Internet Engineering Task Force (IETF)
Request for Comments: 8938
Category: Informational
ISSN: 2070-1721

B. Varga, Ed.
J. Farkas
Ericsson
L. Berger
LabN Consulting, L.L.C.
A. Malis
Malis Consulting
S. Bryant
Futurewei Technologies

November 2020

Deterministic Networking (DetNet) Data Plane Framework

Модель плоскости данных детерминированных сетей (DetNet)

Аннотация

В этом документе описана общая схема плоскости данных детерминированных сетей (DetNet[1]). Докумен охватывает концепции и вопросы, относящиеся к любой спецификации плоскости данных DetNet, а также включает общие вопросы, относящиеся к плоскости контроллера (Controller Plane).

Статус документа

Этот документ не является спецификацией какого-либо стандарта Internet (Internet Standards Track) и публикуется с информационными целями.

Документ является результатом работы IETF[2] и представляет согласованный взгляд сообщества IETF. Документ прошел открытое обсуждение и был одобрен для публикации IESG[3]. Не все документы, одобренные IESG, претендуют на статус стандартов Internet, как отмечено в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, обнаруженных ошибках и способах передачи откликов на документ можно найти на странице https://www.rfc-editor.org/info/rfc8938.

Оглавление

[1]Deterministic Networking.
[2]Internet Engineering Task Force.
[3]Internet Engineering Steering Group.

1. Введение

Детерминированные сети DetNet обеспечивают возможность передачи определенных индивидуальных или групповых потоков данных для приложений в реальном масштабе времени (real-time) с чрезвычайно низким уровень потерь и гарантированным предельным (максимум) значением сквозной задержки. Общее описание основ и концепций DetNet дано в [RFC8655].

Этот документ описывает концепции, потребные для спецификации любой плоскости данных DetNet (т. е. связанного с DetNet использования полей заголовков), и рассматривает вопросы, относящиеся ко всем совместимым реализациям. Документ охватывает компоненты сервиса DetNet, сервисный подуровень DetNet и функции подуровня пересылки DetNet, как описано в архитектуре DetNet [RFC8655].

Архитектура DetNet моделирует связанные с DetNet функции плоскости данных как разделенные на два уровня - сервиса и пересылки. Подуровень сервиса служит для защиты сервиса DetNet и переупорядочения. Подуровень пересылки использует механизмы организации трафика и обеспечивает защиту от перегрузок (малые потери, гарантия низкой задержки и ограниченного нарушения порядка). Конкретный подуровень пересылки может обеспечивать свойства, недоступные другим уровням пересылки. DetNet использует имеющиеся подуровни пересылки с соответствующими возможностями и не требует эквивалентных возможностей разных подуровней пересылки.

Как часть функций сервисного подуровня в этом документе описаны типовые операции плоскости данных DetNet, включая функции репликации (Packet Replication Function или PRF), исключения (Packet Elimination Function или PEF) и упорядочения (Packet Ordering Function или POF) пакетов внутри подуровня. Описан также подуровень пересылки.

Как определено в [RFC8655], потоки DetNet могут передаваться на основе технологий, способных обеспечить требуемые характеристики услуг для DetNet. Например, потоки DetNet MPLS могут передаваться через подсети IEEE 802.1 Time-Sensitive Networking (TSN) [IEEE802.1TSNTG], однако поддержка IEEE 802.1 TSN не требуется в DetNet. Вытеснение кадров TSN является примером свойства уровня пересылки, которое обычно не используется в других технологиях пересылки. Большинство преимуществ DetNet можно обеспечить при работе на основе канальных уровней, не приспособленных специально для поддержки всех возможностей TSN, но для таких сетей и смешанного трафика характеристики задержки и ее вариаций могут различаться из-за внутренних свойств подуровня пересылки.

Различные потоки приложений (например, Ethernet или IP) могут отображаться на сеть DetNet. В DetNet может использоваться информация заголовков, предоставляемая приложениями или общая с ними. Примеры обобщенных полей заголовков приведены в [RFC8939].

В документе также рассмотрены базовые концепции, относящиеся к уровню контроллера и OAM[1]. Детали OAM плоскости данных выходят за рамки документа.

2. Терминология

2.1. Используемые в документе термины

В этом документе используется терминология, представленная в архитектуре DetNet [RFC8655], и предполагается, что читатель знаком с этим документом.

2.2. Сокращения

Ниже приведены расшифровки используемых в документе сокращений.

BGP Border Gateway Protocol - протокол междоменной маршрутизации (граничного шлюза).

CoS Class of Service - класс обслуживания.

d-CW DetNet Control Word - управляющее слово DetNet.

DetNet Deterministic Networking - детерминированная сеть.

[1]Operations, Administration, and Maintenance - операции, администрирование и поддержка.

DN	DetNet
GMPLS	Generalized Multiprotocol Label Switching - обобщенная коммутация по меткам.
GRE	Generic Routing Encapsulation - базовая инкапсуляция маршрутных данных.
IPsec	IP Security - защита IP.
L2	Layer 2 - канальный уровень.
LSP	Label Switched Path - путь с коммутацией по меткам.
MPLS	Multiprotocol Label Switching - многопротокольная коммутация по меткам.
OAM	Operations, Administration, and Maintenance - операции, администрирование и поддержка.
PCEP	Path Computation Element Communication Protocol - коммуникационный протокол элементов расчета пути.
PEF	Packet Elimination Function - функция исключения пакетов.
POF	Packet Ordering Function - функция упорядочения пакетов.
PREOF	Packet Replication, Elimination, and Ordering Functions - функции репликации, исключения и упорядочения пакетов.
PRF	Packet Replication Function - функция репликации пакетов.
PSN	Packet Switched Network - сеть с коммутацией пакетов.
QoS	Quality of Service - качество обслуживания.
S-Label	DetNet "service" label - метка сервиса DetNet.
TDM	Time-Division Multiplexing - мультиплексирование с разделением по времени.
TSN	Time-Sensitive Networking - чувствительные к времени сети.
YANG	Yet Another Next Generation

3. Обзор плоскости данных DetNet

В этом документе описано, как потоки приложений (App-flow) [RFC8655] передаются через сети DetNet. Архитектура DetNet [RFC8655] моделирует относящиеся к DetNet функции плоскости данных как разделенные на два подуровня - сервис и пересылка.

На рисунке 1 из [RFC8655] показана логическая схема сервиса DetNet с двумя подуровнями.

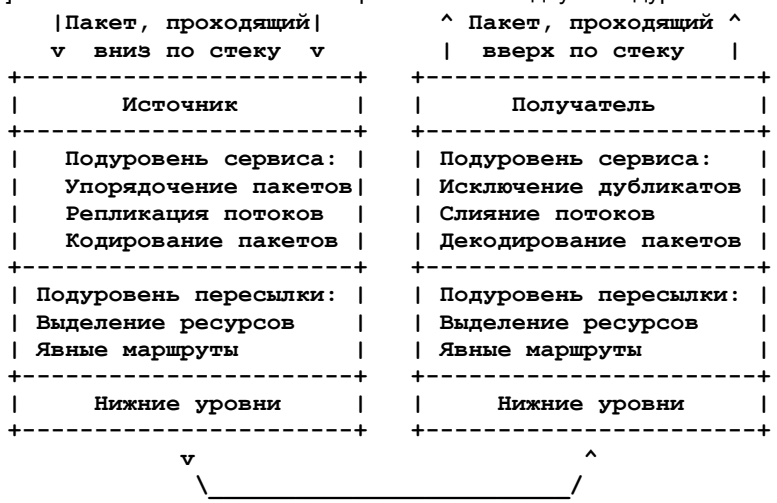

Рисунок 1. Стек протоколов плоскости данных DetNet.

Подуровень пересылки DetNet может напрямую обеспечиваться подуровнем сервиса DetNet, например с помощью туннелей IP или MPLS. Кроме того, может применяться наложение, где пакеты естественным путем передаются между ключевыми узлами сети DetNet (скажем, между узлами PREOF) и применяется подуровень для предоставления информации, требуемой для достижения следующего этапа в наложенной системе.

Подуровень пересылки обеспечивает связанные с QoS функции, требуемые для потоков DetNet. Это можно делать напрямую, используя очереди и методы организации трафика, или с помощью базового уровня. Например, можно использовать возможности IEEE 802.1 TSN [IEEE802.1TSNTG]. Подуровень пересылки использует буферные ресурсы для очередей пакетов и выделения пропускной способности.

Подуровень сервиса обеспечивает дополнительную поддержку сверх обеспечиваемых подуровнем пересылки функций связности (см. параграф 4.3. Функции PREOF. Функции POF используют порядковые номера, добавляемые в пакеты, для реализации разных функций упорядочения от простого сохранения порядка и отбрасывания нарушающих порядок пакетов до комплексного восстановления порядка при фиксированном числе допустимых нарушений и с минимальной задержкой. Для восстановления порядка нужны буферные ресурсы и оно влияет на задержку (и ее вариации) пакетов в потоке DetNet.

Метод создания экземпляров каждого из уровней зависит от конкретной плоскости данных DetNet с возможностью использования множества подходов для данного типа сети.

3.1. Характеристики плоскости данных

Двумя основными характеристиками плоскости данных являются технология и инкапсуляция, рассмотренные ниже.

3.1.1. Технология плоскости данных

Плоскость данных DetNet обеспечивается подуровнями сервиса и пересылки DetNet. Подуровень сервиса DetNet обычно предоставляет свои функции потокам приложений DetNet путем использования имеющихся стандартизованных заголовков и/или инкапсуляции. Подуровень пересылки DetNet может использовать возможности тех же заголовков и инкапсуляции (например, DN IP или DN MPLS) или применять иные технологии, как показано на рисунке 2. Для DetNet в настоящее время определена работа через сети с коммутацией пакетов (IP) и коммутацией по меткам (MPLS).

3.1.2. Инкапсуляция

DetNet кодирует конкретные атрибуты потока (отождествление и порядковый номер) в пакетах. Например, в DetNet IP инкапсуляция не применяется и нет порядковых номеров, в DetNet MPLS связанная с DetNet информация может явно добавляться в пакеты в форме S-Label и d-CW [DetNet-MPLS].

Инкапсуляция потока DetNet позволяет передавать его через плоскости данных, не являющиеся естественными (native). DetNet использует данные заголовков для классификации трафика, т. е. идентификации потоков DetNet, и обеспечения функций сервиса и пересылки DetNet. Как отмечено выше, DetNet может добавлять заголовки, как в случае DN MPLS, или применять уже имеющиеся заголовки, как в DN IP. На рисунке 2 показаны некоторые связи между компонентами.

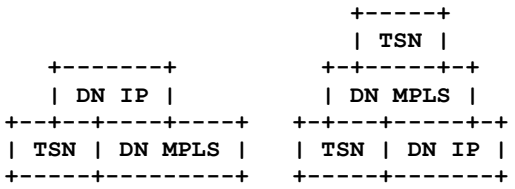

Рисунок 2. Примеры сервиса DetNet.

Использование инкапсуляции также требуется, если плоскости данных DetNet нужна дополнительная информация (метаданные) и (1) нет возможности включить ее в клиентские пакеты данных или (2) спецификация плоскости данных клиента не позволяет изменять пакеты для включения в них дополнительных данных. Примером таких метаданных является включение порядковых номеров, требуемых для PREOF.

Инкапсуляция может также служить для передачи или агрегирования потоков в оборудовании с ограниченными возможностями DetNet.

3.2. Метаданные DetNet

Плоскость данных DetNet может предоставлять и передавать два типа данных:

1. идентификаторы потоков (Flow-ID);
2. порядковые номера.

Плоскость данных DetNet поддерживает Flow-ID (для идентификации потока или агрегата потоков) и/или порядковый номер (для PREOF) в каждом потоке DetNet. Flow-ID применяется подуровнями сервиса и пересылки, а порядковый номер - только сервисным уровнем. Метаданные могут также применяться для OAM и измерений в операциях плоскости данных DetNet.

Включение метаданных может быть явным или неявным. При явном включении указывается выделенное поле заголовка, используемое для включения метаданных в пакет DetNet. При неявном включении для кодирования метаданных служит часть имеющегося заголовка.

Явное включение метаданных возможно за счет использования опций или заголовков расширения IP. Новые опции IP стандартизовать или реализовать в работающей сети уже практически невозможно и это дальше не рассматривается. Заголовки расширения IPv6 становятся популярными в текущих разработках IPv6, в частности, вместе с сегментной маршрутизацией IPv6 (Segment Routing или SRv6) и IP OAM. Разработка новых или изменение имеющихся заголовков расширения IPv6 доступны в наборе инструментов разработчика плоскости данных DetNet IP.

Явное включение метаданных в пакет IP также возможно за счет добавления стека меток MPLS и MPLS d-CW с использованием одного из методов для передачи MPLS по протоколу IP [DetNet-MPLS-over-UDP-IP]. Это более подробно рассматривается в параграфе 3.5.5. Подсети.

Неявные метаданные можно включить в IP путем использования парадигмы сетевого программирования [SRv6-Network-Prog], где суффикс адреса IPv6 служит для представления дополнительной информации, используемой сетью принимающего хоста.

Примером явных данных MPLS являются порядковые номера, используемые PREOF, и даже случай включения всей требуемой информации в стек меток DetNet-over-MPLS (d-CW и DetNet S-Label).

3.3. Плоскость данных DetNet IP

Плоскость данных DetNet IP может работать естественным способом или с использованием инкапсуляции. Требованиям DetNet удовлетворяет много типов инкапсуляции IP и предполагается возможность использования нескольких типов (например, GRE, IPsec).

Одним из вариантов работы плоскости данных DetNet IP без инкапсуляции является использование идентификации потоков на основе кортежей 6-tuple (данные из заголовка IP и вышележащего уровня). Общие сведения об использовании заголовков IP и кортежей 6-tuple для идентификации потоков и поддержки QoS можно найти в [RFC3670]. Дополнительным полем 6-tuple является поле DSCP в пакете. В [RFC7657] представлены полезные

сведения о дифференцированных услугах (Diffserv) и идентификации потоков на основе кортежей. Агрегирование потоков DetNet может быть обеспечено за счет применения шаблонов, масок, префиксов и диапазонов. Работа этого метода подробно описана в [RFC8939].

Плоскость пересылки DetNet может использовать явные маршруты и возможности организации трафика для организации подуровня пересылки, отвечающего за выделение ресурсов и явные маршруты. Такую информацию можно включить в естественные пакеты IP явно или неявно.

3.4. Плоскость данных DetNet MPLS

MPLS обеспечивает подуровень пересылки для трафика по явным или неявным путем к точкам сети, где будет выполняться следующее действие подуровня сервиса DetNet. Это выполняется за счет использования стека с одной или множеством меток с различной семантикой пересылки.

MPLS также позволяет идентифицировать экземпляр сервиса, используемый для обработки пакетов с помощью метки, отображающей пакет на экземпляр сервиса.

В случаях, где требуются метаданные для обработки пакетов с инкапсуляцией MPLS на подуровне сервиса, можно применять d-CW [DetNet-MPLS]. Хотя управляющие слова d-CW часто имеют размер 32 бита, это не является архитектурным ограничением на размер структуры и задается лишь требование, чтобы структура была понятна всем сторонам, работающим на подуровне сервиса DetNet. Работа метода подробно описана в [DetNet-MPLS].

3.5. Другие вопросы плоскости данных DetNet

В этом разделе приведена информация, связанная с предоставлением услуг DetNet потокам на основании данных из заголовков.

3.5.1. Функции, обеспечиваемые на уровне потока

На верхнем уровне обеспечиваются на уровне потока описанные ниже функции.

3.5.1.1. Резервирование и выделение ресурсов

Ресурсы могут резервироваться, чтобы быть доступными для выделения конкретным потокам DetNet. Это может предотвратить «соперничество» и потери пакетов для трафика DetNet, а также снизить вариации задержки (jitter). Ресурсы, выделенные потоку DetNet, защищают его от других потоков трафика. С другой стороны предполагается, что потоки DetNet ведут себя в соответствии с зарезервированным профилем трафика. Должна обеспечиваться возможность обнаружения некорректного поведения потоков DetNet и предотвращения нарушений ими требований QoS других потоков. Очереди, правила и формовка трафика могут служить для распределения ресурсов, резервируемых DetNet.

3.5.1.2. Явные маршруты

Поток можно направить по заданному заранее пути. Это позволяет контролировать задержку в сети, отправляя пакеты с возможностью влияния на физический путь. Явные маршруты дополняют резервирование, позволяя связать согласованный путь с его ресурсами на всем протяжении этого пути. В сочетании с механизмами управления трафиком это ограничивает нарушение порядка пакетов и возможную задержку. При расчете маршрута можно учесть широкий набор ограничений, а также оптимизировать путь по тем или иным характеристикам, например, максимальной пропускной способности или минимальным вариациям задержки. В таких случаях лучшим по некому набору характеристик путем может оказаться не кратчайший. При выборе пути может учитываться множество параметров сети. Некоторые из таких параметров измеряются и распространяются системой маршрутизации как метрика организации трафика.

3.5.1.3. Защита сервиса

Защита сервиса предполагает использование множества потоков пакетов с передачей по множеству путей, например, 1+1 или линейная защита 1:1. Для DetNet это связано в основном с возможностями репликации и исключения пакетов. MPLS обеспечивает множество схем защиты. Безотказную защиту MPLS можно применять для переключения трафика на уже созданный путь с целью быстрого восстановления доставки после отказа. Смена путей даже при восстановлении после отказа может приводить к нарушению порядка пакетов, что требует реализации POF на уровне сервиса DetNet или вышележащем уровне прикладного трафика. Организация новых путей при отказе выходит за рамки услуг DetNet.

3.5.1.4. Сетевое кодирование

Сетевое кодирование (Network Coding) [nwcrg], которое не следует путать с сетевым программированием, включает несколько методов для кодирования множества потоков данных. Получаемые в результате потоки можно передавать по разным путям. Операция кодирования может объединять поток с данными для восстановления ошибок. При декодировании и рекомбинации могут восстанавливаться исходные потоки. Отметим, что сетевое кодирование использует альтернативу попакетному применению PREOF. Поэтому для некоторых вариантов топологии и трафика сетевое кодирование позволяет повысить пропускную способность сети и улучшить параметры эффективности, задержки и расширяемости, а также повысить устойчивость к разделению, атакам и перехвату пакетов по сравнению с традиционными методами. DetNet может применять Network Coding в качестве дополнения к другим средствам защиты. Сетевое кодирование часто применяется в беспроводных сетях и исследуется для других типов сетей.

3.5.1.5. Распределение нагрузки

Использование попакетного (packet-by-packet) распределения нагрузки одного потока DetNet по множеству путей не рекомендуется, за исключением указанных выше случаев, где применяется PREOF для улучшения защиты и сохранения порядка. Попакетное распределение нагрузки, например, по равноценным (Equal-Cost Multipath или ECMP) или неравноценным (Unequal-Cost Multipath или UCMP) путям влияет на порядок и может влиять на вариации задержки.

3.5.1.6. Поиск неисправностей

В DetNet применяется много разных подуровней пересылки, каждый из которых поддерживает свои средства поиска неисправностей в соединениях, например, некорректного поведения потоков. Сервисный уровень DetNet может применять разные механизмы поиска неполадок или мониторинга потоков, такие как используются в сетях IP и MPLS. На уровне приложений клиент службы DetNet может использовать имеющиеся методы обнаружения и отслеживания задержки и потерь.

3.5.1.7. Распознавание потоков для анализа

Сетевая аналитика может наследоваться от технологий, применяемых подуровнями сервиса и пересылки. На границе службы DetNet могут поддерживаться счетчики битов и пакетов (например, переданных, принятых, отброшенных, нарушающих порядок).

3.5.1.8. Сопоставление событий с потоками

Поставщик услуг DetNet может предоставлять другие возможности мониторинга потоков, такие как более подробная статистика потерь или временные метки событий. Рассмотрение этих вопросов выходит за рамки документа.

3.5.2. Защита сервиса

Защита сервиса позволяет повысить отказоустойчивость служб DetNet и поддерживать желаемый уровень гарантий в случаях перегрузки или отказов в сети. DetNet опирается в схемах защиты на возможности используемых базовых технологий. Схемы защиты включают полное или частичное покрытие путей через сеть и активную защиту с использованием комбинаций PRF, PEF и POF.

3.5.2.1. Линейная защита сервиса

На рисунке 3 показан фрагмент сети DetNet MPLS и поток пакетов. Номера на рисунке указывают экземпляры пакета. Пакет 1 является исходным, 1.1 и 1.2 - первые копии исходного пакета, 1.2.1 - копия пакета 1.2 и т. д. Отметим, что эти номера не присутствуют в пакетах и их не следует путать с порядковыми номерами, метками или иными идентификаторами из пакетов. Они приведены здесь лишь для удобства ссылок.

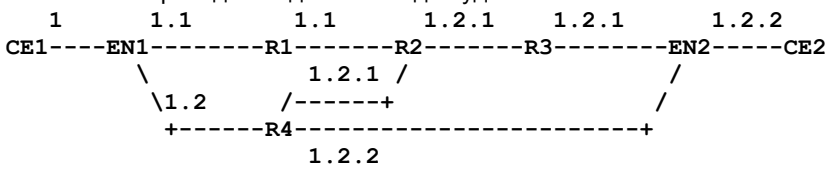

Рисунок 3. Пример потока пакетов, защищенного DetNet.

Пользовательское устройство CE1 передает пакет в сеть с поддержкой DetNet (пакет 1). Краевой узел EN1 инкапсулирует пакет как пакет DetNet и передает его ретранслятору R1 (1.1). EN1 также делает копию пакета (1.2), инкапсулирует ее и передает ретранслятору R4.

Отметим, что ретранслятор R1 может быть подключен к EN1 напрямую или через несколько узлов, которые для простоты на рисунке не показаны. То же можно сказать и о других путях между любыми двумя элементами DetNet.

Ретранслятор R4 можно настроить на отправку одной копии пакета (1.2.1) ретранслятору R2, а другой (1.2.2) - конечному узлу EN2.

R2 получает копию 1.2.1 до прихода копии 1.1 и, поскольку на нем настроено исключение дубликатов для этого потока DetNet, пересылает 1.2.1 ретранслятору R3. Копия 1.1 больше не используется и будет отброшена R2.

Краевой узел EN2 получает копию 1.2.2 от R4 до прихода копии 1.2.1 от R2 через ретранслятор R3. Поэтому EN2 вырезает инкапсуляцию DetNet из копии 1.2.2 и передает пакет CE2. Когда EN2 получает копию 1.2.1, она уже не нужна и отбрасывается.

Для приведенного выше примера можно настроить и другие сценарии.

Пример также иллюстрирует схему защиты 1:1, означающую наличие трафика через каждый сегмент сквозного пути. Локальные ретрансляторы DetNet определяют, какие пакеты нужно переслать, а какие исключить. Схема 1+1, где для трафика в каждый момент применяется лишь один путь, может использовать такую же топологию. В этом случае не будет применяться PRF, а при возникновении отказа произойдет переключение трафика с использованием схемы OAM, отслеживающей отказы. Функция POF может по-прежнему использоваться в этом случае для предотвращения нарушений порядка пакетов. В обоих случаях защитные пути организуются и поддерживаются в течение всего срока работы сервиса DetNet.

3.5.2.2. Дифференциальная зедержка между путями

В предыдущем примере корректное устранение дубликатов и переупорядочение пакетов зависит от числа пакетов с нарушением порядка, которые можно буферизовать, и разницы в задержке прибывающих пакетов. DetNet использует зависящие от потоков требования (например, максимальное число пакетов с нарушением порядка) для настройки связанных с POF буферов. Если дифференциальная задержка разных путей слишком велика или очень много пакетов нарушают порядок, может выполняться отбрасывание пакетов вместо восстановления порядка. Точно так же PEF использует порядковые номера для определения дубликатов и большая дифференциальная задержка в комбинации с большим числом пакетов могут не позволить PEF работать корректно.

3.5.2.3. Защита кольца

Защита кольца может обеспечиваться при ее поддержке базовой технологией. Используется много одинаковых концепций, однако в кольцах обычно применяют защиту 1+1 для обеспечения эффективности обмена данными. В [RFC8227] представлен пример плоскости данных транспортного профиля MPLS (MPLS Transport Profile или MPLS-TP) с поддержкой защиты кольца.

3.5.3. Вопросы агрегирования

Плоскость данных DetNet позволяет также агрегировать потоки DetNet, что может улучшить расширяемость за счет снижения числа состояний для этапов пересылки. Способ реализации этого зависит от плоскостей данных и управления. При агрегировании потоков DetNet транзитные узлы предоставляют услуги агрегату, а не отдельным потокам. Агрегируемые потоки должны быть совместимыми, т. е. иметь одинаковые или близкие характеристики QoS и CoS. В этом случае выполняющие агрегирование узлы будут обеспечивать выполнение требований к обслуживанию для каждого потока.

При резервировании пропускной способности следует указывать сумму отдельных потребностей, иными словами, не должно резервироваться больше, чем требуется суммарно для всех потоков. При ограничении максимальной задержки следует обеспечить для агрегата задержку, не превышающую допустимую для отдельных потоков.

При использовании инкапсуляции выбор между резервированием максимального уровня ресурсов и последующим отслеживанием услуг для агрегата или корректировкой агрегированных ресурсов по мере добавления услуг зависит от реализации и технологии.

На границах для потоков DetNet должна обеспечиваться возможность отклонять агрегирование по причине нехватки ресурсов а также при условиях, когда требования не выполняются.

3.5.3.1. Агрегирование IP

Агрегирование IP включает аспекты плоскостей управления и контроллера. Для плоскости управления потоки могут агрегироваться с целью обработки на основе общих характеристик, таких как 6-tuple [RFC8939]. Дополнительно может применяться инкапсуляция IP для туннелирования агрегата потоков DetNet между ретрансляторами.

3.5.3.2. Агрегирование MPLS

Агрегирование MPLS также включает аспекты плоскостей управления и контроллера. Потоки MPLS часто туннелируются на подуровне пересылки с резервированием, связанным с туннелем MPLS.

3.5.4. Конечные системы

Потоки данных, которым нужен сервис DetNet, создаются и завершаются в конечных системах. Инкапсуляция зависит от приложения и его предпочтений. Например, в домене DetNet MPLS функции подуровня используют d-CW, S-Label и F-Label [DetNet-MPLS] для предоставления услуг DetNet. Однако приложения могут обмениваться параметрами, связанными с потоками (например, временными метками), которые не предоставляются функциями DetNet.

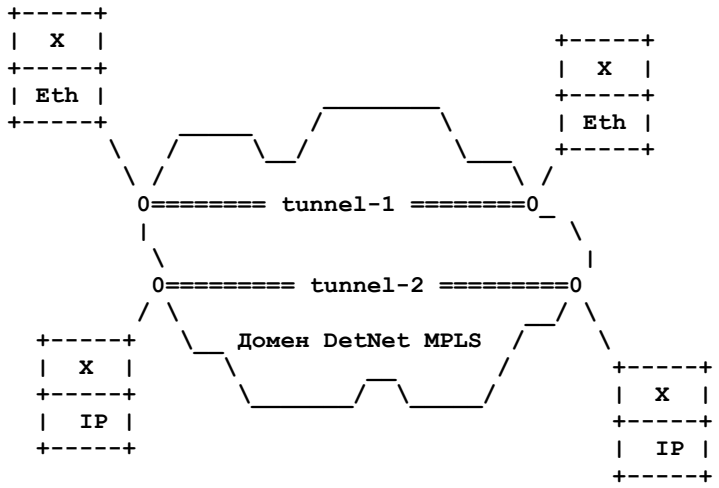

Рисунок 4. Конечные системы и домен DetNet MPLS.

Как правило, домены DetNet способны пересылать любые потоки DetNet и не задают формат инкапсуляции для конечных систем или краевых узлов. Если не используется тот или иной посредник (proxy) конечная система взаимодействует с другой конечной системой, используя общий формат инкапсуляции. Например, на рисунке 4 показано взаимодействие приложений IP и приложений Ethernet.

3.5.5. Подсети

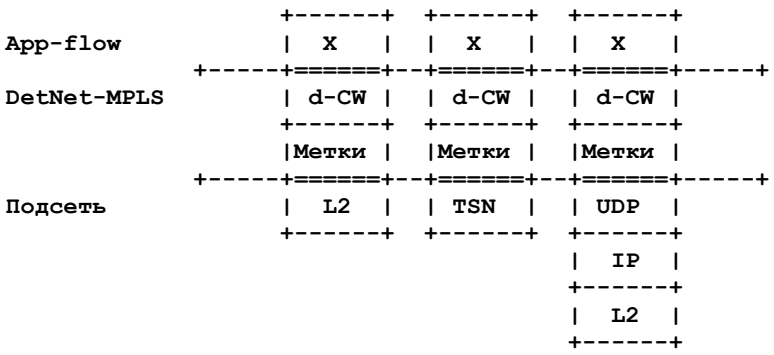

Рисунок 5. Пример инкапсуляции DetNet MPLS в подсетях.

Услуги DetNet любого типа могут предоставляться с использованием другого сервиса DetNet. Узлы MPLS могут быть соединены через подсети с иной технологией, которые могут включать каналы «точка-точка». Каждая из технологий подсетей должна предоставлять услуги, подходящие для потоков DetNet. В некоторых случаях (например, на

выделенных каналах «точка-точка» или при использовании технологии TDM) от узла DetNet требуется лишь подходящая организация очередей для трафика. В иных случаях узлы DetNet должны отображать потоки DetNet на семантику (например, идентификаторы) и механизмы, используемые базовой технологией подсети. На рисунке 5 показано несколько примеров инкапсуляции в подсетях, которая может применяться для передачи потоков DetNet MPLS с использованием других технологий. L2 представляет базовую инкапсуляцию канального уровня, которая может применяться в соединениях «точка-точка». TSN указывает инкапсуляцию IEEE 802.1 TSN [DetNet-MPLS-over-TSN], а UDP/IP - инкапсуляцию DetNet IP PSN [DetNet-MPLS-over-UDP-IP].

4. Плоскость контроллера (поддержка и управление)

4.1. Требования плоскости контроллера DetNet

Плоскость контроллера (Controller Plane) соответствует объединению плоскостей управления и администрирования (Control и Management), описанному в [RFC7426] и [RFC8655]. Подробное рассмотрение плоскости контроллера DetNet выходит за рамки этого документа, однако ниже обсуждаются некоторые вопросы и требования к Controller Plane, связанные с уникальными характеристиками архитектуры DetNet и определенной здесь плоскости данных.

Основные требования к возможностям плоскости контроллера DetNet приведены ниже.

- Создание экземпляров потоков DetNet в домене DetNet (который может, например, включать определение явных путей, резервирование пропускной способности, ограничение потоков в каналы IEEE 802.1 TSN, буферы узлов и другое резервирование ресурсов, спецификация требуемых в пути очередей, возможность управления двухсторонними потоками и т. п.) по мере потребности в потоках.
- В случае MPLS управление выделением и распространением меток DetNet S-Label и F-Label. Использование инкапсуляции DetNet MPLS описано в [DetNet-MPLS].
- Поддержка агрегирования потоков DetNet.
- Анонсирование статических и динамических ресурсов узлов и каналов, таких как возможности и смежность с другими узлами (для динамической сигнализации) или сетевыми контроллерами (централизованный подход).
- Расширение для обработки ожидаемого в домене числа потоков DetNet, для чего может потребоваться сигнализация или обеспечение на уровне потока.
- Предоставление идентификационных данных потоков на каждом узле пути. Идентификация потока может различаться в зависимости от места в домене DetNet (например, транзитный узел и ретранслятор).

Эти требования, как отмечено выше, могут быть выполнены с помощью распределенного сигнального протокола управления (например, RSVP-TE), механизмов централизованного управления сетью (BGP, PCEP, YANG, [DetNet-Flow-Info] и т. п.) или их комбинации, а также можно применять сегментную маршрутизацию на основе MPLS.

Абстрактно результат распределенной сигнализации или централизованного управления будет эквивалентным с точки зрения плоскости данных DetNet - создаются экземпляры потоков, указываются явные маршруты, резервируются ресурсы и пакеты пересылаются через домен с использованием плоскости данных DetNet.

Однако с точки зрения практической реализации варианты плоскости контроллера будут совсем не одинаковыми. Некоторые подходы более расширяемы в плане сигнальной нагрузки на сеть, другие могут обеспечивать преимущества глобального отслеживания ресурсов в домене DetNet для его оптимизации. Некоторые решения могут быть более устойчивы к отказам каналов, узлов или управляющего оборудования. Хотя подробный анализ вариантов плоскости управления выходит за рамки документа, требования этого документа могут использоваться в качестве основы при анализе вариантов.

4.2. Базовая плоскость контроллера

В этом разделе рассматриваются вопросы плоскости управления, не зависящие от технологии плоскости данных, используемой для предоставления услуг DetNet.

Хотя плоскости администрирования и управления обычно рассматривают отдельно, с точки зрения плоскости данных нет практических различий, основанных на источнике информации о предоставлении потоков и в архитектуре DetNet [RFC8655] администрирование и управление отнесены к единой плоскости контроллера (Controller Plane). Поэтому документ не разделяет информацию от распределенных протоколов плоскости управления (например, RSVP-TE [RFC3209] [RFC3473]) и централизованных механизмов управления сетью (например, RESTCONF [RFC8040], YANG [RFC7950], PCEP [PCECC]) или их комбинации. Конкретные вопросы и требования к плоскости контроллера DetNet рассмотрены в разделе 4.1. Требования плоскости контроллера DetNet.

В каждом документе плоскости данных рассматриваются также вопросы плоскости управления для соответствующей технологии. Например, в [RFC8939] охватываются также нормативные аспекты плоскости управления для IP, а в [DetNet-MPLS] - для MPLS.

4.2.1. Управление агрегированием потоков

Агрегирование потоков означает обслуживание множества App-flow одним потоком DetNet. Для агрегирования применяется множество методов, например, в случае IP потоки IP с общими атрибутами 6-tuple или идентификаторами подуровня DetNet можно сгруппировать. Другим примером служит агрегирование с использованием иерархических LSP в MPLS и туннелях.

Управление агрегированием включает набор процедур, перечисленных ниже. Могут применяться все указанные процедуры или их часть, а порядок может меняться.

Сбор и распространение сведений о ресурсах организации трафика

Доступные ресурсы отслеживаются через базы данных плоскостей управления и администрирования и распространяются через контроллеры или узлы, управляющие ресурсами.

Расчет пути и выделение ресурсов

При предоставлении или запросе сервиса DetNet выбирается один или несколько путей с проверкой и записью соответствующих ресурсов.

Координация плоскости данных с назначением ресурсов

Назначение ресурсов на пути зависит от технологии и включает указание соответствующих каналов, координацию очередей и другие средства организации трафика (такие как правила и формовка).

Запись и обновление выделенных ресурсов

В зависимости от конкретной технологии назначенные ресурсы обновляются и информация о них распространяется по базам данных для предотвращения чрезмерного использования.

4.2.2. Явные маршруты

Явные маршруты применяются для гарантированной отправки пакетов по путям с зарезервированными ресурсами, чтобы обеспечить приложениям DetNet требуемое обслуживание. От плоскости контроллера DetNet требуется способность назначить конкретному идентифицированному потоку DetNet IP путь через домен DetNet, которому были выделены требуемые ресурсы на каждом узле. Это обеспечивает подобающую обработку трафика для потока, а также включает как часть пути конкретные каналы, способные поддержать поток DetNet. Например, параметры DetNet можно обеспечить за счет использования каналов IEEE 802.1 TSN [DetNet-MPLS-over-TSN]. Дополнительное рассмотрение требований к плоскости контроллера DetNet приведено в параграфе 4.1. Требования плоскости контроллера DetNet.

Независимо от числа этапов, а также распределенного или централизованного выполнения настройки, расчета и организации рассмотрение этих маршрутов выходит за рамки данного документа.

Существует несколько подходов, которые можно использовать для обеспечения явных маршрутов и выделения ресурсов на подуровне пересылки DetNet. Примеры перечислены ниже.

- Путь может явно устанавливаться контроллером, который рассчитывает маршрут и явно настраивает каждый узел на нем с соответствующей информацией о пересылке и выделении ресурсов.
- Путь может использовать распределенную плоскость управления, такую как RSVP [RFC2205] или RSVP-TE [RFC3473], с расширением для поддержки потоков DetNet IP.
- Путь можно реализовать с использованием сегментной маршрутизации на основе IPv6, расширенной для поддержки выделения ресурсов.

Эти варианты рассмотрены в параграфе 4.1. Кроме того, в [RFC2386] приведены полезные сведения о маршрутизации на основе QoS, а в [RFC5575] (обновлен [Flow-Spec-Rules]) обсуждается конкретный механизм, используемый BGP для задания потоков трафика и маршрутизации на основе правил.

4.2.3. Потери из-за конкуренции и снижение вариаций задержки

Этот документ не задает механизмы, требуемые для предотвращения конкуренции и потери пакетов, а также ограничения вариаций задержки для потоков DetNet на подуровне пересылки DetNet. Способность управлять ресурсами узлов и каналов для обеспечения этих функций является необходимой частью плоскости контроллера DetNet. Необходима также возможность управления требуемыми механизмами очередей, используемыми для обеспечения этих функций на пути через сеть. Эти требования рассматриваются в [RFC8939] и разделе 4.1. Некоторые формы защиты могут минимизировать потерю пакетов или изменить характеристики вариаций задержки при нарушении порядка пакетов, когда такие пакеты получены подуровнем сервиса.

4.2.4. Двухсторонний трафик

Во многих случаях потоки DetNet можно считать односторонними и независимыми. Однако иногда сервис DetNet требует двухстороннего трафика с точки зрения приложений DetNet. В IP и MPLS обычно каждое направление обрабатывается самостоятельно и между встречными направлениями не возникает взаимной зависимости. Рабочая группа IETF MPLS изучила требования к двухстороннему трафику. Определения, представленные в [RFC5654], полезны для иллюстрации двухсторонних потоков, в том числе с общей маршрутизацией. MPLS определяет двухсторонний LSP, связанный с соединением «точка-точка», как два односторонних LSP «точка-точка» (от A к B и от B к A), которые рассматриваются как один логический двухсторонний путь. Это аналог стандартной маршрутизации IP. Двухсторонний LSP «точка-точка» с общей маршрутизацией определяется в MPLS как двухсторонний LSP, удовлетворяющий дополнительному требованию использовать в обоих направлениях один путь (один набор узлов и каналов). Важным свойством таких LSP является «общая судьба» путей в каждом направлении. Для обоих типов двухсторонних LSP резервирование в каждом из направления может быть разным. Концепции связанных двухсторонних потоков (в том числе с общей маршрутизацией) применимы и к потокам DetNet IP.

Хотя плоскость данных DetNet IP должна поддерживать двухсторонние потоки DetNet, нет никаких особых требований, кроме того, что пути обоих направлений двухстороннего потока с общей маршрутизацией должны совпадать. Иными словами, двухсторонние потоки DetNet представлены лишь в плоскостях управления и администрирования без конкретной поддержки в плоскости данных DetNet. Общая судьба и привязка или общая маршрутизация двухсторонних потоков могут поддерживаться на уровне управления.

Использование в DetNet функций PREOF может усложнить работу с двухсторонними потоками, поскольку точки репликации потоков одного направления должны будут совпадать с точками удаления дубликатов обратного направления. В таких случаях оптимальные точки выполнения функций одного направления могут не совпасть с оптимальными точками для обратного направления по причине ограничения сети и трафика. Кроме того, в результате защиты сервиса на уровне пакетов не может обеспечиваться двухсторонняя пересылка. Первый пакет полученного потока участника выбирается функцией исключения дубликатов независимо от пути пакета через сеть.

Механизмы управления и администрирования должны поддерживать двухсторонние потоки, но спецификация таких механизмов выходит за рамки документа. Примеры решений для плоскости управления MPLS можно найти в [RFC3473], [RFC6387] и [RFC7551]. Эти требования включены в раздел 4.1. Требования плоскости контроллера DetNet.

4.3. Функции PREOF

Выбор протокола плоскости контроллера, требуемого для управления работой PREOF, выходит за рамки документа. Тем не менее, следует отметить, что явно требуется возможность определить для конкретного потока оптимальные точки репликации и исключения дубликатов в домене DetNet. Некоторые имеющиеся возможности можно применить или расширить для решения этой задачи, например, сквозное восстановление GMPLS [RFC4872] и восстановление сегментов GMPLS [RFC4873].

5. Вопросы безопасности

Вопросы безопасности DetNet подробно рассматриваются в [DetNet-Security], а базовые проблемы безопасности для архитектуры DetNet - в [RFC8655]. В этом разделе обсуждаются вопросы безопасности на уровне архитектуры DetNet, применимые ко всем плоскостям данных.

Одной из уникальный черт DetNet является способность надежно обеспечивать определенные параметры QoS (доставка потока данных с минимальными потерями пакетов и ограниченной сквозной задержкой), а также связанные с безопасностью аспекты защиты QoS.

Для всех коммуникационных протоколов первоочередной задачей плоскости данных является обеспечение целостности данных и предоставление услуг DetNet через сеть DetNet. Потоки приложений можно защитить любыми способами, предоставляемыми базовой технологией. Например, может применяться шифрование, подобное используемому в IPsec [RFC4301] для потоков IP или MACsec [IEEE802.1AE-2018] для потоков Ethernet (L2).

На уровнях управления и поддержки потоки DetNet идентифицируются индивидуально, что может предоставить атакующему плоскость контроллера дополнительную информацию о потоках данных (по сравнению с плоскостями контроллера, не включающими идентификацию на уровне потока). Это унаследованное свойство DetNet, которое влияет на безопасность и должно учитываться при решении вопроса о применении DetNet для конкретной задачи.

Для обеспечения непрерывной доступности сервиса DetNet могут быть приняты меры против атак на службы (DoS) и атак с задержками. Для защиты от DoS-атак избыточный трафик от вредоносных или некорректно работающих устройств можно предотвратить или ослабить, например, с помощью имеющихся механизмов, таких как правила и формовка на входе в домен DetNet. Для предотвращения вредоносной задержки пакетов DetNet за пределами домена DetNet определения технологии DetNet могут смягчать перехват и изменение в пути с участием человека (MITM[1]-атака), например за счет проверки подлинности и полномочий устройств в домене DetNet.

Для предотвращения или смягчения атак DetNet на другие сети за счет выхода потоков наружу можно, например, применять на выходе из домена DetNet имеющиеся механизмы, такие как правила и формовка.

6. Взаимодействие с IANA

Этот документ не требует действий со стороны IANA.

7. Литература

7.1. Нормативные документы

[RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

7.2. Дополнительная литература

[DetNet-Flow-Info] Varga, B., Farkas, J., Cummings, R., Jiang, Y., and D. Fedyk, "DetNet Flow Information Model", Work in Progress, Internet-Draft, draft-ietf-detnet-flow-information-model-11, 21 October 2020, <https://tools.ietf.org/html/draft-ietf-detnet-flow-information-model-11>.

[DetNet-MPLS] Varga, B., Ed., Farkas, J., Berger, L., Malis, A., Bryant, S., and J. Korhonen, "DetNet Data Plane: MPLS", Work in Progress, Internet-Draft, draft-ietf-detnet-mpls-13, 11 October 2020, <https://tools.ietf.org/html/draft-ietf-detnet-mpls-13>.

[DetNet-MPLS-over-TSN] Varga, B., Ed., Farkas, J., Malis, A., and S. Bryant, "DetNet Data Plane: MPLS over IEEE 802.1 Time Sensitive Networking (TSN)", Work in Progress, Internet-Draft, draft-ietf-detnet-mpls-over-tsn-04, 2 November 2020, <https://tools.ietf.org/html/draft-ietf-detnet-mpls-over-tsn-04>.

[DetNet-MPLS-over-UDP-IP] Varga, B., Ed., Farkas, J., Berger, L., Malis, A., and S. Bryant, "DetNet Data Plane: MPLS over UDP/IP", Work in Progress, Internet-Draft, draft-ietf-detnet-mpls-over-udp-ip-07, 11 October 2020, <https://tools.ietf.org/html/draft-ietf-detnet-mpls-over-udp-ip-07>.

[DetNet-Security] Grossman, E., Ed., Mizrahi, T., and A. Hacker, "Deterministic Networking (DetNet) Security Considerations", Work in Progress, Internet-Draft, draft-ietf-detnet-security-12, 2 October 2020, <https://tools.ietf.org/html/draft-ietf-detnet-security-12>.

[Flow-Spec-Rules] Loibl, C., Hares, S., Raszuk, R., McPherson, D., and M. Bacher, "Dissemination of Flow Specification Rules", Work in Progress, Internet-Draft, draft-ietf-idr-rfc5575bis-27, 15 October 2020, <https://tools.ietf.org/html/draft-ietf-idr-rfc5575bis-27>.

[IEEE802.1AE-2018] IEEE, "IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security", IEEE Std 802.1AE-2018, DOI 10.1109/IEEESTD.2018.8585421, December 2018, <https://ieeexplore.ieee.org/document/8585421>.

[IEEE802.1TSNTG] IEEE, "Time-Sensitive Networking (TSN) Task Group", <https://1.ieee802.org/tsn/>.

[nwcrg] IRTF, "Coding for efficient NetWork Communications Research Group (nwcrg)", <https://datatracker.ietf.org/rg/nwcrg/about>.

[1]Man-in-the-middle - «человек в середине».

[PCECC] Li, Z., Peng, S., Negi, M. S., Zhao, Q., and C. Zhou, "PCEP Procedures and Protocol Extensions for Using PCE as a Central Controller (PCECC) of LSPs", Work in Progress, Internet-Draft, draft-ietf-pce-pcep-extension-for-pce-controller-08, 1 November 2020, <https://tools.ietf.org/html/draft-ietf-pce-pcep-extension-for-pce-controller-08>.

[RFC2205] Braden, R., Ed., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, DOI 10.17487/RFC2205, September 1997, <https://www.rfc-editor.org/info/rfc2205>.

[RFC2386] Crawley, E., Nair, R., Rajagopalan, B., and H. Sandick, "A Framework for QoS-based Routing in the Internet", RFC 2386, DOI 10.17487/RFC2386, August 1998, <https://www.rfc-editor.org/info/rfc2386>.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001, <https://www.rfc-editor.org/info/rfc3209>.

[RFC3473] Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, DOI 10.17487/RFC3473, January 2003, <https://www.rfc-editor.org/info/rfc3473>.

[RFC3670] Moore, B., Durham, D., Strassner, J., Westerinen, A., and W. Weiss, "Information Model for Describing Network Device QoS Datapath Mechanisms", RFC 3670, DOI 10.17487/RFC3670, January 2004, <https://www.rfc-editor.org/info/rfc3670>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4872] Lang, J.P., Ed., Rekhter, Y., Ed., and D. Papadimitriou, Ed., "RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery", RFC 4872, DOI 10.17487/RFC4872, May 2007, <https://www.rfc-editor.org/info/rfc4872>.

[RFC4873] Berger, L., Bryskin, I., Papadimitriou, D., and A. Farrel, "GMPLS Segment Recovery", RFC 4873, DOI 10.17487/RFC4873, May 2007, <https://www.rfc-editor.org/info/rfc4873>.

[RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <https://www.rfc-editor.org/info/rfc5575>.

[RFC5654] Niven-Jenkins, B., Ed., Brungard, D., Ed., Betts, M., Ed., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, DOI 10.17487/RFC5654, September 2009, <https://www.rfc-editor.org/info/rfc5654>.

[RFC6387] Takacs, A., Berger, L., Caviglia, D., Fedyk, D., and J. Meuric, "GMPLS Asymmetric Bandwidth Bidirectional Label Switched Paths (LSPs)", RFC 6387, DOI 10.17487/RFC6387, September 2011, <https://www.rfc-editor.org/info/rfc6387>.

[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>.

[RFC7551] Zhang, F., Ed., Jing, R., and R. Gandhi, Ed., "RSVP-TE Extensions for Associated Bidirectional Label Switched Paths (LSPs)", RFC 7551, DOI 10.17487/RFC7551, May 2015, <https://www.rfc-editor.org/info/rfc7551>.

[RFC7657] Black, D., Ed. and P. Jones, "Differentiated Services (Diffserv) and Real-Time Communication", RFC 7657, DOI 10.17487/RFC7657, November 2015, <https://www.rfc-editor.org/info/rfc7657>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8227] Cheng, W., Wang, L., Li, H., van Helvoort, H., and J. Dong, "MPLS-TP Shared-Ring Protection (MSRP) Mechanism for Ring Topology", RFC 8227, DOI 10.17487/RFC8227, August 2017, <https://www.rfc-editor.org/info/rfc8227>.

[RFC8939] Varga, B., Ed., Farkas, J., Berger, L., Fedyk, D., and S. Bryant, "Deterministic Networking (DetNet) Data Plane: IP", RFC 8939, DOI 10.17487/RFC8939, November 2020, <https://www.rfc-editor.org/info/rfc8939>.

[SRv6-Network-Prog] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "SRv6 Network Programming", Work in Progress, Internet-Draft, draft-ietf-spring-srv6-network-programming-26, 26 November 2020, <https://tools.ietf.org/html/draft-ietf-spring-srv6-network-programming-26>.

Благодарности

Авторы благодарят Pat Thaler, Norman Finn, Loa Andersson, David Black, Rodney Cummings, Ethan Grossman, Tal Mizrahi, David Mozes, Craig Gunther, George Swallow, Yuanlong Jiang, Carlos J. Bernardos за их вклад в работу.

Участники работы

Существенный вклад в создание этого документа внесли Don Fedyk и Jouni Korhonen

Адреса авторов

Balázs Varga (editor)

Ericsson

Budapest

Magyar Tudosok krt. 11.

1117

Hungary

Email: balazs.a.varga@ericsson.com

János Farkas

Ericsson

Budapest

Magyar Tudosok krt. 11.

1117

Hungary

Email: janos.farkas@ericsson.com

Lou Berger

LabN Consulting, L.L.C.

Email: lberger@labn.net

Andrew G. Malis

Malis Consulting

Email: agmalis@gmail.com

Stewart Bryant

Futurewei Technologies

Email: sb@stewartbryant.com

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru