**Введение**

Физический уровень OSI позволяет передавать по сетевой среде биты, из которых состоит кадр канального уровня.

В настоящее время Ethernet является основной во всем мире технологией для локальных сетей. Ethernet функционирует на канальном и физическом уровнях. Стандарты протоколов Ethernet определяют многие аспекты сетевого обмена данными, включая формат и размер кадра, интервал отправки и кодирование. Когда подключенные к сети Ethernet узлы отправляют сообщения, они форматируют их в соответствии со стандартами макета кадра. Кадры также называются протокольными блоками данных (PDU).

Поскольку технология Ethernet состоит из стандартов на этих более низких уровнях, принцип её работы можно лучше всего понять применительно к модели OSI. Модель OSI отделяет функциональные возможности канального уровня адресации, формирования кадров и доступа к среде передачи данных от стандартов физического уровня такой среды. Стандарты Ethernet регламентируют как протоколы второго уровня, так и технологии первого уровня. Несмотря на то, что технические требования Ethernet поддерживают различные среды, полосы пропускания и другие варианты уровней 1 и 2, основной формат кадра и схема адреса будут одинаковыми для всех разновидностей Ethernet.

В этой главе подробно рассматриваются характеристики и работа технологии Ethernet по мере её развития, начиная с того времени, когда она являлась технологией общей среды и ассоциативного обмена данными, и до сегодняшних дней, когда она представляет собой высокоскоростную и полнодуплексную технологию.

**Подуровни LLC и MAC**

На сегодняшний день Ethernet является наиболее широко используемой технологией локальных сетей.

Ethernet функционирует на канальном и физическом уровнях. Это семейство сетевых технологий, которые регламентируются стандартами IEEE 802.2 и 802.3. Технология Ethernet поддерживает передачу данных на скоростях:

* 10 Мбит/с
* 100 Мбит/с
* 1000 Мбит/с (1 Гбит/с)
* 10 000 Мбит/с (10 Гбит/с)
* 40 000 Мбит/с (40 Гбит/с)
* 100 000 Мбит/с (100 Гбит/с)

Как показано на рис. 1, стандарты Ethernet регламентируют как протоколы уровня 2, так и технологии уровня 1. Для протоколов второго уровня, как и в случае со всеми стандартами группы IEEE 802, технология Ethernet полагается на работу этих двух отдельных подуровней канального уровня, а также на подуровни управления логическим каналом (LLC) и MAC.

**Подуровень LLC**

Подуровень LLC технологии Ethernet обеспечивает связь между верхними и нижними уровнями. Как правило, это происходит между сетевым программным обеспечением и аппаратным обеспечением устройства. Подуровень LLC использует данные сетевых протоколов, которые обычно представлены в виде пакета IPv4, и добавляет управляющую информацию, чтобы помочь доставить пакет к узлу назначения. LLC используется для связи с верхними уровнями приложений и перемещает пакет для доставки на нижние уровни.

LLC реализован в программном обеспечении, и его применение не зависит от оборудования. LLC для компьютера можно рассматривать как программное обеспечение драйвера сетевой платы (NIC). Драйвер сетевой платы — это программа, которая непосредственно взаимодействует с аппаратными средствами компьютера на сетевой интерфейсной плате для передачи данных между подуровнем MAC и физической средой.

**Подуровень MAC**

MAC представляет собой более низкий подуровень канального уровня. MAC реализуется аппаратно — обычно в сетевой интерфейсной плате компьютера. Спецификации содержатся в стандартах IEEE 802.3. На рис. 2 приведен список общих стандартов IEEE Ethernet.

**Подуровень MAC**

Как показано на рисунке, подуровень MAC Ethernet выполняет две основные задачи:

* Инкапсуляция данных
* Управление доступом к среде передачи данных

**Инкапсуляция данных**

Процесс инкапсуляции данных включает в себя сборку кадра перед его отправкой и разборку кадра после его получения. При формировании кадра на уровне MAC к PDU сетевого уровня добавляются заголовок и концевик.

Инкапсуляция данных обеспечивает три основных функции.

* **Разделение кадра**. Процесс формирования кадров предоставляет важные разделители, которые используются для определения группы битов, составляющих кадр. Этот процесс обеспечивает синхронизацию между передающими и получающими узлами.
* **Адресация**. Процесс инкапсуляции также обеспечивает адресацию канального уровня. Каждый заголовок Ethernet, добавляемый в кадр, содержит физический адрес (MAC-адрес), посредством которого кадр доставляется к узлу назначения.
* **Обнаружение ошибок**. Каждый кадр Ethernet содержит концевик с циклическим контролем по избыточности (CRC) содержимого кадра. После приёма кадра получающий узел создаёт CRC для сравнения с аналогичным параметром в кадре. Если эти два расчета CRC совпадают, кадр может считаться полученным без ошибок.

Использование кадров помогает при передаче битов, так как они помещаются в среду передачи данных, а также при группировании битов на принимающем узле.

**Управление доступом к среде передачи данных**

Второй функцией подуровня MAC является управление доступом к среде передачи данных. Управление доступом к среде передачи данных отвечает за размещение кадров в этой среде и удаление из нее кадров. Судя по названию этой функции, она позволяет управлять доступом к среде передачи данных. Этот подуровень напрямую взаимодействует с физическим уровнем.

Основная логическая топология Ethernet — это шина с множественным доступом; следовательно, среда передачи данных используется всеми узлами (устройствами) в одном сегменте сети. Ethernet — это способ ассоциативного доступа организации сети. Следует помнить, что метод ассоциативного доступа (или недетерминированный метод) означает, что любое устройство может постоянно предпринимать попытку передать данные в общей среде при наличии у него таких данных для отправки. При этом если несколько устройств в одной среде начнут вместе передавать информацию (подобно тому, как два человека попытаются разговаривать одновременно), то возникнет конфликт при передаче данных, который приведёт к их повреждению и невозможности дальнейшего использования. Чтобы не допустить подобной ситуации, Ethernet задействует метод множественного доступа с контролем несущей (CSMA) для управления общим доступом узлов.

**Управление доступом к среде передачи данных**

Процесс CSMA используется для того, чтобы сначала определить, передаётся ли сигнал в среде. 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. Существует вероятность возникновения сбоя процесса CSMA, в результате чего два устройства будут передавать данные одновременно. Это называется коллизией данных. В этом случае данные, отправленные обоими устройствами, будут повреждены, из-за чего потребуется их повторная отправка.

Способы контроля доступа к среде передачи на основе ассоциативного доступа не требуют наличия механизмов для отслеживания очередности доступа к среде; следовательно, они не обладают нагрузкой на ресурсы, присущей способам контролируемого доступа. 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.

Как показано на рисунке, CSMA обычно используется совместно с одним из методов разрешения конфликтов в среде. К двум наиболее широко распространённым методам относятся следующие.

**Обнаружение коллизий/CSMA**

При обнаружении коллизий/CSMA (CSMA/CD) устройство проверяет среду на наличие в ней сигнала данных. Если этот сигнал отсутствует, указывая на то, что среда передачи не загружена, 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. Для использования этого метода были разработаны традиционные формы Ethernet.

В современных сетях широкое применение технологий коммутации позволило практически полностью исключить первоначальную потребность в CSMA/CD для локальных сетей. Почти все проводные соединения между устройствами в современных локальных сетях являются полнодуплексными, т. е. способность устройства одновременно отправлять и принимать данные. Это означает, что, несмотря на то, что сети Ethernet разрабатывались с учетом использования технологии CSMA/CD, современные промежуточные устройства позволяют устранить коллизии, и процессы, обеспечиваемые CSMA/CD, в действительности уже не требуются.

Тем не менее, для беспроводных соединений в среде локальной сети возможность возникновения таких коллизий всё еще необходимо учитывать. Устройства в беспроводной локальной сети используют метод доступа к среде передачи данных с контролем несущей и предотвращением коллизий (CSMA/CA).

