Сетевая фабрика и Cisco SD-Access

С.Е. Полищук (Компания Cisco)

Указаны типовые трудности, стоящие сегодня перед корпоративной службой ИТ. Предлагается современный подход к их решению на базе сетевой фабрики Cisco Software-Defined Access (SD-Access). Рассматриваются ключевые компоненты и технологии, лежащие в основе Cisco SD-Access, а также принципы их работы. Перечислены основные практические задачи, решаемые с помощью SD-Access.

Ключевые слова: кампусная сеть, корпоративная служба, сетевая фабрика, оверлей, сетевая топология, политика, сервисы.

Сетевая фабрика: сочетая несочетаемое

Корпоративная ИТ служба находится «между молотом и наковальней». С одной стороны, от нее требуется обеспечить высокую доступность сети в режиме 24x7. С другой стороны, пользователи требуют поддержку новых сервисов, типов устройств, типов пользователей (в том числе гостей, партнеров) и т.д. Всем им нужно обеспечить надлежащую и своевременную поддержку со стороны сети. Кроме того, необходимо учесть требования службы информационной безопасности.

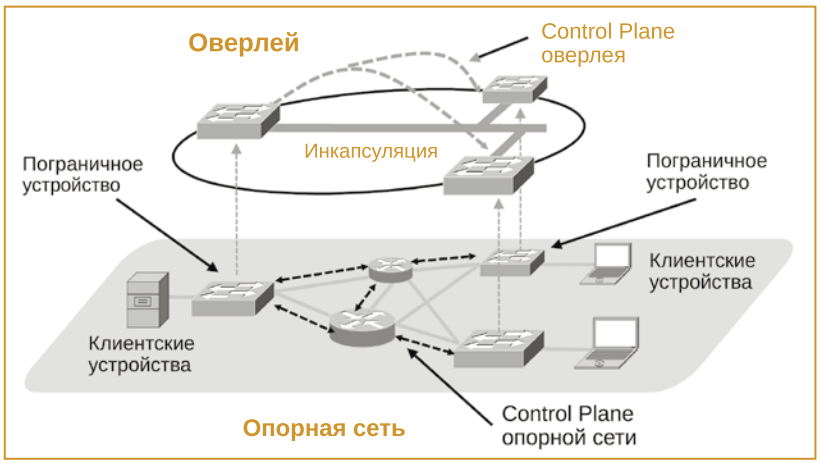

Рис. 1. Концепция сетевой фабрики (оверлея)

Но внедрение новых сервисов сети по определению нарушает ее стабильность, так как привносит в сеть что-то новое, требует внесения изменений. Кроме того, новые сервисы необходимо не просто внедрить, а поддерживать в актуальном состоянии, вносить в них изменения, обеспечивая при этом информационную безопасность.

Для решения подобных противоречий предлагается разбить одну задачу на несколько более простых. Широко известные подобные примеры — семиуровневая модель OSI или четырехуровневая модель DoD в решении задачи сетевого взаимодействия.

В нашем случае полезно использовать концепцию сетевой фабрики или оверлея (overlay) (рис. 1) — логической топологии, построенной поверх некоторой низлежащей топологии (underlay), опорной сети. Оверлей использует некий вид инкапсуляции трафика для передачи поверх опорной сети. Понятие оверлея хорошо знакомо сетевым администраторам. Прокладывая любой туннель в сети, администратор создает оверлей. Типовые примеры — IPSec, GRE, CAPWAP, VXLAN, OTV и т.д.

Таким образом, в сетевой фабрике совмещаются две топологии. Первая, низлежащая топология обеспечивает надежный транспорт на основе маршрутизируемой сети. Это ее единственная задача. Она не реализует сервисы, так как не предназначена для этого. Задачу реализации сервисов и различных видов политик[1] решает вторая, оверлейная сетевая топология. Она отделена от низлежащей топологии, как, например, отделены друг от друга протоколы разных уровней модели OSI. Появление двух сетевых топологий и дает развязку противоречащих друг другу требований.

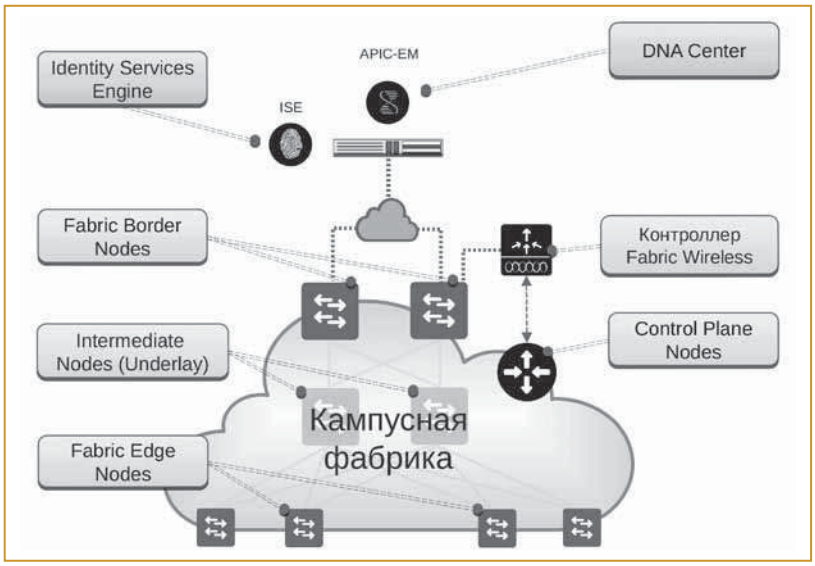

Рис. 2. Архитектура сетевой фабрики Cisco SD-Access

[1] Виды политик можно классифицировать как транспортные (определяющие возможности взаимодействия между областями сети, требования к пути передачи), безопасности (определяющие контроль доступа, аутентичность, целостность, конфиденциальность передаваемых данных), сервисные (определяющие обработку потоков трафика сетевыми функциями), качества обслуживания.

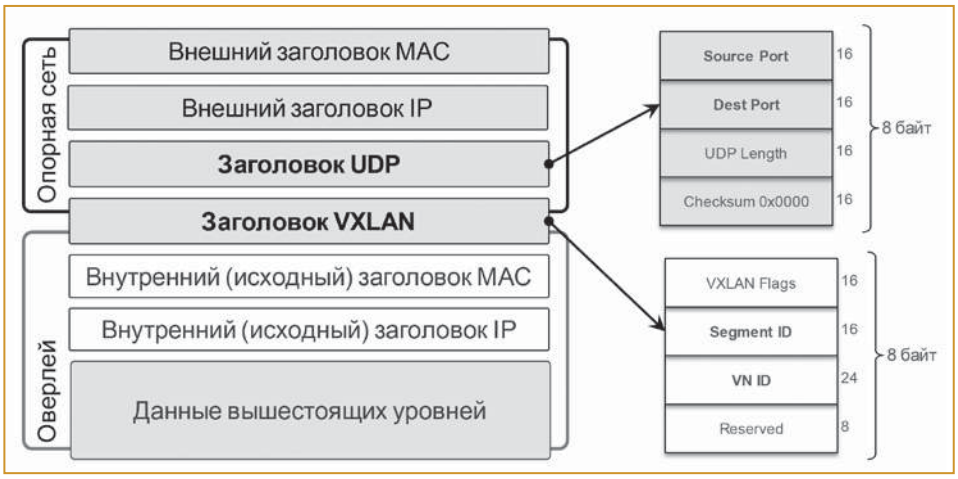

Рис. 3. Инкапсуляция в сетевой фабрике SD-Access

Cisco SD-Access

Концепция сетевой фабрики уже реализована во многих корпоративных сетях. Например, в территориально-распределенных сетях часто используются туннели IPSec; во многих корпоративных беспроводных ЛВС применяются фабрики на основе туннелей CAPWAP; в ЦОД набирают популярность фабрики на основе VXLAN [1] и т.д.

Наступает время для появления сетевой фабрики и в кампусных сетях (рис. 2). Cisco Software-Defined Access (SD-Access) — это реализация Cisco концепции сетевой фабрики для кампусной сети с централизованными средствами управления, автоматизации и оркестрации, а также мониторинга и аналитики [2].

Ключевой компонент решения — контроллер Cisco DNA Center, реализующий Web-интерфейс администратора и интерфейсы API, а также сервисы аналитики на основе служебной информации и данных телеметрии, получаемых от устройств фабрики. DNA Center преобразует массивы разрозненных данных в конкретные выводы и практические рекомендации. Такие выводы и рекомендации касаются текущего состояния сети, ее сервисов и приложений, текущих инцидентов. На основании анализа данных с учетом знания контекста DNA Center предоставляет пользователю аналитику о вероятном влиянии инцидентов на сервисы сети, рекомендует конкретные меры для устранения инцидентов, анализирует тренды, дает рекомендации по планированию емкости сети. Это важная функциональность для мониторинга, быстрого поиска и устранения неисправностей. Она помогает обеспечить высокую доступность бизнес-процессов, работающих поверх фабрики.

DNA Center работает совместно с сервером контроля доступа Cisco Identity Service Engine (ISE). Последний предоставляет фабрике сервисы аутентификации, авторизации и контроля доступа (AAA), обеспечивает динамическое помещение пользователей фабрики в группы, контроль взаимодействия между группами. ISE необходим для реализации в фабрике политики безопасности организации.

Сетевая инфраструктура фабрики включает в себя следующие устройства:

— *Control Plane Nodes* — ведут учет текущего местоположения клиентских устройств в пределах фабрики. Это необходимо для свободного перемещения пользователей в пределах фабрики с сохранением назначенных пользователю прав доступа и обеспечения их мобильности;

— *Fabric Border Nodes* — реализуют подключение фабрики к внешнему миру, то есть к сетям, не являющимся частью фабрики;

— *Fabric Edge Nodes* — обеспечивают подключение к фабрике клиентских устройств, а также точек радиодоступа;

— *Fabric Wireless Controller* — контроллер беспроводных ЛВС, работающий в составе фабрики;

— *Intermediate Nodes* — обеспечивают связь между перечисленными выше устройствами. Они не выполняют никаких функций оверлея, а только реализуют опорную, низлежащую сетевую топологию.

С точки зрения технологий data plane[3] фабрики Cisco SD-Access реализован на базе инкапсуляции Virtual Extensible LAN (VXLAN)[4]. Control plane[5] оверлея использует протокол Locator/ID Separation Protocol (LISP). Политики реализуются на базе тегов Scalable Group Tag (SGT) технологии Cisco TrustSec. Наконец, оверлей работает поверх маршрутизируемой опорной сети. Рассмотрим эти технологии подробнее.

Data plane оверлея: VXLAN

Data plane фабрики Cisco SD-Access построен на базе инкапсуляции VXLAN с Group Policy Option (VXLAN-GPO). Важное преимущество VXLAN заключается в сохранении первоначального Ethernet-заголовка фрейма. В результате обеспечивается мобильность хостов фабрики не только на Уровне 3, но и на Уровне 2. Каковы бы ни были требования приложений, фабрика способна предоставить им любой вид транспорта —

[2] CAN (Campus Area Network — кампусная сеть) — это группа локальных сетей, развернутых на компактной территории (кампусе) какого-либо учреждения и обслуживающие одно это учреждение — университет, промышленное предприятие, порт и т.д. (Прим. ред.).

[3] Control plane — логическая концепция, охватывающая служебную функциональность сетевого оборудования, определяющую, каким образом будет передаваться трафик. Например, к control plane относятся протоколы маршрутизации. (Прим. ред.).

[4] Virtual Extensible LAN (VXLAN) является технологией сетевой виртуализации, изначально разработанной для решения проблемы масштабируемости числа виртуальных сетей VLAN в сетях центров обработки данных. (Прим. ред.).

[5] Data plane — логическая концепция, охватывающая функциональность сетевого оборудования, непосредственно связанную с передачей трафика через устройство. (Прим. ред.).

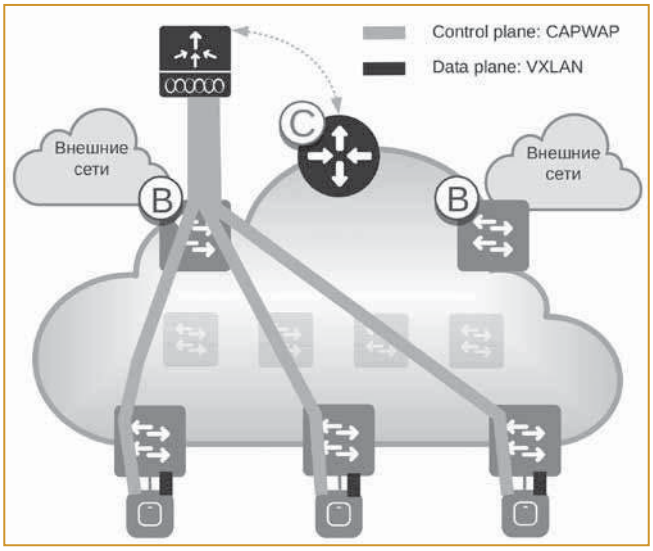

Рис. 4. Интеграция беспроводной ЛВС в фабрику Cisco SD-Access (B — Border Node, C — Control Plane Node)

Уровней 3 и 2 — независимо от направления взаимодействия хостов и их расположения в фабрике.

Трафик data plane фабрики (фреймы Уровня 2) инкапсулируется в пакеты VXLAN и отправляется по сети поверх UDP (User Datagram Protocol) и IP (рис. 3). С точки зрения промежуточных устройств фабрики, это стандартные пакеты IP со вложенными сегментами UDP, адресованными на порт 4789. Номер source-порта UDP определяется хэшем заголовков Уровней 2, 3 и 4 исходных пакетов и таким образом меняется динамически. Это важно для надлежащего распределения нагрузки технологией Cisco Express Forwarding (CEF) в опорной сети.

Оверлей приводит к появлению дополнительных заголовков из-за использования опорной сети для транспорта. Это 8-байтный заголовок VXLAN, 8-байтный заголовок UDP, 20-байтный заголовок IP и 14-байтный заголовок MAC (с опциональными дополнительными 4 байтами) — итого от 50 до 54 байт.

Инкапсуляцию трафика в пакеты VXLAN и обратно в решении Cisco SD-Access выполняют пограничные устройства фабрики. Для трафика внешних сетей это Fabric Border Nodes, для трафика проводных клиентов — Fabric Edge Nodes.

SD-Access также обеспечивает интеграцию беспроводных сетей (БЛВС) в фабрику (рис. 4). Такой режим работы называется Fabric Enabled Wireless (FEW). В отличие от централизованной архитектуры БЛВС, в режиме FEW трафик пользователей БЛВС туннелируется не на контроллер БЛВС в пакетах CAPWAP, а на коммутатор доступа Edge Node в пакетах VXLAN. Таким образом, трафик и проводных, и беспроводных клиентов поступает непосредственно на коммутаторы Edge Node. В результате обеспечивается одинаковая обработка трафика проводных и беспроводных пользователей, оптимизация путей передачи трафика БЛВС, устранение потенциальных «узких мест», характерных для стыка контроллера БЛВС и проводной сети.

Control & management plane беспроводной ЛВС в режиме FEW остается централизованным на контроллере Fabric Wireless. Контроллер использует протокол LISP для обмена данными с Control Plane Nodes о текущем местоположении беспроводных клиентов в фабрике. Точки радиодоступа взаимодействуют с контроллером по протоколу CAPWAP.

Таким образом, архитектура беспроводной сети при интеграции в фабрику получает «лучшее из двух миров».

Control plane оверлея: LISP

Мобильность хостов на Уровнях 2 и 3 — неотъемлемое свойство фабрики. С точки зрения data plane мобильность обеспечивается технологией VXLAN, а в качестве control plane используется протокол Locator/ID Separation Protocol (LISP). Это эффективный протокол, оптимизированный для мобильности хостов. Фабрика содержит централизованную базу данных пользователей Host Tracking Database (HTDB), работающую на устройствах Control Plane Nodes. HTDB хранит информацию о соответствии клиентского хоста (Endpoint ID) текущему местоположению в пределах фабрики, а также ряд дополнительных атрибутов.

Пограничные устройства фабрики, используя протокол LISP, запрашивают базу HTDB, когда им нужно передать пакет на клиентский хост с неизвестным местоположением, и сохраняют эту информацию в локальном кэше. Информация поступает в базу от пограничных устройств фабрики по мере подключения и перемещения клиентских хостов.

Таким образом, Cisco SD-Access позволяет хостам свободно перемещаться в пределах фабрики без смены адресов, обеспечивает их мобильность.

Политика контроля доступа и сегментация: TrustSec

Для решения задач контроля доступа и сегментации пользователей Cisco разработала технологию TrustSec. TrustSec использует метку Scalable Group Tag (SGT)[4] вместо IP-адреса в качестве критерия принадлежности пакета той или иной группе пользователей. Такой подход позволяет отделить адресацию от контроля доступа, использовать специализированные списки контроля доступа SGACL для реализации контроля доступа, придать сети гибкость и автоматизацию применения политики безопасности.

Фабрика Cisco SD-Access позволяет реализовать два уровня сегментации пользователей: VRF для грубой сегментации на высоком уровне (например, для разделения организаций или их подразделений) и группы SGT для тонкой сегментации (например, на уровне от организации до небольших рабочих групп). В первом релизе фабрики SD-Access SGT уникальны в пределах виртуальной сети (VN), но в принципе возможны и так называемые VN-Agnostic группы,

[4] SGT — метка, число, позволяющее различать пакеты. И это число подходит для реализации любых видов политики, не только безопасности. (Прим. ред.).

присутствующие в разных VN, так как SGT не зависит ни от IP-адресов, ни от VRF.

Базовый метод передачи меток внутри домена TrustSec (метод in-line) заключается в инкапсуляции меток в заголовки фреймов или пакетов трафика (в поле Cisco Meta Data). А в фабрике Cisco SD-Access значение метки передается в составе заголовков VXLAN оверлея. Заголовок VXLAN содержит поля VN ID и Segment ID (24-и 16-разрядные соответственно) (рис. 3). Эти поля используются для переноса информации о принадлежности пакета определенной VN (адресуется свыше 16 млн. VRF) и группе SGT технологии TrustSec (адресуется свыше 64 тыс. меток). Кроме того, инкапсуляция метки SGT в заголовок VXLAN облегчает внедрение TrustSec, так как от промежуточных устройств опорной сети не требуется работа с метками.

Контроль доступа, настройка и внедрение политики доступа производится на сервере Cisco ISE, интегрированном в решение Cisco SD-Access. В результате SD-Access предлагает готовые автоматизированные средства реализации политики контроля доступа организации, а также средства сегментации и микросегментации пользователей.

Опорная сеть

Главная задача опорной сети с точки зрения фабрики — обеспечить передачу трафика оверлея. Для оверлея опорная сеть прозрачна. Поэтому в качестве опорной сети может подойти любая современная корпоративная сеть, обеспечивающая адекватный уровень доступности и производительности. Она должна предоставить пограничным устройствам фабрики, таким как Fabric Edge Node, Border Node, Control Plane Node связь по протоколу IP.

В общем случае опорная сеть может быть построена на базе любого сочетания технологий Уровней 2 и 3, хотя Cisco рекомендует строить полностью маршрутизируемую сеть (с маршрутизацией до коммутаторов доступа) и каналами связи, имеющими конфигурацию point-to-point. Протокол маршрутизации тоже может быть любым, рекомендованный вариант — IS-IS, ставший стандартом де-факто в опорных сетях фабрик благодаря своей независимости от адресов Уровня 3, быстрой сходимости и наличию параметров TLV.

В качестве оборудования опорной сети подходит любое отвечающее этим требованиям оборудование как от Cisco, так и от других производителей. Можно использовать уже имеющуюся корпоративную сеть. Это обеспечивает защиту инвестиций в оборудование существующей сети, даже если оно не поддерживается фабрикой. В этом случае опорная сеть будет управляться автономно от фабрики.

Также есть возможность автоматизации управления опорной сети с помощью инструментария фабрики в случае использования соответствующего оборудования Cisco (решение Cisco SD-Access 1.0 обеспечивает автоматизацию опорной сети, построенной на базе коммутаторов Catalyst серий 3850/3650 и 9000). Это сценарий Automated Underlay.

Помимо защиты инвестиций, гибкость требований SD-Access к опорной сети облегчает внедрение — можно начать с пилотного проекта, создания небольшой фабрики, использующей в качестве транспорта существующую опорную сеть, и постепенно провести миграцию на полномасштабное решение.

Cisco SD-Access — применения

Перечислим кратко ряд типовых для ИТ задач, эффективно решаемых с помощью SD-Access [2].

1. Запуск в эксплуатацию новых частей сети или сетей на новых площадках, а также модернизация уже имеющихся сетей.

2. Быстрое и безопасное подключение клиентских устройств, таких как настольные компьютеры и ноутбуки, смартфоны и планшеты, принтеры, камеры видеонаблюдения, сенсоры и устройства Internet of Things и т. д.

3. Быстрое и безопасное подключение новых сервисов и реализация различных видов политики.

4. Создание единой транспортной среды Уровней 3 и 2, охватывающей проводные и беспроводные ЛВС.

5. Сегментация сети.

6. Реализация единой, консистентной сетевой политики за счет средств оркестрации DNA Center и свойств фабрики.

7. Эффективное устранение случившихся и предотвращение будущих инцидентов.

Заключение

Фабрика предлагает службе IT новые мощные возможности в области дизайна, внедрения, эксплуатации корпоративной сети, реализации политик, а также поиска и устранения неисправностей. Эти возможности позволяют IT исполнять требования бизнеса быстро и качественно. Появляется возможность минимизировать рутинную работу, выделить больше времени на стратегические, важные задачи, имеющие более высокую ценность для работодателя, а также дающие конкурентные преимущества на рынке труда.

Бизнес, в свою очередь, получает значительные преимущества в скорости выполнения инициатив и решения задач, опирающихся на сеть. В конечном счете это помогает расширить занимаемую долю рынка, увеличить выручку.

Также Cisco SD-Access предлагает бизнесу значительное снижение рисков сбоев бизнес-процессов, связанных с «человеческим фактором», и принципиально новый уровень безопасности информационной среды.

Список литературы

1. *Скороходов. А.* Сетевые фабрики – новое поколение идеологии сетей ЦОД // CONNECT. http://www.connect-wit.ru
2. *Полищук С.* Зачем IT и бизнесу сетевая фабрика и Cisco SD-Access. 2017. https://habrahabr.ru

Полищук Сергей Евгеньевич *– системный инженер Cisco. Контактный телефон (495) 961-14-10.*