Internet Engineering Task Force (IETF)
Request for Comments: 8321
Category: Experimental
ISSN: 2070-1721

G. Fioccola, Ed.
A. Capello
M. Cociglio
L. Castaldelli
Telecom Italia
M. Chen
L. Zheng
Huawei Technologies
G. Mirsky
ZTE
T. Mizrahi
Marvell

January 2018

Alternate-Marking Method for Passive and Hybrid Performance Monitoring

Метод маркировки с чередованием для пассивного и гибридного мониторинга сети

Аннотация

В этом документе описан метод измерения потерь, задержки и её вариаций на «живом» трафике. Метод основан на чередующейся маркировке (Alternate-Marking или AM), называемой также «окрашиванием». Представлен отчёт для разъяснения примера и демонстрации применимости метода. Технологию можно применять в различных ситуациях для пассивных или гибридных измерений в зависимости от приложения.

Статус документа

Документ не относится к категории Internet Standards Track и публикуется для проверки, экспериментальной реализации и оценки.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Не все одобренные IESG документы являются кандидатами в Internet Standard, см раздел 2 RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc8321.

Оглавление

[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

В настоящее время сети большинства сервис-провайдеров передают трафик, весьма чувствительный к потере пакетов [RFC7680], их задержкам [RFC7679] и вариации задержки [RFC3393]. В связи с этим провайдерам требуются методики и инструменты для мониторинга и измерения производительности сети с достаточной точностью, чтобы постоянно контролировать качество обслуживания своих пользователей. С другой стороны, мониторинг производительности даёт полезные сведения для повышения эффективности управления сетью (например, изоляция сетевых неполадок, устранение неисправностей и т. п.).

Организациями по разработке стандартов (Standards Developing Organization или SDO) проделана большая работа, связанная с функциями эксплуатации, администрирования и поддержки (Operations, Administration, and Maintenance или OAM), включающими также методы мониторинга производительности. В [RFC7276] представлен хороший обзор имеющихся механизмов OAM, разработанных в IETF, ITU-T, IEEE. В IETF выполнена большая работа по обнаружению отказов и проверке связности, а также проведены некоторые работы по мониторингу производительности. Рабочая группа IPPM определила стандартные показатели для измерения производительности сети, однако разработанные этой группой методы связаны в основном с активными измерениями. Недавно рабочая группа MPLS определила механизмы для измерения потерь, односторонней и двухсторонней задержки и её вариаций в сетях MPLS [RFC6374], но применение их для пассивных измерений сталкивается с ограничениями, особенно в сетях без явных соединений.

Отсутствие адекватных инструментов для измерения потери пакетов с желаемой точностью побудило разработать новый метод мониторинга производительности живого трафика простой в реализации и развёртывании. Результатом стал описываемый в этом документе метод, основанный на пассивном мониторинге трафика и потенциально применимый к любому пакетному трафику, будь то Ethernet, IP или MPLS, с использованием индивидуальной или групповой адресации. Метод предназначен в основном для измерения потери пакетов, но его легко расширить для измерения задержки в одном или двух направлениях, а также вариаций задержки.

Метод разработан специально для пассивных измерений, но может применяться и с активными зондами. Пассивыне измерения обычно проще понять клиентам и они обеспечивают лучшую точность, особенно при измерении потерь.

В RFC 7799 [RFC7799] определены пассивные и гибридные методы измерения. Пассивные методы основаны исключительно на наблюдении не нарушаемого и не изменяемого потока интересующих пакетов, а гибридные измерения применяют комбинацию активных и пассивных методов. Учитывая эти определения метод чередующейся маркировки (Alternate-Marking) можно рассматривать как гибридный или пассивный, в зависимости от ситуации. Когда маркировка выполняется путём изменения значений полей в пакетах (например, поля кода дифференцированного обслуживания - DSCP), метод является гибридным. Если же маркировка выполняется в специальном (резервном) поле, заданном спецификацией протокола, метод чередующейся маркировки можно считать пассивным. Например, можно применять для маркировки метки потоков Synonymous Flow Label, описанные в [SFL-FRAMEWORK] или биты маркировки OAM, как указано в [PM-MM-BIER]).

Преимущества описываемого метода указаны ниже.

- Простота реализации. Метод можно реализовать на основе возможностей большинства имеющихся платформ маршрутизации, как описано в параграфе 5. или применить оптимизированную реализацию метода но основе традиционных и новейших технологий.
- Низкие вычислительные затраты. Дополнительная нагрузка при обработке пренебрежимо мала.
- Точное измерение потери пакетов. При пассивных измерениях потери учитываются с точностью в 1 пакет.
- Потенциальная применимость к любому трафику на основе пакетов или кадров. Ethernet, IP, MPLS и т. п. при индивидуальной и групповой адресации.
- Отказоустойчивость. Метод устойчив к нарушению порядка пакетов и не базируется на «специальных» пакетах, потеря которых может оказывать негативное влияние.
- Гибкость. Разрешены все форматы временных меток, поскольку они поддерживаются по отдельному каналу (out of band). Выбор формата NTP (Network Time Protocol) [RFC5905] или IEEE 1588 PTP (Precision Time Protocol) [IEEE-1588] зависит от требуемой точности.
- Нет проблем взаимодействия. Свойства, требуемые для экспериментов и тестирования метода (5.1. Отчёт об эксперименте), доступны на всех текущих платформах маршрутизации. Для сбора данных от маршрутизаторов можно применять централизованное или распределенное решение.

Метод не вызывает особых потребностей в расширении протоколов, но его можно развить с помощью некоторых протокольных расширений. В частности, использование битов DiffServ для «окрашивания» пакетов в некоторых случаях может не подходить и полезным был бы стандартный метод окрашивания для конкретного приложения.

1.1. 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.

2. Обзор метода

Существуют разные подходы к измерению потерь пакетов в рабочем потоке трафика. Самым интуитивно понятным способом является нумерация пакетов, чтобы каждый маршрутизатор на пути потока мог сразу увидеть пропуск. Хотя этот подход очень прост в теории, реализовать его непросто и требуется внедрение порядкового номера в каждый пакет, а устройства должны быть способны извлекать эти номера в реальном масштабе времени. Такую задачу трудно реализовать на «живом» трафике - при использовании транспорта UDP порядковые номера не доступны, а если номер имеется в протоколе вышележащего уровня (например, в заголовке RTP) его извлечение в реальном масштабе времени будет сильно нагружать устройство.

Другим решением является учёт пакетов на передающей и приёмной стороне и сравнение результатов. Эта операция значительно проще в реализации, но требует от устройств синхронизации учёта - для сравнения двух значений требуется, чтобы они были связаны с одним набором пакетов. Поскольку потоки непрерывны и не могут быть остановлены для чтения счётчика, сложно определить, когда нужно считывать значение счётчика. Возможным решением этой проблемы является виртуальное разделение потока на последовательные блоки путём периодической вставки разделителей, чтобы каждый счётчик относился к одинаковому блоку пакетов. Таким разделителем может быть, например, специальный пакет, искусственно внедряемый в поток, однако этому методу присущи некоторые ограничения. Во-первых, он требует генерации дополнительных пакетов в потоке, а оборудование должно обрабатывать эти пакеты. Во-вторых, метод чувствителен к переупорядочению пакетов-разделителей и (в меньшей степени) к их потере.

Предлагаемый здесь метод использует второй подход, но без дополнительных пакетов для деления потока на блоки. Вместо этого пакеты маркируются так, что пакеты одного блока получают одну «окраску», а пакеты следующего блока - другую. Каждая смена цвета представляет сигнал автосинхронизации, гарантирующий согласованность измерений на разных устройствах в пути (см. работы [IP-MULTICAST-PM] и [OPSAWG-P3M], где этот метод был предложен).

На рисунке 1 показана простая сеть и применение метода для учёта потерь в разных сегментах путём проведения измерений на разных интерфейсах в пути. Это может быть мониторинг узла, канала или сквозной мониторинг. Метод достаточно гибок для измерения потерь в любом сегменте сети и может служить для поиска сбойных элементов.

Рисунок 1. Доступные измерения.

3. Подробное описание метода

В этом разделе рассматриваются детали работы метода. Основное внимание уделено измерению потери пакетов, являющееся основным применением метода, а также применимость для измерения задержки и её вариаций.

3.1. Измерение потери пакетов

Идея заключается в виртуальном расщеплении потока трафика на последовательные блоки, каждый из которых представляет измеряемую сущность, однозначно распознаваемую всеми устройствами на пути через сеть. Учитывая число пакетов в каждом блоке, определённое разными сетевыми устройствами на пути, можно определить потери пакетов в любом блоке между парой точек сети.

Как отмечено выше, простым способом создания блоков является «окрашивание» трафика (двух цветов достаточно), чтобы пакеты последовательных блоков различались по цвету. Смена цвета указывает завершение блока и начало нового. Число пакетов каждом блоке зависит от критериев создания блоков:

- если цвет меняется после фиксированного числа пакетов, все блоки без потерь будут содержать одинаковое число пакетов;
- если чвет меняется по фиксированному таймеру, число пакетов в блоке зависит от скорости передачи.

На рисунке 2 показанокак выглядят блоки пакетов после окрашивания.

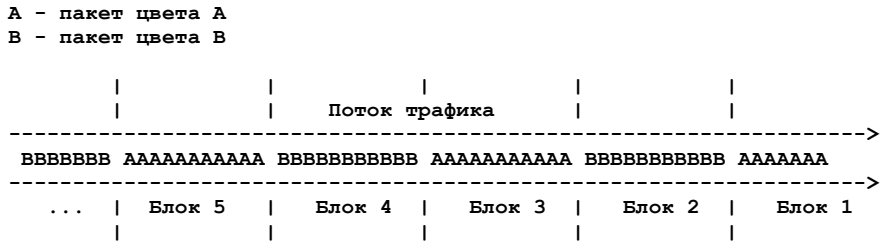

Рисунок 2. Окрашивание трафика.

На рисунке 3 показано применения метода для определения потери пакетов на канале между смежными узлами. Предположим, что мониторинг потери пакетов выполняется между двумя маршрутизаторами R1 и R2. В соответствии с методом трафик окрашивается в цвета A и B. Смена цвета служит сигналом завершения блока, как показано в верхней части рисунка 3.

Если трафик ещё не окрашен, R1 может сделать это сам. Маршрутизатору R1 нужны два счётчика на выходном интерфейсе - C(A)R1 учитывает пакеты цвета A, C(B)R1 - пакеты цвета B. Пока трафик имеет цвет A, инкрементируется лишь счётчик C(A)R1, а при трафике цвета B инкрементируется только C(B)R1. C(A)R1 и C(B)R1 могут служить

эталонными значения для определения потерь между R1 и любой другой точкой измерения на дальнейшем пути. Маршрутизатору R2 тоже нужны два счётчика на входном интерфейсе - C(A)R2 и C(B)R2, учитывающие пакеты цвета A и B, соответственно. По завершении блока A можно сравнить значения C(A)R1 и C(A)R2 для определения числа потерянных пакетов блока. Аналогично при завершении блока B можно сравнить счётчики C(B)R1 и C(B)R2.

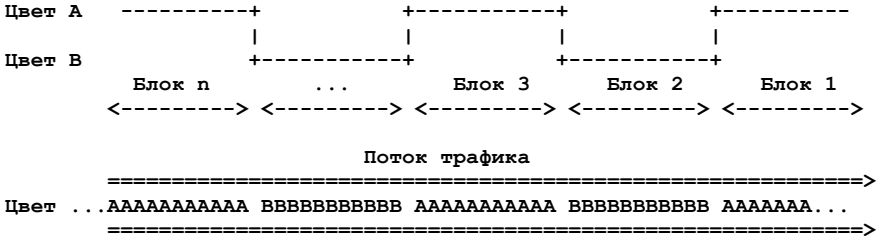

Рисунок 3. Обнаружение потери пакета в канале.

Точно также с использованием двух счётчиков на выходном интерфейсе R2 можно учесть пакеты, переданные интерфейсом R2 и использовать значения счётчиков в качестве эталона для сравнения в следующей точке измерения.

Использование фиксированного таймера для смены окрашивания обеспечивает лучшее управления методом - продолжительность (время) блока может быть достаточно большой для упрощения сбора и сравнения значений на разных сетевых устройствах. Предпочтительно считывать значение счётчика не сразу при смене цвета, чтобы учесть возможное нарушение порядка доставки (некоторые пакеты могут прийти с запозданием и будут увеличивать значение счётчика). Безопасным сроком ожидания представляется L/2 (L - продолжительность каждого блока) перед считыванием счётчика предыдущего блока. Недостатком выбора большой продолжительности блока является более грубое измерение.

В таблице 1 показано, как можно использовать счётчики для определения потерь между R1 и R2. В первом столбце указаны последовательные блоки трафика, а в остальных - значения счётчиков A и B на маршрутизаторах R1 и R2. А этом примере предполагается, что значения счётчиков считываются и сбрасываются в 0 по завершении блока, поэтому в таблице показаны лишь относительные значения, указывающие точное число пакетов в каждом блоке. Если счётчики не сбрасывать, таблица будет содержать кумулятивные значения, а относительные можно определить просто вычитая значение для предыдущего блока того же цвета. Цвет меняется по фиксированному таймеру (нет в таблице), поэтому число пакетов в блоках может меняться.

Таблица 1. Оценка счётчиков для измерения потери пакетов.

Блок	***C(A)R1***	***C(B)R1***	***C(A)R2***	***C(B)R2***	***Потери***
1	375	0	375	0	0
2	0	388	0	388	0
3	382	0	381	0	1
4	0	377	0	374	3
...	...	...	...	...	...
2n	0	387	0	387	0
2n+1	379	0	377	0	2

В блоках A (1, 3, 2n+1) все пакеты имеют цвет A, поэтому счётчики C(A) инкрементируются до числа пакетов, наблюдавшихся на интерфейсе, а C(B) = 0. В блоках B (2, 4, 2n) все пакеты имеют цвет B, счётчики C(A) = 0, а C(B) инкременитруются.

По завершении блока (смена цвета) инкрементирование относительных счётчиков прекращается и можно считать их для сравнения значений на маршрутизаторах R1 и R2 с целью определения потерь в блоке. Например, в таблице указано, что в блоке 1 (A) счётчики C(A)R1 и C(A)R2 имеют значения 375, что говорит об отсутствии потерь в первом блоке. Во втором блоке (B) счётчики R1 и R2 также совпадают (388) и это говорит об отсутствии потерь. В блоках 3 и 4 счётчики R1 и R2 различаются, что говорит о потере пакетов, в нашем примере это один пакет (382-381) в блоке 3 и три пакета (377-374) в блоке 4.

Метод, применяемый к R1 и R2, можно распространить на любые маршрутизаторы и применять в более сложных сетях, поскольку измерения выполняются на пути прохождения потоков трафика.

Следует отметить две стратегии реализации метода.

- По потокам. Этот подход применяется в случаях, когда нужно отслеживать ограниченное число потоков трафика, т. е. маркируется лишь часть потоков. Счётчики для измерения потерь можно создать для каждого потока или набора потоков в зависимости от требуемой детализации. С этим подходом связана проблема необходимости заранее знать путь измеряемого потока. Смена пути и применение балансирования нагрузки усложняет измерения, особенно для индивидуального трафика. Проблему легче решить для группового трафика, где распределение нагрузки применяется редко а для принудительной пересылки и репликации часто применяются статические пути.
- По каналам. Измерения выполняются для всего трафика, проходящего по каналу, который может быть физическим или логическим. Счётчики задаются для трафика в целом или отдельных классов (если нужно отслеживать каждый класс независимо), но во втором случае требуется пара счётчиков для каждого класса.

Как отмечено выше, для измерения по потокам требуется идентификация отслеживаемых потоков и определение пути для нужного потока. Можно отслеживать одие поток или группу потоков, но во втором случае измерение будет согласованным лишь прихождении всех потоков по одному пути. Кроме того, при группировке потоков невозможно точно определить, в каком потоке возникли потери. Для измерений на одном потоке нужно создать счётчики для каждого отслеживаемого потока. Когда контролируемые потоки указаны, требуется настроить мониторинг на соответствующих узлах. Настройка мониторинге означает задание правил для перехвата трафика и настройку счётчиков пакетов. Для выполнения сквозного мониторинга достаточно включить отслеживание на первом и последнем маршрутизаторе пути, в этом случае механизм просто не заметен промежуточным узлам и не зависит от выбора пути. При поэтапном (hop-by-hop) отслеживании на всем пути требуется включить отслеживание на каждом узле от источника до получателя. Если путь не известен заранее (имеется несколько путей между источником и получателем),

требуется включить мониторинг на всех путях. Счётчики на интерфейсах фактического пути будут отслеживать потери пакетов, а прочие просто останутся неиспользуемыми (0).

3.1.1. «Окрашивание» пакетов
Окрашивание является основой создания блоков пакетов и подразумевает выбор места и способа задания цвета.

При измерениях по потокам можно задать поток для отслеживания правилами отбора (например, полей заголовка) для сопоставления с подмножеством пакетов. Таким способом можно контролировать число вовлечённых узлов на пути следования пакетов и размеры потоков. В общем случае может быть один или несколько окрашивающих узлов, при этом использование одного узла упрощает управление и избавляет от конфликтов. При окрашивании на нескольких узлах требуется, чтобы окраска периодически менялась между узлами в соответствии с параграфом 3.2, чтоы каждый измерительный узел на пути мог однозначно идентифицировать окрашенные пакеты. В [MULTIPOINT-ALT-MM] раскрашивание обобщено для потоков «многие со многими» (multipoint-to-multipoint). Кроме того, может быть выгодно окрашивать пакет ближе к источнику, поскольку это позволяет выполнять сквозные измерения, если это разрешено и на последнем маршрутизаторе в пути пакета.

При измерениях по каналам нужно окрашивать весь трафик, передаваемый в канал. Если трафик уже окрашен, он должен перекрашиваться, потому что окрашивание на канале должно быть согласованным. Это означает, что каждый интервал пересылки на пути должен окрасить или перекрасить трафик. Цвета на разных каналах могут отличаться.

Окрашивание трафика можно выполнить путём установки конкретного бита в заголовке пакета и периодической смены значения этого бита. Выбор поля для маркировки зависит от приложение и не задаётся здесь, однако некоторые приложения описаны в разделе 5.

3.1.2. Учёт пакетов
Для измерений по потокам в предположении окрашивания пакетов лишь на узлах-источниках узлы между источником и получателем (включая их) учитывают полученные и пересланные окрашенные пакеты - эта операция может быть включан на всех или части маршрутизаторов на пути, в зависимости от контролируемого сегмента сети (один канал, конкретная область городской сети или весь путь целиком). Поскольку окраска периодически меняется, нужны два счётчика (по одному для каждого цвета). Для каждого отслеживаемого потока или группы потоков и каждого интерфейса, где включён мониторинг, требуется пара счётчиков (по одному на каждый цвет). Например, для раздельного мониторинга трёх потоков маршрутизатору с четырьмя интерфейсами потребуется 24 счётчика (по 2 для каждого потока на каждом интерфейсе). В [MULTIPOINT-ALT-MM] подсчёт обобщен для потоков multipoint-to-multipoint.

В случае измерений по каналам поведение похоже, но окрашивание и учёт ведутся по каналам на конечных точках.

Ещё один важный аспект, который следует учитывать при считывании счётчиков - это момент считывания, позволяющий получить точное число пакетов в блоке. Маршрутизатор должен считывать счётчик, когда блок уже завершён, иными словами, счётчик для цвета A должен считываться, когда текущий блок имеет цвет B, чтобы подсчёт уже завершился. Это можно реализовать двумя способами. Общий подход предполагает периодическое считывание счётчиков несколько раз на протяжении блока и сравнение последовательных результатов. Когда рост значения прекращается, это означает, что текущий блок закончен и значение счётчика можно безопасно обрабатывать. При управлении окрашиванием по таймеру можно настроить считывание по этому же таймеру. Например, можно считывать счётчик A каждый раз около середины последующего блока B. Достаточный запас между концом блока и считыванием позволяет учесть возможное нарушение порядка доставки пакетов.

3.1.3. Сбор данных и расчёт потери пакетов
Узлы, включённые в мониторинг производительности, собирают значения счётчиков, но не могут использовать их напрямую для измерения потери пакетов, поскольку им известны лишь свои значения. Поэтому может применяться внешняя система управления сетью (Network Management System или NMS) для сбора и обработки значений счётчиков при расчёте потерь. NMS сравнивает значения счётчиков от разных узлов и может определить потерю пакетов (даже одного), и место, где это произошло.

Значения счётчиков нужно передавать в NMS сразу после считывания. Это можно реализовать по протоколу SNMP или FTP в режиме выталкивания (Push) или опроса (Polling). В первом случае каждый маршрутизатор периодически передаёт сведения NMS, во втором NMS периодически опрашивает маршрутизаторы для сбора сведений. В обоих случаях NMS нужно собрать все относящиеся к делу значения от всех маршрутизаторов в одном цикле таймера.

Можно применять протокол обмена значениями счётчиков между парой конечных точек для расчёта потери пакетов в каждом направлении.

Варианты архитектуры измерения производительности (performance measurement или PM) рассмотрены в [COLORING], а [IP-FLOW-REPORT] вводит новые информационные элементы в IPFIX (IP Flow Information Export) [RFC7011].

3.2. Вопросы синхронизации
В этом документе представлено два метода смены окрашивания пакетов - по фиксированному числу пакетов и по фиксированному таймеру. Метод на основе таймера предпочтительней, поскольку он более детерминирован, и в дальнейшем рассматривается именно он.

В общем случае часы в сетевых устройствах не точны и время на маршрутизаторах R1 и R2 будет различаться. Для реализации этого метода часы требуется синхронизировать от одного источника с точностью ±L/2, где L - фиксированная продолжительность блока. Тогда каждый окрашенный пакет можно отнести к верному блоку на каждом из маршрутизаторов. Это обусловлено тем, что минимальная дистанция между пакетами одного цвета из разных блоков составляет L (без учёта нарушения порядка, прим. перев).