**Контроль несущей и предотвращение коллизий (CSMA/CA)**

При использовании CSMA/CA устройство проверяет среду передачи данных на наличие в ней сигнала данных. Если среда не загружена, данное устройство отправляет по среде уведомление о намерении использовать её для передачи данных. Затем устройство отправляет данные. Этот способ используется беспроводными сетевыми технологиями стандарта 802.11.

**MAC-адрес: идентификация Ethernet**

Как уже упоминалось ранее, основная логическая топология Ethernet — это шина с множественным доступом. Каждое сетевое устройство подключено к одной и той же общей среде передачи данных, и все узлы получают все передаваемые кадры. Проблема заключается в том, что если все устройства принимают все кадры, как каждое отдельное устройство может определить, является ли оно запланированным получателем, без дополнительной необходимости в обработке и декапсуляции кадра для достижения IP-адреса? Ситуация усложняется ещё больше в крупных сетях с высоким объёмом трафика, в которых пересылается значительное количество кадров.

Для предотвращения чрезмерных нагрузок, возникающих при обработке каждого кадра, был создан уникальный идентификатор — MAC-адрес, который используется для определения фактических узлов источника и назначения в пределах сети Ethernet. Независимо от типа используемой сети Ethernet MAC-адресация обеспечила метод идентификации устройств на более низком уровне модели OSI. Возможно, вы помните, что MAC-адресация добавляется как часть PDU уровня 2. MAC-адрес Ethernet — это 48-битное двоичное значение, выраженное в виде 12 шестнадцатеричных чисел (4 бита для каждой шестнадцатеричной цифры).

**Структура MAC-адресов**

MAC-адреса должны быть уникальными в глобальном масштабе. Значение MAC-адреса — это непосредственный результат применения правил, которые разработаны институтом IEEE для поставщиков, чтобы обеспечить глобальные уникальные адреса для каждого устройства Ethernet. В соответствии с этими правилами каждый поставщик, который занимается реализацией Ethernet-устройств, должен быть зарегистрирован в IEEE. IEEE присваивает поставщику 3-байтный (24-битный) код, который называется уникальным идентификатором организации (OUI).

Институт IEEE требует от поставщиков соблюдения двух простых правил, как показано на рисунке:

* Все MAC-адреса, назначаемые сетевой интерфейсной плате или другому устройству Ethernet, должны в обязательном порядке использовать этот идентификатор OUI поставщика в виде первых 3 байтов.

Всем MAC-адресам с одним и тем же идентификатором OUI должно быть присвоено уникальное значение (код производителя или серийный номер), которое указывается в виде последних 3 байтов.

**Обработка кадров**

MAC-адрес часто называется аппаратным адресом (BIA), поскольку исторически сложилось так, что он записывается в ПЗУ (постоянное запоминающее устройство) на сетевой интерфейсной плате. Это означает, что адрес вносится в чип ПЗУ на аппаратном уровне, и его изменение с помощью программного обеспечения невозможно.

**Примечание**. Операционные системы и сетевые платы современных компьютеров поддерживают возможность изменения MAC-адреса с использованием программ. Это удобно при попытке получения доступа к сети, в которой используется фильтрация на основе BIA; следовательно, фильтрация или отслеживание трафика на основе MAC-адреса более не является надёжным способом.

MAC-адреса присваиваются рабочим станциям, серверам, принтерам, коммутаторам и маршрутизаторам — любому устройству, которое должно отправлять или получать данные в сети. Все устройства, подключённые к локальной сети Ethernet, имеют интерфейсы с использованием MAC-адресов. Различные производители оборудования и программного обеспечения могут представлять MAC-адрес в разных шестнадцатеричных форматах. Форматы адресов могут иметь примерно следующий вид:

* 00-05-9A-3C-78-00
* 00:05:9A:3C:78:00
* 0005.9A3C.7800

При запуске компьютера сетевая плата вначале копирует MAC-адрес из ПЗУ в ОЗУ. Если устройство пересылает сообщение в сеть Ethernet, оно добавляет к пакету информацию заголовка. Информация заголовка содержит MAC-адреса источника и назначения. Исходное устройство отправляет данные по сети.

Каждая сетевая плата в сети просматривает информацию (на подуровне MAC), чтобы узнать, соответствует ли MAC-адрес назначения в кадре MAC-адресу физического устройства в ОЗУ. Если не удаётся обнаружить совпадения, устройство отклоняет кадр. Когда кадр достигает назначения, в котором MAC-адрес сетевой платы соответствует MAC-адресу получателя кадра, сетевая плата передаёт кадр на верхние уровни OSI, где происходит процесс деинкапсуляции.

**Инкапсуляция Ethernet**

С момента создания Ethernet в 1973 г. стандарты технологии совершенствовались, появлялись её более быстрые и гибкие версии. Развитие Ethernet с течением времени — одна из основных причин популярности технологии. Скорость ранних версий Ethernet была сравнительно низкой, всего 10 Мбит/с. Современные версии сети Ethernet работают со скоростью 10 гигабит в секунду и выше. На рис. 1 приведены изменения технологии Ethernet на примере различных версий.

На канальном уровне структура кадра практически идентична для всех скоростей Ethernet. Структура кадра Ethernet добавляет заголовки и концевики вокруг PDU третьего уровня для последующей инкапсуляции отправляемого сообщения.

Как заголовок, так и концевик Ethernet имеют несколько разделов информации, которые используются протоколом Ethernet. Каждый раздел кадра называется полем. Как показано на рис. 2, существуют два стиля формирования кадров Ethernet:

* стандарт Ethernet IEEE 802.3, который несколько раз обновлялся в соответствии с новыми технологиями;
* стандарт Ethernet DIX, который теперь называется Ethernet II.

Различия между стилями формирования кадров минимальны. Наиболее существенным различием между этими двумя стандартами является добавление в стандарте 802.3 начала разделителя кадра (SFD) и изменение поля «Тип» на поле «Длина».

Ethernet II — это формат кадра Ethernet, используемый в сетях TCP/IP.

**Размер кадра Ethernet**

Оба стандарта Ethernet II и IEEE 802.3 определяют минимальный размер кадра как 64 байта, а максимальный — 1518 байт. К этому количеству относятся все байты, начиная с поля «MAC-адрес назначения» и заканчивая полем «Контрольная последовательность кадра (FCS)». Поля «Преамбула» и «Начало разделителя кадра (SFD)» при описании размера кадра не включаются.

Любой кадр с длиной менее 64 байт считается «фрагментом коллизии», или «карликовым кадром», и автоматически отклоняется принимающими станциями.

Стандарт IEEE 802.3ac, выпущенный в 1998 году, позволил увеличить максимальный допустимый размер кадра до 1522 байт. Размер кадра был увеличен для использования технологии, которая называется «виртуальной локальной сетью» (VLAN). Виртуальные локальные сети создаются в пределах коммутируемой сети и будут рассматриваться при изучении одного из последующих курсов. Кроме того, множество технологий, которые обеспечивают качество обслуживания (QoS), используют поле «Приоритет пользователя», чтобы реализовать разные уровни обслуживания, такие как приоритет обслуживания для передачи голосового трафика. На рисунке показаны поля, содержащиеся в маркере 802.1Q VLAN.

Если размер передаваемого кадра меньше минимального значения или больше максимального значения, получающее устройство сбрасывает такой кадр. Отброшенные кадры, скорее всего, являются результатом коллизий или других нежелательных сигналов и, следовательно, считаются недействительными.

На канальном уровне структура кадра практически идентична. На физическом уровне различные версии Ethernet могут использовать разные способы обнаружения и помещения данных в среду передачи.

Кадр Ethernet: введение

Основными полями кадра Ethernet являются следующие.

* **Поля «Преамбула» и «Начало разделителя кадра»**. Поля «Преамбула» (7 байт) и «Начало разделителя кадра (SFD)», которое также называется «Начало кадра» (1 байт), используются для синхронизации отправляющих и получающих устройств. Эти первые 8 байт кадра необходимы для привлечения внимания получающих узлов. По существу, первые несколько байт сообщают получателям о необходимости приготовиться к поступлению нового кадра.
* **Поле «MAC-адрес назначения»**. Это поле (6 байт) является идентификатором для предполагаемого получателя. Как вы помните, этот адрес используется уровнем 2, чтобы помочь устройствам определить, адресован ли кадр именно им. Адрес в кадре сравнивается с MAC-адресом в устройстве. В случае совпадения устройство принимает кадр.
* **Поле «MAC-адрес источника»**. Это поле (6 байт) определяет сетевую плату или интерфейс, отправившие кадр.
* **Поле «Длина»**. В любом стандарте IEEE 802.3, используемом до 1997 года, поле «Длина» определяет точную длину поля данных кадра. Позже оно используется как часть контрольной последовательности кадра (FCS), чтобы обеспечить правильность получения сообщения. В других случаях это поле используется, чтобы описывать, какой протокол более высокого уровня присутствует. Если 2-октетное значение равно или превышает шестнадцатеричный формат 0x0600 или десятичное число 1536, то содержимое поля «Данные» декодируется в соответствии с указанным протоколом EtherType. Если же значение равно или менее шестнадцатеричного формата 0x05DC или десятичного числа 1500, то поле «Длина» позволяет обозначить использование формата кадра IEEE 802.3. Вот таким образом различаются кадры Ethernet II и 802.3.
* **Поле «Данные»**. Это поле (46—1500 байт) содержит инкапсулированные данные из более высокого уровня, который является универсальным PDU уровня 3, или, что используется чаще, — пакетом IPv4. Длина всех кадров должна быть не менее 64 байт. В случае инкапсуляции небольшого пакета используются дополнительные биты, которые называются символами-заполнителями, для увеличения размера кадра до этого минимального значения.
* **Поле «Контрольная последовательность кадра»**. Поле «Контрольная последовательность кадра (FCS)» (4 байта) используется для обнаружения ошибок в кадре. В нём используется циклический контроль избыточности (CRC). Отправляющее устройство включает в себя результаты циклического контроля избыточности в поле FCS кадра. Получающее устройство принимает кадр и создаёт CRC для поиска ошибок. Если расчёты совпадают, ошибки отсутствуют. Несовпадение расчётов означает изменение данных; следовательно, кадр сбрасывается. Данные могут измениться в результате нарушения электрических сигналов, которые представляют биты.

**MAC-адреса и шестнадцатеричная система счисления**

Использование MAC-адресов является одним из наиболее важных аспектов технологии локальной сети Ethernet. MAC-адреса используют шестнадцатеричную систему счисления.

Шестнадцатеричный — это слово, которое используется и как существительное, и как прилагательное. При использовании отдельно (как существительное) оно означает шестнадцатеричную систему счисления. Шестнадцатеричная система счисления обеспечивает удобный способ для представления двоичных значений. Подобно тому, как десятичный формат является системой счисления с основанием 10, а двоичный — с основанием 2, шестнадцатеричный формат представляет собой систему счисления с основанием 16.

В системе счисления с основанием 16 используются цифры от 0 до 9 и буквы от A до F. На рис. 1 показаны соответствующие десятичные и шестнадцатеричные значения для двоичного кода 0000—1111. Нам проще представить значение в виде одной шестнадцатеричной цифры, чем в виде четырёх двоичных битов.

Если 8 бит (байт) — это общепринятая бинарная группа, двоичный код 00000000—11111111 может быть представлен в шестнадцатеричной системе исчисления в качестве диапазона 00–FF. Чтобы заполнить 8-битное представление, всегда отображаются ведущие нули. Например, двоичное значение 0000 1010 показано в шестнадцатеричной системе как 0A.

**Примечание**. Важно отличать шестнадцатеричные значения от десятичных относительно символов от 0 до 9, как показано на рис. 1.

**Представление шестнадцатеричных значений**

Шестнадцатеричное значение обычно представлено в тексте значением, которое располагается после 0x (например, 0x73) или подстрочного индекса 16. В остальных, более редких случаях, за ним может располагаться H (например, 73H). Однако, поскольку подстрочный текст не распознаётся в командной строке или средах программирования, перед техническим представлением шестнадцатеричных значений стоит «0x» (нулевой Х). Так, приведённые выше примеры будут отображаться как 0x0A и 0x73 соответственно.

Шестнадцатеричная система счисления используется для представления MAC-адресов Ethernet и IP-адресов версии 6.

**Шестнадцатеричные преобразования**

Числовые преобразования между десятичными и шестнадцатеричными значениями не вызывают затруднений, однако быстрое деление или умножение на 16 не всегда удобно. При необходимости такого преобразования обычно проще преобразовать десятичное или шестнадцатеричное значение в двоичное, а затем преобразовать двоичное значение либо в десятичное, либо шестнадцатеричное, по мере необходимости.

Обладая определённым опытом, можно распознать шаблоны двоичных разрядов, совпадающих с десятичными и шестнадцатеричными значениями. На рис. 2 такие шаблоны показаны для выбранных 8-битных значений.

**Представления MAC-адресов**

На узле Windows MAC-адрес адаптера Ethernet можно определить с помощью команды**ipconfig /all**. Обратите внимание — на рис. 1 на дисплее отображается, что физический адрес (MAC-адрес) компьютера имеет вид 00-18-DE-C7-F3-FB. Если у вас есть соответствующие права доступа, вы можете выполнить эту операцию на своем компьютере.

В зависимости от устройства и операционной системы вы увидите различные представления MAC-адресов, как показано на рис. 2. Маршрутизаторы и коммутаторы Cisco используют форму XXXX.XXXX.XXXX, где X — это шестнадцатеричный символ.

**MAC-адрес одноадресной рассылки**

В сети Ethernet разные MAC-адреса используются для одноадресной, многоадресной и широковещательной рассылки уровня 2.

MAC-адрес одноадресной рассылки — это уникальный адрес, который используется при отправке кадра от одного передающего устройства к одному устройству назначения.

В примере, приведённом на рисунке, узел с IP-адресом 192.168.1.5 (источник) запрашивает веб-страницу с сервера с IP-адресом 192.168.1.200. Для отправки и приёма одноадресного пакета в заголовке IP-пакета должен указываться IP-адрес назначения. Кроме того, в заголовке кадра Ethernet должен присутствовать MAC-адрес назначения. IP-адрес и MAC-адрес — это данные для доставки пакета одному узлу.

**MAC-адрес широковещательной рассылки**

В пакете широковещательной рассылки содержится IP-адрес назначения, в узловой части которого присутствуют только единицы (1). Эта нумерация в адресе означает, что все узлы в локальной сети (домене широковещательной рассылки) получат и обработают пакет. Многие сетевые протоколы, в частности, DHCP и протокол разрешения адресов (ARP), используют широковещательные рассылки. Использование широковещательных рассылок протоколом ARP для сопоставления адресов уровня 2 с уровнем 3 будет рассмотрено в этой главе немного позже.

Как показано на рисунке, IP-адресу широковещательной рассылки требуется соответствующий MAC-адрес широковещательной рассылки в кадре Ethernet. В сетях Ethernet используется MAC-адрес широковещательной рассылки из 48 единиц, который в шестнадцатеричном формате выглядит как FF-FF-FF-FF-FF-FF.

**MAC-адрес многоадресной рассылки**

Адреса многоадресных рассылок позволяют исходному устройству рассылать пакет группе устройств. Устройства, относящиеся к многоадресной группе, получают ее IP-адрес. Диапазон адресов многоадресных рассылок IPv4 — от 224.0.0.0 до 239.255.255.255. Поскольку адреса многоадресных рассылок соответствуют группам адресов (которые иногда называются группами узлов), они используются только как адресаты пакета. У источника всегда одноадресный адрес.

Адреса многоадресных рассылок используются, например, в играх с удалённым подключением, в которых участвуют несколько человек из разных мест. Кроме того, такие адреса используются при дистанционном обучении в режиме видеоконференции, когда несколько учащихся подключены к одному и тому же курсу.

Как и в случае с адресами для одноадресной и широковещательной рассылки, IP-адресу для многоадресной рассылки требуется соответствующий MAC-адрес, чтобы фактически передавать кадры по локальной сети. MAC-адрес многоадресной рассылки — это особое значение, которое в шестнадцатеричном формате начинается с 01-00-5E. Остальная часть MAC-адреса многоадресной рассылки создаётся путем преобразования нижних 23 бит IP-адреса группы многоадресной рассылки в 6 шестнадцатеричных символов.

Как показано на анимации, в качестве примера используется шестнадцатеричный адрес многоадресной рассылки 01-00-5E-00-00-C8.

**MAC и IP**

Главному устройству присваиваются два основных адреса:

* физический адрес (MAC-адрес)
* логический адрес (IP-адрес)

MAC- и IP-адрес функционируют совместно, чтобы определить устройство в сети. Процесс использования MAC- и IP-адресов для поиска компьютера подобен использованию имени и адреса отдельного человека для отправки ему письма.

Как правило, имя человека не меняется. Адрес же зависит от местожительства и может измениться.

Как и в случае с именем человека, MAC-адрес на узле не меняется — он физически внедрён в сетевую плату узла и известен как физический адрес. Этот адрес остаётся неизменным независимо от расположения узла в сети.

IP-адрес похож на адрес места жительства человека. Он зависит от фактического расположения узла. Используя этот адрес, кадр может определить место, куда он должен быть отправлен. IP-адрес, или сетевой адрес, известен как логический адрес, так как он назначается логическим путем. Такой адрес присваивается каждому узлу сетевым администратором исходя из параметров локальной сети, к которой подключён узел. На рисунке показан иерархический характер определения местоположения отдельного лица с использованием «логического» адреса. Щёлкните каждую группу, чтобы просмотреть, как происходит фильтрация адреса.

Физический MAC-адрес и логический IP-адрес необходимы компьютеру для обмена данными в иерархической сети точно так же, как для отправки письма необходимы имя и адрес человека.

**Сквозное подключение, MAC- и IP-адреса**

Исходное устройство отправит пакет, используя IP-адрес. Одним из наиболее распространённых способов, с помощью которого исходное устройство может определить IP-адрес устройства назначения, является использование сервиса доменных имен (DNS), в котором IP-адрес привязан к имени домена. Например, имя www.cisco.com связано с адресом 209.165.200.225. Используя этот IP-адрес, пакет будет доставлен в то место в сети, в котором находится устройство назначения. Именно этот IP-адрес будут использовать маршрутизаторы, чтобы определить наилучший путь к узлу назначения. Другими словами, IP-адресация позволяет определять поведение IP-пакета при его прохождении от начального узла к конечному.

При этом в каждом канале на своём пути IP-пакет инкапсулируется в кадре в зависимости от используемой технологии канала передачи данных, которая связана с этим каналом, например, технологии Ethernet. Оконечные устройства в сети Ethernet не принимают и не обрабатывают кадры на основе IP-адресов — вместо этого кадр принимается и обрабатывается на основе MAC-адресов.

В сетях Ethernet MAC-адреса используются для определения (на более низком уровне) узлов источника и назначения. Когда подключённый к сети Ethernet узел начинает обмен данными, он рассылает кадры со своим MAC-адресом в качестве источника и MAC-адресом предполагаемого получателя в качестве назначения. Все узлы, которые получают кадр, будут считывать MAC-адрес назначения. Если MAC-адрес назначения совпадёт с MAC-адресом, установленным на сетевой интерфейсной плате узла, только после этого узел начнёт обработку сообщения.

На рис. 1 показано, как пакет данных, содержащий информацию об IP-адресе, инкапсулируется с кадрами канального уровня, содержащими информацию о MAC-адресе.

На рис. 2 показано, как происходит инкапсуляция кадров на основе технологии, используемой для фактического канала.

Каким образом IP-адреса IP-пакетов в потоке данных ассоциируются с MAC-адресами в каждом канале на пути к узлу назначения? Для этого используется протокол разрешения адресов (ARP).

**Протокол ARP: введение**

Следует помнить, что у каждого узла в IP-сети есть как МАС-адрес, так и IP-адрес. Чтобы отправлять данные, узел должен использовать оба адреса. Узел должен использовать собственные МАС- и IP-адреса в полях источника, а также предоставить МАС- и IP-адреса для назначения. Несмотря на то, что IP-адрес назначения будет предоставлен более высоким уровнем OSI, отправляющему узлу необходим способ найти MAC-адрес назначения для данного канала Ethernet. В этом заключается назначение протокола ARP.

В своей работе ARP полагается на конкретные типы широковещательных и одноадресных сообщений Ethernet, которые также называются запросами и ответами ARP.

Протокол ARP выполняет две основные функции:

* сопоставление адресов IPv4 и МАС-адресов
* сохранение таблицы сопоставлений

**Функции ARP**

**Сопоставление адресов IPv4 и МАС-адресов**

Чтобы кадр можно было поместить в среду передачи данных локальной сети, ему необходим MAC-адрес назначения. Когда пакет отправляется к канальному уровню для инкапсуляции в кадре, узел обращается к таблице в его памяти, чтобы найти адрес канального уровня, который сопоставлен с IPv4-адресом назначения. Эта таблица называется таблицей ARP или кэшем ARP. Таблица ARP хранится в оперативной памяти устройства.

Каждая запись или строка в таблице ARP связывает IP-адрес с MAC-адресом. Мы называем отношения между двумя значениями сопоставлением — это означает, что IP-адрес можно найти в таблице и с его помощью определить соответствующий MAC-адрес. Таблица ARP временно сохраняет (кэширует) сопоставление устройств в локальной сети.

Чтобы начать процесс, узел передачи пытается определить MAC-адрес, сопоставленный с IPv4-адресом назначения. Если это сопоставление в таблице будет найдено, узел использует MAC-адрес в качестве MAC-адреса назначения в кадре, который инкапсулирует пакет IPv4. Затем кадр кодируется в сетевой среде передачи данных.

**Сохранение таблицы ARP**

Таблица ARP сохраняется динамически. Существуют два способа, с помощью которых устройство может собирать MAC-адреса. Первый способ — мониторинг трафика, который появляется в сегменте локальной сети. Когда узел получает кадры из среды передачи данных, он может зарегистрировать IP- и MAC-адреса источника в виде сопоставления в таблице ARP. По мере передачи кадров по сети устройство заполняет таблицу ARP, добавляя пары адресов.

Второй способ получения пары адресов для устройства — отправка запроса ARP, как показано на рисунке. Запрос ARP представляет собой широковещательную рассылку уровня 2 на все устройства в локальной сети Ethernet. Запрос ARP содержит IP-адрес узла назначения и MAC-адрес широковещательной рассылки, FFFF.FFFF.FFFF. Поскольку это широковещательная рассылка, все узлы в локальной сети Ethernet получат её и обработают содержимое. Ответ поступит от того узла, у которого IP-адрес совпадает с IP-адресом в запросе ARP. Ответ будет представлен в виде кадра одноадресной рассылки, который содержит MAC-адрес, соответствующий IP-адресу в запросе. Затем этот ответ будет использован для добавления новой записи в таблицу ARP отправляющего узла.

К записям в таблице ARP добавляются временные метки — для этого используется практически такая же процедура, что и при добавлении временных меток для записей таблиц MAC-адресов в коммутаторах. Если к моменту истечения действия временной отметки устройство не получит кадр от какого-либо определённого устройства, запись для этого устройства будет удалена из таблицы ARP.

Кроме того, в таблицу ARP можно добавлять статические записи сопоставления, но это выполняется не часто. Срок действия статических записей в таблице ARP не истекает со временем, поэтому их необходимо удалять вручную.

**Принцип работы ARP**

**Создание кадра**

Как ведет себя узел, когда ему необходимо создать кадр, а кэш ARP не содержит сопоставления IP-адреса с MAC-адресом назначения? Он отправляет запрос ARP!

Когда протокол ARP получает запрос на сопоставление адреса IPv4 с MAC-адресом, он обращается к своей таблице ARP для поиска сопоставления, добавленного в кэш. Если такая запись не найдена, инкапсуляция пакета IPv4 будет невозможна, а процессы уровня 2 уведомят протокол ARP о том, что ему требуется сопоставление. Затем процессы ARP отправляют пакет запроса ARP, чтобы найти MAC-адрес устройства назначения в локальной сети. Если устройство, получившее этот запрос, имеет IP-адрес назначения, оно отправляет ответ ARP. В таблицу ARP добавляется сопоставление. Теперь пакеты для этого адреса IPv4 можно инкапсулировать в кадрах.

Если на запрос ARP не отвечает ни одно устройство, пакет отбрасывается, поскольку создание кадра невозможно. Информация об этом сбое инкапсуляции передаётся на верхние уровни устройства. Если устройство является промежуточным (например, маршрутизатором), верхние уровни могут отправить ответ на узел источника с ошибкой в пакете ICMPv4.

См. рис. 1—5, чтобы ознакомиться с процессом, который используется для получения MAC-адреса узла в локальной физической сети.

**Роль ARP в процессе удалённого обмена данными**

Все кадры должны быть доставлены на узел в сегменте локальной сети. Если узел назначения IPv4 находится в локальной сети, кадр будет использовать MAC-адрес данного устройства в качестве MAC-адреса назначения.

Если узел назначения IPv4 не находится в локальной сети, узлу источника необходимо доставить кадр к интерфейсу маршрутизатора, который является шлюзом, или следующим переходом, используемым для достижения этого узла назначения. Исходный узел будет использовать MAC-адрес шлюза в качестве адреса назначения для кадров, которые содержат пакет IPv4, адресованный узлам в других сетях.

Адрес шлюза интерфейса маршрутизатора сохраняется в IPv4-конфигурации узлов. Когда узел создаёт пакет для адресата, он сравнивает IP-адрес назначения и свой собственный IP-адрес, чтобы определить, находятся ли эти два IP-адреса в одной и той же сети уровня 3. Если узел-получатель находится в пределах другой сети, источник использует процесс ARP для определения МАС-адреса интерфейса маршрутизатора, выступающего в качестве шлюза.

В случае если запись шлюза отсутствует в таблице, обычный процесс ARP отправит запрос ARP для получения MAC-адреса, связанного с IP-адресом интерфейса маршрутизатора.

См. рис. 1—5, чтобы ознакомиться с процессом, который используется для получения MAC-адреса шлюза.

Удаление записей из таблицы ARP

Для каждого устройства таймер кэша ARP удаляет записи ARP, которые не используются в течение указанного периода времени. Этот период может быть разным в зависимости от устройства и его операционной системы. Например, некоторые операционные системы Windows хранят записи кэша ARP в течение 2 минут. Если в течение этого периода запись используется повторно, таймер ARP будет увеличен для неё до 10 минут.

Кроме того, можно использовать некоторые команды, чтобы вручную удалить все или некоторые записи из таблицы ARP. После удаления записи процесс отправки запроса ARP и получения ответа ARP необходимо задействовать повторно, чтобы зарегистрировать сопоставление в таблице ARP.

Для каждого устройства предусмотрена команда, зависящая от используемой операционной системы, с помощью которой можно удалить содержимое кэша ARP. Эти команды не вызывают выполнение ARP. Они только удаляют записи таблицы ARP. Служба ARP интегрирована внутри протокола IPv4 и реализуется устройством. Её работа очевидна как для приложений верхнего уровня, так и для пользователей.

Как показано на рисунке, в некоторых случаях необходимо удалить запись таблицы ARP.

**Протокол ARP и его проблематика**

На рисунке показаны две потенциальные проблемы, которые могут возникнуть при использовании ARP.

**Нагрузка на среду передачи данных**

Являясь кадром широковещательной рассылки, запрос ARP получается и обрабатывается всеми устройствами в локальной сети. В стандартной корпоративной сети такие широковещательные рассылки, скорее всего, не окажут серьёзного влияния на производительность сети. Тем не менее, если необходимо обеспечить питанием большое количество устройств, и все они одновременно попытаются получить доступ к сетевым службам, это может на короткий период времени негативно повлиять на продуктивность работы сети. Например, если все учащиеся, выполняющие лабораторную работу, одновременно выполнят доступ в систему учебных компьютеров и попытаются подключиться к Интернету, это может привести к появлению задержек. При этом, после того как устройства разошлют начальные запросы широковещательной рассылки ARP и получат необходимые MAC-адреса, любое влияние на сеть будет сведено к минимуму.

**Безопасность**

В некоторых случаях использование протокола ARP может представлять определённый риск для безопасности. ARP-спуфинг (также называемый «отравлением» ARP-кэша) используется злоумышленниками, чтобы с помощью фальшивых запросов ARP добавить в сеть заведомо неправильную связь с MAC-адресом. Злоумышленник фальсифицирует MAC-адрес устройства, после чего кадры могут отправляться на неправильный адрес назначения.

Конфигурация статических связей ARP вручную — это один из способов предотвращения ARP-спуфинга. На некоторых устройствах можно указать допустимые MAC-адреса, и в результате доступ к сети смогут получить только указанные устройства.

**Устранение последствий, вызванных проблемами с протоколом ARP**

Используя современные коммутаторы, можно уменьшить количество проблем, связанных с широковещательными рассылками и обеспечением безопасности при работе с протоколом ARP. Коммутаторы Cisco поддерживают несколько технологий обеспечения безопасности, которые специально предназначены для решения проблем в сетях Ethernet, связанных с широковещательными рассылками в целом и с использованием протокола ARP в частности.

Коммутаторы обеспечивают сегментацию локальной сети, разделяя ее на несколько независимых коллизионных доменов. Каждый порт на коммутаторе представляет собой отдельный коллизионный домен и обеспечивает полную пропускную способность для одного или нескольких узлов, подключённых к этому порту. Несмотря на то, что по умолчанию коммутаторы не предотвращают распространение широковещательных рассылок на подключённые устройства, они действительно изолируют одноадресные рассылки в сети Ethernet таким образом, чтобы их могли «услышать» только устройства источника и назначения. Поэтому при наличии большого количества запросов ARP каждый ответ ARP будет передаваться только между двумя устройствами.

Относительно снижения вероятности различных атак с использованием широковещательной рассылки, к которым уязвимы сети Ethernet, сетевые специалисты могут применять технологические разработки, обеспечивающие безопасность коммутаторов Cisco, такие как создание специальных списков доступа и защита портов.

**Основная информация о портах коммутатора**

Следует помнить, что логическая топология сети Ethernet — это шина с множественным доступом, в которой все устройства используют общий доступ к одной и той же среде передачи данных. Эта логическая топология определяет, как узлы в сети просматривают и обрабатывают кадры, отправляемые и получаемые в этой сети. Тем не менее, в настоящее время практически во всех сетях Ethernet используется физическая топология типа «звезда» или «расширенная звезда». Это означает, что в большинстве сетей Ethernet оконечные устройства, как правило, подключаются к коммутатору LAN уровня 2 по принципу «точка-точка».

Коммутатор LAN уровня 2 осуществляет коммутацию и фильтрацию только на основе МАС-адреса канального уровня модели OSI. Коммутатор полностью прозрачен для сетевых протоколов и пользовательских приложений. Коммутатор уровня 2 создаёт таблицу МАС-адресов, которую в дальнейшем использует для принятия решений о пересылке пакетов. В процессе передачи данных между независимыми IP-подсетями коммутаторы уровня 2 полагаются на маршрутизаторы.

**Таблица MAC-адресов коммутатора**

Коммутаторы используют MAC-адреса для передачи данных по сети через свою коммутирующую матрицу на соответствующий порт в направлении узла назначения. Коммутирующая матрица представляет собой интегрированные каналы и дополняющие средства машинного программирования, что позволяет контролировать пути прохождения данных через коммутатор. Чтобы коммутатор смог понять, какой порт необходимо использовать для передачи кадра одноадресной рассылки, сначала ему необходимо узнать, какие узлы имеются на каждом из его портов.

Коммутатор определяет способ обработки входящих кадров, используя для этого собственную таблицу МАС-адресов. Он создаёт собственную таблицу MAC-адресов, добавляя в нее MAC-адреса узлов, которые подключены к каждому из его портов. После внесения MAC-адреса для того или иного узла, подключённого к определённому порту, коммутатор сможет отправлять предназначенный для этого узла трафик через порт, который сопоставлен с узлом для последующих передач.

Если коммутатор получает кадр данных, для которого в таблице нет MAC-адреса назначения, он пересылает этот кадр на все порты, за исключением того, на котором этот кадр был принят. Если от узла назначения поступает ответ, коммутатор вносит MAC-адрес узла в таблицу адресов, используя для этого данные из поля адреса источника кадра. В сетях с несколькими подключёнными коммутаторами в таблицы MAC-адресов вносятся несколько MAC-адресов портов, соединяющих коммутаторы, которые отражают элементы за пределами узла. Как правило, порты коммутатора, используемые для подключения двух коммутаторов, имеют несколько MAC-адресов, внесённых в соответствующую таблицу.

Чтобы увидеть, как это реализуется, просмотрите каждый шаг на рис. 1—6.

Описание этого процесса приведено ниже.

**Шаг 1.** Коммутатор получает кадр широковещательной рассылки от PC1 на порт 1.

**Шаг 2.** Коммутатор вводит МАС-адрес источника и порт коммутатора, получившего кадр, в таблицу МАС-адресов.

**Шаг 3.** Поскольку адрес назначения широковещательный, коммутатор рассылает кадр по всем портам, кроме порта, по которому он был получен.

**Шаг 4.** Устройство назначения отвечает на широковещательную рассылку индивидуальным кадром по адресу PC1.

**Шаг 5.** Коммутатор добавляет МАС-адрес источника PC2 и номер порта коммутатора, получившего кадр, в таблицу МАС-адресов. Адрес назначения кадра и соответствующий порт находятся в таблице МАС-адресов.

**Шаг 6.** Теперь коммутатор может пересылать кадры между устройствами источника и назначения без лавинной рассылки, поскольку у него есть записи в таблице МАС-адресов, которые идентифицируют соответствующие порты.

**Примечание**. Таблицу MAC-адресов иногда называют таблицей ассоциативной памяти (CAM). Хотя понятие «таблица ассоциативной памяти» используется относительно часто, в этом курсе мы будем называть её таблицей MAC-адресов.

**Настройки дуплексного режима**

Несмотря на то, что коммутаторы прозрачны для сетевых протоколов и пользовательских приложений, они способны функционировать в разных режимах, что может как положительно, так и отрицательно отразиться на пересылке кадров Ethernet по сети. Одним из базовых параметров коммутатора является дуплексный режим для каждого отдельного порта, подключённого к каждому главному устройству. Порт на коммутаторе должен быть настроен таким образом, чтобы совпадать с параметрами дуплексного режима определённого типа среды передачи данных. Для обмена данными в сетях Ethernet используются два типа настроек дуплексного режима: полудуплексный и полнодуплексный.

**Полудуплексная передача данных**

Полудуплексная связь использует однонаправленный поток данных, когда отправка и получение данных не выполняются в одно и то же время. Это подобно использованию рации, когда единовременно может говорить только один человек. Если кто-либо пытается говорить во время разговора другого человека, происходит коллизия. В результате при полудуплексной связи используется множественный доступ с контролем несущей и определением коллизий, что позволяет снизить вероятность коллизий и обнаружить их в случае возникновения. При полудуплексной связи возможно снижение производительности, вызванное постоянным пребыванием в режиме ожидания, поскольку данные могут передаваться одновременно только в одном направлении. Полудуплексные соединения, как правило, встречаются на более старом оборудовании, например на концентраторах. Узлы, которые подключены к концентраторам, совместно использующим подключение к порту коммутатора, должны работать в полудуплексном режиме, так как конечные компьютеры должны иметь возможность обнаруживать коллизии. Узлы могут функционировать в полудуплексном режиме, если сетевую интерфейсную плату нельзя настроить для работы в полнодуплексном режиме. В этом случае для порта на коммутаторе по умолчанию также устанавливается полудуплексный режим. Из-за этих ограничений полнодуплексная связь заменила полудуплексную на более современном оборудовании.

**Полнодуплексная передача данных**

В полнодуплексной связи поток данных передаётся в обе стороны, что позволяет одновременно отправлять и получать информацию. Поддержка двухсторонней передачи данных повышает производительность за счёт сокращения времени ожидания между передачами. Большинство продаваемых сегодня сетевых адаптеров Ethernet, Fast Ethernet и Gigabit Ethernet работают в полнодуплексном режиме. В полнодуплексном режиме детектор коллизий отключён. При этом исключена возможность столкновения кадров, пересылаемых двумя связанными конечными узлами, поскольку эти узлы используют два отдельных канала связи в сетевом кабеле. Каждое полнодуплексное соединение использует только один порт. Полнодуплексным соединениям требуется коммутатор, который поддерживает полнодуплексный режим, или прямое подключение, между двумя узлами, каждый из которых поддерживает полнодуплексную передачу данных. Узлы, которые непосредственно подключены к выделенному порту коммутатора с помощью сетевых адаптеров, поддерживающих полнодуплексную связь, должны подключаться к портам коммутатора, настроенных для работы в полнодуплексном режиме.

На рисунке показаны две настройки дуплексного режима, доступные на современном сетевом оборудовании.

Коммутатор Cisco Catalyst поддерживает три настройки дуплексного режима:

* Параметр full устанавливает полнодуплексный режим.
* Параметр half устанавливает полудуплексный режим.
* Параметр auto обеспечивает автоматическое согласование дуплексного режима. При включении автоматического согласования два порта связываются друг с другом, чтобы определить оптимальный режим работы.

Для портов Fast Ethernet и 10/100/1000 по умолчанию выбирается параметр auto. Для портов 100BASE-FX по умолчанию выбирается параметр full. Порты 10/100/1000 функционируют либо в полудуплексном, либо в полнодуплексном режиме, когда работают со скоростью 10 или 100 Мбит/с, и только в полнодуплексном, когда работают со скоростью 1000 Мбит/с.

**Функция Auto-MDIX**

Помимо правильной настройки дуплексного режима необходимо определить соответствующий тип кабеля для каждого порта. Ранее для соединений между определёнными устройствами (типа «коммутатор-коммутатор», «коммутатор-маршрутизатор», «коммутатор-узел» и «маршрутизатор-главное устройство») требовалось использование кабелей особого типа (перекрёстных или прямых). Вместо этого большинство современных коммутирующих устройств поддерживают команду конфигурации интерфейса**mdix auto**, которая доступна через CLI и позволяет использовать автоматическую функцию Auto-MDIX (интерфейс, зависящий от передающей среды с перекрёстным соединением).

При использовании функции Auto-MDIX коммутатор определяет необходимый тип кабеля для медных подключений Ethernet и соответствующим образом настраивает интерфейсы. Таким образом, можно использовать либо перекрёстный, либо прямой кабель для подключений к медному порту 10/100/1000 коммутатора независимо от типа устройства на другом конце соединения.

Функция Auto-MDIX включена по умолчанию на коммутаторах под управлением ОС Cisco IOS 12.2(18)SE или более поздней версии. В версиях Cisco IOS от 12.1(14)EA1 до 12.2(18)SE функция Auto-MDIX по умолчанию отключена.

**Способы пересылки кадра на коммутаторах Cisco**

В прошлом коммутаторы использовали один из следующих способов пересылки для коммутации данных между сетевыми портами:

* Коммутация с буферизацией
* Коммутация без буферизации

На рис. 1 приведены различия между этими двумя способами.

При коммутации с буферизацией, когда коммутатор получает кадр, он хранит данные в буфере до тех пор, пока не будет получен весь кадр. Во время сохранения коммутатор анализирует кадр, чтобы получить информацию о его адресате. При этом коммутатор также выполняет проверку на наличие ошибок, используя концевую часть кадра Ethernet циклического контроля избыточности (CRC).

При CRC используется математическая формула, основанная на количестве бит (единиц) в кадре, что позволяет определить, есть ли ошибка в полученном кадре. После подтверждения целостности кадра он перенаправляется через соответствующий порт к узлу назначения. Если же в кадре обнаружена ошибка, коммутатор отклонит его. Отклонение кадров с ошибками позволяет уменьшить количество пропускной способности, потребляемой повреждёнными данными. Коммутация с буферизацией необходима для анализа качества обслуживания (QoS) в конвергированных сетях, в которых требуется классификация кадра для назначения приоритетов проходящего трафика. Например, при передаче речи по IP потоки данных должны иметь больший приоритет, чем трафик, используемый для просмотра веб-страниц.

На рис. 2 можно воспроизвести анимацию, которая демонстрирует коммутацию с буферизацией. Коммутация с буферизацией — это единственный способ пересылки, используемый в современных моделях коммутаторов Cisco Catalyst.

**Коммутация без буферизации**

При использовании коммутации без буферизации коммутатор обрабатывает данные по мере их поступления даже в том случае, если передача ещё не завершена. Коммутатор добавляет в буфер именно такое количество кадра, которое требуется для чтения MAC-адреса назначения, чтобы он смог определить, на какой порт пересылать данные. MAC-адрес назначения указан в 6 байтах кадра после преамбулы. Коммутатор ищет MAC-адрес назначения в своей таблице коммутации, определяет порт исходящего интерфейса и направляет кадр на свой узел назначения через выделенный порт коммутатора. Коммутатор не проверяет кадр на наличие каких-либо ошибок. Поскольку коммутатору не нужно ждать добавления в буфер всего кадра целиком, и при этом он не выполняет проверку ошибок, коммутация без буферизации происходит быстрее, чем коммутация с буферизацией. Тем не менее, так как коммутатор не проверяет ошибки, он пересылает повреждённые кадры по всей сети. При пересылке повреждённые кадры уменьшают пропускную способность. В конечном итоге сетевая плата назначения отклоняет повреждённые кадры.

Воспроизведите анимацию, чтобы продемонстрировать коммутацию без буферизации.

Существуют два варианта коммутации без буферизации.

* **Коммутация с быстрой пересылкой**. Коммутация с быстрой пересылкой обеспечивает наименьший уровень задержки. При такой коммутации пакет пересылается сразу же после чтения адреса назначения. Поскольку при коммутации с быстрой пересылкой переадресация начинается до получения всего кадра целиком, могут возникнуть случаи, когда пакеты передаются с ошибками. Это происходит редко, и сетевой адаптер назначения отклоняет пакет, содержащий ошибки, после его получения. В режиме быстрой пересылки задержка измеряется с момента получения первого бита до передачи первого бита. Коммутация с быстрой пересылкой является типичным способом коммутации без буферизации.
* **Коммутация с исключением фрагментов**. При коммутации с исключением фрагментов коммутатор сохраняет первые 64 байта кадра перед его отправкой. Коммутацию с исключением фрагментов можно рассматривать как компромиссный вариант между коммутацией с буферизацией и коммутацией с быстрой пересылкой. Причина, по которой при коммутации с исключением фрагментов сохраняют только первые 64 байта кадра, заключается в том, что большинство сетевых ошибок и коллизий происходят именно в первых 64 байтах. Коммутация с исключением фрагментов пытается повысить эффективность коммутации с быстрой пересылкой, выполняя небольшую проверку ошибок в первых 64 байтах кадра, чтобы перед пересылкой кадра убедиться в отсутствии коллизии. Коммутация с исключением фрагментов представляет собой компромисс между большой задержкой с высокой целостностью (коммутация с буферизацией) и малой задержкой с меньшей целостностью (коммутация с быстрой пересылкой).

На рисунке приводится пример коммутации без буферизации.

Некоторые коммутаторы настроены на использование коммутации без буферизации для каждого порта до тех пор, пока не будет достигнуто указанное пользователем предельное количество ошибок, после чего автоматически устанавливается коммутация с буферизацией. После того, как частота повторения ошибок снизится до установленного предельного значения, порт автоматически переключится на использование коммутации без буферизации.

**Буферизация памяти на коммутаторах**

Как уже упоминалось, коммутатор анализирует некоторую часть пакета или весь пакет перед его пересылкой на узел назначения. Коммутатор Ethernet может использовать метод буферизации для хранения кадров до их пересылки. Кроме того, буферизацию можно использовать в том случае, если порт назначения занят по причине его перегрузки, и коммутатор сохраняет кадр до тех пор, пока не появится возможность его передачи.

Как показано на рисунке, существуют два метода буферизации памяти: буферизация на базе портов и буферизация совместного доступа к памяти

**Буферизация памяти на базе портов**

В процессе буферизации памяти на базе портов кадры хранятся в очередях, связанных с определёнными входящими и исходящими портами. Кадр пересылается на исходящий порт только в том случае, если все кадры, находящиеся в очереди перед ним, были успешно отправлены. Один кадр может стать причиной задержки передачи всех кадров в памяти из-за занятости порта назначения. Такая задержка возникает и в том случае, если другие кадры могут быть переданы на открытые порты назначения.

**Буферизация совместного доступа к памяти**

При буферизации совместного доступа к памяти все кадры помещаются в буфер, который является общим для всех портов коммутатора. Количество буферной памяти, которое необходимо каждому порту, выделяется динамически. Кадры в буфере динамически связываются с портом назначения. Это позволяет получать пакет на один порт и затем пересылать его на другой порт без перемещения в другую очередь.

Коммутатор сохраняет сопоставление кадра со связями порта, показывая, куда необходимо переслать пакет. Связь сопоставления удаляется после успешной передачи кадра. Количество кадров, сохранённых в буфере, ограничено размером всего буфера памяти и не ограничивается буфером одного порта. Это позволяет передавать кадры большего объема, при этом число сброшенных кадров будет меньше. Это особенно важно для асимметричной коммутации. Асимметричная коммутация позволяет использовать различные скорости передачи данных на разных портах. Это обеспечивает выделение пропускной способности некоторым портам, например, порту, подключённому к серверу.

**Фиксированная или модульная конфигурация**

При выборе коммутатора важно понимать его основные функции и параметры. Это означает, что необходимо решить, понадобятся ли различные функции, например питание через Ethernet (PoE), и определить предпочитаемую скорость пересылки трафика.

Как показано на рис. 1, функция PoE позволяет коммутатору обеспечивать питание устройств (например, IP-телефонов и некоторых точек беспроводного доступа) по имеющимся кабелям Ethernet. Это даёт большую гибкость для установки.

Скорость пересылки определяет возможности обработки коммутатора, оценивая, сколько данных в секунду перерабатывает коммутатор. Для классификации линеек коммутаторов используется скорость передачи трафика. Коммутаторы базового уровня имеют более низкую скорость пересылки, чем коммутаторы корпоративного уровня. Среди других важных аспектов — поддерживает ли устройство расширяемость конфигурации или нет, а также толщина коммутатора (выражается в количестве стойко-мест) и плотность портов, или количество портов, имеющихся на одном коммутаторе. Плотность портов устройства может различаться в зависимости от его конфигурации — фиксированной или модульной.

Эти параметры иногда называются форм-факторами коммутатора.

**Коммутаторы с фиксированной конфигурацией**

Судя по названию, коммутаторы с фиксированной конфигурацией — это устройства, конфигурацию которых изменить нельзя. Это означает, что вы не можете расширять их функциональные возможности или параметры и будете использовать только те, которые изначально предусмотрены для коммутатора. Доступные функции и параметры зависят от конкретной модели, которую вы приобретёте. Например, если вы приобретёте 24-портовый гигабитный коммутатор с фиксированной конфигурацией, вы уже не сможете в случае необходимости увеличить количество портов. Как правило, существуют различные настройки конфигурации, которые могут отличаться в зависимости от количества и типа установленных портов.

**Модульные коммутаторы**

Модульные коммутаторы предлагают большую гибкость конфигурации. Как правило, они поставляются с шасси различного размера, что позволяет устанавливать несколько модульных линейных плат. Порты фактически располагаются на линейных платах. Линейная плата вставляется в шасси коммутатора подобно платам расширения, устанавливаемым в ПК. Чем больше шасси, тем больше модулей оно поддерживает. Как показано на рисунке, на выбор предлагается множество различных размеров шасси. Если вы приобрели модульный коммутатор с 24-портовой линейной платой, вы можете легко установить еще одну такую же плату, в результате чего общее количество портов будет увеличено до 48.

На рис. 2 приведены примеры коммутаторов с фиксированной, модульной и наращиваемой конфигурацией.

**Параметры модуля для разъёмов коммутатора Cisco**

Линейки коммутаторов Cisco широко используются во всем мире во многом благодаря своей гибкости относительно использования дополнительных модулей. Операционная система Cisco IOS не только обладает самыми широкими функциями по сравнению с любой другой операционной системой для сетевых устройств, но она также разработана в соответствии с параметрами каждого сетевого устройства Cisco, в частности, коммутаторов.

Чтобы продемонстрировать все доступные функции, которых настолько много, что перечислить все из них в рамках этого курса невозможно, мы рассмотрим коммутаторы Catalyst 3560. Коммутаторы Catalyst серии 3560 оснащены портами стандарта SFP (подключаемый модуль с малым форм-фактором), которые поддерживают различные модули трансиверов SFP. Ниже приводится список SFP-модулей, поддерживаемых одним или несколькими типами коммутаторов серии 3560.

**SFP-модули Fast Ethernet** —

* 100BASE-FX (многомодовый оптоволоконный кабель (MMF)) на 2 километра (км)
* 100BASE-LX10 (одномодовый оптоволоконный кабель (SMF)) на 2 км
* 100BASE-BX10 (SMF) на 10 км
* 100BASE-EX (SMF) на 40 км
* 100BASE-ZX (SMF) на 80 км

**SFP-модули 10 Gigabit Ethernet** —

* 1000BASE-SX 50/62,5 мкм (MMF) до 550/220 м
* 1000BASE-LX/LH (SMF/MMF) до 10/0,550 км
* 1000BASE-ZX (SMF) до 70 км
* 1000BASE-BX10-D&1000BASE-BX10-U (SMF) до 10 км
* 1000BASE-T (трансивер для медного кабеля)

**SFP-модули 10 Gigabit Ethernet** —

* 10G-SR (MMF) до 400 м
* 10G-SR-X (MMF) до 400 м (с поддержкой расширенного диапазона температур)
* 10G-LRM (MMF) до 220 м
* FET-10G (MMF) до 100 м (для каналов исходящей связи коммутирующей матрицы Nexus)
* 10G-LR (SMF) до 10 км
* 10G-LR-X (SMF) до 10 км (с поддержкой расширенного диапазона температур)
* 10G-ER (SMF) до 40 км
* 10G-ZR (SMF) до 80 км
* Twinax (трансивер для медного кабеля) до 10 м
* Active Optical до 10 м (для подключений внутри стоек или между ними)

Модули 40 Gigabit Ethernet и 100 Gigabit Ethernet поддерживаются высокопроизводительными устройствами Cisco, к которым относятся такие, как, например, коммутатор Catalyst 6500, маршрутизатор CRS, маршрутизатор серии ASR 9000 и коммутатор серии Nexus 7000.

**Сравнение коммутации уровня 2 и уровня 3**

Помимо определения различных форм-факторов коммутаторов может возникнуть необходимость выбора между коммутатором LAN уровня 2 и коммутатором уровня 3.

Следует помнить, что коммутатор LAN уровня 2 выполняет коммутацию и фильтрацию, используя только MAC-адрес (уровень 2) канального уровня OSI, и при этом зависит от маршрутизаторов для передачи данных между независимыми IP-подсетями (см. рис. 1).

Как показано на рис. 2, коммутатор уровня 3 (например, Catalyst 3560) функционирует подобно коммутатору уровня 2 (например, Catalyst 2960), но вместо использования только одного MAC-адреса уровня 2 для принятия решений о пересылке коммутатор уровня 3 может также использовать также IP-адрес. Вместо того чтобы определять, какие MAC-адреса связаны с каждым из его портов, коммутатор уровня 3 может также установить, какие IP-адреса связаны с его интерфейсами. Это позволяет коммутатору уровня 3 перенаправлять трафик по сети, также используя данные об IP-адресе.

Коммутаторы уровня 3 также могут выполнять функции маршрутизации уровня 3, тем самым снижая необходимость установки выделенных маршрутизаторов в локальной сети. Поскольку в коммутаторах уровня 3 установлено специальное аппаратное обеспечение для коммутации, они, как правило, могут направлять данные со скоростью самой коммутации.

**Технология Cisco Express Forwarding**

Устройства Cisco, которые поддерживают коммутацию уровня 3, используют технологию Cisco Express Forwarding (CEF). Этот метод пересылки пакетов довольно сложен, но, к счастью, как и любая хорошая технология, он в основном выполняется в фоновом режиме. Обычно устройствам Cisco требуется небольшая настройка для использования технологии CEF.

По сути, CEF отделяет обычную строгую взаимозависимость между процессами принятия решений уровня 2 и уровня 3. Замедляет пересылку IP-пакетов постоянное взаимное обращение между структурными компонентами уровня 2 и 3 внутри сетевого устройства. Таким образом, ускорение пересылки пакетов происходит в том объёме, в каком возможно отделение структур данных уровней 2 и 3.

Двумя основными компонентами функционирования технологии CEF являются:

* База данных о переадресации (FIB)
* Таблицы смежности

По своей концепции FIB напоминает таблицу маршрутизации. Маршрутизатор использует таблицу маршрутизации, чтобы определить оптимальный путь к сети назначения, основываясь на сетевой части IP-адреса назначения. При использовании CEF информация, которая ранее хранилась в кэше маршрута, вместо этого сохраняется в нескольких структурах данных для коммутации CEF. Структуры данных обеспечивают оптимизированный поиск эффективной переадресации пакетов. Сетевое устройство использует таблицу поиска FIB, чтобы принять решение о коммутации в зависимости от назначения, не обращаясь при этом к кэшу маршрута.

FIB обновляется при появлении изменений в сети и содержит все маршруты, известные на тот момент.

Таблицы смежности поддерживают адреса следующего перехода уровня 2 для всех записей FIB.

Разделение информации о достижимости (в таблице FIB) и о пересылке (в таблице смежности) предоставляет следующие преимущества.

* Таблица смежности может быть создана независимо от таблицы FIB, что позволяет создавать обе таблицы без коммутации каких-либо обрабатываемых пакетов.
* Перезапись заголовка MAC, используемая для передачи пакета, не хранится в записях кэша, вследствие чего для изменений в строке перезаписи заголовка MAC не требуется аннулирование записей кэша.

По умолчанию использование технологии CEF включено для большинства устройств Cisco, которые выполняют коммутацию уровня 3.