Internet Engineering Task Force (IETF)
Request for Comments: 8939
Category: Standards Track
ISSN: 2070-1721

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

November 2020

Deterministic Networking (DetNet) Data Plane: IP

Плоскость данных DetNet IP

Аннотация

Этот документ определяет работу плоскости данных детерминированной сети (DetNet[1]) для хостов и маршрутизаторов IP, обеспечивающих услуги DetNet для инкапсулированных в IP данных. Специфической для DetNet инкапсуляции не задается для поддержки потоков IP и вместо этого применяется информация из заголовков IP и вышележащего протокола для поддержки идентификации потоков и предоставления услуг DetNet. Документ основан на архитектуре DetNet (RFC 8655) и модели плоскости данных (RFC 8938).

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[2] и представляет согласованный взгляд сообщества IETF. Документ прошел открытое обсуждение и был одобрен для публикации IESG[3]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc8939.

Оглавление

1. Введение....2
2. Терминология....2
2.1. Используемые в документе термины....2
2.2. Сокращения....2
2.3. Уровни требований....3
3. Обзор плоскости данных DetNet IP....3
4. Плоскость данных DetNet IP....4
4.1. Конечные точки....4
4.2. Домен DetNet....4
4.3. Подуровень пересылки....5
4.3.1. Класс обслуживания....5
4.3.2. Качество обслуживания....5
4.3.3. Выбор пути....5
4.4. Агрегирование потоков DetNet....6
4.5. Двухсторонний трафик....6
5. Процедуры плоскости данных DetNet IP....6
5.1. Процедуры идентификации потоков DetNet IP....6
5.1.1. Данные заголовка IP....7
5.1.1.1. Поле адреса отправителя....7
5.1.1.2. Поле адреса получателя....7
5.1.1.3. Поля IPv4 Protocol и IPv6 Next Header....7
5.1.1.4. Поля IPv4 Type of Service и IPv6 Traffic Class....7
5.1.1.5. Поле IPv6 Flow Label....7
5.1.2. Другая информация из заголовков....7

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

5.1.2.1. TCP и UDP....7
5.1.2.1.1. Поле Source Port....7
5.1.2.1.2. Поле Destination Port....7
5.1.2.2. ICMP....7
5.1.2.3. IPsec AH и ESP....7
5.2. Процедуры пересылки....8
5.3. Процедуры обработки трафика DetNet IP....8
6. Поддержка и управление....8
7. Вопросы безопасности....8
8. Взаимодействие с IANA....9
9. Литература....9
9.1. Нормативные документы....9
9.2. Дополнительная литература....9
Благодарности....10
Участники работы....11
Адреса авторов....11

1. Введение

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

Этот документ задает работу плоскости данных DetNet для хостов и маршрутизаторов IP, предоставляющих услуги DetNet для инкапсулированных в IP данных. Специфической для DetNet инкапсуляции не задается для поддержки потоков IP и вместо этого применяется информация из заголовков IP и вышележащего протокола для поддержки идентификации потоков и предоставления услуг DetNet. Общие сведения и информация об управлении для всех плоскостей данных DetNet представлена в [RFC8938].

Архитектура DetNet моделирует связанные с DetNet функции плоскости данных как разделенные на два уровня - сервиса и пересылки. Подуровень сервиса служит для защиты сервиса DetNet (например, с помощью функций PRF[1] и PEF[2]) и переупорядочения. Подуровень пересылки обеспечивает защиту от перегрузок (малые потери, гарантия низкой задержки и ограниченного нарушения порядка). Подуровень сервиса обычно требует для работы использования дополнительных полей заголовка (см. например, [DetNet-MPLS]). Поскольку связанных с DetNet полей не добавляется для поддержки потоков DetNet IP, поддерживаются лишь функции подуровня пересылки с использованием DetNet IP в соответствии с данным документом. Защита сервиса может обеспечиваться на уровне подсети с применением таких технологий, как MPLS [DetNet-MPLS] и Ethernet (в соответствии с IEEE 802.1 TSN) [IEEE802.1TSNTG].

Этот документ содержит обзор плоскости данных DetNet IP в разделе 3 и рассматривает вопросы предоставления услуг DetNet на основе плоскости данных DetNet IP в разделе 4. Раздел 5 описывает процедуры для хостов и маршрутизаторов, поддерживающих услуги DetNet на базе IP, а раздел 6 обобщает сведения, требуемые для идентификации отдельных потоков DetNet.

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

DetNet	Deterministic Networking - детерминированная сеть.
DN	DetNet
Diffserv	Differentiated Services - дифференцированное обслуживание.
DSCP	Differentiated Services Code Point - код дифференцированного обслуживания.
L2	Layer 2 - канальный уровень.
L3	Layer 3 - сетевой 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.
PREOF	Packet Replication, Elimination, and Ordering Functions - функции репликации, исключения и упорядочения пакетов.
PRF	Packet Replication Function - функция репликации пакетов.
QoS	Quality of Service - качество обслуживания.
TSN	Time-Sensitive Networking - чувствительные к времени сети.

[1]Packet Replication Function - функция репликации пакетов.
[2]Packet Elimination Function - функция исключения пакетов.

2.3. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

3. Обзор плоскости данных DetNet IP

В этом документе описано, как IP используется узлами DetNet (т. е. хостами и маршрутизаторами) для идентификации потоков DetNet и обеспечения сервиса DetNet с плоскостью данных IP. С точки зрения плоскости данных используется сквозная модель IP. Как отмечено выше, применяется имеющаяся информация заголовка IP и вышележащего протокола для поддержки идентификации потоков DetNet и предоставления услуг. Базовые процедуры и управляющая информация для всех плоскостей данных DetNet описаны в [RFC8938].

Плоскость данных DetNet IP использует прежде всего идентификацию потока на основе кортежей 6-tuple, включающих данные из заголовков IP и вышележащего протокола. Термин 6-tuple в этом документе соответствует определению [RFC3290] и включает адреса отправителя и получателя, протокол IP, порты отправителя и получателя, а также DSCP. Сведения об использовании заголовков IP и кортежей 5-tuple для идентификации потоков и поддержки QoS приведены в [RFC3670]. В [RFC7657] также представлены полезные сведения по обеспечению Diffserv и идентификации потоков на основе кортежей. Отметим, что 6-tuple представляет собой кортеж 5-tuple с добавлением DSCP.

Для некоторых протоколов кортежи 5-tuple и 6-tuple использовать невозможно, поскольку информация о портах недоступна (например, в ICMP, IPsec, и ESP[1]). Такое возможно и для агрегата потоков. В этом случае используется меньшее число полей, например 3-tuple (2 адреса и протокол IP) и даже 2-tuple (вест трафик между парой адресов IP). Плоскость данных DetNet IP позволяет также сопоставление с полем IPv6 Flow Label [RFC8200].

Пакеты, не относящиеся к DetNet, и пакеты DetNet IP имеют одинаковый формат заголовка пакета при передаче. В общем случае используемые для идентификации потока поля пересылаются без изменений, однако стандартные изменения поля DSCP [RFC2474] не исключены.

Агрегирование потоков DetNet может быть реализовано за счет применения шаблонов, масок, списков, префиксов и диапазонов. Туннели IP также могут служить для поддержки агрегирования. В таких случаях предполагается, что понимающие DetNet промежуточные узлы будут обеспечивать услуги DetNet для агрегата с помощью механизмов выделения ресурсов и контроля перегрузок.

Конкретные процедуры, которые требуется реализовать на узле DetNet, поддерживающем этот документ, описаны в разделе 5. Плоскость контроллера DetNet (Controller Plane) [RFC8655] отвечает за обеспечение каждого узла информацией, требуемой для идентификации и обслуживания каждого потока DetNet.

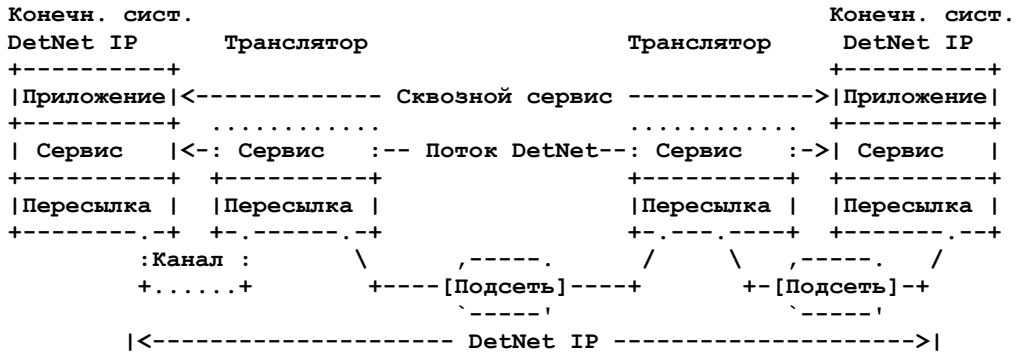

Рисунок 1. Простая сеть IP с поддержкой DetNet.

На рисунке 1 показана сеть IP с поддержкой DetNet. Поддерживающие DetNet конечные системы создают инкапсулированный в IP трафик, который идентифицируется в домене DetNet как поток DetNet на основе данных из заголовка IP. Трансляторам понятны требования к пересылке потока DetNet и они обеспечивают выделение ресурсов, интерфейса и узла для выполнения требований сервиса DetNet. Линии из точек вокруг блока «Сервис» на трансляторе показывают, что транзитные маршрутизаторы понимают сервис DetNet, но не реализуют функций подуровня сервиса DetNet, таких как PREOF. Следует отметить, что подсети могут представлять TSN, сеть MPLS или иную технологию, которая может передавать трафик DetNet IP.

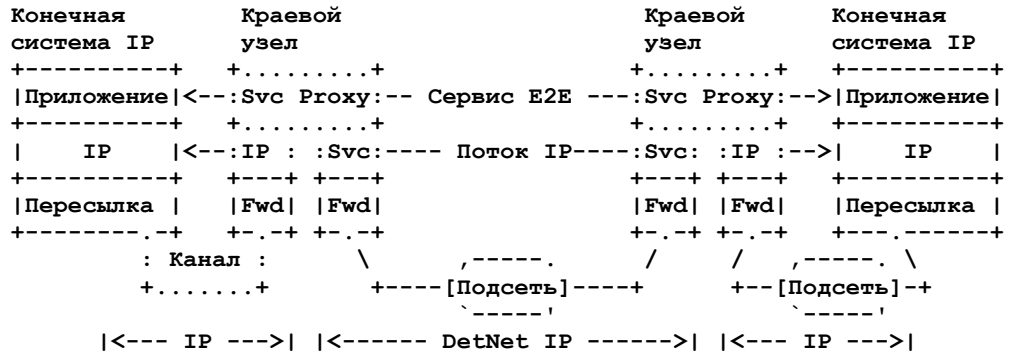

Рисунок 2. Конечные системы без поддержки DetNet в домене DetNet IP.

На рисунке 2 приведен вариант рисунка 1, где конечные системы не понимают DetNet. В этом случае краевые узлы на границе домена DetNet обеспечивают посреднические услуги DetNet для приложений конечных точек путем создания и

[1]Encapsulating Security Payload - инкапсуляция данных защиты.

завершения сервиса DetNet для потоков IP от приложений. Для идентификации потоков DetNet может служить информация из заголовков или подход, описанный в параграфе 4.4. Агрегирование потоков DetNet.

Отметим, что конечные системы IP DetNet могут взаимодействовать через сеть DetNet IP с конечными системами IP.

Поскольку не относящиеся к DetNet пакеты и пакеты DetNet IP имеют одинаковый формат заголовков при передаче, с точки зрения плоскости данных единственным различием между ними служит связанная с потоками DetNet информация каждого узла DetNet, которая определяет связанные с потоком характеристики и требуемое поведение пересылки. Как показано выше, краевые узлы поддерживают функцию Service Proxy, которая связывает один или несколько потоков IP с подходящей информацией о потоках DetNet и обеспечивает для потоков корректную обработку внутри домена.

Отметим, что работа конечных систем IEEE 802.1 TSN через сети IP с поддержкой DetNet не описана в этом документе. Описание TSN over MPLS приведено в [DetNet-TSN-over-MPLS].

4. Плоскость данных DetNet IP

В этом разделе рассматриваются вопросы, связанные с предоставлением услуг DetNet потокам, идентифицированным на основании данных из заголовков.

4.1. Конечные точки

Потоки данных, требующие сервиса DetNet, создаются и завершаются в конечных точках. Этот документ имеет дело лишь с конечными системами IP. Протокол, используемый конечной системой IP, зависит от приложения и конечная система взаимодействует с другой конечной системой (партнером). DetNet использует идентификацию потоков IP на основе кортежей 6-tuple, поэтому DetNet нужно знать не только формат заголовка IP, но и значение следующего протокола в пакете IP (5.1.1.3. Поля IPv4 Protocol и IPv6 Next Header).

Для не знающих DetNet конечных систем IP внутри домена DetNet требуются посреднические функции уровня сервиса.

Когда конечные системы IP понимают DetNet, посреднические функции на уровне приложений или сервиса не нужны в домене DetNet. Конечные системы должны гарантировать поддержку требований к сервису DetNet при обработке пакетов, связанных с потоком DetNet. При отправке пакетов это означает подходящую формовку передаваемого трафика и его обработку в подключенной сети (см. параграфы 4.3.2 и 4.2). При получении это означает требование наличия подходящих локальных ресурсов, например буферов для приема и обработки пакетов потока DetNet.

Важным дополнительным вопросом для понимающих DetNet конечных систем является предотвращение фрагментации IP. Полная идентификация потоков на основе 6-tuple невозможна для фрагментов IP, поскольку они не включают транспортных заголовков и сведений о портах. Поэтому для приложений и/или конечных систем важно использовать размер пакетов IP, позволяющий избежать фрагментации в сети при передаче потоков DetNet. Максимальный размер пакетов можно узнать с помощью Path MTU Discovery [RFC1191] [RFC8201] или от плоскости контроллера. Отметим, что механизм Path MTU Discovery основан на пакетах ICMP, которые могут идти по иному пути, нежели отдельный поток DetNet.

Для максимального использования имеющихся механизмов понимающим DetNet приложениям и конечным системам **не следует** смешивать трафик DetNet с прочим трафиком в рамках одного кортежа 5-tuple.

4.2. Домен DetNet

Как правило, от домена DetNet IP требуется поддержка пересылки любого потока DetNet, указанного кортежем IP 6-tuple. Иное поведение будет ограничивать число идентификаторов потоков 6-tuple, которые могут применять конечные системы. С практической точки зрения это означает, что все узлы на сквозном пути потоков DetNet должны согласовать применяемые для идентификации потоков поля. Возможным следствием отсутствия такого согласия будут помехи, создаваемые одними потоками для других, и неожиданная обработка трафика.

С точки зрения типа подключения возможны два варианта:

1. подключение DN - конечная система напрямую соединяется с краевым узлом или находится за пределами подсети (ES1 и ES2 на рисунке 3);
2. интеграция с DN - конечная система является частью домена DetNet (ES3 на рисунке 3).

Конечные системы L3 (IP) могут применять любой из этих вариантов подключения. Домен DetNet позволяет взаимодействовать любым конечным системам с одинаковым форматом инкапсуляции независимо от типа подключения и свойств DetNet. Подключенные к DN конечные системы не знают о домене DetNet и его формате инкапсуляции. Примеры подключений даны на рисунке 3.

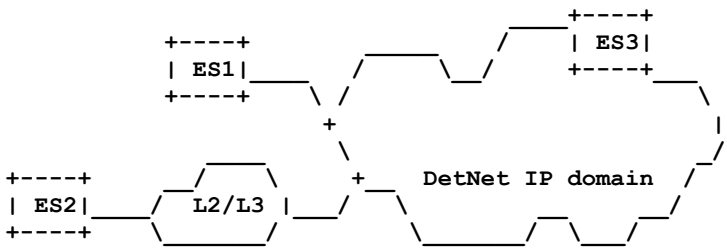

Рисунок 3. Типы подключения конечных систем L3.

Внутри домена DetNet маршрутизаторы IP с поддержкой DetNet соединены между собой каналами и подсетями для поддержки сквозной доставки потоков DetNet. С точки зрения архитектуры DetNet эти маршрутизаторы являются ретрансляторами DetNet, поскольку они должны понимать сервис DetNet. Такие маршрутизаторы идентифицируют потоки DetNet на основе кортежей IP 6-tuple и обеспечивают обработку, требуемую сервисом DetNet, на самом узле и в подключенных к нему подсетях.

Это решение обеспечивает сквозные функции DetNet, но не делает этого на уровне соединений или подсетей. Защита от перегрузок, контроль задержки и выделение ресурсов (очереди, правила, формовка) поддерживаются с использованием механизмов базового канала или подсети. Однако сквозная защита сервиса (PRF и PEF) не обеспечивается на уровне DetNet и должна предоставляться на уровне соединения (базовый канал L2) и подсети.

Поток сервиса DetNet отображается на ресурсы канала или подсети с использованием возможностей базовых систем. Это предполагает, что каждый узел пути, понимающий DetNet, заглядывает в пересылаемый поток сервиса DetNet и использует, например, кортежи 6-tuple для создания требуемого на узле отображения.

Как отмечено выше, защита должна быть организована в соединениях и подсетях независимо с использованием зависящих от домена механизмов. Это связано с отсутствием унифицированной информации о сквозном упорядочении, которую можно было бы применять на промежуточных узлах. Поэтому защита сервиса (если она включена) может обеспечиваться лишь внутри подсетей. Это показано в варианте с 3 подсетями на рисунке 4, где каждая подсеть может обеспечивать защиту сервиса между своими границами. R и E на рисунке указывают точки репликации и устранения дубликатов в подсети.

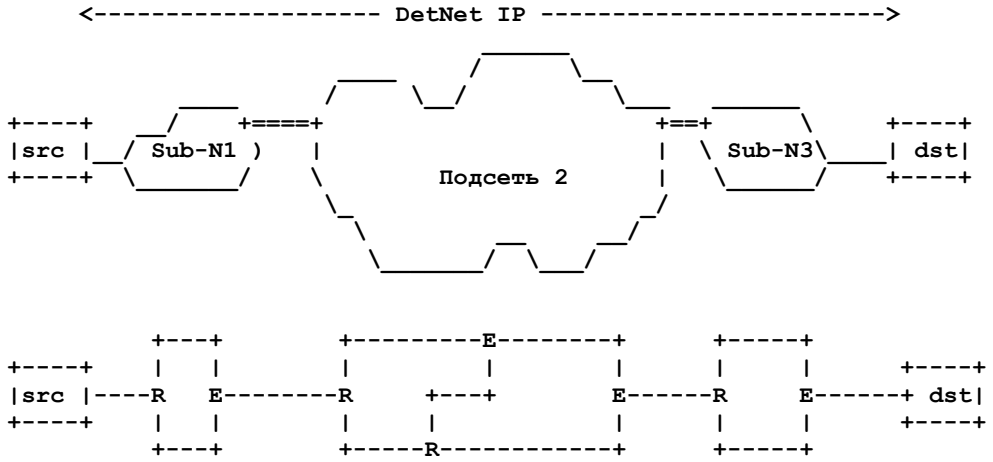

Рисунок 4. Репликация и исключение в подсетях для DetNet IP.

Если желательна сквозная защита сервиса, ее можно реализовать, например, с помощью конечных систем DetNet, используя транспортные (L4) или прикладные протоколы, однако это выходит за рамки документа.

Отметим, что отсутствие смешения трафика DetNet с прочим в рамках одного кортежа 5-tuple, как указано выше, позволяет упростить фильтры 5-tuple, применяемые на краях сети DetNet для предотвращения выхода трафика DetNet, не реагирующего на перегрузки, за пределы домена DetNet.

4.3. Подуровень пересылки

4.3.1. Класс обслуживания

Класс обслуживания (CoS) для потоков DetNet передаваемых в пакетах IPv4 и IPv6, обеспечивается стандартным полем DSCP [RFC2474] и связанными с ним механизмами.

Дополнительный вопрос для узлов DetNet, поддерживающих услуги CoS, заключается в том, что они должны обеспечить отсутствие влияния классов обслуживания CoS на механизмы защиты от перегрузки и контроля задержек, применяемые для DetNet QoS. Это похоже на требование к маршрутизаторам MPLS LSR[1], где CoS LSP не должны влиять на ресурсы, выделенные для TE LSP [RFC3473].

4.3.2. Качество обслуживания

Качество обслуживания (QoS) для потоков сервиса DetNet, передаваемых по IP, должно обеспечиваться локально знающими о DetNet узлами и маршрутизаторами, поддерживающими потоки DetNet. Поддержка зависит от базовых сетевых уровней, таких как 802.1 TSN. Использование внутренних механизмов управления трафиком на узлах для обеспечения QoS потокам DetNet с инкапсуляцией IP выходит за рамки этого документа. С точки зрения инкапсуляции кортеж 6-tuple (5-tuple и DSCP) и, возможно, метка потока однозначно указывает поток DetNet IP.

Пакеты, идентифицированные как часть потока DetNet IP, но не относящиеся к выполненному резервированию, могут нарушать QoS для корректно зарезервированных потоков DetNet, используя выделенные тем ресурсы. Поэтому узлы сети DetNet **должны** предотвращать использование такими потоками ресурсов, не выделенных DetNet. Имеется много методов, которые реализация может использовать для защиты обслуживания зарезервированных потоков DetNet, включая перечисленные ниже.

- Обработка пакетов, связанных с незавершенным резервированием, как не относящихся к DetNet.
- Отбрасывание пакетов, связанных с незавершенным резервированием.
- Перемаркировка пакетов, связанных с незавершенным резервированием, которая может быть реализована изменением поля DSCP с установкой значения, в соответствии с которым пакет не будет совпадать с зарезервированным потоком DetNet IP.

4.3.3. Выбор пути

Хотя алгоритмы и механизмы выбора пути выходят за рамки определения плоскости данных DetNet, важно подчеркнуть влияние идентификации потоков DetNet IP на выбор пути и следующего интервала. Как отмечено выше,

[1]Label Switching Router - маршрутизатор с коммутацией по меткам.

плоскость данных DetNet IP идентифицирует потоки по данным из заголовков (6-tuple), а также (необязательным) меткам потоков. Обычно DetNet позволяет обрабатывать трафик и выбирать следующий интервал на уровне потока.

При пересылке не относящихся к DetNet пакетов IP обычно предполагается такая же последовательность next hop, т. е. для данного кортежа 5-tuple (в некоторых случаях, например, [RFC5120] — 6-tuple) будет использован тот же путь. Использование разных next hop для разных 5-tuples не имеет особого значения для приложений, понимающих DetNet.

Следует соблюдать осторожность при использовании разных next hop для одного кортежа 5-tuple. Как отмечено в [RFC7657], возможно неожиданное поведение когда в потоке приложения с данным 5-tuple происходит нарушение порядка в результате отправки по разным путям. Требуется понимать роль приложения и транспортного протокола при использовании разных next hop для одного кортежа 5-tuple, если это предполагается. Отметим, что это лишь косвенно влияет на выбор путей для потоков DetNet и данный документ.

4.4. Агрегирование потоков DetNet

Как описано в [RFC8938], возможность объединять отдельные потоки и связанное с этим управление ресурсами является важным способом повышения уровня расширяемости за счет уменьшения числа состояний на интервал пересылки. Агрегирование в плоскости данных DetNet IP может происходить на одном узле, когда тот поддерживает состояния для агрегированных и индивидуальных потоков. Это также может выполняться между узлами, когда один поддерживает лишь состояние для агрегата, а другой - для всех или части объединенных потоков. В любом случае функции управления и поддержки агрегирования должны обеспечивать адекватную настройку и выделение ресурсов для комбинации потребностей в обслуживании отдельных потоков. Поскольку DetNet заботится о задержках и их вариациях, требуется учитывать не только пропускную способность.

С точки зрения одного узла агрегирование потоков IP влияет на идентификацию потоков и выделение ресурсов в плоскости данных DetNet IP. Как обсуждалось выше, для идентификации потока IP служат кортежи IP 6-tuple. Потоки DetNet IP могут объединяться с использованием любого из полей 6-tuple, а также метки потока. Использование префиксов, списков и диапазонов значений позволяет узлу DetNet идентифицировать агрегированные потоки DetNet. С точки зрения выделения ресурсов узлы DetNet должны предоставлять обслуживание на уровне агрегированного потока, а не его компонентов.

Плоскость контроллера DetNet отвечает за корректное использование механизмов агрегирования. Это включает обеспечение совместимости (или существенного сходства) агрегируемых потоков по характеристикам QoS и CoS (см. параграф 4.3.2), а также гарантии выполнения в рамках агрегата всех требований на уровне отдельных потоков (раздел 5.3).

Плоскость контроллера DetNet **должна** гарантировать, что трафик DetNet, не реагирующий на перегрузки, не пересылается за пределы домена DetNet.

4.5. Двухсторонний трафик

Хотя плоскость данных DetNet IP должна поддерживать двухсторонние потоки DetNet, в ней не предусмотрено специальных двухсторонних функций. Особый случай двухсторонних потоков DetNet с общей маршрутизацией представлен лишь на уровнях управления и поддержки без какой-либо специальной информации или поддержки в плоскости данных DetNet. Общая судьба и привязка или общая маршрутизация двухсторонних потоков могут поддерживаться на уровне управления.

Механизмы управления и администрирования должны поддерживать двухсторонние потоки, но спецификация таких механизмов выходит за рамки документа. Пример решения для плоскости управления MPLS можно найти в [RFC7551].

5. Процедуры плоскости данных DetNet IP

В этом разделе описаны процедуры плоскости данных DetNet IP, которые разделены на три категории - идентификация потоков, пересылка и обработка трафика. Идентификация потоков включает процедуры, относящиеся к сопоставлению заголовков IP и вышележащего протокола с данными потока DetNet (состояние) и требованиями сервиса. Иногда идентификацию потоков называют классификацией трафика (например, в [RFC5777]). Пересылка включает процедуры, относящиеся к выбору следующего интервала (next-hop) и доставке пакетов. Обработка трафика включает процедуры, связанные с предоставлением потокам DetNet требуемого обслуживания.

Процедуры организации и работы плоскости данных DetNet IP вносят требования к системам управления и поддержки для потоков DetNet, также упоминаемые в этом разделе. В частности, раздел указывает множество информационных элементов, которые должны поддерживаться узлом DetNet на интерфейсах управления и поддержки. Конкретные механизмы такой поддержки выходят за рамки этого документа и приведена лишь сводка требований к информации, связанной с управлением и поддержкой. В сводке не задаются уровни требований, поскольку она относится к будущим механизмам, таким как определяемые моделями YANG [DetNet-YANG].

5.1. Процедуры идентификации потоков DetNet IP

Для идентификации потоков DetNet применяется информация из заголовков IP и вышележащего протокола. Все реализации DetNet, соответствующие этому документу, **должны** идентифицировать отдельные потоки DetNet на основе данных, указанных в этом разделе. Отметим, что в будущем могут быть заданы дополнительные требования к идентификации потоков, например, для поддержки иных протоколов вышележащего уровня.

Данные конфигурации и управления, используемые для идентификации отдельного потока DetNet, **должны** упорядочиваться реализацией. Реализации **должны** поддерживать фиксированный порядок для идентификации потоков, а также **должны** идентифицировать (распознавать) поток DetNet по первому набору совпадающих данных.

Реализации этого документа **должны** поддерживать идентификацию потоков DetNet при работе на конечных системах, ретрансляторах и краевых узлах DetNet.

5.1.1. Данные заголовка IP

Реализации этого документа **должны** поддерживать идентификацию потоков DetNet на основе заголовков IP. Заголовок IPv4 определен в [RFC0791], IPv6 - в [RFC8200].

5.1.1.1. Поле адреса отправителя

Реализации этого документа **должны** поддерживать идентификацию потоков DetNet на основе поля Source Address[1] в пакете IP. Реализациям **следует** поддерживать для этого поля сопоставление по наибольшей длине префикса (см. [RFC1812] и [RFC7608]). Отметим, что сопоставление с префиксом размера 0 означает игнорирование поля.

5.1.1.2. Поле адреса получателя

Реализации этого документа **должны** поддерживать идентификацию потоков DetNet на основе поля Destination Address в пакете IP. Реализациям **следует** поддерживать для этого поля сопоставление по наибольшей длине префикса (см. [RFC1812] и [RFC7608]). Отметим, что сопоставление с префиксом размера 0 означает игнорирование поля.

5.1.1.3. Поля IPv4 Protocol и IPv6 Next Header

Реализации этого документа **должны** поддерживать идентификацию потоков DetNet на основе поля IPv4 Protocol при обработке пакетов IPv4 и поля IPv6 Next Header при обработке пакетов IPv6. Это включает значение следующего протокола, определенное в параграфе 5.1.2, и другие значения, в том числе 0. Реализациям **следует** поддерживать возможность игнорировать это поле для конкретного потока DetNet.

5.1.1.4. Поля IPv4 Type of Service и IPv6 Traffic Class

Эти поля служат для поддержки дифференцированного обслуживания [RFC2474] [RFC2475]. Реализации этого документа **должны** поддерживать идентификацию потоков DetNet на основе поля DSCP в поле IPv4 Type of Service для пакетов IPv4 и поля DSCP в поле IPv6 Traffic Class для пакетов IPv6. Реализации **должны** поддерживать сопоставление полей DSCP со списком возможных значений при идентификации конкретного потока DetNet. Реализациям **следует** поддерживать возможность игнорировать это поле для конкретного потока DetNet.

5.1.1.5. Поле IPv6 Flow Label

Реализациям этого документа **следует** поддерживать идентификацию потоков DetNet на основе поля IPv6 Flow Label. Поддерживающие это реализации **должны** разрешать возможность игнорировать поле для конкретного потока DetNet. При использовании поля для идентификации конкретного потока DetNet реализация **может** исключить поле IPv6 Next Header и данные следующего заголовка из процесса идентификации потока DetNet.

5.1.2. Другая информация из заголовков

Реализации этого документа **должны** поддерживать идентификацию потоков DetNet на основе информации из заголовков, указанной в этом разделе. Определена поддержка для потоков TCP, UDP, ICMP и IPsec, а в будущем список протоколов может быть расширен.

5.1.2.1. TCP и UDP

Идентификация потоков DetNet для TCP [RFC0793] и UDP [RFC0768] выполняется на основе полей Source Port и Destination Port в заголовке каждого пакета. Эти поля используют одинаковые формате и для них применяются общие процедуры идентификации потоков DetNet.

Определенные в этом параграфе правила применимы только к полям IPv4 Protocol и IPv6 Next Header, содержащим определенные IANA значения для UDP и TCP.

5.1.2.1.1. Поле Source Port

Реализации этого документа **должны** поддерживать идентификацию потоков DetNet на основе поля Source Port в заголовках TCP и UDP. Реализации **должны** поддерживать идентификацию потоков на основе точного совпадения значений, а также **следует** поддерживать сопоставление с диапазоном значений. Реализации **должны** обеспечивать возможность игнорировать это поле для конкретного потока DetNet.

5.1.2.1.2. Поле Destination Port

Реализации этого документа **должны** поддерживать идентификацию потоков DetNet на основе поля Destination Port в заголовках TCP и UDP. Реализации **должны** поддерживать идентификацию потоков на основе точного совпадения значений, а также **следует** поддерживать сопоставление с диапазоном значений. Реализации **должны** обеспечивать возможность игнорировать это поле для конкретного потока DetNet.

5.1.2.2. ICMP

Идентификация потоков DetNet для ICMP [RFC0792] обеспечивается на основе номера протокола в заголовке IP. Отметим, что тип ICMP не применяется для идентификации потоков.

5.1.2.3. IPsec AH и ESP

Протоколы IPsec Authentication Header (AH) [RFC4302] и Encapsulating Security Payload (ESP) [RFC4303] используют общий формат для поля Security Parameters Index (SPI) field. Реализации **должны** поддерживать идентификацию на основе точного совпадения значений. Реализациям **следует** поддерживать возможность игнорировать это поле для конкретного потока DetNet.

Определенные в этом параграфе правила применимы только к полям IPv4 Protocol и IPv6 Next Header, содержащим определенные IANA значения для AH и ESP.

[1]Отметим, что сравниваться могут любые адреса IP, включая групповые адреса получателей.

5.2. Процедуры пересылки

Общие требования к узлам IP заданы в [RFC1122], [RFC1812], [RFC8504] и данный документ их не меняет. DetNet влияет на типичный процесс выбора следующего этапа пересылки (next-hop). В частности, реализациям этого документа **нужно** использовать данные управления и поддержки для выборе одного или нескольких выходных интерфейсов в качестве следующего этапа пересылки пакетов, связанных с потоком DetNet. Конкретные данные управления и поддержки будут определены в будущих документах, например, [DetNet-YANG].

Использование множества путей или каналов (например, ECMP) для поддержки одного потока DetNet **нерекомендуется**. ECMP **можно** использовать с не относящимися к DetNet потоками в домене DetNet.

Сказанное выше применимо к функциям управления и поддержки, которые будут определены для реализации этого требования, например, [DetNet-YANG].

5.3. Процедуры обработки трафика DetNet IP

Реализации этого документа должны обеспечивать для потоков DetNet обработку трафика, предусмотренную конфигурацией или плоскостью контроллера (например, через [DetNet-YANG]). Общие сведения о сервисе DetNet можно найти в [DetNet-Flow-Info]. Типичные механизмы обеспечения разной обработки для разных потоков включают выделение системных ресурсов (таких как очереди и буферы) и предоставление соответствующих параметров (формовка и правила). Поддержка также может быть обеспечена за счет базовой сетевой технологии, такой как MPLS [DetNet-IP-over-MPLS] или IEEE 802.1 TSN [DetNet-IP-over-TSN]. Другие механизмы, кроме применяемых в случае TSN, выходят за рамки этого документа.

6. Поддержка и управление

Ниже приведена сводка данных, требуемых для идентификации индивидуальных и агрегированных потоков DetNet.

- Поле IPv4 или IPv6 Source Address.
- Размер префикса адреса отправителя IPv4 или IPv6, где значение 0 указывает игнорирование поля Source Address.
- Поле IPv4 или IPv6 Destination Address.
- Размер префикса адреса получателя IPv4 или IPv6, где значение 0 указывает игнорирование поля Destination Address.
- Поле IPv4 Protocol. Разрешен ограниченный набор значений, желательна возможность игнорировать поле.
- Поле IPv6 Next Header. Разрешен ограниченный набор значений, желательна возможность игнорировать поле.
- Для полей IPv4 Type of Service и IPv6 Traffic Class:
  - используется ли поле DSCP для классификации потока (не обязательно);
  - при использовании DSCP идентификационные данные (для этого потока) включают список применяемых потоком значение DSCP.
- Поле IPv6 Flow Label (не обязательно). При использовании этого поля оно может служить заменой сопоставления с полем Next Header.
- Порт отправителя TCP и UDP Source Port. Требуется поддержка точного и шаблонного совпадения, возможно сопоставление с диапазоном.
- Порт отправителя TCP и UDP Destination Port. Требуется поддержка точного и шаблонного совпадения, возможно сопоставление с диапазоном.
- Поле IPsec Header SPI. Требуется поддержка точного совпадения и рекомендуется поддерживать шаблоны.
- Для конечных систем - (необязательный) максимальный размер пакетов IP, который следует применять для данного исходящего потока DetNet IP.

Эта информация **должна** предоставляться на уровне потока DetNet путем настройки, например, через плоскость контроллера или систему управления.

Реализация **должна** поддерживать упорядочение набора информации, служащей для идентификации отдельного потока DetNet. Это может применяться, например, для предоставления услуг DetNet конкретному потоку UDP с определенной комбинацией Source Port и Destination Port с одновременным предоставлением других услуг агрегату из всех прочих потоков с таким же значением UDP Destination Port.

Плоскость контроллера DetNet отвечает за предоставление данных идентификации потоков и относящихся к потоку ресурсов, требуемых для обработки потока в соответствии с его потребностями. Это применимо к индивидуальным и агрегированным потокам.

7. Вопросы безопасности

Вопросы безопасности DetNet подробно перечислены в [DetNet-Security], а более общее рассмотрение их приведено в [RFC8655]. В этом разделе рассматриваются вопросы безопасности, специфичные для плоскости данных DetNet IP.

Уникальными для DetNet являются аспекы безопасности, связанные с обеспечением конкретных требований QoS для DetNet, предназначенных в первую очередь для доставки пакетов потока с минимально возможными потерями и ограниченной сквозной задержкой. Достижение малых потерь и ограниченной задержки может стать невозможным перед лицом серьезного противника, такого как указан в модели угроз Internet из BCP 72 [RFC3552], который может произвольно отбрасывать или задерживать любой или весь трафик. Чтобы представить значимые вопросы безопасности, здесь рассматривается не столь сильный противник, который не может контролировать физические каналы домена DetNet, но способен управлять узлом сети в домене DetNet.

Основным вопросом для плоскости данных DetNet является поддержка целостности и предоставление услуг DetNet, проходящих через сеть DetNet. Поскольку в плоскости данных DetNet IP нет специфичных для DetNet полей, целостность и конфиденциальность потоков приложений могут быть защищены любыми средствами, предоставляемыми базовой технологией. Например, может применяться шифрование, такое как обеспечиваемое IPsec [RFC4301] для потоков IP или базовой сеть с использованием MACsec [IEEE802.1AE-2018] при передаче IP в потоках Ethernet (L2).

С точки зрения плоскости данных этот документ не меняет и не добавляет какой-либо информации в заголовках.

На уровне управления и поддержки потоки DetNet идентифицируются индивидуально, что может позволить атакующим плоскость контроллера получить дополнительные сведения о потоках данных (по сравнению с плоскостью контроллера, где нет идентификации на уровне потоков). Это унаследованное свойство DetNet влияет на свойства защиты и должно учитываться при решении вопроса об использовании DetNet в конкретном случае.

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 или на краю домена IEEE 802.1 TSN. 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.

8. Взаимодействие с IANA

Этот документ не требует действий со стороны IANA.

9. Литература

9.1. Нормативные документы

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, DOI 10.17487/RFC0768, August 1980, <https://www.rfc-editor.org/info/rfc768>.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, DOI 10.17487/RFC0792, September 1981, <https://www.rfc-editor.org/info/rfc792>.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <https://www.rfc-editor.org/info/rfc793>.

[RFC1812] Baker, F., Ed., "Requirements for IP Version 4 Routers", RFC 1812, DOI 10.17487/RFC1812, June 1995, <https://www.rfc-editor.org/info/rfc1812>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <https://www.rfc-editor.org/info/rfc2474>.

[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>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/info/rfc4302>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC7608] Boucadair, M., Petrescu, A., and F. Baker, "IPv6 Prefix Length Recommendation for Forwarding", BCP 198, RFC 7608, DOI 10.17487/RFC7608, July 2015, <https://www.rfc-editor.org/info/rfc7608>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[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>.

[RFC8938] Varga, B., Ed., Farkas, J., Berger, L., Malis, A., and S. Bryant, "Deterministic Networking (DetNet) Data Plane Framework", RFC 8938, DOI 10.17487/RFC8938, November 2020, <https://www.rfc-editor.org/rfc/rfc8938>.

9.2. 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>.

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

[DetNet-IP-over-MPLS] Varga, B., Ed., Berger, L., Fedyk, D., Bryant, S., and J. Korhonen, "DetNet Data Plane: IP over MPLS", Work in Progress, Internet-Draft, draft-ietf-detnet-ip-over-mpls-09, 11 October 2020, <https://tools.ietf.org/html/draft-ietf-detnet-ip-over-mpls-09>.

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

[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-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>.

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

[DetNet-YANG] Geng, X., Chen, M., Ryoo, Y., Fedyk, D., Rahman, R., and Z. Li, "Deterministic Networking (DetNet) Configuration YANG Model", Work in Progress, Internet-Draft, draft-ietf-detnet-yang-09, 16 November 2020, <https://tools.ietf.org/html/draft-ietf-detnet-yang-09>.

[IEEE802.1AE-2018] IEEE, "IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security", IEEE 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/>.

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <https://www.rfc-editor.org/info/rfc1122>.

[RFC1191] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, DOI 10.17487/RFC1191, November 1990, <https://www.rfc-editor.org/info/rfc1191>.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, DOI 10.17487/RFC2475, December 1998, <https://www.rfc-editor.org/info/rfc2475>.

[RFC3290] Bernet, Y., Blake, S., Grossman, D., and A. Smith, "An Informal Management Model for Diffserv Routers", RFC 3290, DOI 10.17487/RFC3290, May 2002, <https://www.rfc-editor.org/info/rfc3290>.

[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>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[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>.

[RFC5120] Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, DOI 10.17487/RFC5120, February 2008, <https://www.rfc-editor.org/info/rfc5120>.

[RFC5777] Korhonen, J., Tschofenig, H., Arumaithurai, M., Jones, M., Ed., and A. Lior, "Traffic Classification and Quality of Service (QoS) Attributes for Diameter", RFC 5777, DOI 10.17487/RFC5777, February 2010, <https://www.rfc-editor.org/info/rfc5777>.

[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>.

[RFC8201] McCann, J., Deering, S., Mogul, J., and R. Hinden, Ed., "Path MTU Discovery for IP version 6", STD 87, RFC 8201, DOI 10.17487/RFC8201, July 2017, <https://www.rfc-editor.org/info/rfc8201>.

[RFC8504] Chown, T., Loughney, J., and T. Winters, "IPv6 Node Requirements", BCP 220, RFC 8504, DOI 10.17487/RFC8504, January 2019, <https://www.rfc-editor.org/info/rfc8504>.

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 и Carlos J. Bernardos за их вклад в работу. David Black был техническим советником рабочей группы DetNet во время создания этого документа и предоставил много полезных замечаний. Комментарии от IESG предоставили Murray Kucherawy, Roman Danyliw, Alvaro Retana, Benjamin Kaduk, Rob Wilton и Érik Vyncke.

Участники работы

Редактор документа выражает благодарность и признательность людям, внесшим важный вклад в разработку этого документа и по сути являющимся соавторами.

Jouni Korhonen

Email: jouni.nospam@gmail.com

Andrew G. Malis

Malis Consulting

Email: agmalis@gmail.com

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

Don Fedyk

LabN Consulting, L.L.C.

Email: dfedyk@labn.net

Stewart Bryant

Futurewei Technologies

Email: sb@stewartbryant.com

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru