Лекция 7.

Дополнительные функции маршрутизаторов

В состав наиболее известных дополнительных функций и функциональных возможностей маршрутизаторов входят:

- фильтрация пакетов
- формирование трафика (shaping)
- IP-туннелирование
- трансляция IP-адресов (NAT)
- зеркалирование портов
- виртуализация портов и наделение портов подключенного коммутатора полной функциональностью порта маршрутизатора
- поддержка протокола MPLS

Перечисленные функциональные возможности вкратце рассматриваются ниже.

7.1. Фильтрация пакетов

Функция фильтрации пакетов обеспечивает возможности построения простых межсетевых экранов (firewall). Средствами фильтрации пакетов (отбрасывания их по определенным критериям) можно, например, запретить как доступ **к** некоторой совокупности внутренних компьютеров сети из множества определенных внешних IP-сетей с использованием всех либо определенных прикладных протоколов, так и запретить доступ **из** определенной совокупности внутренних компьютеров сети ко всем или определенным внешним сетям с использованием любых или указанных сетевых протоколов. Таким образом, можно исключить нежелательные взаимодействия компьютеров сети с внешними компьютерами.

Функция фильтрации пакетов обычно конфигурируется для внешнего порта пограничного маршрутизатора сети, связывающего эту сеть с внешними сетями и может быть применена как к входящим так и к исходящим IP-пакетам. Критерии фильтрации пакетов определяются задаваемыми сетевым администратором списками контроля доступа ACL (Access Control List), различными для входящего и исходящего потоков трафика, которые фильтруются независимо друг от друга. Входящие в такой список элементарные критерии формулируются в терминах значений IP-адресов (с масками подсети) и номеров портов (номера портов однозначно определяют соответствующие прикладные протоколы, как это изучалось в курсе «Компьютерные сети») отправителя и получателя IP-пакетов.

Для того, чтобы получить значения номеров портов IP-пакета функция пакетной фильтрации должна “заглядывать” не только в заголовок IP-пакета, но и в заголовок инкапсулированного в этот пакет транспортного сообщения.

Отметим, что каждый из списков ACL может быть сформулирован в разрешительной (пакет, удовлетворяющий условию, пропускается “сквозь фильтр”) или в запретительной (пакет, удовлетворяющий условию, отбрасывается фильтром) форме. Это позволяет описывать критерии доступа в более лаконичном виде, указывая в каждом элементе списка либо правила фильтрации, либо правила пропуска трафика через фильтр в зависимости от того, что проще описать.

В завершение обсуждения функции фильтрации пакетов и используемых этой функцией списков контроля доступа укажем, что при поступлении на порт входящего или исходящего пакета он последовательно сопоставляется со всеми элементами соответствующего (по направлении пересылки) ACL. Сопоставление прекращается и пакет выбрасывается, если в соответствии с очередным запретительным элементом ACL пакет должен быть отфильтрован. Если же в соответствии с очередным разрешительным элементом ACL пропуск пакета разрешён, то он отправляется далее в направлении к его получателю. При исчерпании элементов ACL пакет также отправляется в направлении к его получателю.

7.2. Формирование трафика (shaping)

Формирование трафика (shaping или просто шейпинг), это функция, обычно конфигурируемая сетевым администратором для портов, через которые эта сеть подключена каналами доступа к внешним сетям (сетям операторов связи). Но шейпинг может быть применен и на внутренних каналах сети организации, соединяющих множества подсетей, суммарная потребность которых в обмене трафиком может существенно превышать емкость доступного канала. Для простоты ограничимся рассмотрением применения функции шейпинга на внешнем канале сети организации. Функция позволяет организовать жёсткое разделение емкости (пропускной способности) внешних каналов связи между группами подсетей, организовав для каждой из таких групп логический канал определенной емкости. При этом сумма емкостей таких логических каналов не должна превосходить емкости соответствующего физического канала.

Нераспределенный остаток емкости основного канала предоставляется всем не участвовавшим в распределении емкости канала подсетям.

Выделение определенной емкости канала некоторой совокупности подсетей выполняется путем создания сетевым администратором списка контроля доступа ACL, подобного спискам контроля доступа функции фильтрации пакетов.

Для каждого из ACL шейпинга указывается величина доступной канальной емкости и список подсетей и/или индивидуальных компьютеров, которым в совокупности выделяется указанная емкость. Элементом такого списка (который может быть сформулирован во включающей или исключающей форме) является IP-адрес подсети (с маской подсети) или IP-адрес индивидуального компьютера. При использовании включающей формы в элемент списка включаются указанные в нём адреса, а при использовании исключающей – все адреса, кроме указанных в элементе списка. Для проверки того, принадлежит ли текущий пересылаемый IP-пакет определяемому списком ACL логическому каналу, IP-адрес получателя этого пакета (в случае разделения входящей емкости внешнего канала) последовательно проверяется на выполнение условий всех элементов списка и считается принадлежащим каналу при успешном прохождении всех проверок. Отметим, что при помощи ACL такого относительно простого вида за счёт определенного упорядочивания включающих и исключающих элементов ACL можно задавать достаточно сложно устроенные множества IP-адресов. Так, например, множество IP-адресов, включающее все адреса сети N кроме подсети N1 и адреса IP1, входящих в состав сети N может быть задано ACL-списком вида (искл (N1), искл (IP1), вкл(N)).

Для каждого логического канала, соответствующего тому или иному ACL постоянно вычисляется текущий уровень загрузки этого канала. Если передача очередного пакета приведет к превышению уровня загрузки над выделенной каналу емкостью, пакет выбрасывается. Благодаря работе механизма обратной связи протокола TCP, рассматриваемого в курсе КС, это вынудит отправителей пакетов, направляющих их через “шейпингуемый” канал, снизить темп отправки этих пакетов (путем уменьшения размеров окна TCP).

Отметим, однако, что если механизм шейпинга используется для ограничения емкостей входящего трафика внешних каналов, то конфигурирование этого механизма на пограничном маршрутизаторе, находящемся на “ближнем” конце дорогого протяжённого канала к сети оператора, неэффективно. Дело в том, что в этом случае выбрасывается часть пакетов, уже прошедших через “узкое

горло” внешнего канала, и их выбрасывание приводит к снижению эффективности использования этого “узкого горла”. В этом случае более правильное решение состоит в установке собственного маршрутизатора на “дальнем” конце внешнего канала в PoP (точке присутствия) оператора (провайдера) или в IX - точке обмена трафиком с несколькими операторами (провайдерами) и конфигурировании функций шейпинга на этом “дальнем” маршрутизаторе. В этом случае пакеты отбрасываются до передачи их через “узкое горло” внешнего канала, что не снижает эффективности его использования.

7.3. IP-туннелирование

IP-туннелирование является средством обеспечения возможности работы в едином непрерывном адресном пространстве двух или более удаленных друг от друга сетей, не связанных между собою прямыми каналами передачи данных, а взаимодействующих через интернет. Такая потребность может возникнуть, например, для сетей организаций, имеющих один или несколько географически удаленных филиалов. В качестве других примеров использования IP-туннелирования сошлемся на упоминавшиеся в курсе «Компьютерные сети» и рассматриваемые в 2-х следующих лекциях настоящего курса способы построения магистральных сетей 6Bone IPv6 и MBone групповой маршрутизации соответственно.

IP-туннель обеспечивает передачу через интернет IP-пакетов с такими IP-адресами получателей, для которых стандартные процедуры маршрутизации в интернете не в состоянии обеспечить корректную доставку этих пакетов.

Так адреса единого адресного пространства удаленных головной организации и филиала (для упрощения дальнейшего изложения будем рассматривать случай организации с одним удаленным филиалом) могут быть либо внутренними адресами (и не маршрутизироваться в интернете), либо быть ”привязанными” к интернет-провайдеру только одной из двух удаленных подсетей головной организации и филиала (иначе они не будут составлять блока смежных адресов). В последнем случае при использовании стандартных механизмов маршрутизации все IP-пакеты, адресованные в любую из удаленных подсетей организации, будут доставляться только в ту подсеть, диапазон адресов которой использован в качестве диапазона адресов интегрированной сети головной организации и филиала.

В случае же передачи через интернет IP-пакетов сетей, входящих в магистрали 6Bone и MBone соответственно, либо формат IP-пакета (для 6Bone), либо требуемые правила его интерпретации (для MBone) “не известны” стандартному модулю IP и, поэтому, не могут быть им корректно обработаны.

Механизм IP-туннелирования позволяет обеспечить корректную доставку IP-пакетов получателю во всех рассмотренных выше случаях.

Эта возможность обеспечивается инкапсуляцией при отправке через IP-туннель исходных IP-пакетов внутрь других, “несущих” IP-пакетов в которых в качестве IP-адресов отправителя и получателя указываются IP-адреса начальной и конечной точек туннеля. При доставке такого пакета в точку окончания IP-туннеля выполняется декапсуляция (извлечение) исходного пакета из несущего и он может далее маршрутизироваться (по правилам маршрутизации, используемым в принявшей пакет сети) по указанному в нем адресу получателя.

В качестве конечных точек туннеля (каждая из таких точек в зависимости от направления пересылки может выступать в роли начальной или точки окончания туннеля) конфигурируются внешние (направленные в сторону интернета) порты пограничных маршрутизаторов соединяемых IP-туннелем сетей. Указанное конфигурирование выполняется при помощи соответствующих средств сетевыми администраторами.

7.4. Трансляция IP-адресов (NAT)

При рассмотрении системы IP-адресации в курсе «Компьютерные сети» нами упоминались 3 диапазона внутренних, или “серых” IP-адресов, которые свободно могут использоваться в любой абонентской сети (для обеспечения адресного пространства требуемого размера), но которые не маршрутизируются в интернете: пакеты с такими адресами просто выбрасываются маршрутизаторами сетей операторов связи (интернет-провайдеров) любого уровня. Но это не означает, что для компьютеров с такими адресами закрыт доступ к интернету. Просто для обеспечения такого доступа используются специальные механизмы NAT (Network Address Translation - трансляция сетевых адресов), практически незаметные для пользователей компьютеров с внутренними адресами.

Эти механизмы конфигурируются сетевыми администраторами на внешних портах пограничных маршрутизаторов внутренних «серых» IP-сетей. Рассмотрим основные разновидности NAT.

7.4.1. Обычный NAT

При использовании обычного NAT трансляция адресов исходящих и входящих пакетов на внешнем порте пограничного маршрутизатора «серой» сети выполняется соответствии с таблицей трансляции адресов, формат строки которой приведен на рис.1.

внутренний IP-адрес источника	внутренний № порта источника	внешний № порта маршрутизатора (NAT-а)

Рис.1. Формат строки таблицы трансляции адресов NAT

Напомним, что номера портов идентифицируют прикладные процессы клиентских и серверных программ различных протоколов

При отправке пакета изнутри сети внешнему получателю в таблицу трансляции добавляется строка, в 1-е и 2-е поля которой заносятся значения соответствующих полей из заголовка IP-пакета. Значение 3-го поля динамически выделяется маршрутизатором NAT для указания в качестве гарантированно уникального номера порта источника в отправляемом пакете (и одновременно - уникального идентификатора строки в таблице NAT).

После этого в заголовке пакета IP-адрес источника заменяется на IP-адрес внешнего порта маршрутизатора, номер порта источника - на содержимое 3-го поля сформированной строки таблицы, и пакет отправляется получателю. Указанный в 3-м поле строки номер порта достаточен для поиска строки таблицы при выполнении обратной трансляции адресов во время получения ответа на отправленный пакет.

Однако для повышения уровня информационной безопасности путем исключения получения ответов не с тех серверов, на которые посылался запрос, созданы два расширения обычного NAT: Address-restricted NAT и Port-restricted NAT.

Первое предусматривает добавление в строку таблицы трансляции поля со значениями IP-адреса внешнего получателя пакета. Второй тип Port-restricted NAT вместе с IP-адресом внешнего получателя пакета добавляет еще и поле с его портом.

Созданная строка сохраняется в таблице трансляции для следующего использования. Если за время, указанное в настройке “NAT translation timeout” пакетов, соответствующих строке в таблице трансляции, больше не приходило, то строка удаляется.

При получении ответа по полю 3 ищется строка таблицы трансляции и, если применяется Address-restricted NAT или Port-restricted NAT, то выполняется проверка корректности соответственно только IP-адреса или IP-адреса и номера порта внешнего источника пакета. Если для принятого пакета не находится соответствующей строки в таблице трансляции (она может быть удалена по таймауту) либо пакет не проходит проверку корректности, то он признается некорректным и выбрасывается. При корректности полученного пакета в нем выполняется замена адреса получателя на значение поля 4, а номера порта получателя — на значение поля 5 из найденной строки таблицы трансляции. После этого пакет маршрутизируется внутрь сети.

Это простейшая схема. При ее использовании можно обращаться изнутри сети, работающей на внутренних адресах (внутренней сети), к серверам, расположенным во внешних сетях. Но нет никакой возможности обратиться из внешних сетей к серверам, расположенных во внутренней сети. Такая возможность обеспечивается следующей разновидностью NAT.

7.4.2. Система DNAT

В системе DNAT (Dynamic NAT – динамический NAT) можно указать (при конфигурировании), что все входящие внешние пакеты с определенным номером порта получателя отправляются на один и тот же внутренний адрес. При этом автоматически обеспечиваются 2 свойства:

1. во внутренней сети может быть не более 1-го сервера каждого типа, кроме WWW
2. каждый такой сервер не может быть доступен (и атакован) пакетами других сетевых протоколов, отличных от протокола запросов к серверу.

Но иногда возникает потребность организации взаимодействия компьютеров, работающих на внутренних адресах внутри различных сетей, например для общения пользователей этих компьютеров через систему видеотелефонии Skype. Эта возможность обеспечивается следующей разновидностью NAT.

7.4.3. Связь «серых» компьютеров через NAT (Hole punching NAT)

В связи с повсеместным внедрением трансляторов адресов в интернете возникла острая *проблема связи компьютеров с серыми адресами между собой*. Первоначальные попытки ее решения заключались в использовании третьего компьютера с “белым” IP-адресом. С ним устанавливали соединения оба

абонента с “серыми” адресами и пересылали через него данные. Так работали первые версии программы голосовой телефонии Skype и программ пирингового обмена файлами. Однако процент абонентов с белыми адресами становился все меньше, а транзитный трафик через них - все больше. Переход программ на использование транспортного протокола UDP и использование способов работы с этим протоколом большинства трансляторов адресов позволили избежать нагрузки на третью сторону по пересылке трафика и использовать её только в момент установления соединения.

Название технологии “Hole punching NAT” дословно переводится как “пробивка дыр в NAT”, что отражает ее сущность.

Рассмотрим процесс установление соединения компьютеров А и Б, находящихся за NAT, подробно (см. рис.2).

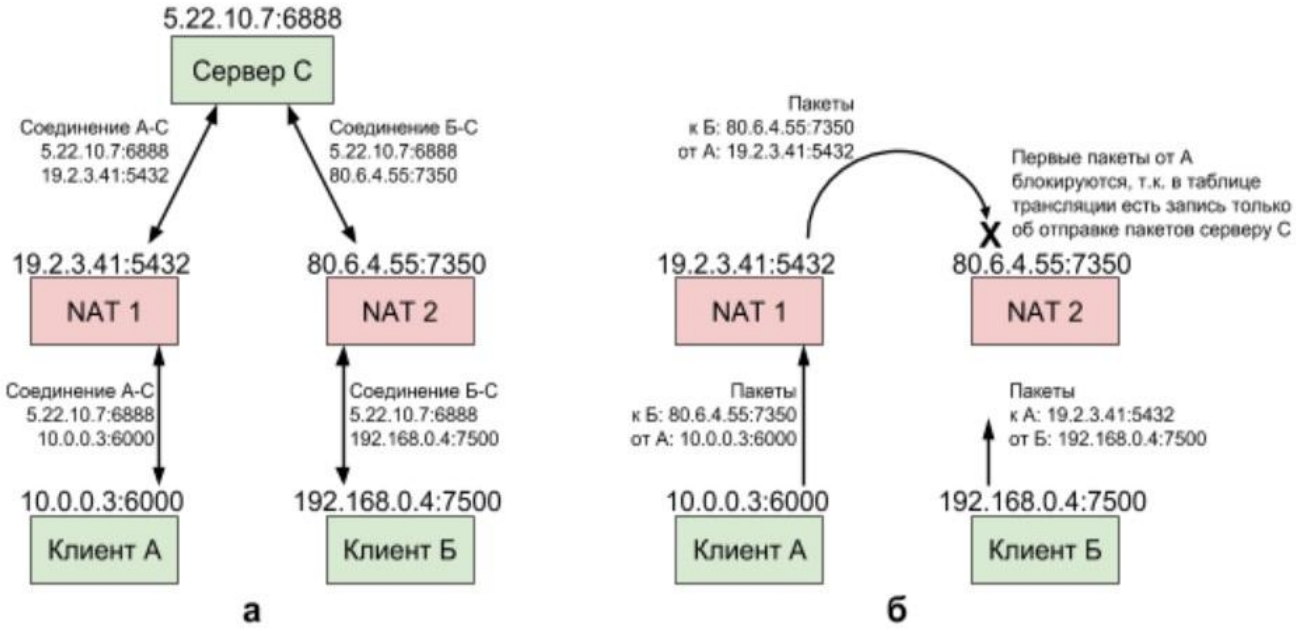

Рис.2. Установка соединения между компьютерами, находящимися за NAT

Для установления соединения (но не для передачи трафика) компьютерам за NAT требуется наличие третьей стороны с белым IP-адресом. Назовем ее сервер С (см. рис. 2а).

Компьютеры А и Б отправляют UDP-пакеты серверу С, из которых он узнает внешние адреса А и Б (адреса NAT): 19.2.3.41:5432 и 80.6.4.55:7350. Внешний адрес А сервер С сообщает компьютеру Б, а внешний адрес Б - компьютеру А.

После этого А и Б начинают собственно процесс “пробивки дыр” (см. рис. 2б). Многие трансляторы адресов обладают важным для технологии Hole punching NAT свойством: при пересылке UDP пакета другому компьютеру назначенный ранее (для пересылки другого пакета и, возможно, другому компьютеру) исходящий внешний адрес, применяемый для отправки UDP пакета, не меняется. Таким образом, когда А и Б начинают пересылать друг другу UDP-пакеты, трансляторы адресов отправляют от имени тех же внешних адресов: 19.2.3.41:5432 и 80.6.4.55:7350. На рис. 2б компьютер А начал отправлять пакеты чуть раньше. Из-за этого первые из дошедших пакетов компьютера А могут быть заблокированы транслятором адресов NAT 2 так как компьютер Б еще не успел отправить хотя бы один пакет для А. Но после отправки компьютером Б первого пакета транслятор NAT 2 создаст запись в своей таблице трансляции и будет далее пропускать все входящие пакеты от А. Так как А начал отправлять пакеты чуть раньше Б, то его транслятор адресов NAT 1 создал запись в таблице трансляции до прихода пакетов от Б, поэтому все пакеты от Б будут получены без сбоев.

7.5. Зеркалирование портов

“Зеркальная” копия входящего или исходящего потоков трафика одного порта маршрутизатора может быть направлен на другой порт. Эта возможность полезна для построения анализаторов потоков трафика, проверяющих трафик параллельно с его пересылкой адресату. На базе этой возможности построены, например, системы блокировки доступа к запрещенным сайтам и/или страницам сайтов. Такие системы анализируют зеркальную копию исходящего трафика внешнего канала. При обнаружении запросов на доступ к запрещенным страницам и/или сайтам они посылают соответствующему серверу (на котором размещен запрещенный ресурс) от имени компьютера, с которого был направлен запрос, пакет разрыва соединения по протоколу TCP, а самому этому компьютеру направляют специальную страницу сообщения о попытке доступа к запрещенному ресурсу.

7.6. Виртуализация портов маршрутизатора и наделение портов подключенного коммутатора полной функциональностью портов маршрутизатора

На базе одного порта маршрутизатора может быть сконфигурировано несколько виртуальных портов, трафик каждого из которых выделяется на основе протокола IEEE 802.1q, применяемого для разделения VLAN. Эта возможность предназначена для подключения к порту маршрутизатора транкового канала коммутатора, используемого для соединения с маршрутизатором нескольких VLAN.

Порты коммутатора, подключенного к одному из портов маршрутизатора, сами могут быть *наделены полной функциональностью портов маршрутизаторов*. Для обеспечения этой возможности коммутатор должен быть подключен транковым каналом к виртуализированному порту маршрутизатора так, чтобы каждый порт коммутатора был подключен к маршрутизатору отдельным виртуальным портом.

Применение этой возможности позволяет существенно увеличить количество портов маршрутизатора с существенно меньшими затратами, чем при установке эквивалентного по количеству портов интерфейсных модулей, вставляемых в слоты расширения портов маршрутизатора. На базе указанной возможности создается типовая структура из 2-х коммуникационных устройств, изображенная на рис. 3 и называемая однорукими маршрутизатором.

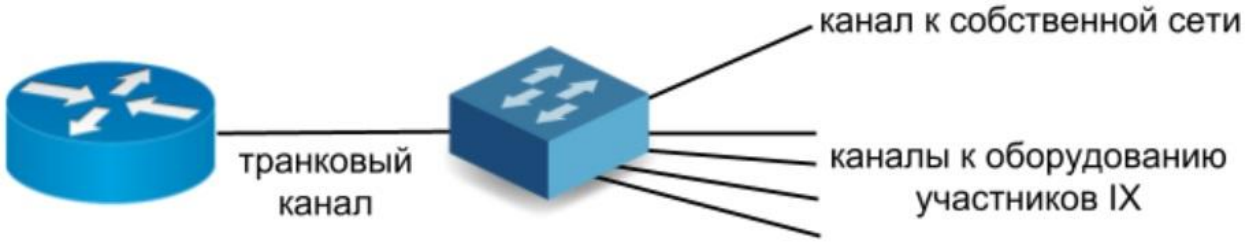

Рис. 3. Однорукий маршрутизатор и его использование в IX

Однорукие маршрутизаторы часто используются в IX участниками обмена трафиком, как это показано на рис. 3.

7.7. Основы протокола MPLS

Протокол MPLS (MultiProtocol Label Switching - Многопротокольная коммутация на основе меток пакетов) предназначен для повышения

эффективности прохождения информационных потоков (путем замены маршрутизации коммутацией), транзитом проходящих через MPLS-сеть. В частности в виде MPLS-сети может быть оформлена как магистраль сети предприятия, так и магистраль сети оператора связи национального масштаба.

Строго говоря, MPLS *работает ниже уровня 3* (между уровнями 2 и 3), поскольку не использует адресную информацию 3-го уровня, а использует значения специальных 4-байтных меток потоков, помещаемых перед заголовками IP-пакетов (между заголовком кадра и заголовком IP-пакета). Но поскольку протокол обычно реализуется на базе маршрутизаторов, условно отнесём его к уровню 3.

MPLS сеть создается на базе совокупности связанных между собой каналами передачи данных маршрутизаторов LSR (Label Switching Router – маршрутизаторов, коммутирующих по значению метки). Множество всех LSR разбивается на внутренние, не связанные с маршрутизаторами, не являющимися LSR, и пограничные (edge - крайний), связанные хотя бы с одним маршрутизатором, не являющимся LSR (внешним маршрутизатором). Пример структуры MPLS-сети приведен на рис. 4.

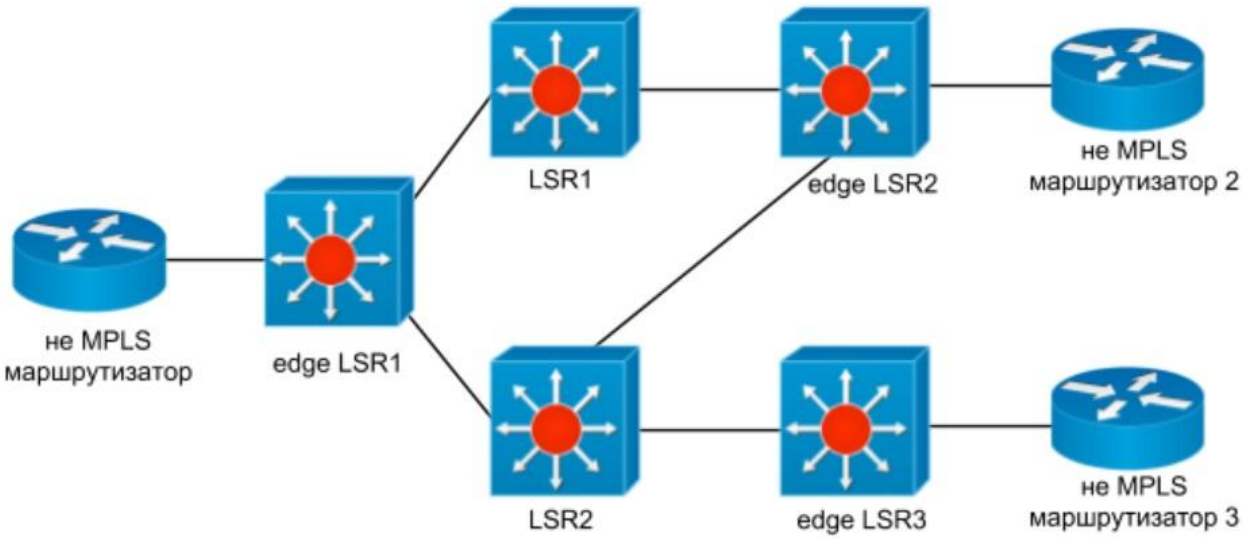

Рис. 4. Пример структуры MPLS-сети

Пограничные LSR выполняют классификацию трафика, поступающего с внешних (не MPLS) маршрутизаторов, на принадлежность этого трафика к некоторым агрегированным потокам (например, потокам, адресованным в определенную подсеть или исходящим из определенных подсетей, потокам приложений передачи голосового трафика VoIP, или потокам трафика отличных от IP сетевых протоколов). *Правила классификации задаются в виде*

соответствующих ACL, подобных ACL механизма шейпинга. По результатам классификации они и присваивают каждому классу метку, которая присоединяется к IP-пакету перед его заголовком. Метка MPLS имеет формат, представленный на рис. 5.

Значение метки	CoS	S	TTL
<- 20 бит ->	<- 3 ->	<1>	<- 8 бит ->

Рис. 5. Структура метки MPLS

Здесь 3-битное поле CoS содержит результат классификации (Class of Service), поле «значение метки» предопределяет маршрут пересылки пакета через сеть MPLS, бит S является признаком последней метки (см. ниже), а поле TTL задаёт «время жизни» пакета.

Маршруты дальнейшей пересылки пакетов определяются значениями их меток, так что пакеты различных классов могут передаваться по различным маршрутам. На основании значения полученной при классификации метки *пакет коммутируется на один из внутренних LSR*. Каждый из внутренних LSR знает, что в начале каждого пакета расположена метка и выполняет коммутацию пакетов на основе значений меток этих пакетов. При этом, перед направлением пакета в выходной порт коммутатор выполняет замену значения метки на основании содержимого поля метки исходящего пакета строки таблицы коммутации подобно тому, как на каждом шаге коммутации меняются значения VCI и VPI коммутаторами ATM.

То есть при обработке пакета с меткой M_{IN}, поступившего на порт P_{IN} в соответствии со строкой таблицы коммутации, структура которой представлена на рис. 6, значение метки пакета заменяется на M_{OUT} и пакет отправляется в порт P_{OUT}. Напомним, что *подобный приём позволяет заменить труднореализуемое требование уникальности значения метки во всей MPLS сети на простое в реализации требование уникальности значения метки внутри одного LSR*.

При выходе пакета из MPLS сети (через внешний порт пограничного LSR) метка пакета отбрасывается.

P_{IN}	M_{IN}	P_{OUT}	M_{OUT}

Рис. 6. Структура строки таблицы коммутации LSR

Коммутация пакетов в LSR выполняется очень эффективно, поскольку таблицы коммутации меток невелики. При этом каждый из классов трафика коммутируется по собственному маршруту. Таким образом, обеспечивается возможность передачи по различным маршрутам, например, трафика различных приложений, что зачастую бывает востребованным.

Существует специальная методология TE (Traffic Engineering) эффективного распределения трафика различных классов по маршрутам, основанная на прокладке специальных TE-туннелей в сети MPLS с использованием расширенной версии протокола управления маршрутизацией OSPF – OSPF-TE.

Тот факт, что LSR выполняют коммутацию только на основе внешних меток и не анализируют заголовок пакета сетевого уровня, позволяет передавать через MPLS сеть потоки трафика различных сетевых протоколов уровня 3 (IP, IPX и др.).

MPLS сети могут иметь иерархическую структуру: в состав MPLS сети могут входить одна или несколько вложенных MPLS сетей, каждая из которых, в свою очередь, может включать вложенные MPLS сети. При этом при входе пакета во вложенную MPLS сеть через пограничный LSR этой сети формируется дополнительная метка, которая заносится в начало пакета перед предыдущей меткой. *При этом в бите S последней (и только последней) метки указывается признак “1” последней метки.* По выходу из вложенной MPLS-сети верхняя (самая левая) метка отбрасывается.

Таким образом, в начале пакета фактически находится стек меток, верхняя из которых является меткой MPLS сети текущего уровня вложенности.

Важно отметить, что каналы передачи данных сетей MPLS в определённом смысле скрывают информацию об отправителях и получателях передаваемых IP-пакетов, поскольку эта информация «прячется» за одной или несколькими метками MPLS.

Кроме того, технология MPLS предоставляет средства гарантирования некоторых параметров качества сетевого обслуживания (QoS) . В частности, MPLS предоставляет возможности обеспечения гарантированной CIR (Committed Information Rate – Согласованная скорость передачи данных), например, путём применения протокола MPLS RSVP-TE, который будет вкратце рассмотрен нами далее при рассмотрении службы QoS). Поэтому технологию MPLS совместно с предоставляемыми ею возможностями QoS часто называют технологией MPLS VPN (Virtual Private Network – виртуальная частная сеть.

Технология MPLS VPN в настоящее время высоко востребована операторами телекоммуникационных сетей различного масштаба (от городского до национального). Она используется ими для предоставления абонентам возможности аренды как каналов гарантированной пропускной способности, так и сетей связи нескольких абонентских подсетей с гарантированной емкостью соединений между этими подсетями. При построении крупных корпоративных сетей технология MPLS VPN (L3 VPN) используется для организации работы магистралей таких сетой.

В завершение отметим, что включение в пакет дополнительных меток приводит к повышению требований на размер MTU. Так, например, если на каналах между LSR используется технология QinQ (IEEE 802.1ad), то минимально необходимый для создания одноуровневой MPLS сети размер MTU составляет 1530, а при необходимости использования N дополнительных уровней вложенности это значение должно быть увеличено на 4*N.