УДК 519.25+004.9
DOI: 10.15827/0236-235X.131.430-438
Дата подачи статьи: 17.04.20
2020. Т. 33. № 3. С. 430–438

Особенности SDN-технологии от Cisco Systems

Ю.М. Лисецкий [1], *д.т.н., генеральный директор, Yurii.Lisetskyi@snt.ua*

[1] *ДП «ЭС ЭНД ТИ УКРАИНА», г. Киев, 03680, Украина*

Статья посвящена программно-определяемым сетям, занимающим в настоящее время доминирующее положение по сравнению с классическими сетями, которые с их традиционными инструментами управления и автоматизации оказались не готовыми к современной динамике изменений конфигурации и масштабирования, а также к виртуализации. Концепция распределенного управления, при которой вся интеллектуальная составляющая работы сети была распределена по сетевому оборудованию, стала недостаточно эффективной. Именно этим обусловлено появление новой концепции и технологии SDN (Software-defined Networking) – сети, в которой уровень управления отделен от уровня передачи данных и реализован программно. Таким образом, в соответствии с концепцией SDN вся логика управления сетью должна быть изъята из сетевых устройств и реализована на отдельном сервере – SDN-контроллере.

В статье рассмотрены SDN-технологии компании Cisco Systems, их развитие и особенности. Существенное отличие этих технологий в их несоответствии основному принципу SDN, который заключается в разделении control-plane с data-plane. В своих технологиях, таких как ACI и SD-Access, Cisco сохраняет на сетевых устройствах значительный control-plane-функционал, расширив его некоторыми дополнительными возможностями. Основой данных технологий являются overlay-сети – логическая топология, используемая для виртуального соединения устройств и построенная поверх произвольной физической (underlay) топологии.

Новой технологией Cisco в области WAN-сетей является SD-WAN, представляющая собой результат применения SDN-концепции к распределенным сетям. Среда передачи SD-WAN – оверлей, работающий через Internet. Как и свойственно SDN-технологиям, в SD-WAN, в отличие от SD-ACCESS, соблюдено разделение control-plane и data-plane с вынесением функционала control-plane на отдельные специализированные устройства. Как результат смены идеологии построения enterprise-сетей компания Cisco представила новую концепцию построения сетей – DNA, которая также дает возможность на основе облачных технологий получать сервисы из облака Cisco.

Ключевые слова: *программно-определяемая сеть, концепция, принципы, технология, топология, функционал, сервер, контроллер, виртуализация, сервисы, облако.*

Классические сети с их традиционными инструментами управления и автоматизации оказались не готовыми к современной динамике изменений конфигурации и масштабирования, а также к требованиям виртуализации [1]. Концепция распределенного управления, при которой вся интеллектуальная составляющая работы сети распределена по сетевому оборудованию, недостаточно эффективна [2]. Именно этими причинами было обусловлено появление новой концепции и технологии SDN (Software-defined Networking – программно-определяемая сеть) [3].

В сети SDN уровень управления отделен от уровня передачи данных и реализован программно [4]. Таким образом, в соответствии с концепцией SDN вся логика управления сетью должна быть изъята из сетевых устройств и реализована на отдельном сервере – SDN-контроллере [5], а сетевые устройства должны ограничиться функционалом data-plane и специальным программным интерфейсом, позволяющим SDN-контроллеру управлять работой их data-plane [6]. Функционал, связанный с конфигурированием и визуализацией, также выносится на отдельный уровень (Application Layer) и может быть реализован за пределами SDN-контроллера (рис. 1).

Взаимодействие SDN-контроллера с сетевыми устройствами происходит через его интерфейс, носящий название Southbound Interface (южный интерфейс). С различными приложениями контроллер взаимодействует через так называемый Northbound Interface (северный интерфейс).

В результате данных новшеств заказчик получает функционально простое и недорогое сетевое оборудование, растет число его производителей на рынке, отсутствие необходимости разбираться в особенностях работы конкретного оборудования облегчает программирование сетевого функционала, привязанного к

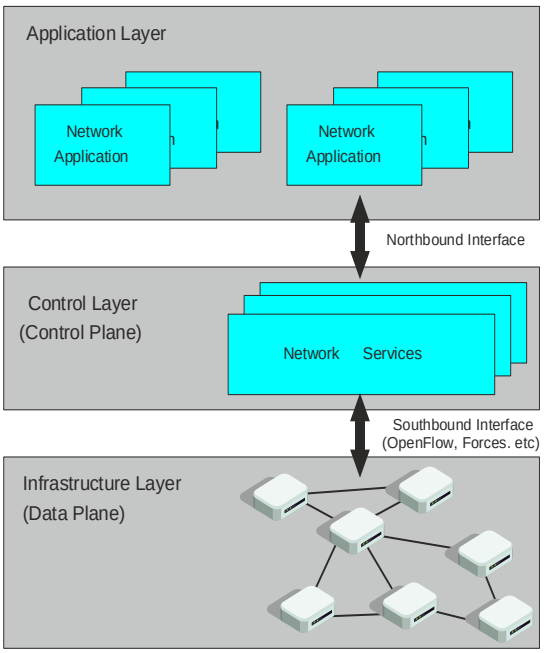

Рис. 1. Уровни SDN-сети

Fig. 1. SDN network levels

контроллеру. Наиболее распространенным протоколом взаимодействия сетевых устройств с контроллером (Southbound Interface) является протокол OpenFlow [7]. Кроме OpenFlow, используются также протоколы NETCONF и OVSDB.

Взаимодействие контроллера с приложениями (Northbound Interface) осуществляется с помощью RESTful API. REST (REpresentational State Transfer – передача состояния представления) – это архитектурный стиль взаимодействия компонентов распределенного приложения в сети [8]. Данному стилю могут соответствовать и HTTP-запросы, в теле которых могут использоваться такие форматы представления данных, как JSON и XML. К веб-сервису, соответствующему REST, применяется термин RESTfull. Сервис RESTfull API позволяет разработчикам создавать приложения для управления сетью без необходимости изучения работы конкретных сетевых устройств.

Изменения вектора развития сетевых технологий вынуждают всех участников ИТ-рынка обратить пристальное внимание на технологию SDN, которая весьма привлекательна для заказчиков. Именно поэтому организация Open Network Foundation (ONF) объединила множество производителей SDN на базе протокола OpenFlow, что укрепило его позиции и перспективы [9].

Программно-определяемая сеть от компании Cisco Systems

Компания Cisco Systems, являющаяся мировым лидером в области сетевых технологий, также не оставила без внимания SDN-технологию. Cisco создала собственный аналог OpenFlow под названием OpFlex [10]. Компания рассчитывает со временем превратить OpFlex в отраслевой стандарт. Тем не менее, сегодня Cisco в контексте SDN представляет технологии, концептуально отличающиеся от SDN, но похожие на него внешне.

Сходство состоит в возможности централизованного управления сетями и большой гибкости. Различие – в несоответствии данных решений основному принципу SDN, который заключается в разделении control-plane с data-plane. В своих технологиях, таких как ACI и SD-Access, Cisco сохраняет на сетевых устройствах значительный control-plane-функционал, расширив его некоторыми дополнительными возможностями [11]. Основой данных технологий являются overlay-сети – логическая топология, используемая для виртуального соединения устройств и построенная поверх произвольной физической (underlay) топологии (рис. 2).

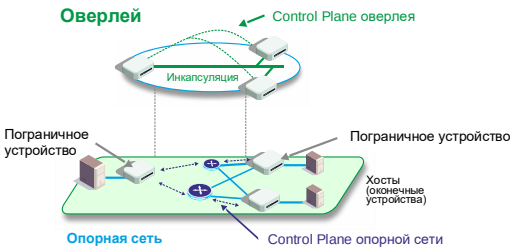

Рис. 2. Опорная и виртуальная сети

Fig. 2. Backbone network and virtual network

Поверх физической инфраструктуры строятся туннели, например VXLAN, LISP, являющиеся основой для желаемой логической топологии, которая может в корне отличаться от топологии опорной сети [12]. В технологии активно используются такие инструменты, как OSPF или IS-IS, VXLAN, LISP, VRF, Cisco TrustSec [13]. Инкапсуляция для VXLAN внутри SD-ACCESS представлена на рисунке (см. http://www.swsys.ru/uploaded/image/2020-3/2020-3-dop/5.jpg).

Одним из базовых инструментов SD-Access является Cisco TrustSec (CTS) [14]. Кроме того,

CTS выделяется в отдельную плоскость управления – policy-plane, позволяющую на основе TrustSec гибко настраивать ограничения доступа к сети, легко применяя их на границе сети, в том числе и на уровне доступа (см. http://www.swsys.ru/uploaded/image/2020-3/2020-3-dop/6.jpg). Появляется возможность использовать профилирование пользователей, применяя к ним специальные группы доступа. Принадлежность пользователя к конкретной группе доступа определяется в процессе аутентификации. Далее всему входящему трафику пользователя назначается специальный тег – SGT (Security Group Tag), что позволяет не учитывать IP-адреса при управлении доступом [15].

Технология в принципе снимает ограничения, накладываемые на IP-адресацию. Кроме удобного управления доступом, это также значит, что благодаря overlay адресация больше не привязана к физическому расположению устройств и их логическому группированию (как, например, принадлежность к общему VLAN), что дает возможность пользователям стать мобильными.

Опорная сеть представляет собой единую сетевую фабрику, построенную в соответствии с Leaf-and-Spine-архитектурой. Набор компонентов сети представлен на рисунке 3.

Как видно из рисунка, в составе сети присутствуют также такие компоненты управления и мониторинга, как DNA Center и ISE [16]. Это основные точки взаимодействия администратора с сетью, позволяющие достаточно легко осуществлять централизованное управление и визуализацию вне зависимости от ее физической инфраструктуры и значительно сократить объем работы по конфигурированию сети. SD-Acces успешно работает с беспроводными сетями (см. http://www.swsys.ru/uploaded/image/2020-3/2020-3-dop/7.jpg).

Как обычно, точки доступа (AP) используют Wireless Controller (WLC) и могут работать в составе SD-Access-сети как в традиционном режиме local mode, так и в fabric mode, дающем ряд принципиальных преимуществ. Точка доступа (AP) в fabric mode-режиме на уровне control-plane взаимодействует с WLC, однако в качестве data-plane используется VXLAN, который устанавливается между AP и Fabric Edge-устройством (см. http://www.swsys.ru/uploaded/image/2020-3/2020-3-dop/8.jpg).

Необходимым требованием является непосредственное подключение точки доступа к коммутатору фабрики. Контроллер (WLC) также должен поддерживать данный режим работы. Режим fabric mode позволяет трафику клиента оптимально использовать ресурсы сети в обход WLC. Благодаря VXLAN-инкапсуляции прозрачно использовать SGT (см. http://www.swsys.ru/uploaded/image/2020-3/2020-3-dop/9.jpg) и Virtual Networks (VNs) (см. http://www.swsys.ru/uploaded/image/2020-3/2020-3-dop/10.jpg).

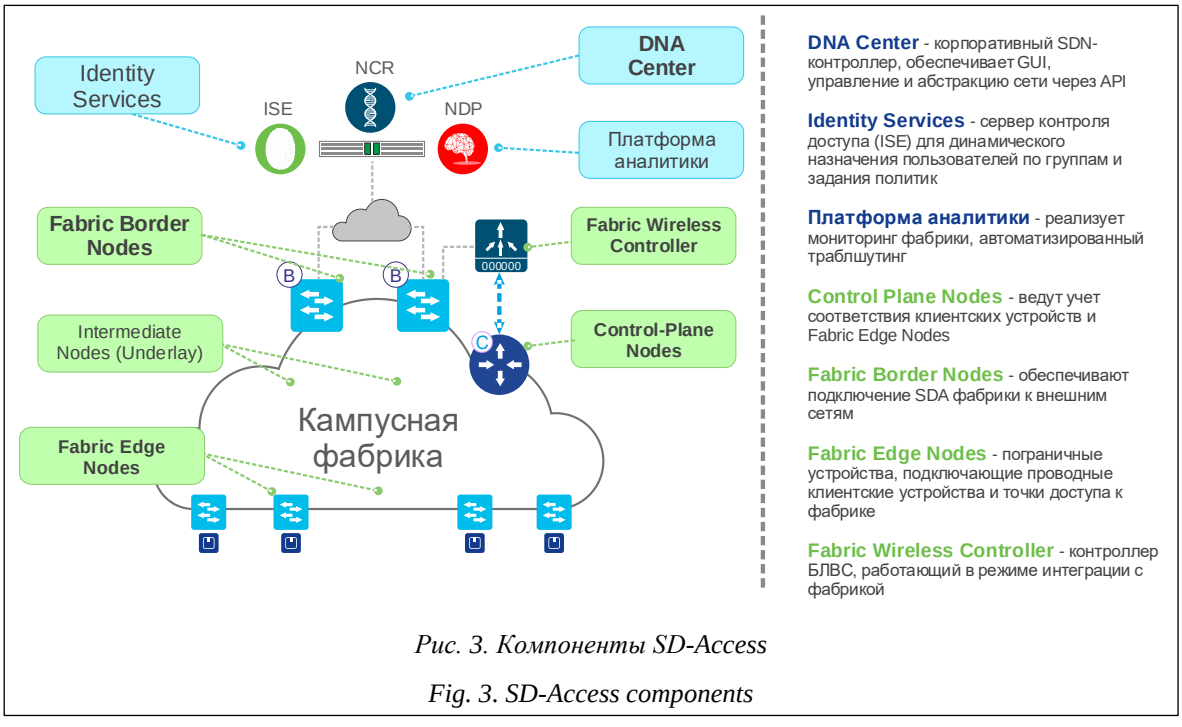

Рис. 3. Компоненты SD-Access

Fig. 3. SD-Access components

Технология SD-WAN

Традиционные глобальные сети перестали удовлетворять достаточно большому количеству современных требований, среди которых простота развертывания и администрирования, легкая масштабируемость, гибкость конфигурации, мобильность клиентов, высокая пропускная способность, надежные средства защиты информации, обеспечение качества работы приложений. Новые требования к дизайну и функционалу WAN определили дальнейшие перспективные направления работы для основных производителей сетевых технологий.

Новой технологией Cisco в области WAN-сетей является SD-WAN, которая базируется на разработках поглощенной Cisco компании Viptela. SD-WAN – результат применения SDN-концепции к распределенным сетям [17]. Среда передачи SD-WAN – оверлей, работающий через Internet. Разработчики SD-WAN выделяют в данной технологии следующие основные преимущества: обеспечение гибкой эксплуатации, гибкой и безопасной связанности, качества работы приложений и поддержка облачных сред.

Как свойственно SDN-технологиям, в SD-WAN, в отличие от SD-ACCESS, соблюдено разделение control-plane и data-plane с вынесением функционала control-plane на отдельные специализированные устройства. Кроме того, над control-plane добавлена надстройка в виде плоскости администрирования и оркестрации, позволяющая централизованно и с минимальными затратами администрировать сеть.

Представим компоненты технологии SD-WAN (рис. 4).

- vBond. Реализует функционал оркестрации фабрики. Обеспечивает связанность между плоскостями администрирования, управления и передачи данных, является вспомогательным звеном для обхода NAT. Является начальной точкой аутентификации, передает список vSmart- и vManage-устройств на все vEdge-устройства. Требует публичного IP-адреса и высокой отказоустойчивости.
- vManage – плоскость администрирования. Обеспечивает единую консоль управления, централизованный провижинг, формирование политик и шаблонов, мониторинг и траблшутинг, обновление ПО, программный интерфейс (REST, NETCONF).
- vSMART – плоскость управления. Обеспечивает обнаружение устройств в фабрике, распространяет control-plane-информацию на все vEdge-устройства, распространяет политики data-plane и политики маршрутизации по приложениям на все vEdge-устройства и применяет политики control-plane (рис. 5).
- vEdge – data-plane. Граничные маршрутизаторы WAN. Обеспечивают безопасную передачу данных с удаленными vEdge-маршрутизаторами, а также маршрутизацию на основе политик по приложениям. Поддерживает в полном объеме стандартные протоколы маршрутизации, такие как OSPF, BGP, и протоколы внешней маршрутизации, такие как FHRP,

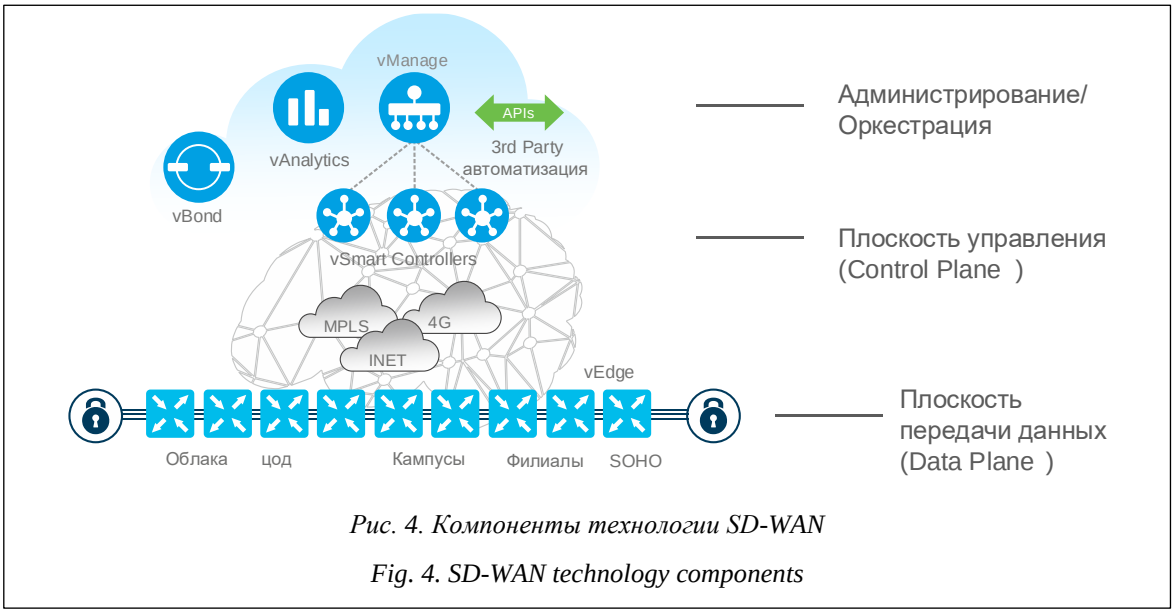

Рис. 4. Компоненты технологии SD-WAN

Fig. 4. SD-WAN technology components

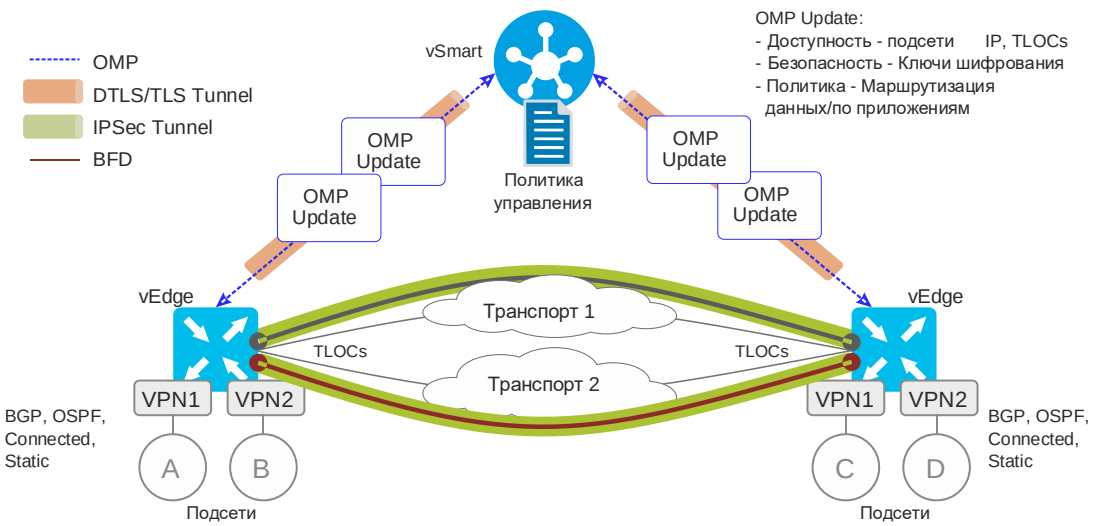

Рис. 5. Взаимодействие control-plane и data-plane в Cisco SD-WAN

Fig. 5. Interaction of control plane and data plane in Cisco SD-WAN

VRRP. Осуществляет безопасные управляющие соединения (OMP) с vSMART-контроллерами. Поддерживает ZTP (Zero Touch Provisioning). Экспортирует статистику о производительности. Устройства vEdge могут быть как физическими (100 Mbps ÷ 20 + Gbps), так и виртуальными. Контроллеры vBond, vManage, vSMART могут быть развернуты как в корпоративной сети (ESXi, KVM), так и в публичном облаке (Azure, AWS). vSmart-контроллер взаимодействует с vEdge по протоколу OMP (Overlay Management Protocol). Протокол функционирует внутри TLS/DTLS-соединений, обеспечивая ему безопасность. Внутри оверлейной сети работает BFD, что значительно повышает сходимость сети.

В отличие от iWAN инфраструктура SD-WAN может одновременно поддерживать множество независимых VPN-сетей, то есть представляет собой архитектуру Multi-tenant (см. http://www.swsys.ru/uploaded/image/2020-3/2020-3-dop/11.jpg). Каждая VPN при этом может иметь свою собственную логическую топологию.

Объединение новых технологий и DNA

Тотальное проникновение ИТ в область бизнес-процессов привело к очередному пересмотру и трансформации идеологии enterprise-сетей. Трансформация происходила сразу по нескольким направлениям: виртуализация сетевых функций (NFV – Network Functions Virtualisation), использование SDN-технологий, автоматизация процессов управления, аналитика, безопасность, использование облачных сервисов.

В результате такой трансформации сеть превращалась в унифицированную гибкую и ориентированную на работу приложений высоконадежную инфраструктуру с легко перестраиваемым и расширяемым функционалом, единым центром управления, едиными политиками безопасности, возможностью быстрого и детального анализа происходящих в ней процессов, а также с низкими операционными затратами. Компания Cisco также представила новую концепцию построения сетей – DNA (Digital Network Architecture) (рис. 6).

Функционал NFV перешел в enterprise-сегмент из операторских сетей, позволив равноценно заменить множество отдельных сетевых устройств различного назначения виртуальными сущностями внутри ограниченного набора физических устройств-хостов с возможностью почти мгновенного развертывания, клонирования и переконфигурирования (см. http://www.swsys.ru/uploaded/image/2020-3/2020-3-dop/12.jpg).

Для большинства аппаратных платформ Cisco уже существуют виртуальные версии, например, Cisco CSR 1000v (программный аналог Cisco ASR 1000), Cisco ASAv (программный аналог Cisco ASA) и др. Для хостинга

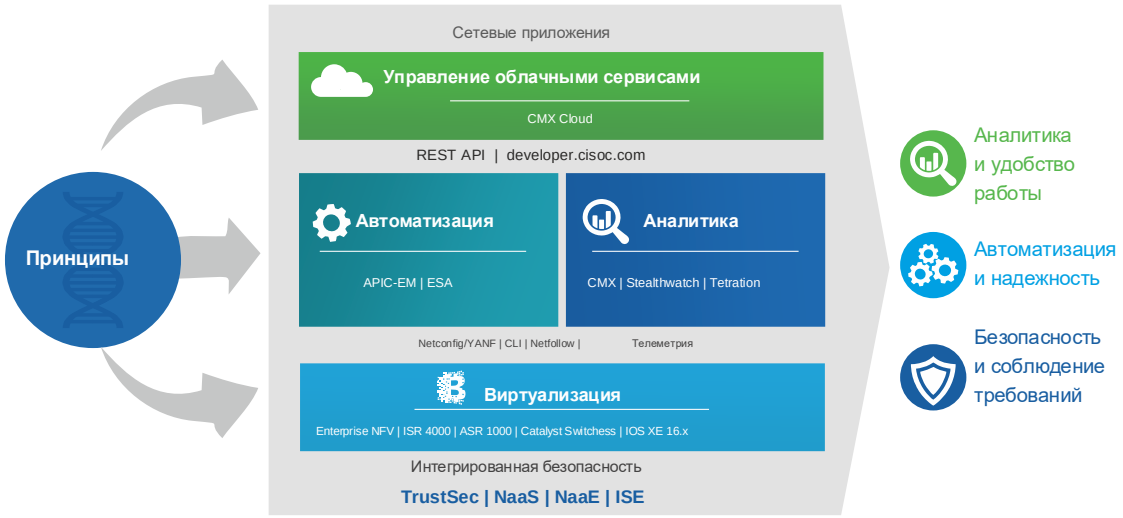

Рис. 6. Концепция DNA

Fig. 6. DNA concept

VNF можно также использовать непосредственно сетевые устройства. Например, в некоторых случаях это могут быть устройства серии Cisco Catalyst 3650/3850, Cisco ISR 4000, Cisco ASR 1000. Решение Cisco Enterprise NFV призвано обеспечить весь жизненный цикл виртуальной инфраструктуры удаленного офиса предприятия. При этом управление организовано через открытые программные интерфейсы Netconf API, RESTconf API.

Неотъемлемыми инструментами взаимодействия с сетевой инфраструктурой являются средства автоматизации. Эти инструменты сами по себе не новы, поскольку и прежний подход к организации работы сетей предполагал наличие NMS (Network Management System). Однако современный взгляд на автоматизацию предполагает гораздо более тесную интеграцию средств управления и автоматизации в сетевую инфраструктуру для обеспечения полноты управления. В больших составных сетях сложно добиться единого подхода к автоматизации, тем более возможностями единого инструментария, а DNA позволяет без особых трудностей реализовать данный подход.

В качестве инструмента автоматизации Cisco предлагает продукт Cisco Application Policy Infrastructure Controller – Enterprise Module (Cisco APIC-EM) (рис. 7). Cisco APIC-EM – первый коммерческий SDN-контроллер Cisco для корпоративной кампусной, распределенной проводной и беспроводной сетей, позволяющий взять под управление все домены корпоративной сети.

Одной из задач управления сетью, не решаемой инструментами автоматизации, является задача контроля качества предоставляемых услуг. Для ее решения служит набор программных средств аналитики DNA Аналитика. Программы аналитики получают телеметрию с устройств сетевой инфраструктуры с возможностью ее дальнейшего анализа в масштабе реального времени, например, изучения тенденций, сравнения состояний, оценки соответствия сервисов критериям качества. Примерами средств аналитики являются Cisco Tetration Analytics и Cisco Connected Mobile Experience (CMX). Cisco Tetration Analytics – это новейшая платформа от Cisco для реализации аналитики приложений и пользователей в рамках ЦОД. Cisco CMX – технология для анализа беспроводных сетей, позволяющая строить отчеты о местоположении беспроводных клиентов и профили их поведения в сети.

Безопасность сети обязательно должна быть обеспечена специальным набором инструментов, например, Cisco ISE – для контроля доступа к корпоративной сети, включающим сервисы аутентификации, авторизации и учета (AAA), оценки состояния, профилирования, а также Cisco Stealthwatch – для мониторинга и анализа безопасности сети, основанным на сборе телеметрии с сетевых устройств (см. http://www.swsys.ru/uploaded/image/2020-3/2020-3-dop/13.jpg).

Cisco ISE и Cisco Stealthwatch предъявляют особые требования к сетевому оборудованию – возможность работать и как средство контроля

Рис. 7. Применение согласованных политик в пределах составной сети

Fig. 7. Application of agreed policies within the composite network

(Network-as-Enforcer), и как сенсор (Network-as-a-Sensor).

Еще одним инструментом, активно использующимся сегодня, являются облачные сервисы. Cisco DNA к настоящему времени предлагает ряд продуктов на основе облачных технологий, которые позволяют заказчикам получать сервисы из облака Cisco или предоставлять подобные услуги самостоятельно на базе собственных ЦОДов. Один из таких продуктов – Cisco CMX Cloud – облачный вариант реализации инструментов аналитики (Connected Mobile Experience).

Заключение

В статье рассмотрены SDN-технологии компании Cisco Systems, их развитие и особенности. Существенное отличие этих технологий в их несоответствии основному принципу SDN, который заключается в разделении control-plane с data-plane. В своих технологиях, таких как ACI и SD-Access, Cisco сохраняет на сетевых устройствах значительный control-plane-функционал, расширив его некоторыми дополнительными возможностями. Основой данных технологий являются overlay-сети – логическая топология, используемая для виртуального соединения устройств и построенная поверх произвольной физической (underlay) топологии.

Новая технология Cisco в областии WAN-сетей – SD-WAN, являющаяся результатом применения SDN-концепции к распределенным сетям. Среда передачи SD-WAN – оверлей, работающий через Internet. Как и свойственно SDN-технологиям, в SD-WAN, в отличие от SD-ACCESS, соблюдено разделение control-plane и data-plane с вынесением функционала control-plane на отдельные специализированные устройства.

Как результат смены идеологии построения enterprise-сетей компания Cisco представила новую концепцию построения сетей – DNA, которая также дает возможность на основе облачных технологий получать сервисы из облака Cisco.

Таким образом, предоставленные современные технологии для построения программно-определяемых сетей заняли доминирующее положение на ИТ-рынке в сравнении с классическими сетями.

Литература

1. Лисецкий Ю.М. Виртуализация: динамика развития и перспективы // Інформаційні управляючі Системи та Технології: сб. матер. III Междунар. конф. Украина. Одесса. 2014. С. 271–273 (рус.).

2. Рыпалов С., Демин Д. Дизайн современной корпоративной LAN сети. URL: https://www.cisco.com/c/dam/m/ru_ru/training-events/2019/cisco-connect/pdf/sda_distributed_campus.pdf (дата обращения: 11.03.2020).

3. Haleplidis E. Overview of RFC7426: SDN Layers and Architecture Terminology. URL: https://sdn.ieee.org/newsletter/september-2017/overview-of-rfc7426-sdn-layers-and-architecture-terminology (дата обращения: 12.03.2020).

4. Introduction to Software Defined Networks (SDN). URL: https://www.researchgate.net/publication/311479628_Introduction_to_Software_Defined_Networks_SDN. DOI: 10.5120/ijais2016451623 (дата обращения: 11.03.2020).

5. Семеновых А.А., Лапонина О.Р. Сравнительный анализ SDN-контроллеров. INJOIT. 2018. Т. 6. № 7. С. 50–56 (рус.).

6. Control and Data Planes. URL: https://networkdirection.net/articles/network-theory/controlanddataplane (дата обращения: 11.03.2020).

7. OpenFlow. URL: http://flowgrammable.org/sdn/openflow (дата обращения: 11.03.2020).

8. Архитектура REST. URL: https://habr.com/ru/post/38730 (дата обращения: 11.03.2020).

9. Open Networking Foundation (ONF). URL: https://www.sdxcentral.com/listings/open-networking-foundation (дата обращения: 11.03.2020).

10. OPFLEX. URL: https://ipwithease.com/opflex (дата обращения: 11.03.2020).

11. Cisco ACI vs Cisco SD-Access. URL: https://www.trustradius.com/compare-products/cisco-application-centric-infrastructure-aci-vs-cisco-software-defined-access-sd-access (дата обращения: 11.03.2020).

12. Moreno V. Introduction to LISP and VXLAN – Scalable Technology Overlays for Switching. URL: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2016/pdf/BRKRST-3045.pdf (дата обращения: 11.03.2020).

13. IS-IS vs OSPF. URL: http://prosto-seti.blogspot.com/2016/08/is-is-vs-ospf.html (дата обращения: 11.03.2020).

14. Cisco TrustSec. URL: https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-726831.pdf (дата обращения: 11.03.2020).

15. Security Group Tagging Basics. URL: https://www.networkworld.com/article/2224825/security-group-tagging-basics.html (дата обращения: 11.03.2020).

16. Cisco ISE Configuration for Cisco DNA Center. URL: http://www.unifiedguru.com/cisco-ise-configuration-for-cisco-dna-center (дата обращения: 11.03.2020).

17. Сравнение SD-WAN и традиционной архитектуры WAN. URL: http://blog.sedicomm.com/2017/07/18/sravnenie-sd-wan-i-traditsionnoj-arhitektury-wan (дата обращения: 11.03.2020).

Software & Systems Received 17.04.20
DOI: 10.15827/0236-235X.131.430-438 2020, vol. 33, no. 3, pp. 430–438

Special features of SDN technology by Cisco Systems

Yu.M. Lisetskyi [1], *Dr.Sc. (Engineering), Managing Director, Yurii.Lisetskyi@snt.ua*

[1] *S&T Ukraine, Kiev, 03680, Ukraine*

Abstract. The paper is devoted to software-defined networks currently dominating over traditional networks, which management and automation tools do not meet requirements of modern dynamic changes to configuration and scaling as well as virtualization. Distributed management concept where all the logic component of network operation is spread over network equipment is no more efficient enough. This is the reason for the emergence of a new concept and technology SDN (Software-defined Networking) – a network in which the management level is separated from the data transfer level and implemented programmatically. Thus, in accordance with the SDN concept, all network management logic must be removed from network devices and implemented on a separate server – the SDN controller.

The paper considers SDN technologies of Cisco Systems company, their development, and features. An important difference between these technologies is that they do not meet the basic principle of SDN, which is a separation of control and data planes. Such Cisco technologies as ACI and SD-Access preserve significant control plane functionality in the network devices and expand it with additional features. The basis for these technologies is the overlay networks or logical topology for the virtual connection of devices, which is built over arbitrary underlay topology.

SD-WAN is a new Cisco WAN technology, which resulted from the application of SDN concept to distributed networks. Data plane of SD-WAN is the Internet overlay, working via the Internet. In accordance with SDN concept, the SD-WAN, unlike SD-ACCESS, keeps control plane and data plane decoupled and control plane functionality implemented in separate specialized devices. Having changed the ideology of implementation of enterprise networks Cisco has introduced DNA which is a new network concept enabling different services from the Cisco cloud.

Keywords: software-defined network, concept, principles, technology, topology, functionality, server, controller, virtualization, services, cloud.

References

1. Lisetskyi Yu. Virtualization: development dynamics and prospects. *Proc. 3rd Int. Sci. Pract. Conf. Information Control Systems and Technologies*, Odessa, 2014, pp. 271–273 (in Russ.).
2. Rypalov S., Devin D. *The Modern Enterprise LAN Network Design*. Available at: https://www.cisco.com/c/dam/m/ru_ru/training-events/2019/cisco-connect/pdf/sda_distributed_campus.pdf (accessed March 11, 2020).
3. Haleplidis E. *Overview of RFC7426: SDN Layers and Architecture Terminology*. Available at: https://sdn.ieee.org/newsletter/september-2017/overview-of-rfc7426-sdn-layers-and-architecture-terminology (accessed March 12, 2020).
4. *Introduction to Software Defined Networks (SDN)*. Available at: https://www.researchgate.net/publication/311479628_Introduction_to_Software_Defined_Networks_SDN. DOI: 10.5120/ijais2016451623 (accessed March 11, 2020).
5. Semenovykh A.A., Laponina O.R. Comparative analysis of SDN controllers. *INJOIT*, 2018, vol. 6, no. 7, pp. 50–56 (in Russ.).
6. *Control and Data Planes*. Available at: https://networkdirection.net/articles/network-theory/controlanddataplane (accessed March 11, 2020).
7. *OpenFlow*. Available at: http://flowgrammable.org/sdn/openflow (accessed March 11, 2020).
8. *Architecture REST*. Available at: https://habr.com/ru/post/38730 (accessed March 11, 2020).
9. *Open Networking Foundation (ONF)*. Available at: https://www.sdxcentral.com/listings/open-networking-foundation (accessed March 11, 2020).
10. *OPFLEX*. Available at: https://ipwithease.com/opflex (accessed March 11, 2020).
11. *Cisco ACI vs Cisco SD-Access*. Available at: https://www.trustradius.com/compare-products/cisco-application-centric-infrastructure-aci-vs-cisco-software-defined-access-sd-access (accessed March 11, 2020).
12. Moreno V. *Introduction to LISP and VXLAN – Scalable Technology Overlays for Switching*. Available at: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2016/pdf/BRKRST-3045.pdf (accessed March 11, 2020).
13. *IS-IS vs OSPF*. Available at: http://prosto-seti.blogspot.com/2016/08/is-is-vs-ospf.html (accessed March 11, 2020).
14. *Cisco TrustSec*. Available at: https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-726831.pdf (accessed March 11, 2020).
15. *Security Group Tagging Basics*. Available at: https://www.networkworld.com/article/2224825/security-group-tagging-basics.html (accessed March 11, 2020).
16. *Cisco ISE Configuration for Cisco DNA Center*. Available at: http://www.unifiedguru.com/cisco-ise-configuration-for-cisco-dna-center (accessed March 11, 2020).
17. *Comparison of SD-WAN and Traditional WAN Architecture*. Available at: http://blog.sedicomm.com/2017/07/18/sravnenie-sd-wan-i-traditsionnoj-arhitektury-wan (accessed March 11, 2020).

Для цитирования

Лисецкий Ю.М. Особенности SDN-технологии от Cisco Systems // Программные продукты и системы. 2020. Т. 33. № 3. С. 430–438. DOI: 10.15827/0236-235X.131.430-438.

For citation

Lisetskyi Yu.M. Special features of SDN technology by Cisco Systems. *Software & Systems*, 2020, vol. 33, no. 3, pp. 430–438 (in Russ.). DOI: 10.15827/0236-235X.131.430-438.