



В этой главе...

- **Базовые концепции коммутации.** В этом разделе объяснены основные процессы, связанные с коммутацией в локальных сетях.
- **Основы дизайна локальных сетей.** В этом разделе описана терминология и методы построения корректно работающих локальных сетей.

Базовые концепции Ethernet-коммутации

В главе 3 “Основы локальных сетей” были достаточно подробно рассмотрены основные концепции и атрибуты технологии Ethernet для локальных сетей. В ней были описаны как основы технологии, так и кабельная система на основе UTP-кабеля, принципы работы концентраторов и коммутаторов, а также было приведено сравнение различных стандартов Ethernet, описаны механизмы передачи на канальном уровне, адресация и фреймирование.

Во этой части продолжено описание локальных сетей (LAN) на основе технологии Ethernet, а в главе 11 описаны беспроводные сети. В текущей главе подробно объяснены темы, оставшиеся за рамками предыдущих глав, например, главы 3 “Основы локальных сетей”. В частности, в текущей главе намного более детально описаны принципы работы коммутаторов, методы построения сетей с использованием концентраторов, мостов, коммутаторов и маршрутизаторов. В главах 8–10 рассказано, как подключиться к коммутаторам компании Cisco и как их настроить. В главе 8 “Работа с коммутаторами компании Cisco” подробно описан интерфейс командной строки пользователя, в главе 9 “Конфигурирование Ethernet-коммутаторов” рассмотрена базовая конфигурация коммутаторов, а в главе 10 “Поиск и устранение неисправностей в Ethernet-коммутаторах” рассказано, как проверять сеть и устранять неисправности в коммутаторах компании Cisco. В главе 11 “Беспроводные локальные сети”, завершающей вторую часть первого тома книги, описаны основные концепции беспроводных локальных сетей.

Контрольные вопросы: знаете ли вы уже темы главы

Этот раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на девять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 7.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно определить свои знания в той или иной области. Ответы на вопросы приведены в приложении А “Ответы на контрольные вопросы”.

Таблица 7.1. Темы контрольных вопросов

Основная тема	Номера вопросов
Концепции коммутации в локальных сетях	1–5
Принципы построения локальных сетей	6–8

1. Какое из утверждений правильно описывает принимаемое коммутатором решение об отправке фрейма для известного ему одноадресатного (unicast) MAC-адреса получателя?
 - а) Коммутатор сравнивает адрес получателя с таблицей коммутации (т.е. таблицей MAC-адресов).
 - б) Коммутатор сравнивает адрес отправителя с таблицей коммутации (т.е. таблицей MAC-адресов).
 - в) Устройство рассылает фрейм через все интерфейсы в данной сети VLAN, кроме того, через который он был получен.
 - г) Коммутатор сравнивает IP-адрес получателя с MAC-адресом получателя.
 - д) Устройство сравнивает идентификатор входного интерфейса с MAC-адресом отправителя в таблице MAC-адресов.
2. Какое из утверждений правильно описывает принимаемое коммутатором решение об отправке фрейма для широковещательного (broadcast) MAC-адреса получателя?
 - а) Коммутатор сравнивает адрес получателя с таблицей коммутации (т.е. таблицей MAC-адресов).
 - б) Коммутатор сравнивает адрес отправителя с таблицей коммутации (т.е. таблицей MAC-адресов).
 - в) Устройство рассылает фрейм через все интерфейсы в данной сети VLAN, кроме того, через который он был получен.
 - г) Коммутатор сравнивает IP-адрес получателя с MAC-адресом получателя.
 - д) Устройство сравнивает идентификатор входного интерфейса с MAC-адресом отправителя в таблице MAC-адресов.
3. Какое из утверждений правильно описывает принимаемое коммутатором решение об отправке фрейма для неизвестного ему одноадресатного (unicast) MAC-адреса получателя?
 - а) Устройство рассылает фрейм через все интерфейсы в данной сети VLAN, кроме того, через который он был получен.
 - б) Устройство пересылает фрейм через один интерфейс, для которого есть соответствующая запись в таблице MAC-адресов.
 - в) Коммутатор сравнивает IP-адрес получателя с MAC-адресом получателя.
 - г) Устройство сравнивает идентификатор входного интерфейса с MAC-адресом отправителя в таблице MAC-адресов.
4. Какие действия выполняет коммутатор, если ему нужно принять решение о том, добавлять или нет новый MAC-адрес в таблицу коммутации?

- а) Устройство сравнивает одноадресатный адрес получателя с записями в таблице коммутации (MAC-адресов).
 - б) Устройство сравнивает одноадресатный адрес отправителя с записями в таблице коммутации (MAC-адресов).
 - в) Устройство сравнивает идентификатор сети VLAN (ID) с записями в таблице коммутации (MAC-адресов).
 - г) Устройство сравнивает IP-адрес получателя из записи в ARP-кэше с записями в таблице коммутации (MAC-адресов).
5. Персональный компьютер ПК1 с MAC-адресом 1111.1111.1111 подключен к интерфейсу Fa0/1 коммутатора SW1. Компьютер ПК2 с MAC-адресом 2222.2222.2222 подключен к интерфейсу Fa0/2 коммутатора SW1, а компьютер ПК3 с MAC-адресом 2222.2222.2222 подключен к интерфейсу Fa0/3 того же коммутатора. Изначально в таблице коммутатора нет никаких динамических записей о MAC-адресах. ПК1 пересылает фрейм с адресом получателя 2222.2222.2222. Если после этого ПК3 пересылает фрейм компьютеру ПК2 с адресом получателя 2222.2222.2222, что будет происходить в коммутаторе?
- а) Коммутатор перешлет фрейм через интерфейс Fa0/1.
 - б) Коммутатор перешлет фрейм через интерфейс Fa0/2.
 - в) Коммутатор перешлет фрейм через интерфейс Fa0/3.
 - г) Коммутатор отбросит (или отфильтрует) такой фрейм.
6. В каком случае два компьютера будут в одном и том же домене коллизий?
- а) Если компьютеры разделены Ethernet-концентратором.
 - б) Если компьютеры разделены прозрачным мостом.
 - в) Если компьютеры разделены Ethernet-коммутатором.
 - г) Если компьютеры разделены маршрутизатором.
7. В каком случае два компьютера будут в одном и том же широковещательном домене?
- а) Если компьютеры разделены Ethernet-концентратором.
 - б) Если компьютеры разделены прозрачным мостом.
 - в) Если компьютеры разделены Ethernet-коммутатором.
 - г) Если компьютеры разделены маршрутизатором.
8. В каком из Ethernet-стандартов максимальная длина кабеля не может превышать 100 м?
- а) 100BASE-TX.
 - б) 1000BASE-LX.
 - в) 1000BASE-T.
 - г) 100BASE-FX.

Введение

Эта глава начинается с описания концепций локальных сетей (Local Area Network — LAN), в частности подробного описания процесса передачи Ethernet-фреймов коммутаторами. В середине главы подробно рассмотрены основные принципы дизайна сетей и приведена соответствующая терминология. В текущей главе также представлен небольшой обзор оптоволоконных вариантов технологии Ethernet, позволяющей реализовывать сегменты большей длины, чем UTP-среда.

Базовые концепции коммутации

В главе 3 “Основы локальных сетей” была подробно описана технология Ethernet, а также принцип работы коммутаторов и концентраторов локальных сетей. Чтобы разобраться в принципах работы LAN-коммутаторов, следует хорошо разбираться в принципах более старых устройств: концентраторов (hub) и мостов (bridge). В первой части этого раздела рассказано, зачем вообще были разработаны коммутаторы, а во второй описаны три их основные функции и некоторые другие детали устройств.

Развитие сетевых устройств: концентраторы, мосты и коммутаторы

Как было рассказано выше, в главе 3, первым вариантом технологии Ethernet была физическая шинная топология на основе коаксиального кабеля. Следующим распространенным вариантом технологии был стандарт 10BASE-T, надежность которого была значительно выше за счет того, что проблемы в одном кабеле не влияли на всю сеть (характерная ситуация для сетей 10BASE2 и 10BASE5 с топологией разделяемой шины). В технологии 10BASE-T использовалась неэкранированная витая пара (unshielded twisted-pair — UTP), которая значительно дешевле, чем коаксиальный кабель. Кроме того, во многих организациях витая пара использовалась для телефонии, поэтому стандарт 10BASE-T очень быстро стал разумной альтернативой Ethernet-сетям стандартов 10BASE2 и 10BASE5. Типичные топологии для сети стандарта 10BASE2 и сети 10BASE-T с использованием концентратора показаны на рис. 7.1.

Несмотря на то, что технология 10BASE-T была заметным шагом вперед в развитии сетевых технологий, у нее все же было несколько существенных недостатков, связанных с использованием концентраторов:

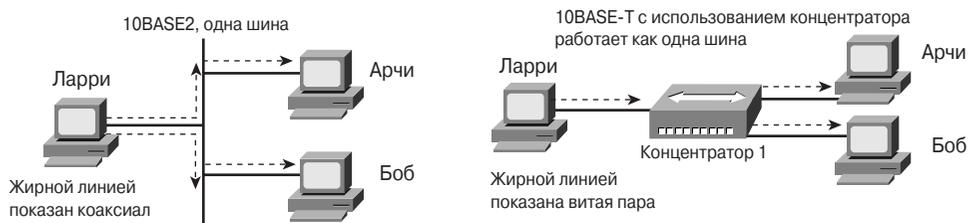


Рис. 7.1. Физические топологии для сети 10BASE2 и сети 10BASE-T с использованием концентратора

- фрейм, пересылаемый любым устройством, может послужить причиной коллизии в сети, если он “столкнется” с фреймом от другого устройства в том же самом сегменте;
- только одно устройство может пересылать фрейм в один момент времени, т.е. устройства в сегменте работают в режиме конкуренции и разделяют общую полосу пропускания (в 10 Мбит/с);
- широковещательные фреймы, отправляемые одним устройством, будут получены и обработаны всеми устройствами в локальной сети.

Когда три указанных выше стандарта Ethernet были разработаны, разделяемая полоса пропускания в 10 Мбит казалась просто огромной величиной! До того как появились локальные сети (LAN), для работы зачастую использовались упрощенные терминалы, подключенные через канал в 56 Кбит/с к центральному серверу в сети, и множество таких терминалов использовали эту полосу пропускания (всего 56 Кбит/с!) в режиме разделения. Когда появилась технология 10BASE-T Ethernet, ее скорость была просто невероятной для того времени, например, как если бы вы из дому в сеть Интернет подключались через модем, а потом вдруг стали использовать гигабитовое подключение. Поэтому инженерам и пользователям казалось, что такая высокая скорость никогда не понадобится.

С течением времени производительность Ethernet-сетей стала заметно ухудшаться. Производители программного обеспечения стали разрабатывать приложения, использующие большую полосу пропускания в локальной сети. В сетях появилось намного больше устройств, чем было изначально. В локальных сетях стали появляться заторы трафика, поскольку устройства в одном и том же сегменте Ethernet не могут пересылать больше чем 10 Мбит/с потоков данных, кроме того они разделяют эту полосу пропускания между собой. Увеличение объемов трафика привело к росту числа коллизий в локальных сетях. Фактически задолго до того, как нагрузка Ethernet-сетей достигла 10 Мбит/с, в ней появились проблемы из-за большого числа коллизий.

Чтобы решить проблемы с производительностью сети, были разработаны мосты. Они решали проблемы заторов в Ethernet-сетях двумя методами:

- уменьшали количество коллизий в сети;
- увеличивали в сегменте доступную полосу пропускания.

Структура сети с использованием прозрачного моста (transparent bridge) проиллюстрирована на рис. 7.2. В верхней части рисунка показана сеть 10BASE-T без использования моста, а в нижней — *сегментированная* с помощью прозрачного моста. Такой мост создает два *домена коллизий*, поскольку фреймы от компьютера Фреда могут вступать в коллизии с фреймами от компьютера Барни, но не с фреймами от компьютеров Вилмы или Бетти. Если один из сегментов локальной сети перегружен и мост не сможет передать в него фрейм, то он просто буферизирует его (хранит в памяти) до тех пор, пока среда передачи данных не освободится. Несмотря на то, что количество устройств в сети, а также ее загруженность потоками данных не изменилась, уменьшение числа коллизий приводит к заметному увеличению производительности телекоммуникационной инфраструктуры.

За счет установки моста (bridge) между двумя концентраторами (hub) сеть разделяется на две независимые 10BASE-T-сети: одна слева и одна справа. В 10BASE-T-сети слева есть свои собственные разделяемые 10 Мбит/с, аналогично и в сети спра-

ва, поэтому в рассмотренном примере фактически полоса пропускания вырастет почти до 20 Мбит/с по сравнению с сетью, показанной в верхней части рис. 7.2.

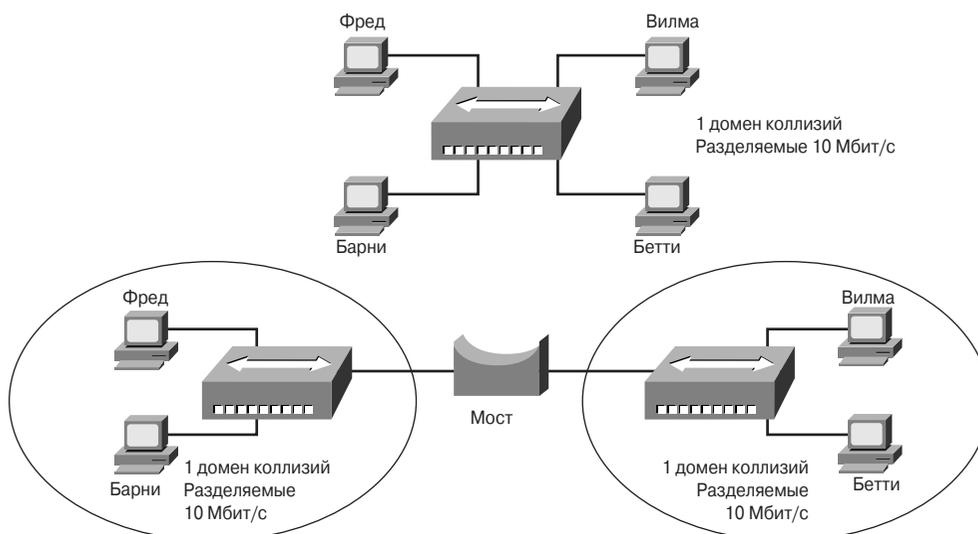


Рис. 7.2. Мост создает два домена коллизий и два разделяемых сегмента Ethernet

Коммутаторы локальных сетей (LAN switches) выполняют те же самые базовые функции, что и мосты, но у них есть множество дополнительных функций. Как и мосты, коммутаторы сегментируют сеть на различные участки, каждый сегмент представляет собой отдельный домен коллизий. В коммутаторах может быть очень большое число интерфейсов, специально оптимизированное аппаратное обеспечение, поэтому даже младшие модели Ethernet-коммутаторов могут коммутировать миллионы фреймов в секунду. За счет того, что коммутаторы создают отдельный домен коллизий для каждого своего интерфейса и виртуальный маршрут для потока данных между двумя портами, они фактически увеличивают скорость передачи данных. Как было рассказано в главе 3 “Основы локальных сетей”, если порт коммутатора подключен к одному какому-либо устройству, в таком Ethernet-сегменте будет использоваться дуплексный режим (full-duplex), поэтому скорость передачи данных удвоится.

ВНИМАНИЕ!

Разбиение домена коллизий коммутатором в локальной сети на меньшие домены для каждого интерфейса называется *микросегментацией* сети.

Рассмотренные выше ключевые концепции проиллюстрированы на рис. 7.3. На нем показаны те же самые рабочие станции, что и на рис. 7.2, но теперь они соединены посредством коммутатора, интерфейсы которого работают со скоростью 100 Мбит/с и создают четыре домена коллизий. Следует также запомнить, что все интерфейсы работают в дуплексном режиме, поскольку только один компьютер включен в каждый порт, а также что в такой структуре сети вообще не будет коллизий.

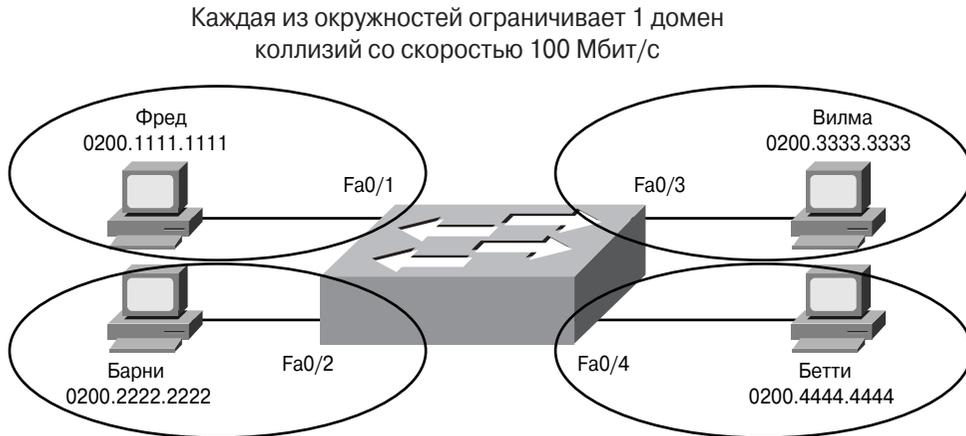


Рис. 7.3. Коммутатор разделяет четыре Ethernet-сегмента и создает четыре домена коллизий

В следующем разделе описан процесс пересылки Ethernet-фреймов коммутаторами.

Принципы коммутации фреймов

Вполне очевидно, что основная задача коммутатора в локальной сети состоит в пересылке Ethernet-фреймов. Для выполнения такой функции устройство использует определенные алгоритмы, основанные на анализе MAC-адресов отправителя и получателя в Ethernet-заголовках фреймов. Чтобы понять, как именно работает коммутатор, сначала следует запомнить основные типы адресов, используемые в современных сетях.

Согласно стандартам Института IEEE MAC-адреса технологии Ethernet можно разделить на три категории:

- **одноадресатные (unicast addresses)**, или те, которые идентифицирует один интерфейс, сетевую плату или порт локальной сети;
- **широковещательные (broadcast addresses)** — фрейм с широковещательным адресом в качестве получателя (FFFF.FFFF.FFFF) должен быть принят и обработан всеми устройствами в сегменте локальной сети (LAN);
- **многоадресатные (multicast addresses)** позволяют одновременно принимать трафик некоторой динамически изменяющейся группы сетевых устройств в локальной сети.

ВНИМАНИЕ!

В протоколе IP поддерживается многоадресатная рассылка пакетов. Когда многоадресатный IP-пакет передается в среде Ethernet, используется специализированный многоадресатный MAC-адрес определенного формата. Адрес выглядит таким образом: 0100.5exx.xxxx, где значение от 00.0000 до 7f.ffff может быть использовано во второй половине адреса вместо символов “x”. Многоадресатные MAC-адреса среды Ethernet выходят за рамки данной книги.

Итак, основная задача любого Ethernet-коммутатора заключается в получении фреймов из локальной сети и последующем принятии решения: следует такой фрейм

переслать через какой-либо порт (порты) или проигнорировать (т.е. отбросить) его. Чтобы выполнить эту задачу, коммутаторы (как, впрочем, и прозрачные мосты) выполняют следующие действия.

1. Принимают решение о том, следует переслать фрейм или отфильтровать (не пересылать) на основании MAC-адреса устройства-получателя.
2. Изучают MAC-адреса и строят таблицу коммутации на основании MAC-адресов устройств-отправителей фреймов.
3. Поддерживают топологию второго уровня без петель с другими коммутаторами за счет использования протокола распределенного связующего дерева (Spanning Tree Protocol — STP).



Первое из указанных выше действий — это основная задача любого коммутатора, два остальных являются второстепенными, но необходимыми. В последующих разделах подробно описаны указанные выше главные функции коммутаторов.

Фильтрация и передача фрейма

Чтобы принять решение о том, следует ли пересылать фрейм, коммутатор использует динамически создаваемую таблицу коммутации, в которой содержатся MAC-адреса и идентификаторы выходных интерфейсов. Коммутатор сравнивает MAC-адрес получателя фрейма с записью в такой таблице, чтобы принять решение о том, следует передать фрейм дальше или проигнорировать его. Например, обратимся к сети, проиллюстрированной на рис. 7.4, и представим, что компьютер Фреда пересылает фрейм компьютеру Барни.

На рис. 7.4 показан как пример принятия решения о пересылке фрейма, так и о фильтрации. Компьютер Фреда пересылает фрейм с MAC-адресом получателя 0200.2222.2222 (т.е. MAC-адресом компьютера Барни); коммутатор сравнивает такой адрес получателя со своей таблицей коммутации, чтобы найти совпадение. Таким образом, в рассматриваемой ситуации будет найден выходной интерфейс, через который можно доставить фрейм получателю с MAC-адресом 0200.2222.2222. Поскольку интерфейс, через который был получен фрейм (Fa0/1), отличается от того, через который он должен быть передан (Fa0/2), устройство принимает решение об отправке фрейма через интерфейс Fa0/2, как показано в таблице на рис. 7.4.

ВНИМАНИЕ!

Таблицу MAC-адресов коммутатора также называют таблицей коммутации (switching table), мостовой таблицей (bridging table), или даже САМ-таблицей (Content Addressable Memory — адресуемая по содержимому память). Последний термин обычно используется, чтобы указать тип памяти, используемой для хранения коммутационной информации.

Чтобы понять, куда коммутатор должен отправить фрейм, нужно уметь просматривать и анализировать его таблицу адресов. В таблице содержится информация об адресах и используемых устройством интерфейсах для отправки пакетов к ним. Например, в таблице записано, что адрес 0200.3333.3333 связан с интерфейсом Fa0/3, следовательно, фрейм для такого получателя будет отправлен именно через этот интерфейс (для компьютера Вилмы).

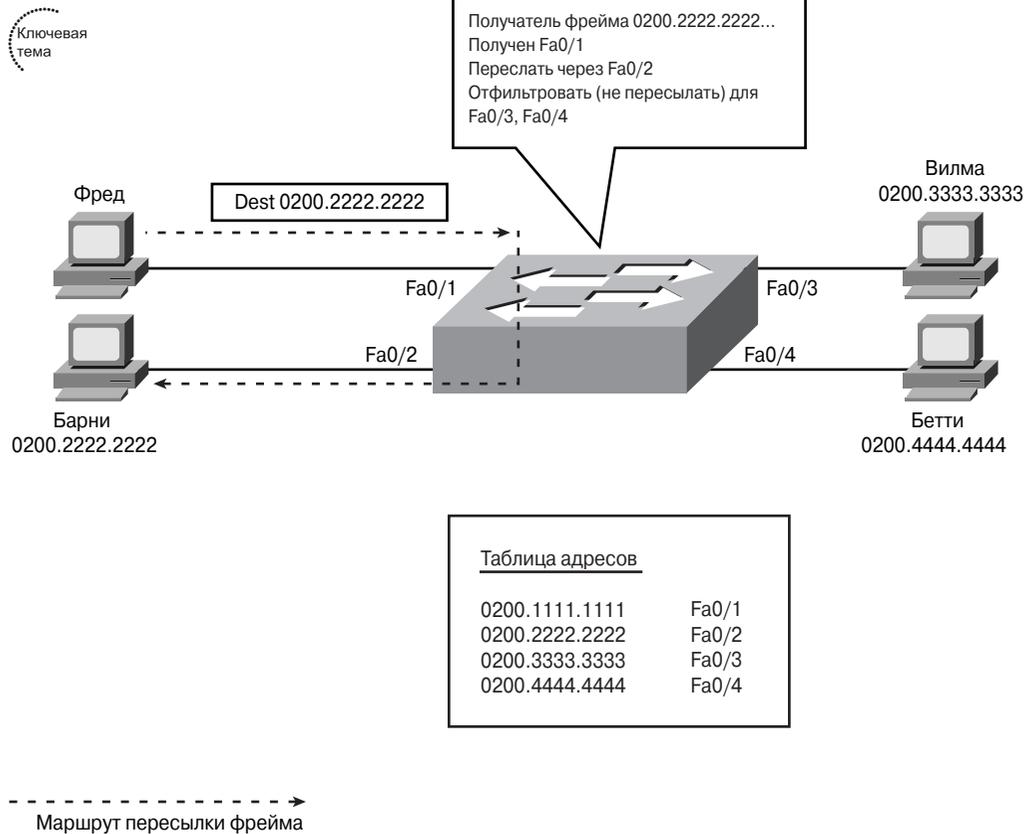


Рис. 7.4. Пример коммутации и фильтрации фреймов

На рис. 7.5 проиллюстрирован другой вариант развития событий — коммутатор отфильтровывает фрейм. В данном случае компьютеры Фреда и Барни подключены к концентратору, который, в свою очередь, подключен к порту коммутатора. В таблице MAC-адресов коммутатора в этом примере будут записи для компьютеров Фреда и Барни, связанные с одним и тем же интерфейсом, Fa0/1, и устройство должно пересылать фреймы с соответствующими идентификаторами получателей через него. Когда коммутатор получает фрейм, отправленный компьютером Фреда (т.е. с MAC-адресом отправителя 0200.1111.1111) и предназначенный компьютеру Барни (т.е. с MAC-адресом получателя 0200.2222.2222), он обнаруживает, что входной и выходной интерфейсы для такого фрейма совпадают, следовательно, пересылать его повторно в тот интерфейс, из которого он был получен, бессмысленно, и фрейм будет отфильтрован (т.е. отброшен) устройством.

Следует помнить, что концентратор просто воспроизводит электрический сигнал на всех выходных интерфейсах, следовательно, биты передаваемого компьютером Фреда фрейма будут попадать как в интерфейс компьютера Барни, так и в порт коммутатора. Коммутатор принимает решение о фильтрации фрейма (т.е. об отбрасывании), потому что MAC-адрес получателя связан с входным интерфейсом для данного фрейма (т.е. с тем же самым портом — выходным интерфейсом для отправителя).

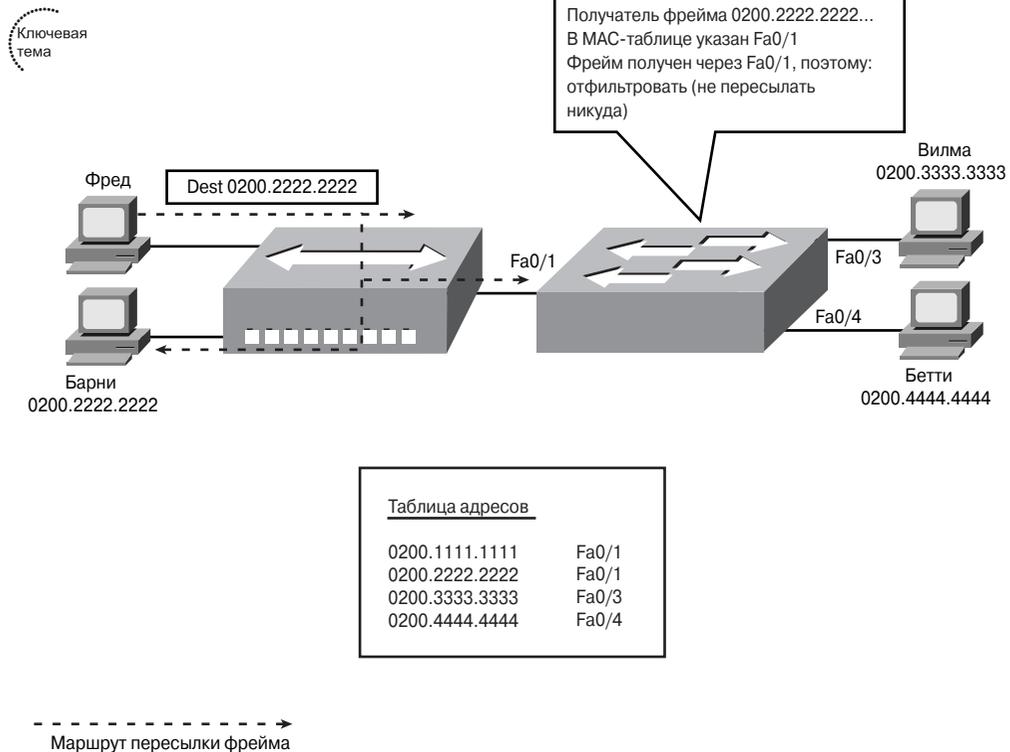


Рис. 7.5. Пример фильтрации фреймов

Как коммутатор находит MAC-адреса

Другой важной функцией коммутатора является механизм обнаружения MAC-адресов и построение таблицы коммутации для них. Если таблица коммутации устройства правильная и точная, коммутатор будет принимать правильные и точные решения об отправке или фильтрации фреймов.

Коммутаторы строят таблицу адресов, просматривая входящие фреймы и записывая из них *MAC-адреса получателей*. Если на вход какого-либо порта устройства получен фрейм и MAC-адрес в поле отправителя фрейма отсутствует в таблице коммутации, коммутатор создает соответствующую ему запись в таблице. В таблицу помещается адрес и идентификатор интерфейса, через который был получен фрейм.

На рис. 7.6 показана сеть, подобная представленной на рис. 7.4, но в этом примере коммутатор еще не построил себе таблицу коммутации, она пустая. В рассматриваемом на рис. 7.6 случае показаны два начальных фрейма коммуникации между двумя устройствами, первый фрейм пересылает компьютер Фреда компьютеру Барни, второй представляет собой ответ от компьютера Барни.

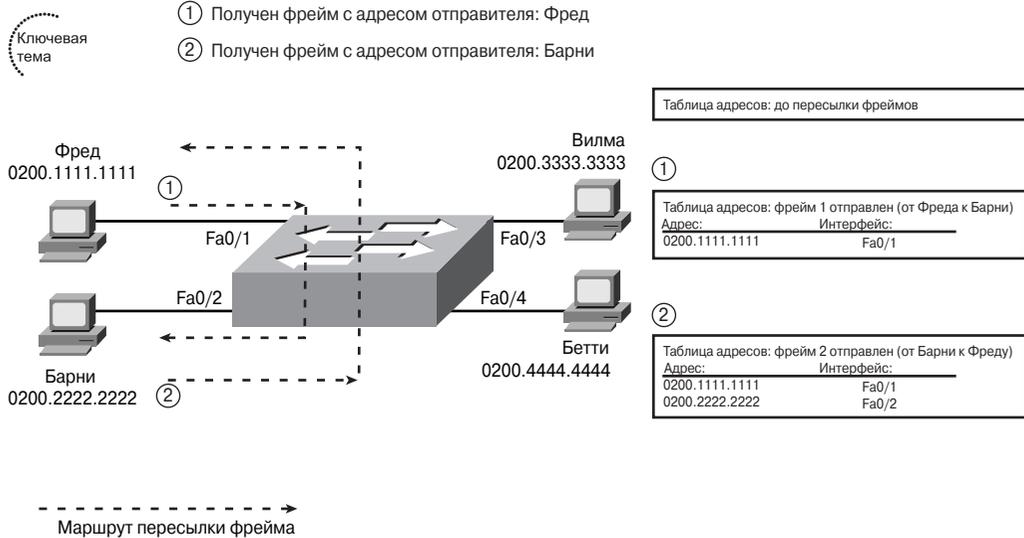


Рис. 7.6. Самообучение коммутатора: пустая таблица и два начальных фрейма

Как показано на рис. 7.6, после того как компьютер Фреда переслал первый фрейм (обозначен как “фрейм 1”) компьютеру Барни, коммутатор добавляет запись для MAC-адреса 0200.1111.1111 в таблицу коммутации и связывает ее с интерфейсом Fa0/1. Когда на втором этапе компьютер Барни пересылает ответный фрейм, его адрес, 0200.2222.2222, вместе с идентификатором интерфейса Fa0/2, т.е. порта, через который получен фрейм, добавляется в таблицу коммутации устройства. Коммутатор всегда для построения таблицы адресов использует MAC-адрес отправителя фрейма.

Лавинная рассылка фреймов

Обратимся снова к рис. 7.6 и проиллюстрированному на нем процессу рассылки фреймов. Как поступит коммутатор с первым фреймом от компьютера Фреда, т.е. на первом этапе обмена данными, если записи в таблице MAC-адресов еще нет? Когда получен фрейм с адресом получателя, отсутствующим в таблице, коммутатор пересылает такой фрейм через все интерфейсы кроме того, откуда он пришел. Итак, следует запомнить, что коммутатор всегда рассылает *одноадресатный фрейм, адрес получателя которого отсутствует в таблице коммутации (unknown unicast frame)*, через все интерфейсы в надежде, что искомое устройство окажется в каком-либо из подключенных к нему Ethernet-сегментов и ответит на такой фрейм и, следовательно, можно будет внести правильную запись в таблицу MAC-адресов устройства.

Например, как показано на рис. 7.6, коммутатор пересылает первый фрейм через интерфейсы Fa0/2, Fa0/3 и Fa0/4, несмотря на то, что MAC-адрес получателя 0200.2222.2222 (т.е. компьютер Барни) находится за интерфейсом Fa0/2. Коммутатор не отправляет фрейм обратно в интерфейс Fa0/1, поскольку он был получен через этот порт. Следует заметить, что на рис. 7.6 не показаны фреймы, пересылаемые через Fa0/3 и Fa0/4, поскольку основное внимание на иллюстрации уделяется процессу самообучения коммутатора. Когда компьютер Барни отвечает компьютеру

Фреда, коммутатор добавляет запись для MAC-адреса 0200.2222.2222 (и интерфейса Fa0/2) в таблицу адресов. Все последующие фреймы, передаваемые для адреса получателя 0200.2222.2222, не будут пересылаться в интерфейсы Fa0/3 и Fa0/4, а только в порт Fa0/2.

Процесс пересылки фреймов через все активные интерфейсы коммутатора, кроме того, откуда он пришел, называют *лавинной рассылкой* (flooding). Коммутаторы с использованием лавинной рассылки передают как одноадресатные фреймы, адреса получателей которых отсутствуют в таблице, так и широковещательные. Аналогично устройства поступают с многоадресатными (multicast) фреймами, кроме тех случаев, когда в коммутаторах явно сконфигурированы некоторые средства оптимизации многоадресатных потоков данных. Многоадресатные технологии выходят за рамки данной книги и рассматриваться не будут.

Коммутатор отсчитывает специальный таймер для каждой записи в таблице MAC-адресов, обычно называемый *таймером бездействия* (inactivity timer). Для каждой новой записи, т.е. нового адреса отправителя, такой таймер выставляется в ноль. Каждый раз при получении фрейма с тем же самым MAC-адресом отправителя таймер сбрасывается в нулевое значение. Значение таймера постоянно увеличивается, следовательно, устройство всегда может отследить, какие записи давно не обновлялись и от каких устройств давно не приходили фреймы. Если вдруг у коммутатора закончится место в оперативной памяти для адресных записей, самые старые MAC-адреса могут быть найдены по значению таймера бездействия и удалены из таблицы.

Защита от кольцевых маршрутов с помощью протокола STP

Третья главная функция коммутаторов локальных сетей заключается в предотвращении кольцевых маршрутов с помощью протокола распределенного связующего дерева (Spanning Tree Protocol — STP). Без протокола STP фреймы могут бесконечно долго курсировать по кольцевому маршруту, если в Ethernet-сети есть резервные каналы. Чтобы избежать заикливания фреймов, протокол STP блокирует некоторые порты и они не могут пересылать данные, при этом в сети между сегментами (т.е. доменами коллизий) существует только один активный маршрут для передачи данных. Результат работы протокола распределенного связующего дерева очевиден и прост: в сети остается один маршрут, заикливания фреймов не происходит, локальная сеть работает стабильно. Несмотря на то, что в локальной сети есть резервные каналы, которые станут активными в случае отказа основного соединения, при использовании протокола STP нельзя получить балансировку нагрузки.

Чтобы избежать кольцевых маршрутов на втором уровне, на всех коммутаторах должен быть запущен протокол STP, который каждый из портов каждого устройства переводит или в заблокированный режим (blocking state), или в режим передачи данных (forwarding). Под *блокированием* (Blocking) понимают такое состояние интерфейса, в котором он не может передавать или принимать фреймы пользовательских данных, но может обмениваться только служебными сообщениями протокола STP. В *режиме передачи данных* (forwarding) интерфейс может передавать и принимать пользовательские фреймы с данными. Если протокол заблокировал правильный набор интерфейсов, в сети останется только один активный логический маршрут между каждой парой сегментов.

ВНИМАНИЕ!

Протокол STP абсолютно одинаково работает в коммутаторах и прозрачных мостах, поэтому такие термины, как мост (bridge), коммутатор (switch) и мостовое устройство (bridging device) используются как синонимы в описаниях протокола STP.

Преимущества протокола STP становятся очевидными, если рассмотреть такой простой пример. Вспомним, что коммутаторы лавинно рассылают фреймы с неизвестным им MAC-адресом получателя и широковещательные сообщения через все интерфейсы.

На рис. 7.7 проиллюстрирована ситуация, когда один фрейм, отправленный компьютером Ларри компьютеру Боба, будет заикливаться, поскольку в сети есть резервный канал и нет протокола STP.

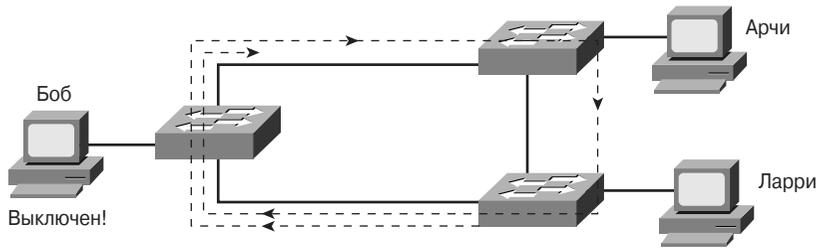


Рис. 7.7. Сеть с резервными каналами без протокола STP — фрейм заикливается

Компьютер Ларри отправляет единственный фрейм компьютеру Боба, который выключен, следовательно, MAC-адреса узла Боба нет в таблице коммутации у обоих коммутаторов. Поскольку это первый фрейм, то он представляет собой фрейм с неизвестным коммутаторам MAC-адресом получателя (unknown unicast) и он должен быть переслан устройством через все порты, кроме того, откуда он был получен. Такой фрейм будет попадать в бесконечный кольцевой маршрут второго уровня, так как коммутаторы не могут никакими средствами обнаружить адрес компьютера Боба (поскольку он выключен и адрес его не известен устройствам). Коммутаторы будут рассылать этот фрейм снова и снова и так до бесконечности.

Аналогично коммутаторы будут пересылать широковещательные фреймы. Если какой-либо из компьютеров отправит такой фрейм, он также будет курсировать бесконечно по кольцевому маршруту.

Один из вариантов решения описанной выше проблемы — построить локальную сеть без использования резервных каналов, тем не менее, большинство инженеров преднамеренно разрабатывают сети с избыточными каналами для обеспечения отказоустойчивости. На практике, когда какой-либо из каналов отказывает, желательно, чтобы сеть все же работала, поэтому при ее разработке используют резервирование. Правильным решением в таком случае будет то, которое включает в себя коммутируемую локальную сеть с резервными каналами и протокол STP, в задачу которого входит блокирование некоторых интерфейсов, чтобы в сети между двумя конечными устройствами существовал только один активный маршрут второго уровня.

Методы коммутации в коммутаторах Cisco

Выше было рассказано, как коммутатор принимает решение о том, переслать или отфильтровать фрейм. Когда коммутатор компании Cisco принимает решение об отправке фрейма, он может использовать один из механизмов пересылки, которые описаны ниже. Подавляющее большинство устройств на сегодняшний день использует метод коммутации с буферизацией фреймов (store-and-forward), тем не менее, все описанные ниже методы внутренней обработки потоков данных реализованы, как минимум, в одном из выпускаемых компанией Cisco коммутаторов.

Большинство прозрачных мостов и коммутаторов на сегодняшний день использует метод *коммутации с буферизацией фреймов* (store-and-forward processing). В этом механизме устройство должно получить фрейм полностью, прежде чем начать отправку его первого бита через выходной интерфейс. Существует еще два метода внутренней обработки фреймов: сквозная коммутация (cut-through) и бесфрагментная (fragment-free). MAC-адрес получателя расположен в начале Ethernet-заголовка, поэтому коммутатор может начать передачу задолго до того, как он примет весь фрейм. Сквозная и бесфрагментная коммутации работают именно таким образом, передача начинается задолго до того, как будет принят весь фрейм, следовательно, время обработки и отправки (т.е. задержка, delay) значительно уменьшается.

Метод сквозной коммутации (cut-through) — устройство начинает передачу фрейма как можно раньше, т.е. как только принята часть заголовка, содержащая адрес получателя. Этот метод очень заметно уменьшает задержку в сети, но побочным его результатом будет распространение ошибок в сети. Контрольная сумма фрейма (frame check sequence — FCS) находится в Ethernet-концевике, следовательно, коммутатор не может определить, есть ли ошибки во фрейме, перед тем как начать передачу. Используя этот метод, следует помнить о двух основных моментах: задержка за счет обработки фреймов устройством значительно уменьшается, но за это приходится платить свою цену — фреймы с ошибками могут быть переданы дальше.

Метод бесфрагментной коммутации (fragment-free processing) работает аналогично методу сквозной коммутации, но меньшее количество ошибок передается через устройство. Одна интересная особенность технологии CSMA/CD (Carrier Sense Multiple Access With Collision Detection — множественный доступ с контролем несущей и обнаружением коллизий) состоит в том, что большинство коллизий происходит на первых 64 байтах фрейма. Бесфрагментная коммутация похожа на сквозную в том понимании, что в ней также принимается только часть фрейма, 64 байта, и начинается передача. Задержка за счет обработки фрейма коммутатором в таком случае будет заметно меньше, чем при буферизации, и чуть больше, чем при сквозном методе. Количество передаваемых устройством ошибок также будет намного меньше, чем в методе коммутации с буферизацией.

На сегодняшний день большинство рабочих станций подключено к сети соединениями со скоростью 100 Мбит/с, вышестоящие каналы обычно работают на скорости 1 Гбит/с, в коммутаторах используются очень быстро работающие специализированные микросхемы (Application-Specific Integrated Circuits — ASIC) для аппаратной обработки потоков данных, поэтому в современных коммутаторах преимущественно используется метод коммутации с буферизацией фреймов, поскольку на таких скоростях передачи данных заметного уменьшения задержки не происходит.

Внутренние механизмы обработки фреймов в коммутаторах могут сильно отличаться у разных производителей, тем не менее, все методы можно свести к трем основным или к некоторым их производным, которые перечислены в табл. 7.2.



Таблица 7.2. Методы коммутации фреймов

Метод коммутации	Описание
С буферизацией фреймов (store-and-forward processing)	Коммутатор получает фрейм полностью, до последнего бита (сохраняет — store), а потом начинает его передачу (forward). Этот метод позволяет проверить целостность фрейма посредством контрольной суммы (FCS) до его отправки
Сквозная (cut-through)	Коммутатор отправляет фрейм как только получена нужная информация — MAC-адрес получателя. Этот метод значительно уменьшает задержку, но фреймы с неправильной контрольной суммой (FCS) не будут отброшены устройством
Бесфрагментная (fragment-free processing)	Коммутатор начинает передачу, как только получит первые 64 байта фрейма. Этот метод позволяет исключить большинство ошибочных фреймов при коммутации и результатов коллизий

Преимущества и недостатки механизмов коммутации в сетях LAN

В коммутаторах есть множество дополнительных функций, отсутствующих в устаревших устройствах для локальных сетей (LAN), таких как концентратор и мост. В частности, к основным достоинствам коммутаторов можно отнести перечисленные ниже.

- Если к порту коммутатора подключено всего одно сетевое устройство, то он выполняет микросегментацию сети и предоставляет выделенную полосу пропускания для устройства.
- Коммутаторы позволяют осуществлять передачу множественных одновременных потоков данных между устройствами, подключенными к разным интерфейсам.
- Если к порту коммутатора подключено всего одно сетевое устройство, работающее в дуплексном режиме, то эффективная полоса пропускания удваивается.
- Коммутаторы выполняют согласование скорости, означающее, что устройства, подключенные посредством разных по скорости технологий Ethernet, могут взаимодействовать через коммутатор (через концентратор — не могут).

В коммутаторах используются специальные алгоритмы второго уровня, инспектирующие заголовки канального уровня для принятия решения о пересылке фрейма. В частности, коммутаторы принимают решение об отправке или фильтрации фрейма, строят таблицу MAC-адресов и используют протокол STP, чтобы разомкнуть кольцевые маршруты согласно приведенной ниже последовательности.

- Этап 1.** Коммутаторы пересылают фреймы на основании адреса получателя в заголовке фрейма.



- Если адрес получателя является широковещательным, многоадресным (multicast) или одноадресным, который отсутствует в таблице коммутации, то устройство лавинно рассылает фрейм (flood).
- Когда адрес получателя известен (т.е. присутствует в таблице MAC-адресов устройства):
 - если в таблице MAC-адресов выходной интерфейс не совпадает со входным для фрейма, коммутатор пересылает фрейм через найденный в таблице интерфейс;
 - если выходной интерфейс совпадает со входным интерфейсом, коммутатор отфильтровывает фрейм, т.е. просто игнорирует его и никуда дальше не передает.

Этап 2. Коммутаторы используют следующий алгоритм для заполнения таблицы MAC-адресов.

- Для каждого принятого фрейма считывается MAC-адрес отправителя и запоминается интерфейс, откуда он был получен.
- Если пары “адрес-интерфейс” нет в таблице устройства, они добавляются в таблицу коммутации, таймер (inactivity timer) устанавливается в нулевое значение.
- Если для обнаруженного MAC-адреса уже есть запись в таблице коммутации устройства, таймер сбрасывается (устанавливается в нулевое значение).

Этап 3. Коммутаторы используют протокол STP для предотвращения образования кольцевых маршрутов путем блокирования некоторых интерфейсов, т.е. переключения их в такой режим, что они не могут принимать и передавать пользовательские фреймы.

Основы дизайна локальных сетей

До сих пор в этой книге в основном рассматривались отдельные разрозненные функции локальных компьютерных сетей. Например, выше было рассказано о том, как коммутаторы пересылают фреймы, были описаны различные варианты распылки UTP-кабеля, рассмотрен алгоритм CSMA/CD и как он справляется с коллизиями передачи фреймов. Выше также были описаны различия между коммутаторами и концентраторами, отличия в их принципах работы, например, что концентраторы создают единый домен коллизий, а коммутаторы — несколько и т.д.

В этом разделе представлен более концептуальный подход к проблемам локальных сетей, дальше будут рассмотрены принципы дизайна средних и крупных локальных сетей. При построении сети малого размера можно купить буквально один коммутатор, подключить к нему правильными кабелями все необходимые устройства, и сеть готова. При разработке же сетей среднего и крупного размера выбор сетевых продуктов значительно больше и вариантов дизайна тоже больше, поскольку можно использовать концентраторы, коммутаторы и маршрутизаторы. Кроме всего прочего, нужно также хорошо обдумать свой выбор, например, моделей коммутаторов, они отличаются по размеру, по количеству портов, производительностью, набором функций и, в конце концов, ценой. Среда передачи данных в локальной сети

также может быть различной. Инженеру придется взвесить все “за” и “против” как для UTP-кабеля (низкая цена и простота установки), так и, например, для оптоволоконной среды (больше длина сегмента и лучшая защита на физическом уровне).

Ниже рассмотрены несколько наиболее важных тем, имеющих непосредственное отношение к дизайну локальных сетей. В частности, сначала рассмотрено поведение сети при использовании в ней концентраторов, коммутаторов и маршрутизаторов для объединения сегментов сети. Далее описана основная терминология компании Cisco в области сетевого дизайна. Завершает раздел краткое описание наиболее популярных разновидностей технологии Ethernet и типов кабелей, а также перечислены ограничения на максимальную длину для каждой технологии.

Широковещательный домен и домен коллизий

Создавая локальную Ethernet-сеть, инженер устанавливает в ней некие сетевые устройства, на сегодняшний день обычно коммутаторы, несколько маршрутизаторов и, возможно, несколько концентраторов. Разные участки сети могут быть построены и вести себя по-разному, с точки зрения производительности и выполняемых функций, в зависимости от типа используемых устройств; разные функции оборудования нужно учитывать при принятии решения о дизайне сети.

Термины *домен коллизий* (collision domain) и *широковещательный домен* (broadcast domain) описывают два важных принципа сегментации локальных компьютерных сетей с помощью оборудования разного типа. В этом разделе описаны основные концепции, связанные с этими терминами в дизайне сетей, а основная цель заключается в том, чтобы объяснить, как концентраторы, коммутаторы и маршрутизаторы влияют на границы доменов коллизий и широковещательных доменов.

Домены коллизий

Как было замечено выше, *домен коллизий* (collision domain) представляет собой набор интерфейсов локальной сети, фреймы от которых могут вступать в коллизии друг с другом, но не с фреймами от остальных устройств в сети. На рис. 7.8 проиллюстрированы домены коллизий.

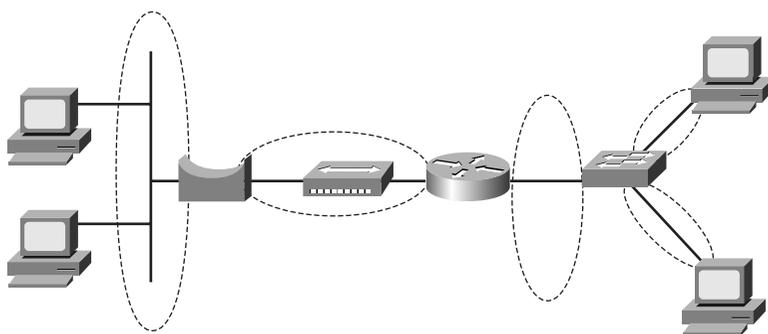


Рис. 7.8. Домены коллизий

Отдельные сегменты, или домены коллизий, показаны на рис. 7.8 пунктирной линией. Коммутатор, изображенный на схеме справа, разделяет локальную сеть на отдельные домены коллизий на каждом порту. Аналогично, маршрутизатор и мост разделяют сеть

на отдельные домены коллизий (роль маршрутизаторов в этой книге раньше подробно описана не была). Из всех показанных на схеме устройств только концентратор, показанный в центре схемы сети, не создает множество отдельных доменов коллизий для каждого интерфейса. Это устройство просто повторяет фреймы на всех своих портах без буферизации и задержки фрейма перед отправкой в загруженный сегмент сети.

ВНИМАНИЕ!

Структура сети, показанная на рис. 7.8, не является типичным дизайном реальной компьютерной инфраструктуры. Ее основное предназначение — просто проиллюстрировать домены коллизий и сравнить концентраторы, коммутаторы и маршрутизаторы.

Широковещательные домены

Термин *широковещательный домен* (broadcast domain) описывает участок сети, где могут распространяться широковещательные фреймы. Широковещательный домен включает в себя набор устройств, в котором когда одно устройство отправляет широковещательное сообщение, все оставшиеся его получают и обрабатывают. Так, например, поскольку коммутаторы пересылают все широковещательные и многоадресные сообщения через все свои порты, кроме того, откуда они пришли, следовательно, коммутатор создает единый широковещательный домен.

Только маршрутизаторы являются барьером между широковещательными фреймами, т.е. не пропускают их через себя. На рис. 7.9 показаны границы широковещательных доменов для схемы сети, проиллюстрированной на рис. 7.8.

Широковещательное сообщение, отправленное одним устройством в широковещательном домене, не пересылается устройствам в другом широковещательном домене. В проиллюстрированном на рис. 7.9 примере есть два широковещательных домена, т.е. маршрутизатор не будет пересылать широковещательные фреймы, отправленные компьютером, показанным на схеме слева, в сетевой сегмент, расположенный на схеме справа. Раньше иногда маршрутизаторы, которые не пересылали широковещательные сообщения, называли *широковещательным брандмауэром* (broadcast firewall).

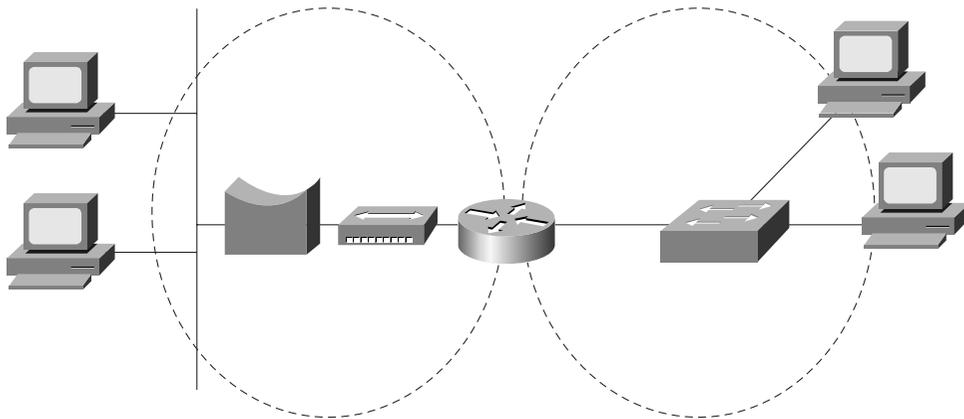


Рис. 7.9. Широковещательные домены

Краткие определения широковещательного домена и домена коллизий приведены ниже.

- *Домен коллизий* представляет собой группу сетевых интерфейсов (интерфейсных плат, Network Interface Cards — NIC), для которых характерно, что фрейм, отправленный одним из них, может столкнуться в коллизии с фреймом, отправленным другим интерфейсом.
- *Широковещательный домен* представляет собой группу сетевых интерфейсов, для которых характерно, что широковещательный фрейм, отправленный одним из них, будет получен и обработан всеми интерфейсами в группе.



Влияние широковещательных доменов и доменов коллизий на дизайн сети

При разработке локальной сети нужно помнить основные особенности поведения сетевых интерфейсов разных устройств при подсчете их количества в каждом широковещательном домене и домене коллизий. Прежде всего следует рассмотреть поведение устройств в одном домене коллизий и помнить, что:

- устройства разделяют между собой одну доступную полосу пропускания;
- устройства могут неэффективно использовать такую полосу пропускания из-за коллизий, в частности когда сеть сильно загружена.

Например, в сегменте сети планируется поставить десять персональных компьютеров с Ethernet-интерфейсами 10/100. Если все десять компьютеров подключить к портам концентратора с пропускной способностью 100 Мбит/с, то результатом будет единый домен коллизий и компьютеры будут разделять между собой общую полосу пропускания в 100 Мбит/с. При высокой загрузке сети производительность такой сети с использованием концентратора (hub) будет заметно падать. Если в той же самой топологии использовать коммутатор вместо концентратора, каждый порт последнего будет создавать свой собственный домен коллизий, внутри которого будет доступна полоса пропускания в 100 Мбит/с (т.е. будет создано 10 независимых доменов коллизий). Если к тому же включить дуплексный режим работы для каждого интерфейса, эффективная полоса пропускания для каждого порта (и для каждого домена коллизий!) будет приближаться к 200 Мбит/с, что в сумме для 10 компьютеров будет давать около 2 Гбит/с — очень заметное улучшение производительности сети!

В современных сетях преимущества использования коммутаторов вместо концентраторов вполне очевидны на фоне ошеломляющего увеличения производительности. Честно говоря, во всех новых внедряемых сетях на сегодняшний день используются исключительно коммутаторы. Тем не менее, многие производители все еще выпускают концентраторы, поскольку они немного дешевле стоят, чем коммутаторы, и их вполне можно встретить и в некоторых современных сетях.

Далее мы рассмотрим проблемы, связанные с широковещательными сообщениями. Когда сетевой узел получает широковещательное сообщение, он обязан его обработать. Такое утверждение означает, что сетевая карта должна отправить центральному процессору (CPU) прерывание, а процессор должен выделить некоторые свои ресурсы на обработку такого фрейма. Все сетевые узлы время от времени отправляют широковещательные фреймы — они необходимы для их нормальной ра-

боты. Например, сообщения протокола ARP используют широковещательный механизм работы, как было описано в главе 5 “Основы IP-адресации и маршрутизации”. Таким образом, широковещание будет присутствовать в любой сети, это нормальный режим работы, но широковещательные фреймы требуют затрат ресурсов всех сетевых устройств на их обработку.

Рассмотрим теперь локальную сеть большего размера, состоящую из нескольких коммутаторов и 500 компьютеров. Коммутаторы вместе образуют единый широковещательный домен, поэтому если один из 500 компьютеров отправляет широковещательное сообщение, оставшиеся 499 его получают и обрабатывают. Если широковещательных фреймов в такой сети много, то они могут очень заметно снизить производительность персональных компьютеров в сети. Предположим, что мы модифицируем сеть так, чтобы у нас было 5 сегментов по 100 компьютеров, которые разделены маршрутизатором, следовательно, в такой сети будет существовать 5 широковещательных доменов. В такой схеме сети широковещательное сообщение от одного компьютера будет вызывать прерывание у 99 других компьютеров, а 400 будут им “не затронуты”, что приведет к меньшему снижению производительности рабочих станций.

ВНИМАНИЕ!

Построение широковещательных доменов меньшего размера в сети может также значительно улучшить безопасность сети как за счет уменьшения количества широковещательных сообщений, так и за счет расширенных функций безопасности в маршрутизаторах.

Обычно выбор между концентраторами и коммутаторами прост и заканчивается в пользу последних, решить же, когда следует использовать маршрутизаторы для разделения широковещательных доменов, намного сложнее. Подробное описание всех достоинств и недостатков разных устройств третьего уровня и возможных вариантов их реализации выходит за рамки данной книги. Тем не менее читатель должен понимать концепции широковещательных доменов, а именно, что маршрутизатор разбивает сеть на несколько широковещательных доменов, концентратор или коммутатор — нет.

В сертификационном экзамене CCNA, скорее всего, будет много вопросов, связанных с терминологией сегментации локальных сетей и ее преимуществ, и будет мало простых вопросов, ориентированных просто на факты, имеющие отношение к широковещательным доменам и доменам коллизий. В табл. 7.3 перечислены основные преимущества сегментации, которые следует знать. Описанные в таблице функции можно выразить одним вопросом: “Какие из перечисленных ниже преимуществ могут быть получены при установке концентратора, коммутатора или маршрутизатора в Ethernet-сети?”



Таблица 7.3. Преимущества сегментации Ethernet-сетей с помощью концентраторов, коммутаторов и маршрутизаторов

Преимущество	Концентратор	Коммутатор	Маршрутизатор
В сети общая длина кабеля может быть больше	Да	Да	Да
Сеть разбивается на множество доменов коллизий	Нет	Да	Да
Увеличивается доступная узлам полоса пропускания (bandwidth)	Нет	Да	Да
Сеть разбивается на множество широковещательных доменов	Нет	Нет	Да

Сети VLAN

Во многих сетях предприятий (Enterprise) на сегодняшний день используются виртуальные локальные сети (virtual LAN — VLAN). Прежде чем перейти к описанию терминологии и принципов работы сетей VLAN, необходимо вспомнить наиболее краткое и точное определение локальной сети (Local Area Network — LAN). Несмотря на то, что понятие *локальной сети* может быть читателю знакомо из других книг и источников, мы приведем наиболее точное определение с нашей точки зрения: локальной сетью (LAN) называют совокупность сетевых устройств в одном и том же широковещательном домене.

Следовательно, первое, что следует запомнить: без сетей VLAN коммутатор все свои интерфейсы связывает с одним широковещательным доменом. Другими словами, все подключенные к нему устройства находятся в одной локальной сети (LAN). (В коммутаторах компании Cisco такое поведение реализовано за счет того, что все интерфейсы устройства стандартно связаны с одной сетью VLAN с номером 1.) Если виртуальные сети VLAN все же используются, то коммутатор, согласно конфигурации, помещает одни интерфейсы в один широковещательный домен, другие — в другой. На практике устройство просто связывает некоторые порты с одной сетью VLAN, некоторые — с другой, а точнее, просто с идентификатором соответствующей виртуальной локальной сети. Такие отдельные широковещательные домены в коммутаторе и носят название сетей VLAN.

На двух рисунках ниже проиллюстрированы две локальные сети и показано, как на них повлияют сети VLAN. В первом примере (рис. 7.10), чтобы создать два отдельных широковещательных домена, приходится использовать два независимых коммутатора: по одному на каждый широковещательный домен.

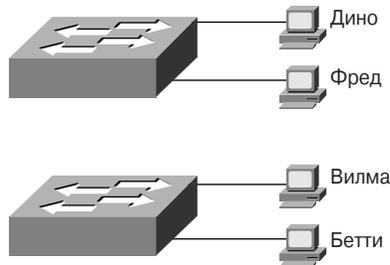


Рис. 7.10. Сеть с двумя широковещательными доменами без сетей VLAN

В качестве альтернативного решения можно предложить проиллюстрированную на рис. 7.11 схему сети с отдельными широковещательными доменами. В ней используется только один коммутатор, а отдельные широковещательные домены создаются с помощью виртуальных локальных сетей (VLAN).

В сети, показанной на рис. 7.11, в действительности не очень нужны сети VLAN, поскольку она невелика. Тем не менее виртуальные локальные сети могут быть внедрены по многим причинам, в частности:

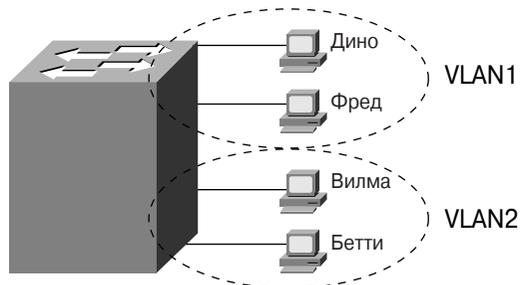


Рис. 7.11. Сеть с двумя широкоэмительными доменами и двумя сетями VLAN с использованием одного коммутатора

- чтобы создать более гибкую сетевую инфраструктуру и сгруппировать на логическом уровне пользователей по подразделениям, по выполняемым функциям и рабочим группам, а не на физическом;
- чтобы разбить сеть на более мелкие сегменты (т.е. широкоэмительные домены) с целью уменьшения нагрузки на узлы в каждой сети VLAN;
- чтобы уменьшить нагрузку для протокола STP, например, ограничив сеть VLAN одним коммутатором доступа к сети;
- чтобы повысить защиту сети за счет того, что узлы, работающие с критичными для компании потоками данных, вынесены в отдельную сеть VLAN;
- чтобы разделить трафик от IP-телефона и потоки данных от подключенного к нему персонального компьютера.

Конфигурирование, а также поиск и устранение неисправностей в сетях VLAN подробно описаны во втором томе книги.

Терминология дизайна территориальных сетей LAN

Территориальные (или кампусные) локальные сети представляют собой локальные сети, охватывающие крупные здания или несколько рядом расположенных зданий, т.е. некоторую территорию. Так, например, компания может арендовать несколько офисных помещений в разных зданиях одного большого офисного комплекса (office park). Сетевые инженеры такой компании могут построить сеть с использованием магистральных коммутаторов в каждом здании, которые соединены между собой посредством Ethernet-линий, и создать территориальную локальную сеть.

В процессе планирования и разработки территориальной локальной сети инженеры должны рассмотреть различные варианты технологии Ethernet и учесть максимальную длину кабеля в каждой из них. Кроме того, следует учесть различные скорости передачи данных в разных технологиях и подумать о том, что к некоторым коммутаторам будут напрямую подключены устройства пользователей, а к другим будут подключены только коммутаторы доступа к сети пользователей. Кроме всего прочего, в большинстве проектов инженеру приходится учитывать уже имеющееся в сети оборудование и оценивать, нужно ли увеличение пропускной способности и скорости существующих сегментов и следует ли покупать новое оборудование.

Например, большинство уже установленных в сети компьютеров на сегодняшний день укомплектовано сетевыми картами со скоростями передачи данных 10/100, а новые компьютеры имеют встроенные сетевые карты со скоростями 10/100/1000. При использовании правильного типа кабелей такие новые современные рабочие станции могут за счет автосогласования использовать режим 10BASE-T (10 Мбит/с), 100BASE-TX (100 Мбит/с), или 1000BASE-T (1000 Мбит/с, или 1 Гбит/с) в Ethernet-сети, причем по тому же самому UTP-кабелю. Поэтому перед инженером будет стоять задача, выбрать коммутатор с портами, поддерживающими режим 10/100, или устройство с интерфейсами 10/100/1000. На момент написания этой книги (лето 2007 года) разница в цене коммутаторов, поддерживающих скорость передачи до 100 Мбит/с и до 1000 Мбит/с, все еще была очень существенной, чтобы озадачить руководство компании, планирующей установить себе сеть. Тем не менее при использовании коммутаторов с режимом работы интерфейсов 10/100/1000 можно построить более масштабируемое решение и подключить практически любое пользовательское устройство. Кроме того, такая сеть будет готова к переходу со скорости передачи в 100 Мбит/с на рабочие станции с подключением в 1000 Мбит/с по мере покупки новых рабочих станций.

Чтобы упорядочить все требования к территориальным локальным сетям, а также облегчить процесс обсуждения принципов дизайна сети между специалистами, в сетях, построенных на оборудовании компании Cisco, используется некоторая общая терминология для описания основных принципов и компонентов. Типичная структура крупной территориальной сети вместе с основными терминами проиллюстрирована на рис. 7.12. Рассмотрим кратко представленную на иллюстрации терминологию.

Согласно подходу компании Cisco используется три основных термина для описания роли каждого коммутатора (или сетевого устройства) в сети: *уровень доступа к сети (access)*, *уровень распределения (distribution)* и *ядро сети (core)*. Роль устройств определяется исходя из двух основных характеристик:

- подключены ли к коммутатору устройства конечных пользователей;
- должен ли коммутатор пересылать фреймы между разными коммутаторами и подключен ли он к множеству различных коммутаторов.

К *коммутаторам уровня доступа к сети (access switches)* непосредственно подключены устройства конечных пользователей, которым предоставляется доступ к локальной сети. В нормальных условиях такие коммутаторы только пересылают фреймы от пользовательских рабочих станций и не должны (по крайней мере, с точки зрения правильного дизайна сети) передавать трафик от одного коммутатора уровня доступа к другому. Например, в нормальных условиях работы сети, показанной на рис. 7.12, коммутатор Access1 не должен пересылать трафик для компьютеров, подключенных к коммутатору Access3, через коммутатор Access4. Поскольку коммутаторы уровня доступа к сети должны передавать только пользовательский трафик, они менее высокопроизводительны и стоят дешевле; обычно от них требуется только достаточное количество портов для подключения оконечных устройств на этаже или в здании.

В крупных территориальных локальных сетях *коммутаторы уровня распределения (distribution switches)* обеспечивают маршруты для передачи потоков данных между коммутаторами уровня доступа к сети. Согласно стандартным требованиям дизайна

сетей каждый коммутатор уровня доступа должен быть подключен как минимум к одному коммутатору уровня распределения. Тем не менее разработчики сетей зачастую используют каналы к двум разным коммутаторам вышестоящего уровня (см. рис. 7.12) чтобы получить сеть с резервированием.

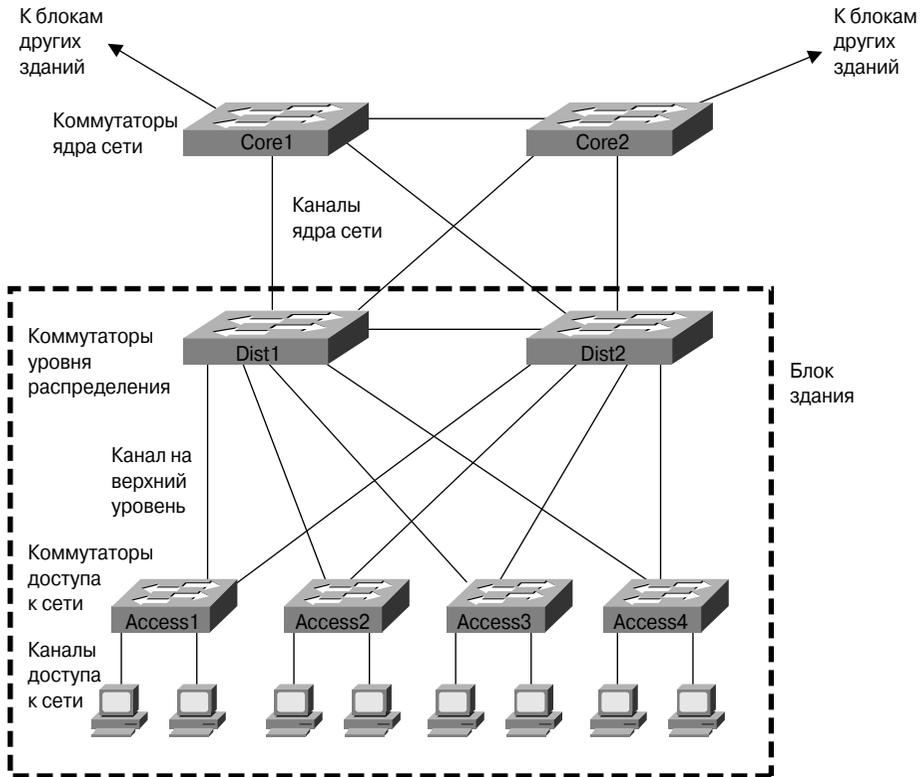


Рис. 7.12. Территориальные сети и их терминология

Если в структуре сети использовать коммутаторы уровня распределения, то такой подход может принести некоторые преимущества, как с точки зрения кабельной системы, так и в плане повышения производительности инфраструктуры в будущем. Представим себе сеть, в которой есть 30 коммутаторов уровня доступа к сети и для которой разработчик решил построить такую схему, где каждый из коммутаторов уровня доступа к сети должен быть подключен к остальным напрямую кабелем. В такой структуре понадобится 435 кабелей только для того, чтобы подключить друг к другу все коммутаторы! Как второй существенный недостаток такой схемы можно указать наличие только одного сегмента для соединения двух коммутаторов. Проблемы будут возникать в том случае, если канал между двумя устройствами обрывается и потоки данных идут через другой, например, соседний, коммутатор. Следует учесть, что коммутаторы уровня доступа к сети не предназначены для обработки гигантских объемов данных, они имеют меньшую производительность и за счет этого — меньшую стоимость. Если же подключить рассматриваемые 30 коммутаторов уровня доступа к двум высокопроизводительным коммутаторам уровня распре-

деления, то понадобится всего 60 кабелей (т.е. каналов). Кроме того, правильно подобранные коммутаторы уровня распределения могут обработать большие потоки данных от устройств смежных уровней и обычно позволяют достигнуть более высоких скоростей передачи данных. Такой дизайн сети с использованием двух вышестоящих коммутаторов уровня распределения и двумя каналами от коммутаторов уровня доступа к сети до них предоставляют высокую степень надежности и позволяют построить резервируемую инфраструктуру.

Коммутаторы ядра сети (core) дают еще больший выигрыш в плане агрегирования каналов, чем устройства уровня распределения. Эти коммутаторы работают на еще более высоких скоростях и коммутируют потоки данных еще быстрее, на сегодняшний день их типичная производительность составляет сотни миллионов фреймов в секунду. Тем не менее коммутаторы ядра сети выполняют практически те же самые функции, что и устройства уровня распределения, но с небольшими отличиями. Зачастую в средних, а обычно в малых территориальных сетях функции обоих уровней, распределения и ядра, объединяют в один.

Ниже приведено краткое резюме по функциям коммутаторов в территориальных сетях.

- **Уровень доступа к сети** предоставляет точки доступа, или подключения, устройств конечного пользователя. На этом уровне фреймы между двумя коммутаторами доступа к сети в нормальных условиях напрямую не передаются, а должны быть отправлены на уровень распределения.
- **Уровень распределения** является точкой агрегирования каналов от коммутаторов уровня доступа к сети, пересылает фреймы между коммутаторами, но не служит для подключения устройств конечного пользователя.
- **Уровень ядра сети** агрегирует каналы от коммутаторов уровня распределения в крупных территориальных локальных сетях и обеспечивает очень высокие скорости коммутации потоков данных.

Ethernet-среда и длина кабелей

Проектируя территориальную локальную сеть, инженер должен прежде всего оценить необходимую длину кабелей и выбрать на основе такой информации необходимую ему технологию Ethernet, поддерживающую сегменты нужной длины. Например, компания арендует помещения в пяти разных зданиях офисного комплекса, поэтому инженеру нужно вычислить длину кабельного маршрута между зданиями и подобрать подходящий Ethernet-канал.

Наиболее распространенными на сегодняшний день являются три технологии Ethernet: 10BASE-T, 100BASE-TX, и 1000BASE-T. Для всех указанных технологий характерна максимальная длина кабеля в 100 м, но они слегка отличаются используемым кабелем. Ассоциации EIA/TIA стандартизировали и стандартизируют новые технологии Ethernet, а именно кабельные системы для них, в частности, например, качество кабеля. В каждом из стандартов технологии Ethernet указана категория кабеля, которую можно использовать, причем это минимально требуемая категория, в сети вполне может быть использован и более качественный кабель. Например, в стандарте 10BASE-T рекомендуется использовать кабель категории 3 (Category 3 — CAT3), в технологии 100BASE-TX используется кабель пятой категории (CAT5), а в стандарте 1000BASE-TX нужно использовать

кабели категорий 5е или 6 (CAT5е или CAT6). Если же инженер планирует использовать (чтобы не пропала!) существующую кабельную систему, он (или она) должен знать, какой тип UTP-кабеля установлен, а также какие ограничения по скорости для соответствующей Ethernet-технологии и кабеля существуют.

В нескольких Ethernet-технологиях используются оптоволоконные кабели. В кабеле UTP (Unshielded Twisted Pair — неэкранированная витая пара) в качестве среды передачи используются медные проводники, по которым протекает ток; в оптоволоконных кабелях используется ультратонкое стеклянное волокно, через которое передаются световые импульсы. Чтобы передать биты, оптические интерфейсы могут менять уровень света, делать ярче или слабее, соответственно, кодируя таким образом 1 и 0 в кабеле.

Для оптических кабелей характерна большая длина кабельного сегмента, которая заметно превышает 100 м для UTP-кабелей в медных технологиях Ethernet. В оптических кабелях практически нет интерференции сигнала, вызываемой внешними источниками помех и в зависимости от технологии в оптических коммутаторах в качестве источника сигнала могут быть использованы как лазеры, так и светодиоды (light-emitting diode — LED). При использовании лазеров длина кабеля может быть очень большой, например, порядка 100 км на сегодняшний день. Для светодиодов, которые намного дешевле, характерны меньшие расстояния, вполне достаточные для подключения офисов и помещений в рамках территориальной сети.

И в заключение следует учесть, что используемая технология также определяет максимальную длину кабеля. Для оптоволоконных соединений следует помнить, что многомодовое оптическое волокно поддерживает меньшие расстояния, но зато стоит дешевле и позволяет использовать в качестве источника сигнала недорогие светодиоды. Второй тип оптоволоконных каналов, одномодовое волокно, поддерживает намного большие длины кабелей, но стоит дорого. Опять же, коммутирующее оборудование на основе светодиодов (т.е. для многомодового оптоволокна) стоит намного дешевле, чем оборудование с лазерными источниками (для одномодового оптоволокна).

В табл. 7.4 перечислены наиболее распространенные типы Ethernet-технологий и приведены их ограничения и типы кабелей.

Таблица 7.4. Технологии Ethernet, их среда и максимальная длина сегмента (согласно стандартам Института IEEE)

Технология Ethernet	Среда	Максимальная длина сегмента, м (фут)
10BASE-T	UTP-кабель стандарта TIA/EIA категории CAT3 или лучше, используются две пары	100 (328)
100BASE-TX	UTP-кабель стандарта TIA/EIA категории CAT5 или лучше, используются две пары	100 (328)
100BASE-FX	Многомодовое оптическое волокно 62,5/125 микрон	400 (1312,3)
1000BASE-CX	STP-кабель ²	25 (82)
1000BASE-T	UTP-кабель стандарта TIA/EIA категории CAT5е или лучше, используются две пары	100 (328)

² Экранированная витая пара (*shielded twisted pair*). — Примеч. ред.

Окончание табл. 7.4

Технология Ethernet	Среда	Максимальная длина сегмента, м (фут)
1000BASE-SX	Многомодовое оптоволокно	275 (853) для оптоволокна 62,5 микрон 550 (1804,5) для оптоволокна 50 микрон
1000BASE-LX	Многомодовое оптоволокно	550 (1804,5) для оптоволокна 62,5 и 50 микрон
1000BASE-LX	Одномодовое оптоволокно 9 микрон	10 000 (6,2 мили)

Большинство инженеров обычно помнят только общие тенденции, а конкретные числа для максимальной длины кабеля подглядывают в каком-нибудь справочнике или таблице в книге (например, в табл. 7.4). Следует также принимать во внимание физический путь, по которому будет проложен кабель — он может значительно повлиять на длину кабельного сегмента. Например, нужно проложить кабель из одного конца здания в другой. “Напрямую” это может быть не так уж и много, но нужно учесть, что кабель будет проложен по коробам, т.е. сначала будут выведены спуски, например, из-под фальшпотолка до оборудования кабельного узла. Потом кабель будет проложен по коробам этажа, которые могут быть очень даже извилистыми и похожими на лабиринт — такой маршрут, вполне очевидно, может быть не самым коротким. И только после расчета реальной протяженности кабельного маршрута следует обратиться к таблице или справочнику и выбрать подходящую среду передачи данных.

Подготовка к экзамену

Повторите все ключевые темы

Следует повторить все ключевые темы данной главы, которые помечены пиктограммой на полях. В табл. 7.5 перечислены все основные ключевые темы и соответствующие им страницы.



Таблица 7.5. Ключевые темы главы 7

Элемент	Описание	Номер страницы
Список	Указаны преимущества коммутаторов	222
Рис. 7.4	Пример алгоритма коммутации фреймов	223
Рис. 7.5	Пример алгоритма фильтрации фреймов	224
Рис. 7.6	Пример построения таблицы MAC-адресов коммутатором	225
Табл. 7.2	Резюме по трем алгоритмам коммутации фреймов	229
Список	Преимущества коммутации	229
Список	Резюме по алгоритмам коммутации, фильтрации фреймов и по построению таблиц MAC-адресов	229
Список	Определения широковещательного домена и домена коллизий	233
Табл. 7.3	Четыре особенности дизайна локальных сетей при использовании концентраторов, коммутаторов и маршрутизаторов	234
Рис. 7.11	Иллюстрация концепции сетей VLAN	236

Заполните таблицы и списки по памяти

Распечатайте приложение 3 (Appendix H) с компакт-диска или его раздел, относящийся к этой главе, и заполните таблицы и списки по памяти. В приложении И (Appendix I) приведены заполненные таблицы и списки для самоконтроля.

Ключевые термины главы

Дайте определения перечисленных ниже терминов и проверьте правильность их написания в списке терминов:

широковещательный домен, широковещательный фрейм, домен коллизий, сквозная коммутация, лавинная рассылка фреймов, бесфрагментная коммутация, микросегментация, сегментация, протокол STP (Spanning Tree Protocol), коммутация с буферизацией фреймов, одноадресатный фрейм с неизвестным получателем, виртуальная локальная сеть (VLAN).

