МЕТОДЫ ВИРТУАЛИЗАЦИИ МАГИСТРАЛЬНОГО ЯДРА ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ЮЖНОГО ФЕДЕРАЛЬНОГО УНИВЕРСИТЕТА

А.А. Букатов, О.В. Шаройко

Магистральное ядро распределенной корпоративной телекоммуникационной сети (ТС) Южного федерального университета (ЮФУ) одновременно выполняет функции центрального участка магистралей ТС ЮФУ и научно-образовательной телекоммуникационной сети (НОТС) Южного федерального округа (ЮФО). Фактически на единую (консолидированную) магистральную инфраструктуру накладываются различные логические (виртуальные) магистральные инфраструктуры ТС ЮФУ и НОТС ЮФО.

Следует отметить, что целесообразность создания консолидированных структур (совокупности коммуникационных узлов, связанных друг с другом и с внешними сетями каналами передачи данных), обеспечивающих потребности различных ТС с последующим выделением виртуальных структур, необходимых для функционирования конкретных ТС достаточно очевидна. Таким способом обеспечивается существенная экономия затрат на создание сетевой инфраструктуры.

Следует также отметить, что потребность в выделении логически изолированных подсетей существует для любой современной корпоративной ТС с развитым набором сетевых служб, так как некоторые из таких служб требуют изоляции используемой ими подсети от других подсетей корпоративной ТС. В качестве примеров подобных служб можно указать службу проведения видеоконференций, службу IP-телефонии, службу контроля доступа персонала в здания и помещения, службы доступа к центрам коллективного пользования уникальными вычислительными и экспериментальными ресурсами и некоторые другие службы.

В настоящей работе рассматриваются методы создания требуемых виртуальных сетей, использующие виртуализацию функций телекоммуникационной сети на различных уровнях стека сетевых протоколов. Эти методы фактически применяются для организации требуемого режима использования магистрального ядра ТС ЮФУ.

В настоящее время сетевым инженерам доступен некоторый набор стандартизованных средств и методов, предназначенных для виртуализации различных аспектов работы телекоммуникационной сети. Выбирая тот или иной метод, следует руководствоваться несколькими основными принципами: выбранный метод должен обеспечивать полную изоляцию сетевых структур друг от друга, должен быть эффективным и иметь минимальный негативный эффект на производительность сетевого оборудования и телекоммуникационных каналов, должен быть удобным для выполнения настройки и администрирования.

Вполне естественно ожидать, что на различных участках ТС целесообразно применять различные методы виртуализации. Рассмотрим участок ТС от конечных устройств, таких как ПК, до маршрутизаторов или коммутаторов 3-го уровня (данный участок сети обычно называется сетью доступа). Можно говорить, что для виртуализации сетей доступа стандартом де-факто является применение технологии виртуальных локальных сетей (VLAN) и протокола IEEE 802.1q. Данные средства позволяют накладывать на одну физическую сеть доступа множество изолированных друг от друга логических сетей. Данное решение удовлетворяет всем перечисленным выше требованиям и доступно в оборудовании самых разных производителей. По своей сути применение технологии VLAN протокола IEEE 802.1q позволяет создавать виртуальные каналы передачи данных и виртуальные коммутаторы, чего оказывается вполне достаточно для создания виртуальных сетей доступа. Что же касается виртуализации на магистральном участке НОТС, то решить эту задачу только указанными выше способами вообще невозможно, так как на магистрали сети применяются устройства, работающие не на втором, а на третьем и более высоких уровнях модели стека сетевых протоколов и выполняющие специальные процессы построения таблиц маршрутизации на этих уровнях. Таким образом, для виртуализации магистрали, как минимум, необходимы средства виртуализации этих устройств. В ряде сетевых устройств такие средства реализованы, например, в маршрутизаторах и коммутаторах Cisco используется технология VRF Lite, позволяющая создавать виртуальные маршрутизаторы. Технически технологии VRF Lite в сочетании с протоколом IEEE 802.1Q достаточно для развертывания виртуальных сетей на магистральном участке ТС. Однако практически широкое применение такого подхода оказывается крайне затруднительным, так как для добавления новой виртуальной сети требуется настройка каждого устройства, относящегося к магистральному участку.

В ТС ЮФУ реализован другой подход, позволяющий строить виртуальные сети на магистральном участке и требующий настройки только пограничных устройств, т.е. тех устройств, к которым непосредственно подключены виртуальные сети доступа. Данный подход основан на технологии BGP/MPLS VPN [1]. Результаты опытной эксплуатации решения на основе BGP/MPLS VPN позволяют говорить о том, что задача виртуализации магистрального участка ТС может быть полностью решена средствами данной технологии. В технологии MPLS к каждому IP

пакету приписывается одна или несколько меток. Если к одному пакету приписано несколько меток, то они образуют стек. Маршрутизаторы, работающие с помеченными пакетами, принимают решение о том, что делать с пакетом не на основе анализа IP заголовка, что применяется в обычной IP маршрутизации, а на основе поиска в таблице меток записи, соответствующей самой верхней метке пакета. Такой подход, помимо прочего, позволяет полностью виртуализовать процесс пересылки пакетов по MPLS сети. Действительно, путь следования пакетов через сеть определяется меткой и не зависит от содержимого классических таблиц маршрутизации и заголовков пакета. При этом правило назначения метки определяется идентификатором виртуальной сети доступа и задается только в точке подключения этой сети.

Таким образом, можно говорить, что технология MPLS позволяет достаточно изящно заменить протокол IEEE 802.1q на магистрали сети и обеспечить виртуальную среду передачи данных. Причем при добавлении новой виртуальной сети нет необходимости настраивать каждое устройство магистрали ТС.

Технология BGP/MPLS VPN тесно взаимодействует с технологией виртуальных маршрутизаторов (VRF Lite) и в пограничных маршрутизаторах существует не одна, а сразу несколько таблиц маршрутизации. Как уже указывалось ранее маршрутизаторы и коммутаторы магистральных участков сети обмениваются специальной информацией, позволяющей автоматически строить таблицы маршрутов. Однако в различных виртуальных сетях таблицы маршрутизации могут содержать различные маршруты для одинаковых адресов, ведь виртуализация предполагает полную изоляцию виртуальных сетей друг от друга. Для того чтобы различать маршруты, относящиеся к различным таблицам маршрутизации, с каждой таблицей связывается уникальный в пределах всей сети идентификатор - 8-ми байтовый Route Distinguisher (RD). В соответствии с технологией BGP/MPLS VPN между пограничными маршрутизаторами сети запускается обмен информацией о маршрутах по протоколу BGP, с использованием многопротокольных расширений BGP [2]. Данные расширения протокола BGP позволяют передавать маршруты, относящиеся к различным "семействам адресов". Технология BGP/MPLS VPN вводит понятие семейства адресов VPN-IPv4. Адрес в данном семействе состоит из 12 байт, при этом в первых 8 байтах хранится RD, а оставшиеся 4 байта содержат собственно IP адрес. В результате, даже совпадающие адреса, относящиеся к различным RD перестают совпадать, что позволяет передавать их между маршрутизаторами с использованием протокола BGP. Таким образом, на пограничных устройствах может существовать несколько независимых таблиц маршрутизации, которыми пограничные устройства могут обмениваться между собой. Так как на одном пограничном устройстве существует нескольких таблиц маршрутизации, то необходим некоторый механизм, который позволит определить, к какой из них относятся поступающие на маршрутизатор пакеты. Для пакетов, поступающих со стороны сети доступа, такое соответствие задается в конфигурации устройств, так как одному подключению может соответствовать только одна таблица, что является вполне естественным требованием. Однако, пакеты, поступающие со стороны MPLS сети, могут относиться к различным таблицам. Для решения этой проблемы каждая запись в таблицах маршрутизации, распространяемых между пограничными устройствами, дополняется специальным атрибутом "Target VPN". В данный атрибут записывается идентификатор таблицы маршрутизации, к которой относится маршрут. Когда пакет поступает в MPLS сеть от сети доступа, пограничное устройство выполняет поиск маршрута в соответствующей таблице маршрутизации и размещает атрибут "Target VPN" в MPLS метке. Затем в стек меток записывается еще одна метка, определяющая путь пакета через MPLS сеть к точке его выхода из нее. Верхняя метка используется внутренними маршрутизаторами для пересылки пакета, а нижняя как раз и позволяет пограничному устройству на точке выхода определить таблицу маршрутизации, к которой относится поступивший со стороны MPLS сети пакет.

Таким образом, технология BGP/MPLS VPN действительно позволяет виртуализировать магистральный участок НОТС, что было подтверждено опытной эксплуатацией описанных методов, проведенной в ЮФУ. Эксперименты по исследованию применения технологии BGP/MPLS VPN проводились на оборудовании производства Cisco systems, применяемом в сети ЮФУ: маршрутизаторах серий 7206, 3640, 3660 и 3745 и коммутаторах серий 2924, 2950-24 и 3550-24. Следует отметить, что коммутаторы серии 2950-24 непригодны для решения требуемой задачи, так как они позволяют передавать пакеты размером не более 1522-х байт. В то же время для передачи пакетов, дополненных двумя метками, как предполагает технология BGP/MPLS VPN, необходимо передавать пакеты размером до 1530 байт.

ЛИТЕРАТУРА:

1. Rosen E., Rekhter Y., BGP/MPLS VPNs, RFC 2547, March 1999
2. Bates T., Chandra, R., Katz D., Rekhter Y., Multiprotocol Extensions for BGP4, RFC 2283, February 1998