**Введение**

Для удобства нашей коммуникации модели взаимодействия открытых систем (OSI) разделяют функции сети передачи данных на уровни. Для передачи данных каждый уровень используется с уровнями, расположенными в непосредственной близости к нему. Два уровня в рамках модели OSI связаны настолько тесно, что в соответствии с моделью TCP/IP представляют собой один уровень. Ими являются канальный и физический уровень.

На отправляющем устройстве роль канального уровня состоит в подготовке данных для передачи и контроле над доступом данных к физической среде. Однако именно физический уровень контролирует передачу данных в физическую среду, кодируя двоичные представления данных в сигналы.

На принимающей стороне физический уровень принимает сигналы из среды передачи данных. После декодирования сигнала в данные физический уровень передаёт их канальному уровню для обработки.

В начале этой главы представлена информация об общих функциях физического уровня, а также о стандартах и протоколах, которые обеспечивают передачу данных по локальной среде. Кроме того, в данной главе содержатся сведения о функциях канального уровня и протоколах, которые с ним связаны.

**Подключение к сети**

При подключении к домашнему локальному принтеру или веб-сайту в другой стране необходимо сначала установить физическое подключение к локальной сети, прежде чем произойдёт передача данных по сети. Физическое подключение может осуществляться проводным подключением с помощью кабеля или беспроводным подключением с помощью радиоволн.

Тип используемого физического подключения полностью зависит от конфигурации сети. Например, офисы многих компаний оборудованы настольными компьютерами или ноутбуками с физическим подключением к совместно используемому коммутатору посредством кабеля. Это проводная сеть, в которой данные передаются по физическому кабелю.

Помимо возможности проводного подключения некоторые компании также обеспечивают беспроводное подключение для ноутбуков, планшетных компьютеров и смартфонов. В беспроводных устройствах данные передаются с помощью радиоволн. Беспроводное подключение всё чаще используется по мере того, как частные пользователи и компании оценивают преимущества предоставления сервисов беспроводного подключения. Для обеспечения беспроводного подключения сеть должна иметь точку беспроводного доступа (WAP), к которой смогут подключаться устройства.

Часто устройства и точки беспроводного доступа — это два отдельных выделенных устройства внутри сети. При этом существуют устройства, которые предполагают использование как проводного, так и беспроводного подключения. Например, во многих домах пользователи используют домашние маршрутизаторы с интеграцией сервисов (ISR), как показано на рисунке 1. Маршрутизаторы с интеграцией сервисов предлагают компонент коммутации с несколькими портами, что позволяет различным устройствам подключаться к локальной сети (LAN) с помощью кабелей, как показано на рисунке 2. Кроме того, многие маршрутизаторы с интеграцией сервисов также содержат WAP, что также обеспечивает подключение беспроводных устройств.

**Сетевые интерфейсные платы**

Сетевые интерфейсные платы (NIC) служат для подключения устройства к сети. Сетевые интерфейсные платы Ethernet используются для проводного подключения, а сетевые интерфейсные платы беспроводной локальной сети — для беспроводного подключения. Устройство конечного пользователя может содержать один или оба типа интерфейсных плат. Например, сетевой принтер может быть оснащён только сетевой интерфейсной платой Ethernet, поэтому ему необходимо подключаться к сети с помощью кабеля Ethernet. Другие устройства, например, планшетные ПК и смартфоны, могут быть оснащены только сетевой интерфейсной платой беспроводной локальной сети, при этом необходимо использование беспроводного подключения.

Не все физические соединения одинаковы с точки зрения уровня производительности при подключении к сети.

Например, производительность беспроводного устройства может снижаться в зависимости от расстояния к точке беспроводного доступа. Чем дальше устройство находится от точки доступа, тем слабее сигнал, который она получает. Это может привести к уменьшенной пропускной способности или потере беспроводного подключения. На рисунке показано, что расширитель беспроводного диапазона можно использовать для повторной передачи беспроводного сигнала в другие части дома, которые расположены слишком далеко от точки беспроводного доступа. Напротив, качество проводного подключения не ухудшится, но при этом перемещение точки подключения ограничено и должно находиться в одном месте.

Все беспроводные устройства должны иметь общий доступ к радиоэфиру точки беспроводного доступа. Это означает, что при одновременном подключении большого количества беспроводных устройств производительность сети может снизиться. Проводному устройству не нужен общий доступ к сети. Каждое проводное устройство имеет отдельный канал связи по отдельным кабелям Ethernet. Это важно при работе с некоторыми приложениями, например с онлайн-играми, потоковым видео и видеоконференциями, которые требуют более высокой пропускной способности по сравнению с другими приложениями.

Физический уровень

Физический уровень OSI позволяет передавать по сетевой среде биты, из которых состоит кадр канального уровня. Этот уровень принимает весь кадр от канального уровня и кодирует его в серию сигналов, которые передаются по локальной среде. Закодированные биты, из которых состоит кадр, будут получены либо оконечным, либо промежуточным устройством.

При переходе от узла источника к узлу назначения данные подвергаются следующему процессу.

* Пользовательские данные разделяются на сегменты транспортным уровнем, распределяются по пакетам сетевым уровнем, далее инкапсулируются в кадры канальным уровнем.
* Физический уровень кодирует кадры и создает электрические, оптические или радиоволны, которые представляют биты в каждом кадре.
* Затем эти сигналы поочередно отправляются через среду передачи данных.
* Физический уровень узла назначения получает эти отдельные сигналы из среды, восстанавливает их к битовым представлениям и передаёт биты до канального уровня в виде целого кадра.

**Средства передачи данных физического уровня**

Существуют три основных вида сред передачи данных. Физический уровень создаёт представление и группы битов для каждого типа среды, к которым относятся следующие.

* **Медный кабель**: сигналы представляют собой шаблоны электрических импульсов.
* **Оптоволоконный кабель**: сигналы представляют собой световые шаблоны.
* **Беспроводная сеть**: сигналы представляют собой шаблоны микроволновой передачи.

На рисунке показаны примеры сигналов для медных, оптоволоконных и беспроводных сред передачи данных.

Для обеспечения функциональной совместимости на физическом уровне все аспекты этих функций регламентируются организациями по стандартизации.

**Основные принципы физического уровня**

Стандарты физического уровня направлены на три функциональные области:

**Физические компоненты**

Физические компоненты — это электронные аппаратные устройства, средства передачи данных, а также другие блоки соединения, которые передают и переносят сигналы для представления битов. Все аппаратные компоненты, такие как сетевые адаптеры (NIC), интерфейсы и блоки соединения, кабельные материалы и конструкции кабелей, указаны в стандартах, относящихся к физическому уровню. Различные порты и интерфейсы на маршрутизаторе Cisco 1941 также являются примерами физических компонентов с определёнными разъёмами и схемами подключения в зависимости от стандартов.

**Кодирование**

Кодирование или кодирование канала — это способ преобразования потока бит в предопределённый «код». Коды — это группы бит, использующихся для обеспечения заданного шаблона, который может распознать как получатель, так и отправитель. В сети кодирование определяется правилом изменения напряжения или тока, используемого для представления бит: нулей и единиц.

Кроме кодирования данных, кодирование на физическом уровне также может создавать коды в целях контроля, например, для определения начала и конца кадра.

Общие методы кодирования сети включают в себя:

* **Манчестерское кодирование**: нули представлены переходом от высокого к низкому напряжению; единицы представлены переходом от низкого к высокому напряжению. Этот тип кодирования используется в предыдущих версиях Ethernet, RFID-устройствах и в технологии Near Field Communication (NFC).
* **Без возврата к нулю (NRZ)**: распространённый способ кодирования данных, у которого есть два состояния, обозначенные «нулем» и «единицей» без нейтрального или исходного положения. Нуль может быть представлен в среде передачи данных одним уровнем напряжения; единицы должны быть представлены другим уровнем напряжения.

**Примечание**. Увеличение скорости передачи данных требует более сложного кодирования, например, 4B/5B. Однако в данном курсе эти способы не описаны.

**Передача сигнала**

Физический уровень должен создавать электрические, оптические и беспроводные сигналы, которые представляют в среде «1» и «0». Метод представления битов называется методом передачи сигнала. Стандарты физического уровня должны определять, какой тип сигнала соответствует «1», а какой тип соответствует «0». Это может быть просто переменой уровня напряжения электрического сигнала или длительности оптического импульса. Например, длинный импульс может представлять 1, а короткий может представлять 0.

Это подобно тому, как азбука Морзе используется для связи. Азбука Морзе — один из способов передачи сигналов, который использует звуковые или световые импульсы, клики разной продолжительности для отправки текста по телефонным проводам или передачи сигналов между судами в море.

Сигналы передаются одним из двух способов.

* **Асинхронный**: сигналы передаются без соответствующего тактового сигнала. Временные промежутки между символами или группами данных могут быть произвольными, то есть они не имеют стандартов. Поэтому для обозначения начала и конца кадра необходимы флаги.
* **Синхронный**: сигналы данных посылаются в соответствии с тактовым сигналом, который отмеряет равные промежутки времени, которые называются временем передачи бита.

Существует множество способов передачи сигналов. Распространённый метод отправки данных — с применением технологии модуляции. Модуляция — это процесс, при котором характеристика одной волны (сигнал) изменяет другую волну (модулируемый сигнал). При передаче данных по среде распространены следующие методы модуляции.

* **Частотная модуляция (ЧМ)**: способ передачи, при котором несущая частота зависит от сигнала.
* **Амплитудная модуляция (AM)**: способ передачи, при котором несущая амплитуда зависит от сигнала.
* **Импульсно-кодовая модуляция (ИКМ)**: способ передачи, при котором аналоговый сигнал, например голос, преобразуется в цифровой сигнал путём дискретизации амплитуды сигнала и выражением амплитуд в двоичной системе. Частота дискретизации должна быть как минимум вдвое выше максимальной частоты в спектре сигнала.

Свойства фактических сигналов, представляющих биты в среде передачи данных, будут зависеть от используемого способа передачи. Некоторые из способов могут использовать один атрибут отдельного сигнала для представления нуля, а для представления единицы использовать другой атрибут сигнала.

На рис. 2 показано, как способы частотной и амплитудной модуляции используются для передачи сигнала.

**Пропускная способность**

Разные физические среды передачи данных поддерживают разные скорости передачи бит. Как правило, передача данных обсуждается с точки зрения заявленной пропускной способности (bandwidth) и производительности (throughput).

Пропускная способность (bandwidth) — это способность среды передавать данные. Цифровая пропускная способность определяет объём данных, передаваемый из одного пункта в другой за определённое время. Обычно пропускная способность измеряется в килобитах в секунду (Кбит/с) или мегабитах в секунду (Мбит/с).

Фактическая пропускная способность сети определяется совокупностью следующих факторов.

* Свойства физической среды
* Технологии, выбранные для передачи и обнаружения сигналов в сети

В определении доступной пропускной способности важную роль играют свойства физической среды, современные технологии и законы физики.

В следующей таблице приведены наиболее используемые единицы измерения пропускной способности.

**Производительность (throughput)**

Производительность (throughput) — это измерение скорости передачи битов по среде за указанный промежуток времени.

Из-за множества факторов производительность (throughput) обычно не соответствует заявленной пропускной способности (bandwidth) в средах на физическом уровне. На производительность (throughput) влияет ряд факторов, в том числе:

* объём трафика
* тип трафика
* время ожидания, вызванное конфликтом нескольких сетевых устройств между источником и назначением

Время ожидания (Latency) — это общее время, которое включает задержки (delays) для перемещения данных от одной точки к другой.

При сетевом взаимодействии или в сети с несколькими сегментами производительность (throughput) не может быть выше, чем самое медленное соединение между источником и получателем. Даже если все или большинство сегментов имеют высокую заявленную пропускную способность (bandwidth), производительность всего канала (throughput) определяется сегментом пути с наинизшей производительностью, который создаёт узкое место для производительности всей сети.

Существует много способов онлайн-проверки скорости, которые могут отобразить пропускную способность интернет-соединения. Рисунок отображает пример результатов проверки скорости.

**Примечание**. Существует третий способ измерения передачи используемых данных, который называется полезной пропускной способностью (goodput). Полезная пропускная способность (goodput) — измерение данных, переданных за указанный промежуток времени. Полезная пропускная способность (goodput) — это производительность полосы минус потери трафика для создания сеансов, подтверждений и инкапсуляции.

**Типы физической среды**

Физический уровень создаёт представление потока бит в виде изменений уровней напряжения, модулированных сигналов на определённых радиочастотах или световых импульсов. Различные организации по стандартизации представили определения физических, электрических и механических свойств сред передачи данных для различных видов коммуникаций. Эти спецификации гарантируют, что кабели и разъёмы будут функционировать соответствующим образом при работе канального уровня.

Например, стандарты сред передачи данных на основе медного кабеля определены для:

* типа используемых медных кабелей;
* пропускной способности связи;
* типа используемых разъёмов;
* схем подключения и цветовых кодов подключений к среде;
* максимальной протяжённости кабеля.

На данном рисунке показаны различные типы интерфейсов и портов, доступных на маршрутизаторе 1941.

**Характеристики медных кабелей**

Сети используют медные кабели, потому что они не требуют больших затрат, удобны в установке и обладают низким сопротивлением электрическому току. Однако медные кабели ограничены расстоянием и помехами сигнала.

Данные передаются по медным кабелям в виде электрических импульсов. Детектор в сетевом интерфейсе целевого устройства должен получить сигнал, который может быть легко раскодирован для соответствия отправленному сигналу. Однако чем дольше сигнал передаётся по сети, тем быстрее он затухает (attenuation - ослабление сигнала). Именно поэтому вся среда передачи данных, основанная на медном кабеле, должна следовать строгим ограничениям на расстояния в соответствии со стандартами.

Значения расчёта времени и напряжения электрических импульсов также зависят от двух аспектов.

* **Электромагнитные помехи (ЭМП) или радиочастотные помехи (РЧП) —** сигналы ЭМП и РЧП могут искажать и повреждать сигналы данных, передаваемые по медному кабелю. Потенциальные источники ЭМП и РЧП включают в себя радиоволны и электромагнитные устройства, например, флуоресцентные лампы или электродвигатели, как показано на рисунке.
* **Перекрёстные помехи** — это помехи, вызванные электрическими или магнитными полями сигнала на одном кабеле по отношению к сигналу в смежном кабеле. В телефонных каналах помехи могут привести к тому, что в одном канале будет услышана часть постороннего разговора. В частности, когда электрический ток проходит через провод, он создаёт небольшое круглое магнитное поле вокруг провода, разговор на котором может быть услышан на другом проводе.

Воспроизведите анимацию в диаграмме, чтобы увидеть, как передача данных может быть нарушена помехами.

Для борьбы с нежелательными последствиями ЭМП и РЧП некоторые типы медных кабелей обёрнуты в металлическую защиту и требуют правильного заземляющего устройства.

Для борьбы с нежелательными последствиями перекрёстных помех некоторые типы медных кабелей имеют провода с противоположным течением тока перекрученные между собой (говорят, что они образуют витую пару), что эффективно оберегает соединение от помех.

Сопротивление медных кабелей к электрическому шуму может быть ограничено:

* выбором типа кабеля и категории, подходящих данной сетевой среде;
* проектированием инфраструктуры кабеля для предотвращения известных и потенциальных источников помех в структуре здания;
* использованием методов прокладки кабеля, которые подразумевают правильное обращение и обработку кабелей.

**Медные кабели**

В сетевых технологиях существуют три основных типа медных кабелей:

* **неэкранированная витая пара (UTP)**
* **экранированная витая пара (STP)**
* **коаксиальный кабель**

Эти кабели используются для соединения узлов в локальной сети и устройств сетевой инфраструктуры, таких как коммутаторы, маршрутизаторы и точки беспроводного доступа. Каждый тип соединения и соответствующие устройства имеют определённые требования кабелей, предусмотренные стандартами физического уровня.

Различные стандарты физического уровня определяют использование различных разъёмов. Эти стандарты определяют механические размеры разъёмов и допустимые электрические свойства каждого типа. Сетевая среда использует модульные разъёмы и штепсели для обеспечения простого подключения и отключения. Кроме того, один тип физического разъёма может быть использован для нескольких типов подключений. Например, в локальных сетях разъём RJ-45 широко распространён с одним типом среды, а в глобальных сетях — с другим типом.

**Кабель типа незащищённая витая пара (UTP)**

Кабель типа незащищённая витая пара (UTP) — наиболее распространённая сетевая среда. Кабели UTP с разъёмами RJ-45 используются для связи сетевых узлов с промежуточными сетевыми устройствами, такими как коммутаторы и маршрутизаторы.

В локальных сетях кабель UTP состоит из четырёх пар проводов с цветной маркировкой. Эти провода перекручены между собой и защищены от небольших физических повреждений гибкой пластиковой оболочкой. Перекручивание проводов защищает провода от помех со стороны других проводов.

Как видно на рисунке, цветные маркировки определяют отдельные пары и провода в парах, а также облегчают оконцовку кабелей.

**Кабель на основе экранированной витой пары (STP)**

Кабели на основе экранированной витой пары (STP) имеют повышенный уровень защиты в отличие от кабелей на основе незащищённой витой пары (UTP). При этом они обходятся значительно дороже и сложны в установке. Как и UTP, кабели STP используют разъём RJ-45.

Кабели типа защищённая витая пара (STP) сочетают методы защиты от ЭМП и РЧП с перекручиванием проводов. Более того, такие кабели должны быть оконцованы специальными защищёнными разъёмами STP. Если кабель неправильно заземлён, экран может выступать в качестве антенны и принимать нежелательные сигналы.

Доступны различные типы кабелей STP с различными характеристиками. При этом существуют два распространённых вида защищённых витых пар:

* STP защищает целую связку проводов фольгой, что устраняет практически все помехи.
* STP защищает весь пучок проводов, а также отдельные пары проводов фольгой, что устраняет все помехи.

В кабеле STP, показанном на рисунке, используются четыре пары проводов, каждая из которых обёрнута экраном из фольги, а затем металлической оплёткой или фольгой.

В течение многих лет защищённые витые пары служили кабельной структурой при прокладке локальной сети с маркерным доступом (TokenRing, IEEE 802.5). В результате падения спроса на такие сети использование защищённых витых пар также значительно снизилось. Однако новый стандарт 10 гигабайт для Ethernet предполагает использование защищённых витых пар, что обеспечивает возобновление интереса к ним.

**Коаксиальный кабель**

Коаксиальный кабель называется так потому, что два проводника в нём используют одну и ту же ось. Как показано на рисунке, коаксиальный кабель состоит из следующих элементов:

* медный проводник, используемый для передачи электрических сигналов;
* медный проводник, окружённый изоляцией из эластичного пластика;
* изолирующий материал, окружённый медной оплёткой или металлической фольгой, который выступает в качестве второго провода в канале, а также экрана для внутреннего проводника. Этот второй уровень, или экран, также снижает количество внешних электромагнитных помех.
* Весь кабель покрыт кабельной оболочкой для защиты от небольших физических повреждений.

**Примечание**. С коаксиальным кабелем используются различные типы разъёмов.

В прошлом коаксиальный кабель использовался в кабельном телевидении, которое передавало сигналы только в одном направлении. Кроме того, он широко использовался в системах Ethernet.

Несмотря на то, что кабель UTP, по сути, заменил коаксиальный кабель в современной проводке Ethernet, строение коаксиального кабеля было модернизировано для использования в радиоустановках и установках интернет-кабелей.

* **Радиоустановки**. Коаксиальные кабели подсоединяют антенны к беспроводным устройствам. Коаксиальный кабель передаёт радиочастотную энергию между антеннами и радиооборудованием.
* **Установки интернет-кабелей**. В настоящее время поставщики кабельных услуг преобразуют односторонние системы в двухсторонние, чтобы предоставлять заказчикам возможность подключения к Интернету. Для возможности предоставления таких услуг блоки коаксиальных кабелей и их элементы амплификации заменяются на оптоволоконные кабели. Однако для обеспечения окончательного соединения на участке и проведения проводов в помещениях заказчика по-прежнему используется коаксиальный кабель. Совместное использование оптоволокна и коаксиала называется гибридной волоконно-коаксиальной связью (HFC).

**Безопасность медных кабелей**

Все три типа медных средств передачи уязвимы к огню и электрическому току.

Угроза пожара может возникнуть из-за воспламеняемости кабельной изоляции и экранов. При строительстве учреждений или организаций, возможно, потребуется оговорить стандарты безопасности для установки кабелей и соответствующего оборудования.

Опасность поражения током может возникнуть из-за того, что медные кабели могут проводить электричество там, где это нежелательно. Это может подвергнуть персонал и оборудование различным видам поражения электрическим током. Например, сетевое устройство с дефектом может передавать ток в корпуса других сетевых устройств. Кроме того, при подключении устройств, имеющих источники питания с различными нулевыми потенциалами, сетевые кабели могут создавать нежелательные уровни напряжения. Такие ситуации возможны при использовании медных кабелей для подключения сетей в различных зданиях или на разных этажах зданий, в которых установлено электрическое оборудование. Наконец, медные кабели могут передавать напряжение, вызванное ударами молнии по сетевым устройствам.

В результате нежелательных уровней напряжения и тока могут быть повреждены сетевые устройства и подключённые компьютеры, или могут быть травмированы сотрудники. Поэтому, чтобы избежать потенциально опасных ситуаций, медные кабели должны быть правильно установлены, в соответствии со спецификациями и строительными нормами и правилами.

На рисунке изображено правильное использование кабелей во избежание пожара или поражения током.

**Особенности прокладки кабелей типа UTP**

UTP-кабель состоит из четырёх пар проводов с цветной маркировкой, которые перекручены между собой и упакованы в оболочку из эластичного пластика. Сетевой кабель UTP имеет четыре пары медных проводов калибра 22 или 24 (диаметра примерно 0,5 мм). Кабель UTP имеет внешний диаметр примерно 0,43 см (0,17 дюймов). Кабель UTP имеет внешний диаметр примерно 0,43 см (0,17 дюймов). Его компактные размеры могут облегчить процесс установки.

Кабель UTP не использует защиту от ЭМП и РЧП. Вместо этого проектировщиками кабелей было выявлено, что ограничить отрицательное влияние помех можно следующими способами:

* **Отмена (Canсellation)**: проектировщики объединяют пары проводов в одну схему. Когда в двух проводах пары ток течёт в противоположных направлениях магнитные поля вокруг проводников противоположны друг другу. Таким образом, два магнитных поля самоуничтожаются, а также обеспечивается защита от внешних наводок от других пар, ЭМП и РЧП.
* **Изменение количества витков в витой паре**: для повышения эффекта отмены разработчики изменяют количество витков в каждой витой паре. Кабели UTP должны точно соответствовать спецификациям, регламентирующим количество разрешённых витков или оплёток на 1 метр кабеля. Обратите внимание, что на рисунке оранжевые и бело-оранжевые пары перекручены меньше, чем синие и бело-синие пары. Каждая покрашенная пара переплетена разное количество раз.

Чтобы ограничить затухание сигнала и обеспечить самозащиту пар проводов в сетевой среде, кабель UTP полагается исключительно на эффект отмены.

**Стандарты прокладки кабелей типа UTP**

Кабели UTP соответствуют требованиям стандартов, установленных организацией TIA/EIA. В частности, TIA/EIA-568A описывает коммерческие стандарты прокладки кабеля в локальных сетях. К указанным элементам относятся:

* типы кабелей
* длина кабелей
* разъёмы
* оконцовка кабелей
* способы проверки кабелей

Электрические характеристики медных кабелей определяются институтом инженеров по электротехнике и электронике (IEEE). IEEE классифицирует кабели незащищённых витых пар (UTP) в соответствии с производительностью. Кабели разделены на категории в соответствии с их возможностями передачи на более высокой скорости. Например, кабель категории 5 (Cat5), как правило, используется при установке FastEthernet 100BASE-TX. К другим категориям относятся: расширенный кабель категории 5 (Cat 5e), категории 6 (Cat6) и категории 6а.

Кабели более высших категорий разработаны и сконструированы для передачи данных на более высокой скорости. По мере развития и внедрения новых технологий Ethernet для гигабитных скоростей передачи данных минимально допустимым типом кабелей является Сat5e, а Cat6 рекомендуется для прокладки новых сетей.

На схеме выделены различные категории кабелей UTP.

**Примечание**. Некоторые производители завышают характеристики кабелей категории 6a TIA/EIA, указывая их как кабели категории 7.

**Разновидности кабелей типа UTP**

В различных ситуациях кабели типа UTP должны быть подключены в соответствии с различными правилами. Это означает, что отдельные провода кабеля должны быть подключены в разном порядке к различным наборам контактов в разъёмах RJ-45.

Основные типы кабелей, которые используются согласно определённым правилам, перечислены ниже.

* **Прямой кабель Ethernet**: наиболее распространённый тип сетевого кабеля; как правило, используется для подключения узла к коммутатору и коммутатора к маршрутизатору.
* **Перекрёстный кабель Ethernet**: не распространённый тип кабеля; используется для соединения аналогичных устройств друг к другу, например, для подключения коммутатора к коммутатору, узла к узлу или маршрутизатора к маршрутизатору.
* **Инверсный кабель**: кабель, запатентованный компанией Cisco; используется для подключения к маршрутизатору или порту консоли коммутатора.

Неправильное использование перекрёстного или прямого кабеля между устройствами не повредит устройствам, но при этом между ними не произойдёт соединения или связи. Такая ошибка часто встречается на практике. При отсутствии подключения сначала нужно проверить правильность подключения устройств.

На рисунке показаны кабель типа UTP, связанные с ним стандарты и типичные способы применения этих кабелей. Также на рисунке изображены отдельные пары проводов для стандартов TIA 568A и TIA 568B.

**Тестирование кабелей UTP**

После установки кабеля UTP необходимо использовать устройство для проверки следующих параметров:

* схема проводки
* длина кабеля
* потеря сигнала вследствие ослабления
* перекрёстные помехи

Рекомендуется тщательно проверить, что все требования к установке UTP выполнены.

**Особенности прокладки оптоволоконных кабелей**

Оптоволоконные кабели приобрели большую популярность благодаря их способности объединять сетевые устройства инфраструктуры. Их применение позволяет передавать данные на большие расстояния при более высокой пропускной способности (скорости передачи данных), чем при использовании других сетевых средств передачи данных.

Оптическое волокно — это гибкий, но очень тонкий и прозрачный кабель из чистого стекла (кварца) толщиной в человеческий волос. В оптоволоконном кабеле биты кодируются в виде световых импульсов. Оптоволоконный кабель действует как световод, передавая свет двумя концами кабеля с минимальной потерей сигнала.

Для аналогии представьте себе пустой рулон от бумажного полотенца, внутренние стенки которого покрыты зеркальной поверхностью длиной в тысячу метров, а также небольшую лазерную указку, используемую для передачи сигналов Морзе со скоростью света. По сути, именно так функционирует оптоволоконный кабель, только он имеет гораздо меньший диаметр и использует сложные светоизлучающие и принимающие технологии.

В отличие от медных проводов, оптоволоконный кабель может передавать сигналы при более низком показателе ослабления, а также он абсолютно устойчив к воздействию электромагнитных и радиочастотных помех.

В настоящее время оптоволоконные кабели используются в четырёх типах производства.

* **Корпоративные сети**. Оптоволоконный кабель используется для прокладки магистральной кабельной системы и связи сетевых устройств, реализующих инфраструктуру.
* **Технология «оптоволокно до квартиры» и сети доступа**. Технология «оптоволокно до квартиры» (Fiber to the Home, FTTH) используется для обеспечения постоянного подключения сетей широкополосного доступа для индивидуальных пользователей и небольших предприятий. Технология FTTH поддерживает использование высокоскоростного доступа в Интернет, а также дистанционной передачи данных, телемедицины и видео по запросу.
* **Сети дальней связи**. Поставщики используют наземные оптоволоконные сети дальней связи для обеспечения международного и междугороднего соединения. Обычно эти сети действуют в диапазоне от нескольких десятков до нескольких тысяч километров и поддерживают скорость до 10 Гбит/с.
* **Подводные сети**. Используются специальные оптоволоконные кабели для обеспечения надёжных высокоскоростных каналов с высокой пропускной способностью, которые способны работать в тяжёлых глубоководных условиях и пролегают через океаны.

Мы сосредоточены на использовании оптоволоконного кабеля в рамках предприятия.

**Конструкция оптоволоконного кабеля**

Хотя оптоволокно очень тонкое, оно состоит из двух типов стекла и защищено наружным экраном. В частности, к компонентам оптоволокна относятся:

* **Сердечник** — состоит из прозрачного стекла и является частью волокна, по которому проходит свет.
* **Оболочка оптического волокна** — стекло, которое окружает сердцевину и выступает в качестве зеркала. Световые импульсы, которые проходят по сердцевине, отражаются оболочкой. Благодаря этому они удерживаются в сердцевине волокна, представляя собой феномен полного внутреннего отражения.
* **Внешняя оболочка** — как правило, выполнена из поливинилхлорида (PVC), который защищает сердцевину и оболочку кабеля. В состав оптоволокна также могут входить укрепляющие материалы и буфер (обшивка), которые защищают стекло от царапин и влаги.

Хотя сердцевина и оболочка восприимчивы к изгибам под острым углом, они стали менее им подвержены в результате изменения свойств на молекулярном уровне. Оптическое волокно прошло тщательную производственную проверку. Было доказано, что оптоволокно выдерживает минимум 20 тысяч кг на квадратный сантиметр. Оптическое волокно достаточно прочно, поэтому не повреждается во время установки и использования в тяжёлых природных условиях.

**Типы оптоволоконных кабелей**

Световые импульсы, которые представляют передаваемые данные в виде битов в среде, генерируются посредством:

* лазеров;
* светоизлучающих диодов;

полупроводниковых устройств, называемых фотодиодами, которые определяют световые импульсы и преобразуют их в электрические сигналы, которые затем могут быть преобразованы в кадры данных.

**Примечание**. Лазерный луч, передаваемый по оптоволоконному кабелю, может нанести вред глазам. Поэтому следует предпринимать меры предосторожности при работе с активным оптоволоконным кабелем.

Оптоволоконные кабели можно классифицировать по двум типам.

* **Одномодовый оптоволоконный кабель (ООК)**: состоит из сердечника небольшого диаметра и для передачи луча света использует дорогостоящую лазерную технологию. Такой кабель повсеместно используется для проведения соединения на несколько сотен километров, например для дальней телефонии и приложений кабельного телевидения.
* **Многомодовый оптоволоконный кабель (МОК)**: состоит из сердцевины большего диаметра и для передачи световых импульсов использует светодиоды. Импульс из светоизлучающего индикатора входит в многомодовое волокно под разными углами. МОК часто используется в локальных сетях, поскольку может функционировать с помощью недорогих светодиодов. Такой тип кабеля обеспечивает пропускную способность до 10 Гбит/с на расстоянии до 550 метров.

На рис. 1 и 2 выделены характеристики МОК и ООК. Одно из основных отличий между МОК и ООК — значение дисперсии. Дисперсия — это рассеивание светового импульса в течение определённого промежутка времени. Чем больше дисперсия, тем больше потеря сигнала.

**Сетевые оптоволоконные разъёмы**

Оптоволоконный разъём размещается на конце оптического волокна. Существуют различные разъёмы для оптоволоконных кабелей. Основные отличия между этими типами разъёмов состоят в размерах и методах механических соединений. Как правило, организации отдают предпочтение одному типу разъёма, в зависимости от используемого оборудования, или присваивают каждому типу волокна отдельный тип разъёма (один для кабелей МОК, другой — для кабелей ООК). В настоящее время используются около 70 типов всевозможных разъёмов.

Как показано на рисунке 1, к трём наиболее распространённым типам разъёмов для оптоволоконных сетей относятся следующие.

* **Прямоконечный разъём (ST)**: устаревший тип разъёма, широко используемый с многомодовым волокном.
* **Разъём абонента (SC)**: также называется квадратным или стандартным. Этот тип разъёма, широко используемый в локальных и глобальных сетях, оснащён самозапирающимся механизмом для обеспечения надёжного монтажа. Также он используется с многомодовым и одномодовым оптоволоконным кабелем.
* **Светящийся разъём (LC)**: также называется малым или локальным разъёмом. Его популярность стремительно растёт благодаря небольшому размеру. Он используется с одномодовым оптоволоконным кабелем и поддерживает многомодовый кабель.

**Примечание**. Другие разъёмы для волоконных кабелей, например обжимной соединитель (FC) или подминиатюрный А (SMA), редко используются в локальных и глобальных сетях. Биконический разъём и разъём D4 являются устаревшими типами разъёмов. Эти разъёмы не рассматриваются в данной главе.

Поскольку по оптоволокну свет передаётся только в одном направлении, для работы в полнодуплексном режиме требуются два оптоволоконных кабеля. Таким образом, оптоволоконные соединительные кабели могут связывать два оптоволоконных кабеля с парой стандартных разъёмов. Некоторые оптоволоконные разъёмы можно подсоединить как к передающему, так и принимающему волоконному кабелю с помощью одного соединителя, который называется дуплексным соединителем. Он показан на рис. 1.

Для соединения устройств инфраструктуры требуются соединительные оптоволоконные кабели. Некоторые из распространённых соединительных кабелей показаны на рис. 2.

* Соединительный многомодовый кабель SC-SC
* Соединительный одномодовый кабель LC-LC
* Соединительный многомодовый кабель ST-LC
* Соединительный одномодовый кабель SC-ST

Неиспользуемые оптоволоконные кабели должны быть защищены небольшой пластиковой крышкой.

Кроме того, обратите внимание на цветовые маркировки для различения одномодовых и многомодовых соединительных кабелей. Согласно стандарту TIA-598 жёлтая оболочка используется для одномодовых волоконных кабелей, а для многомодовых кабелей используется оранжевая (или цвета морской волны).

**Проверка оптоволоконных кабелей**

Оконцовка и соединение оптоволоконных кабелей требует специальной подготовки и оборудования. Неправильная оконцовка оптоволоконного кабеля приведёт к уменьшению расстояния распространения сигнала или полному нарушению передачи.

К трём наиболее распространённым ошибкам при оптоволоконной оконцовке и соединении относятся следующие.

* **Смещение**: оптоволоконные кабели не прилегают друг к другу при соединении.
* **Рассоединение**: кабели не полностью соприкасаются при сращивании или соединении.
* **Полировка**: концы кабелей недостаточно очищены от грязи.

Для быстрой и простой проверки кабеля нужно использовать яркий электрический фонарь, направив его в один конец волокна и одновременно наблюдая за вторым концом. Если свет виден, то волокно может передавать свет. Хотя такая проверка не измеряет производительность волокна, она представляет собой быстрый и недорогой способ обнаружить поврежденное волокно.

Для проверки оптоволоконных кабелей рекомендуется использовать оптический тестер, как показано на рисунке. Оптический рефлектометр временной области (OTDR) можно использовать для проверки каждого сегмента оптоволоконного кабеля. Это устройство вводит тестовый импульс света в кабель, измеряя обратное рассеивание и отражение света в зависимости от промежутка времени. Оптический рефлектометр рассчитывает приблизительное расстояние, на котором обнаружены проблемы, по всей длине кабеля.

**Оптоволоконные кабели и медные кабели**

Использование оптоволоконных кабелей даёт множество преимуществ по сравнению с медными кабелями.

Поскольку волокна, используемые в оптоволоконной среде передачи данных, не являются проводниками тока, данная среда не подвержена электромагнитным помехам и не проводит нежелательный электрический ток благодаря заземлению. Так как оптические волокна тонкие и отличаются сравнительно малой потерей сигнала, их можно использовать на гораздо больших расстояниях по сравнению с медной средой передачи данных, без необходимости восстановления сигнала. Некоторые спецификации оптоволокна на физическом уровне обеспечивают передачу данных на несколько километров.

При внедрении оптоволоконных кабелей следует учесть следующие моменты.

* Больше затрат при прокладке на одинаковых расстояниях в отличие от медных кабелей (при этом они обеспечивают большую пропускную способность).
* Требуются специальные навыки и оборудование для оконцовки и сращения инфраструктуры кабеля.
* Требуют более осторожного обращения, нежели медные кабели.

В настоящее время в большинстве корпоративных сред для создания кабельной магистрали и обеспечения высокоскоростных соединений «точка-точка» между устройствами, а также для связи в комплексе зданий предпочтительно использовать оптоволоконные кабели. Поскольку оптоволоконный кабель не проводит электричество и отличается малой потерей сигнала, он оптимально подходит для этих целей.

На данном рисунке выделены некоторые отличия.

**Особенности беспроводной среды**

С помощью сверхвысоких частот беспроводные среды передачи данных переносят электромагнитные сигналы, которые представляют биты передаваемой информации.

В отличие от медных и оптоволоконных кабелей, беспроводная сеть в качестве сетевой среды не ограничивается проводниками или путями. Беспроводная среда передачи данных характеризуется наибольшей мобильностью. Кроме того, количество устройств беспроводной связи постоянно растёт. Именно поэтому беспроводная сеть стала предпочтительной средой для домашних сетей. Также популярность беспроводных сетей быстро увеличивается благодаря растущей пропускной способности сети.

На рисунке выделены различные символы, связанные с беспроводным соединением.

Однако беспроводная сеть имеет некоторые проблемные области, к которым относятся следующие.

* **Зона покрытия**. Беспроводные технологии передачи данных хорошо работают в открытых пространствах. Однако некоторые конструкционные материалы, используемые в зданиях и строениях, а также условия местности могут ограничить зону покрытия.
* **Помехи**. Беспроводная сеть восприимчива к перекрёстным помехам, и её функционирование может быть нарушено обычными устройствами, например, беспроводными телефонами, телевизионными приёмниками, некоторыми типами флуоресцентных ламп, микроволновыми печами и другими беспроводными коммуникациями.
* **Безопасность**. Покрытие беспроводной связи не ограничивается условиями доступа к среде. Поэтому доступ к передаче могут получить неавторизованные пользователи и устройства. Следовательно, средства обеспечения сетевой безопасности являются основной составляющей администрирования беспроводной сети.

Хотя популярность беспроводных сетей для подключения настольных компьютеров растёт, медные и оптоволоконные кабели являются наиболее популярной сетевой средой передачи данных на физическом уровне.

**Типы беспроводных средств передачи данных**

Телекоммуникационные и отраслевые стандарты IEEE для беспроводной передачи данных покрывают как канальный, так и физический уровни.

К беспроводным сетям применимы следующие три стандарта передачи данных.

* **Стандарт IEEE 802.11**: технология беспроводных локальных сетей (WLAN), которая чаще всего называется Wi-Fi, использует конкурирующую или недетерминированную систему с множественным доступом с контролем несущей (CSMA/CA).
* **Стандарт IEEE 802.15**: стандарт беспроводной персональной сети, более известный, как Bluetooth; для передачи данных на расстояниях от 1 до 100 метров требует близкого расположения двух устройств.
* **Стандарт IEEE 802.16**: более известен как протокол широкополосной радиосвязи (WiMAX); использует топологию «точка-точка» для обеспечения беспроводного широкополосного доступа.

На данном рисунке выделены некоторые отличия между беспроводными средствами передачи данных.

**Примечание**. Другие беспроводные технологии, например сети сотовой связи или спутниковая связь, также обеспечивают соединение сети передачи данных. Однако эти беспроводные технологии не рассматриваются в данной главе.

В каждом из указанных выше примеров технические характеристики физического уровня применимы к следующим областям:

* кодирование данных в радиосигнал
* частота и мощность передачи
* требования к приёму и декодированию сигнала
* проектирование и структура антенны

**Примечание**. Wi-Fi — это торговая марка Wi-Fi Alliance. Wi-Fi используется с сертифицированными товарами, которые относятся к устройствам беспроводной локальной сети (WLAN) и основаны на стандартах IEEE 802.11.

**Беспроводная локальная сеть (LAN)**

Беспроводное соединение устройств к локальной сети обеспечивает беспроводную передачу данных. Обычно для установления беспроводной локальной сети требуются следующие сетевые устройства.

* **Точка беспроводного доступа (АР)**: концентрирует беспроводные сигналы от пользователей и с помощью медного кабеля подключается к имеющейся сетевой инфраструктуре, например, к Ethernet. Беспроводные маршрутизаторы для дома и малых предприятий сочетают функции маршрутизатора, коммутатора и точки доступа в одном устройстве, как показано на рисунке.
* **Беспроводные сетевые адаптеры**: обеспечивают беспроводную связь для каждого сетевого узла.

По мере развития технологии количество стандартов беспроводной локальной сети (WLAN) на основе Ethernet возросло. Приобретая беспроводные устройства, их следует тщательно выбирать, чтобы обеспечить нужную совместимость и функциональность.

Преимущества беспроводных технологий передачи данных очевидны, особенно в отношении экономии на дорогостоящих проводах для помещений и удобства мобильности узла. Однако администраторам сети необходимо разрабатывать и применять строгие правила безопасности и процессы для защиты беспроводных локальных сетей от неавторизованного доступа и потенциального ущерба.

**Стандарты Wi-Fi 802.11**

С течением времени происходит развитие стандартов 802.11. Существуют следующие стандарты.

* **IEEE 802.11a**: работает в частотном диапазоне от 5 ГГц и обеспечивает скорость до 54 Мбит/с. Поскольку этот стандарт работает на более высоких частотах, он имеет меньшую зону покрытия и менее эффективен внутри зданий. Устройства, работающие в соответствии с данным стандартом, несовместимы со стандартами 802.11b и 802.11g, описанными ниже.
* **IEEE 802.11b**: работает в частотном диапазоне от 2,4 ГГц и обеспечивает скорость до 11 Мбит/с. Устройства, работающие в соответствии с этими стандартами, имеют больший диапазон и эффективнее работают внутри зданий по сравнению с устройствами стандарта 802.11a.
* **IEEE 802.11g**: работает в частотном диапазоне от 2,4 ГГц и обеспечивает скорость до 54 Мбит/с. Устройства, работающие в соответствии с аналогичным стандартом, работают с той же радиочастотой и диапазоном, что и устройства со стандартом 802.11b, но имеют пропускную способность стандарта 802.11a.
* **IEEE 802.11n**: работает в частотных диапазонах 2,4 ГГц и 5 ГГц. Поддерживает скорость от 150 Мбит/c до 600 Мбит/c и работает в диапазоне до 70 метров. Этот стандарт обладает обратной совместимостью с устройствами стандартов 802.11a/b/g.
* **IEEE 802.11ac**: работает в полосе частот 5 ГГц и обеспечивает скорость передачи данных от 450 Мбит/с до 1,3 Гбит/с (1300 Мбит/с). Совместим с прежними версиями устройств 802.11a/n.
* **IEEE 802.11ad**: также называется «WiGig». Этот стандарт использует связь Wi-Fi с тремя частотными диапазонами: 2,4 ГГц, 5 ГГц и 60 ГГц, а также теоретически обеспечивает скорость передачи до 7 Гбит/с.

**Канальный уровень**

Уровень доступа к сети модели TCP/IP объединяет два уровня сетевой модели OSI:

* канальный (уровень 2)
* физический (уровень 1)

Как показано на рисунке, канальный уровень отвечает за обмен кадров между узлами по физической сетевой среде. Он позволяет верхним уровням получать доступ к среде передачи данных, а также управляет способами размещения и получения данных в этой среде.

**Примечание**. На втором уровне сетевое устройство, подключённое к общей среде, называется узлом.

Канальный уровень обеспечивает два базовых сервиса (или две базовых функции):

* принимает пакеты уровня 3 и объединяет их в блоки данных, которые называются кадрами;
* контролирует управление доступом к среде и выполняет обнаружение ошибок.

Канальный уровень эффективно скрывает переходы пакета из одной среды передачи данных в другую среду от процессов на более высоких уровнях сетевой модели OSI. Канальный уровень получает и отправляет пакеты в протокол верхнего уровня (в данном случае это протокол IPv4 или IPv6). Протоколам верхнего уровня не требуется знать, какая среда будет использоваться при передаче данных.

**Примечание**. В этой главе понятие «среда» не относится к цифровому контенту и средствам мультимедиа (например, аудио, анимация, телевидение и видео). Среда — это материал для передачи сигналов данных, например, медный или оптоволоконный кабель.

**Подуровни каналов данных**

Канальный уровень делится на следующие два подуровня.

* **Управление логическим каналом (LLC)**: это верхний подуровень, который определяет программные процессы, предоставляющие службы протоколам сетевого уровня. Он помещает в кадре информацию, которая определяет, какой протокол сетевого уровня используется для данного кадра. Данная информация позволяет протоколам уровня 3, таким как IPv4 и IPv6, использовать один и тот же сетевой интерфейс и одно и то же средство передачи данных.
* **Управление доступом к среде передачи данных MAC**: это нижний подуровень, который определяет ключевые процессы доступа к среде передачи, выполняемые аппаратным обеспечением. Он обеспечивает адресацию на канальном уровне и разделение данных в соответствии с физическими требованиями к сигнализации, а также тип используемого протокола канального уровня.

Разделение сетей канального уровня на подуровни предоставляет одному типу кадра, определённому верхним уровнем, доступ к разным типам сред, определённых нижним уровнем. Это касается многих технологий локальной сети, в том числе Ethernet.

На рисунке показано, как канальный уровень разделяется на подуровни управления логическим каналом и управления доступом к среде передачи данных MAC. Управление логическим каналом взаимодействует с сетевым уровнем, а подуровень MAC обеспечивает работу различных технологий сетевого доступа. Например, подуровень MAC взаимодействует с технологией локальной сети Ethernet для передачи и приёма кадров по медному или оптоволоконному кабелю. Также подуровень MAC взаимодействует с такими беспроводными технологиями, как Wi-Fi и Bluetooth для беспроводной передачи и приёма кадров.

**Управление доступом к среде передачи данных**

Протоколы уровня 2 определяют инкапсуляцию пакета в кадр, а также методы получения и отправки инкапсулированных пакетов по средам передачи данных. Технология, используемая для получения и отправки кадра, называется методом контроля доступа к среде.

При прохождении пакетов от узла источника к узлу назначения они обычно проходят по различным физическим сетям. Эти физические сети могут состоять из различных типов физических сред передачи данных, например медных и оптоволоконных кабелей, беспроводных сетей, состоящих из электромагнитных сигналов, радио- и микроволновых частот, а также спутниковых каналов.

Пакеты не имеют прямого доступа к этим средам. Канальный уровень OSI подготавливает пакеты сетевого уровня для передачи и контролирует доступ к физическим средам. Способы управления доступом к среде передачи данных, описанные протоколами канального уровня, определяют процессы, с помощью которых сетевые устройства могут получить доступ к сетевой среде и передавать кадры в различных сетевых средах.

Без канального уровня протоколы сетевого уровня, например IP, должны обеспечить соединение для каждого типа передающей среды, которые могут находиться по пути следования пакета. Более того, протоколу IP необходимо каждый раз адаптироваться к новой сетевой технологии или среде. Этот процесс затруднил бы обновление и развитие сетевых сред передачи. Это основная причина использования многоуровневого подхода в сети.

Анимация на рисунке приводит пример ПК, который находится в Париже и подключается к ноутбуку в Японии. Несмотря на то, что два узла осуществляют передачу данных через IP, для передачи IP-пакетов по различным типам локальных и глобальных сетей могут использоваться разные протоколы канального уровня. Каждый переход на маршрутизаторе может потребовать иного протокола канального уровня для передачи в новой среде.

**Предоставление доступа к среде**

В рамках одного сеанса связи могут потребоваться различные методы управления доступом к среде передачи данных. Каждая сетевая среда, по которой проходят пакеты в течение передачи от локального до удалённого узла, может иметь разные характеристики. Например, локальная сеть Ethernet состоит из множества узлов, которые борются за доступ к среде передачи. Последовательные каналы состоят из прямого подключения между двумя устройствами, по которым следуют потоки данных в виде битов.

Интерфейсы маршрутизатора инкапсулируют пакет в соответствующий кадр. Для доступа к каждому каналу используется подходящий способ контроля доступа к среде передачи. В любом обмене пакетами сетевого уровня может быть множество переходов между канальным уровнем и средой. На каждом переходе по пути маршрутизатор:

* принимает кадр от передающей среды;
* деинкапсулирует кадр;
* повторно инкапсулирует пакет в новый кадр;
* передаёт новый кадр, который соответствует среде данного сегмента физической сети.

Маршрутизатор на рисунке имеет интерфейс Ethernet для подключения к локальной сети и последовательный интерфейс для подключения к глобальной сети (WAN). По мере того как маршрутизатор обрабатывает кадры, он использует службы канального уровня для получения кадра из одной передающей среды, затем деинкапсулирует кадр для протокольного блока данных уровня 3, повторно инкапсулирует блок данных в новый кадр и отправляет в среду следующего канала сети.

**Форматирование данных для последующей передачи**

Канальный уровень подготавливает пакет для передачи по локальной среде передачи путём его инкапсуляции с заголовком и концевиком для создания кадра. Описание кадра — это ключевой элемент каждого протокола канального уровня.

Для функционирования протоколам канального уровня требуется контрольная информация. Такая информация обычно отвечает на следующие вопросы.

* Между какими узлами осуществляется связь?
* Когда связь между отдельными узлами начинается, а когда заканчивается?
* Какие ошибки возникли при связи узлов?
* Между какими узлами произойдёт дальнейшая связь?

В отличие от других протокольных блоков данных, которые рассматриваются в данном курсе, кадр канального уровня состоит из следующих элементов.

* **Заголовок**: содержит контрольную информацию (например, адресация) и расположен в начале протокольного блока данных.
* **Данные**: содержит заголовок IP, заголовок транспортного уровня и данные.
* **Концевик**: содержит контрольную информацию для выявления ошибок, которая добавлена в конце протокольного блока данных.

Эти элементы кадра показаны на рисунке и будут рассмотрены более подробно.

**Создание кадра**

Во время перемещения данных по среде передачи они преобразуются в поток битов, или единиц и нулей. Если узел получает длинные потоки битов, как он определяет конец и начало кадра, а также какие биты представляют адрес?

Кадрирование делит поток в поддающиеся расшифровке группы. Контрольная информация помещается в заголовке и концевике в виде значений в разных полях. Этот формат предоставляет физическим сигналам структуру, которая может быть получена узлами и в месте назначения декодирована в пакеты.

Как показано на рисунке, типы полей кадра состоят из следующих элементов.

* **Флаги начала и конца кадра**: используются подуровнем MAC для определения границ начала и конца кадра.
* **Адресация**: используется подуровнем MAC для определения узлов источника и назначения.
* **Тип**: используется управлением логического канала для определения протокола уровня 3.
* **Управление**: определяет специальные службы управления потоком.
* **Данные**: содержит полезную нагрузку кадра (т. е. заголовок пакета, заголовок сегмента и данные).
* **Обнаружение ошибок**: размещается после данных для создания концевика. Эти поля кадра используются для обнаружения ошибок.

Не каждый протокол содержит все эти поля. Стандарты для конкретного канального протокола определяют фактический формат кадра.

**Примечание**. Примеры форматов кадра будут рассмотрены в конце данной главы.

**Стандарты канального уровня**

В отличие от протоколов верхних уровней набора протоколов TCP/IP, протоколы канального уровня, как правило, не определяются запросами на комментарии (документы RFC, имеющие статус стандартов). Несмотря на то, что Инженерная группа по развитию Интернета (IETF) поддерживает функциональные протоколы и сервисы для набора протоколов TCP/IP в верхних уровнях, IETF не определяет функции и принципы работы уровня доступа к сети этой модели.

Службы канального уровня и спецификации определены многочисленными стандартами на основе различных технологий и средств передачи данных, к которым применяются протоколы. Некоторые из этих стандартов сочетают в себе службы уровней 2 и 1.

Функциональные протоколы и службы на канальном уровне описываются следующими организациями:

* инженерными организациями, которые устанавливают общественные и открытые стандарты и протоколы;
* коммуникационными компаниями, которые устанавливают и применяют собственные протоколы для использования преимуществ технологических инноваций или рыночных возможностей.

К инженерным организациям, которые определяют открытые стандарты и протоколы, применимые к канальному уровню, относятся следующие.

* Институт инженеров по электротехнике и электронике (IEEE)
* Международный союз электросвязи (ITU)
* Международная организация по стандартизации (ISO)
* Американский национальный институт стандартизации (ANSI)

В таблице на рисунке выделены различные организации, которые устанавливают стандарты, а также некоторые из наиболее важных данных о протоколах канального уровня.

**Управление доступом к среде передачи данных**

Размещение кадров данных в среде контролируется подуровнем управления доступом к среде передачи данных.

Управление доступом к среде передачи данных работает так же, как правила дорожного движения, которые регулируют въезд автомобилей на дорогу. Отсутствие каких-либо мер управления доступом к среде передачи данных можно сравнить с поведением водителей, которые въезжают на дорогу, игнорируя движение других транспортных средств. Однако не все дороги и въезды одинаковы. Транспортные средства могут въезжать на дорогу, сливаясь с другими средствами передвижения или ожидая своей очереди у знака остановки или подчиняясь сигналам светофора. Водитель подчиняется различным правилам при въезде на дорогу.

Аналогичным образом существуют различные способы контроля размещения кадров в среде передачи данных. Протоколы канального уровня определяют правила для доступа в различные среды передачи данных. Некоторые методы контроля доступа используют тщательно отслеживаемые процессы для проверки безопасного размещения кадров в среде. Эти методы заданы сложными протоколами, которые требуют механизмов, приводящих к увеличению циркуляции служебной информации в сети.

Среди различных вариантов реализации протоколов канального уровня существуют разнообразные способы управления доступом к такой среде. Данные способы управления доступом к среде определяют, используют ли узлы данную среду совместно и каким образом это происходит.

Выбор способа контроля доступа к среде передачи зависит от следующих факторов.

* **Топология**: как связь между узлами отображается для канального уровня.
* **Общий доступ к среде**: как осуществляется общий доступ узлов к среде. Совместное использование среды может осуществляться соединением «точка-точка», как в глобальной сети, или может быть открыт общий доступ, как в локальных сетях.

**Физическая и логическая топология**

Топология сети — расположение или взаимоотношение сетевых устройств, а также взаимозависимость между ними. Топологии локальных и глобальных сетей можно рассматривать в двух видах.

* **Физическая топология**: термин, используемый для обозначения физических подключений, определяет, каким образом подключены оконечные устройства и устройства сетевой инфраструктуры, такие как маршрутизаторы, коммутаторы и беспроводные точки доступа. Физическая топология может быть двухточечной («точка-точка») или звездообразной. См. рисунок 1.
* **Логическая топология**: термин, используемый для обозначения способа передачи кадров от одного узла к следующему. Такое расположение состоит из виртуальных соединений между узлами сети. Эти логические пути сигнала определены протоколами канального уровня. Логическая топология двухточечных каналов сравнительно проста. При этом общая среда предлагает детерминированные и недетерминированные методы контроля доступа. См. рисунок 2.

При контроле доступа данных к сети канальный уровень «просматривает» логическую топологию сети. Именно логическая топология влияет на тип сетевой синхронизации и используемое средство управления доступом к среде.

**Наиболее распространенные физические топологии глобальной сети**

Глобальные сети часто подключены с помощью следующих физических топологий.

* **Двухточечная топология («точка-точка»)**: это простейшая топология, которая представляет собой постоянное соединение между двумя конечными устройствами. Именно по этой причине данная топология наиболее распространена в глобальной сети.
* **Топология hub-and-spoke (звезда)**: версия топологии типа «звезда» для глобальной сети, в которой центральный узел подключает филиалы с помощью двухточечных соединений.
* **Полносвязная (mesh) топология**: эта топология предоставляет высокую доступность, но требует, чтобы каждая конечная система была связана с каждой другой системой. Поэтому административные и физические расходы могут быть весьма значительными. Каждый канал является двухточечным каналом для другого узла. Варианты этой топологии включают в себя сильносвязную (partial mesh) топологию, к которой подключены некоторые, но не все оконечные устройства.

На рисунке показаны три наиболее распространённые физические топологии глобальной сети.

**Физическая двухточечная топология («точка-точка»)**

Физические двухточечные топологии напрямую связывают два узла, как показано на рисунке.

В данном расположении двум узлам не нужно совместно использовать одну среду передачи с другими узлами. Кроме того, узлу не нужно определять, адресован ли входящий кадр именно для него или адресован на другой узел. Поэтому логические протоколы канального уровня могут быть очень простыми, т. к. все кадры в среде могут быть направлены к двум узлам или от них. Один узел размещает кадры на одном конце, а другой узел получает эти кадры на другом конце двухточечного соединения.

Протоколы канального уровня могут обеспечить более сложные процессы управления доступом к среде передачи данных для логических двухточечных топологий, но это привело бы к лишним непроизводительным издержкам протокола.

**Логическая топология «точка-точка»**

Конечные узлы, сообщающиеся по двухточечной сети, могут быть физически подключены с помощью нескольких промежуточных устройств. Однако использование физических устройств в сети не влияет на логическую топологию.

Как показано на рис. 1, узлы источника и назначения с определённым расстоянием между собой могут быть косвенно подключены друг к другу. В некоторых случаях логическое соединение между узлами формирует так называемый виртуальный канал. Виртуальный канал — это логическое соединение, созданное в сети между двумя сетевыми устройствами. Два узла по обоим концам виртуального канала обмениваются кадрами между собой. Это происходит и в том случае, если кадры передаются через промежуточные устройства. Виртуальные каналы — это важные логические структуры связи, используемые некоторыми технологиями уровня 2.

Метод доступа к среде, используемый в сети протоколом канала передачи данных, определяется логической двухточечной топологией, а не физической топологией. Это означает, что логическое двухточечное соединение между двумя узлами не обязательно связывает два физических узла на каждом конце одного физического канала связи.

На рис. 2 показаны физические устройства между двумя маршрутизаторами.

**Полудуплексная и полнодуплексная передача данных**

На рис. 1 показана двухточечная топология. В двухточечных сетях данные передаются одним из двух следующих способов.

* **Полудуплексная передача**: оба устройства могут передавать и получать данные в среде, но не одновременно. Для разрешения конфликтов, возникающих в случае, когда сразу несколько станций пытаются передать данные одновременно, в сети Ethernet установлены особые правила. На рис. 2 показана полудуплексная передача.
* **Полнодуплексная передача**: оба устройства могут одновременно передавать и получать данные в среде. На канальном уровне может происходить одновременная передача данных на оба узла. Поэтому на канальном уровне нет необходимости в особых правилах. На рис. 3 показана полнодуплексная передача.

**Физические топологии локальной сети**

Физическая топология определяет, как физически соединены конечные системы. В локальных сетях с разделяемой (совместно используемой) средой передачи данных оконечные устройства могут быть соединены с помощью следующих физических топологий.

* **Топология типа «звезда»**: оконечные устройства подключаются к центральному промежуточному устройству. Прежние топологии типа «звезда» соединяли оконечные устройства с помощью концентраторов. Однако теперь в топологиях типа «звезда» используются коммутаторы. Топология типа «звезда» - это наиболее распространённая физическая топология локальной сети, главным образом потому, что она проста в установке, модификации (легко добавлять и удалять оконечные устройства) и удобна в устранении неполадок.
* **Расширенная звездообразная или гибридная**. В расширенной звездообразной топологии центральные промежуточные устройства соединяют остальные звездообразные топологии. В гибридной топологии звездообразные сети могут соединяться с использованием топологии шины.
* **Топология шины**: все конечные системы связаны друг с другом общей шиной (проводником, кабелем) и имеют оконцовку на концах шины. Для соединения оконечных устройств не требуются коммутаторы. Шинные топологии использовались в устаревших сетях Ethernet, поскольку были дешёвыми и легко устанавливались.
* **Кольцевая топология**: конечные системы подключены к соседнему узлу, формируя связь в форме кольца. В отличие от шинной топологии, кольцевая не требует оконцовки. Кольцевые топологии использовались в устаревших сетях оптоволоконных линий связи (FDDI). Оптоволоконные линии связи (FDDI) используют второе кольцо для повышения отказоустойчивости и производительности.

На рисунке показано, как оконечные устройства подключены в локальных сетях.

**Логическая топология совместных средств передачи данных**

Логическая топология сети тесно связана с механизмом, используемым для управления доступом к сети. Методы доступа предоставляют способы для управления доступом к сети таким образом, чтобы все станции были доступны. Когда несколько сущностей (узлов) совместно используют одну среду передачи данных, для управления доступом к среде необходим некоторый механизм. Методы доступа применяются в сетях для обеспечения такого механизма доступа к среде передачи данных.

Некоторые сетевые топологии используют общую среду с несколькими узлами. В любое время может возникнуть ситуация, при которой несколько устройств попытаются отправить или получить данные с помощью сетевой среды. Для общего использования среды существуют особые правила.

Для общего использования среды существуют два основных метода управления доступом.

* **Доступ на конкурентной основе (Contention-based access)**: все узлы конкурируют за использование среды, но имеют особый план действий в случае коллизий. На рис. 1 показан конкурентный доступ.
* **Контролируемый доступ (Controlled access)**: каждый узел использует среду в специально отведённое время. На рис. 2 показан контролируемый доступ.

Протокол канального уровня определяет способ управления доступом к среде передачи, что обеспечивает необходимый баланс между управлением кадром, защитой кадра и дополнительными накладными расходами при передаче данных в сети.

**Ассоциативный доступ**

При использовании недетерминированного конкурентного метода сетевое устройство может попытаться получить доступ к среде всегда, когда ему нужно отправить данные. Для предотвращения полной неупорядоченности в среде эти методы используют процесс множественного доступа с контролем несущей (CSMA), чтобы сначала обнаружить, передаёт ли среда сигнал.

Если в среде обнаружен сигнал несущей частоты, исходящий от другого узла, это значит, что в данный момент другое устройство осуществляет передачу данных. Если среда занята, когда устройство пытается передать данные, оно подождёт и повторит попытку позже. Если сигнал несущей частоты не обнаружен, данное устройство начнёт передачу данных. Конкурентный способ управления доступом к среде передачи данных используется беспроводными сетями и сетями Ethernet.

Процесс множественного доступа с контролем несущей (CSMA) может завершиться сбоем, из-за чего два устройства будут осуществлять передачу одновременно, создавая коллизию данных. В этом случае данные, отправленные обоими устройствами, будут повреждены, из-за чего потребуется их повторная отправка.

Конкурентные методы контроля доступа не имеют каких-либо дополнительных механизмов контроля доступа. Механизм для отслеживания очереди доступа к среде не требуется. Однако ассоциативные системы не отличаются хорошей масштабируемостью в условиях сильной загруженности среды. По мере увеличения интенсивности нагрузки и количества узлов снижается вероятность получить доступ к среде без коллизий. Кроме того, пропускная способность среды также уменьшается, так как для исправления ошибок, вызванных такими коллизиями, требуется задействовать механизмы восстановления.

Процесс множественного доступа с контролем несущей (CSMA) обычно используется совместно со способом разрешения конфликтов в среде. К двум наиболее широко распространённым методам относятся следующие.

* **Множественный доступ с контролем несущей и обнаружением коллизий (CSMA/CD)**: оконечное устройство отслеживает сигнал данных в среде. Если сигнал данных не найден, и, следовательно, среда свободна, то устройство передаёт данные. Если позже обнаруживаются сигналы о том, что в то же время передачу данных осуществляло другое устройство, передача данных на всех устройствах прерывается и переносится на другое время. Этот метод используется традиционными формами сетей Ethernet.
* **Множественный доступ с контролем несущей и предотвращением коллизий (CSMA/CA)**: оконечное устройство изучает сигнал данных в среде. Если среда не загружена, данное устройство отправляет по среде уведомление о намерении использовать её для передачи данных. Устройство посылает данные после того, как среда будет признана незагруженной. Этот способ используется беспроводными сетевыми технологиями стандарта 802.11.

На рисунке показано следующее:

* Как функционируют конкурентные методы доступа
* Характеристики конкурентных методов доступа
* Примеры конкурентных методов доступа

**Топология с множественным доступом**

Логическая топология с множественным доступом позволяет нескольким узлам обмениваться информацией друг с другом посредством совместного доступа к среде. Данные могут быть размещены в среде только с одного узла единовременно. Каждый узел видит все кадры в среде, но только тот узел, которому адресован кадр, обрабатывает содержимое кадра.

Для контроля передачи данных и предотвращения коллизий между сигналами при подключении к среде сразу нескольких узлов необходим метод контроля доступа к среде передачи данных.

Чтобы увидеть, как узлы получают доступ к среде в топологии с множественным доступом, включите анимацию.

**Контролируемый доступ**

При использовании контролируемого метода доступа сетевые устройства получают доступ к среде в порядке очереди. Если оконечному устройству не требуется доступ к среде, то возможность доступа переходит к следующему оконечному устройству. Этот процесс осуществляется с помощью маркера. Оконечное устройство получает маркер и размещает кадр в среде. Ни одно другое устройство не имеет права выполнять это действие до тех пор, пока кадр не будет получен и обработан в узле назначения, после чего маркер будет снова доступен.

**Примечание**. Этот метод также известен как «доступ по расписанию», или детерминированный доступ.

Хотя контролируемый доступ хорошо упорядочен и обеспечивает прогнозируемую пропускную способность, детерминированные методы могут оказаться неэффективными, поскольку устройству необходимо дождаться своей очереди, чтобы использовать среду.

К примерам контролируемого доступа относятся:

* Маркерное кольцо (IEEE 802.5)
* Оптоволоконная линия связи (FDDI), которая основывается на шинном протоколе IEEE 802.4.

**Примечание**. Оба эти метода управления доступом к среде передачи данных считаются устаревшими.

На рисунке показано следующее:

* Как функционируют контролируемые методы доступа
* Характеристики контролируемых способов доступа
* Примеры контролируемых способов доступа

**Кольцевая топология**

В логической кольцевой топологии каждый узел в свою очередь получает кадр. Если кадр не адресован узлу, получившему кадр, то этот узел пересылает кадр следующему узлу. Это позволяет кольцевой сети использовать контролируемый метод управления доступом к среде передачи данных, который называется эстафетной передачей.

Узлы в логической кольцевой топологии удаляют кадр из кольца, проверяют адрес и отправляет его дальше, если он адресован другому узлу. Все узлы кольца проверяют этот кадр (при пересылке между узлом источника и узлом назначения по маршруту движения).

Существует множество методов управления доступом к среде передачи данных, которые могут использоваться с логическими кольцами в зависимости от требуемого уровня контроля. Например, обычно в один момент времени по кольцу передаётся только один кадр. Если нет данных для передачи, то по кольцу по кругу передается пустой кадр (специальный сигнал), который называется маркером доступа. Узел имеет право передавать данные, только если он получил такой маркер.

Запомните, канальный уровень «видит» логическую кольцевую топологию. Реальная физическая топология может быть совершенно другой.

Чтобы увидеть, как узлы получают доступ к среде в логической кольцевой топологии, включите анимацию.

**Кадр**

Хотя многие протоколы канального уровня описывают кадры канального уровня, каждый тип кадра состоит из трех основных компонентов:

* Заголовок
* Данные
* Концевик

Все протоколы канального уровня инкапсулируют протокольный блок данных (PDU) уровня 3 в пределах поля данных конкретного кадра. Однако структура кадра и полей, содержащихся в заголовке и концевике, отличается в зависимости от протокола.

Протокол канального уровня описывает функции, требуемые для передачи пакетов по различным средам. Эти функции протокола сочетаются с инкапсуляцией кадра. Когда кадр прибывает по назначению, а протокол канального уровня принимает кадр, данные кадра читаются и отбрасываются.

Ни одна структура кадра не соответствует требованиям всех видов передачи данных во всех типах сред. В зависимости от окружающей среды, количество управляющей информации, требуемой в кадре, отличается, чтобы удовлетворить требования, выдвигаемые уровнем управления доступом к среде и логической топологией.

Как показано на рисунке 1, хрупкая среда требует больше возможностей контроля. При этом безопасная среда, как показано на рисунке 2, требует меньше мер контроля.

**Заголовок**

Заголовок кадра содержит управляющую информацию, определяемую протоколом канального уровня для используемой логической топологии и среды передачи данных.

Управляющая информация кадра уникальна для каждого типа протокола. Она используется протоколом уровня 2 и предоставляет функциональные возможности, требуемые коммуникационной средой.

На рисунке показаны поля заголовка кадра Ethernet.

* **Поле начала кадра**: показывает начало кадра.
* **Поля адресов источника и назначения**: указывает узлы источника и назначения в среде.
* **Поле типа**: отображает сервис верхнего уровня, который содержится в кадре.

Различные протоколы канального уровня могут использовать разные поля из указанных выше. Например, к полям заголовка кадра другого протокола уровня 2 могут относиться также следующие.

* **Поле приоритета и качества обслуживания (QoS)**: отображает отдельный вид коммуникационных услуг, подлежащий обработке.
* **Поле управления логическим соединением**: используется для установки логической связи между узлами.
* **Поле управления физическим каналом**: используется для установления соединения.
* **Поле управления потоком**: используется для запуска и остановки потока данных по среде.
* **Поле управления перегрузками**: отображает перегрузки в среде.

Поскольку назначение и функции протоколов канального уровня связаны с конкретными топологиями и средами передачи данных, нужно отслеживать каждый протокол, чтобы получать ясную картину его структуры кадра. По мере рассмотрения протоколов в данном курсе мы подробнее изучим структуру кадра.

**Адрес уровня 2**

Канальный уровень предоставляет адресацию, которая используется во время передачи кадра по совместно используемой локальной среде передачи данных. Адреса устройств на этом уровне называются физическими адресами. Адресация канального уровня содержится в заголовке кадра и указывает узел назначения кадра в локальной сети. Заголовка кадра также может содержать адрес источника кадра.

В отличие от логических адресов уровня 3, которые являются иерархическими, физические адреса не указывают, в какой сети находится устройство. Более того, физический адрес является уникальным адресом устройства. Если устройство переходит в другую сеть или подсеть, оно продолжит функционировать с тем же физическим адресом уровня 2.

Адрес, который принадлежит устройству и не является иерархическим, не может указывать местоположение устройства в больших сетях или в сети Интернет. Это так же сложно, как искать один конкретный дом в целом мире, зная лишь номер дома и название улицы. Однако физический адрес можно использовать для обнаружения устройства в ограниченной зоне. Поэтому адрес канального уровня используется только для доставки пакетов в рамках локальной сети. Адреса этого уровня используются в только пределах локальной сети. Сравните их с уровнем 3, где адреса в заголовке пакета передаются от узла-источника к узлу-назначения независимо от количества переходов сети на маршруте.

Если данные должны перейти в другой сегмент сети, необходимо промежуточное устройство, например маршрутизатор. Маршрутизатор должен принять кадр на основе физического адреса и деинкапсулировать кадр для просмотра иерархического адреса или IP-адреса. С помощью IP-адреса маршрутизатор может определить местоположение устройства назначения в сети, а также наилучший путь для его достижения. Узнав, куда необходимо передать пакет, маршрутизатор создаёт для него новый кадр, который отправляется на следующий сегмент к месту назначения.

На рисунке выделены требования адреса уровня 2 для коллективного доступа и двухточечных топологий.

**Концевик**

Протоколы канального уровня добавляют концевик в конец каждого кадра. Концевик используется для того, чтобы определить, есть ли в принятом кадре ошибки. Этот процесс называется обнаружением ошибок и реализуется путем размещения специальных кодов (битовых последовательностей) в концевике кадра. Обнаружение ошибок добавляется на канальном уровне, т. к. сигналы в среде могут быть подвержены помехам, искажениям или потерям, которые изменят значения битов, представленных сигналами. Такие коды (коды обнаружения и исправления ошибок) вычисляются по специальным математическим алгоритмам.

Передающий узел вычисляет специальный код на основе содержания кадра. Этот код называется CRC-кодом (Cyclic redundancy check code — циклическим избыточным кодом). Это значение размещено в поле контрольной последовательности кадра (FCS) и вычисляется на основе содержимого кадра.

Нажмите на рисунке поля «FCS» и «Остановка кадра», чтобы получить подробные сведения.

Когда кадр прибывает на узел места назначения, узел вычисляет значение CRC кадра. Принимающий узел сравнивает эти два значения CRC. Если значения совпадают, то считается, что кадр получен без потерь. Если значение CRC отличается от значения CRC, рассчитанного на принимающем узле, то кадр сбрасывается.

Таким образом, поле «FCS» используется, чтобы выявить наличие ошибок при передаче и приёме кадра. Механизм обнаружения ошибок, осуществляемый с помощью поля «FCS», обнаруживает большинство ошибок, полученных в среде.

Всегда существует небольшая вероятность того, что кадр с правильным расчетом CRC действительно повреждён. Ошибки в битах могут отменить друг друга при расчете CRC. Для обнаружения и исправления потерь данных понадобятся протоколы верхнего уровня.

**Кадры LAN и WAN**

В сети на основе стека протоколов TCP/IP все протоколы уровня 2 модели OSI работают по IP на уровне 3 OSI. Однако фактически используемый протокол уровня 2 зависит от логической топологии сети и реализации на физическом уровне. С учетом широкого спектра физических средств передачи данных, используемых в различных топологиях в сетях, используется еще больше протоколов уровня 2.

Каждый протокол осуществляет управление доступом к среде передачи данных для указанных логических топологий уровня 2. Это означает, что при реализации этих протоколов несколько различных сетевых устройств могут выступать в качестве узлов, которые работают на канальном уровне. К таким устройствам относятся сетевой адаптер или сетевые интерфейсные платы (NIC) на компьютерах, а также интерфейсы на маршрутизаторах и коммутаторах уровня 2.

Протокол уровня 2, используемый для конкретной топологии сети, определяется технологией, которая используется для реализации этой топологии. Технология, в свою очередь, определяется размером сети (с точки зрения количества узлов и географической территории) и сервисами, предоставляемыми в этой сети.

Технологии локальных сетей обычно используют высокую пропускную способность, которая может поддерживать много узлов. Локальные сети функционируют на сравнительно небольшой территории (в одном здании или комплексе зданий), и высокая плотность пользователей делает эту технологию очень рентабельной.

Однако использование высокой пропускной способности обычно не настолько рентабельно для глобальных сетей, которые охватывают обширные территории (например, города или целые области). Стоимость физических каналов для обширных территорий и технологий, используемых для передачи сигналов по этим территориям, обычно приводит к низкой пропускной способности.

Разница в пропускной способности требует использования различных протоколов для локальных и глобальных сетей.

К распространённым протоколам канального уровня относятся:

* Ethernet
* Протокол «точка-точка» (протокол PPP)
* Беспроводной доступ 802.11

Среди других протоколов, рассматриваемых в учебной программе CCNA, — протокол высокоуровневого управления каналом передачи данных (HDLC) и технология ретрансляции кадров (FrameRelay).

Чтобы увидеть примеры протоколов уровня 2, нажмите кнопку «Воспроизведение».

**Кадр Ethernet**

**Ethernet**

Ethernet — это основная технология локальных сетей. Это семейство сетевых технологий, которые регламентируются стандартами IEEE 802.2 и 802.3.

Стандарты Ethernet регламентируют как протоколы второго уровня, так и технологии первого уровня. Ethernet — это наиболее используемая технология локальной сети, которая поддерживает пропускную способность данных со скоростью 10 Мбит/с, 100 Мбит/с, 1 Гбит/с (1000 Мбит/с) или 10 Гбит/с (10 000 Мбит/с).

Основной формат кадра и подуровни IEEE уровней 1 и 2 модели OSI не меняются во всех формах Ethernet. Однако способы обнаружения и отправки информации в среду могут меняться в зависимости от различных реализаций.

Ethernet обеспечивает услугу передачи данных без установления соединения и подтверждения доставки по общей (разделяемой) среде с использованием множественного доступа с обнаружением коллизий и контролем несущей (CSMA/CD) как метода доступа к среде. Совместное использование среды требует, чтобы заголовок кадра Ethernet использовал адрес канального уровня для определения узлов источника и назначения. Как и в большинстве протоколов локальной сети, этот адрес называется MAC-адресом узла. MAC-адрес сети Ethernet состоит из 48 бит и обычно представлен в шестнадцатеричном формате.

На рисунке показано множество полей кадра Ethernet. На канальном уровне структура кадра практически идентична для всех скоростей Ethernet. Однако на физическом уровне различные версии Ethernet размещают биты в среде различными способами. В следующей главе сеть Ethernet рассматривается подробнее.