

Internet Engineering Task Force (IETF)
Request for Comments: 8468
Updates: 2330
Category: Informational
ISSN: 2070-1721

A. Morton
AT&T Labs
J. Fabini
TU Wien
N. Elkins
Inside Products, Inc.
M. Ackermann
Blue Cross Blue Shield of Michigan
V. Hegde
Consultant
November 2018

IPv4, IPv6, and IPv4-IPv6 Coexistence: Updates for the IP Performance Metrics (IPPM) Framework

Обновление схемы измерения производительности IP (IPPM) для IPv4, IPv6 и сосуществования IPv4-IPv6

Аннотация

Этот документ обновляет схему показателей производительности IP (IP Performance Metrics или IPPM), определённую в RFC 2330, рассматривая дополнительные методы измерений и тесты. Обновлено определение стандартных пакетов для включения IPv6, отменено определение минимального пакета IP, дополнены аспекты различий, называемые Type-P, для тестовых пакетов из RFC 2330. Документ указывает, что сосуществование IPv4 и IPv6 может осложнять измерения в рамках IPPM. Примеры использования включают, помимо прочего, трансляцию IPv4-IPv6, NAT, инкапсуляцию. Рассмотрено сжатие заголовков IPv6 и использование в сетях 6LoWPAN¹ с исключением этих вариантов из оценки для стандартизованных пакетов.

Статус документа

Документ не относится к категории Internet Standards Track и публикуется лишь для информации.

Документ является результатом работы IETF² и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG³. Дополнительную информацию о стандартах Internet можно найти в разделе 2 RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <https://www.rfc-editor.org/info/rfc8468>.

Авторские права

Авторские права (Copyright (c) 2018) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

Документ может содержать материалы из IETF Document или IETF Contribution, опубликованных или публично доступных до 10 ноября 2008 года. Лица, контролирующие авторские права на некоторые из таких документов, могли не предоставить IETF Trust права разрешать внесение изменений в такие документы за рамками процессов IETF Standards. Без получения соответствующего разрешения от лиц, контролирующих авторские права этот документ не может быть изменён вне рамок процесса IETF Standards, не могут также создаваться производные документы за рамками процесса IETF Standards за исключением форматирования документа для публикации или перевода с английского языка на другие языки.

Оглавление

1. Введение.....	2
2. Уровни требований.....	2
3. Область действия.....	2
4. Пакеты Type-P.....	2
5. Пакеты стандартного формата.....	3
6. NAT, переход IPv4-IPv6 и методы сжатия.....	4
7. Вопросы безопасности.....	4
8. Взаимодействие с IANA.....	5
9. Литература.....	5
9.1. Нормативные документы.....	5
9.2. Дополнительная литература.....	6

¹IPv6 over Low-Power Wireless Area Networks - сети IPv6 на основе беспроводных каналов со слабым питанием.

²Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

³Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

Благодарности.....	6
Адреса авторов.....	6

1. Введение

Рабочая группа IETF IPPM (IP Performance Metrics) описала схему для разработки показателей в [RFC2330]. Эта схема проверена временем и позволила разработать множество фундаментальных показателей. Схема была обновлена в части состава показателей [RFC5835] и в нескольких областях, связанных с активными измерениями потоков в современных сетях с реактивными свойствами [RFC7312].

В схеме IPPM [RFC2330] отмечено (раздел 13), что многие свойства пакетов IP могут влиять на обработку пакета в процессе его передачи через сеть.

В разделе 15 [RFC2330] определён «пакет стандартного формата» (standard-formed). Однако это определение не было расширено для пакетов IPv6, хотя авторы [RFC2330] явно указали необходимость такого обновления в разделе 15: «с полем версии 4 (позднее будет описан случай для версии 6)».

В частности, заголовки расширения IPv6 и протоколы, использующие сжатие заголовков IPv6, применяются все шире. Этот документ содержит обновления исходного определения [RFC2330].

2. 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. Область действия

Целью этого документа является расширение сферы действия IPPM за счёт включения IPv6, указания дополнительных параметров тестовых пакетов и включение этого в схему IPPM.

Цель состоит в обновлении ключевых разделов [RFC2330] с добавлением соображений, которые помогут в разработке новых методов измерения для современных сетей IP. В частности, документ расширяет набор примеров Type-P из раздела 13 в [RFC2330] и определение пакетов стандартного формата (раздел 15 в [RFC2330]) включением параметров заголовка IPv6 и других свойств.

