НОВЫЕ СТАНДАРТЫ АДАПТИВНОГО УПРАВЛЕНИЯ СЕТЕВОЙ ИНФРАСТРУКТУРОЙ

[1]Сосенушкин С.Е.

[1]Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технологический университет «СТАНКИН», 127994, Россия, г. Москва, Вадковский пер., 3а, e-mail: ss@stankin.ru

Представлены результаты анализа перспектив применения новых стандартов и спецификаций программного конфигурирования информационно-телекоммуникационных сетей с учетом специфики области применения – центры обработки данных и инновационные предприятия. Результаты анализа подтверждены серией модельных экспериментов на основе имитационной программной модели исследуемой сети. Отмечена необходимость стандартизации указанных технологий.

Ключевые слова: программно-конфигурируемая сеть, информационно-телекоммуникационная сеть, протокол Openflow, адаптивное управление трафиком.

NEW STANDARDS FOR NETWORK INFRASTRUCTURE ADAPTIVE MANAGEMENT

[1] Sosenushkin S.E.

[1]Federal State Educational Institution of Higher Education "Moscow State Technological University" STANKIN "(FGBOU IN" MSTU "STANKIN"), 127055, Russia, Moscow, Vadkovsky lane, 3a, e-mail: ss@stankin.ru

The results of the analysis of prospects for the adoption of new standards and specifications, software configuration information and telecommunication networks, taking into account the specifics of the application - data centers and innovative enterprises. Results of the analysis confirmed a series of simulation experiments based on a simulation program model studied network. There was a need to standardize these technologies.

Keywords: software-defined networks, SDN, OpenFlow protocol, adaptive traffic management.

Введение

Компьютерные сети являются стратегическим фактором развития почти всех современных информационных технологий, однако сетевая архитектура, основы которой формировались еще во второй половине шестидесятых годов прошлого столетия, устарела и на данный момент не всегда способна адекватно и эффективно отвечать динамично растущим потребностям рынка. Внедрение новых технологий, предназначенных для решения этой проблемы, таких как SDN, создает дополнительные риски, т.к. для них еще не накоплен достаточный опыт применения, а многие из них еще только являются объектом стандартизации. Настоящая статья посвящена анализу перспектив применения и стандартизации указанных технологий.

Сегодня одним из важнейших критериев большинства организаций является способность адаптации к современным быстроменяющимся условиям. Сетевые технологии являются главным фактором, влияющим на быстроту адаптации бизнес-процессов. Информационно-телекоммуникационная сеть рассматривается как совокупность сервисов, предоставляющих различные услуги, а не как совокупность компьютеров, соединенных между собой кабелем. Множество домашних, коммерческих и мобильных сетевых тенденций продвигаются в основном за счёт комбинаций трафика видео, социальных сетей, и современных мультиплатформенных приложений. По статистике, собранной и подсчитанной компанией Cisco Systems, совокупный мировой IP-трафик только за последний год вырос в 1,5 раза и будет увеличиваться еще не менее чем в четыре раза в течение ближайших пяти лет [5].

Отметим основные тренды, появившиеся в последние несколько лет и значительно повлиявшие на мировую вычислительную инфраструктуру, такие как развитие облачных технологий, взрывной рост мобильности устройств, рост трафика и изменение его структуры (по прогнозам аналитиков к 2018 году объем трафика

увеличится в четыре раза по отношению к 2015 г., 90% составляет видеотрафик), а также несоответствие темпов роста трафика и темпов роста доходов операторов [5]. В связи с ростом значимости облачных вычислений возрастает значение специализированных центров обработки данных. В связи с этим телекоммуникационное оборудование и каналы передачи данных ЦОД испытывают постоянно возрастающие нагрузки, нередко превышающие номинальную производительность.

Появляются факторы, требующие повышенной гибкости сетевых ресурсов и устройств ЦОДов [7]:

– диверсификация приоритетов различных типов трафика;
– непредсказуемость перегрузок конечных устройств;
– отсутствие гибкости сетевых протоколов;
– ограничения пропускной способности физической среды передачи данных.

В процессе решения этих задач традиционными средствами балансировки трафика, такими как адаптивная маршрутизация, возникают новые проблемы [7]:

– расход ресурсов сетевых каналов и устройств на передачу множества сервисных сообщений протоколов маршрутизации;
– трудоёмкость перенастройки сети в горячем режиме;
– ограничения и сложность настройки различных сценариев для работы сетевых устройств по ситуации.

Обеспечение гибкости управления потоками трафика в обход вышеперечисленных трудностей возможно с использованием технологии программного конфигурирования сетей.

Программно-конфигурируемые сети (далее ПКС) – это относительно новый вид сетевой архитектуры (концепция появилась в 2006 году), отделяющий управление сетью от передачи данных и позволяющий автоматизировать процесс настройки и администрирования сетевого оборудования. Как и в традиционных информационно-телекоммуникационных сетях, данные передаются по каналам связи между коммутаторами. Однако в ПКС данные управления передаются по специальным каналам связи между специальными управляющими устройствами (контроллерами) и коммутаторами. Принципиальное отличие архитектуры ПКС от традиционной архитектуры заключается в том, что обзор поведения сети происходит не с позиции взаимодействия сетевых устройств, а с точки зрения их пользовательских свойств, при этом приведение в соответствие этих концепций ложится на контроллер.

Контроллер – сетевая операционная система, используемая для управления таблицами потоков коммутаторов, на основании которых принимается решение о передаче принятого пакета на конкретный порт коммутатора. Таким образом в сети формируются прямые сетевые соединения с минимальными задержками передачи данных и необходимыми параметрами. Это управление заменяет или дополняет работающую на коммутаторе или маршрутизаторе встроенную программу, осуществляющую построение маршрута, создание карты коммутации и т.д.

Openflow — это первый стандартизованный протокол управления процессом обработки данных, передающихся по сети передачи данных маршрутизаторами и коммутаторами, реализующий технологию программно-конфигурируемой сети. Протокол используется для управления сетевыми коммутаторами и маршрутизаторами с центрального устройства — контроллера сети (например, с сервера или даже персонального компьютера). Коммутаторы с поддержкой Openflow выпускаются под ведущими мировыми брендами (Extreme Networks, Juniper, Cisco, HP, IBM, NEC и др.), а Google использует ПКС во внутренней сети своих распределённых центров обработки данных [6]. В настоящее время все крупные производители сетевого оборудования состоят в консорциум ONF (Open Networking Foundation), нацеленный на развитие и стандартизацию технологий SDN, в частности развитии и поддержки протокола OpenFlow [3].

В основе технологии ПКС лежит ряд идей, принципиально отличающих их от классических сетей. Главная из них архитектурная – разделение процессов передачи и управления данными на два разных архитектурных уровня, отдельно для контроллеров и коммутаторов. Между ними работает единый, унифицированный, не зависящий от вендора интерфейс (например, OpenFlow). Контроллер и реализованные поверх него сетевые приложения осуществляют логически централизованное управление сетью. Программная реализация уровня управления обуславливает возможность виртуализация сетевой инфраструктуры.

Однако, как и любая технология на ранних этапах развития, ПКС имеет ряд недостатков. Среди них выделяется отсутствие четких требований к устройствам и протоколам, обусловленное отсутствием международных стандартов на ПКС, что может вызывать проблемы несовместимости различных решений. Кроме этого, технологии ПКС пока не имеют широкого распространения в индустрии ИТ, и с этим связан недостаток специалистов, способных внедрять решения на основе ПКС. Наконец, внедрение ПКС несет финансово-экономические риски, обусловленные высокой стоимостью проприетарных решений, и недостаточной надежностью решений открытых. Как следствие, на рынке пока что присутствуют только гибридные коммутаторы с поддержкой Openflow, стоимость которых выше, чем у традиционных сетевых устройств.

На основании обзора проблем и пробелов современных информационно-телекоммуникационных сетей [1-2, 4], а также общих рекомендаций TIER к проектированию центров обработки данных, был сформирован следующий список требований к участкам информационно телекоммуникационных сетей центров обработки данных с применением технологии ПКС:

– балансировка трафика по приоритету скорости;
– изоляция потоков данных на уровне доступа;
– гибкость конфигурирования;
– экономия сетевого оборудования;
– отказоустойчивость.

С учетом обозначенных требований разработан проект участка сети на основе ПКС. Его 3-уровневая архитектура представлена на рисунке 1. На верхнем уровне: прокси-сервер FlowVisor и 2 ПКС-контроллера, на среднем – 4 openflow-коммутатора. Ниже – терминальное оборудование: серверы и компьютеры. h1, h2, h3, h4 – экземпляры конечного оборудования, использованные в эксперименте. В целях упрощения модели выхода в интернет не предусмотрено.

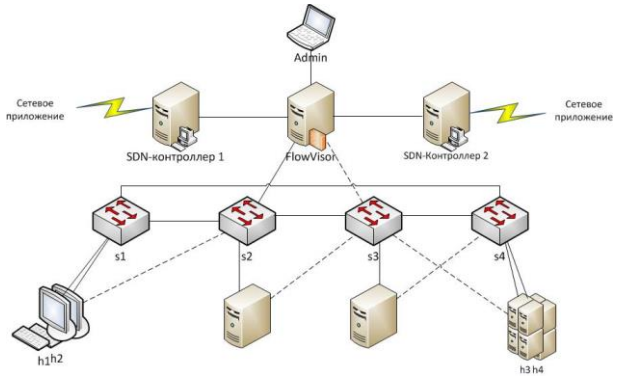

Рис. 1. Принципиальная схема экспериментального участка сети

При необходимости возможна реализация подключения к внешним сетям или расширение сети для обеспечения дополнительных функций через один из коммутаторов.

Для обоснования эффективности предложенного решения разработана имитационная модель описанного участка сети. Модель использована для проведения серии экспериментов по оценке влияния конфигурации сети на эффективность участка сети при различных условиях загрузки канала, в том числе, при полной загрузке.

Для выполнения эксперимента были использованы следующие открытые (open source) программные средства:

– Ubuntu 14.04 64-bit– внешняя операционная система;
– Mininet 2.1.0 – эмулятор программно-конфигурируемой сети;
– FlowVisor 1.4.0 – инструментальное средство, агрегирования команд нескольких контроллеров для изоляции срезов ПКС;
– Beacon 1.0.4 – сетевая операционная система.

В этой среде на основе схемы проекта созданы две программные модели. На рисунке 2 изображена их общая физическая топология.

Топология представляет собой 4 дезагрегированных коммутатора (s1, s2, s3, s4), объединённые каналом передачи данных в кольцо, и четыре конечных устройства, подключенных к двум из них, находящихся на расстоянии двух хопов друг от друга. Канальная пропускная способность между s1-s2, s2-s4 равна 50 Мбит/с, между s1-s3, s3-s4 – 500 Мбит/с. Серверы FlowVisor и контроллеров, а также подключения к ним, запускаются во внешней среде, поэтому на схеме отсутствуют.

Первый эксперимент проведён с моделью, в которой имеет место логическое разделение сети на виртуальные срезы по доменному принципу по аналогии с технологией VLAN. Пакет, отправленный из среза Up, не сможет достичь хостов среза Down в соответствии соображениям безопасности.

Суть деления сети на виртуальные срезы – делегирование управления потоками между срезами. OpenFlow позволяет гибко определять эти потоки. В контексте центра обработки данных такое деление оправдано как из соображений безопасности, так и для удобства распределения производственных мощностей между клиентами. Результаты первого эксперимента приведены в таблице 1.

Второй эксперимент произведён с моделью, в которой произведено логическое разделение сети на виртуальные подсети по приоритетному принципу. В данной модели членство в срезах обозначается портами и приоритетом скорости входящего/исходящего трафика в пределах одной физической сети, хотя доступны также варианты организации по IP и MAC адресам сетевых интерфейсов.

В контексте центра обработки данных такое деление оправдано в качестве решения для организации балансировки трафика в условиях ограниченного количества сетевых устройств. Подобное сетевое решение реализуемо и методами традиционной организации сетей. Однако, в этом случае администратору придётся на каждом коммутаторе вручную определять правила управления доступом для направления трафика с того или иного интерфейса на целевой сервер или порт по нестандартному маршруту. Разница в том, что методами ПКС, и FlowVisor в частности, эти политики могут быть более гибкими, т.к. контроллер среза с высокой пропускной способностью может более динамично маршрутизировать трафик и определять приоритеты для динамических срезов трафика. Результаты второго эксперимента приведены в таблице 2.

Таблица 1

Средние значения пропускной способности (эксперимент 1)

Канальная ПС, Мбит/с	Показания со стороны сервера		Показания со стороны клиента	
	Фактическое время теста, сек	Информационная ПС, Мбит/с	Фактическое время теста, сек	Информационная ПС, Мбит/с
1	159,8	0,912	107,3	1,36
10	102,8	9,55	102,2	9,63
50	102,2	47,5	100,5	48,3
500	100,3	455	100,1	456

Таблица 2

Средние значения пропускной способности (эксперимент 2)

Канальная ПС, Мбит/с	Показания со стороны сервера		Показания со стороны клиента	
	Фактическое время теста, сек	Информационная ПС, Мбит/с	Фактическое время теста, сек	Информационная ПС, Мбит/с
1	159,8	0,914	107,2	1,368
10	102,8	9,53	102,2	9,63
50	102,0	46,8	100,2	47,4
500	100,3	455	100,1	456,6

Проведенный анализ экспериментальных данных позволяет сделать следующие выводы.

Политики деления сети на логические срезы не оказывают негативного влияния на информационную пропускную способность.

Спроектированное архитектурное решение наиболее эффективно при высокой загрузке каналов передачи данных, что даёт наиболее благоприятный баланс между показателями пропускной способности и задержек. Следовательно, областью возможного применения предложенного решения являются высоконагруженные участки информационно-телекоммуникационных сетей.

Выбор используемой сетевой операционной системы и сетевых приложений может оказывать влияние на информационную пропускную способность. Необходимо учитывать этот фактор при выборе сетевой операционной системы.

Результаты работы могут быть использованы как основа для дальнейших исследований в области оценки и повышения эксплуатационных характеристик информационно-телекоммуникационных сетей, а также в области виртуализации сетевого оборудовании и комбинации виртуальных устройств с физическими.

Заключение

Технологии ПКС эффективно справляются с задачей повышения гибкости управления сетевой инфраструктурой и ее адаптации к быстро меняющимся информационным потокам. Однако следует отметить недостаточную взаимную совместимость отельных элементов, устройств и решений в исследуемой предметной области. Для снижения рисков интероперабельности необходима работа по стандартизации технологий ПКС на международном и национальном уровнях.

Список литературы

1. Левин М.В., Сосенушкин С.Е., Климанов В.П. Анализ способов модернизации университетской корпоративной сети / Левин М.В., Сосенушкин С.Е., Климанов В.П. // Вестник МГТУ «СТАНКИН», № 4(27). М.: ФГБОУ ВПО МГТУ «СТАНКИН», 2013 г., С. 92-98

2. Левин М.В., Сосенушкин С.Е., Климанов В.П. Анализ эффективности университетской корпоративной сети на основе использования математического аппарата сетей массового обслуживания // Вестник МГТУ «СТАНКИН», № 4(31). М.: ФГБОУ ВПО МГТУ «СТАНКИН», 2014 г., С. 175-181

3. Смелянский Р.Л., Программно-конфигурируемые сети [Электронный ресурс] / Р.Л. Смелянский // Открытые системы 2012 – № 09 – Режим доступа: http://www.osp.ru/os/2012/09/13032491 (дата обращения 16.05.2015)

4. Сосенушкин С.Е. Адаптивная маршрутизация сетевых пакетов на основе балансировки трафика. / Сосенушкин С.Е. – М.: ФГБОУ ВПО МГТУ «СТАНКИН», 2012. – 82 с.

5. Cisco Visual Networking Index: Forecast and Methodology, 2014-2019 White Paper May 27, 2015 [Электронный ресурс] – Режим доступа: http://www.cisco.com/c/en/us/solutions/ collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_ c11-481360.html (дата обраще-ния 16.05.2015)

6. Steven Levy. Going With the Flow: Google's Secret Switch to the Next Wave of Networking [Электронный ресурс] // WIRED – Режим доступа: http://www.wired.com/2012/04/going-with-the-flow-google/ (дата обращения 16.05.2015)

7. Software-Defined Networking: The New Norm for Networks ONF White Paper April 13, 2012 [Электронный ресурс] – Режим доступа: https://www.opennetworking.org/images/stories/downloads/sdn-resources/ white-papers/wp-sdn-newnorm.pdf (дата обращения 16.05.2015)

Reference

1. Levin M.V., Sosenushkin S.E., Klimanov V.P. Analysis of ways to modernize the university corporate network / Levin MV Sosenushkin SE, Klimanov VP // Vestnik MSTU "STANKIN», № 4 (27). M .: MSTU VPO "STANKIN", 2013, C. 92-98

2. Levin M.V., Sosenushkin S.E., Klimanov V.P. Analysis of the effectiveness of university corporate network through the use of mathematical apparatus of queuing networks // Vestnik MSTU "STANKIN», № 4 (31). M .: MSTU VPO "STANKIN" 2014, C. 175-181

3. Smelyanskiy R.L. Software-configurable network [electronic resource] / RL Smelyanskiy // Open Systems in 2012 - number 09 - Access mode: http://www.osp.ru/os/2012/09/13032491 (reference date 05/16/2015)

4. Sosenushkin S.E. Adaptive routing network packets based on traffic balancing. / Sosenushkin SE - M .: MSTU VPO "STANKIN", 2012. - 82 p.

5. Cisco Visual Networking Index: Forecast and Methodology, 2014-2019 White Paper May 27, 2015 [electronic resource] - Access mode: http://www.cisco.com/c/en/us/solutions/ collateral / service- provider / ip-ngn-ip-next-generation-network / white_paper_ c11-481360.html (the date of the Treatment of 05.16.2015)

6. Steven Levy. Going With the Flow: Google's Secret Switch to the Next Wave of Networking [Electronic resource] // WIRED - Access: http://www.wired.com/2012/04/going-with-the-flow-google/ (treatment 16/05/2015) date

7. Software-Defined Networking: The New Norm for Networks ONF White Paper April 13, 2012 [electronic resource] - Access mode: https://www.opennetworking.org/images/stories/downloads/sdn-resources/ white-papers /wp-sdn-newnorm.pdf (reference date 05/16/2015)