Администрирование сетей Cisco: освоение за месяц

Бен Пайпер

ДМК ПРЕСС ИЗДАТЕЛЬСТВО

MANNING

УДК 004.71
ББК 32.972.5
П12

Пайпер Б.
П12 Администрирование сетей Cisco: освоение за месяц / пер. с анг. М. А. Райтмана. – М.: ДМК Пресс, 2018. – 316 с.: ил.

ISBN 978-5-94074-519-6

Эта книга в доступной форме рассказывает об администрировании сетей с применением оборудования Cisco. С помощью практических заданий вы сможете за месяц получить полное представление о том, как работают сети, и получите знания, которые сможете использовать уже сегодня. Вы сможете не только усовершенствовать свои навыки, но так же будете в состоянии объяснить, почему сети работают так, а не иначе.

Издание будет полезно начинающим администраторам сетей.

УДК 004.71
ББК 32.972.5

ISBN 978-1-617-29363-4 (анг.)
ISBN 978-5-94074-519-6 (рус.)

Содержание

Глава 2

Что такое сети Cisco?

Любая организация проводит основные объемы трафика через устройства двух типов: коммутаторы и маршрутизаторы. Cisco – наиболее популярный бренд, производящий надежные коммутаторы и маршрутизаторы, поэтому многие компании приняли его как стандарт для подобного рода устройств. Для прочего сетевого оборудования, например брандмауэра или точки беспроводного доступа, кто-то предпочитает Cisco, кто-то выбирает что-нибудь другое или использует бренды совместно. Но если сеть построена с использованием маршрутизаторов и коммутаторов Cisco, то это сеть Cisco.

Нет никаких обязательных требований к тому, чтобы использовать исключительно этот бренд. Вы можете использовать коммутаторы Cisco с маршрутизаторами Juniper, и они будут прекрасно работать вместе. Можно использовать маршрутизатор Cisco с коммутатором Juniper, и они тоже прекрасно уживутся. Но есть парочка возражений против подобных тандемов.

Во-первых, последовательность конфигурирования устройств Cisco в корне отлична от настройки оборудования Juniper. Синтаксис команд и терминология совершенно различны. Администрирование смешанных сетей требует знаний обеих платформ и принципов их взаимодействия, а эта книга посвящена только оборудованию компании Cisco.

Во-вторых, если у вас возникают проблемы и вы не уверены, связаны они с маршрутизатором или коммутатором, вам придется обращаться за техподдержкой сразу к обеим компаниям. В худшем случае каждая компания начнет тыкать пальцем в конкурента. В лучшем случае это чревато задержками, пока они придут к соглашению.

Использование в одной сети коммутаторов и маршрутизаторов разных брендов – это плохая идея. Вот почему большинство компаний использует и маршрутизаторы, и коммутаторы только компании Cisco. Так проще. И даже если у вас смешанная сетевая среда, эта книга все равно будет вам полезна, чтобы научиться администрировать коммутаторы и маршрутизаторы Cisco. Просто напомню, что в этой книге описывается сеть Cisco, и это *всегда* маршрутизаторы и коммутаторы компании Cisco.

На рис. 2.1 показано, как мой компьютер пересылает «конверт», содержащий некоторые данные, на сервер базы данных. В этой главе вы узнаете, как коммутаторы и маршрутизаторы определяют наилучший путь для передачи данных.

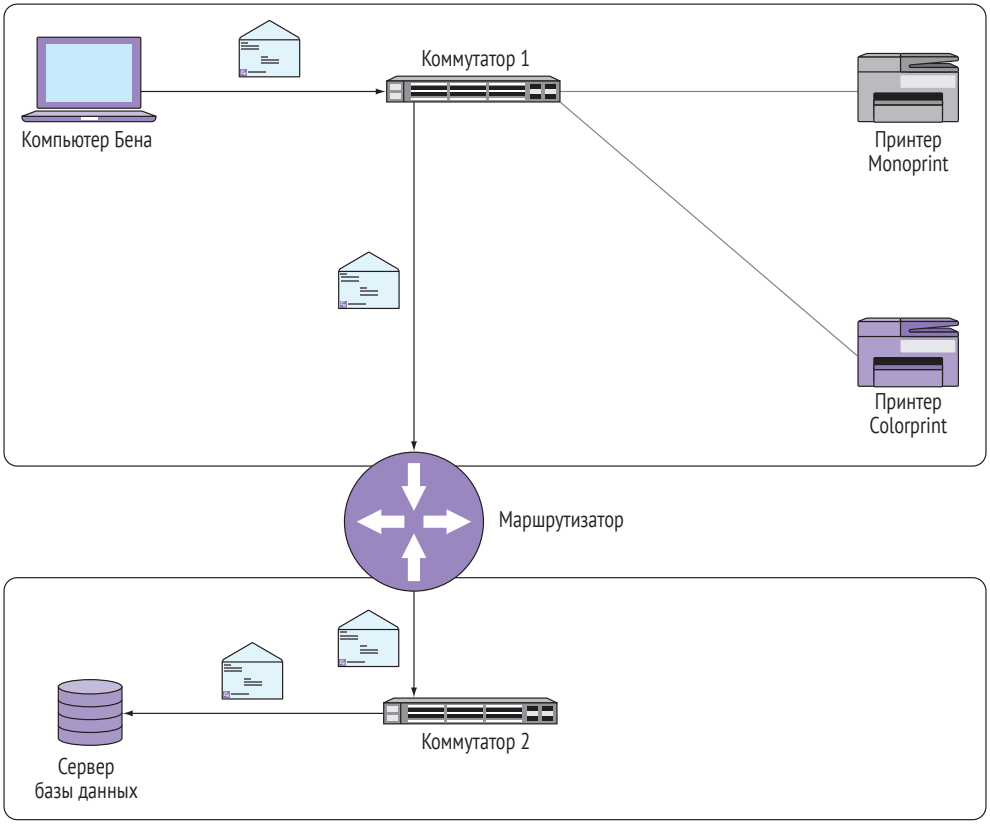

Рис. 2.1 ❖ Коммутаторы и маршрутизатор в сети

2.1. Правда о коммутаторах и маршрутизаторах

Новички часто задают два вопроса:

- что на самом деле делают коммутаторы и маршрутизаторы?
- почему эти устройства имеют и MAC- и IP-адреса?

Эти, казалось бы, простые вопросы не имеют простых ответов. Я неоднократно наблюдал попытки дать ответ на эти вопросы в нескольких предложениях, но все эти попытки вносили лишь больше сумятицы и еще больше запутывали.

Истина в том, что и коммутаторы, и маршрутизаторы – это порождение конкретной технологической необходимости, а не каких-либо общих практических надобностей. В принципе, ни один из этих приборов не наделен какой-то особенной интеллектуальностью, хотя Cisco и снабжает их некоторым количеством «мозгов», чтобы улучшить их функциональность. Как и большинство

технологий, коммутаторы и маршрутизаторы появились как результат сомнительных решений, принятых десятилетия назад.

Новые технологии обычно строятся на более ранних. Например, электронные книги позаимствовали концепции *страниц* и *закладок* у традиционных печатных книг. Попробуйте объяснить, что такое страница, кому-нибудь, кто знаком с прокруткой, но никогда не видел традиционных печатных книг. Как вы это сделаете? Прежде чем объяснять, что такое страница, надо объяснить, зачем они существуют.

Поэтому, прежде чем объяснять, что такое маршрутизатор или коммутатор, я должен коротко пояснить, для решения каких проблем они служат. После того как вы это поймете, все встанет на свои места, и вы сразу же сможете администрировать собственную сеть Cisco.

2.2. MAC-адрес

Много лет назад кто-то решил, что все сетевые приборы должны иметь определенный идентификатор, чтобы идентифицировать друг друга в сетевом пространстве, и назвал этот идентификатор MAC-адресом (от англ. Media Access Control – управление доступом к среде). MAC-адрес – это строка длиной 48 бит, содержащая шестнадцатеричное число, примерно вот так: `0800.2700.EC26`. Вероятно, вы уже встречались с чем-то подобным.

Что интересно: производители сетевых устройств присваивают им MAC-адреса еще на стадии изготовления. Целесообразность этого состоит в том, что можно просто включить устройства в сеть и коммутировать их между собой, не имея никакого руководства по конфигурации. Звучит достойно, но есть одна проблема: производитель присваивает MAC-адрес в отсутствие связи с тем, куда именно будет помещено устройство в конечном итоге. То есть это не совсем адрес, поскольку он совершенно не помогает в определении месторасположения устройства.

Практикум

Запустите оболочку командной строки Windows и введите команду `ipconfig /all`. В появившемся списке MAC-адрес сетевой карты вашего компьютера будет указан в строке **Физический адрес** (Physical Address). Если установлено несколько сетевых карт, вы увидите несколько MAC-адресов.

MAC-адрес сродни полному имени человека. Его присваивают при рождении для простой идентификации, чтобы выделить человека из толпы или послать сообщение на его имя. Если мы с вами находимся в толпе людей и вы хотите послать мне сообщение, но понятия не имеете, где я, вы можете, набрав побольше воздуха, крикнуть: «Бен Пайпер, где ты?» И если я в той толпе, то получу ваше сообщение.

Сетевые устройства общаются друг с другом таким же образом, но вместо полного имени используют MAC-адреса. Предположим, мой компьютер имеет MAC-адрес `0800.2700.EC26`, и его надо напечатать на сетевом принтере с именем Monoprint и MAC-адресом `0020.3500.CE26`. Мой компьютер физически соединен с принтером через устройство, называемое коммутатором, как показано на рис. 2.2. Точнее, мой компьютер и принтер *физически* присоединены к отдельным Ethernet-портам коммутатора. Отметим, что, в отличие от беспроводной точки доступа, подключение к коммутатору *всегда* производится с помощью кабеля. Таким образом, коммутатор – это место сбора всех сетевых устройств. Подобно тому, как я с вами и с другими могу собраться на переполненном рынке, сетевые устройства собираются вместе в коммутаторе. Такой набор соединенных между собой устройств называется локальной вычислительной сетью (ЛВС, от англ. Local area network, LAN).

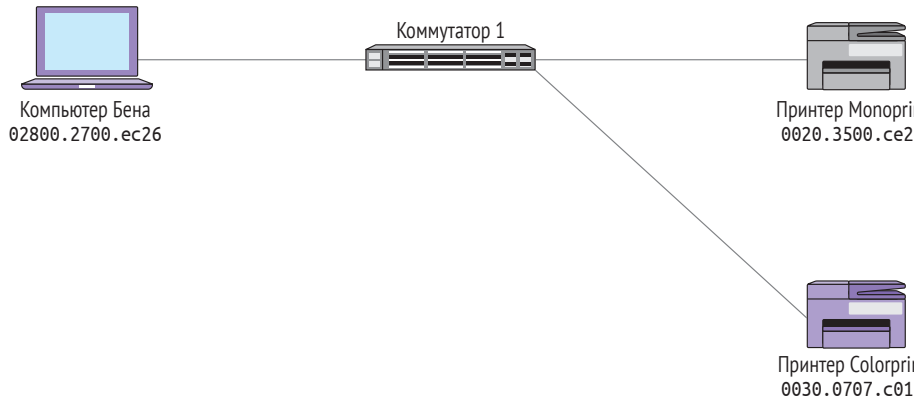

Рис. 2.2 ❖ Два принтера соединены с компьютером через коммутатор

Но здесь возникает проблема: мой компьютер не знает, где расположен принтер Monoprint, не знает даже, является ли он частью локальной сети – частью «толпы», подключенной к коммутатору. *MAC-адрес, подобно полному имени, может служить хорошим идентификатором, но он не может указать точного месторасположения устройства.* Именно поэтому мой компьютер вынужден просто «кричать в рупор», вызывая Monoprint по его MAC-адресу.

Дополнительно

Каждое устройство в процессе изготовления получает заводской уникальный идентификатор (organizationally unique identifier, OUI) в виде строки, содержащей шестнадцатеричное число. Идентификатор OUI образует левую часть MAC-адреса,

присваиваемого при изготовлении. Его можно рассматривать как «фамилию» прибора. Хотя они и присваиваются при «рождении», устройства одной серии имеют идентичный номер QUI. Остальная часть MAC-адреса – это просто следующий член возрастающей последовательности. Таким образом, производитель достигает уникальности MAC-адреса каждого устройства.

2.3. Ethernet-кадр: большой конверт

Мой компьютер создает *Ethernet-кадр*, содержащий указания на источник – его собственный MAC-адрес – и конечный адресат – MAC-адрес принтера. Рисунок 2.3 демонстрирует Ethernet-кадр в виде большого конверта с адресами отправителя и получателя.

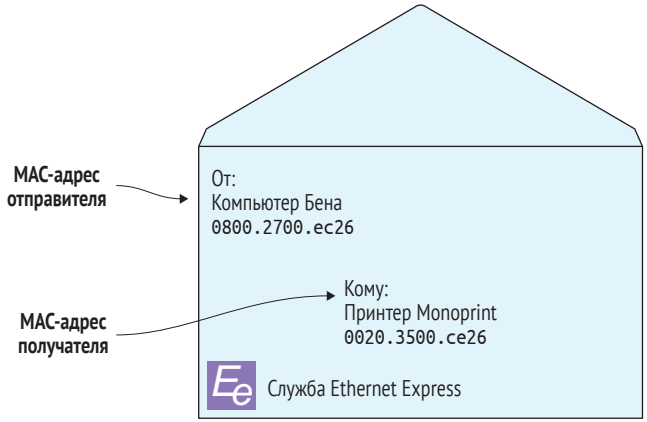

Рис. 2.3 ❖ Ethernet-кадр содержит MAC-адреса отправителя и получателя

Мой компьютер собирает данные, которые хочет обработать на принтере, помещает их в «большой конверт» и отправляет на коммутатор. Коммутатор получает кадр и обращается к MAC-адресу удаленного принтера. Изначально коммутатор не знает, подключен к нему принтер или нет, поэтому он рассылает кадр всем остальным подключенным сетевым устройствам для определения, есть ли среди них принтер. Это называется *лавинной передачей*.

На шаге 1, на рис. 2.4, мой компьютер отправляет Ethernet-кадр, адресованный принтеру Monoprint, со своим MAC-адресом (`0020.3500.ce26`). На шаге 2 коммутатор рассылает этот кадр всем подключенным устройствам.

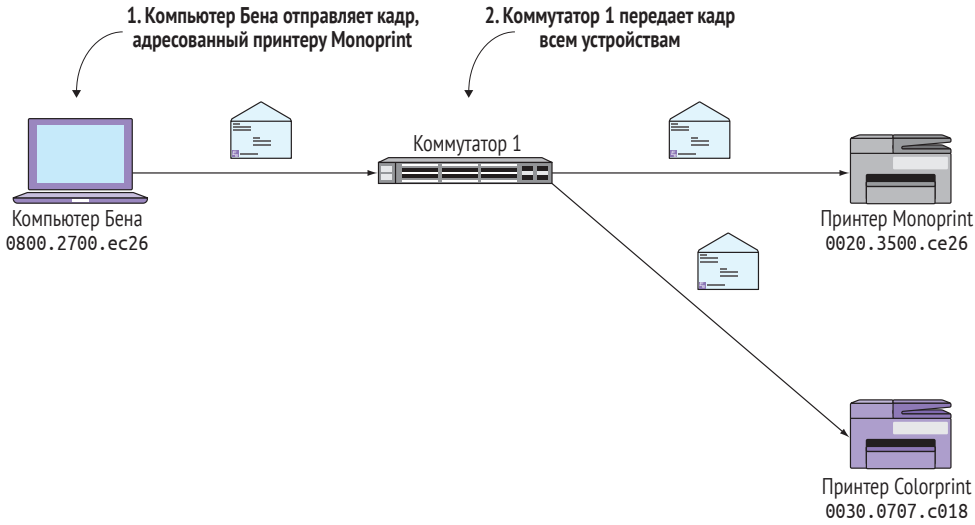

Рис. 2.4 ❖ Лавинная передача Ethernet-кадра

2.3.1. Когда все говорят, никто не слушает

Лавинная передача имеет тот же эффект, что и крик в рупор в большой толпе. Все слышат вас, но в то же время в толпе люди не могут расслышать друг друга. Для увеличения эффективности вы временно прекращаете их общение. Но даже после того, как вы прокричали в рупор, пройдет какое-то время, после того как люди получат ваше сообщение и поймут, что оно адресовано не им. То же самое происходит, когда коммутатор рассылает сообщение всем устройствам. Все они не в состоянии слышать друг друга, пока идет лавинная передача. А затем они должны обработать сообщение, чтобы понять – должны ли они что-то сделать в соответствии с ним. Это явление называется *прерыванием*.

Хотя несколько рассылок кадров и прерываний и не представляется чем-то значительным, представьте, что произойдет в толпе, скажем человек на 1000, в которой у каждого есть рупор. Как раз в тот момент, как вы собрались отправить мне сообщение через свой рупор, кто-то прямо рядом с вами кричит что-нибудь еще через свой. После того как у вас утихнет звон в ушах, вы поднимаете свой рупор только для того, чтобы опять быть прерванным кем-нибудь еще. Пока, наконец, не произойдет пауза, достаточная для пересылки сообщения. Да, это проблема. Вы действуете со всеми остальными в одной среде – в воздухе. При таком методе коммуникации «один – многим» трудно ожидать, что конкретная персона получит сообщение вовремя. И чем больше толпа, тем больше проблем.

В сети с несколькими устройствами лавинная передача не представляет проблем. А если в локальной сети сотни или тысячи устройств, то это проблематично. И это порождает другую проблему. Сеть, которая не может связать тысячи устройств, практически бесполезна.

2.4. Широковещательные домены

Предположим, что вы добавили в топологию сети еще один коммутатор, назвали его Коммутатор 2 и присоединили к нему сервер базы данных, как показано на рис. 2.5. Когда мой компьютер отправляет кадр на MAC-адрес сервера, Коммутатор 1 начинает лавинную передачу (и прерывание) на все устройства, присоединенные к его портам, включая и Коммутатор 2! Коммутатор 2, в свою очередь, тоже передает кадр всем устройствам. В этом случае сервер базы данных – всего лишь рядовое устройство, присоединенное к Коммутатору 2.

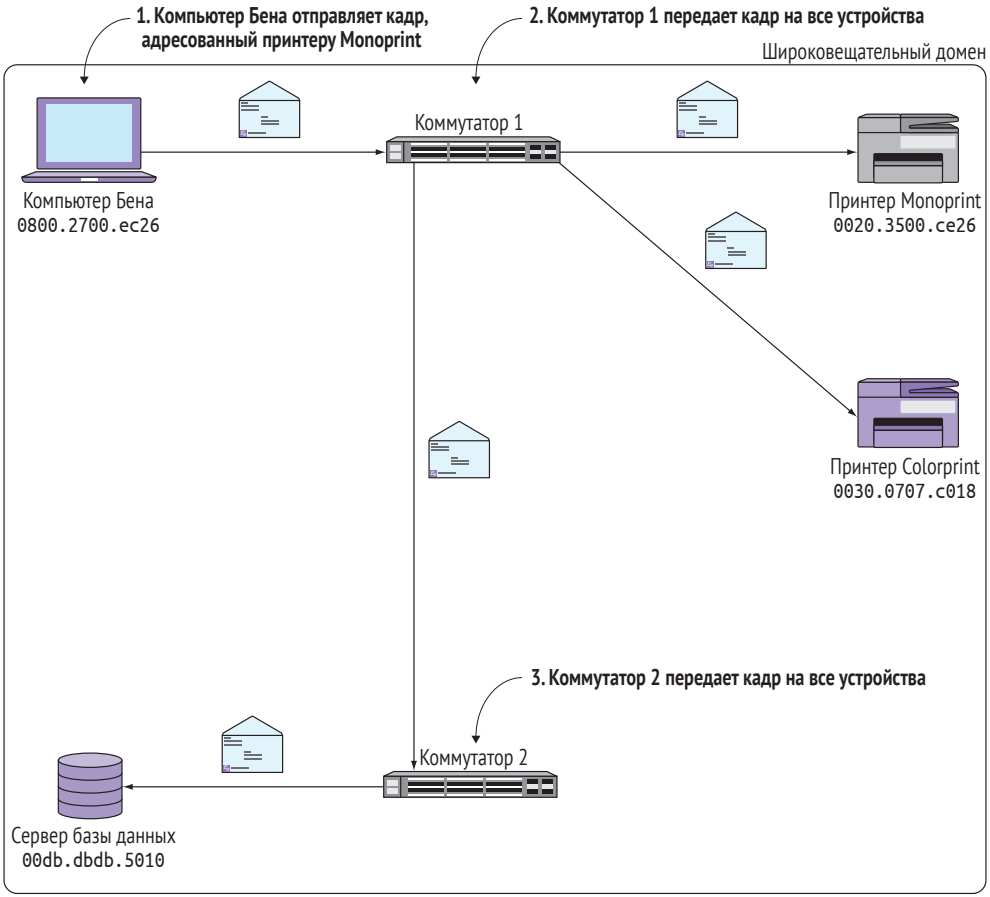

Рис. 2.5 ❖ Коммутатор 2 расширяет широковещательный домен

В шаге 1 мой компьютер пересылает кадр на MAC-адрес сервера базы данных (`00db.dbdb.5010`). В шаге 2 Коммутатор 1 рассылает кадр всем устройствам. И наконец, в шаге 3 Коммутатор 2 передает кадр на сервер базы данных.

Все эти устройства, которые получили кадр, – члены одного *широковещательного домена*. Широковещательный домен – это не устройство и даже не настраиваемый параметр, а скорее неотъемлемый атрибут сети. Для лучшего понимания представлю следующую аналогию.

Когда вы стоите один в центре улицы, вы – не толпа. Но если несколько человек собирается вокруг вас, вы становитесь частью толпы. И вы становитесь частью еще большей толпы, когда вокруг вас собирается больше людей. Вы не меняетесь, но меняется ваше виртуальное свойство – часть толпы, – в зависимости от того, сколько людей собралось вокруг вас. Точно так же и устройство становится частью широковещательного домена тех устройств, которые получили кадр при лавинной передаче.

2.4.1. Избавление от лавинной передачи: таблица MAC-адресов

Лавинная передача – неизбежная операция при использовании MAC-адресов. К счастью, коммутаторы используют ловкий трюк, чтобы уменьшить необходимость лавинной передачи. Каждый раз, когда коммутатор получает кадр, он изучает MAC-адрес источника и порт, к которому присоединен источник кадра. Эта информация используется для построения *таблицы MAC-адресов*.

Дополнительно

В документации Cisco таблица MAC-адресов иногда называется ассоциативной памятью (content addressable memory, CAM), но это одно и то же.

Когда Коммутатор 1 получает кадр от моего компьютера, он записывает его MAC-адрес `0800.2700.ac26`, а также порт, к которому компьютер подключен, – FastEthernet0/1. Эта информация добавляется в таблицу MAC-адресов, как показано в табл. 2.1.

Таблица 2.1. Таблица MAC-адресов Коммутатора 1

Устройство	MAC-адрес	Порт коммутатора
Компьютер Бена	`0800.2700.ec26`	FastEthernet0/1

Теперь предположим, сервер базы данных отправляет кадр с MAC-адресом моего компьютера. Кадр попадает на Коммутатор 2, который отправляет его прямиком на Коммутатор 1. Но вместо слепого забрасывания кадром всех устройств Коммутатор 1 проверяет таблицу MAC-адресов.

Он видит, что MAC-адрес `0800.2700.ec26` соответствует устройству, подключенному к порту FastEthernet0/1, и отправляет кадр *только* на этот порт, как показано на рис. 2.6. Это работает по принципу старого телефонного коммутатора, откуда и происходит термин *коммутатор*.

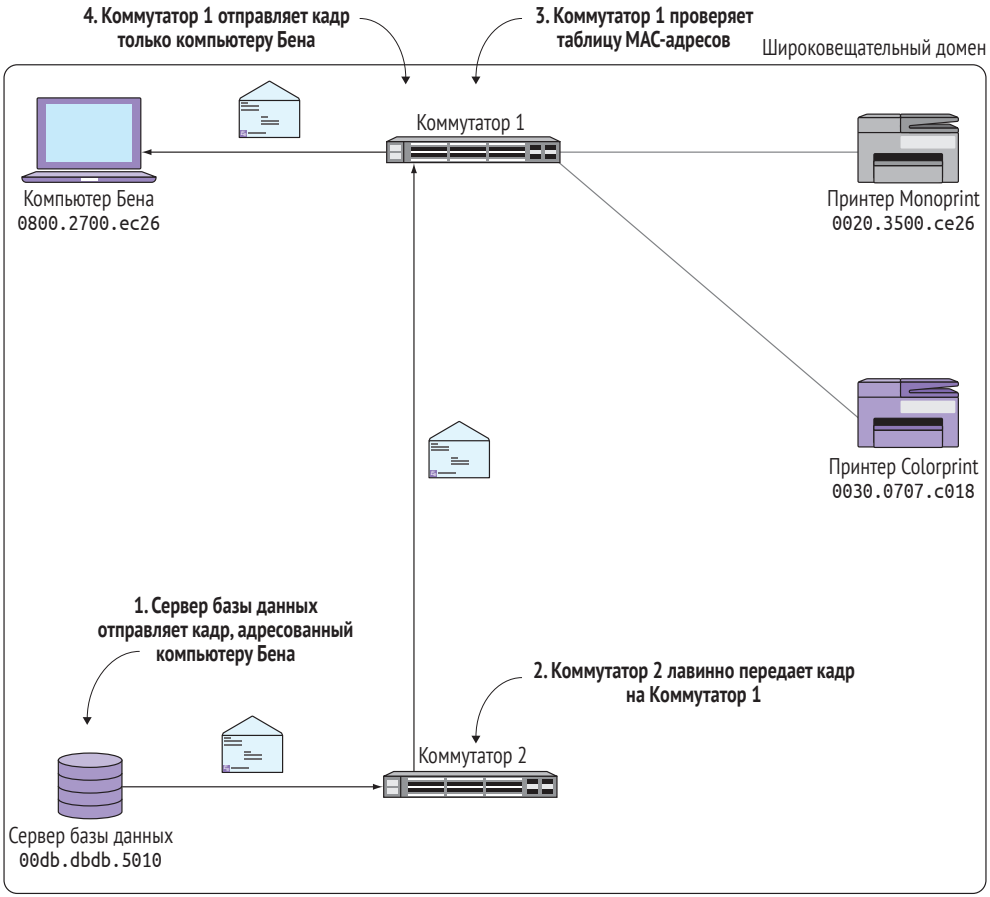

Рис. 2.6 ❖ Как таблица MAC-адресов позволяет избавиться от лавинной передачи

На шаге 1 сервер базы данных отправляет кадр на MAC-адрес моего компьютера (`0800.2700.ec26`). На шаге 2 Коммутатор 2 (лавинно) отправляет кадр на Коммутатор 1. На шаге 3 Коммутатор 1 сверяется с таблицей MAC-адресов и находит порт запрашиваемого адреса. На шаге 4 Коммутатор 1 отправляет кадр только на порт моего компьютера, а не лавинно передает кадр на все остальные устройства.

2.4.2. Разделение широковещательного домена

С ростом размера широковещательного домена коммуникации становятся все более затруднительными. И как следствие, широковещательный домен, состоящий из сотен устройств, начинает работать неудовлетворительно. Но современной компании требуется сеть, соединяющая тысячи устройств. И просто наличия связи недостаточно. Сеть должна быть быстрой и надежной.

Решение заключается в ограничении размера широковещательного домена. Это значит, что его нужно разбить на части таким образом, чтобы отдельные части имели связь друг с другом.

Возвращаясь к нашему примеру, мы видим, что простейший путь разбить широковещательный домен – это отключить Ethernet-кабель, соединяющий Коммутаторы 1 и 2, как показано на рис. 2.7. Отмечу, что коммутаторы не соединяются каким-либо иным способом. Это простая часть. А теперь сложная: мой компьютер и сервер базы данных размещены на разных широковещательных доменах. Не существует путей для их связи друг с другом. Что вы натворили? Вы не можете просто заново соединить коммутаторы, потому что воссоздадите то, что было, – единый широковещательный домен.

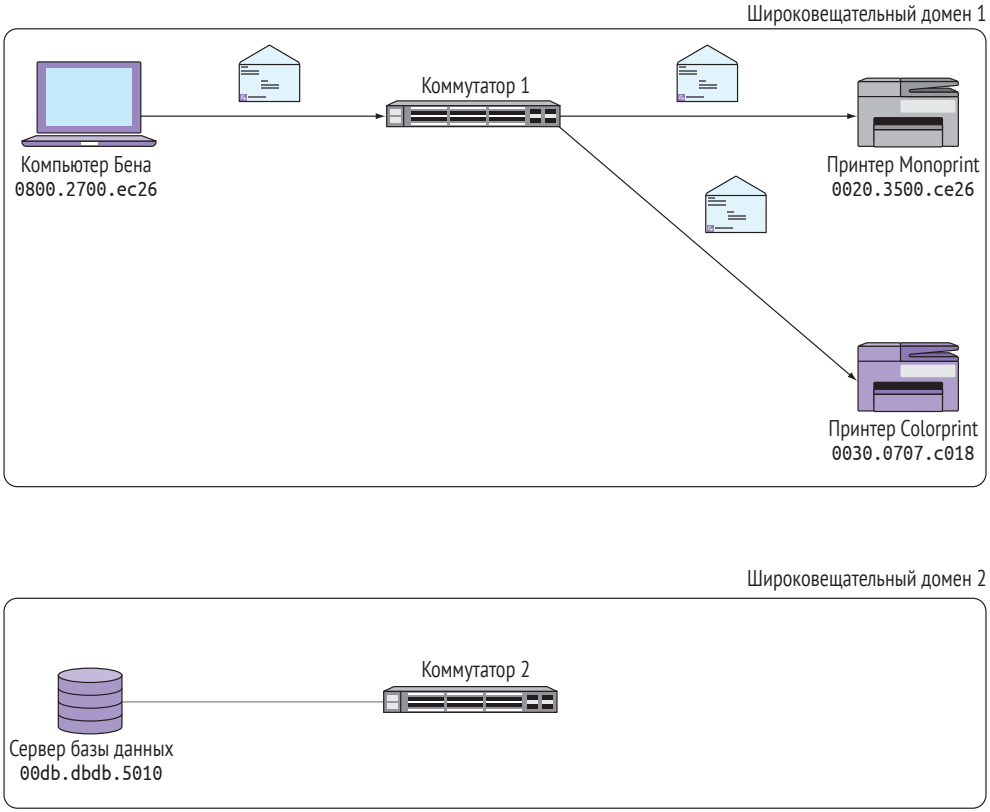

Рис. 2.7 ❖ Два широковещательных домена

2.4.3. Соединение широковещательных доменов

Для соединения двух широковещательных доменов без повторения этой ужасной проблемы лавинной передачи необходимо сделать две вещи.

Во-первых, так как два широковещательных домена не имеют связи, вам нужно специальное устройство, физически соединяющее их, но таким образом, чтобы рассылка кадров не выходила за границы широковещательного домена. Так как кадр содержит MAC-адреса и отправителя, и адресата, это устройство будет эффективно скрывать MAC-адреса одного широковещательного домена от другого.

Во-вторых, так как MAC-адреса одного широковещательного домена скрыты от другого, вам нужна другая схема адресации устройств для обращения к оборудованию в разделенных доменах. Новая адресная схема, в отличие от MAC-адресов, должна не только идентифицировать прибор, но и предоставлять какие-то указания на то, в каком домене прибор размещен. Давайте начнем с последнего.

2.4.4. Адресация устройств из разных широковещательных доменов

Схема адресации должна удовлетворять следующим требованиям:

- во-первых, адрес должен быть уникальным для всех широковещательных доменов. Два устройства из одного домена не могут иметь одинаковый адрес;
- во-вторых, адрес должен сообщать, какому домену он принадлежит. *Адрес должен быть не только уникальным идентификатором прибора, но также и сообщать другим устройствам, к какому домену он принадлежит.* Все это для того, чтобы избежать этих ужасных проблем лавинной передачи;
- в-третьих, адреса не могут присваиваться «при рождении», подобно MAC-адресу. Они должны конфигурироваться вами как сетевым администратором.

К счастью, вам нет необходимости ломать над этим голову. Такая адресная схема существует, и вы уже пользовались ею.

2.5. Адреса протокола Интернета

Вы уже знаете, как выглядят IP-адреса. Один из самых распространенных IP-адресов – `192.168.1.1`. Это последовательность четырех восьмеричных чисел (*октетов*), разделенных точкой, каждое число может располагаться в диапазоне от `0` до `255`.

Вы, вероятно, видели адреса типа `192.168.`*`x`*`.`*`x`*, всплывающие в различных местах. Это связано с тем, что адреса `192.168.`*`x`*`.`*`x`* зарезервированы для использования в частных сетях, используемых у вас дома или на работе. Они глобально не уникальны, так как не доступны в общем пространстве Интернета. Но вы можете их использовать для адресации устройств в своей собственной внутренней сети.

В отличие от MAC-адресов, вы можете присваивать IP-адрес любому устройству, какому захотите. Вы можете создать собственную схему адресации, основанную на месторасположении прибора, а не просто на том, что они есть. Давайте рассмотрим пример.