**Глава 4. Мосты**

Итак, мосты используются для соединения локальных сегментов СПД на основе канала с множественным доступом (СПД КМС). При этом трафик в каждом отдельном сегменте остается прежним.

Вот некоторые важнейшие характеристики мостов:

* работают на уровне 2 модели OSI;
* более «разумны», чем концентраторы (hub), они могут анализировать входящие кадры и пересылать (или удалять) их в зависимости от определенных данных об адресе;
* могут буферизовать кадры между сегментами СПД КМС;
* позволяют сразу нескольким устройствам в разных сегментах передавать данные, не вызывая коллизий;
* динамически поддерживают таблицы MAC-адресов.

Благодаря этим характеристикам применение мостов позволяет:

* изолировать потенциальные проблемы отдельных сегментов так, чтобы они не влияли на другие сегменты;
* локализовать сетевой трафик путем фильтрации кадров внутри сегментов СПД КМС или между ними;
* расширить СПД на большие расстояния путем объединения нескольких сегментов.

## 4.7. Сетевые коммутаторы

Сетевой коммутатор (далее просто коммутатор) представляет собой устройство с несколькими портами, к которым можно подключать сегменты СПД КМД, например, сегменты 802.3. На основании таблицы коммутации, расположенной в памяти коммутатора, кадры с входного порта коммутатор передает на надлежащий выходной порт. Тем самым трафик на отдельных сегментах существенно ниже, чем на коммутаторе в целом. Коммутаторы работают на более высоких скоростях, чем мосты, и функционально более гибкие.

По сравнению с мостами у коммутаторов больше портов. Достаточно распространены коммутаторы с 24 и 48 портами со скоростями 10 Мбит/с и 100 Мбит/с. Коммутаторы на крупных предприятиях могут поддерживать сотни портов. У коммутаторов больше размер буферного пространства для сохранения принимаемых кадров. Это весьма полезно, особенно если порты, серверы и другие элементы сети перегружены. В зависимости от стоимости коммутатора возможна поддержка локальных сегментов СПД КМД с разными скоростями: 10 Мбит/с, 100 Мбит/с, 1 Гбит/с или 10 Гбит/с.

* **Большие буферы кадров.** Возможность сохранять принимаемые кадры Это весьма полезно, особенно если порты, серверы и другие элементы сети перегружены.
* **Скорости портов.** В зависимости от стоимости коммутатора возможна поддержка носителей с разными скоростями: 10 Мбит/с, 100 Мбит/с, 1 Гбит/с или 10 Гбит/с.

Для коммутации данных между сетевыми портами коммутаторы используют один из следующих методов.

* **Коммутация без буферизации пакетов.** При использовании этого метода, коммутатор, получив 6 байтный МАС адрес получателя, сразу занимает нужный выходной порт и начинает передачу. Обнаружение ошибок при этом не происходит. Если на входе произойдет коллизия, то кадр будет потерян.
* **Коммутация с буферизацией кадров.** При этом методе коммутатор сохраняет в буфере весь кадр. Во время сохранения коммутатор анализирует кадр и выполняет обнаружение ошибок. После этого, убедившись в отсутствии коллизии на входе, он передает кадр.
* **Коммутация с исключением фрагментов.** Коммутация без буферизации пакетов обеспечивает малое время задержки. Получив 64 байтный заголовок кадра, коммутатор занимает нужный выходной порт и начинает передачу. Обнаружение ошибок при этом не происходит. Коммутация с исключением фрагментов гарантирует, что из источника читается достаточное количество байтов, чтобы обнаружить коллизию до пересылки.

Коммутация с исключением фрагментов - это компромисс между большим временем задержки и гарантией передачи кадра при коммутации с буферизацией, и небольшим временем задержки и риском потери кадра без буферизации пакетов. На практике разница между коммутацией с буферизацией и без буферизации кадров не важна, потому что несущественное уменьшение времени задержки при коммутации без буферизации, возмещается незначительными колебаниями времени ожидания при коммутации с буферизацией.

