**Коммутаторы канального уровня**

До сих пор мы специально не уточняли, что именно делает коммута­тор и как он работает. Задача коммутатора — получать входящие кадры канального уровня и передавать их по исходящим каналам. Сейчас мы подробно изучим эту функцию перенаправления. Мы убедимся, что коммутатор как таковой является **прозрачным** для хо­стов и маршрутизаторов, работающих в подсети. Это означает, что хост или маршрутизатор адресуют кадр для другого хоста или маршрутиза­тора (а не для коммутатора) и спокойно отсылают этот кадр по локаль­ной сети, не учитывая этап работы коммутатора, который получит кадр и переадресует его. Скорость, с которой кадры поступают на любой из выходных интерфейсов коммутатора, иногда может превышать произ­водительность канала, подключенного к этому интерфейсу. Чтобы спра­виться с этой проблемой, выходные интерфейсы коммутатора снабжены буферами — точно так же, как выходные интерфейсы маршрутизатора имеют буферы для хранения дейтаграмм. Итак, давайте подробнее озна­комимся с функционированием коммутатора.

**Перенаправление данных и фильтрация**

**Фильтрацией** называют способность коммутатора определять, сле­дует ли передать кадр определенному интерфейсу или его можно про­сто отбросить. **Перенаправлением данных** называют способность ком­мутаторов определять, какому из интерфейсов следует направить кадр. Фильтрация и перенаправление кадров осуществляются при помощи **таблицы коммутации.** В таблице коммутации содержатся записи для некоторых (не обязательно всех) узлов локальной сети. Каждая запись таблицы коммутации содержит, во-первых, МАС-адрес узла, во-вторых, номер интерфейса коммутатора, ведущего к узлу, и, в-третьих, время включения этой информации в таблицу Пример таблицы для само­го верхнего коммутатора, представленного на рис. 5.15, приведен на рис. 5.22.

|  |  |  |
| --- | --- | --- |
| **Адрес** | **Интерфейс** | **Время** |
| 62-FE-F7-11-89-A3 | 1 | 9:32 |
| 7С-ВА-В2-В4-91-10 | 3 | 9:36 |
| **• ••** | **...** | **...** |

**Рис. 5.22. Часть таблицы для самого верхнего коммутатора, изображенного**

**на рис. 5.15**

Хотя представленное здесь описание механизмов перенаправления кадра может напомнить описание перенаправления дейтаграмм, мы вскоре обнаружим существенные различия. Следует отметить, что коммутаторы используют МАС-адреса, а не адреса сетевого уровня (например, IP-адреса). Мы также вскоре увидим, что процесс форми­рования таблицы коммутации значительно отличается от построения таблицы маршрутизации.

Чтобы понять механизмы фильтрации и перенаправления, предпо­ложим, что на коммутатор поступает кадр с адресом получателя DD-DD-DD-DD-DD-DD по интерфейсу *х.* Коммутатор делает выборку из своей таблицы по МАС-адресу. Далее возможны три случая:

• В таблице нет записи, соответствующей DD-DD-DD-DD-DD-DD. В таком случае коммутатор переправляет копии кадра во *все* выход­ные буферы, расположенные на всех интерфейсах, кроме *х.* Иными словами, если запись для адреса назначения отсутствует, то комму­татор передает кадр широковещательным образом.

* В таблице есть запись, ассоциирующая DD-DD-DD-DD-DD-DD с интерфейсом *х.* В данном случае сегмент приходит из сегмента ЛВС, содержащего адаптер DD-DD-DD-DD-DD-DD. He требует­ся перенаправлять кадр на какие-либо другие интерфейсы, поэтому коммутатор выполняет фильтрацию, просто отбрасывая этот кадр.
* В таблице есть запись, ассоциирующая DD-DD-DD-DD-DD-DD с интерфейсом ***у*** *ф х.* В таком случае кадр должен быть переправлен в тот сегмент локальной сети, который ассоциирован с интерфейсом *у.* Коммутатор выполняет функцию перенаправления, помещая кадр в выходной буфер, предшествующий интерфейсу г/.

Рассмотрим работу этих правил на примере самого верхнего комму­татора с рис. 5.15 и его таблицы коммутации, показанной на рис. 5.22. Предположим, что кадр с адресом получателя 62-FE-F7-11-89-A3 при­бывает на коммутатор через интерфейс 1. Коммутатор сверяется с та­блицей и определяет, что получатель находится в сегменте локальной сети, соединенном с интерфейсом 1 (то есть в локальной сети электро­технического факультета). Это означает, что данный кадр уже получили все хосты этой локальной сети, поэтому коммутатор отфильтровывает (то есть отбрасывает) его. Теперь предположим, что кадр с тем же адре­сом получателя прибывает на коммутатор по интерфейсу 2. Коммута­тор снова заглядывает в таблицу и видит, что адресат доступен через ин­терфейс 1. Поэтому коммутатор переправляет кадр в выходной буфер интерфейса 1. Из этого примера должно быть ясно, что, пока таблица коммутатора содержит полную и точную информацию, коммутатор до­ставляет кадры хостам-получателям, не прибегая к широковещанию.

В этом отношении коммутатор гораздо «интеллектуальнее» концен­тратора. Но каким же образом конфигурируется таблица коммутатора? Существуют ли на канальном уровне аналоги протоколов маршрутиза­ции сетевого уровня? Либо несчастный менеджер должен выкраивать время и конфигурировать таблицу коммутации вручную?

**Самообучение**

Коммутатор обладает замечательным свойством (особенно для пе­ретрудившегося администратора), состоящим в том, что его таблица формируется автоматически, динамически и автономно — без вмешательства администратора вычислительной сети или протокола конфи­гурирования. Другими словами, коммутаторы обладают способностью **самообучения,** которая реализуется следующим образом.

1. Изначально таблица коммутатора пуста.
2. Для каждого полученного кадра коммутатор сохраняет в своей та­блице, во-первых, МАС-адрес, содержащийся в *поле адреса отпра­вителя* кадра, во-вторых, номер интерфейса, по которому прибыл кадр, в-третьих, время получения кадра. Таким образом, коммутатор сохраняет в своей таблице сведения о том, в каком сегменте локаль­ной сети располагается узел, отправивший кадр. Если каждый узел локальной сети передаст по кадру, тогда в таблице коммутации ока­жутся МАС-адреса всех узлов.
3. Если за определенный период времени **(время старения)** коммута­тор не получает кадров с некоторым адресом, этот адрес удаляется из таблицы. Таким образом, если один персональный компьютер в сети заменяется другим (с другим адаптером), локальный адрес первого персонального компьютера в конце концов будет удален из таблицы коммутации.

