

Independent Submission
Request for Comments: 8597
Category: Informational
ISSN: 2070-1721

IM. Contreras
Telefonica
CJ. Bernardos
UC3M
D. Lopez
Telefonica
M. Boucadair
Orange
P. Iovanna
Ericsson
May 2019

Архитектура CLAS для программно-определяемых сетей Cooperating Layered Architecture for Software-Defined Networking (CLAS)

Аннотация

Программно-определяемые сети (SDN¹) ратуют за отделение уровня управления от уровня данных на узлах сети и концентрацию управления на одном или множестве управляющих элементов. Большая часть интеллекта сетей и/или служб перемещается в эти элементы управления. Обычно такой элемент рассматривается как набор взаимодействующих функций управления с вертикальной интеграцией. Перенос функций управления из множества сетевых узлов в логический центральный элемент концептуально объединяет множество функций управления, имеющих разные цели. В результате имеющиеся решения не обеспечивают чёткого разделения между управлением транспортом и услугами, которые опираются на возможности транспорта.

В этом документе описан подход, названный многоуровневой архитектурой взаимодействия для программно-определяемых сетей (Cooperating Layered Architecture for Software-Defined Networking или CLAS), где связанные с транспортом функции управления отделены от функций, связанным с услугами так, что они могут предоставляться, поддерживаться и развиваться независимо и самостоятельно.

Статус документа

Этот документ не является спецификацией Internet Standards Track и публикуется с информационными целями.

Этот документ в серии RFC не связан с каким-либо потоком RFC. Редактор (RFC Editor) принял решение о публикации документа по своему усмотрению и не делает каких-либо заявлений о возможности реализации или развёртывания. Документ одобрен для публикации редактором и не претендует на статус Internet Standard (см. раздел 2 в RFC 7841).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <https://www.rfc-editor.org/info/rfc8597>.

Авторские права

Авторские права (Copyright (c) 2019) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно.

Оглавление

1. Введение.....	2
2. Терминология.....	2
3. Обзор архитектуры.....	3
3.1. Функциональные слои.....	4
3.1.1. Транспортный слой.....	4
3.1.2. Сервисный слой.....	4
3.1.3. Рекурсия уровней.....	4
3.2. Разделение уровней.....	5
3.2.1. Уровень управления.....	5
3.2.2. Уровень администрирования.....	5
3.2.3. Уровень ресурсов.....	5
4. Требуемые функции.....	5
5. Взаимодействие между контроллерами SDN.....	5
6. Варианты развёртывания.....	5
6.1. Среда SDN.....	5
6.1.1. Множество сервисных слоёв с одним транспортным слоём.....	6
6.1.2. Один сервисный слой с множеством транспортных слоёв.....	6
6.2. Гибридные среды.....	6
6.2.1. Сервисный слой SDN и унаследованный транспортный слой.....	6
6.2.2. Унаследованный сервисный слой и транспортный слой SDN.....	6

¹Software-Defined Networking.

6.3. Многодоменные варианты в транспортном слое.....	6
7. Примеры использования.....	6
7.1. Виртуализация сетевых функций (NFV).....	6
7.2. Абстракции и управление в сетях TE.....	6
8. Реализация взаимодействия между слоями сервиса и транспорта.....	6
9. Взаимодействие с IANA.....	7
10. Вопросы безопасности.....	7
11. Литература.....	7
11.1. Нормативные документы.....	7
11.2. Дополнительная литература.....	7
Приложение А. Связь с RFC 7426.....	8
Благодарности.....	8
Адреса авторов.....	8

1. Введение

Успехи в сфере программных сетевых решений облегчают внедрение программируемых служб и инфраструктуры операторов связи. Обычно это достигается за счёт применения программно-определяемых сетей (SDN) [RFC7149] [RFC7426], включая контроллеры и оркестраторы.

Однако имеются и другие задачи, которые решаются с помощью возможностей SDN. С одной стороны, нужны действия, сосредоточенные на программировании сетей для обеспечения связности и пересылки цифровых данных между удалёнными узлами сети. С другой стороны, нужны действия по программированию функций или служб, которые обрабатывают (манипулируют) такими цифровыми данными.