**4.7.1. Функционирование сетевого коммутатора**

Для каждого порта коммутатор формирует таблицу МАС-адресов, связанных с сегментом, подключенным к порту коммутатора. Затем коммутатор использует эти МАС-адреса при принятии решения о дальнейших операциях над кадрами – фильтрация, пересылка или лавинная рассылка.

Когда порт поступает кадр, коммутатор сравнивает МАС-адрес адресата с адресами в таблицах. Если МАС-адрес получателя кадра находится в том же сегменте сети, что и отправитель, коммутатор сбрасывает кадр. Этот процесс называется фильтрацией, и с его помощью коммутаторы могут значительно уменьшить трафик между сегментами сети. Если МАС-адрес получателя кадра находится в другом сегменте, коммутатор пересылает кадр на порт, к которому подключен соответствующий сегмент. Если у коммутатора *нет* записи об адресе получателя, он передаст кадр всем портам, кроме порта, с которого кадр был получен. Устройство-получатель отвечает на широковещательную рассылку специаьным кадром по адресу отправителя. Коммутатор вводит искомый МАС-адрес получателя и номер соответствующего порта коммутатора в таблицу МАС-адресов. Теперь коммутатор может пересылать кадры между отправителем и получателем без широковещательной рассылки.

**4.7.2. Структурирование трафика**

Коммутируемые СПД КМД – это сегодня самый распространенный тип СПД для локальных сетей. Сегодня цена за порт на коммутаторе уменьшилась настолько, что концентраторы и мосты больше не рассматриваются при принятии решения о покупке сетевого оборудования.

Коммутаторы позволяют структурировать трафик, т.е. разбить его на фрагменты по определенному признаку. Чаще всего – это физическое расположение абонентских машин пользователей. Например, все пользователи, подключенные к коммутатору на первом этаже офисного здания, будут принадлежать одной и той же рабочей группе, в то время как пользователи, подключенные к коммутатору на втором этаже, будут принадлежать к другой рабочей группе. Такая организация позволяет каждой группе обращаться к устройствам в сети, например серверам, с меньшей вероятностью коллизий и повышает общую производительность сети.

## 4.7.3. Сравнение коммутаторов и мостов

Во многом схожие с мостами, сетевые коммутаторы обладают особыми характеристиками, которые делают их эффективным средством снижения перегрузки сетей за счет увеличения фактической полосы пропускания. В этом разделе описываются сходства и различия коммутаторов и мостов.

Сходства мостов и коммутаторов.

* И мосты, и коммутаторы соединяют сегменты СПД КМС.
* И мосты, и коммутаторы используют таблицу МАС-адресов для идентификации сегмента, в который нужно переслать кадр с данными.
* И мосты, и коммутаторы помогают уменьшить сетевой трафик.

Однако коммутаторы предлагают следующие важные функции, которые обеспечивают дополнительные преимущества для устранения коллизий.

* **Выделенный канал связи между устройствами.** Если на каждый порт сетевого коммутатора подключить только линию от одного абонента, это так называемая микросегментация, то каждый пользователь получает доступ к каналу передачи и не конкурирует с другими. В результате коллизии не возникают.
* **Параллельные сеансы связи.** Параллелизмсеансов связи обеспечиваются путем одновременной пересылки нескольких кадров, что увеличивает полосу пропускания сети в соответствии с числом поддерживаемых сеансов связи. Например, когда кадры пересылаются между портами 1 и 2, другой сеанс связи может проходить между портами 5 и 6.
* **Полнодуплексная система связи** После того как подключение микросегментировано, в нем участвуют только коммутатор и подключенный абонент. Теперь можно настроить порт так, чтобы он мог получать и отправлять данные в одно и то же время, т.е.обеспечивать дуплексный канал. Например, соединения 100 Мбит/с типа «точка-точка» обладают скоростью передачи 100 Мбит/с и скоростью приема 100 Мбит/с, что обеспечивает эффективную полосу пропускания 200 Мбит/с на одном соединении. Конфигурация между полудуплексом и дуплексом автоматически согласуется во время создания канала.
* **Адаптация к скорости среды.** Сетевой коммутатор с портами разных скоростей может автоматически выбирать между скоростями 10/100 Мбит/с *или* между 100/1 000 Мбит/с.

**4.8. VLAN – виртуальные сети**

**4.8.1. Основная идея построения виртуальных сетей**

При создании СПД на основе каналов с множественным доступом для локальной сети всем узлам сети доступен широковещательный трафик. Ни концентратор, ни мост, ни коммутатор изначально не ограничивает широковещательный трафик.

Виртуальной сетью LAN называют **[Пахомов]** группу узлов сети, в которой весь трафик, включая и широковещательный, полностью изолирован на канальном уровне от других узлов сети. Это означает, что передача кадров между узлами сети, относящимися к различным виртуальным сетям, на основании адреса канального уровня невозможна (хотя виртуальные сети могут взаимодействовать друг с другом на сетевом уровне с использованием маршрутизаторов). Основным средством структурирования СПД на основе каналов с множественным доступом в виде системы виртуальных сетей являются коммутаторы.

Изолирование отдельных узлов сети на канальном уровне с использованием технологии виртуальных сетей позволяет решать одновременно несколько задач. Во-первых, виртуальные сети способствуют повышению производительности сети, локализуя широковещательный трафик в пределах виртуальной сети. Широковещательные кадры (а также кадры с групповыми и неизвестными адресами) пересылают внутри виртуальной сети, но не между виртуальными сетями. Во-вторых, изоляция виртуальных сетей друг от друга на канальном уровне позволяет повысить безопасность сети, делая часть ресурсов для определенных категорий пользователей недоступной.

**4.8.2**. **Типы виртуальных сетей**

До появления стандарта по организации виртуальных сетей IEEE 802.1Q каждый производитель сетевого оборудования использовал собственную технологию организации VLAN. Такой подход имел существенный недостаток — технологии одного производителя были несовместимы с технологиями других фирм. Поэтому при построении виртуальных сетей на базе нескольких коммутаторов необходимо было использовать только оборудование от одного производителя. Появление стандарта виртуальных сетей IEEE 802.1Q позволило преодолеть проблему несовместимости, однако до сих пор существуют коммутаторы, которые либо не поддерживают стандарт IEEE 802.1Q, либо, кроме возможности организации виртуальных сетей по стандарту IEEE 802.1Q, предусматривают и иные технологии.

Существует несколько способов построения виртуальных сетей, но сегодня в коммутаторах главным образом реализуется технология группировки портов или используется спецификация IEEE 802.1Q.

**4.8.3. Виртуальные сети на основе группировки портов**

Виртуальные сети на основе группировки портов (Port-based) обычно реализуются в так называемых Smart-коммутаторах или в управляемых коммутаторах — как дополнение к возможности организации VLAN на базе стандарта IEEE 802.1Q.

Этот способ создания виртуальных сетей достаточно прост. Каждый порт коммутатора приписывается к той или иной виртуальной сети, то есть порты группируются в виртуальные сети. Адресация кадра в этой сети основывается на MAC-адресе получателя и ассоциированного с ним порта. Если к порту, которому назначена принадлежность к определенной виртуальной сети, например к VLAN#1, подключить ПК пользователя, то этот ПК автоматически будет принадлежать сети VLAN#1. Если же к данному порту подключается коммутатор, то все порты этого коммутатора также будут принадлежать VLAN#1.

При использовании технологии группировки портов один и тот же порт может быть одновременно приписан к нескольким виртуальным сетям, что позволяет реализовывать разделяемые ресурсы между пользователями различных виртуальных сетей. Например, чтобы реализовать совместный доступ к сетевому принтеру или к файл-серверу пользователей виртуальных сетей VLAN#1 и VLAN#2, тот порт коммутатора, к которому подключается сетевой принтер или файл-сервер, нужно приписать одновременно к сетям VLAN#1 и VLAN#2 (рис. 1).

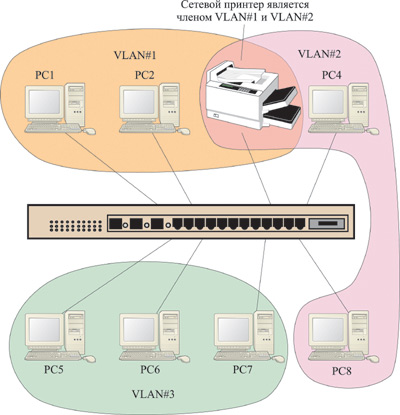


Рис. 1. Создание разделяемого ресурса между несколькими виртуальными сетями с использованием технологии группировки портов

Описываемая технология обладает рядом преимуществ в сравнении с использованием стандарта IEEE 802.1Q, но имеет и свои недостатки.

К достоинствам построения виртуальной сети на основе группировки портов можно отнести простоту конфигурации виртуальных сетей. При этом не требуется, чтобы конечные узлы сети поддерживали стандарт IEEE 802.1Q. При такой организации виртуальных сетей можно создавать разделяемые сетевые ресурсы.

Однако если сеть достаточно крупная и построена на нескольких коммутаторах, то возможности по организации виртуальных сетей на основе группировки портов имеют существенные ограничения. Прежде всего, эта технология ограничивает возможности по наращиванию как числа VLAN, так и количество узлов к каждой виртуальной сети. В большинстве случаев эта технология ограничивается лишь одним коммутатором.

Рассмотрим для примера ситуацию, когда сеть построена на базе двух коммутаторов, поддерживающих технологию организации виртуальных сетей на основе группировки портов (рис. 2).

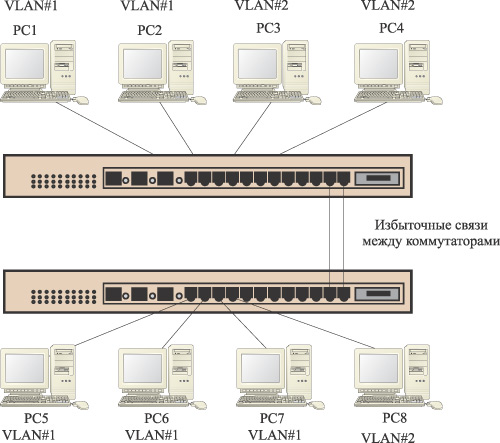


Рис. 2. Реализация виртуальных сетей на основе группировки портов при использовании двух коммутаторов

Пусть необходимо, чтобы часть портов первого и второго коммутаторов относилась к VLAN#1, а другая часть — к VLAN#2. Для этого нужно, во-первых, чтобы оба коммутатора позволяли не только организовывать виртуальные сети на основе группировки портов, но и распространять такие сети на несколько коммутаторов (подобная функция реализована далеко не у всех коммутаторов), во-вторых, чтобы между коммутаторами было установлено столько физических соединений, сколько создано виртуальных сетей. Рассмотрим два шестипортовых коммутатора. Пусть в первом коммутаторе порты 1 и 2 относятся к VLAN#1, а порты 3 и 4 — к VLAN#2; во втором коммутаторе порты 1, 2 и 3 относятся к VLAN#1, а порт 4 — к VLAN#2. Чтобы пользователи VLAN#1 первого коммутатора могли общаться с пользователями VLAN#1 второго коммутатора, эти коммутаторы должны быть связаны между собой портами, относящимися к VLAN#1 (например, порт 5 первого и второго коммутаторов необходимо приписать к VLAN#1). Аналогично, для общения пользователей VLAN#2 первого коммутатора с пользователями VLAN#2 второго коммутатора следует связать эти коммутаторы через порты, приписанные к VLAN#2 (это могут быть порты 6 на обоих коммутаторах). Таким образом, проблема наращивания числа виртуальных сетей на основе технологии группировки портов решается (правда, не во всех случаях) за счет установления избыточных связей между коммутаторами.

**4.8.4.** **Виртуальные сети на основе стандарта IEEE 802.1Q**

В виртуальных сетях, основанных на стандарте IEEE 802.1Q, информация о принадлежности передаваемых Ethernet-кадров к той или иной виртуальной сети встраивается в сам передаваемый кадр. Таким образом, стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети.