На практике в дополнение к ошибкам часов на реализацию метода влияют задержки между измерительными точками, которые могут меняться от пакета к пакету и пакеты вблизи границы блока могут даже прийти среди пакетов следующего блока. Это означает, что без учёта ошибок часов следует выжидать в течение времени L/2 после смены цвета для получения верного значения счетчика.

Таким образом, нужно учитывать расхождение часов в точках измерения и интервал ожидания для пакетов с нарушением порядка доставки. Обе эти проблемы показаны на рисунке 4.

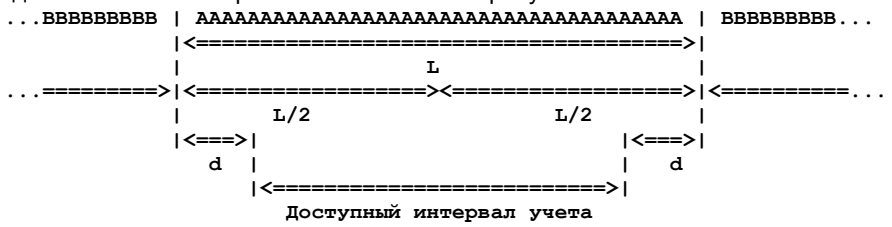

Рисунок 4. Аспекты синхронизации.

Предполагается, что все сетевые устройства синхронизированы с общим эталоно с точностью ±A/2. Таким образом, разница между любой парой часов на ограничена значением A. «Защитная полоса» определяется выражением

```
d = A + D_max – D_min,
```

где A - точность часом, D_max - верхняя, а D_min - нижняя граница задержки между пакета устройствами.

Допустимый интервал учёта составляет L - 2d и должен быть больше нуля. Условие, которое должно выполняться и требование к точности синхронизации имеет вид

```
d < L/2.
```

3.3. Измерение односторонней задержки

Тот же принцип применяется при измерении задержки в одном направлении, где имеется 3 вариант, описанных ниже. Отметим, что для всех вариантов можно определить круговую задержку, суммируя значения для двух направлений.

3.3.1. Методика с одним маркером

Чередование цветов можно использовать как метку времени для расчёта задержки. Когда цвет меняется новый блок), сетевое устройство может записать временную метку первого пакета в новом блоке, а затем это значение можно сравнить с меткой времени того же пакета на другом маршрутизаторе для расчёта задержки пакета. В примере, показанном на рисунке 2, маршрутизатор R1 сохраняет метку TS(A1)R1 при отправке первого пакета блока 1 (A), а метку TS(B2)R1 - при отправке первого пакета блока 2 (B) и т. д. R2 выполняет аналогичные операции на приёмной стороне, записывая TS(A1)R2, TS(B2)R2 и т. д. Поскольку метки относятся к конкретным пакетам (первому в каждом блоке), сравнение этих меток также будет относиться к этим пакетам и можно вычислить задержку пакета. Сравнивая метки TS(A1)R1 и TS(A1)R2 (аналогично, TS(B2)R1 и TS(B2)R2 и т. д.), можно определить задержку между R1 и R2. Для большего числа измерений можно сохранять дополнительные метки, относящиеся к другим пакетам того же блока.

Для когерентного сравнения временных меток от разных маршрутизаторов часы на узлах сети должны быть синхронизированы. Кроме того, измерения действительны лишь при отсутствии потерь и переупорядочения пакетов, поскольку в ином случае первый пакет на одном маршрутизаторе (R1) может оказаться не первым на другом (R2), например, при потере или нарушении порядка пакетов между маршрутизаторами R1 и R2.

В таблице 2 показано, как можно использовать временные метки для расчёта задержки между R1 и R2. В первом столбце указана последовательность блоков, в остальных - временные метки первых пакетов блока на R1 и R2. Разница между значениями меток указывает задержку. Для простоты все значения даны в миллисекундах.

Таблица 2. Оценка временных меток для измерения задержки.

Блок	***TS(A)R1***	***TS(B)R1***	***TS(A)R2***	***TS(B)R2***	***Задержка R1-R2***
1	12,483	-	15,591	-	3,108
2	-	6,263	-	9,288	3,025
3	27,556	-	30,512	-	2,956
	-	18,113	-	21,269	3,156
...	...	...	...	...	...
2n	77,463	-	80,501	-	3,038
2n+1	-	24,333	-	27,433	3,100

В первой строке показаны метки R1 и R2 для первого пакета блока 1 (A). Задержка определяется разностью меток R2 и R1. Во второй строке показаны метки (в миллисекундах) R1 и R2 для первого пакета блока 2 (B). сравнивая метки от разных узлов, относящиеся к одному пакету (указывается сменой цвета), можно определить задержку в сегменте сети.

Для простоты в рассмотренном примере выполнялось одно измерение в каждом блоке (для первого пакета блока). Число измерений можно легко увеличить, рассматривая несколько пакетов из блока - можно записывать метки, например, для одного из каждых N пакетов. В предельном случае можно определять задержку для каждого пакета в блоке (непрактично с точки зрения реализации).

3.3.1.1. Средняя задержка

Как отмечено выше, метод, представленный для измерения задержки, подвержен влиянию нарушений порядка доставки пакетов. Для решение этой проблемы был рассмотрен подход, основанный на концепции средней задержки, которая рассчитывается из среднего времени прибытия пакетов в одном блоке. Сетевое устройство локально сохраняет временные метки для каждого пакета в блоке, суммирует их значения и делит сумму на число полученных в блоке пакетов. Разность среднего времени прибытия от двух смежных устройств даёт среднюю задержку между этими узлами. При расчёте средней задержки измерительная ошибка может возрастать из-за накопления ошибок множества пакетов. Этот метод устойчив к переупорядочению пакетов и их потерям, которые вносят незначительный вклад в ошибку. Кроме того, это значительно сокращает число меток, собираемых системой управления (1 на блок). С другой стороны, метод даёт лишь один результат для всего блока и не позволяет определить минимальную, максимальную и медианную задержку [RFC6703]. Детализацию измерений можно повысить, сократив продолжительность блока (например, до нескольких секунд, но это предполагает сильно оптимизированную реализацию метода.

3.3.2. Методика с двумя маркерами

Методика измерения односторонней задержки с одним маркером чувствительная к нарушению порядка доставки пакетов. Подход к решению проблемы на основе измерения средней задержки описан в предыдущем параграфе, однако он не позволяет получить сведений о распределении задержки в блоке. Кроме того, иногда полезно определить минимальную, максимальную и медианную задержку для получения статистики. Поэтому для получения большего объёма информации о задержках и устойчивости к переупорядочению пакетов предложен иной подход, основанный на применении двух маркеров.

Идея применения второго маркера, по сути, заключается в создании дополнительного потока и выбора в рамках окрашенного потока пакетов для измерения задержки и её вариаций (jitter). Первый маркер нужен для измерения потери пакетов и средней задержки, а второй создаёт новый набор помеченных пакетов, которые идентифицируются в сети, чтобы сетевые устройства могли сохранять метки времени из этих пакетов. Сравнение временных меток одного пакета на разных маршрутизаторах позволяет рассчитать задержку для этого пакета. Число измерений легко менять, устанавливая частоту второй маркировки, однако она не должна быть слишком высокой, чтобы избежать проблем при нарушении порядка пакетов. Между пакетами со вторым маркером должен быть «интервал безопасности» (например, интервал не менее средней задержки в сети, рассчитанной первым методом), чтобы избежать проблем при нарушении порядка, а также иметь достаточное число измерений независимо от скорости. При потере пакета со вторым маркером измерение задержки для соответствующего блока нарушается и результаты следует отбрасывать.

