# Канальный уровень

**Канальный уровень** (англ. Data Link layer) — протоколы, предназначенные для передачи данных узлам, находящимся в том же сегменте локальной сети.

Наиболее распространённым протоколом канального уровня в современном мире является Ethernet (для проводных соединений) и IEEE 802.11 (для беспроводных соединений, то есть для Wi-Fi).

Канальный уровень отвечает за доставку кадров (frame) между устройствами, подключёнными к одному сетевому сегменту. Кадры канального уровня не пересекают границ сетевого сегмента. Кадры передаются последовательно с обработкой кадров подтверждения, отсылаемых обратно получателем.

Функции межсетевой маршрутизации и глобальной адресации осуществляются на более высоких уровнях модели, что позволяет протоколам канального уровня сосредоточиться на локальной доставке и адресации.

Когда устройства пытаются использовать среду одновременно, возникают коллизии кадров. Протоколы канального уровня выявляют такие случаи и обеспечивают механизмы для уменьшения их количества или же их предотвращения.

Некоторые протоколы канального уровня не имеют подтверждения о приёме кадра, некоторые протоколы даже не имеют контрольной суммы для проверки целостности кадра. В таких случаях нам помогают другие, более высокие уровни модели TCP/IP и берут на себя функцию проверки целостности и факта доставки.

## Функции канального уровня

**Получение доступа к среде передачи**. Обеспечение доступа — важнейшая функция канального уровня. Она требуется всегда, за исключением случаев, когда реализована полносвязная топология (например, два компьютера, соединённых через кроссовер, или компьютер с коммутатором в полнодуплексном режиме).
**Выделение границ кадра**. Эта задача также решается всегда. Среди возможных решений этой задачи — резервирование некоторой последовательности, обозначающей начало или конец кадра.
**Аппаратная адресация (или адресация канального уровня).** Требуется в том случае, когда кадр могут получить сразу несколько адресатов. В локальных сетях аппаратные адреса (MAC-адреса) применяются всегда.
**Обеспечение достоверности принимаемых данных**. Во время передачи кадра есть вероятность, что данные исказятся. Важно это обнаружить и не пытаться обработать кадр, содержащий ошибку. Обычно на канальном уровне используются алгоритмы контрольных сумм, дающие высокую гарантию обнаружения ошибок.

**Адресация протокола верхнего уровня**. В процессе декапсуляции указание формата вложенного PDU существенно упрощает обработку информации, поэтому чаще всего указывается протокол, находящийся в поле данных, за исключением тех случаев, когда в поле данных может находиться один-единственный протокол.

## Ethernet

Минимальная единица, которой оперирует этот протокол, называется кадр (фрейм).

Тип протокола вышестоящего уровня (EtherType) — двухбайтовый код. Контрольная сумма (CRC/FCS — control redundant checksum / frame check sequence) нужна для защиты от ошибок передачи. Отправитель считает контрольную сумму на основе всех остальных октетов кадра и записывает в кадр, а получатель повторяет расчёт и сверяет с присланной. В случае несовпадения можно сделать вывод, что кадр был повреждён при передаче, и не обрабатывать его.

Преамбула (preamble) и межкадровый интервал (inter-frame gap) необходимы, чтобы различать начало и конец кадра в потоке битов, генерируемом физическим уровнем. Максимальным размером кадра считается 1518 октетов с учётом контрольной суммы.

Ограничение сверху на размер кадра влечёт ограничение на размер полезных данных в нём — MTU (maximum transmission unit), для Ethernet это 1500 октетов, но может быть настроено меньше.

Адрес отправителя и получателя — MAC-адреса из шести октетов каждый. MAC-адреса записываются чаще всего через двоеточия (12:34:56:78:90:ab), через дефисы (12-34-56-78-90-ab) или по два байта через точки (1234.5678.90ab).

В порт может поступить кадр с любым MAC-адресом назначения, и узел должен решить, считать ли, что кадр направлен ему. В свою очередь, кадр может быть направлен: одному конкретному узлу — адресная рассылка (unicast);
каждому узлу некой группы — многоадресная рассылка на L2 (MAC multicast);
всем узлам локальной сети — широковещательная рассылка (broadcast).

Большая часть трафика является адресной рассылкой. Непременное техническое требование к MAC-адресам сетевых портов для этого — уникальность в локальной сети.

Многоадресная (или групповая) рассылка используется в основном в корпоративных и промышленных сетях. Групповые MAC-адреса имеют нечётный первый октет.

Протокол разрешения адресов (address resolution protocol, ARP) и предназначен для нахождения MAC-адреса по IP-адресу. Клиент шлёт широковещательный пакет на MAC-адрес ff:ff:ff:ff:ff:ff со своего MAC-адреса. Смысл пакета — запрос, чтобы тот узел, которой обладает указанным IP, ответил клиенту. IP-адрес указывается как target protocol address, MAC-адрес и IP-адрес отправителя заносятся как sender addresses, а target hardware address обнуляется.

При получении ответа ARP клиент считывает MAC-адрес и IP-адрес из ответа и добавляет их в свою таблицу ARP. (Содержимое таблицы в Windows, Linux и macOS можно просмотреть программой arp.)

Может показаться, что ответ ARP избыточен: MAC-адрес сервера уже указан в кадре как MAC отправителя, а искомый IP-адрес дублируется из запроса. Но избыточности нет.
Клиент может одновременно сделать несколько ARP-запросов для разных IP. Если не указывать искомый IP в ответе, клиент не сможет определить, к какому IP относится MAC сервера.

В сложных случаях для передачи запросов ARP может использоваться один протокол канального уровня, а для связи с искомым узлом — другой. При этом адрес отправителя в кадре-ответе и адрес отправителя в ответе ARP (содержимом кадра) не будут или даже не могут совпадать. Строго говоря, ARP не ограничен MAC- и IP-адресами, но применяется в основном для них.

**Как мы можем узнать MAC-адрес на своей виртуальной машине?**
Для этого можно использовать команду ip, которая покажет нам информацию о сетевых интерфейсах (несмотря на то что у виртуальной машины сетевой интерфейс также виртуальный, он есть).

```
ip a
```

lo — это интерфейс локальной петли, а вот это сетевой интерфейс, который предоставляет нам доступ к интернету и доступ к компьютеру, на котором расположена виртуальная машина, по сети. Вот наш MAC-адрес и вот broadcast-адрес.
Для того чтобы просмотреть arp-кэш на машине, мы можем использовать команду arp, которую установим с пакетом net-tools:

```
sudo apt-get install net-tools
```

Теперь команда arp -a покажет нам всё содержимое arp-кэша на виртуальной машине.