

## Support of the IEEE 1588 Timestamp Format in a Two-Way Active Measurement Protocol (TWAMP)

Поддержка меток формата IEEE 1588 в протоколе TWAMP

### Аннотация

В этом документе описана необязательная функция для протокола активных измерения, позволяющая применять метки времени в формате протокола точного времени (Precision Time Protocol), определённом в IEEE 1588v2 в качестве альтернативы используемым в настоящее время меткам протокола сетевого времени (Network Time Protocol).

### Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF<sup>1</sup> и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG<sup>2</sup>. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <http://www.rfc-editor.org/info/rfc8186>.

### Авторские права

Авторские права (Copyright (c) 2017) 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).

## Оглавление

1. Введение.....	1
1.1. Используемые соглашения.....	2
1.1.1. Сокращения.....	2
1.1.2. Уровни требований.....	2
2. Расширения OWAMP и TWAMP.....	2
2.1. Согласование формата меток при организации соединения OWAMP.....	2
2.2. Согласование формата меток при организации соединения TWAMP.....	3
2.3. Обновления OWAMP-Test и TWAMP-Test.....	3
2.3.1. Режим TWAMP Light.....	3
3. Взаимодействие с IANA.....	3
4. Вопросы безопасности.....	3
5. Нормативные документы.....	3
Благодарности.....	4
Адреса авторов.....	4

## 1. Введение

Протокол односторонних активных измерений (One-Way Active Measurement Protocol или OWAMP) [RFC4656] задаёт лишь формат меток времени NTP [RFC5905] для применения в протоколе OWAMP-Test. Протокол двухсторонних активных измерений (Two-Way Active Measurement Protocol или TWAMP) [RFC5357] принял формат пакетов OWAMP-Test и дополнил его форматом отражённых тестовых пакетов. Предполагается, что метки времени в пакетах отправителя и рефлектора используют 64-битовый формат NTP [RFC5905]. Протокол NTP при использовании в Internet обычно обеспечивает точность от 5 до 100 мсек. Проведённые недавно исследования показали, что 90% устройств обеспечивают точность лучше 100 мсек и 99% - лучше 1 сек. Следует отметить, что NTP синхронизирует часы плоскости управления, а не плоскости данных. Распределение времени внутри узла может поддерживаться независимым доменом NTP или через обмен между процессами в многопроцессорной распределённой системе. Любое из этих решений подвержено влиянию дополнительных задержек в очередях, негативно влияющих на точность часов в плоскости данных.

Протокол точного времени (Precision Time Protocol или PTP) [IEEE.1588] получил широкую поддержку с момента разработки OWAMP и TWAMP. В PTP использует поддержку в пути и другие механизмы, обеспечивающие точность в доли микросекунд. Протокол PTP сейчас поддерживается во многих реализациях скоростных машин пересылки, таким

<sup>1</sup>Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

<sup>2</sup>Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

образом, точность PTP является точностью часов в плоскости данных. Возможность использовать более точные часы в качестве источника временных меток при измерении производительности IP является одним из преимуществ этой спецификации. Другое преимущество реализуется за счёт упрощения аппаратной части в плоскости данных. Для поддержки OWAMP или TWAMP метки времени тестового протокола должны быть преобразованы из формата PTP в NTP. Для этого нужны ресурсы, применение микрокода или дополнительных элементов обработки, что всегда ограничено. Для решения проблемы этот документ предлагает расширения протоколов Control и Test, поддерживающие использование формата IEEE 1588v2 как необязательной альтернативы формату меток NTP.

Одной из целей этой спецификации является не только возможность конечным точкам сессии применять отличный от NTP формат меток, но и поддержка совместимости с узлами, которые ещё не реализуют это расширение.

## 1.1. Используемые соглашения

### 1.1.1. Сокращения

#### **NTP**

Network Time Protocol - протокол сетевого времени

#### **PTP**

Precision Time Protocol - протокол точного времени.

#### **TWAMP**

Two-Way Active Measurement Protocol - двухсторонний протокол активных измерений.

#### **OWAMP**

One-Way Active Measurement Protocol - односторонний протокол активных измерений.

### 1.1.2. 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.

## 2. Расширения OWAMP и TWAMP

Соединения OWAMP организуются по процедуре, заданной в параграфе 3.1 [RFC4656], а в TWAMP применяются дополнительные шаги, описанные в параграфе 3.1 [RFC5357]. В этих процедурах поле Modes служит для идентификации и выбора конкретных свойств связи. В то же время поле Modes признается и применяется как механизм расширения [RFC6038]. Новой функции требуется 1 битовая позиция для Server и Control-Client, чтобы согласовать формат меток времени, используемый в некоторых или всех тестовых сессиях, вызванных из этого управляющего соединения. Конечная точка соединения - Session-Sender и Session-Receiver (OWAMP) или Session-Reflector (TWAMP), - поддерживающая это расширения, **должна** быть способна интерпретировать форматы меток времени NTP и PTPv2. Если конечная точка не поддерживает это расширения, флаг PTPv2 Timestamp **должен** быть сброшен (0), поскольку он размещается в поле Must Be Zero. Если флаг PTPv2 Timestamp имеет значение 0, анонсирующий узел может использовать и интерпретировать лишь метки формата NTP. Реализации OWAMP и/или TWAMP **могут** включать элемент настройки для обхода процесса согласования и использования вместо него локально настроенных значений.

Использование флагов PTPv2 Timestamp рассматривается в последующих параграфах. Детали выделенных значений и битовые позиции описаны в разделе 3.

### 2.1. Согласование формата меток при организации соединения OWAMP

В OWAMP-Test [RFC4656] элементы Session-Receiver и/или Fetch-Client интерпретируют собранные метки времени. Таким образом, Server использует поле Modes для указания форматов, которые способен интерпретировать Session-Receiver. Control-Client проверяет значения, заданные сервером для форматов меток времени и устанавливает значения в поле Modes сообщения Set-Up-Response в соответствии с форматами меток, которые может использовать Session-Sender. Правила установки флагов временных меток в поле Modes сообщений Server Greeting и Set-Up-Response и их интерпретации приведены ниже.

- Если Session-Receiver поддерживает это расширения, то Server, организующий тестовую сессию от его имени, **должен** установить (1) флаг PTPv2 Timestamp в сообщении Server Greeting в соответствии с требованиями, приведёнными в параграфе 2. Расширения OWAMP и TWAMP. В ином случае флаг PTPv2 Timestamp сбрасывается (0) для индикации того, что Session-Receiver интерпретирует лишь формат NTP.
- Если Control-Client получает приветственное сообщение (greeting) со сброшенным флагом PTPv2 Timestamp, Session-Sender **должен** использовать для меток в тестовой сессии формат NTP, а клиенту Control-Client **следует** установить для флага PTPv2 Timestamp значение 0 в соответствии с [RFC4656]. Если Session-Sender не может использовать метки NTP, клиенту Control-Client **следует** закрыть соединение TCP, связанное с сессией OWAMP-Control.
- Если Control-Client получает приветственное сообщение с установленным флагом PTPv2 Timestamp и Session-Sender может создавать метки формата PTPv2, клиент Control-Client **должен** установить (1) флаг PTPv2 Timestamp в поле Modes сообщения Set-Up-Response, Session-Sender **должен** использовать формат PTPv2.
- Если Session-Sender не поддерживает это расширение и может создавать метки только в формате NTP, флаг PTPv2 Timestamp в поле Modes сообщения Set-Up-Response будет сбрасываться (0) как часть поля Must Be Zero и Session-Sender будет использовать формат NTP.

Если OWAMP-Control использует команды Fetch-Session, выбор и использование формата меток времени определяется локальным решением Session-Sender и Session-Receiver.

## 2.2. Согласование формата меток при организации соединения TWAMP

В TWAMP-Test [RFC5357] отправитель Session-Sender интерпретирует собранные метки времени. Поэтому в поле Modes сервер анонсирует форматы меток, которые Session-Reflector может использовать в сообщении TWAMP-Test. Выбор формата меток для использования Session-Sender определяется локальным решением. Control-Client проверяет поле Modes и устанавливает флаги меток для индикации формата, который будет использовать Session-Reflector. Правила установки и интерпретации флагов указаны ниже.

- Сервер **должен** установить (1) флаг PTPv2 Timestamp в приветственном сообщении, если Session-Reflector может создавать метки в формате PTPv2. В ином случае флаг PTPv2 Timestamp должен сбрасываться (0).
- Если флаг PTPv2 Timestamp в принятом сообщении Server Greeting сброшен (0), Session-Reflector не поддерживает это расширение и будет использовать формат NTP. Клиенту Control-Client **следует** сбросить (0) флаг PTPv2 Timestamp в сообщении Set-Up-Response в соответствии с [RFC4656].
- Control-Client **должен** установить (1) флаг PTPv2 Timestamp в поле Modes сообщения Set-Up-Response, если Server указал, что Session-Reflector может применять метки формата PTPv2. В противном случае флаг **должен** быть сброшен (0).
- Если флаг PTPv2 Timestamp в сообщении Set-Up-Response сброшен (0), это значит, что Session-Sender может интерпретировать лишь метки NTP, поэтому Session-Reflector **должен** использовать формат NTP. Если Session-Reflector не поддерживает формат NTP, **сервер** должен закрыть соединение TCP, связанное с сессией TWAMP-Control.

## 2.3. Обновления OWAMP-Test и TWAMP-Test

Участники тестовой сессии должны указать, какой формат меток времени они будут применять. В настоящее время для этого служит поле Z в Error Estimate, определённое в параграфе 4.1.2 [RFC4656]. Однако этот документ расширяет Error Estimate для указания формата собираемых меток в дополнение к оценке ошибки синхронизации. Эта спецификация также меняет семантику бита Z (поле между S и Scale fields) для указания формата Timestamp. Поле **должно** иметь значение 0 для 64-битового формата NTP и 1 для усечённого формата PTPv2.

Поэтому значение поля Z из Error Estimate, Sender Error Estimate (TWAMP) или Send Error Estimate (OWAMP) и Receive Error Estimate **не следует** игнорировать и оно **должно** использоваться при расчёте показателей задержки и её вариаций на основе собранных меток времени.

### 2.3.1. Режим TWAMP Light

Этот документ не задаёт способ информирования Session-Sender и Session-Reflector в режиме TWAMP Light об используемом формате меток времени. Предполагается, что может применяться, например, конфигурация, направляющая Session-Sender и Session-Reflector на использование формата меток в соответствии с их возможностями и правилами из параграфа 2.2.

## 3. Взаимодействие с IANA

Агентство IANA зарегистрировало PTPv2 Timestamp в реестре TWAMP-Modes [RFC5618].

Таблица 1. Новая возможность временных меток.			
Битовая позиция	Описание	Семантика	Документ
9	PTPv2 Timestamp Capability	Раздел 2	RFC 8186 (этот документ)

## 4. Вопросы безопасности

Использование определённого формата меток времени в тестовой сессии не создаёт дополнительной угрозы безопасности для хостов, взаимодействующих с OWAMP и/или TWAMP, как определено в [RFC4656] и [RFC5357], соответственно. Соображения безопасности, применимые к любому активному измерению в работающей сети, уместны и здесь. См. разделы «Вопросы безопасности» в [RFC4656] и [RFC5357].

## 5. Нормативные документы

- [IEEE.1588] IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE Std 1588-2008, DOI 10.1109/IEEESTD.2008.4579760.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](http://www.rfc-editor.org/info/rfc2119), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", [RFC 4656](http://www.rfc-editor.org/info/rfc4656), DOI 10.17487/RFC4656, September 2006, <<http://www.rfc-editor.org/info/rfc4656>>.
- [RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiary, "A Two-Way Active Measurement Protocol (TWAMP)", [RFC 5357](http://www.rfc-editor.org/info/rfc5357), DOI 10.17487/RFC5357, October 2008, <<http://www.rfc-editor.org/info/rfc5357>>.
- [RFC5618] Morton, A. and K. Hedayat, "Mixed Security Mode for the Two-Way Active Measurement Protocol (TWAMP)", [RFC 5618](http://www.rfc-editor.org/info/rfc5618), DOI 10.17487/RFC5618, August 2009, <<http://www.rfc-editor.org/info/rfc5618>>.
- [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, <<http://www.rfc-editor.org/info/rfc5905>>.
- [RFC6038] Morton, A. and L. Ciavattone, "Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features", [RFC 6038](http://www.rfc-editor.org/info/rfc6038), DOI 10.17487/RFC6038, October 2010, <<http://www.rfc-editor.org/info/rfc6038>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, [RFC 8174](http://www.rfc-editor.org/info/rfc8174), DOI 10.17487/RFC8174, May 2017, <<http://www.rfc-editor.org/info/rfc8174>>.

## **Благодарности**

Авторы признательны Ramanathan Lakshminathan и Suchit Bansal за дельные предложения. Спасибо также David Allan за тщательное рецензирование и вдумчивые комментарии.

## **Адреса авторов**

**Greg Mirsky**

ZTE Corp.

Email: [gregimirsky@gmail.com](mailto:gregimirsky@gmail.com)

**Israel Meilik**

Broadcom

Email: [israel@broadcom.com](mailto:israel@broadcom.com)

## **Перевод на русский язык**

Николай Малых

[nmalykh@protokols.ru](mailto:nmalykh@protokols.ru)