Средняя задержка рассчитывается для всех пакетов выборки на основе метода с одним маркером. В некоторых случаях измерения средней задержки недостаточно для характеристики выборки и нужна дополнительная статистика задержек, например, процентили, вариации и медиана. Традиционного диапазона (минимум-максимум) следует избегать по некоторым причинам, включая стабильность максимальной задержки из-за влияния пиков. В параграфе 6.5 RFC 5481 [RFC5481] отмечено, что процентили 99,9 для задержки и её вариаций более полезен для планирования производительности. Идея преодоления этого недостатка состоит в комбинации средней задержки для всего блока и метода двойной маркировки, где часть пакетов блока выбирается для расширенного расчёта задержек. В этом случае можно выполнить детальный анализ на основе пакетов с двойной маркировкой. Следует отметить, что имеются классические алгоритмы расчёта медианы и вариаций, но их рассмотрение выходит за рамки документа. Сравнение средней задержки для всего блока и пакетов с двойной маркировкой даёт полезную информацию, позволяющую понять, действительно ли измерения с двойной маркировкой отражают тенденции задержки.

3.4. Измерение вариаций задержки

Подобно измерению односторонней задержки (с одним или двумя маркерами), метод подходит для измерения вариаций межпакетны интервалов (inter-arrival jitter) на основе определения RFC 3393 [RFC3393]. Смену цвета при использовании одного маркера можно применять в качестве отметки времени для измерения вариаций задержки. При двойной маркировке такие отметки задают пакеты со вторым маркером. В примере на рисунке 2 маршрутизатор R1 сохраняет метку TS(A)R1 при отправке первого пакета блока, а R2 сохраняет метку TS(B)R2 при получении первого пакета блока. Вариации можно легко получить по результатам измерения односторонней задержки, оценивая изменения задержки для последовательных выборок.

Концепция средней задержки тоже применима к измерению вариаций путём оценки среднего изменения интервала между последовательными пакетами блока от маршрутизаторов R1 и R2.

4. Вопросы методологии

В этом разделе рассматриваются некоторые вопросы методологии измерений.

4.1. Синхронизация часов

Метод чередующейся маркировки не требует строгой синхронизации, особенно при измерении потерь и круговой задержки. Синхронизация часов в устройствах нужна лишь для измерения односторонней задержки.

Смены цвета является сигналом для сетевого устройства и единственное требование состоит в том, чтобы все устройства на пути распознавали блоки пакетов.

При продолжительности интервала измерения L все сетевые устройства должны быит синхронизированы с общим эталоно с точностью ±L/2 (без учёта задержки в сети). Такая точность гарантирует, что все устройства будут согласованно сопоставлять цвет с блоком. Например, если цвет меняется каждую секунду (L = 1 сек.), часы должны быть синхронизированы от общего источника с точностью не хуже ±0,5 сек.

Это требование можно выполнить даже при сравнительно грубом методе синхронизации и подходит для измерения потерь и круговой задержки. Однако для измерения односторонней задержки нужна более точная синхронизация.

Таким образом, при измерении лишь потерь и круговой задержки синхронизации не требуется, поскольку значение времени по часам сетевого устройства не влияет на рсчет круговой задержки.

4.2. Сопоставление данных

Сопоставление данных - это механизм сравнения значений счётчиков и временных меток при расчёте потерь, задержки и её вариаций. Его можно выполнить разными способами в зависимости от варианта применения чередующейся маркировки. Некоторые способы указаны ниже.

- Применение централизованной системы NMS для сопоставления данных.
- Распределённое решение на основе нового протокола или расширения имеющихся протоколов (например, RFC 6374 [RFC6374], TWAMP [RFC5357] или OWAMP [RFC4656]) для передачи между узлами значений счётчиков и временных меток.

В следующих параграфах рассматривается пример механизма сопоставления, который можно применять независимо от принятых решений.

Когда данные (например, значения счётчиков для измерения потерь) собираются на восходящих или нисходящих узлах и периодически передаются или запрашиваются NMS, **следует** использовать тот или иной механизм, чтобы помочь узлам или NMS узнать, какие счётчики или временные метки относятся к одному промаркированному пакету.

Описанный здесь метод AM делит пакеты измерительного потока на блоки и каждому блоку можно присвоить номер (Block Number или BN). Значения BN генерируются каждый раз, когда узел считывает данные (счётчик или временная метка), и связывается с каждым значением счётчика или временной метки, передаваемым другим узлам или NMS. Значение BN может рассчитываться из локального времени (в момент считывания) с интервалом маркировки в качестве модуля.

Когда узел или NMS видит, например, одинаковые BN для двух пакетов от восходящего или нисходящего узла, эти пакеты относятся к одному блоку маркеров от узла. Предполагается, что механизм BN используется с синхронизированными часами узлов, что требует использовать на узлах синхронизацию часов, например, по протоколу сетевого времени (Network Time Protocol или NTP) [RFC5905] или протоколу точного времени IEEE 1588 (Precision Time Protocol или PTP) [IEEE-1588]). Вопросы синхронизации рассмотрены в параграфе 4.1.

4.3. Переупорядочение пакетов

В результате использования ECMP переупорядочение пакетов часто происходит в сетях IP. Точность PM на основе маркеров, особенно при оценке потерь, может зависеть от переупорядочения пакетов. Рассмотрим пример (Рисунок 5).

```
Блок    :    1    |    2    |    3    |    4    |    5    |...
--------|---------|---------|---------|---------|---------|---
Узел R1 : AAAAAAA | BBBBBBB | AAAAAAA | BBBBBBB | AAAAAAA |...
Узел R2 : AAAAABB | AABBBBA | AAABAAA | BBBBBBA | ABAAABA |...
```

Рисунок 5. Переупорядочение пакетов.

Поток пакетов для узла R1 упорядочен и их можно безопасно связать с интервальными блоками, но на узле R2 порядок уже нарушен (например, пакет B в блоке 3) и нет надёжного способа отнести этот пакет к блоку 2 или 4.

В общем случае требуется связывать пакеты цвета B или A с корректным интервальным блоком. Большинство нарушений порядка происходит на краях смежных блоков и с этим легко справиться, если блоки достаточно велики. В этом случае можно предположить, что пакеты с другой маркировкой относятся к ближенму блоку того же цвета. При коротких блоках сложно, а иногда невозможно определить к какому блоку относится пакет.

Важно выбрать правильный интервал, но этот вопрос выходит за рамки документа. Реализациям **следует** поддерживать возможность настройки интервала и разрешать определённую степень переупорядочения пакетов.

5. Приложения, реализация и развёртывание

Описанную выше методологию можно применять в различных ситуациях. По сути, метод AM подходит для многих случаев измерения производительности. Единственным требованием является выбор и маркировка потоков для отслеживания - отправитель организует блоки пакетов, чередуя их маркировку так, чтобы получатель легко мог её распознать. Некоторые недавние варианты применения метода чередующейся маркировки приведены ниже.

- Измерение производительности потока (IP Flow Performance Measurement или IPFPM) с использованием маркировки, описанной в [COLORING]. Например, в этом документе предложен в качестве маркера последний резервный бит поля Flag в заголовке IPv4, а для IPv6 можно применять заголовок расширения IPv6.
- Пассивное измерение производительности OAM. В [RFC8296] два бита OAM из заголовка Bit Index Explicit Replication (BIER) являются резервом для пассивного измерения производительности с использованием маркеров. В [PM-MM-BIER] описаны измерения для групповых служб в домене BIER. Кроме того, метод AM можно использовать в домене с цепочками сервисных функций (Service Function Chaining или SFC). Применение маркировки для виртуализации в сети L3 (Network Virtualization over Layer 3 или NVO3) рассмотрено в [NVO3-ENCAPS].
- Измерение производительности MPLS. В RFC 6374 [RFC6374] применяются пакеты измерения потерь (Loss Measurement или LM) в качестве точек раздела для учёта пакетов. К сожалению это вызывает проблемы, которые могут вести к существенным ошибкам учёта. В [MPLS-FLOW] рассмотрены жедаемые свойства определения потоков MPLS для более эффективного мониторинга по основному каналу для пользовательских пакетов данных. Для идентификации служат синонимы меток потоков (Synonymous Flow Label или SFL), предложенные в [SFL-FRAMEWORK], а в [SYN-FLOW-LABELS] описано измерение производительности RFC 6374 с применением SFL.
- Активное измерение производительности. В [ALT-MM-AMP] описан способ расширения протокола активных измерений для реализации метода AM. В [ALT-MM-SLA] описано расширение для Cisco SLA Protocol Measurement-Type UDP-Measurement.

Пример реализации и развёртывания в следующем параграфе поясняет работу метода.

5.1. Отчёт об эксперименте

Описанный здесь метод, известный также как мониторинг производительности пакетной сети (Packet Network Performance Monitoring или PNPM), был придумен и разработан в Telecom Italia.

Важно подчеркнуть, что общее описание метода в этом документе основано на эксплуатационном эксперименте. Были проверены основные элементы метода и полученных при эксперименте опыт вдохновил на формализацию метода чередующейся маркировки, описанного выше.

Метод применядся для эксперимента в сети Telecom Italia с групповыми каналами IPTV и иными потоками трафика с высокими требованиями QoS (например, трафик Mobile Backhauling, реализованный с MPLS VPN).

Технология была развёрнута с использованием доступных на маршрутизаторах IP функций и инструментов и в настоящее время применяется для мониторинга потерь в некоторых частях сети Telecom Italia. Применение метода для измерения задержки оценивалось в лабораториях Telecom Italia.

В этом параграфе описан способ проведения эксперимента и, в частности, функции, доступные на имеющихся платформах маршрутизации, которые можно использовать для реализации метода, чтобы представить пример реализации и развёртывания.

В описываемом тесте используется основанная на потоках стратегия, как описано в разделе 3. Стратегию на основе каналов можно применить на физических или логических каналах (например, Ethernet VLAN или MPLS PW).

Для реализации метода использовались доступные функции маршрутизаторов, поскольку эксперимент проводился сервис-провайдером Telecom Italia в своей сети. В текущих реализациях маршрутизаторов для маркировки доступны лишь поля и свойства QoS для гибкого управления маркировкой пакетов. Если сервис-провайдер использует лишь 3 старших бита поля DSCP (соответствуют IP Precedence) для классификации QoS и очередей, младшие биты поля DSCP (биты 0 и 1) могут служить для маркировки пакетов без влияния на политику QoS. Именно этот подход применялся в эксперименте. Бит 0 можно использовать для идентификации потоков, где выполняется мониторинг (установка бита означает отслеживание потока), а бит 1 - для окрашивания и создания блоков.

В эксперименте к потоку относились все пакеты с одинаковыми адресами IP (отправитель и получатель). На практике после определения потока можно реализовать окрашивание с использованием поля DSCP путём настройки списков доступа на выходных интерфейсах маршрутизаторов. Список перехватывает пакеты и применяет к ним заданные правила для соответствующей установки поля DSCP. Поскольку окрашивание должно меняться с течением времени, правила нужно периодически менять, для чего был создан автоматический сценарий, выполняющий эту задачу по таймеру. Сценарий загружался в маршрутизатор и обеспечивал операции, требуемые для реализации метода.

После окрашивания трафика с использованием поля DSCP все маршрутизаторы на пути могут выполнять учёт. Для этого могут служит списки доступа с проверкой значений DSCP, учитывающие пакеты отслеживаемых потоков. На всех маршрутизаторах можно применять один список доступа. В дополнение можно использовать мониторинг потоков, такой как предложен в IPFIX [RFC7011], для распознавания временных меток в первом/последнем потоке блока, чтобы использовать один из описанных в параграфе 3.3 вариантов измерений задержки.

В эксперименте Telecom Italia устанавливался таймер смены цвета на 5 минут и последовательность действий сценария также менялась каждые 5 минут. Это значение оказалось хорошим компромиссом между частотой и стабильностью измерений (т. е. возможностью сбора всех измерений, относящихся к одному и тому же блоку). В эксперименте значения счётчиков и иные данные собирались с помощью автоматического сценария, передающего данные в NMS. Система NMS выполняла расчёты для потери пакетов, сравнивая значения от маршрутизаторов на пути потока. Пятиминутные интервалы смены цвета обеспечивали надёжное считывание счётчиков и согласованность с окном отчётов NMS.

Отметим, что использование поля DSCP для маркировки предполагает, что метод применяется лишь внутри домена с единым администрированием.

Эксперимент в Telecom Italia расширялся до 1000 отслеживаемых на одном маршрутизаторе потоков, а при реализации теста на выделенном оборудовании в условиях лаборатории число потоков было ещё больше.

5.1.1. «Прозрачность» метрики

Описанное здесь приложение для сервис-провайдера позволяет применять метод для сквозного мониторинга предоставляемых клиентам услуг. Поэтому важно отметить, что метод должен быть незаметен (прозрачен) за пределами домена провайдера.

В реализации Telecom Italia узлы-источники окрашивали пакеты по правилам, периодически изменяющимися на основе автоматического сценария, меняющего значение поля DSCP в пакетах. Узлы между источником и получателем (включая их) использовали списки доступа для учёта окрашенных пакетов, которые они получали и пересылали.

Кроме того, на узлах-получателях окрашенные пакеты перехватывались и правила восстанавливали для всех пакетов исходные значение полей DSCP. Это обеспечивало «прозрачность» показателя за пределами сегмента сети, где проводился эксперимент. Благодаря такому восстановлению элементы за пределами домена мониторинга AM (например, узлы Provider Edge в Mobile Backhauling VPN MPLS) ничего не знали о маркировке пакетов. Таким образом, восстановление делало чередующуюся маркировку совершенно не заметной за пределами домена мониторинга.

6. Гибридные измерения

Этот метод был специально разработан для пассивных измерений, но его можно применять и в активных измерениях. Для сквозных и промежуточных измерений (гибридных) конечные точки могут обмениваться синтезированными потоками трафика и применять для них чередующуюся маркировку. В промежуточных точках синтезированный трафик обрабатывается аналогично реальному и выполняются описанные здесь измерения. Таким образом, метод маркировки может упростить активные измерения, как описано в [ALT-MM-AMP].

7. Соответствие рекомендациям RFC 6390

В RFC 6390 [RFC6390] определена модель и процессы для разработки показателей производительности (Performance Metrics) протоколов выше и ниже уровня IP (таких, как приложения IP работающие с гарантированным и основанным на дейтаграммах транспортом).

Целью этого документа является предложение не нового показателя производительности, а нового метода измерения для нескольких показателей производительности, которые уже стандартизованы. Тем не менее, к документу следует применять рекомендации [RFC6390] для более полного и согласованного описания метода. Авторы использовали шаблон Performance Metric Definition, заданный в параграфе 5.4 [RFC6390] и зависимости, указанные в параграфе 5.5.

- Имя и описание показателя. Уже отмечено, что этот документ не задаёт показателей производительности, а описывает новый метод для измерения потерь [RFC7680]. Та же концепция с незначительными изменениями может служить для измерения задержки [RFC7679] и её вариаций [RFC3393]. Документ прежде всего описывает применимость метода для измерения потерь.

- Метод измерения или расчёта. В соответствии с предыдущими разделами документа число потерянных пакетов рассчитывается как разность значений счётчиков на узлах отправки и получения. Оба счётчика должны относиться к одному цвету (блоку). Расчёт выполняется для установившихся значений счётчиков, что является неотъемлемой чертой счётчиков маркировки, поскольку чередование цветов даёт установившееся (стабильное) значение счётчика для одного цвета за каждый интервал маркировки.

- Единицы измерения. Метод рассчитывает и сообщает точное число пакетов, которые были переданы источником, но не дошли до получателя.

- Точки измерения с возможной областью измерения. Измерения могут выполняться между соседними узлами или, на канале или пути с множественными пересылками (multi-hop) при прохождении трафика по этому пути. Для пути с множественной пересылкой измерения могут быть сквозными и поэтапными (hop-by-hop).

- Синхронизация измерений. Метод ограничивает частоту измерений, как описано в параграфе 3.2, задавая интервал маркировки и строго связанную с ним «защитную полосу» для предотвращения проблем, связанных с нарушением порядка пакетов. Это связано с тем, что для расчётов нужны установившиеся значения счётчиков, которые возникают уже в процессе получения блока другого цвета. Например, в проведенном эксперименте интервал смены цвета составлял 5 минут, в то время как другие реализации могут сокращать этот интервал до нескольких секунд.

- Реализация. В эксперименте применялось 2 кодировки поля DSCP для окрашивания пакетов, это позволяет использовать на маршрутизаторах правила, позволяющие окрашивать пакеты в соответствии с настройкой. Путь отслеживаемого трафика следует знать заранее для настройки на нём счётчиков и возможности сравнивать значения.

- Проверка. Как в лаборатории, так и в рабочей сети метод был протестирован для измерения потери и задержки пакетов с использованием генераторов трафика в комбинации с точными инструментами и сетевыми эмуляторами.

- Применение. Метод можно использовать для измерения потери пакетов с высокой точностью на «живом» трафике. Утем комбинирования измерений на каналах со сквозными измерениями можно определить места возникновения потерь.

- Модель отчётов. Значения счётчиков передаются централизованной системе управления, которая выполняет расчёты. Такие выборки должны указывать временной интервал, когда измерения проводились, чтобы система управления могла выполнить корректные сопоставления. Выборки следует передавать, когда значения счётчиков уже установились (стабилизировались) в измерительном интервале, в иных случаях значение выборки следует сохранять локально.

- Зависимости. Значения счётчиков должны сопоставляться с интервалом времени, к которому они относятся. Поскольку измерения основаны на значениях DSCP, должны применяться неиспользуемые биты DSCP, чтобы не оказывать влияния на связанные с QoS настройки и поведение. Промежуточным узлам недопустимо менять значение поля DSCP, чтобы не препятствовать измерениям.

- Организация результатов. Метод служит для выполнения одиночных измерений (singleton).

- Параметры. В настоящее время основным параметром метода является интервал смены окрашивания пакетов, в соответствии с которым считываются значения счётчиков.

8. Взаимодействие с IANA

Документ не требует действий IANA.

9. Вопросы безопасности

Этот документ задаёт метод для выполнения измерений в контексте сети сервис-провайдера и не предназначенный для измерений в Internet, поэтому он не влияет напрямую на безопасность Internet или приложений сети Internet. Однако при реализации метода нужно помнить о безопасности и приватности.

Проблемы безопасности могут связаны с помехами измерениям и нарушением работы сети при измерениях.

- Вред, вызванный измерениями. Описанные здесь измерения являются пассивными и в сеть не внедряется новых пакетов, способных повредить трафику данных. Тем не менее, метод подразумевает изменение заголовков или инкапсуляции пакетов «на лету». Эти действия должны выполняться так, чтобы не оказывалось влияния на качество обслуживания выбранных для измерения пакетов, а также на стабильность и производительность маршрутизаторов, выполняющих измерения. Одной из основных угроз безопасности в протоколах OAM является сетевая разведка - злоумышленник может собрать информацию о работе сети, пассивно прослушивая сообщения OAM. Преимущество описанного здесь метода заключается в том, что сетевые устройства обмениваются лишь битами маркировки, поэтому пассивных перехват пакетов плоскости данных не позволит злоумышленнику получить сведения о производительности сети.

- Вред самим измерениям может быть нанесён маршрутизаторами, меняющими маркировку пакетов или злоумышленниками, внедряющими искусственный трафик. Можно применять методы аутентификации, такие как цифровые подписи, для защиты от атак с внедрением трафика. Поскольку на измерения могут влиять маршрутизаторы (или иные устройства) на пути пакетов IP, намеренно меняя биты маркировки, как отмечено выше, описанный в документе механизм следует применять лишь в контексте контролируемого домена, где применяется единое (локальное) администрирование для маршрутизаторов (и иных устройств), что позволяет предотвратить упомянутые атаки. Кроме того, злоумышленник не может получить сведений о производительности сети из одной точки мониторинга, он должен использовать синхронизированные точки измерений на пути, поскольку ему нужно выполнить такие же измерения и агрегирования, которые выполняет сервис-провайдер.

Проблемы приватности при выполнении измерений незначительны, поскольку метод использует лишь сведения из заголовков (инкапсуляции) и не затрагивает данные пользователей. Хотя сведения в заголовках и инкапсуляции являются метаданными, которыми можно воспользоваться для нарушения приватности пользователей, маловероятно, что описанный в документе метод повысит имеющиеся риски. Теоретически можно модулировать маркировку для создания скрытого канала, но это будет слишком низкоскоростной канал, чтобы повлиять на измерительную систему,служащую для мониторинга маркировки.

Другой потенциальной угрозой в контексте этого документа являются атаки с задержкой. Измерения задержки выполняются с использованием конкретных пакетов в каждом блоке, выделенных цветом. Поэтому злоумышленник в MITM-атаке (man-in-the-middle) может лишь искусственно задержать соответствующие пакеты, внося систематическую ошибку в измерение задержки. Как отмечено выше, описанный метод основан на базовом протоколе синхронизации часов. Таким образом, атакуя этот протокол, злоумышленник потенциально может нарушить целостность измерений. Подробное описание угроз для протоколов синхронизации и способов их смягчения дано в RFC 7384 [RFC7384].

10. Литература

10.1. Нормативные документы

[IEEE-1588] IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE Std 1588-2008.

[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>.

[RFC3393] Demichelis, C. and P. Chimento, "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)", RFC 3393, DOI 10.17487/RFC3393, November 2002, <https://www.rfc-editor.org/info/rfc3393>.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <https://www.rfc-editor.org/info/rfc5905>.

[RFC7679] Almes, G., Kalidindi, S., Zekauskas, M., and A. Morton, Ed., "A One-Way Delay Metric for IP Performance Metrics (IPPM)", STD 81, RFC 7679, DOI 10.17487/RFC7679, January 2016, <https://www.rfc-editor.org/info/rfc7679>.

[RFC7680] Almes, G., Kalidindi, S., Zekauskas, M., and A. Morton, Ed., "A One-Way Loss Metric for IP Performance Metrics (IPPM)", STD 82, RFC 7680, DOI 10.17487/RFC7680, January 2016, <https://www.rfc-editor.org/info/rfc7680>.

[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>.

10.2. Дополнительная литература

[ALT-MM-AMP] Fioccola, G., Clemm, A., Bryant, S., Cociglio, M., Chandramouli, M., and A. Capello, "Alternate Marking Extension to Active Measurement Protocol", Work in Progress, draft-fioccola-ippm-alt-mark-active-01, March 2017.

[ALT-MM-SLA] Fioccola, G., Clemm, A., Cociglio, M., Chandramouli, M., and A. Capello, "Alternate Marking Extension to Cisco SLA Protocol RFC6812", Work in Progress, draft-fioccola-ippm-rfc6812-alt-mark-ext-01, March 2016.

[COLORING] Chen, M., Zheng, L., Mirsky, G., Fioccola, G., and T. Mizrahi, "IP Flow Performance Measurement Framework", Work in Progress, draft-chen-ippm-coloring-based-ipfpm-framework-06, March 2016.

[IP-FLOW-REPORT] Chen, M., Zheng, L., and G. Mirsky, "IP Flow Performance Measurement Report", Work in Progress, draft-chen-ippm-ipfpm-report-01, April 2016.

[IP-MULTICAST-PM] Cociglio, M., Capello, A., Bonda, A., and L. Castaldelli, "A method for IP multicast performance monitoring", Work in Progress, draft-cociglio-mboned-multicast-pm-01, October 2010.

[MPLS-FLOW] Bryant, S., Pignataro, C., Chen, M., Li, Z., and G. Mirsky, "MPLS Flow Identification Considerations", Work in Progress[1], draft-ietf-mpls-flow-ident-06, December 2017.

[MULTIPOINT-ALT-MM] Fioccola, G., Cociglio, M., Sapio, A., and R. Sisto, "Multipoint Alternate Marking method for passive and hybrid performance monitoring", Work in Progress[2], draft-fioccola-ippm-multipoint-alt-mark-01, October 2017.

[NVO3-ENCAPS] Boutros, S., Ganga, I., Garg, P., Manur, R., Mizrahi, T., Mozes, D., Nordmark, E., Smith, M., Aldrin, S., and I. Bagdonas, "NVO3 Encapsulation Considerations", Work in Progress, draft-ietf-nvo3-encap-01, October 2017.

[OPSAWG-P3M] Capello, A., Cociglio, M., Castaldelli, L., and A. Bonda, "A packet based method for passive performance monitoring", Work in Progress, draft-tempia-opsawg-p3m-04, February 2014.

[PM-MM-BIER] Mirsky, G., Zheng, L., Chen, M., and G. Fioccola, "Performance Measurement (PM) with Marking Method in Bit Index Explicit Replication (BIER) Layer", Work in Progress, draft-ietf-bier-pmmm-oam-03, October 2017.

[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>.

[1]Опубликовано в RFC 8372. *Прим. перев.*
[2]Опубликовано в RFC 8889. *Прим. перев.*

[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>.

[RFC5481] Morton, A. and B. Claise, "Packet Delay Variation Applicability Statement", RFC 5481, DOI 10.17487/RFC5481, March 2009, <https://www.rfc-editor.org/info/rfc5481>.

[RFC6374] Frost, D. and S. Bryant, "Packet Loss and Delay Measurement for MPLS Networks", RFC 6374, DOI 10.17487/RFC6374, September 2011, <https://www.rfc-editor.org/info/rfc6374>.

[RFC6390] Clark, A. and B. Claise, "Guidelines for Considering New Performance Metric Development", BCP 170, RFC 6390, DOI 10.17487/RFC6390, October 2011, <https://www.rfc-editor.org/info/rfc6390>.

[RFC6703] Morton, A., Ramachandran, G., and G. Maguluri, "Reporting IP Network Performance Metrics: Different Points of View", RFC 6703, DOI 10.17487/RFC6703, August 2012, <https://www.rfc-editor.org/info/rfc6703>.

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <https://www.rfc-editor.org/info/rfc7011>.

[RFC7276] Mizrahi, T., Sprecher, N., Bellagamba, E., and Y. Weingarten, "An Overview of Operations, Administration, and Maintenance (OAM) Tools", RFC 7276, DOI 10.17487/RFC7276, June 2014, <https://www.rfc-editor.org/info/rfc7276>.

[RFC7384] Mizrahi, T., "Security Requirements of Time Protocols in Packet Switched Networks", RFC 7384, DOI 10.17487/RFC7384, October 2014, <https://www.rfc-editor.org/info/rfc7384>.

[RFC7799] Morton, A., "Active and Passive Metrics and Methods (with Hybrid Types In-Between)", RFC 7799, DOI 10.17487/RFC7799, May 2016, <https://www.rfc-editor.org/info/rfc7799>.

[RFC8296] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A., Tantsura, J., Aldrin, S., and I. Meilik, "Encapsulation for Bit Index Explicit Replication (BIER) in MPLS and Non-MPLS Networks", RFC 8296, DOI 10.17487/RFC8296, January 2018, <https://www.rfc-editor.org/info/rfc8296>.

[SFL-FRAMEWORK] Bryant, S., Chen, M., Li, Z., Swallow, G., Sivabalan, S., and G. Mirsky, "Synonymous Flow Label Framework", Work in Progress[1], draft-ietf-mpls-sfl-framework-00, August 2017.

[SYN-FLOW-LABELS] Bryant, S., Chen, M., Li, Z., Swallow, G., Sivabalan, S., Mirsky, G., and G. Fioccola, "RFC6374 Synonymous Flow Labels", Work in Progress, draft-ietf-mpls-rfc6374-sfl-01, December 2017.

Благодарности

Предыдущими спецификациями IETF с описанием этого метода были [IP-MULTICAST-PM] и [OPSAWG-P3M].

Авторы благодарны Alberto Tempia Bonda, Domenico Laforgia, Daniele Accetta, Mario Bianchetti за их вклад при разработке и реализации метода.

Спасибо Spencer Dawkins, Carlos Pignataro, Brian Haberman, Eric Vyncke за помощь, подробные и точные рецензии.

Адреса авторов

Giuseppe Fioccola (editor)
Telecom Italia
Via Reiss Romoli, 274
Torino 10148
Italy
Email: giuseppe.fioccola@telecomitalia.it

Alessandro Capello
Telecom Italia
Via Reiss Romoli, 274
Torino 10148
Italy
Email: alessandro.capello@telecomitalia.it

Mauro Cociglio
Telecom Italia
Via Reiss Romoli, 274
Torino 10148
Italy
Email: mauro.cociglio@telecomitalia.it

Luca Castaldelli
Telecom Italia
Via Reiss Romoli, 274
Torino 10148
Italy
Email: luca.castaldelli@telecomitalia.it

Mach(Guoyi) Chen
Huawei Technologies
Email: mach.chen@huawei.com

Lianshu Zheng
Huawei Technologies
Email: vero.zheng@huawei.com

Greg Mirsky
ZTE
United States of America
Email: gregimirsky@gmail.com

Tal Mizrahi
Marvell
6 Hamada St.
Yokneam
Israel
Email: talmi@marvell.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1]Опубликовано в RFC 8957. *Прим. перев.*