Рассмотрим способность к самообучению на примере самого верх­него коммутатора с рис. 5.15 и его таблицы коммутации, показанной на рис. 5.22. Пусть в момент времени 9:39 кадр с адресом источника 01-12-23-34-45-56 прибывает по интерфейсу 2. Предположим, что этот адрес отсутствует в таблице. В таком случае коммутатор добавляет к таблице новую запись (рис. 5.23).

|  |  |  |
| --- | --- | --- |
| **Адрес** | **Интерфейс** | **Время** |
| 01-12-23-34-45-56 | 2 | 9:39 |
| 62-FE-F7-11-89-A3 | 1 | 9:32 |
| 7С-ВА-В2-В4-91-10 | 3 | 9:36 |
| **...** | **• ••** | **...** |

**Рис. 5.23. Коммутатор узнает о местоположении адаптера с адресом**

**01-12-23-34-45-56**

Продолжая данный пример, предположим, что время старения для коммутатора составляет 60 минут и между 9:32 и 10:32 на коммутатор не поступают кадры с адресом источника 62-FE-F7-11-89-A3. В таком случае, в 10:32 коммутатор удаляет этот адрес из своей таблицы.

Коммутаторы являются **самонастраивающимися устройствами,**

и для их запуска не требуется вмешательство администратора вычисли­тельной сети или пользователя. Администратор, желающий установить коммутатор, должен просто подключить сегменты локальной сети к ин­терфейсам коммутатора. Специалисту не приходится конфигурировать таблицы коммутатора на этапе установки или при удалении хоста из одного из сегментов локальной сети. Кроме того, коммутаторы являют­ся полнодуплексными: это означает, что любой интерфейс коммутатора может одновременно как отправлять, так и получать информацию.

**Свойства коммутации на канальном уровне**

Описав общие принципы работы коммутатора канального уровня, рассмотрим его особенности и свойства. Можно перечислить ряд пре­имуществ, связанных с использованием коммутаторов, а не устройств с широковещательными каналами — таких как шины или звездообраз­ные топологии с применением концентратора:

* *Устранение коллизий.* Если локальная сеть построена с применени­ем коммутаторов (а не концентраторов), полоса передачи данных совершенно не расходуется впустую, так как в ней не возникает кол­лизий! Коммутаторы буферизуют кадры и никогда не передают бо­лее одного кадра в определенный сегмент сети в конкретный момент времени. Как и при работе с маршрутизатором, максимальная сово­купная пропускная способность коммутатора равна суммарной ча­стоте всех интерфейсов коммутатора. Следовательно, коммутаторы позволяют существенно увеличить производительность локальной сети по сравнению с использованием широковещательных каналов.
* *Гетерогенные каналы.* Поскольку коммутатор изолирует кана­лы друг от друга, разные каналы в локальной сети могут работать с разной скоростью и находиться на разных носителях. Например, у самого верхнего коммутатора на рис. 5.22 может быть три кана­ла 1000ВASE-T с медными кабелями, скорость передачи каждого 1 Гбит/с, два канала 100BASE-FX с оптоволоконными кабелями, скорость передачи — по 100 Мбит/с, а также один канал с медным кабелем, стандарт 100BASE-T. Такой коммутатор идеально подхо­дит для одновременного использования в сети как устаревающего, так и современного оборудования.
* *Управление.* Наряду с обеспечением повышенной безопасности, коммутатор также упрощает управление сетью. Например, если адаптер выходит из строя и на­чинает непрерывно посылать Ethernet-кадры (такой адаптер иногда называют «болтливым»), коммутатор может выявить эту пробле­му и на внутрисистемном уровне отключить данный адаптер. Рас­полагая такой возможностью, администратор вычислительной сети может спать спокойно, а не вскакивать с постели среди ночи и не лететь на работу, чтобы исправить ситуацию. Аналогично, если об­резать кабель, то отключится лишь тот хост, который был подсоеди­нен этим кабелем к коммутатору. Во времена коаксиальных кабелей многим администраторам вычислительной сети приходилось тра­тить целые часы, «проходя по линии» (точнее говоря, «проползая по полу»), чтобы отыскать повреждение кабеля, из-за которого легла вся сеть. Позднее мы поговорим и о том, что коммутаторы собирают статистику об использовании полосы передачи данных, частоте воз­никновения коллизий и типах трафика, предоставляя всю эту ин­формацию администратору вычислительной сети. Все эти сведения могут использоваться для отладки и устранения проблем, а также для планирования развития локальной сети. Существуют исследо­вания, рассматривающие возможности дальнейшего расширения управляющих функций в локальных сетях Ethernet, которые уже реализуются в пилотных конфигурациях.

**О БЕЗОПАСНОСТИ**

**Анализ коммутируемой локальной сети: отравление коммутатора**

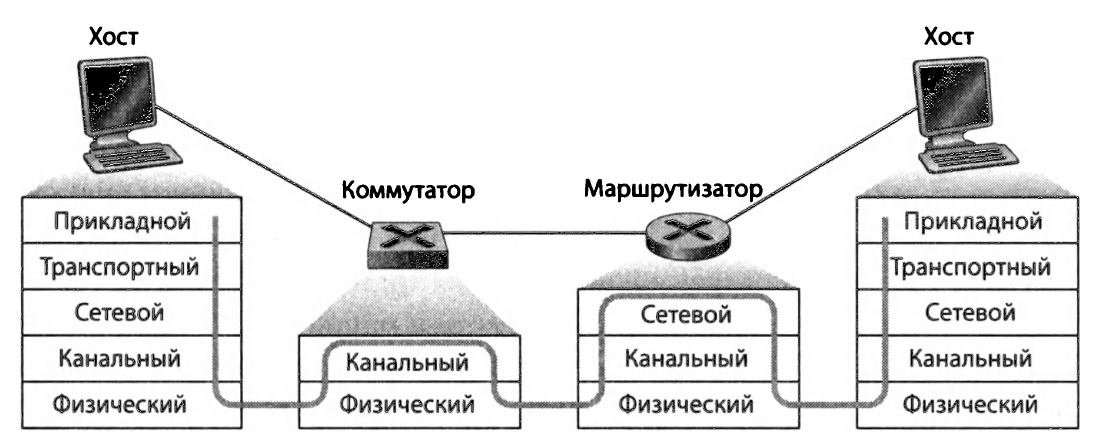
Когда хост подключается к коммутатору, он, как правило, получа­ет только те кадры, которые предназначены именно ему. Вернем­ся, например, к коммутируемой локальной сети, изображенной на рис. 5.17. Когда хост А отправляет кадр хосту Б, а в таблице ком­мутации есть запись для хоста Б, коммутатор направит этот кадр только хосту Б. Если на хосте В это время будет работать анализа­тор, то хост В сможет просмотреть содержимое пакета, идущего от А к Б. Соответственно, в среде коммутируемой локальной сети (в отличие от широковещательной локальной сети, такой, как 802.11 LAN или Ethernet-сети на основе концентратора) злоумышленнику сложнее анализировать кадры таким образом. Однако, поскольку коммутатор широковещательно передает кадры с адресами на­значения, отсутствующими в таблице коммутации, анализатор на хосте В все-таки может просмотреть некоторые кадры, которые не предназначены самому В. Более того, анализатор сможет просматривать и широковещательные кадры Ethernet, имеющие ши­роковещательный адрес назначения FF-FF-FF-FF-FF-FF. Широко известная разновидность атак в коммутируемых сетях называется **отравлением коммутатора.** При такой тактике на коммутатор на­правляется масса пакетов со множеством разных фиктивных МАС-адресов. В результате таблица коммутатора быстро заполняется такими фиктивными адресами до отказа, и в ней не остается места для МАС-адресов настоящих хостов. В результате коммутатор на­чинает передавать большую часть кадров широковещательным об­разом, и анализатор легко их просматривает. Однако, посколь­ку такая атака является достаточно сложной даже для опытного злоумышленника, коммутаторы значительно менее уязвимы для несанкционированного сетевого анализа, нежели концентраторы и беспроводные локальные сети.

**Сравнение коммутаторов и маршрутизаторов**

Как мы узнали ранее, маршрутизатор — это устройство для ком­мутации пакетов, которое работает с промежуточным хранением и пе­ремещает пакеты, опираясь на адресацию сетевого уровня. Хотя ком­мутатор также обеспечивает передачу с промежуточным хранением, он принципиально отличается от маршрутизатора тем, что при перена­правлении пакетов использует их МАС-адреса. Итак, маршрутизатор осуществляет коммутацию пакетов на третьем уровне, а коммутатор — на втором.

Пусть между маршрутизаторами и коммутаторами и существуют фундаментальные отличия, администратору вычислительной сети зача­стую приходится выбирать одно из устройств, которое должно служить в сети соединительным узлом. Например, в сети с рис. 5.15 администра­тор вычислительной сети вполне мог бы установить маршрутизатор, а не коммутатор, соединив с его помощью факультетские локальные сети, серверы и шлюз, стоящий на границе локальной сети и Интерне­та. Действительно, маршрутизатор мог бы обеспечивать обмен инфор­мацией между факультетами без возникновения коллизий. Итак, если сетевые взаимодействия можно обеспечивать как при помощи комму­таторов, так и с применением маршрутизаторов, то каковы достоинства и недостатки каждого из этих подходов?

Сначала поговорим о коммутаторах. Как было указано выше, ком­мутаторы являются самонастраивающимися устройствами — за что их так обожают вечно занятые администраторы вычислительной сети во всем мире. Кроме того, коммутаторы могут достаточно быстро выпол­нять фильтрацию и перенаправление данных. Как показано на рис. 5.24, коммутатору приходится обрабатывать кадры лишь до второго уровня, а маршрутизатор обрабатывает дейтаграммы до третьего уровня. С дру­гой стороны, для предотвращения зацикливания широковещательных кадров активная топология коммутируемой сети ограничена связую­щим деревом. Кроме того, в больших коммутируемых сетях нужны объ­емные ARP-таблицы на хостах и маршрутизаторах, из-за чего будет ге­нерироваться существенный ARP-трафик, нуждающийся в обработке. Вдобавок коммутаторы очень чувствительны к широковещательным штормам. Если какой-нибудь хост «спятит» и начнет генерировать бес­конечный поток Ethernet-кадров, то коммутаторы будут транслировать все эти кадры, из-за чего сеть просто рухнет.

****

**Рис. 5.24. Обработка пакетов на коммутаторах, маршрутизаторах и хостах**

Теперь рассмотрим достоинства и недостатки маршрутизаторов. Поскольку адресация на сетевом уровне зачастую является иерархи­ческой (а не плоской, как в случае с МАС-адресами), пакеты обычно не движутся через маршрутизатор циклически, даже если в сети есть дублирующие пути. Конечно, такое зацикливание пакетов может про­исходить, если таблицы маршрутизаторов сконфигурированы непра­вильно. Однако протокол IP применяет специальное поле заголовка дейтаграммы, которое позво­ляет ограничить такую цикличность. Следовательно, возможные пути пакетов не ограничиваются связующим деревом, пакет выбирает опти­мальную траекторию между исходным и конечным хостом. Поскольку маршрутизаторы не имеют ограничений, обусловленных связующим деревом, они позволяют выстраивать в Интернете очень насыщенную топологию, которая включает в себя, в частности, множество активных каналов между Европой и Северной Америкой. Еще одна особенность маршрутизаторов заключается в том, что они обеспечивают защиту от широковещательных штормов второго уровня, применяя для этого брандмауэр. Вероятно, самый серьезный недостаток маршрутизато­ров заключается в том, что их приходится настраивать вручную — не­обходимо конфигурировать IP-адреса как для маршрутизаторов, так и для подключенных к ним хостов. Кроме того, маршрутизатор обычно тратит больше времени на обработку одного пакета, чем коммутатор, поскольку ему приходится оперировать полями вплоть до третьего уровня.

Учитывая, что и коммутаторов, и у маршрутизаторов есть свои до­стоинства и недостатки (см. табл. 5.1), попробуем разобраться: в каких случаях сеть организации (например, университетская или корпора­тивная) должна использовать коммутаторы, а в каких — маршрутиза­торы? Как правило, если сеть невелика и включает в себя несколько сотен хостов, то и LAN-сегментов в ней немного. Такая сеть вполне может обслуживаться лишь коммутаторами, поскольку они локализу­ют трафик и повышают суммарную пропускную способность, не тре­буя никакой дополнительной конфигурации IP-адресов. Но если мы имеем дело с большой сетью, количество хостов в которой исчисля­ется тысячами, то в ней, как правило, есть и маршрутизаторы (наряду с коммутаторами). Маршрутизаторы обеспечивают более надежное разграничение трафика, справляются с широковещательными штор­мами и более интеллектуально прокладывают маршруты между хо­стами в сети.

**Табл. 5.1**. Сравнение важнейших возможностей распространенных устройств, обеспечивающих сетевые взаимодействия

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Концентраторы** | **Маршрутизаторы** | **Коммутаторы** |
| Изоляция трафика | **Нет** | **Да** | **Да** |
| Самонастройка | **Да** | Нет | **Да** |
| Оптимальная маршрутизация | **Нет** | **Да** | Нет |

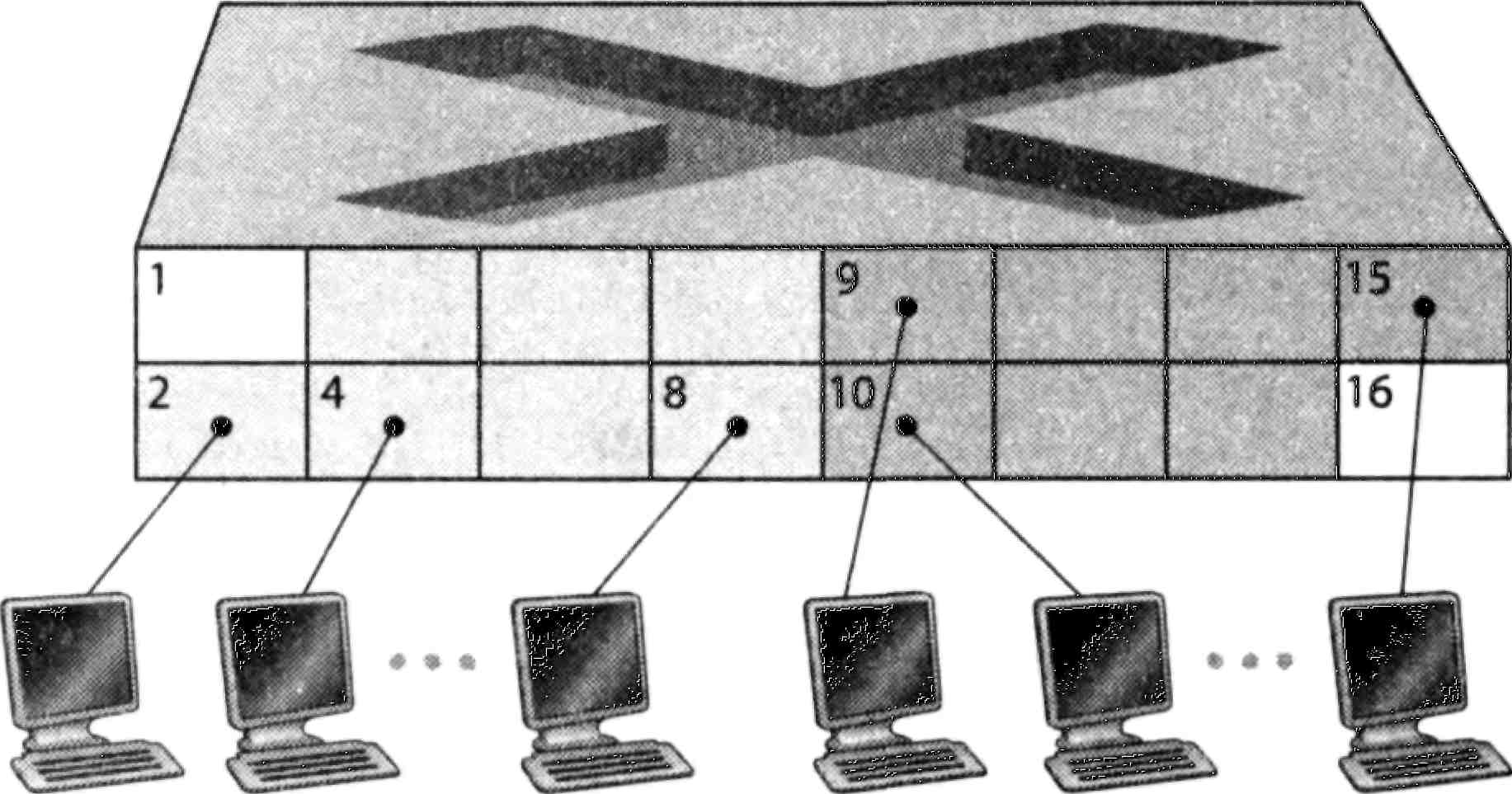
Более подробно достоинства и недостатки сетей с коммутаторами и маршрутизаторами рассмотрены в работах Мейерса и Кима. Здесь также затрагивается тема того, как можно усовершенствовать техноло­гию LAN, чтобы количество хостов в локальных сетях удалось увели­чить на два порядка по сравнению с сегодняшним уровнем.

**Виртуальные локальные сети**

Выше, обсуждая рис. 5.15, мы уже отмечали, что современные ком­пьютерные сети организаций зачастую имеют иерархическую конфигура­цию. В каждой рабочей группе (отделе или факультете) есть собственная коммутируемая локальная сеть, соединенная с коммутируемыми локаль­ными сетями других отделов при помощи иерархической структуры из коммутаторов. В идеальном мире такая конфигурация должна функцио­нировать превосходно, но на практике все зачастую складывается иначе. В конфигурации сети с рис. 5.15 можно отметить три недостатка:

* *Отсутствует изоляция трафика.* Хотя иерархия и позволяет огра­ничить групповой трафик в пределах одного коммутатора, широкове­щательный трафик (то есть, кадры с ARP- или DHCP-сообщениями, либо кадры, чье место назначения еще не известно самообучающе­муся коммутатору) по-прежнему должны обходить всю сеть орга­низации. Ограничив область действия такого широковещательного трафика, мы сможем улучшить производительность локальной сети. Что еще важнее, иногда желательно ограничивать широковещатель­ный трафик локальной сети по соображениям безопасности/конфи­денциальности. Так, если к одной группе относятся менеджеры выс­шего звена данной компании, а к другой — недовольные сотрудники, применяющие анализаторы пакетов Wireshark, то администратору вычислительной сети стоит принять меры, чтобы трафик руководи­телей ни в коем случае не попадал на компьютеры таких сомнитель­ных подчиненных. Чтобы обеспечить изоляцию такого типа, можно заменить центральный коммутатор на рис. 5.15 маршрутизатором. Чуть ниже мы убедимся, что такое ограничительное решение реали­зуемо и при помощи одних лишь коммутаторов (на уровне 2).
* *Неэффективное использование коммутаторов.* Если бы в организа­ции было не 3 группы, а 10, то потребовалось бы 10 коммутаторов первого уровня. Если бы каждая из этих групп была невелика — ска­жем, включала бы по 10 человек, — то хватило бы всего одного ком­мутатора на 96 портов, чтобы удовлетворить потребности каждого, однако такой коммутатор не обеспечивал бы изоляцию каналов.
* *Управление пользователями.* Если тот или иной сотрудник может переходить из одной группы в другую, то на рис. 5.15 придется ме­нять физическую прокладку кабелей, чтобы подключить сотрудни­ка к другому коммутатору. Если сотрудник может одновременно от­носиться к двум группам, проблема тем более усложняется.

К счастью, все эти проблемы решаются при помощи коммутато­ра, поддерживающего **виртуальные локальные сети** (virtual local area networks, **VLAN).** Как понятно из названия, такой коммутатор позволя­ет определять множество *виртуальных* частных сетей в пределах одной *физической* инфраструктуры. Хосты в рамках виртуальной локальной сети взаимодействуют так, как если бы они (и только они) были под­ключены к одному коммутатору. В виртуальной локальной сети на основе портов порты (интерфейсы) коммутатора делятся на группы ад­министратором вычислительной сети. Каждая такая группа представля­ет собой виртуальную локальную сеть, причем порты каждой образуют широковещательный домен (это означает, что широковещательный тра­фик с любого порта из группы будет попадать только на другие порты этой же группы). На рис. 5.25 показан один коммутатор с 16 портами.



Электротехнический Факультет информатики

факультет (порты VLAN 9-15)

(порты VLAN 2-8)

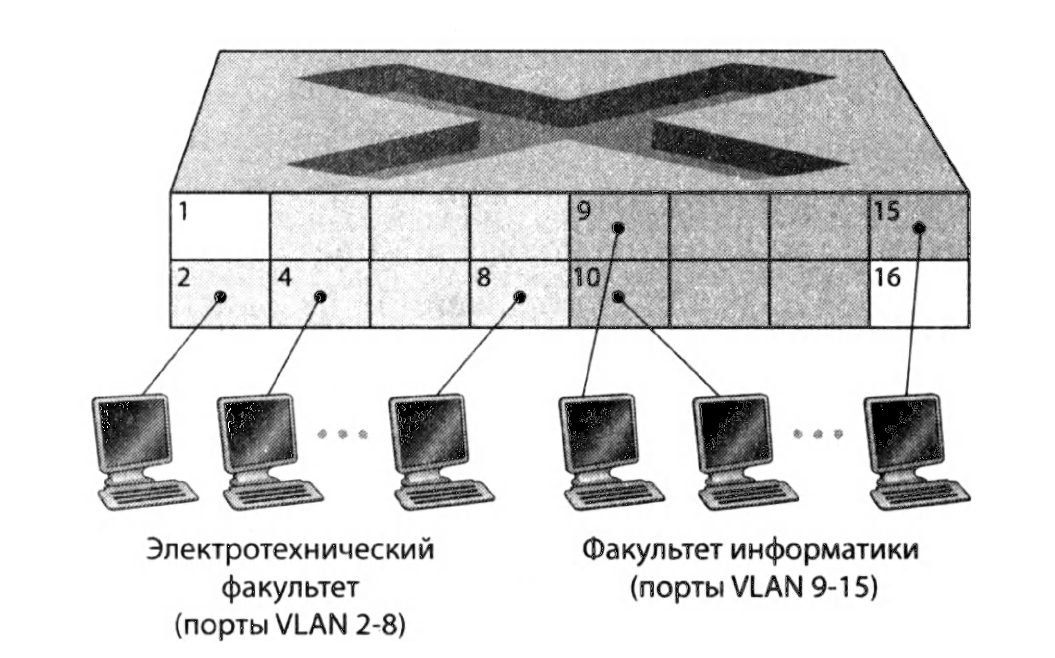
**Рис. 5.25. Один коммутатор, на котором сконфигурированы две виртуальные**

**локальные сети**

Порты 2-8 относятся к виртуальной локальной сети электротехни­ческого факультета, порты 9-15 относятся к виртуальной локальной сети факультета информатики (порты 1 и 16 к локальным сетям не от­носятся). Виртуальная локальная сеть решает все проблемы, обозна­ченные выше: кадры из локальных сетей двух факультетов будут изо­лированы друг от друга, два коммутатора с рис. 5.15 заменяются одним, а если пользователь с порта 8 переходит на факультет информатики, то администратор вычислительной сети просто переконфигурирует про­граммное обеспечение VLAN так, чтобы порт 8 относился к виртуальной локальной сети факультета информатики. Не составляет труда предста­вить себе, как конфигурируется и работает коммутатор VLAN. Адми­нистратор вычислительной сети объявляет, что порт относится к той или иной виртуальной локальной сети (причем те порты, которые не присвоены той или иной сети явно, считаются портами виртуальной ло­кальной сети, заданной по умолчанию). Это делается при помощи про­граммы для управления коммутатором. В коммутаторе ведется таблица, в которой записываются соответствия между портами и виртуальными локальными сетями. Аппаратная часть коммутатора просто доставляет кадры между портами, относящимися к одной и той же виртуальной ло­кальной сети.

Но добившись полного разграничения двух виртуальных локальных сетей, мы столкнулись с новой сложностью. Как теперь передать трафик с электротехнического факультета на факультет информатики? Воз­можное решение — подключить один из портов коммутатора, обслужи­вающего виртуальную локальную сеть (например, порт 1 на рис. 5.25) к внешнему маршрутизатору и сконфигурировать этот порт как от­носящийся к виртуальным локальным сетям сразу двух факультетов. В данном случае, хотя электротехнический факультет и факультет ин­форматики и станут физически использовать один и тот же коммутатор, логическая конфигурация будет такова, как если бы у этих факультетов имелись отдельные коммутаторы, соединенные через маршрутизатор. IP-дейтаграмма, идущая с электротехнического факультета на факуль­тет информатики, сначала пройдет через VLAN электротехнического факультета, чтобы попасть на маршрутизатор, а затем маршрутизатор перешлет ее в виртуальную локальную сеть факультета информатики, на нужный хост с этого факультета. К счастью, производители коммута­торов облегчают администратору вычислительной сети создание таких конфигураций, конструируя единое устройство, в котором есть *и* ком­мутатор VLAN, *и* маршрутизатор, поэтому отдельный внешний марш­рутизатор не требуется. В одной из задач для самостоятельной работы к этой главе мы исследуем подобный сценарий более детально.