SDN предлагает разделять уровни управления и данных в сетевых устройствах путём абстрагирования обоих уровней, позволяющего централизовать логику управления в объекте, обычно называемом контроллером SDN (в сети может применяться один или множество контроллеров). Затем определяется программный интерфейс между элементом пересылки (в узлах сети) и управляющим элементом. Через этот интерфейс управляющий элемент инструктирует узлы уровня пересылки и меняет нужным образом их поведение в части пересылки трафика. Поддержка дополнительных возможностей (например, мониторинга производительности, контроля отказов и т. п.) также может осуществляться через этот программный интерфейс [RFC7149].

Большая часть интеллекта переносится в контроллеры. Обычно такой контроллер рассматривается как набор взаимодействующих функций управления с вертикальной интеграцией. Подход, в котором рассматривается «всемогущий» элемент управления охватывающий все аспекты сети (в частности, транспортную сеть и услуги на базе этого транспорта), сталкивается с несколькими проблемами.

- С точки зрения провайдера, где обычно за услуги и связность (т. е. транспорт для услуг) отвечают разные подразделения, предложенный подход размывает ответственность за предоставление и доставку услуг.
- Комплексное и многократное использование функций для предоставления услуг.
- Закрытая, монолитная архитектура управления.
- Сложность взаимодействия и взаимозаменяемости функциональных компонент.
- Размытие границ бизнеса между провайдерами, особенно в случаях, где один провайдер обеспечивает связность, а другой - услуги на базе этой связности.
- Сложность диагностики и обслуживания сети, а также поиска неполадок (в частности, определение ответственного за отказ уровня).

Перемещение функций управления из множества распределённых сетевых узлов в другой элемент концептуально собирает вместе множество возможностей управления, имеющих разные цели. В результате существующие решения SDN не обеспечивают чёткого разделения между управлением транспортом и услугами. В этом документе разделение услуг и транспорта следует стандарту [Y.2011] и определению в разделе 2.

Этот документ описывает подход, названный многоуровневой архитектурой взаимодействия для программно-определяемых сетей (CLAS), где связанные с транспортом функции управления отделены от функций, связанным с услугами так, что они могут предоставляться, поддерживаться и развиваться независимо и самостоятельно.

Несмотря на такое различие, тесное взаимодействие между уровнями услуг и транспорта (или слоями в [Y.2011]) и связанными компонентами требуется для эффективного использования ресурсов.

2. Терминология

Ниже приведены определения используемых в документе терминов.

Transport - транспорт

Возможности передачи данных, предоставляемые сетевой инфраструктурой. Возможности передачи могут быть основаны на методах IP или иных технологиях, таких как MPLS или оптические сети.

Service – сервис (услуга, служба)

Логическая конструкция, использующая транспортные возможности.

В этом документе не принимается допущений о функциональном периметре услуг, которые могут быть организованы на базе транспортной архитектуры. Таким образом, услуга может предоставляться клиентам или вызываться для предоставления других (добавленных) услуг.

Layer - уровень

Набор элементов с возможностями транспорта или услуг в соответствии с предшествующими определениями. В [Y.2011] уровни называются слоями (stratum) и в этом документе применяются оба термина.

Domain - домен

Набор элементов с общим свойством или характеристикой. В этом документе рассматриваются административные (элементы одной организации), технологические (элементы с одной технологией, например, оптической) и другие домены.

SDN Intelligence - интеллект SDN

Процесс принятия решений, реализованный на узле или наборе узлов, называемых контроллерами SDN.

Интеллект может быть распределенным или централизованным. В документе рассматриваются оба варианта.

Интеллект SDN опирается на входные данные от множества различных функциональных блоков, таких как определение топологии сети, определение топологии сервиса, выделение ресурсов, профили клиентов, профили служб и т. п.

Точная декомпозиция интеллекта SDN, за исключением описанных здесь уровней, выходит за рамки документа.

Кроме того, в документе используются перечисленные ниже сокращения.

CLAS

Cooperating Layered Architecture for SDN - многоуровневая архитектура взаимодействия для программно-определяемых сетей.

FCAPS

Fault, Configuration, Accounting, Performance, and Security - отказы, настройка, учёт, производительность и безопасность.

SDN

Software-Defined Networking - программно-определяемая сеть.

SLA

Service Level Agreement - соглашение об уровне обслуживания.

3. Обзор архитектуры

Современные операторские сети поддерживают множество услуг (например, VoIP¹, IPTV, мобильные услуги VoIP и т. п.) на основе разных транспортных технологий. Предоставление и доставка услуг независимо от базового транспорта требует разделения связанной с транспортом функциональности и абстракции транспортной сети, чтобы скрыть специфику базовых транспортных технологий, сохраняя базовый набор возможностей.

