



Локтионов
Олег Викторович,
начальник ЦИТСиЗИ ГУ МВД России
по г. Санкт-Петербургу и Ленинградской области,
полковник внутренней службы

Анализ концепции программно-конфигурируемых сетей как способа построения современной региональной сети связи МВД России

Существующие в настоящее время региональные сети связи МВД России, как собственные, так и доверенных операторов, имеют традиционную многоуровневую и многопротокольную архитектуру, которая была разработана в 70–80-е гг. прошлого века. В ее основе лежит стек протоколов TCP/IP и множество других сетевых протоколов и технологий, созданных к данному моменту в рамках модели взаимосвязи открытых систем Международного союза электросвязи (OSI ISO). Этим обусловлены как несомненные достоинства с позиций апробированности унификации и распространенности, применяемых технических и технологических решений, так и наличие ряда ограничений и недостатков, присущих принятому подходу к проектированию сетевой инфраструктуры и выбору сетевого оборудования.

Среди ограничений и недостатков можно выделить следующие:

- Многопротокольность архитектуры сетей и используемых инфокоммуникационных технологий. Совершенствование телекоммуникационных сетей в направлении увеличения их пропускной способности, количества и качества предоставляемых пользователям телекоммуникационных услуг в рамках существующей архитектуры, приводит к постоянному возникновению новых протоколов и технологий, число которых исчисляется сотнями. Существующие протоколы и технологии разрабатывались относительно независимо друг от друга (такая изоляция ле-

жит в основе многоуровневых моделей сетевой архитектуры OSI и TCP/IP). Причем многие из протоколов являются проприетарными. Это увеличивает сложность сетей и порождает проблему организации взаимодействия сетевых протоколов и технологий между собой. Настройка сетевого оборудования и администрирования сети становятся трудоемкими процессами, что необоснованно ужесточает требования к квалификации специалистов и усложняет их подготовку.

- Использование на узлах разнотипного сетевого оборудования разных производителей, в том числе иностранного производства. Это приводит к тому, что функционалы различных сетевых устройств избыточны и частично дублируют друг друга, что ведет к излишним затратам. К тому же усложняется задача сопряжения сетевого оборудования, что зачастую преодолевается путем использования дополнительных устройств сопряжения.
- Сложность архитектуры существующих телекоммуникационных сетей, а также использование для их построения разнородного телекоммуникационного оборудования, отличающегося реализованными в нем протоколами управления (в том числе проприетарными), вызывают проблему автоматизированного управления сетями. Эти же факторы существенно затрудняют решение задач обеспечения стабильности процессов функционирования сетей, достижения требуемых значений сетевых характеристик и показателей качества обслуживания пользователей.
- При существующем подходе к построению телекоммуникационных сетей МВД России ограничены возможности по обеспечению гибкости и масштабируемости сетевой

инфраструктуры и сетевого телекоммуникационного оборудования.

Одним из перспективных направлений развития телекоммуникационных сетей является переход к новой концепции сетевой архитектуры, получившей наименование программно-конфигурируемых сетей [1–4].

Программно-конфигурируемая сеть¹ — это новый подход к построению архитектуры инфокоммуникационных сетей, при котором уровень управления сетью (состоянием сетевой инфраструктуры и потоками данных в сети) и уровень передачи данных (инфраструктурный уровень) разделяются за счет переноса функций управления (выполняемых в традиционной сети маршрутизаторами и коммутаторами) на отдельное центральное устройство, называемое контроллером. Такой подход позволяет уровню управления абстрагироваться от физической сетевой инфраструктуры уровня передачи данных, используя некоторое логическое представление сети.

Основные идеи, которые закладывались в ПКС, заключаются в следующем [1–4]:

- разделение процессов передачи и управления данными;
- централизованное управление сетью, осуществляемое с помощью специализированного контроллера ПКС;
- унифицированный открытый интерфейс между уровнем управления и уровнем передачи данных;
- виртуализация физических ресурсов сети и сетевых функций.

Архитектура ПКС имеет три уровня: - инфраструктурный уровень (уровень передачи данных) включает набор сетевых устройств (коммутаторов, маршрутизаторов) и каналов передачи данных;

¹ Далее «ПКС».



- уровень управления, представленный центральным контроллером с сетевой операционной системой (ОС), на котором реализуются функции мониторинга текущего состояния сетевого оборудования уровня передачи данных, распределения потоков в сети и функции управления сетевыми устройствами. Уровень управления взаимодействует с уровнем передачи данных посредством унифицированного открытого интерфейса, а с приложениями — с помощью программного интерфейса (API);

- уровень сетевых приложений, в которых реализуются различные функции управления сетью: управление потоками данных в сети, управление безопасностью, мониторинг трафика, управление качеством сервиса, управления политиками и так далее. Архитектура ПКС представлена на рис. 1.

В ПКС все интеллектуальные функции сетевых устройств (коммутаторов, маршрутизаторов) вынесены в контроллер, который на основе оценки состояния сети формирует таблицы коммутации для каждого сетевого устройства и рассылает их всем узлам сети. Так формируется потоковая логическая структура сети, которая представляет собой совокупность виртуальных путей, подобно технологии многопротокольной коммутации по меткам (MPLS). При этом сетевые устройства по своему функционалу упрощаются и удешевляются. Настройка сетевого оборудования и сети в целом переносится с каждого сетевого устройства в контроллер, интеллектуальные функции которого (мониторинг сети, управление потоками и др.) выполняются программно-сетевой операционной системой. Конфигурацию и настройку сети можно изменять в реальном времени, а новые приложения внедрять за гораздо более короткое время, чем в традиционной архитектуре.

Система управления МВД России строится по иерархическому принципу, поэтому централизация функций управления сетью в ПКС не противоречит принятой системе управления, а применение концепции ПКС представляется возможным для построения сетей МВД России, начиная с регионального уровня и выше.

Одной из наиболее перспективных и развивающихся реализаций подхода программно-конфигурируемых сетей является технология OpenFlow. Основными ее документами являются

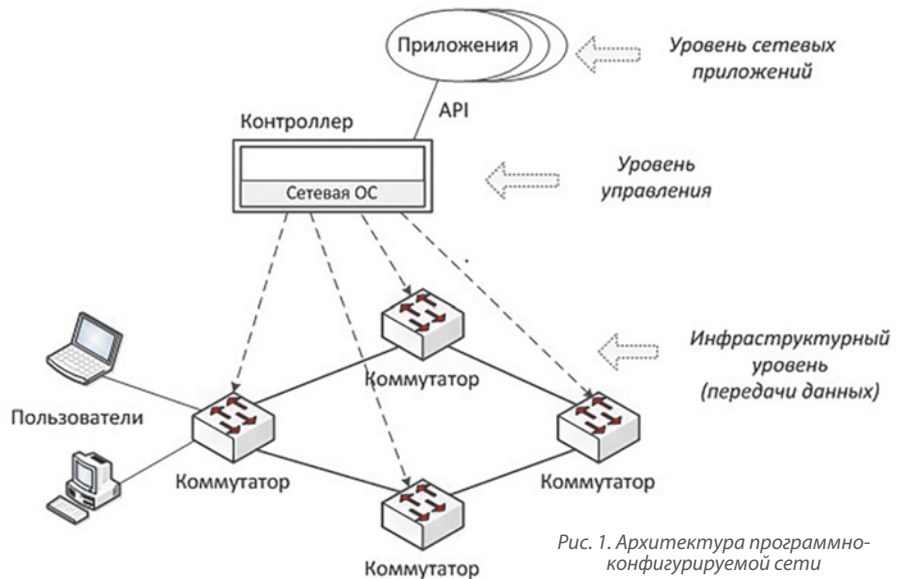


Рис. 1. Архитектура программно-конфигурируемой сети

спецификации OpenFlow [5, 6], в которых описываются основные компоненты OpenFlow-сети, принципы работы и взаимодействия компонентов (протокол OpenFlow). Стандартизирующей организацией для спецификации является ONF — Open Networking Foundation.

Отдельно следует остановиться на виртуализации физических ресурсов сети и сетевых функций. Технологии виртуализации (VLAN, VPN-MPLS, VPN-IPSec, VXLAN, NVGRE, STT и др.), предполагающие решение задач логической структуризации сетей, широко используются в существующих телекоммуникационных сетях и на центрах обработки данных².

Виртуализация сетевых функций или NFV (network function virtualization) [1, 7], в отличие от традиционных технологий виртуализации, означает, что специализированные для выполнения отдельных функций программно-аппаратные сетевые устройства заменяются на программное обеспечение, работающее на процессорах общего назначения и устанавливаемое на комплексной платформе виртуализации сетей. NFV отличается от традиционных способов виртуализации и тем, что вместо отдельных программно-аппаратных решений для реализации каждой функции виртуализируемая сетевая функция может включать классы взаимосвязанных функций для предоставления телекоммуникационных услуг (сервисов), а также облачные инфраструктуры.

Виртуализация сетевых функций возможна во всей сети, или в тех ме-

стах, где она наиболее эффективна и экономически оправдана: в ЦОД, в сетевых узлах и подсетях пользователей.

В инфокоммуникационных сетях МВД России перспективным представляется использование ЦОД не только для выполнения функций хранения и обработки данных, но и управления сетями, начиная с регионального уровня и выше. Применительно к управлению виртуальными сетями в ЦОД технология ПКС позволяет вынести всю логику управления сетевым оборудованием в контроллер и таким образом централизовать и автоматизировать управление сетью.

Использование технологии ПКС позволит разбивать трафик сети на различные классы (потоки) и реализовывать свою логику управления для каждого потока или группы потоков. В качестве примера использования ПКС для разделения уровня управления в виртуальных сетях можно привести средство FlowVisor (рис. 2). FlowVisor выделяет заданные множества потоков в отдельные срезы сети (slices), каждый из которых имеет свое логическое представление сети и логику управления [1, 7]. Срез сети определяется множеством потоков, передаваемых в данном срезе, и логическим представлением топологии сети (маршрутизаторы, коммутаторы, порты коммутаторов, соединения).

С точки зрения архитектуры ПКС, FlowVisor является прокси-сервером между сетевыми устройствами и контроллером ПКС. К одному FlowVisor может быть подключено несколько контроллеров, реализующих различную логику управления, каждый из которых управляет своим срезом сети.

² Далее «ЦОД».

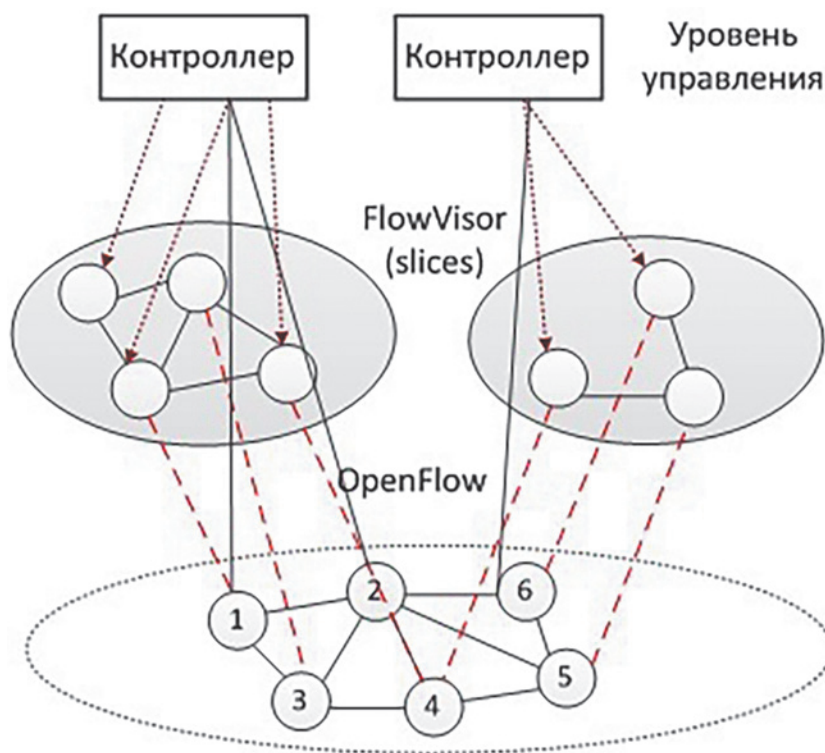


Рис. 2 Виртуализация сетевых функций с использованием FlowVisor

FlowVisor определяет, какие потоки относятся к той или иной логической виртуальной сети и, следовательно, могут управляться соответствующим контроллером, предоставляет каждому контроллеру собственное видение логической структуры сети и обеспечивает логическое разделение сетевых ресурсов. Таким образом, FlowVisor позволяет создавать виртуальные сети, разделяющие как уровень передачи данных, так и уровень управления.

Виртуализация сетевых функций в сетях ПКС как способа построения современной региональной сети связи МВД России позволит:

- повысить гибкость сетей и услуг, т. е. своевременно и легко развертывать или реконфигурировать сети, запускать новые услуги;
- повысить масштабируемость сетевых ресурсов, т. е. услуги, организованные на базе программного обеспечения, позволяют более оперативно изменять объем используемых ресурсов одного и того же аппаратного обеспечения в зависимости от нагрузки;
- повысить эффективность распределения сетевых ресурсов и сбалансировать нагрузку на них;
- обеспечить не только многофункциональность, но и гибкую функциональность программно-аппаратных сетевых средств, что в свою

очередь позволяет уменьшить линейку сетевого оборудования, предназначенного для выполнения различных сетевых функций. Например, отпадает необходимость создания и эксплуатации специализированных комплексов, таких как системы видеоконференцсвязи, АТС, межсетевые экраны, средства трансляции адресов и т. д., так как их функции будут выполнять виртуальные машины, устанавливаемые на платформе виртуализации;

- повысить безопасность за счет изоляции потоков разных пользователей и приложений в рамках одной физической сети;
- снизить стоимость, т. к. гибкость развертывания NFV ведет к снижению расходов на управление предоставляемыми услугами и сокращает издержки, связанные с управлением всей сетью;
- сделать жизненные циклы программного и аппаратного обеспечения независимыми друг от друга.

Разработкой стандартов ПКС и изысканиями в этом направлении в настоящее время занимается большое число отраслевых объединений и международных организаций [3], в которых участвуют заинтересованные коммерческие компании — производители сетевого оборудования, операторы сетей связи, разработчики программ-

ного обеспечения (ПО): ONE, IETF, Исследовательская группа интернет-технологий (Internet Research Task Force, IRTF), Европейский институт по стандартизации в области телекоммуникаций (European Telecommunications Standards Institute, ETSI), МСЭ-Т и др.

В России исследованиями и разработкой технологий ПКС занимается Центр прикладных исследований компьютерных сетей (Сколково), который заявил о создании первого российского ПКС-контроллера Runos [8], а также ряд других организаций.

Таким образом, учитывая потенциал отечественных разработок, а также существенный положительный эффект от внедрения рассмотренного подхода, можно сделать вывод о перспективности применения технологичной программно-конфигурируемых сетей для построения региональных сетей связи МВД России.

Список использованных источников:

1. Р. Л. Смелянский. Технологии SDN и NFV: новые возможности для телекоммуникаций. «Вестник связи» // январь, 2014 г.
2. А. А. Красотин, И. В. Алексеев. Программно-конфигурируемые сети как этап эволюции сетевых технологий // Моделирование и анализ информационных сетей, Т. 20, № 4, 2013.
3. В. А. Ефимушкин, Т. В. Ледовских, Д. М. Корабельников, Д. Н. Языков. Международная стандартизация программно-конфигурируемых сетей // «ЭЛЕКТРОСВЯЗЬ», № 8, 2014 г.
4. Thomas D. Nadeau, Ken Gray, SDN: Software Defined Networks, O'Reilly, 2013. 10–25 с.
5. OpenFlow Switch Specification Version 1.4.0 (Wire Protocol 0x05) October 14, 2013.
6. ONF OpenFlow Management and Configuration Protocol (OFConfig), v. 1.2.— 2014.
7. Отчет о НИР «Создание прототипа отечественной ИКС платформ управления сетевыми ресурсами и потоками с помощью сетевой операционной системы (СОС) на основе анализа и оценки существующих сетевых операционных систем для ПКС сетей и выбора одной из них для последующего развития по критериям производительности, масштабируемости, надежности, безопасности». — М.: МГУ им. М. В. Ломоносова, 2013. — 252 с.
8. [http:// www.arccn.ru/](http://www.arccn.ru/)