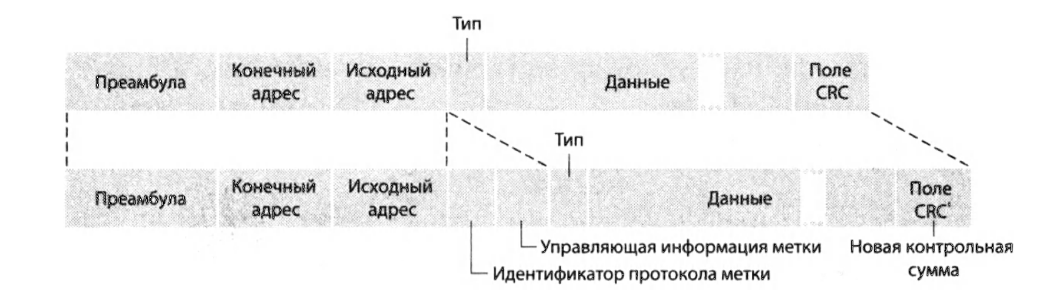
Возвращаясь к рис. 5.15, предположим, что у нас нет отдельного факультета системного проектирования, зато отдельные кафедры элек­тротехнического факультета и факультета информатики расположены в разных корпусах, где им (конечно!) требуется доступ в сеть, причем кафедры одного факультета должны относиться к его общей вирту­альной локальной сети. На рис. 5.26 показан еще один коммутатор на 8 портов, и его порты по мере необходимости назначаются как элементы разных виртуальных локальных сетей — электротехнического факуль­тета или факультета информатики. Но как же подключить друг к другу два этих коммутатора? Есть следующее простое решение: на каждом из коммутаторов можно определить по одному порту, относящемуся к сети электротехнического факультета (и по одному — для факультета инфор­матики), а потом соединить эти порты друг с другом, как показано на рис. 5.26(a). Однако такое решение не масштабируется, поскольку для *N* виртуальных локальных сетей потребуется задействовать по *N* портов на каждом коммутаторе, просто чтобы объединить два устройства.

****

**Рис. 5.26. Соединение двух коммутаторов с двумя виртуальными локальными**

**сетями: (а) два кабеля (б) магистральный канал**

Более удобный для масштабирования метод подключения ком­мутаторов из виртуальных локальных сетей называется **VLAN-тран-кингом.** При использовании такого метода, проиллюстрированного на рис. 5.26(6), на каждом коммутаторе выделяется специальный порт (на коммутаторе слева это порт 16, на коммутаторе справа — порт 1), который конфигурируется как магистральный (trunk port) и предназна­чается именно для соединения двух VLAN-коммутаторов. Магистраль­ный порт относится ко всем виртуальным локальным сетям, и кадры, направляемые в любую сеть VLAN, проходят по магистральному каналу на другой коммутатор. Но здесь возникает еще один вопрос: как ком­мутатор узнает, что кадр, прибывший на магистральный порт, относит­ся к конкретной виртуальной локальной сети? Институт IEEE описал расширенный формат кадров Ethernet 802.1Q, специально для работы с кадрами, проходящими по магистральному каналу. Как показано на рис. 5.27, кадр 802.1Q состоит из стандартного Ethernet-кадра и 4-байт-ной **метки VLAN.** Эта метка содержит идентификационную информацию той виртуальной локальной сети, к которой относится данный кадр. Метка VLAN записывается в кадр коммутатором на стороне отправите­ля, а на стороне получателя считывается и удаляется другим коммутато­ром. Сама VLAN-метка состоит из двухбайтного поля TPID (Tag Protocol Identifier — идентификатор протокола метки) с фиксированным шест-надцатеричным значением 81-00, из двухбайтного поля управляющей информации метки (Tag Control Information), содержащего 12-битное поле идентификатора VLAN, и трехбитного поля приоритета, которое функционально напоминает поле TOS из заголовка 1Р-дейтаграммы.

****

**Рис. 5.27.** Исходный кадр Ethernet (вверху) и VLAN-кадр Ethernet, снабженный

меткой стандарта 802.1Q (внизу)

Здесь мы лишь кратко коснулись темы VLAN и сосредоточились на обсуждении таких виртуальных локальных сетей, которые работают на основе портов. Также необходимо отметить, что существует и ряд дру­гих способов определения сетей VLAN. В виртуальных локальных се­тях на основе МАС-адресов администратор вычислительной сети задает множество МАС-адресов, относящихся к конкретной виртуальной сети. Когда устройство подключается к порту, мы относим этот порт к соот­ветствующей сети VLAN в зависимости от МАС-адреса устройства. Вир­туальные локальные сети также могут определяться на основе протоко­лов сетевого уровня (например, Ipv4, Ipv6 или Appletalk) и по другим критериям. Подробнее эти возможности описаны в стандарте 802.1Q234.

**Виртуализация каналов: сеть как канальный уровень**

Теперь давайте поговорим о том, как развивались трактовка и значение термина *канал.* В начале мы рассма­тривали канал как физическую сущность (провод). Этот провод связы­вает два хоста, обменивающиеся информацией. При изучении протоколов множественного доступа мы убедились, что несколько хостов могут быть соединены совместно используемым (разделяемым) кабелем и что в роли такого «кабеля» также могут выступать радиоволны или другие носители. Таким образом, мы рассматривали канал как все более аб­страктную сущность. В разделе о локальных Ethernet-сетях (рис. 5.15) мы узнали, что среда для соединения хостов может представлять собой довольно сложную инфраструктуру, в которой применяются коммута­торы. Но в ходе всего этого развития понятий сами хосты «все так же считали», что соединительная среда представляет собой обычный про­вод, работающий на канальном уровне, к которому эти хосты подклю­чены. Так, мы могли убедиться, что Ethernet-хост может совершенно не представлять, как именно он подключен к другим хостам локальной сети: одним коротким LAN-сегментом (рис. 5.17), территориально рас­средоточенной коммутируемой локальной сетью (рис. 5.15) или вирту­альной локальной сетью (рис. 5.26).

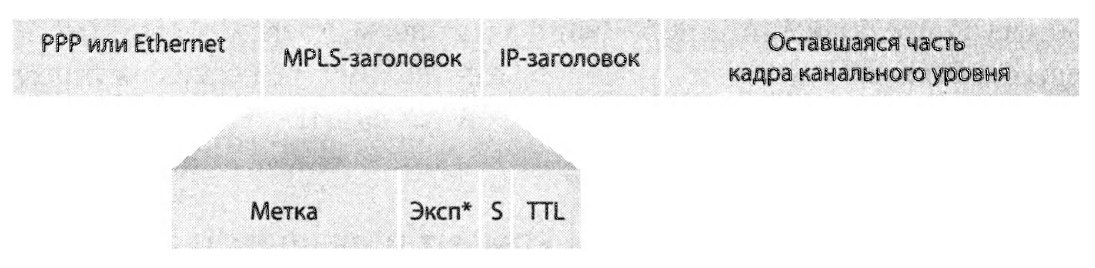
Если соединение между двумя хостами устанавливается с помощью модема коммутируемого доступа, то канал фактически представляет собой линию из телефонной сети. Это логически самостоятельная гло­бальная телекоммуникационная сеть с собственными коммутаторами, каналами и стеками протоколов для передачи данных и обмена сигна­лами. Однако на канальном уровне Интернета коммутируемое соедине­ние по телефонной линии воспринимается как связь по обычному «ка­белю». Можно сказать, что Интернет виртуализует телефонную сеть, трактуя ее как технологию канального уровня и обеспечивая соединяе-мость канального уровня между двумя хостами. Возможно, вы помните, что оверлейная (наложенная) сеть трактует Интернет просто как носитель для обеспечения связи между двумя наложенными узла­ми. Она выстраивается на базе Интернета, точно как Интернет выстраи­вается на телефонной сети.

Сейчас мы рассмотрим сети MPLS, в которых осуществля­ется многопротокольная коммутация по меткам. Сети MPLS, в отличие от телефонных сетей с коммутацией каналов, работают с коммутацией пакетов и с установлением виртуальных соединений. В сетях MPLS ис­пользуются собственные форматы пакетов и методы пересылки данных. Поэтому с учебной точки зрения обсуждение сетей MPLS органично вписывается в материал как о сетевом, так и о канальном уровне. Но в контексте Интернета можно рассматривать MPLS как технологию, со­поставимую с телефонными сетями и коммутируемым Ethernet, кото­рая служит для соединения IP-устройств. Именно поэтому мы обсудим MPLS в главе о канальном уровне. Сети с ретрансляцией кадров и архи­тектура ATM также могут применяться для соединения IP-устройств, хотя две эти технологии и являются уже сравнительно старыми (впро­чем, их по-прежнему активно внедряют) и здесь рассматриваться не будут. Об этих технологиях подробно рассказано в очень интересной книге Горальски. Здесь мы можем позволить себе лишь краткое вве­дение в эту технологию, поскольку по ней можно написать целые тома (и такие тома уже написаны). Подробное изложение технологии MPLS дается в книге Дэви. Мы поговорим, в основном, о том, как MPLS-сер­веры соединяют IP-устройства, но также позволим себе несколько более глубокое изучение технологий, лежащих в основе MPLS.

**Многопротокольная коммутация по меткам**

Многопротокольная коммутация по меткам (MPLS) — это техноло­гия, появившаяся в результате ряда промышленных разработок, которые начались еще в середине и конце 90-х. Цель этих разработок заключалась в повышении скорости пересылки данных на IP-маршрутизаторах путем внедрения в них одной из основных концепций, принятых на вооружение в сетях с виртуальными каналами. Эта сущность — метка с фиксирован­ной длиной. Цель разработчиков этих технологий заключалась не в отказе от инфраструктуры передачи IP-дейтаграмм, основанной на маршрути­зации, в пользу альтернативной архитектуры на основе меток фиксиро­ванной длины и виртуальных каналов, а в дополнении имеющейся архи­тектуры путем выборочной пометки дейтаграмм и далее маршрутизации дейтаграмм с применением меток фиксированной длины, когда это осу­ществимо. Важно отметить, что такие функции выполняются в тесном взаимодействии с протоколом IP, используют IP-адресацию и маршрути­зацию. Организация IETF унифицировала все эти разработки в протоко­ле MPLS, фактически интегрировав техники работы с виртуальными каналами в сеть с маршрутизацией дейтаграмм.

Начиная наше изучение MPLS, рассмотрим формат кадра каналь­ного уровня, который обрабатывается маршрутизатором, поддержива­ющим MPLS. На рис. 5.28 видно, что кадр канального уровня, переда­ваемый между устройствами с поддержкой MPLS, содержит небольшой MPLS-заголовок, добавляемый между заголовком уровня 2 (например, Ethernet) и уровня 3 (то есть, IP). В стандарте RFC 3032 определяется формат MPLS-заголовка для таких каналов. В других стандартах RFC также определяются заголовки для сетей ATM и сетей с ретрансляцией кадров. Среди полей MPLS-заголовка есть, в частности, метка (выпол­няющая роль такого идентификатора виртуального канала, о котором мы говорили ранее). 3 бита зарезервированы для экспери­ментального использования. Еще в заголовке есть один бит S, который обозначает конец серии расположенных друг над другом MPLS-заго­ловков (это отдельная более сложная тема, которую мы не будем здесь рассматривать), а также поле предписанного времени жизни.

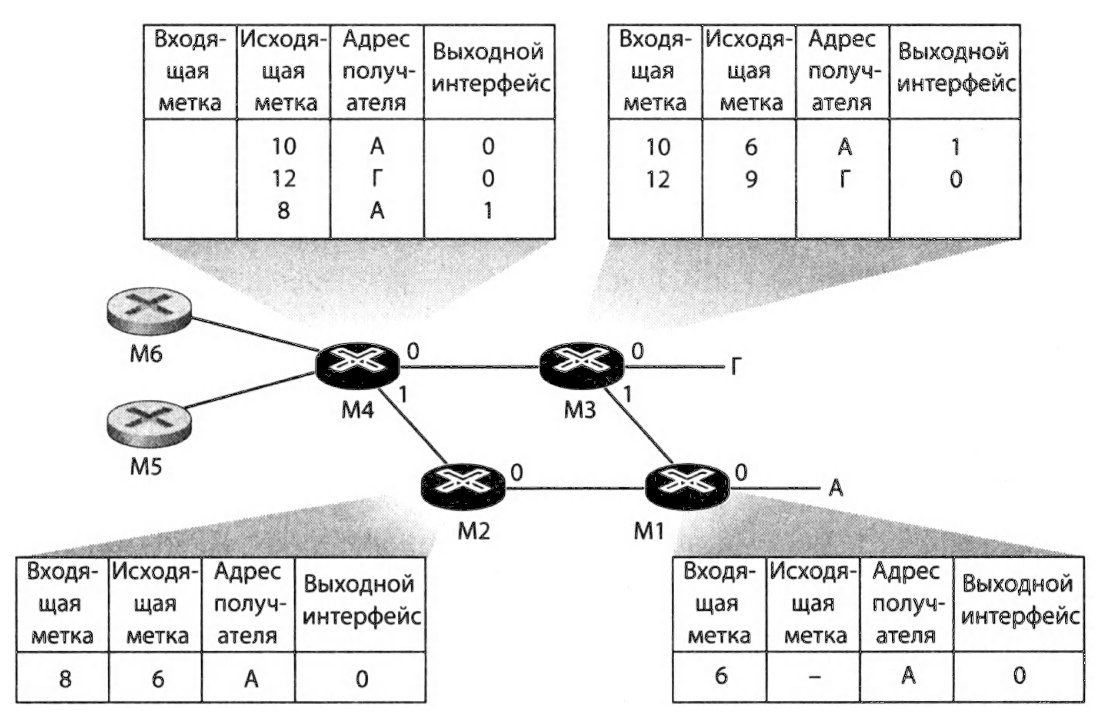
****

**Рис. 5.28. MPLS-заголовок размещен между заголовками канального**

**и сетевого уровней**

Из рис. 5.28 сразу становится понятно, что усовершенствованный MPLS-кадр можно пересылать лишь между устройствами, поддержива­ющими протокол MPLS (ведь обычный маршрутизатор будет изрядно озадачен, если найдет MPLS-заголовок там, где ожидает встретить IP-заголовок!) Маршрутизаторы, поддерживающие MPLS, зачастую име­нуются **маршрутизаторами с коммутацией по меткам.** Такие устрой­ства пересылают MPLS-кадр, сверяясь с MPLS-меткой в своей таблице маршрутизации, а затем сразу же передают кадр на соответствующий выходной интерфейс. Соответственно, маршрутизатор с поддержкой MPLS *не* извлекает IP-адрес назначения и не ищет совпадения самого длинного префикса в таблице маршрутизации. Но как маршрутизатор узнает, поддерживает ли его маршрутизатор-сосед MPLS, а также какая метка должна быть ассоциирована с заданным IP-адресом? Чтобы отве­тить на эти вопросы, давайте рассмотрим, как взаимодействует группа маршрутизаторов с поддержкой MPLS.

В примере на рис. 5.29 маршрутизаторы от Ml до М4 поддержива­ют MPLS. M5 и Мб — стандартные IP-маршрутизаторы. Ml объявляет М2 и МЗ, что он (Ml) может переправить информацию в точку А и что полученный кадр с MPLS-меткой б будет передан в точку А. Маршру­тизатор МЗ объявляет М4, что он может направлять информацию к точкам назначения А и Г и что туда отправятся соответственно входящие кадры с MPLS-метками 10 и 12. Наконец, маршрутизатор М2 объяв­ляет маршрутизатору М4, что он (М2) может отправить информацию в точку А и что полученный кадр с MPLS-меткой 8 будет направлен к А. Итак, маршрутизатор М4 оказывается в интересной ситуации: он знает два MPLS-пути, по которым может достичь А: через интерфейс 0 с исходящей MPLS-меткой 10 и через интерфейс 1 с исходящей MPLS-меткой 8. Общая картина, проиллюстрированная на рис. 5.29, такова: IP-устройства М5, Мб, А и Г соединены друг с другом через MPLS-инфраструктуру (маршрутизаторы Ml, М2, МЗ и М4 поддерживают MPLS). Это соединение выполнено примерно таким же образом, как коммутируемая локальная сеть или ATM-сеть соединяется при помощи IP-устройств. Кроме того, как и в коммутируемых локальных сетях или ATM, маршрутизаторы Ml — М4 с поддержкой MPLS взаимодейству­ют, *даже не притрагиваясь к IP-заголовку пакета.*

****

**Рис. 5.29. Перенаправление информации с поддержкой MPLS**

Выше мы не указали конкретный протокол, который применяется для распространения меток между маршрутизаторами, поддерживаю­щими технологию MPLS. Дело в том, что подробное обсуждение обмена сигналами в MPLS выходит за рамки этой книги. Правда, мы отметим, что рабочая группа IETF по технологии MPLS указала в стандарте RFC 3468, что для обеспечения обмена сигналами в MPLS будет использоваться протокол RSVP-TE, являющийся расширением над протоко­лом RSVP. Кроме того, мы не обсудили, как именно вычисляются пути для передачи пакетов между маршрутизаторами, поддерживающими MPLS, ни как MPLS собирает информацию о состоянии канала (напри­мер, ширину полосы передачи данных, не зарезервированную MPLS), применяемую в таких расчетах путей. Для подачи такой информации в маршрутизаторы с поддержкой MPLS применяются усовершенство­ванные варианты алгоритмов с учетом состояния канала (например, OSPF). Интересно отметить, что сами алгоритмы расчета пути не стан­дартизированы и в настоящее время определяются производителями устройств.

До сих пор в нашем обсуждении MPLS мы делали акцент на том факте, что этот протокол выполняет коммутацию на основе меток, со­ответственно, ему не нужно учитывать при работе IP-адрес пакета. Но наиболее важные преимущества MPLS и причины огромного интереса, который в настоящее время проявляется к этому протоколу, заключают­ся не в потенциальном увеличении скорости коммутации, а в новых воз­можностях управления трафиком, которые дает MPLS. Как было указа­но выше, у маршрутизатора М4 есть *два* MPLS-пути к точке А. Если бы пересылка выполнялась на IP-уровне, на основании IP-адреса, то прото­колы IP-маршрутизации, изученные нами ранее, дали бы всего один путь к узлу А путь с наименьшей стоимостью. Следовательно, MPLS позволяет вести пакеты по таким маршрутам, которые недоступны при использовании стандартных IP-протоколов маршрутизации. Здесь мы имеем дело с одним из простых вариантов **управления трафиком** при по­мощи MPLS. В данном случае оператор сети может переопре­делять стандартную IP-маршрутизацию и принудительно направлять часть трафика к месту назначения по заданному пути. Одновременно к тому же месту назначения уже по другому пути может направляться другой трафик (выбор иного пути может быть связан с соображениями политики, безопасности или с какими-то другими причинами).

MPLS также можно использовать и в других целях. Например, для быстрого восстановления путей MPLS-маршрутизации, то есть для перенаправления трафика по заранее рассчитанному резервному пути в случае отказа основного. Наконец, отметим, что MPLS может применяться (и действительно применяется) при создании так называе­мых **виртуальных частных сетей** (virtual private networks, **VPN).** Ор­ганизуя виртуальные частные сети для заказчика, Интернет-провайдер, чтобы объединить их, использует свою сеть с поддержкой MPLS. MPLS может применяться для отграничения как ресурсов, так и адресации, применяемой в частной виртуальной сети заказчика, от адресации и ре­сурсов других пользователей, работающих в сети данного Интернет-провайдера.

Мы вынуждены ограничиться столь кратким обсуждением MPLS. Рекомендуем вам ознакомиться с источниками, упомянутыми в этом разделе. Учитывая, как разнообразны варианты применения MPLS, эта технология вскоре может превратиться в настоящий швейцарский армейский нож для управления Интернет-трафиком! Для несведущих следует пояснить, что швейцарский армейский нож известен своей уни­версальностью и годится «на все случаи жизни».