

УДК 378.2

ОБЕСПЕЧЕНИЕ КАЧЕСТВА ПЕРЕДАЧИ ДАННЫХ В ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЯХ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ STATIC VXLAN С ДИНАМИЧЕСКИМ ИЗМЕНЕНИЕМ ПОЛОСЫ ПРОПУСКАНИЯ

В.А. ВИШНЯКОВ, Б.А. МОНИЧ

*Учреждение образования «Белорусская государственная академия связи»,
ул. Ф. Скорины, 8/2, Минск, 220076, Беларусь*

Поступила в редакцию 26 июня 2021

Рассмотрена возможность использования модели передачи данных в программно-определяемых сетях на основе использования статических маршрутов (туннелей) в оверлейных сетях с динамической полосой пропускания (VXLAN). Проведен сравнительный анализ представленной архитектуры программно-определяемой сети с классической архитектурой. Определены преимущества использования рассмотренной конфигурации по сравнению со стандартными подходами к реализации программно-определяемых сетей.

Ключевые слова: Virtual Extensible Local Area Network (VXLAN), NorthBound Interface (NBI), SouthBound Interface (SBI), Virtual endpoint tunnel (VTEP).

Введение. В настоящее время в отрасли инфокоммуникационных технологий происходит активное развитие технологий облачных вычислений. Облачные вычисления – модель обеспечения удобного сетевого доступа по требованию к некоторому общему фонду конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам – как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру. Использование облачных вычислений требует от оператора предоставления услуг качественной инфраструктуры, которая способна обеспечить доведение сервисов до конечных клиентов максимально быстро и качественно. Высокие требования предъявляются к маршрутизации, резервированию каналов связи и защите информации. В большинстве случаев сети операторов «облачных услуг» строятся на основе программно-определяемых (программно-конфигурируемых) сетей. Одним из вариантов обеспечения качества передачи данных в программно-конфигурируемых сетях является способ использования статических маршрутов в оверлейных сетях с динамической полосой пропускания [1].

Целью данной работы является определение такой архитектуры программно-определяемой сети (ПОС), чтобы обеспечить требуемое качество передачи данных.

Компоненты сегментированной структуры программно-определяемой сети. В работе авторов [2] приведено понятие качества (QoS) программно определяемых сетей в облачных технологиях и рассмотрен подход к описанию модели качества ПОС. Для обеспечения качества используется сегментирование ПОС. Рассмотрим основные компоненты такой структуры (рис. 1).

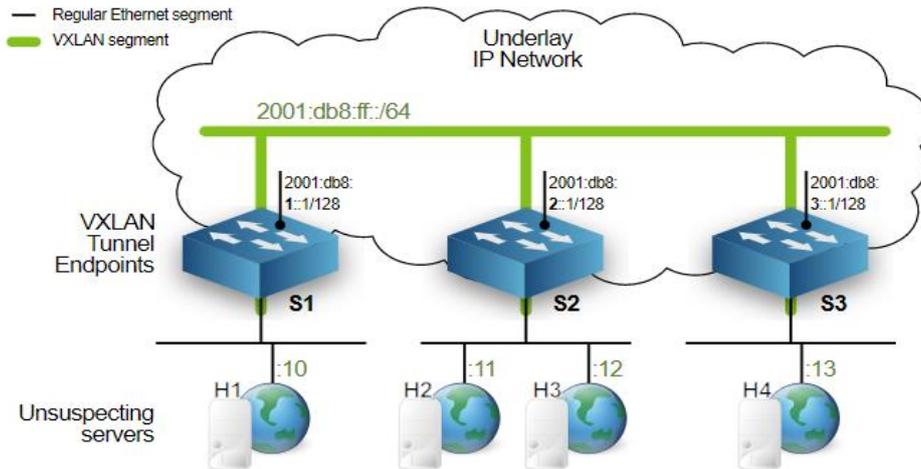


Рис. 1. Обобщенная структура сети с использованием VXLAN сегмента

VXLAN (Virtual eXtensible Local Area Network) – это оверлейная сеть, предназначенная для передачи Ethernet-трафика по существующей (масштабируемой и высокодоступной) IP-сети с одновременным размещением множества пользовательских групп. VXLAN имеет собственный идентификатор, длина которого составляет 24 бита (VxLAN Network Identifier – VNI), что позволяет создать 16 277 214 уникальных соединения на каждом сегменте программно-определяемой сети.

В VXLAN связь устанавливается между двумя конечными точками логического туннеля VXLAN tunnel endpoints (VTEP), при этом оригинальные пакеты инкапсулируются в новый заголовок. VXLAN позволяет организовывать логические сети поверх существующих физических сетей с внесением минимальных изменений в существующую инфраструктуру сетевого взаимодействия [3].

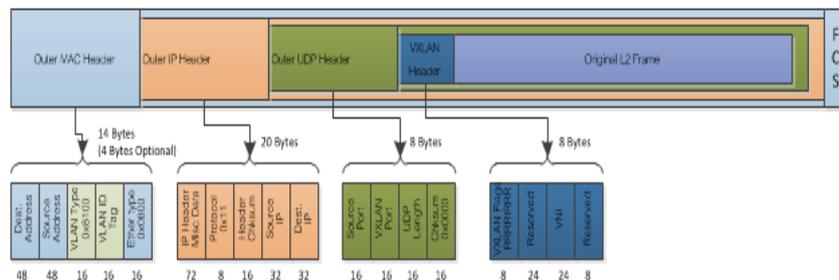


Рис. 2. Структура VXLAN пакета

VXLAN пакет содержит следующие поля (рис. 2):

- Destination Address – это MAC-адрес VTEP назначения, если этот VTEP является локальным по отношению к ближайшему роутеру, или MAC-адрес самого роутера, если VTEP находится за ним;
- VLAN – опциональное поле с тэгом VLAN (не обязательно в VXLAN-реализации);
- Ethertype – тип пакета (для IPv4 установлен в 0x0800);
- Outer IP Header;
- Protocol – содержит значение 0x11, чтобы обозначить, что это UDP-пакет;
- Source IP – IP-адрес VTEP источника;
- Destination IP – IP-адрес VTEP назначения;
- UDP Header;
- Source Port – устанавливается передающим VTEP;
- VXLAN Port – порт VXLAN IANA (еще не определен);

- UDP Checksum – контрольная сумма пакета на уровне VXLAN;
- VXLAN Header;
- VXLAN Flags – различные флаги;
- VNI – 24-битное поле с идентификатором VXLAN;
- Reserved – набор зарезервированных полей.

Архитектура программно-определяемой сети. Концепция использования статических маршрутов (туннелей) в VXLAN с динамической полосой пропускания позволяет использовать до 95 % общей доступной полосы пропускания, ограниченной физическим оборудованием [4]. При этом, в стандартной концепции ПОС во время высокой загрузки установленного маршрута происходит поиск альтернативного маршрута передачи информации (Load Balancing). В рассматриваемом варианте реализации программно-конфигурируемой сети, при передаче больших объемов информации по конкретной VXLAN происходит динамическое расширение туннеля, используя всю доступную полосу.

Использование данной реализации программно-определяемой сети позволяет сократить время передачи информации, а также приводит к экономии энергоресурсов. Время принятия решения на расширение полосы на каждом конкретном узле для VXLAN быстрее на 3 мс, чем принятие решения контроллером выбора альтернативного маршрута при стандартной реализации, поскольку контроллеру приходится анализировать загрузку не только состояния ближайшего альтернативного узла (next hop), но и следующего за этим.

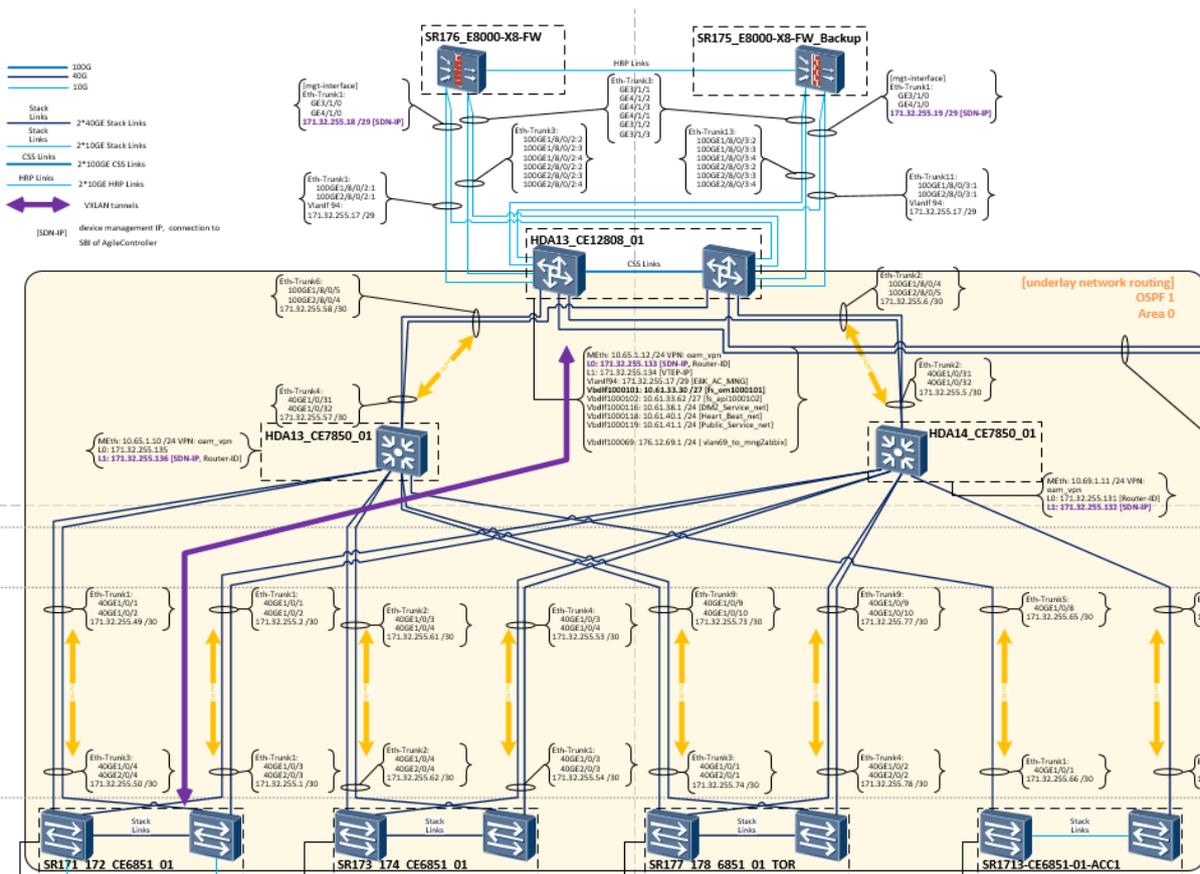


Рис. 3. NBI программно-определяемой сети

Поскольку программно-определяемые сети имеют техническую возможность разделения пользовательской информации и информации управления существует возможность реализации двух независимых интерфейсов для приема данной информации со стороны центра обработки данных (ЦОД). Реализация программно-определяемой сети с использованием северного клиентского интерфейса (North Bound Interface – NBI, рис. 3) и южного интерфейса

для управления физическими и виртуальными узлами (South Bound Interface – SBI, рис. 4) позволяет повысить защищенность клиентских данных и информации управления.

В реализации данной архитектуры программно-определяемой сети принято решение о сегментировании управления элементами сети по назначению. Предусмотрены отдельные сегменты для управления сетевой инфраструктурой ЦОДа, системами хранения данных (СХД), серверами приложений, а также управление виртуальными машинами, включая выделение необходимого количества процессоров и оперативной памяти для работы приложений. Каждый сегмент имеет резервирование по принципу N+1. При передаче информации происходит агрегация данных сегментов на узлах агрегации.

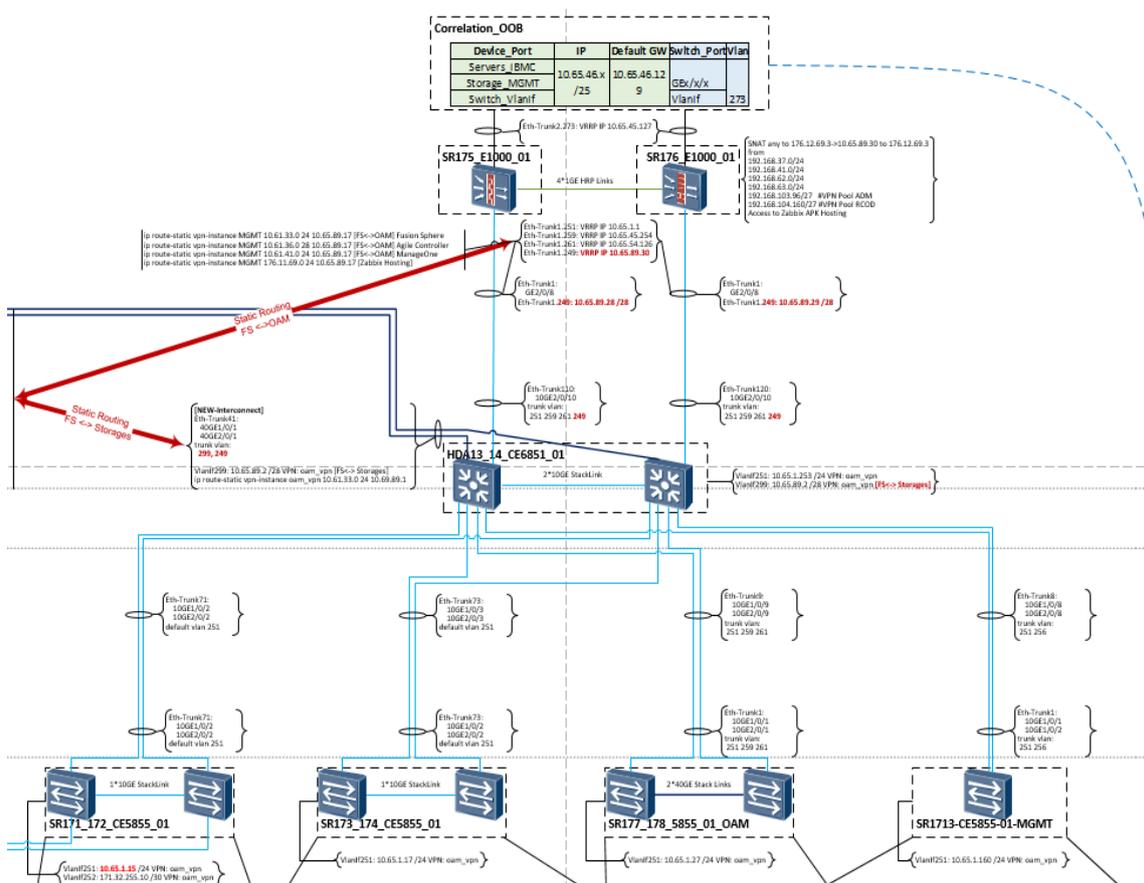


Рис. 4. SBI программно-определяемой сети

Южный интерфейс отвечает за управление и мониторинг ресурсов со стороны центра обработки данных оператора программно-определяемой сети. На основании статистических данных, полученных от агрегационных коммутаторов, SDN-контроллер принимает решения об увеличении (уменьшении) пропускной способности VxLAN, количестве выделяемых ресурсов для обработки информации на уровне приложений и уровне инфраструктуры, удалении и миграции виртуальных машин, а также запускает динамическую синхронизацию таблиц потоков трафика через различные коммутаторы, как физические, так и виртуальные.

В данном случае, при сегментировании участков инфраструктуры центра обработки данных, контроллер программно-определяемой сети является виртуальным распределенным элементом управления, который является уникальным для каждого клиента, а также оценивает работу не только каждого сегмента сети, но и взаимосвязь всех информационных ресурсов в целом, представленных оператором облачной инфраструктуры.

В соответствии с указанным подходом, каждый VTEP имеет свою уникальную метку для каждого сегмента для каждого клиента центра обработки данных. От распределенных виртуальных коммутаторов данные передаются на агрегационные узлы. Для каждого сегмента на агрегационных узлах зарезервированы независимые порты. После принятия информации

агрегационные узлы с помощью протокола Link aggregation protocol (LACP), а также на основе полученных меток передают общий поток пользовательской информации адресату.

Для обработки сигнальной информации и изменения параметров работы программно-определяемой сети со стороны клиента используются https-запросы через выделенный веб-интерфейс. Для управления и обработки запросов на изменение параметров и конфигурации выделенной клиенту облачной инфраструктуры используется стандартный протокол сетевого управления Simple Network Management Protocol (SNMP) – стандартный интернет протокол для управления устройствами в IP-сетях.

Обеспечение качества передачи данных. Для логирования всех изменений параметров, конфигурации, изменения количества выделенных ресурсов для пользователя, а также хранения всех данных об инцидентах, проходящих на сети, используется системный журнал (System Log – SYSLOG). SYSLOG – это стандарт отправки и регистрации сообщений о происходящих в системе событиях.

В таких системных журналах содержится информация о данных пользователей, которые осуществляли различные запросы, данные о выполнении (невыполнении) запросов, причина отказа, если запрос не выполнен, а также информация о произошедших инцидентах на облачной инфраструктуре и программно-определяемой сети провайдера, время обнаружения, устранения и закрытия инцидента. Системный журнал позволяет производить полноценный анализ работы облачной инфраструктуры и программно-определяемой сети, с целью улучшения качества работы физических и виртуальных устройств и правил их взаимодействия с внешними устройствами (сетями).

С целью уменьшения физических соединений принято решение об использовании TOR-коммутаторов (top of rack). TOR-коммутатор имеет 48 портов с интерфейсами SFP+10 Гбит/с и четыре магистральных порта с интерфейсами QSFP+ 40 Гбит/с, что позволяет получать производительность 1,28 Тбит/с от каждой стойки в выделенном сегменте. В данной программно-определяемой сети используется разделение SBI на управление сетью как оператором, предоставляющим инфраструктуру, так и клиентом, использующим ресурсы центра обработки данных и программно-определяемой сети.

В данном случае, поверх физической инфраструктуры программно-определяемой сети (underlay network) используются логические сети (overlay network), которые позволяют обеспечить повышенную защищенность данных различных клиентов, поскольку при использовании данной архитектуры логические сетевые элементы программно-определяемой сети независимы друг от друга. Каждая логическая сеть является отдельной сетью, из которой доступны только отдельные логические элементы и виртуальные выделенные ресурсы, определенные оператором программно-определяемой сети, что позволяет ограничить взаимодействие между различными логическими сетями и препятствует несанкционированному доступу потенциальных злоумышленников.

Указанный подход к реализации архитектуры облачной инфраструктуры способствует экономии вычислительных ресурсов, что, в свою очередь, помогает экономить потребляемую электроэнергию оборудования и, соответственно, затраты оператора облачной инфраструктуры.

Представленная архитектура и выбранная конфигурация рассмотренной программно-определяемой сети на основе использования статических маршрутов (туннелей) имеет ряд существенных преимуществ по сравнению со стандартными подходами к реализации программно-конфигурируемых сетей, используемых в масштабируемых высоконагруженных распределенных системах облачных вычислений. Одним из важнейших преимуществ рассмотренной конфигурации является сокращение времени передачи информации за счет отсутствия необходимости поиска альтернативных оптимальных маршрутов, при высокой загрузке маршрута существующего канала передачи информации между центром обработки данных и стороной клиента, как для пользовательского (data plane), так и для сигнального трафика (control plane). При этом также сокращаются потери пакетов, задержки (latency) и фазовое дрожание цифрового сигнала (jitter) на 0,3 мс на каждом физическом (виртуальном) узле (next hop) передачи данных.

Поскольку оверлейная сеть на основе статических маршрутов (туннелей) позволяет использовать 16 277 214 уникальных соединений для каждого из представленных сегментов каждой подсети представляется возможность использования изолированной системы между центром обработки данных и каждым клиентом. В данном случае каждый клиент получает собственную изолированную сеть передачи данных с разделением передаваемой клиентской (data plane) и сигнальной (control plane) информации.

Заключение. Выбранный подход с разделением управления отдельными сегментами различных составляющих информационных систем (пример – Infrastructure as a Service), такими как сетевой инфраструктурой, системами хранения данных, серверами приложений и виртуальными машинами, позволяют сократить время на изменение конфигурации системы облачных вычислений. При этом сокращаются потери пакетов, задержки (latency) и фазовое дрожание цифрового сигнала (jitter) на 0,3 мс на каждом физическом (виртуальном) узле (next hop) передачи данных.

Данный принцип позволяет быстро локализовать и устранить вышедшие аварии на сети, тем самым дает возможность сохранить ключевые показатели эффективности (Key Performance Indicator – KPI) работы программно-определяемой сети и центра обработки данных, а также выполнить соглашение об уровне обслуживания (Service Level Agreement – SLA) по устранению любых недостатков в работе предоставленной оператором облачной инфраструктуры для нужд клиентов.

DATA QUALITY ASSURANCE IN SOFTWARE-DEFINED NETWORKS BASED ON STATIC VXLAN WITH DYNAMIC BANDWIDTH

U.A. VISHNIAKOU, B.A. MONICH

Abstract

Considered the possibility of using a model of data transmission in software-defined networks based on the use of static routes (tunnels) in overlay networks with dynamic bandwidth (VXLAN). The comparative of the presented architecture of the software-defined network with the classical architecture is carried out. The advantages of using the considered configuration in comparison with standart approaches to the implementation of software-defined networks are determined.

Список литературы

1. Программно-определяемые сети (Software Defined Networks) : настоящее и будущее [Электронный ресурс]. – Режим доступа : <https://habr.com/en/company/hpe/blog/160531/>. – Дата доступа : 15.01.2021.
2. Вишняков, В. А. Модели и управление качеством программно-определяемых сетей / В. А. Вишняков, Б. А. Монич // Проблемы инфокоммуникаций. – 2019. – № 1. – С. 42–47.
3. VMware technical datasheet. Best practice for performance tuning of latency-sensitive workloads in VMs. Technical white paper. – 2013. – 10 p.
4. Yeganeh, Soheil Hassas University of Toronto : About scalability of software-defined network // IEEE Communications magazine, February. – 2019. – P. 136–141.