Такое разделение может обеспечить гибкость конфигурации и адаптивность с точки зрения услуг или транспортной сети. На основе одной транспортной архитектуры может поддерживаться множество услуг и разные технологии могут выполнять требования связности определённого сервиса. Тесная связь между этими элементами нужна для согласованного предоставления услуг (межуровневая кооперация).

Этот документ в основном посвящён решению перечисленных ниже задач:

- представление транспортных возможностей сервису;

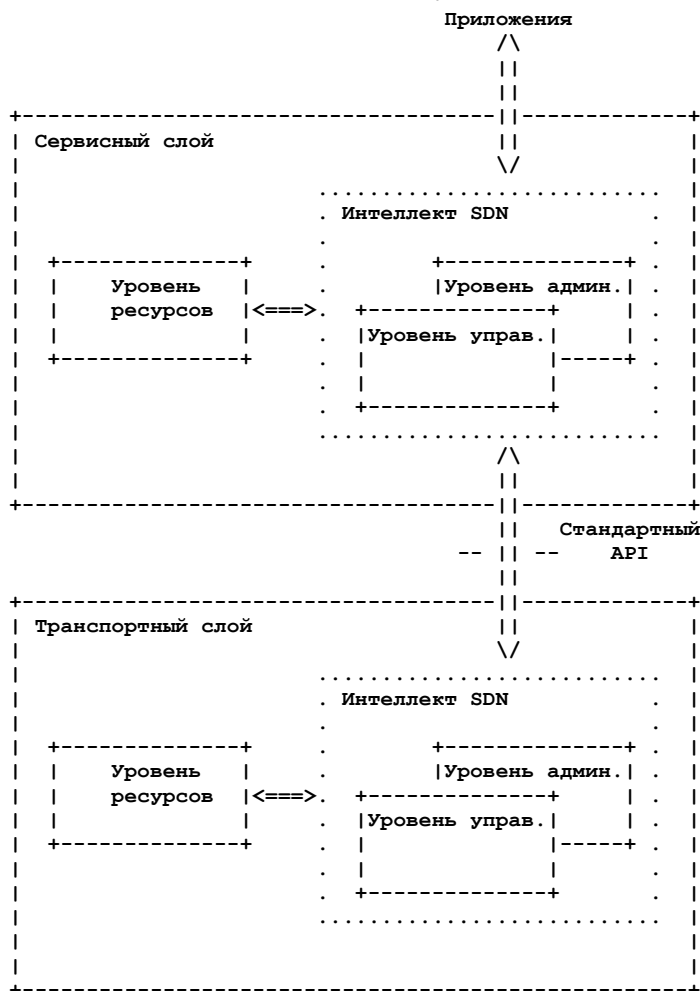


Рисунок 1. Архитектура CLAS.

- фиксация требований сервиса к транспорту;
- уведомление сервисного интеллекта о транспортных событиях, например, для корректировки процесса принятия решения при том или ином событии на транспорте;

¹Voice over IP - голосовая связь по протоколу IP.

- информирование базового транспорта о новых требованиях и т. п.

Примером является гарантия некоторых уровней качества обслуживания (QoS¹). Различные предложения на основе QoS могут быть представлены на сервисном и транспортном уровне. Должны быть предусмотрены вертикальные связи между механизмами QoS транспортного и сервисного уровня, чтобы гарантировать качество обслуживания конечному пользователю.

Архитектура CLAS предполагает, что логически централизованные функции разделены на два функциональных уровня. Один из уровней содержит связанные с сервисом функции, а другой - функции, связанные с транспортом. Предполагается взаимодействие этих уровней через стандартные интерфейсы.

На рисунке 1 показана архитектура CLAS, основанная на функциональном разделении архитектуры NGN², определённой ITU-T в стандарте [Y.2011], где заданы два слоя (уровня) функциональности. Эти слои называются сервисным (Service Stratum) и транспортным (Transport Stratum). Функции каждого из этих уровней дополнительно группируются по уровням управления, администрирования и данных (пользовательский).

CLAS принимает структурную модель, описанную в [Y.2011], но применяет её для решения задач программируемости с помощью SDN [RFC7149]. В этом отношении CLAS предлагает разделение услуг и транспорта на основе различия их задач.

В архитектуре CLAS функции управления и администрирования выполняются на одном или множестве контроллеров SDN (например, для расширяемости и надёжности), обеспечивая интеллект SDN таким способом, что контроллеры SDN представлены в сервисном и транспортном слое. Функции администрирования считаются частью интеллекта SDN, обеспечивающего эффективную работу в экосистеме сервис-провайдера [RFC7149], хотя в некоторых предложениях эти функции не считались частью среды SDN [ONFArch].

Кроме того, базовые пользовательские функции и функции уровня данных, включённые в архитектуру NGN, называются здесь функциями уровня ресурсов. Этот уровень в каждом слое управляется соответствующим интеллектом SDN через стандартный интерфейс.

Контроллеры SDN взаимодействуют для предоставления и доставки услуг. Имеется иерархия, в которой интеллект сервисной SDN делает запросы к интеллекту транспортной SDN для предоставления транспортных возможностей.

Интеллект сервисной SDN выступает клиентом интеллекта транспортной SDN.

Кроме того, интеллект транспортной SDN взаимодействует с интеллектом сервисной SDN для информирования о событиях в транспортной сети, которые могут вызывать действия на уровне сервиса.

Несмотря на то, что это не показано на рисунке 1, уровни ресурсов каждого слоя могут быть соединены. Это зависит от типа предоставляемых услуг. Кроме того, сервисный слой может предоставлять интерфейс для приложений, обеспечивающий раскрытие возможностей сетевых служб этим приложениям или пользователям.

3.1. Функциональные слои

Как отмечено выше, существует функциональное разделение между транспортом и услугами. Оба эти слоя взаимодействуют для согласованного предоставления услуг.

Согласованность определяется и характеризуется уровнем сервиса.

3.1.1. Транспортный слой

Транспортный слой включает функции, ориентированные на передачу данных между взаимодействующими конечными точками (например, между пользовательскими устройствами, сервисными шлюзами и т. п.). Узлы пересылки данных управляются и поддерживаются компонентой Transport SDN.

Уровень управления в SDN Intelligence отвечает за указание устройствам пересылки создавать сквозной путь передачи данных для каждого взаимодействия или обеспечивать надлежащую настройку услуг пересылки. Пересылка не может зависеть исключительно от настроенных заранее элементов - это значит, что можно включить средства динамического построения путей маршрутизации и пересылки (это может потребовать от узлов поддержки некоторых функций управления). Наконец, уровень управления выполняет функции управления (т. е., FCAPS) на этих устройствах как часть возможностей транспортного слоя.

3.1.2. Сервисный слой

Сервисный слой содержит функции, связанные с предоставлением услуг и возможностями, предлагаемыми внешним приложениям. Уровень ресурсов состоит из ресурсов, вовлечённых в предоставление услуг, таких как вычислительные ресурсы, реестры, базы данных и т. п.

Уровень управления отвечает за управление и настройку этих ресурсов, а также за взаимодействие с уровнем управления транспортного слоя в качестве клиента для запроса транспортных возможностей для данного сервиса. Таким же способом уровень администрирования реализует административные действия на связанных с сервисом ресурсах и взаимодействует с уровнем администрирования транспортного слоя для обеспечения кооперации уровней.

3.1.3. Рекурсия уровней

В некоторых вариантах применения может использоваться рекурсивное деление на уровни, где транспортный слой дополнительно делится на сервисный и транспортный слои. Это может возникать в случаях предоставления транспортных услуг, дополненных расширенными возможностями (например, для поддержки SLA [RFC7297]).

Рекурсия уровней рассмотрена в [ONFArch] как способ обеспечения расширяемости и модульности, где каждый вышележащий уровень может обеспечивать большие возможности абстракции. Кроме того, рекурсивные уровни могут

¹Quality-of-Service.

²Next Generation Network - сеть следующего поколения.

быть полезны в некоторых многодоменных системах с участием одного или множества административных доменов, как описано в параграфе 6.3.

3.2. Разделение уровней

Архитектура CLAS усиливает разделение уровней. Как отмечено в параграфах 3.1.1 и 3.1.2, в каждом слое выделяются три разных уровня. Взаимодействие между соответствующими уровнями в разных слоях основано на стандартных, открытых интерфейсах.

3.2.1. Уровень управления

Уровень управления логически централизует функции управления каждого слоя и непосредственно управляет соответствующими ресурсами. Роль уровня управления в архитектуре SDN рассмотрена в [RFC7426]. Этот уровень является частью SDN Intelligence и может взаимодействовать с другими уровнями управления в том же или другом слое для реализации управляющих функций.

3.2.2. Уровень администрирования

Уровень администрирования логически централизует административные функции каждого слоя, включая администрирование уровней управления и ресурсов. Уровень администрирования в среде SDN описан в [RFC7426]. Этот уровень также является частью SDN Intelligence и может взаимодействовать с соответствующими уровнями администрирования в контроллерах SDN того же или другого слоя.

3.2.3. Уровень ресурсов

Уровень ресурсов включает ресурсы для выполнения транспортных или сервисных функций. В некоторых случаях сервисные ресурсы могут быть подключены к транспортным (например, служить точками завершения транспортных функций), в других они могут быть полностью отделены от ресурсов транспорта (например, база данных с реестром для конечных пользователей). Уровни пересылки и операций, предложенные в [RFC7426], являются в данной архитектуре частью уровня ресурсов.

4. Требуемые функции

Поскольку архитектура CLAS подразумевает взаимодействие разных уровней с разными целями и зонами ответственности, требуется поддержка множества функций, перечисленных ниже.

- Абстрагирование - отображение физических ресурсов на соответствующие абстрактные ресурсы.
- Трансляция параметров сервиса (например, в форме SLA) в параметры (возможности) транспорта в соответствии с различными правилами.
- Мониторинг - механизмы (например, уведомления о событиях) для динамического обновления состояний (абстрагированных) ресурсов с учётом, например, уровня трафика.
- Расчёт ресурсов - функции, способные определить ресурсы, требуемые для данного запроса услуг. Например, функции, подобные PCE, могут служить для расчёта и выбора того или иного пути.
- Оркестровка - возможность комбинировать разные ресурсы (например, IT и сетевые) оптимальным способом.
- Чет использования ресурсов.
- Безопасность - защищённое взаимодействие между компонентами с предотвращением атак (например, DoS).

5. Взаимодействие между контроллерами SDN

Между контроллерами SDN сервисного и транспортного слоя требуется организовать чёткую координацию. Нужно определить механизмы обмена относящейся к взаимодействию информацией для каждого слоя.

С точки зрения сервиса требуется Service SDN Intelligence для упрощения доступа к транспортным ресурсам через чётко определённые интерфейсы API, чтобы определить возможности, предоставляемые транспортным слоем. Могут применяться разные способы получения информации о транспорте, например, механизмы обнаружения или публикации. В первом случае Service SDN Intelligence может обрабатывать полную информацию о транспортных возможностях (включая ресурсы), предлагаемых транспортным слоем. Во втором варианте транспортный слой раскрывает доступные возможности (например, через каталог), снижая объем передаваемых через сеть деталей.

С другой стороны, транспортный слой должен чётко фиксировать требования сервисного слоя. Это может включать требования SLA с конкретной метрикой (например, задержка), уровнем защиты, максимальной и минимальной ёмкостью, ограничениями доступных ресурсов и т. п.

Взаимодействие между контроллерами должно быть защищено, например, путём предотвращения атак на службы или иных угроз (должно быть защищено и взаимодействие между узлами сети).

6. Варианты развёртывания.

Варианты развёртывания. могут существенно различаться в зависимости от характеристик используемой сети.

6.1. Среда SDN

В этом варианте сети, участвующие в предоставлении и доставке услуг, обладают возможностями SDN.

6.1.1. Множество сервисных слоёв с одним транспортным слоем

Один транспортный слой может обеспечивать транспортные функции для одного или множества сервисных слоёв. Транспортный слой обеспечивает стандартные интерфейсы для каждого сервисного слоя. Сервисные слои являются

клиентами транспортного слоя. Среди предлагаемых транспортным слоем возможностей могут быть изоляция (секционирование) транспортных ресурсов, независимая маршрутизация и т. п.

6.1.2. Один сервисный слой с множеством транспортных слоёв

Один сервисный слой может использовать различные транспортные слои для предоставления определённой услуги. Сервисный слой обращается к стандартным интерфейсам каждого транспортного слоя и управляет предоставленными транспортными возможностями для организации нужного сквозного транспорта.

6.2. Гибридные среды

В этом разделе рассмотрены варианты где один из слоёв является полностью или частично унаследованным (не SDN).

6.2.1. Сервисный слой SDN и унаследованный транспортный слой

Сервисный слой SDN может взаимодействовать с унаследованным транспортным слоем с помощью функций межсетевого взаимодействия, которые способны адаптировать основанные на SDN команды управления и администрирования, связанные с сервисом, для традиционных протоколов, связанных с транспортным уровнем, которые понятны унаследованному транспортному слою.

Интеллект SDN в сервисном слое не знает об унаследованной природе базового транспортного слоя.

6.2.2. Унаследованный сервисный слой и транспортный слой SDN

Унаследованный сервисный слой может работать с транспортным слоем SDN на основе функций межсетевого взаимодействия, способных интерпретировать команды от унаследованных сервисных функций и транслировать их в протокол SDN для операция с транспортным слоем SDN.

6.3. Многодоменные варианты в транспортном слое

Транспортный слой может включать ресурсы транспорта, относящиеся к разным административным, топологическим или технологическим доменам. Сервисный слой может взаимодействовать с одним объектом транспортного слоя, если обеспечиваются те или иные возможности абстрагирования для эмуляции транспортной части как одного слоя.

Эти возможности абстрагирования составляют услугу, предоставляемую транспортным слоем использующим его службам. Эта услуга ориентирована на предоставление транспортных возможностей, которые отличаются от конечной транспортной услуги, использующей такие возможности.

В этом конкретном случае рекурсия делает возможным использовать множество доменов на транспортном уровне.

Многодоменные варианты могут возникать при использовании сетей как одного, так и множества операторов.

В варианте с одним оператором многодоменная или сквозная абстрактная компонента может обеспечить однородное представление возможностей разнородного базового транспорта.

В случае с транспортным слоем с сетями множества операторов следует поддерживать программируемую организацию сквозных путей через вовлечённые сети. Например, это может быть обеспечено в каждом административном домене путём обмена данными организации трафика [RFC7926].

7. Примеры использования

В этом разделе представлены примеры использования в качестве иллюстрации применимости модели CLAS.

7.1. Виртуализация сетевых функций (NFV)

Среды NFV¹ включает два возможных уровня управления SDN [GSNFV-EVE005]. Одним из уровней является необходимость управлять инфраструктурой NFV (NFVI) для обеспечения сквозной связности между VNF (Virtual Network Function - функция виртуальной сети) или между VNF и PNF (Physical Network Function - функция физической сети). Вторым уровнем является настройка и управление VNF (настройка сетевых служб, реализуемых VNF), которая выигрывает от программных возможностей SDN. Эти уровни разделены по своей природе, однако можно предполагать взаимодействие между ними для оптимизации, расширяемости и влияния друг на друга.

7.2. Абстракции и управление в сетях TE

Модель ACTN² [RFC8453] позволяет создавать виртуальные сети, предлагаемые клиентам. Роль провайдера в ACTN ограничивается предоставлением услуг виртуальных сетей. Эти услуги по сути являются транспортными и соответствуют транспортному слою в CLAS. Сервисный слой CLAS может считаться клиентом в контексте ACTN.

ACTN определяет иерархию контроллеров для облегчения создания и функционирования виртуальных сетей. Определён интерфейс для взаимодействия между клиентами, запрашивающими услуги виртуальных сетей, и контроллером, отвечающим за оркестровку и обслуживание таких запросов. Такой интерфейс эквивалентен показанному на рисунке 1 (раздел 3) интерфейсу между сервисным и транспортным слоем.

8. Реализация взаимодействия между слоями сервиса и транспорта

Различия между сервисными и транспортными задачами порождают множество проблем при взаимодействии между слоями. Ниже приведён список некоторых известных проблем такого рода.

- Стандартные механизмы взаимодействия между слоями. В настоящее время имеется множество предложений, которые способны удовлетворять запросы от сервисного слоя к транспортному.

¹Network Function Virtualization.

²Abstraction and Control of TE Networks.

Некоторые из таких предложений могут быть решениями, подобными [CPNP³] или I-CPI⁴ [ONFArch].

Другими кандидатами могут служить транспортный API [TAPI] или транспортный интерфейс северного моста [TRANS-NORTH]. Каждый из этих вариантов имеет свою область действия.

- Поддержка множества провайдеров. В многодоменных системах, где на транспортном уровне работает более одного провайдера сервисный слой может знать или не знать о наличии множества доменов.

Если сервисный слой не знает о множестве доменов, транспортный слой выступает в качестве единой точки взаимодействия для запросов сервисного слоя и должен отвечать за взаимодействие с разными доменами.

Если сервисный слой осведомлен о наличии множества доменов, ему следует самостоятельно распределять запросы к разным транспортным слоям для организации сквозных путей между конечными точками (т. е., функциями) сервиса.

- Отображение SLA. Оба слоя будут обрабатывать SLA, но природа этих SLA может различаться. Поэтому от объектов каждого слоя требуется отображение сервисных SLA на транспортные (связность) для надлежащей доставки услуг.
- Связи между слоями могут настраиваться заранее или оба слоя могут использовать механизмы обнаружения для динамической организации таких связей.
- Безопасность. Как отмечено выше, взаимодействие между слоями требуется защищать для предотвращения атак и угроз. Кроме того, должна обеспечиваться конфиденциальность, особенно при использовании на транспортном уровне множества провайдеров.
- Чет. Контроль и учёт использования ресурсов услугами должен поддерживаться для связей между слоями.

9. Взаимодействие с IANA

С этим документом не связано действий IANA.

10. Вопросы безопасности

Архитектура CLAS опирается на функциональные элементы, определённые в [RFC7149] и [RFC7426]. Поэтому следует принимать в внимание вопросы безопасности, отмеченные в разделе 5 [RFC7149].

Связи между транспортными и сервисными контроллерами SDN должны быть защищены с использованием:

- взаимной аутентификации сторон до выполнения каких-либо действий;
- защиты целостности сообщения.

Каждый из контроллеров должен быть снабжён инструкциями относительно набора информации (и детализации), которая может быть раскрыта партнерскому контроллеру. Должны обеспечиваться меры предотвращения утечки конфиденциальных данных (например, из сервисного слоя в транспортный). Конкретный набор совместно используемой информации зависит от местных требований.

Повреждённый контроллер может нарушать работу других контроллеров, поэтому нужна защита от таких атак.

Защиту взаимодействий между слоями следует применять к API (и/или протоколам), которые применяются для связи. Поэтому вопросы безопасности будут определяться конкретным решением.

11. Литература

11.1. Нормативные документы

[Y.2011] International Telecommunication Union, "General principles and general reference model for Next Generation Networks", ITU-T Recommendation Y.2011, October 2004, <<https://www.itu.int/rec/T-REC-Y.2011-200410-I/en>>.

11.2. Дополнительная литература

[CPNP] Boucadair, M., Jacquenet, C., Zhang, D., and P. Georgatsos, "Connectivity Provisioning Negotiation Protocol (CPNP)", Work in Progress, draft-boucadair-connectivity-provisioning-protocol-15, December 2017.

[GSNFV-EVE005] ETSI, "Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework", ETSI GS NFV-EVE 005, V1.1.1, December 2015, <https://www.etsi.org/deliver/etsi_gs/NFV-EVE/001_099/005/01.01.01_60/gs_nfv-eve005v010101p.pdf>.

[ONFArch] Open Networking Foundation, "SDN Architecture, Issue 1", June 2014, <https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf>.

[RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", [RFC 7149](#), DOI 10.17487/RFC7149, March 2014, <<https://www.rfc-editor.org/info/rfc7149>>.

[RFC7297] Boucadair, M., Jacquenet, C., and N. Wang, "IP Connectivity Provisioning Profile (CPP)", RFC 7297, DOI 10.17487/RFC7297, July 2014, <<https://www.rfc-editor.org/info/rfc7297>>.

[RFC7426] Haleplidis, E., Ed., Pentikousis, K., Ed., Denazis, S., Hadi Salim, J., Meyer, D., and O. Koufopavlou, "Software-Defined Networking (SDN): Layers and Architecture Terminology", [RFC 7426](#), DOI 10.17487/RFC7426, January 2015, <<https://www.rfc-editor.org/info/rfc7426>>.

³Connectivity Provisioning Negotiation Protocol - протокол согласования связности.

⁴Intermediate-Controller Plane Interface - интерфейс с промежуточным контроллером.

- [RFC7926] Farrel, A., Ed., Drake, J., Bitar, N., Swallow, G., Ceccarelli, D., and X. Zhang, "Problem Statement and Architecture for Information Exchange between Interconnected Traffic-Engineered Networks", BCP 206, RFC 7926, DOI 10.17487/RFC7926, July 2016, <<https://www.rfc-editor.org/info/rfc7926>>.
- [RFC8453] Ceccarelli, D., Ed. and Y. Lee, Ed., "Framework for Abstraction and Control of TE Networks (ACTN)", RFC 8453, DOI 10.17487/RFC8453, August 2018, <<https://www.rfc-editor.org/info/rfc8453>>.
- [SDN-ARCH] Contreras, LM., Bernardos, C.J., Lopez, D., Boucadair, M., and P. Iovanna, "Cooperating Layered Architecture for SDN", Work in Progress, draft-irtf-sdnrg-layered-sdn-01, October 2016.
- [TAPI] Open Networking Foundation, "Functional Requirements for Transport API", June 2016, <https://www.opennetworking.org/wp-content/uploads/2014/10/TR-527_TAPI_Functional_Requirements.pdf>.
- [TRANS-NORTH] Busi, I., King, D., Zheng, H., and Y. Xu, "Transport Northbound Interface Applicability Statement", Work in Progress, draft-ietf-ccamp-transport-nbi-app-statement-05, March 2019.

Приложение А. Связь с RFC 7426

В [RFC7426] введена таксономия SDN путём определения множества плоскостей, уровней абстракции и интерфейсов или API между ними для прояснения связей между разными составляющими SDN (сетевые устройства, управление, администрирование). Определено множество уровней (плоскостей), включая:

- уровень пересылки, обеспечивающий доставку пакетов через путь данных на основе инструкций от уровня управления;
- операционный уровень, обеспечивающий поддержку рабочего состояния сетевого устройства;
- уровень управления, предназначенный для инструктирования устройств в части пересылки пакетов;
- уровень администрирования, отвечающий за мониторинг и поддержку сетевых устройств;
- уровень приложений, обеспечивающий использование для решения различных задач (определяются приложениями) всех управляемых таким способом устройств.

Кроме этого [RFC7426] предлагает множество уровней абстракции, позволяющих объединить разные плоскости через общие интерфейсы. Архитектура CLAS фокусируется на уровнях управления, администрирования и ресурсов в качестве базовых компонент. По существу, уровень управления меняет поведение и действия контролируемых ресурсов. Уровень администрирования обеспечивает мониторинг и получение статуса этих ресурсов. А уровень ресурсов группирует все ресурсы, связанные с задачами каждого слоя.

С этой точки зрения уровни CLAS можно считать надмножеством уровней [RFC7426]. Однако в некоторых случаях не все уровни [RFC7426] могут полностью присутствовать в представлении CLAS (например, уровень пересылки в сервисном слое). При этом внутренняя структура слоя CLAS может соответствовать таксономии [RFC7426]. Отличительная особенность заключается в специализации сред SDN за счёт разделения услуг и транспорта.

Благодарности

Этот документ рассмотрен и принят исследовательской группой IRTF SDN как [SDN-ARCH]. После завершения работы группы IRTF SDN RG документ был преобразован в независимое представление (Independent Submission) некоторыми из участников групповых обсуждений.

Авторы выражают свою признательность (в алфавитном порядке) Bartosz Belter, Gino Carrozzo, Ramon Casellas, Gert Grammel, Ali Haider, Evangelos Haleplidis, Zheng Haomian, Giorgios Karagianis, Gabriel Lopez, Maria Rita Palatella, Christian Esteve Rothenberg и Jacek Wytrowski за их комментарии и предложения.

Спасибо Adrian Farrel за рецензию.

Адреса авторов

Luis M. Contreras

Telefonica

Ronda de la Comunicacion, s/n

Sur-3 building, 3rd floor

Madrid 28050

Spain

Email: luismiguel.contrerasmurillo@telefonica.com

URI: <http://lmcontreras.com>

Carlos J. Bernardos

Universidad Carlos III de Madrid

Av. Universidad, 30

Leganes, Madrid 28911

Spain

Phone: +34 91624 6236

Email: cjbc@it.uc3m.es

URI: <http://www.it.uc3m.es/cjbc/>

Diego R. Lopez

Telefonica

Ronda de la Comunicacion, s/n

Sur-3 building, 3rd floor

Madrid 28050

Spain

Email: diego.r.lopez@telefonica.com

Mohamed Boucadair

Orange

Rennes 35000

France

Email: mohamed.boucadair@orange.com

Paola Iovanna

Ericsson

Pisa

Italy

Email: paola.iovanna@ericsson.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru