**TCP/IP**

Стек TCP/IP - сетевая модель передачи данных в сети, она определяет порядок взаимодействия устройств. Данные поступают на канальный уровень и обрабатываются поочередно каждым уровнем выше. Стек представлен в виде абстракции, которая объясняет принципы обработки и приема данных.

Стек протоколов сети TCP/IP имеет 4 уровня:

1. Канальный (Link).
2. Сетевой (Internet).
3. Транспортный (Transport).
4. Прикладной (Application).

**Прикладной уровень**

Прикладной уровень обеспечивает возможность взаимодействия между приложением и другими уровнями стека протоколов, анализирует и преобразовывает поступающую информацию в формат, подходящий для программного обеспечения. Является ближайшим к пользователю и взаимодействует с ним напрямую.

Самые распространенные протоколы:

* HTTP;
* FTP;
* SMTP;
* DNS.

HTTP (HyperText Transfer Protocol) предназначен для передачи данных. По нему отправляются, например, документы в формате HTML, которые служат основой веб-страницы. Упрощенно схема работы представляется как «клиент – сервер». Клиент отправляет запрос, сервер его принимает, должным образом обрабатывает и возвращает конечный результат.

[FTP (File Transfer Protocol)](https://yandex.ru/turbo/fb.ru/s/article/199479/kak-nastraivat-portyi-ftp-chto-takoe-ftp-portyi?parent-reqid=1605115682411751-417597375434735045600275-prestable-app-host-sas-web-yp-180&utm_source=turbo_turbo) служит стандартом передачи файлов в сети. Клиент посылает запрос на некий файл, сервер ищет этот файл в своей базе и при успешном обнаружении отправляет его как ответ.

[SMTP (Simple Mail Transfer Protocol)](https://yandex.ru/turbo/fb.ru/s/article/258458/smtp-server-dlya-rassyilki-kak-nastroit-smtp-server?parent-reqid=1605115682411751-417597375434735045600275-prestable-app-host-sas-web-yp-180&utm_source=turbo_turbo) используется для передачи электронной почты. SMTP-операция включает в себя три последовательных шага:

1. Определение адреса отправителя. Это необходимо для возвращения писем.
2. Определение получателя. Этот шаг может повторяться некоторое количество раз при указании нескольких адресатов.
3. Определение содержимого сообщения и отправка. В качестве служебной информации передаются данные о типе сообщения. Если сервер подтверждает готовность принять пакет, то совершается сама транзакция.

**Заголовок (Header)**

В заголовке содержатся служебные данные. Важно понимать, что они предназначаются только для конкретного уровня. Это значит, что как только пакет отправится к получателю, то будет обработан там по такой же модели, но в обратном порядке. Вложенный заголовок будет нести специальную информацию, которая может быть обработана только определенным образом.

Например, заголовок, вложенный на транспортном уровне, на другой стороне может быть обработан только транспортным уровнем. Другие просто его проигнорируют.

**Транспортный уровень**

На транспортном уровне полученная информация обрабатывается как единый блок, вне зависимости от содержимого. Полученные сообщения делятся на сегменты, к ним добавляется заголовок, и все это отправляется ниже.

Протоколы передачи данных:

* TCP;
* UDP.

[TCP (Transmission Control Protocol)](https://yandex.ru/turbo/fb.ru/s/article/251615/tcp-portyi-spisok-portov-tcp-i-udp?parent-reqid=1605115682411751-417597375434735045600275-prestable-app-host-sas-web-yp-180&utm_source=turbo_turbo) - самый распространенный протокол. Он отвечает за гарантированную передачу данных. При отправке пакетов контролируется их контрольная сумма, процесс транзакции. Это значит, что информация дойдет «в целости и сохранности» независимо от условий.

UDP (User Datagram Protocol) - второй по популярности протокол. Он также отвечает за передачу данных. Отличительное свойство кроется в его простоте. Пакеты просто отправляются, не создавая особенной связи.

**Сетевой уровень**

Сетевой уровень из полученной информации образует пакеты и добавляет заголовок. Наиболее важной частью данных являются IP и MAC-адреса отправителей и получателей.

IP-адрес (Internet Protocol address) – логический адрес устройства. Содержит информацию о местоположении устройства в сети. Пример записи: [192.168.33.4].

MAC-адрес (Media Access Control address) – физический адрес устройства. Используется для идентификации. Присваивается сетевому оборудованию на этапе изготовления. Представлен как шестибайтный номер. Например: [08-00-27-AB-0E-25].

Сетевой уровень отвечает за:

* Определение маршрутов доставки.
* Передачу пакетов между сетями.
* Присвоение уникальных адресов.

Маршрутизаторы - устройства сетевого уровня. Они прокладывают путь между компьютером и сервером на основе полученных данных.

Самый популярный протокол этого уровня – IP.

IP (Internet Protocol) - интернет-протокол, предназначенный для адресации в сети. Используется для построения маршрутов, по которым происходит обмен пакетами. Не обладает никакими средствами проверки и подтверждения целостности. Для обеспечения гарантий доставки используется TCP, который использует IP в качестве транспортного протокола. Понимание

**Виды IP-адресов**

В сетях используются два вида IP-адресов:

1. Публичные.
2. Приватные.

Публичные (Public) используются в Интернете. Главное правило – абсолютная уникальность. Пример их использования – маршрутизаторы, каждый из которых имеет свой IP-адрес для взаимодействия с сетью Интернет. Такой адрес называется публичным.

Приватные (Private) не используются в Интернете. В глобальной сети такие адреса не являются уникальными. Пример – локальная сеть. Каждому устройству присваивается уникальный в пределах данной сети IP-адрес.

Взаимодействие с сетью Интернет ведется через маршрутизатор, который, как уже было сказано выше, имеет свой публичный IP-адрес. Таким образом, все компьютеры, подключенные к маршрутизатору, представляются в сети Интернет от имени одного публичного IP-адреса.

**IPv4**

Самая распространенная версия интернет-протокола. Предшествует IPv6. Формат записи - четыре восьмибитных числа, разделенные точками. Через знак дроби указывается маска подсети. Длина адреса - 32 бита. В подавляющем большинстве случаев, когда речь идет об IP-адресе, имеется в виду именно IPv4.

Формат записи: [192.168.7.2/24].

**IPv6**

Эта версия предназначается для решения проблем предыдущей версией. Длина адреса - 128 бит.

Основная проблема, которую решает IPv6 – это исчерпание адресов IPv4. Предпосылки начали проявляться уже в начале 80-х годов. ».

Главное преимущество IPv6 – более быстрое интернет-соединение. Это происходит из-за того, что для этой версии протокола не требуется трансляции адресов. Выполняется простая маршрутизация. Это является менее затратным и, следовательно, доступ к интернет-ресурсам предоставляется быстрее, чем в IPv4.

Пример записи: [4003:0af3:06s8:11f3:8b4e:09d8:623b:d34f].

Существует три типа IPv6-адресов: Unicast. Anycast. Multicast.

Unicast – тип одноадресных IPv6. При отправке пакет достигает только интерфейса, расположенного на соответствующем адресе.

Anycast относится к групповым IPv6-адресам. Отправленный пакет попадет в ближайший сетевой интерфейс. Используется только маршрутизаторами.

Multicast являются многоадресными. Это значит, что отправленный пакет достигнет всех интерфейсов, находящихся группе мультивещания. В отличие от broadcast, который является «вещанием для всех», multicast вещает лишь определенной группе.

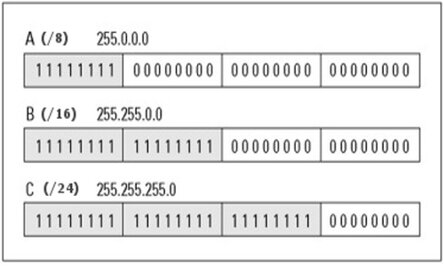
**Маска подсети**

Маска подсети выявляет из IP-адреса подсеть и номер хоста.

Например, IP-адрес [192.168.38.2] имеет маску [255.255.255.0]. В таком случае формат записи будет выглядеть так [192.168.38.2/24]. Число «24» – это количество бит в маске. Восемь бит равняется одному октету, который также может называться байтом.

Если подробнее, то маску подсети [255.255.255.0] можно представить в двоичной системе счисления таким образом: [11111111.11111111.11111111.00000000]. В ней имеется четыре октета, и запись состоит из «1» и «0». Если сложить количество единиц, то получим в сумме «24». К счастью, считать по единице не обязательно, ведь в одном октете – 8 значений. Видим, что три из них заполнены единицами, складываем [8+8+8+0] и получаем «24».

Если говорить именно о маске подсети, то в двоичном представлении она имеет в одном октете либо единицы, либо нули. При этом последовательность такова, что сначала идут байты с единицами, а только потом с нулями.



Рассмотрим небольшой пример. Есть IP-адрес [192.168.46.2] и маска подсети [255.255.255.0]. Считаем и записываем: [192.168.46.2/24]. Теперь сопоставляем маску с IP-адресом. Те октеты маски, в которых все значения равны единице (255) оставляют соответствующие им октеты в IP-адресе без изменения. Если же в значении нули (0), то октеты в IP-адресе также становятся нулями. Таким образом, в значении адреса подсети получаем [192.168.46.0].

**Подсеть и хост**

Подсеть отвечает за логическое разделение. По сути, это устройства, использующие одну локальную сеть. Определяется диапазоном IP-адресов.

Хост – это адрес сетевого интерфейса (сетевой карты). Определяется из IP-адреса с помощью маски. Например: [192.168.15.2/24]. Так как первые три октета - подсеть, то остается [0.0.0.2]. Это и есть номер хоста.

Диапазон адресов хоста – от 0 до 255. Хост под номером «0» является, собственно, адресом самой подсети. А хост под номером «255» является широковещательным.

**Адресация**

Для адресации в стеке протоколов TCP/IP используются три типа адресов:

1. Локальные.
2. Сетевые.
3. Доменные имена.

Локальными называются MAC-адреса. Они используются для адресации в таких технологиях локальной сети как, например, Ethernet. В контексте TCP/IP слово «локальные» означает, что они действуют лишь в пределах подсети.

Сетевым адресом в стеке протоколов TCP/IP является IP-адрес. При отправке файла из его заголовка считывается адрес получателя. С его помощью маршрутизатор узнает номер хоста и подсеть и, основываясь на этой информации, прокладывает маршрут к конечному узлу.

Доменные имена – это удобочитаемые адреса веб-сайтов в Интернете. Веб-сервера в сети Интернет доступны по публичному IP-адресу. Он успешно обрабатывается компьютерами, однако для людей представляется слишком неудобным. Для того чтобы избежать подобных сложностей, используются доменные имена, которые состоят из областей, называемых «доменами». Они располагаются в порядке строгой иерархии, от верхнего уровня к нижнему.

Домен первого уровня представляет конкретную информацию. Общие (.org, .net) не ограничены какими-либо строгими границами. Обратная ситуация - с локальными (.us, .ru). Они, как правило, привязаны территориально.

Домены низших уровней – это все остальное. Он может быть любого размера и содержать любое количество значений.

[DNS (Domain Name System)](https://yandex.ru/turbo/fb.ru/s/article/474280/kak-rabotaet-dns-struktura-i-sistematika-printsip-rabotyi-i-ustranenie-nepoladok?parent-reqid=1605115682411751-417597375434735045600275-prestable-app-host-sas-web-yp-180&utm_source=turbo_turbo) устанавливает соответствие между доменными именами и публичным IP-адресом. При наборе доменного имени в строке браузера DNS обнаружит соответствующий IP-адрес и сообщит устройству. Устройство обработает этот [машинный код](https://yandex.ru/turbo/fb.ru/s/article/351250/mashinnyiy-kod-kak-yazyik-programmirovaniya-yazyik-assemblera?parent-reqid=1605115682411751-417597375434735045600275-prestable-app-host-sas-web-yp-180&utm_source=turbo_turbo) и вернет его в виде веб-страницы.

**Канальный уровень**

На канальном уровне определяется взаимосвязь между устройством и физической средой передачи, добавляется заголовок. Отвечает за кодировку данных и подготовку фреймов для передачи по физической среде. На этом уровне работают сетевые коммутаторы.

Самые распространенные протоколы:

1. Ethernet.
2. WLAN.

Ethernet – наиболее распространенная технология проводных локальных сетей.

WLAN – локальная сеть на основе беспроводных технологий. Взаимодействие устройств происходит без физических кабельных соединений. Пример самого распространенного метода – Wi-Fi.

**Способы передачи данных**

Данные передаются через физическую среду тремя способами:

* Simplex.
* Half-duplex.
* Full Duplex.

Simplex – это односторонняя связь. Передача ведется только одним устройством, в то время как другое только принимает сигнал. Можно сказать, что информация транслируется только в одном направлении.

Half-duplex – это двусторонняя связь. Однако только один узел может передавать сигнал в определенный момент времени. При такой связи два устройства не могут одновременно использовать один канал. Полноценная [двусторонняя связь](https://yandex.ru/turbo/fb.ru/s/article/421877/dupleksnaya-svyaz-ponyatie-printsip-deystviya-naznachenie-i-primenenie?parent-reqid=1605115682411751-417597375434735045600275-prestable-app-host-sas-web-yp-180&utm_source=turbo_turbo) может быть невозможна физически или приводить к коллизиям. Говорится, что они конфликтуют за среду передачи. Этот режим применяется при использовании коаксиального кабеля.

Пример полудуплексной связи - общение по рации на одной частоте.

Full Duplex – полноценная двусторонняя связь. Устройства могут одновременно транслировать сигнал и производить прием. Они не конфликтуют за среду передачи. Этот режим применяется при использовании технологии Fast Ethernet и соединении с помощью витой пары.