Другие аспекты [RFC2330], которые могут быть обновлены или дополнены, оставлены на будущее. К таким вопросам относятся пассивные и гибридные измерения.

4. Пакеты Type-P

Фундаментальное свойство многих показателей Internet заключается в том, что измеряемое значение зависит от параметров пакетов IP, применяемых для измерения. Факторы влияния включают поля заголовков IP и их значения, а также заголовки вышележащего протокола и их значения. Например, для метрики связности IP значения будут зависеть от использования общеизвестных портов TCP или незарезервированных портов UDP, наличия ошибок в контрольных суммах IPv4, значение TTL или Hop Limit (например, 16). В некоторых случаях различия будут диктовать специальную обработку пакетов на промежуточных узлах и оконечных системах, например, при использовании Diffserv [RFC2474], явного уведомления о перегрузке (Explicit Congestion Notification или ECN) [RFC3168], Router Alert [RFC6398], расширений Hop-by-Hop [RFC7045], меток потоков (Flow Label) [RFC6437], а также наличия в пути межсетевых экранов или резервирования RSVP.

Из-за таких различий введено понятие пакетов Type-P, который в некоторых вариантах контекста P определяется явно (т. е. тип пакета задаётся точно), частично (например, в размере данных B октетах) или остаётся базовым. Таким образом, можно говорить о базовой связности IP-Type-P-connectivity или более конкретно о IP-port-HTTP-connectivity. Некоторые показатели и методики можно задать с использованием базовых определений Type-P, которые конкретизируются при выполнении фактических измерений.

Когда значение показателя зависит от типа вовлечённых в тест пакетов, имя параметра будет включать конкретный тип или фразу вида Type-P. Таким образом определяется не метрика IP-connectivity, а метрика IP-Type-P-connectivity и/или, например, IP-port-HTTP-connectivity. Такое соглашение об именовании служит важным напоминанием о необходимости точно учитывать тип используемого для измерений трафика.

Если установлено, что сведения, определяющие Type-P у отправителя (Source), изменились на стороне получателя (Destination) или в точке измерения между отправителем и получателем, как в [RFC5644], изменённые значения **должны** быть указаны в отчёте о результатах. Некоторые изменения происходят в соответствии с условиями на пути (например, уведомлением о перегрузке) или требованиями сегментов пути между отправителем и получателем. Например, размер пакета будет меняться, если заголовки IP будут преобразованы к другой версии (семейству адресов), а также при добавлении или удалении заголовков расширения. Даже обычно изменяемые в пути поля заголовка, такие как TTL/Hop Limit, могут влиять на некоторые тесты. Например, пакеты протокола обнаружения соседей (Neighbor Discovery Protocol или NDP) [RFC4861] передаются с Hop Limit = 255 и для их корректности у получателя это поле **должно** иметь значение 255. Хотя в других тестах поле TTL/Hop Limit может исключаться из определения Type-P, для этого теста значение Hop Limit важно и **должно** включаться в определение Type-P.

Локальные правила промежуточных узлов, проверяющие заголовки расширения IPv6, могут влиять на повторяемость измерений. Если промежуточные узлы выполняют рекомендации [RFC7045], повторяемость в той или иной степени может быть улучшена.

Важное замечание. Было бы очень полезно знать, обрабатывает ли данная часть (хост, канал, путь) Internet одинаково класс C (это обозначение не относится к классам адресов) разных типов пакетов. Если это так, для последующих измерений в этой части можно использовать любой из этих типов пакетов. Это предполагает разработку метрики или набора показателей, с попыткой определить класс C.

Распределение нагрузки между параллельными путями является одним из примеров, где такой класс C будет сложно определить в измерениях IPPM. Балансировщики и маршрутизаторы часто применяют идентификаторы потоков в форме хэш-значений заголовка пакета (для конкретного пути), которые служат для выбора среди доступных путей. Пакеты с идентичным хэш-значением относятся к одному потоку и пересылаются одному ресурсу в балансировщике (маршрутизаторе). Наличие балансировки в пути измерения, а также конкретные заголовки и поля, применяемые в решении о пересылке, не будут известны, когда измерительный путь является «чёрным ящиком». Возможные варианты оценки включают измерение одного из параллельных путей и измерение всех доступных параллельных путей, которые могут применяться для балансировки. Поэтому знание определения потоков в балансировщике (или связанная с классом C обработка полей заголовка в части хэширования) является необходимым условием для повторяемости измерений. На пути может оказаться несколько балансировщиков, что усложнит определение класса C.

5. Пакеты стандартного формата

Если не указано иное, все определения показателей, относящиеся к пакетам IP, неявно включают допущение о стандартном формате пакетов. Пакет считается имеющим стандартный формат, если он соответствует **требованиям**:

- наличие действительного (корректного) заголовка IP с учётом версии протокола;
- не является фрагментом IP;
- адреса отправителя и получателя (включая групповых получателей) соответствуют предусмотренным Source и Destination;
- при наличии транспортного заголовка, он содержит корректную контрольную сумму и другие поля.

Для стандартных пакетов IPv4 (в соответствии с [RFC791] и обновляющими его RFC) **требуется**:

- значение 4 в поле версии;
- значение размера заголовка (Internet Header Length или IHL) не менее 5 и корректная контрольная сумма;
- соответствие общего размера пакета в заголовке IPv4 размеру заголовка и данных (payload);
- пакет имеет достаточное значение TTL для доставки от Source к Destination, если TTL декрементируется на каждом этапе пересылки, или TTL = 255;
- пакет не содержит опция IP, которые не указаны явно.

Для стандартных пакетов IPv6 (в соответствии с [RFC8200] и будущими обновлениями) **требуется**:

- значение 6 в поле версии;
- соответствие общего размера пакета размеру заголовка IPv6 (40 октетов) и размеру данных (payload) в заголовке IPv6;
- соответствие размера данных (включая заголовки расширения) спецификации IPv6;
- пакет имеет достаточное значение Hop Limit для доставки от Source к Destination, если Hop Limit декрементируется на каждом этапе пересылки, или Hop Limit = 255;
- пакет не включает заголовков расширения или число и тип этих заголовков корректно указаны в пакете и порядок заголовков соответствует спецификации (Next Header);
- все параметры в заголовке и заголовках расширения присутствуют в реестре Internet Protocol Version 6 (IPv6) Parameters, заданном в [IANA-6P].

В контексте стандартных пакетов требуется обсудить два механизма - 6LowPAN [RFC4944] и отказоустойчивое сжатие заголовков (Robust Header Compression или ROHC) [RFC3095]. Определение 6LowPAN дано в [RFC4944] и обновлено в [RFC6282] компрессией заголовков и в [RFC6775] оптимизацией обнаружения соседей. В 6LowPAN предложено решение для использования IPv6 в сетях с ограниченными ресурсами. Уровень адаптации позволяет передавать пакеты IPv6 через сети с MTU меньше минимального значения IPv6 MTU. Фрагментация и сборка пакетов IPv6, а также результирующее состояние, хранящееся на промежуточных узлах, создают серьёзные проблемы для измерений. Точно так же ROHC работает с сохранением состояний сжатия заголовков на субпутях в промежуточных точках (хостах). Изменение Type-P для измерительных пакетов в ROHC и 6LowPAN требует существенных усилий, как и требования в части стандартных пакетов для этих 2 протоколов. По этой причине пакеты ROHC и 6LowPAN исключены из числа стандартных форматов пакетов.

Тема заголовков расширения IPv6 вызывает споры, как отмечено в [RFC6564] и [RFC7045]. Однако измерения в контексте схемы IPPM, такие как OAM [IOAM-DATA] в корпоративной среде, могут выигрывать от проверки, изменения, добавления или удаления заголовков расширения IPv6 на хостах в измерительном пути.

[RFC8250] поддерживает использование IPv6 Destination Option для измерений в соответствии с уместными спецификациями, одобренными IETF.

При наличии заголовков расширения возникают указанные ниже дополнительные вопросы.

- Проверка заголовков расширения. Некоторые промежуточные узлы могут проверять заголовки расширения или передаваемые пакеты IPv6 целиком. В исключительных случаях они могут отбрасывать пакеты или направлять их по неоптимальному пути, что может делать измерения ненадёжными или неповторяемыми. Пакет (если он приходит) может иметь стандартный формат с соответствующим Type-P.
- Изменение заголовков расширения. В заголовках Hop-by-Hop для опций TLV может быть разрешено изменение на промежуточных узлах. Результирующий пакет может иметь стандартный формат с соответствующим Type-P.
- Вставка или удаление заголовков расширения. Хотя такое поведение не поддерживается текущими стандартами, заголовки расширения могут добавляться или исключаться из цепочки заголовков.

Результирующий пакет может иметь стандартный формат с соответствующим Type-P. Это требует от разработчиков измерительных систем готовности к непредвиденным обстоятельствам и уведомления пользователей о таких событиях. Имеются проблемы, связанные со вставкой и удалением заголовков расширения, например превышение MTU в результате добавления заголовков и т. п.

- Изменение размера пакетов (по сравнению с размерами у источника) или заголовков имеет важное значение для измерений в Internet и **требуется** указывать изменённый Type-P в результатах теста.

Дополнительно **требуется**, чтобы для пакета размером В октетов выполнялось условие $0 \leq V \leq 65535$, а если В указывает размер данных (payload) в октетах, $V \leq (65535 - \text{размер заголовка IP с учётом заголовков расширения})$. Это не учитывает джамбограммы, определённые в [RFC2675], но при наличии IPv6 Jumbo Payload Hop-by-Hop Option Header пакет соответствующего размера **должен** считаться стандартным. На практике значение path MTU будет ограничивать размер стандартных пакетов, которые можно передать по данному пути. Для предотвращения фрагментации рекомендуется применять механизм Path MTU Discovery для IP версии 6 (PMTUD, [RFC8201]) или Packetization Layer Path MTU Discovery (PLPMTUD, [RFC4821]).

Например, можно представить определение показателя IP-связности как «IP-Type-P-connectivity для стандартных пакетов с IP Diffserv = 0» или более кратко как «IP-Type-P-connectivity с IP Diffserv = 0», поскольку соглашение уже предполагает стандартный формат. Смена содержимого поля, например, на Diffserv Code Point, биты ECN или Flow Label может существенно повлиять на обработку пакетов в процессе передачи, но пакеты не перестанут быть стандартными. Аналогично, добавление, изменение или удаление заголовков расширения может изменить обработку пакетов на промежуточных хостах.

В [RFC2330] определён «минимальный пакет IP от А к В» как определённый тип пакета со стандартным форматом, который зачастую полезно рассмотреть. При определении показателей IP ни один пакет меньше или проще минимального не может быть передан через корректно работающую сеть IP. Однако концепция минимального пакета IP не нашла широкого применения (поскольку активные системы измерения обычно используют транспортный протокол и данные). Поэтому данный документ отменяет эту концепцию.

6. NAT, переход IPv4-IPv6 и методы сжатия

В этом документе добавлены соображения по использованию IPv6 в двух важнейших соглашениях схемы IPPM о пакетах Type-P и пакетах стандартного формата. Необходимость сосуществования IPv4 и IPv6 вызвала создание переходных стандартов, таких как трансляция IPv4/IPv6 [RFC6144] и IP/ICMP [RFC7915] [RFC7757].

Определение и проведение измерений в контексте IPPM сталкивается с проблемами при наличии упомянутых механизмов трансляции на пути измерений. В случаях трансляции IPv4-IPv6, NAT, протокольной инкапсуляции, сжатия заголовков rIPv6 пакеты Type-P на пути измерения могут изменяться. Все такие изменения **должны** указываться в отчёте. Некоторые примеры последствий приведены ниже.

- Изменение или добавление заголовков или полей на промежуточных узлах. Преобразование IPv4-IPv6 или сжатие заголовков IPv6 может менять Type-P измерительных пакетов. В результате хосты на пути измерения могут по-разному трактовать пакеты. При измерениях в точках наблюдения на пути может потребоваться дополнительный контекст для однозначной идентификации пакета.
- Трансляторы сетевых адресов (Network Address Translator или NAT) на пути могут оказывать непредсказуемое влияние на измерение задержки (в части дополнительного времени обработки) и, возможно, других показателей. Обычно это влияние невозможно контролировать, поскольку у тестировщиков может не быть средств воздействия на базовую сеть и промежуточные устройства. Существует вероятность того, что NAT с учётом состояния будет вызвать нестабильность производительности потока с конкретным Type-P, поскольку требуется создать состояние для первого пакета в потоке и это состояние может быть утеряно позднее, если у транслятора NAT недостаточно ресурсов. Однако это не делает Type-P непригодным для теста, например, в случае измерения влияния NAT на вариации задержки. Наличие NAT может означать изменение измеренной производительности Type-P между источником и получателем. Это может вызывать проблемы при сопоставлении измерений, выполненных на сегментах пути с трансляторами NAT. Поэтому наличие (или отсутствие) трансляторов адресов следует учитывать при измерениях.
- Изменение задержки в зависимости от внутреннего состояния. Одним из побочных эффектов преобразований IPv4-IPv6 является переменная задержка на промежуточных узлах в результате преобразования заголовков. Как и в случае NAT, выделение внутреннего состояния и организация контекста на промежуточных узлах может приводить к переменным задержкам, зависящим от картины измерительного потока и размещения пакета в потоке. Например, первый пакет потока обычно вызывает организацию внутреннего состояния на промежуточных хостах с преобразованием IPv4-IPv6. Это состояние будет обеспечивать более быструю обработку последующих пакетов. Однако при больших интервалах между пакетами состояние может теряться и для последующих пакетов придётся создавать его заново. Следует отметить, что такая переменная задержка в результате создания внутреннего состояния на промежуточных узлах сама может быть предметом изучения (измерения).
- Переменная задержка пакетов разного размера. Преобразование IPv4-IPv6 или сжатие заголовков меняет размер измерительных пакетов, что может влиять на трактовку пакетов в пути измерений.

7. Вопросы безопасности

Здесь применимы соображения безопасности, относящиеся к любым активным измерениям (см. [RFC4656] и [RFC5357]).

В плане приватности вовлечённых в измерения сторон возможность утечки при активных измерениях существенно ниже. Пассивные наблюдения за пользовательским трафиком создают риск утечки конфиденциальных сведений. Читателям рекомендуется обратиться к документу [RFC7594], где более рассматриваются активные и пассивные измерения.

8. Взаимодействие с IANA

Этот документ не требует действий IANA.

9. Литература

9.1. Нормативные документы

- [RFC791] Postel, J., "Internet Protocol", STD 5, [RFC 791](#), DOI 10.17487/RFC0791, September 1981, <<https://www.rfc-editor.org/info/rfc791>>.
- [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>>.
- [RFC2330] Paxson, V., Almes, G., Mahdavi, J., and M. Mathis, "Framework for IP Performance Metrics", [RFC 2330](#), DOI 10.17487/RFC2330, May 1998, <<https://www.rfc-editor.org/info/rfc2330>>.
- [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>>.
- [RFC2675] Borman, D., Deering, S., and R. Hinden, "IPv6 Jumbograms", [RFC 2675](#), DOI 10.17487/RFC2675, August 1999, <<https://www.rfc-editor.org/info/rfc2675>>.
- [RFC3095] Bormann, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L.-E., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Yoshimura, T., and H. Zheng, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", RFC 3095, DOI 10.17487/RFC3095, July 2001, <<https://www.rfc-editor.org/info/rfc3095>>.
- [RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", [RFC 3168](#), DOI 10.17487/RFC3168, September 2001, <<https://www.rfc-editor.org/info/rfc3168>>.
- [RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", [RFC 4656](#), DOI 10.17487/RFC4656, September 2006, <<https://www.rfc-editor.org/info/rfc4656>>.
- [RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", [RFC 4821](#), DOI 10.17487/RFC4821, March 2007, <<https://www.rfc-editor.org/info/rfc4821>>.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), DOI 10.17487/RFC4861, September 2007, <<https://www.rfc-editor.org/info/rfc4861>>.
- [RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <<https://www.rfc-editor.org/info/rfc4944>>.
- [RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", [RFC 5357](#), DOI 10.17487/RFC5357, October 2008, <<https://www.rfc-editor.org/info/rfc5357>>.
- [RFC5644] Stephan, E., Liang, L., and A. Morton, "IP Performance Metrics (IPPM): Spatial and Multicast", RFC 5644, DOI 10.17487/RFC5644, October 2009, <<https://www.rfc-editor.org/info/rfc5644>>.
- [RFC5835] Morton, A., Ed. and S. Van den Berghe, Ed., "Framework for Metric Composition", RFC 5835, DOI 10.17487/RFC5835, April 2010, <<https://www.rfc-editor.org/info/rfc5835>>.
- [RFC6144] Baker, F., Li, X., Bao, C., and K. Yin, "Framework for IPv4/IPv6 Translation", RFC 6144, DOI 10.17487/RFC6144, April 2011, <<https://www.rfc-editor.org/info/rfc6144>>.
- [RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <<https://www.rfc-editor.org/info/rfc6282>>.
- [RFC6398] Le Faucheur, F., Ed., "IP Router Alert Considerations and Usage", BCP 168, RFC 6398, DOI 10.17487/RFC6398, October 2011, <<https://www.rfc-editor.org/info/rfc6398>>.
- [RFC6437] Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme, "IPv6 Flow Label Specification", RFC 6437, DOI 10.17487/RFC6437, November 2011, <<https://www.rfc-editor.org/info/rfc6437>>.
- [RFC6564] Krishnan, S., Woodyatt, J., Kline, E., Hoagland, J., and M. Bhatia, "A Uniform Format for IPv6 Extension Headers", RFC 6564, DOI 10.17487/RFC6564, April 2012, <<https://www.rfc-editor.org/info/rfc6564>>.
- [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", [RFC 6775](#), DOI 10.17487/RFC6775, November 2012, <<https://www.rfc-editor.org/info/rfc6775>>.
- [RFC7045] Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", RFC 7045, DOI 10.17487/RFC7045, December 2013, <<https://www.rfc-editor.org/info/rfc7045>>.
- [RFC7312] Fabini, J. and A. Morton, "Advanced Stream and Sampling Framework for IP Performance Metrics (IPPM)", [RFC 7312](#), DOI 10.17487/RFC7312, August 2014, <<https://www.rfc-editor.org/info/rfc7312>>.
- [RFC7757] Anderson, T. and A. Leiva Popper, "Explicit Address Mappings for Stateless IP/ICMP Translation", RFC 7757, DOI 10.17487/RFC7757, February 2016, <<https://www.rfc-editor.org/info/rfc7757>>.
- [RFC7915] Bao, C., Li, X., Baker, F., Anderson, T., and F. Gont, "IP/ICMP Translation Algorithm", [RFC 7915](#), DOI 10.17487/RFC7915, June 2016, <<https://www.rfc-editor.org/info/rfc7915>>.
- [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>>.

[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>>.

[RFC8250] Elkins, N., Hamilton, R., and M. Ackermann, "IPv6 Performance and Diagnostic Metrics (PDM) Destination Option", RFC 8250, DOI 10.17487/RFC8250, September 2017, <<https://www.rfc-editor.org/info/rfc8250>>.

9.2. Дополнительная литература

[IANA-6P] IANA, "Internet Protocol Version 6 (IPv6) Parameters", <<https://www.iana.org/assignments/ipv6-parameters>>.

[IOAM-DATA] Brockners, F., Bhandari, S., Pignataro, C., Gredler, H., Leddy, J., Youell, S., Mizrahi, T., Mozes, D., Lapukhov, P., Chang, R., daniel.bernier@bell.ca, d., and J. Lemon, "Data Fields for In-situ OAM", Work in Progress, draft-ietf-ippm-ioam-data-03, June 2018.

[RFC7594] Eardley, P., Morton, A., Bagnulo, M., Burbridge, T., Aitken, P., and A. Akhter, "A Framework for Large-Scale Measurement of Broadband Performance (LMAP)", RFC 7594, DOI 10.17487/RFC7594, September 2015, <<https://www.rfc-editor.org/info/rfc7594>>.

Благодарности

Авторы благодарны Brian Carpenter за указание отсутствия охвата IPv6 в схеме IPPM и перечисление дополнительных факторов различия для пакетов Type-P. Brian и Fred Baker обсудили с соавторами многие интересные аспекты IPv6, что улучшило цельность первого предварительного варианта документа, спасибо им. Спасибо Bill Jouris за редактирование текста pre-00. В конце работы Nevil Brownlee, Mike Heard, Spencer Dawkins, Warren Kumari и Suresh Krishnan внесли ценные предложения.

Адреса авторов

Al Morton
AT&T Labs
200 Laurel Avenue South
Middletown, NJ 07748
United States of America
Phone: +1 732 420 1571
Fax: +1 732 368 1192
Email: acm@research.att.com

Joachim Fabini
TU Wien
Gusshausstrasse 25/E389
Vienna 1040
Austria
Phone: +43 1 58801 38813
Fax: +43 1 58801 38898
Email: Joachim.Fabini@tuwien.ac.at
URI: <http://www.tu.wien.ac.at/about-us/staff/joachim-fabini/>

Nalini Elkins
Inside Products, Inc.
Carmel Valley, CA 93924
United States of America
Email: nalini.elkins@insidethestack.com

Michael S. Ackermann
Blue Cross Blue Shield of Michigan
Email: mackermann@bcbsm.com

Vinayak Hegde
Consultant
Brahma Sun City, Wadgaon-Sheri
Pune, Maharashtra 411014
India
Phone: +91 9449834401
Email: vinayakh@gmail.com
URI: <http://www.vinayakhegde.com>

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru