных, в котором переносится полезная информация и заголовок, в котором заложен весь функционал протокола, заголовок пакета IPv4 содержит 14 полей, тринадцать из которых обязательные и одно опциональное. Вообще, протокол IPv4 дает нам в распоряжение 2 в 32 степени IP-адресов или же 4 294 967 296. Но этих адресов уже начинает не хватать, дело все в том, что этот протокол был разработан 1980-ом году, тогда это число выглядело ужасающе большим, сейчас во времена интернет-чайников и тостеров со встроенным Wi-Fi этого пространства начинает не хватать.

Осознание того, что 4.2 млрд адресов не хватит начало приходить в 90-ых годах, а в 1996 году появился протокол IPv6, который должен когда-нибудь заменить IPv4. Дело всё в том, что под IP-адрес в IPv6 выделено 128 бит или 16 байт, а это уже совсем другая история. Теперь давайте попытаемся немного по сравнивать IPv4 и IPv6. Во-первых, IPv6 делает такую технологию, как NAT в текущих условиях бесполезной (для кого-то это плюс, а для кого-то это минус, поскольку NAT не только позволяет «перебивать» много частных IP-адресов в один публичный, но является первой линией защиты вашей компьютерной сети).

Маршрутизация в чистом своем виде (а есть и нечистые маршрутизации, которые очень ускоряют процесс обработки пакетов роутером) в IPv6 стала быстрее, чем в IPv4 даже несмотря на то, что адрес IPv6 значительно больше, дело все в том, что количество полей в IPv6 стало меньше, хотя сам заголовок оказался несколько длиннее, также немного изменен алгоритм обработки IPv6 пакетов маршрутизатором. Сейчас не будем далее углубляться в IPv6, а лучше перейдем к следующим темам, в которых мы разберемся с IPv4.

Маска подсети и IP-адреса

Маска подсети помогает маршрутизатору понять, как и куда передавать пакет. Подсетью может являться любая сеть со своими протоколами. Маршрутизатор передает пакет напрямую, если получатель находится в той же подсети, что и отправитель. Если же подсети получателя и отправителя различаются, пакет передается на второй маршрутизатор, со второго на третий и далее по цепочке, пока не достигнет получателя.

Протокол IP (Internet Protocol) используется маршрутизатором, чтобы определить, к какой подсети принадлежит получатель. Свой уникальный IP-адрес есть у каждого сетевого устройства, при этом в глобальной сети не может существовать два устройства с одинаковым IP.

IPv4 предусматривает назначение каждому устройству 32-битного IP-адреса, что ограничивало максимально возможное число уникальных адресов 4 миллиардами (2^32). В более привычном для человека десятичном виде IPv4 выглядит как четыре блока (октета) чисел от 0 до 255, разделенных тремя точками. Первый октет IP-адреса означает класс сети, классов всего 5: A, B, C, D, E. При этом адреса сети D являются мультикастовыми, а сети E вообще не используются.

Рассмотрим, например, IPv4 адрес класса С 223.135.100.7. Первые три октета определяют класс и номер сети, а последний означает номер конечного устройства. Например, если необходимо отправить информацию с компьютера номер 7 с IPv4 адресом 223.135.100.7 на компьютер номер 10 в той же подсети, то адрес компьютера получателя будет следующий: 223.135.100.10.

IPv6 имеет вид восьми блоков по четыре шестнадцатеричных значения, а каждый блок разделяется двоеточием. IPv6 выглядит следующим образом:

2dab:ffff:0000:0000:01aa:00ff:dd72:2c4a.

Для написания адреса используются строчные буквы латинского алфавита: a, b, c, d, e, f.

Ведущие нули допускается не указывать — например, в адресе выше :00ff: можно записать как :ff:.

Группы нулей, идущие подряд, тоже допустимо сокращать и заменять на двойное двоеточие. На примере выше это выглядит так: 2dab:аааа::01aa:00ff:dd72:2c4a. Допускается делать не больше одного подобного сокращения в адресе IPv6 на наибольшей последовательности нулей. Если одинаково длинных последовательностей несколько — на самой левой из них.

IP предназначен для определения адресата и доставки ему информации. Он предоставляет услугу для вышестоящих уровней, но не гарантирует целостность доставляемой информации.

IP способен инкапсулировать другие протоколы, предоставлять место, куда они могут быть встроены. К таким протоколам, например, относятся ICMP (межсетевой протокол управляющих сообщений) и IGMP (межсетевой протокол группового управления). Информация о том, какой протокол инкапсулируется, отражается в заголовке IP-пакета. Так, ICMP будет обозначен числом 1, а IGMP будет обозначен числом 2.

ICMP в основном используется устройствами в сети для доставки сообщений об ошибках и операционной информации, сообщающей об успехе или ошибке при связи с другим устройством. Например, именно с использованием ICMP осуществляется передача отчетов о недоступности устройств в сети. Кроме того, ICMP используется при диагностике сети — к примеру, в эксплуатации утилит ping или traceroute.

ICMP не передает какие-либо данные, что отличает его от протоколов, работающих на транспортном уровне — таких как TCP и UDP. ICMP, аналогично IP, работает на межсетевом уровне и фактически является неотъемлемой частью при реализации модели TCP/IP. Стоит отметить, что для разных версий IP используются и разные версии протокола ICMP.

Point-to-Point протоколы

Point-to-Point (от точки к точке, двухточечный) протоколе, также известном как PPP. PPP уникален по своим функциям, он применяется для коммуникации между двумя маршрутизаторами без участия хоста или какой-либо сетевой структуры в промежутке. При необходимости PPP обеспечивает аутентификацию, шифрование, а также сжатие данных. Он широко используется при построении физических сетей, например, кабельных телефонных, сотовых телефонных, сетей по кабелю последовательной передачи и транк-линий (когда один маршрутизатор подключают к другому для увеличения размера сети).

У PPP есть два подвида — PPPoE (PPP по Ethernet) и PPPoA (PPP через асинхронный способ передачи данных — ATM), интернет-провайдеры часто их используют для DSL соединений.

PPP и его старший аналог SLIP (протокол последовательной межсетевой связи) формально относятся к межсетевому уровню TCP/IP, но в силу особого принципа работы, иногда выделяются в отдельную категорию. Преимущество PPP в том, что для установки соединения не требуется сетевая инфраструктура, а необходимость маршрутизаторов отпадает. Эти факторы обуславливают специфику использования PPP протоколов.