Internet Engineering Task Force (IETF)
Request for Comments: 6673
Category: Standards Track
ISSN: 2070-1721

A. Morton
AT&T Labs

August 2012

# Round-Trip Packet Loss Metrics

Показатель потерь при круговом обходе

**Аннотация**

Многие пользовательские приложения (и транспортные протоколы, делающие их возможными) требуют двухстороннего обмена. Для оценки такой возможности и упрощения систем тестирования на практике часто применяют измерение потерь при круговом обходе. Протокол двухсторонних активных измерений TWAMP (Two-Way Active Measurement Protocol), заданный в RFC 5357, позволяет измерить потери при круговом обходе в Internet. Однако в настоящее время нет показателей потерь при круговом обходе в соответствии с моделью RFC 2330.

Этот документ определяет показатели потерь при круговом обходе (IP Performance Metrics или IPPM).

**Статус документа**

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 5741.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc6673.



# Оглавление



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

# *1. Введение*

Документ определяет показатель для количественной оценки способности сети IP передавать пакеты в обоих направлениях от одного хоста к другому. Двухсторонняя связь требуется почти всегда, поэтому отказ при передаче в любом из направлений ведёт к потерям при круговом обходе (round-trip packet loss).

Документ определяет показатель круговых потерь на путях Internet, основанный на понятиях и соглашениях модели показателей производительности IP (IP Performance Metrics или IPPM) [RFC2330]. В документе часто упоминаются и изменяются в соответствии с рассматриваемым здесь двухсторонним обменом показатели потерь в одном направлении [RFC2680] и круговой задержки [RFC2681] для IPPM. Предполагается, что читатель знаком с упомянутыми документами, поэтому материал из [RFC2681] здесь не дублируется.

Термины двухсторонний (two-way) и круговой (round-trip) применяются в документе как синонимы.

## 1.1. Мотивация

Многим пользовательским приложениям и поддерживающим их транспортным протоколам требуется двухстороннее взаимодействие. Например, трёхстороннее согласование TCP SYN->, <-SYN-ACK, ACK->, используемое постоянно, не может завершиться без двухсторонней связности примерно с одинаковыми временными параметрами для каждого направления. Таким образом, измерение круговых потерь в Internet обеспечивает основу для определения производительности приложений.

Разработчики измерительных систем также признали преимущества простоты решений, где хост просто возвращает (отражает) тестовые пакеты отправителю. Измерения круговых потерь пакетов часто выполняются на практике. Широко используемый инструмент ping позволяет измерить круговую задержку и потери, но обычно требует поддержки ICMP Echo-Request/Reply, а для пакетов ICMP на пути измерения может применяться особая обработка (см. параграф 2.6 в [RFC2681]). Протокол двухсторонних активных измерений TWAMP, предложенный в [RFC5357] обеспечивает возможность измерения круговых потерь в Internet. Однако в настоящее время нет показателя для круговых потерь, соответствующего модели [RFC2330].

В [RFC2681] сказано, что круговые измерения иногда могут сталкиваться с асимметричными путями. При наблюдении потерь в круговых измерениях зачастую возникает желание определить, на каком из двух направлений потерян пакет. В некоторых обстоятельствах это возможно. Метод измерения на круговом пути вызывает некоторые сложности при интерпретации односторонних результатов и пользователю следует помнить об этом.

В [RFC2681] также указано, что последовательное измерение путей в каждом направлении, указываемое как круговое измерение, может дать именно желаемые показатели. С другой стороны, может оказаться сложным определить круговые потери из односторонних измерений в каждом направлении, если заранее не согласовать метод соответствующих односторонних измерений.

Многие измерительные системы указывают статистику условного распределения задержки. Это приведено в [RFC3393], [RFC5481], [RFC6703]. В результате о потере пакетов нужно сообщать отдельно, в соответствии со стандартизованными показателями. Этот документ определяет такие показатели.

Дополнительная мотивация для показателей потери пакетов приведена в параграфе 1.1 [RFC2680].

## 1.2. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с RFC 2119 [RFC2119].

# *2. Область действия*

Этот документ определяет показатель круговых потерь на основе соглашений модели IPPM [RFC2330].

Документ определяет одиночное измерение, выборку и статистику, как в [RFC2330]. Модель [RFC2330] предназначена для активных методов. Хотя описанные показатели можно применить и к пассивным измерениям, рассмотрение пассивных измерений выходит за рамки нормативной части документа.

В документе также рассматривается вопрос вывода потерь в одном направлении из круговых измерений и приведены некоторые важные соображения.

# *3. Общие спецификации показателей кругового обхода*

Для снижения объёма избыточной информации в последующих параграфах с описаниями показателей здесь приведены сведения, относящиеся по меньшей мере к двум показателям. В этом разделе применяются такие же параграфы, как при описании отдельных показателей.

## 3.1. Type-P-*

Все показатели используют соглашение Type-P, как описано в [RFC2330]. Остальная часть имени уникальна для каждого показателя.

## 3.2. Параметры показателя

Src - IP- адрес хоста
Dst - IP- адрес хоста
T - время начала теста
Tf - время завершения теста

lambda - скорость в 1/сек (для потоков Пуассона)
incT - номинальная продолжительность интервала следования пакетов (от первого бита до первого бита, для периодических потоков)
T0 - время, которое должно случайно выбираться из интервала [T, T+dT] для запуска генерации пакетов и проведения измерений (для периодических потоков)
TstampSrc - время в линии (wire time) для пакета, измеренное в MP(Src) при отправке для Dst
TstampDst - время в линии, измеренное в MP(Dst), которое присваивается пакетам, прибывшим в «разумное» время (меньше Tmax)
Tmax - максимальное время ожидания прибытия пакетов в Src, достаточно большое, чтобы отличить задержку пакета от потери (отбрасывания)
M - общее число пакетов, переданных между T0 и Tf
N - общее число пакетов, полученных в Dst (переданы между T0 и Tf)
Type-P в соответствии с [RFC2330] включает любые поля, которые могут влиять на обработку пакета при прохождении через сеть.

## 3.3. Определение показателя

Сведения, относящиеся к конкретному показателю.

## 3.4. Единицы измерения

Единицы измерения являются логическими (1 или 0) при описании потери одного пакета, где 0 указывает успешную передачу пакета, 1 - потерю.

Единицы времени заданы в [RFC2330].

Другие единицы измерения при необходимости определяются в соответствующих параграфах (например, параграф 6.1 для Type-P-Round-trip-Loss-<Sample>-Ratio).

# *4. Показатель одиночного измерения потерь*

## 4.1. Имя показателя

Type-P-Round-trip-Loss

## 4.2. Параметры показателя

См. параграф 3.2.

## 4.3. Определение и единицы измерения

Type-P-Round-trip-Loss нужно представлять двоичными логическими значениями (или их эквивалентами) с учётом приведённых ниже условий.

Type-P-Round-trip-Loss = 0:

- Src передаёт первый бит пакета Type-P получателю Dst в момент TstampSrc;
- Dst получает этот пакет;
- Dst передаёт пакет Type-P обратно Src как можно быстрее (конечно меньше Tmax и достаточно быстро для предусмотренной цели);
- Src получает первый бит отражённого пакета до времени в линии TstampSrc + Tmax.

Type-P-Round-trip-Loss = 1:

- Src передаёт первый бит пакета Type-P получателю Dst в момент TstampSrc;
- после этого Src не получает последнего бита отражённого пакета до истечения момента TstampSrc + Tmax.

Возможными причинами установки Loss = 1 могут быть:

- Dst не получил пакет;
- Dst не передал пакет Type-P обратно Src
- Src не получил отражённого пакета Type-P от Dst.

Следуя прецеденту из параграфа 2.4 в [RFC2681], принимается упрощение, что круговые потери, измеренные между двумя хостами, равны, независимо от того, какой из хостов начинает тест

**`Type-P-Round-trip-Loss(Src->Dst->Src) = Type-P-Round-trip-Loss(Dst->Src->Dst)`**
(согласитесь, что это скромная плата за эффективность измерения).

Таким образом, каждое одиночное измерение (singleton) можно представить парой элементов, как показано ниже.

- TstampSrc - время в линии для пакета в Src (начало кругового обмена).
- L - 0 или 1 (или некоторый эквивалент), где L=1 указывает потерю, а L=0 - успешный круговой обход до момента TstampSrc + Tmax.

## 4.4. Обсуждение и другие детали

В [RFC2680] и [RFC2681] рассмотрены методы измерения, ошибки и погрешности, а также другие фундаментальные вопросы, которые не повторяются здесь. Мы добавляем рекомендацию относящуюся к процессу ответчика по «отправке пакета Type-P обратно Src как можно быстрее».

Отклик, который не был создан в интервале Tmax, не подходит для какого-либо реалистического теста и Src будет отбрасывать такие отклики. Ответчику, выполняющему типовое тестирование круговых потерь (связанное с тестирование производительности приложений вышележащего уровня), **следует** создавать не более 1 отклика в секунду. Неспособному выполнить это требование ответчику **следует** записать этот факт в системный журнал (log), чтобы оператор мог настроить должным образом нагрузку и приоритеты. Анализу временных меток [RFC5357], обнаружившему, что отклик не был создан своевременно, **следует** уведомить оператора, а тому **следует** приостановить тестирование ответчика, поскольку он может быть перегружен. Дополнительное рассмотрение измерений приведено в разделе 8.

# *5. Выборка для показателя круговых потерь*

На основе одиночного показателя Type-P-Round-trip-Loss определяется выборка таких одиночных измерений. Идея заключается в отборе конкретной связки параметров Src, Dst, Type-P и последующем определении выборки значения параметра TstampSrc. Это можно сделать несколькими способами, включая указанные ниже.

1. Пуассновская выборка. Псевдослучайный пуассоновский процесс потока для скорости lambda со значениями между T и Tf. Временной интервал между последовательными значениями TstampSrc будет средним значением 1/lambda в соответствии с параграфом 11.1.1 в [RFC2330].

2. Периодическая выборка. Периодический процесс потока с псевдослучайным временем запуска T0 между T и dT и номиналиным интервалом передачи пакетов incT в соответствии с [RFC3432].

В имени показателя переменную часть <Sample> **нужно** заменить процессом, служащим для определения выборки, используя один из упомянутых выше процессов или иной процесс, соответствующий критериям параграфа 11.1 в [RFC2330], детали которого **должны** быть включены в отчет.

## 5.1. Имя показателя

Type-P-Round-trip-Loss-<Sample>-Stream

## 5.2. Параметры показателя

См. параграф 3.2.

## 5.3. Определение и единицы измерения

На основе одного из методов определения интервала тестирования (выборки значений TstampSrc или иных параметров показателя) получается последовательность одиночных измерений Type-P-Round-trip-Loss, как определено в параграфе Section 4.3.

Потоку Type-P-Round-trip-Loss-<Sample>-Stream **нужно** быть последовательностью пар показанных ниже элементов.

- TstampSrc, как указано выше.
- L - 0 или 1 (или иной логический эквивалент), где L=1 указывает потерю, L=0 — успешную круговую доставку для истечения TstampSrc + Tmax.

Вместо <Sample> **нужно** указать Poisson, Periodic или подходящее обозначение иного метода выборки, как указано выше в параграфе 5.

## 5.4. Обсуждение и другие детали

В [RFC2680] и [RFC2681] широко рассмотрены методы измерений, ошибки и погрешности, а также друние фундаментальные вопросы, которые нет необходимости повторять здесь. Однако на момент выхода этих документов показатель переупорядочения пакетов [RFC4737] ещё не были определены и вопросы переупорядочения ещё не были решены в методологии IPPM.

В [RFC4737] сказано, что пакет, «запаздывающий» относительно порядка отправки, считается переупорядоченным. Например, когда пакеты приходят в порядке 4, 7, 5, 6, пакеты 5 и 6 являются переупорядоченными и они обычно не теряются при условии прибытия в течение некого разумного срока ожидания. Наличие переупорядочения на круговом пути оказывает некоторое влияние на измерения, как указано ниже.

1. Методам измерения следует продолжать ожидание пакетов в течение заданного времени, чтобы избежать объявления пакетов потерянными при наблюдении пропуска в номерах или иных ошибок.

2. Распределение времени одиночных измерений в выборках существенно изменено.

3. Исходный или отражённый поток может сталкиваться с нестабильностью пути и исходные условия могут отсутствовать.

Реализации измерений **должны** учитывать возможность переупорядочения пакетов для предотвращения связанных с этим ошибок в своих процессах.

# *6. Статистика круговых потерь*

В этом разделе рассмотрена первичная и общая статистика потерь. **Можно** применять также дополнительные варианты статистики и показателей, разработанные для потерь в одном направлении.

## 6.1. Type-P-Round-trip-Loss-<Sample>-Ratio

Для Type-P-Round-trip-Loss-<Sample>-Stream средним значением всех логических параметров (L) в потоке будет Type-P-Round-trip-Loss-<Sample>-Ratio. Это отношение указывается числом потерянных пакетов, поделенным на число круговых передач. Значение Type-P-Round-trip-Loss-<Sample>-Ratio является неопределённым для пустой выборки.

# 7. Круговые тесты и отчёты для одного направления

Здесь обсуждаются результаты, полученные с использованием архитектуры двухсторонних измерений, такой как TWAMP [RFC5357].

Процесс выборки для обратного пути (Dst->Src) является условным и зависит от прибытия пакета в Dst и корректной работы Dst по генерации отражённого пакета. Поэтому на выборку из обратного пути будут существенно влиять заметные потери на пути Src→Dst, делающие недействительной оценку производительности пути возврата (в плане потерь и возможно других показателей).

Кроме того, время выборки на обратном пути (Dst->Src) определяется случайным процессом, зависящим от исходного времени выборки (TstampSrc), односторонней задержки для успешного прибытия пакета в Dst и времени, потребного Dst для создания отражённого пакета. Поэтому на процесс выборки для пути возврата будет существенно влиять заметное изменение задержки на пути Src->Dst, делающее недействительной попытку оценки производительности обратного пути (в плане потерь и возможно других показателей).

Как отмечено в параграфе 5.4, переупорядочение пакетов возможно всегда. Кроме существенных вариаций задержки, обычно способствующих переупорядочению, изменение порядка на пути Src->Dst будет вызывать несовпадение порядковых номеров Dst по сравнению с номерами у источника. При реализации измерений это **должно** учитываться.

# 8. Измерение и калибровка

Перед выполнением измерений участвующие в них хосты **должны** быть настроены на передачу и приём тестовых пакетов выбранного Type-P. Стандартные протоколы измерений способны справиться с этой задачей [RFC5357], но достаточно любого надёжного метода (например, можно устранить проблемы, связанные с ICMP, которые рассмотрены в параграфе 2.6 [RFC2681], и выполнить требования параграфов 4.3 и 4.4 перед использованием ICMP).

Два важных свойства принимающего тестовые пакеты и возвращающего отклики на них хоста описаны в параграфе 4.2 [RFC5357]. Каждый полученный пакет **должен** вызывать отклик и отклики **должны** генерироваться как можно скорей. Это предполагает быстрое обслуживание буферов интерфейса и крайне редкое отбрасывание буферов. Эти свойства измерительного оборудования **должны** калиброваться в соответствии с параграфом 3.7.3 [RFC2679] при работе с заметным уровнем измерительной нагрузки (в соответствии с определением пользователя). **Должны** записываться как неожиданное отбрасывание пакетов, так и систематические и случайные ошибки и погрешности.

Отметим, что в параграфе 4.2.1 [RFC5357] указан метод сбора всех 4 значимых временных меток, требуемых для описания круговой задержки пакетов [RFC2681] и исключения времени обработки на отвечающем хосте. Эти сведения поддерживают измерение соответствующих односторонних задержек, встречающихся на круговом пути, что может выявить асимметрию путей или неожиданное время обработки на отвечающем узле.

# 9. Вопросы безопасности

## 9.1. Отказ в обслуживании (DoS)

Для этого показателя нужен поток пакетов, передаваемых от одного хоста (источник) к другому (получатель) через промежуточные сети. Этот метод можно использовать для организации DoS-атак, направленных на получателя и/или промежуточные сети.

Администраторам источника, получателя и промежуточных сетей следует заключить двух- или многосторонние соглашения о времени, продолжительности и частоте выполняемых выборок. Использование методов измерений сверх согласованных условий может приводить к незамедлительному отбрасыванию или отклонению пакетов, а также к другим процедурам, определенным затрагиваемыми сторонами.

## 9.2. Конфиденциальность данных пользователей

При активном использовании этого метода создаются потоки для выборки, а не отбираются пакеты пользователей, поэтому конфиденциальность данных не нарушается. При пассивных измерениях должны вноситься ограничения на просмотр содержимого пакетов (только заголовки). Поскольку данные пользователей могут временно сохраняться для анализа размера пакетов, **должны** приниматься меры по сохранению конфиденциальности этих сведений. В большинстве случаев хеширование обеспечит получение значений, подходящих для сравнения содержимого пакетов.

## 9.3. Влияние на показатели

Можно идентифицировать принадлежность пакета или потока пакетов к выборке и на основе этого обработать пакеты по-иному у получателя и/или в промежуточной точке (например, увеличивая или снижая задержку) для влияния на результаты измерений. Можно также создать дополнительные пакеты, которые будут выглядеть частью выборки показателей. Эти дополнительные пакеты будут вероятно сочтены дубликатами или за дубликаты будут приняты исходные пакеты (если они прибудут позже), что повлияет на результаты выборки.

Методы проверки подлинности и шифрования, такие как цифровые подписи **можно** применять в подходящих случаях для защиты от атак с вставкой трафика. Свойства аутентификации и шифрования рассмотрены в [RFC5357].

# 10. Взаимодействие с IANA

Показатели, определённые ранее в IETF, включены в реестр IANA IPPM Metrics Registry, однако этот процесс был прерван, когда структуру реестра сочли неадекватной и реестр был отменен [RFC6248].

Хотя показатели из этого документа могут рассматриваться в будущем для той или иной регистрации, в настоящий момент действий IANA не требуется.

# 11. Благодарности

Авторы благодарны Tiziano Ionta за внимательное рецензирование документа, результатом которого в первую очередь стали соображения об использовании протокола TWAMP [RFC5357] как примера метода. рецензии Adrian Farrel и Benoit Claise также способствовали ясности документа.

# 12. Литература

## 12.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2330] Paxson, V., Almes, G., Mahdavi, J., and M. Mathis, "Framework for IP Performance Metrics", RFC 2330, May 1998.

[RFC2679] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Delay Metric for IPPM", RFC 2679, September 1999.

[RFC2680] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Packet Loss Metric for IPPM", RFC 2680, September 1999.

[RFC2681] Almes, G., Kalidindi, S., and M. Zekauskas, "A Round-trip Delay Metric for IPPM", RFC 2681, September 1999.

[RFC3393] Demichelis, C. and P. Chimento, "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)", RFC 3393, November 2002.

[RFC3432] Raisanen, V., Grotefeld, G., and A. Morton, "Network performance measurement with periodic streams", RFC 3432, November 2002.

[RFC4737] Morton, A., Ciavattone, L., Ramachandran, G., Shalunov, S., and J. Perser, "Packet Reordering Metrics", RFC 4737, November 2006.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, October 2008.

## 12.2. Дополнительная литература

[RFC5481] Morton, A. and B. Claise, "Packet Delay Variation Applicability Statement", RFC 5481, March 2009.

[RFC6248] Morton, A., "RFC 4148 and the IP Performance Metrics (IPPM) Registry of Metrics Are Obsolete", RFC 6248, April 2011.

[RFC6703] Morton, A., Ramachandran, G., and G. Maguluri, "Reporting IP Network Performance Metrics: Different Points of View", RFC 6703, August 2012.

**Адреса авторов**

**Al Morton**
AT&T Labs
200 Laurel Avenue South
Middletown, NJ 07748
USA
Phone: +1 732 420 1571
Fax: +1 732 368 1192
EMail: acmorton@att.com
URI: http://home.comcast.net/~acmacm/

**Перевод на русский язык**

Николай Малых

nmalykh@protokols.ru