К кадру Ethernet добавляется метка (Tag) длиной 4 байта — такие кадры называют кадрами с метками (Tagged frame). Дополнительные биты содержат информацию по принадлежности кадра Ethernet к виртуальной сети и о его приоритете (рис. 3).

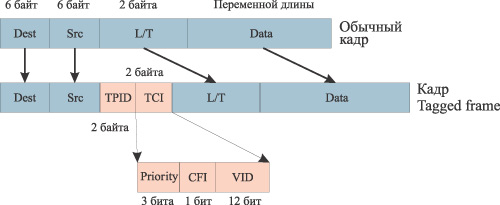


Рис. 3. Сравнение обычного Ethernet-кадра и кадра с меткой

Добавляемая метка кадра включает в себя двухбайтовое поле TPID (Tag Protocol Identifier) и двухбайтовое поле TCI (Tag Control Information). Поле TCI, в свою очередь, состоит из полей Priority, CFI и VID. Поле Priotity длиной 3 бита задает восемь возможных уровней приоритета кадра. Поле VID (VLAN ID) длиной 12 бит является идентификатором виртуальной сети. Эти 12 бит позволяют определить 4096 различных виртуальных сетей, однако идентификаторы 0 и 4095 зарезервированы для специального использования. Поэтому всего в стандарте 802.1Q возможно определить 4094 виртуальные сети. Поле CFI (Canonical Format Indicator) длиной 1 бит зарезервировано для обозначения кадров СПД других типов (например, FDDI, см. раздел 5.2), передаваемых по магистрали Ethernet, и для кадров Ethernet всегда равно 0.

Изменение формата кадра Ethernet приводит к тому, что сетевые устройства, не поддерживающие стандарт IEEE 802.1Q (такие устройства называют Tag-unaware), не могут работать с кадрами, в которые вставлены метки, а сегодня подавляющее большинство сетевых устройств (в частности, сетевые Ethernet-контроллеры конечных узлов сети) не поддерживают этот стандарт. Поэтому для обеспечения совместимости c устройствами, поддерживающими стандарт IEEE 802.1Q (Tag-aware-устройства), коммутаторы стандарта IEEE 802.1Q должны поддерживать как традиционные Ethernet-кадры, то есть кадры без меток (Untagged), так и кадры с метками (Tagged).

Входящий и исходящий трафики, в зависимости от типа источника и получателя, могут быть образованы и кадрами типа Tagged, и кадрами типа Untagged — только в этом случае можно достигнуть совместимости с внешними по отношению к коммутатору устройствами. Трафик же внутри коммутатора всегда образуется пакетами типа Tagged. Поэтому для поддержки различных типов трафиков и для того, чтобы внутренний трафик коммутатора образовывался из пакетов Tagged, на принимаемом и передающем портах коммутатора кадры должны преобразовываться в соответствии с предопределенными правилами.

**4.8.4.1. Правила входящего порта (Ingress rules)**

Рассмотрим более подробно процесс передачи кадра через коммутатор (рис. 4). По отношению к трафику каждый порт коммутатора может быть как входным, так и выходным. После того как кадр принят входным портом коммутатора, решение о его дальнейшей обработке принимается на основании предопределенных правил входного порта (Ingress rules). Поскольку принимаемый кадр может относиться как к типу Tagged, так и к типу Untagged, то правилами входного порта определяется, какие типы кадров должны приниматься портом, а какие отфильтровываться. Возможны следующие варианты: прием только кадров типа Tagged, прием только кадров типа Untagged, прием кадров обоих типов. По умолчанию для всех коммутаторов правилами входного порта устанавливается возможность приема кадров обоих типов.



Рис.4. Процесс продвижения кадров в коммутаторе, совместимом со стандартом IEEE 802.1Q

Если правилами входного порта определено, что он может принимать кадр Tagged, в котором имеется информация о принадлежности к конкретной виртуальной сети (VID), то этот кадр передается без изменения. А если определена возможность работы с кадрами типа Untagged, в которых не содержится информации о принадлежности к виртуальной сети, то прежде всего такой кадр преобразуется входным портом коммутатора к типу Tagged (напомним, что внутри коммутатора все кадры должны иметь метки о принадлежности к виртуальной сети).

Чтобы такое преобразование стало возможным, каждому порту коммутатора присваивается уникальный PVID (Port VLAN Identifier), определяющий принадлежность порта к конкретной виртуальной сети внутри коммутатора (по умолчанию все порты коммутатора имеют одинаковый идентификатор PVID=1). Кадр типа Untagged преобразуется к типу Tagged, для чего дополняется меткой VID. Значение поля VID входящего Untagged-кадра устанавливается равным значению PVID входящего порта, то есть все входящие Untagged-кадры автоматически приписываются к той виртуальной сети внутри коммутатора, к которой принадлежит входящий порт.

**Правила продвижения пакетов (Forwarding Process)**

После того как все входящие кадры отфильтрованы, преобразованы или оставлены без изменения в соответствии в правилами входящего порта, решение об их передаче к выходному порту основывается на предопределенных правилах продвижения пакетов. Правило продвижения пакетов внутри коммутатора заключается в том, что пакеты могут передаваться только между портами, ассоциированными с одной виртуальной сетью. Как уже отмечалось, каждому порту присваивается идентификатор PVID, который используется для преобразования принимаемых Untagged-кадров, а также для определения принадлежности порта к виртуальной сети внутри коммутатора с идентификатором VID=PVID. Таким образом, порты с одинаковыми идентификаторами внутри одного коммутатора ассоциируются с одной виртуальной сетью. Если виртуальная сеть строится на базе одного коммутатора, то идентификатора порта PVID, определяющего его принадлежность к виртуальной сети, вполне достаточно. Правда, создаваемые таким образом сети не могут перекрываться, поскольку каждому порту коммутатора соответствует только один идентификатор. В этом смысле создаваемые виртуальные сети не обладали бы такой гибкостью, как виртуальные сети на основе портов. Однако стандарт IEEE 802.1Q с самого начала задумывался для построения масштабируемой инфраструктуры виртуальных сетей, включающей множество коммутаторов, и в этом состоит его главное преимущество по сравнению с технологией образования VLAN на основе портов. Но для того, чтобы расширить сеть за пределы одного коммутатора, одних идентификаторов портов недостаточно, поэтому каждый порт может быть ассоциирован с несколькими виртуальными сетями, имеющими различные идентификаторы VID.

Если адрес назначения пакета соответствует порту коммутатора, который принадлежит к той же виртуальной сети, что и сам пакет (могут совпадать VID пакета и VID порта или VID пакета и PVID порта), то такой пакет может быть передан. Если же передаваемый кадр принадлежит к виртуальной сети, с которой выходной порт никак не связан (VID пакета не соответствует PVID/VID порта), то кадр не может быть передан и отбрасывается.

**Правила выходного порта (Egress rules)**

После того как кадры внутри коммутатора переданы на выходной порт, их дальнейшее преобразование зависит от правил выходного порта. Как уже говорилось, трафик внутри коммутатора создается только пакетами типа Tagged, а входящий и исходящий трафики могут быть образованы пакетами обоих типов. Соответственно правилами выходного порта (правило контроля метки — Tag Control) определяется, следует ли преобразовывать кадры Tagged к формату Untagged.

Каждый порт коммутатора может быть сконфигурирован как Tagged или Untagged Port. Если выходной порт определен как Tagged Port, то исходящий трафик будет создаваться кадрами типа Tagged с информацией о принадлежности к виртуальной сети. Следовательно, выходной порт не меняет тип кадров, оставляя их такими же, какими они были внутри коммутатора. К указанному порту может быть подсоединено только устройство, совместимое со стандартом IEEE 802.1Q, например коммутатор или сервер с сетевой картой, поддерживающей работу с виртуальными сетями данного стандарта.

Если же выходной порт коммутатора определен как Untagged Port, то все исходящие кадры преобразуются к типу Untagged, то есть из них удаляется дополнительная информация о принадлежности к виртуальной сети. К такому порту можно подключать любое сетевое устройство, в том числе коммутатор, не совместимый со стандартом IEEE 802.1Q, или ПК конечных клиентов, сетевые карты которых не поддерживают работу с виртуальными сетями этого стандарта.