Internet Engineering Task Force (IETF)
Request for Comments: 8762
Category: Standards Track
ISSN: 2070-1721

G. Mirsky
G. Jun
ZTE Corp.
H. Nydell
Accedian Networks
R. Foote
Nokia

March 2020

Simple Two-Way Active Measurement Protocol

Простой протокол двухстороннего активного измерения STAMP

Аннотация

Этот документ описывает простой протокол двухстороннего активного измерения (Simple Two-way Active Measurement Protocol или STAMP), позволяющий измерять параметры производительности, такие как задержка, ее вариации и потеря пакетов в одном направлении или при обходе по кругу (туда и обратно).

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 7841.

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке https://www.rfc-editor.org/info/rfc8762.

Оглавление

1. Введение

Разработка и внедрение протокола двухстороннего активного измерения (Two-Way Active Measurement Protocol или TWAMP) [RFC5357] и его расширений (например, [RFC6038], где определяется симметричный размер для TWAMP)

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

принесли ценный опыт. Имеется несколько независимых реализаций TWAMP и TWAMP Light, которые развернуты и обеспечивают важные измерения рабочих параметров производительности.

В то же время наблюдается заметный интерес к использованию более простого механизма для активного мониторинга производительности, обеспечивающего детерминированное поведение и внутреннее разделение функций управления (фирменная настройка и «оркестровка») и тестирования. Недавняя работа Performance Measurement from IP Edge to Customer Equipment using TWAMP Light [BBF.TR-390] в рамках Broadband Forum показала, что взаимодействие между реализациями TWAMP Light затруднено по причине того, что устройство и работа TWAMP Light достаточно слабо описаны в [RFC5357]. В соответствии с [RFC8545] TWAMP Light включает подмножество функций TWAMP-Test. Таким образом, для получения полнофункционального инструментария для измерения потери и задержки пакетов требуется поддержка других приложений, например, для управления и защиты.

Этот документ определяет протокол активного измерения производительности (Simple Two-way Active Measurement Protocol или STAMP), который позволяет измерять в одном или обоих направлениях параметры производительности, включая задержку и ее вариации, а также потери пакетов. Поддержка некоторых необязательных расширения TWAMP, например, [RFC7750], обсуждается в [STAMP-OPTION].

2. Используемые соглашения

2.1. Сокращения

STAMP
: Simple Two-way Active Measurement Protocol (простой протокол активных двухсторонних измерений).

NTP
: Network Time Protocol (протокол сетевого времени).

PTP
: Precision Time Protocol (протокол точного времени).

HMAC
: Hashed Message Authentication Code (хэшированный код аутентификации сообщения).

OWAMP
: One-Way Active Measurement Protocol (протокол односторонних активных измерений).

TWAMP
: Two-Way Active Measurement Protocol (протокол двухсторонних активных измерений).

MBZ
: Must be Zero (должно быть 0).

PDU
: Protocol Data Unit (блок данных протокола).

2.2. 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), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

3. Операции и управление измерениями STAMP

На рисунке 1 представлены отправитель Session-Sender и рефлектор Session-Reflector измерительной сессии STAMP, которая в этом документе называется просто сессией STAMP. Сессия представляет собой двухсторонних поток пакетов между одним конкретным отправителем и одним конкретным рефлектором в течение определенного времени. Настройка и управления для отправителя, рефлектора и сессии STAMP могут выполняться разными способами, рассмотрение которых выходит за рамки документа. Примерами могут служить командный интерфейс CLI (Command Line Interface), система поддержки операций телекоммуникационного сервиса (Operational Support System или OSS, Business Support System или BSS), SNMP, и контроллеры программно определяемых сетей (Software-Defined Networking илм SDN) на основе NETCONF и YANG.

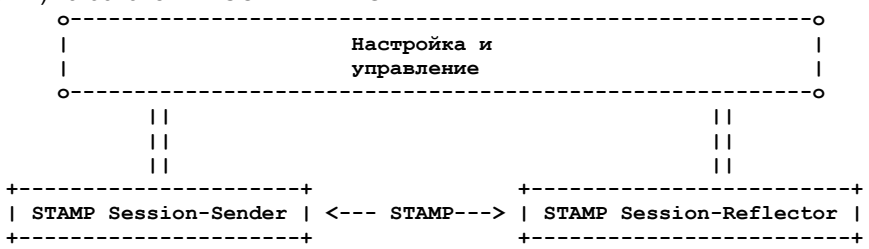

Рисунок 1. Эталонная модель STAMP.

4. Теория операций

Отправитель STAMP Session-Sender передает тестовые пакеты по протоколу UDP в направлении STAMP Session-Reflector. Рефлектор получает пакеты от Session-Sender и действует в соответствии с конфигурацией. Два режима работы Session-Reflector характеризуют ожидаемое поведение и измеряемые параметры.

Stateless - без учета состояния
: STAMP Session-Reflector не поддерживает состояние для теста и использует значение порядкового номера в принятых пакетах в качестве поля Sequence Number отраженных пакетов. В результате порядковые номера в пакетах отправителя и рефлектора совпадают и в этом режиме можно обнаружить лишь потерю пакетов на круговом пути.

Stateful - с учетом состояния
: STAMP Session-Reflector поддерживает состояние теста, что позволяет отправителю определить направление, на котором теряются пакеты, используя комбинацию порядковых номеров в своих пакетах и откликах. Для этого

STAMP Session-Reflector **должен** поддерживать состояние в каждой настроенной сессии STAMP-Test для однозначной привязки тестовых пакетов к экземпляру сессии и добавление порядкового номера в пакеты STAMP-Test с увеличением на 1 для каждого пакета в сессии.

STAMP поддерживает работу с аутентификацией и без нее. Тестовые пакеты без аутентификации (параграфы 4.2.1 и 4.3.1) обеспечивают взаимодействие между STAMP и TWAMP Light, как описано в параграфе 4.6.

По умолчанию STAMP использует симметричные пакеты, т. е. размер пакетов отправителя и рефлектора совпадает.

4.1. Номера портов UDP в тестах STAMP

Отправитель STAMP **должен** использовать порт UDP 862 (TWAMP-Test Receiver) в качестве принятого по умолчанию целевого порта UDP. Реализация STAMP на стороне Session-Sender **должна** быть способна использовать номера портов назначения из диапазонов User Ports (Registered Ports) и Dynamic Ports (Private or Ephemeral Ports), заданных в [RFC6335]. Перед использованием порта из диапазона User Ports **должно** быть внимательно рассмотрено влияние на сеть и согласовано применение со всеми пользователями домена, где планируется тестирование.

По умолчанию реализация STAMP Session-Reflector **должна** принимать пакеты STAMP-Test на порту UDP 862. Поддерживающая эту спецификацию реализация Session-Reflector **должна** быть способна задать номер порта для приема пакетов STAMP-Test из диапазонов User Ports и Dynamic Ports, заданных в [RFC6335]. STAMP определяет два формата тестовых пакетов, один из которых применяет Session-Sender, другой - Session-Reflector.

4.2. Поведение и формат пакетов отправителя

STAMP Session-Reflector по умолчанию поддерживает симметричный размер тестовых пакетов, как указано в разделе 3 [RFC6038]. Базовый отраженный пакет включает информацию от рефлектора, поэтому должен быть больше. Для поддержки симметрии между базовыми пакетами STAMP в базовый пакет STAMP Session-Sender включено поле нулей MBZ с учетом размера базового отраженного пакета STAMP. Поэтому базовый пакет STAMP Session-Sender имеет минимальный размер 44 октета в режиме без аутентификации (рисунок 2) и 112 октетов в режиме с аутентификацией (рисунко 4). Генерация пакетов STAMP переменного размера описана в [STAMP-OPTION].

4.2.1. Формат пакетов в режиме без аутентификации

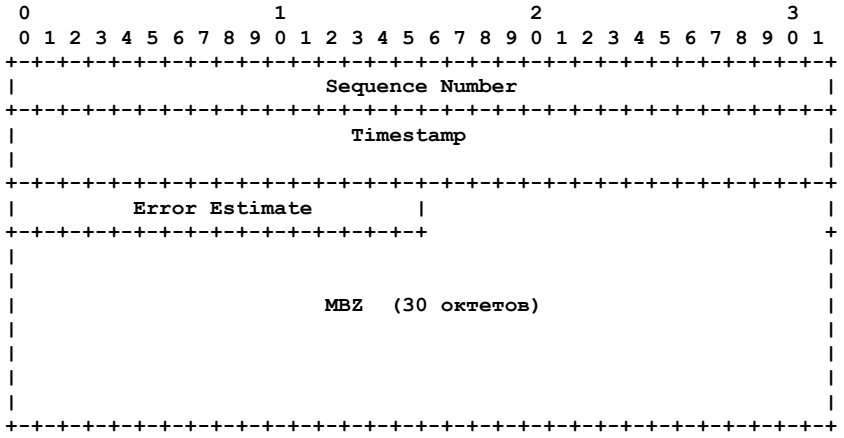

Рисунок 2. Формат пакета отправителя в режиме без аутентификации.

Sequence Number

4-октетное поле порядкового номера. Для каждой новой сессии значения начинается с 0 и инкрементируется в каждом переданном пакете.

Timestamp

8-октетное поле с временной меткой. Узел STAMP **должен** поддерживать 64-битовые метки протокола сетевого времени (Network Time Protocol или NTP) версии 4 [RFC5905], формат которых задан в [RFC5357]. Узел STAMP **может** поддерживать метки протокола IEEE 1588v2 Precision Time Protocol (PTP), усеченные до 64 битов [IEEE.1588.2008] и применяемые в [RFC8186]. Использование конкретного формата NTP или PTP задается в конфигурации Session-Sender или для конкретной сессии.

Error Estimate

2-октетное поле, формат которого показан на рисунке 3.

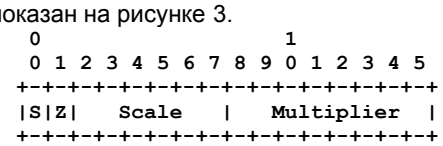

Рисунок 3. Формат оценки ошибок.

Поля S, Scale и Multiplier интерпретируются в соответствии с параграфом 4.1.2 в [RFC4656], поле Z - в соответствии с параграфом 2.3 в [RFC8186]:

0

64-битовые временные метки NTP.

1

усеченные временные метки PTPv2.

По умолчанию отправитель и рефлектор STAMP используют формат временных меток NTP (Z = 0). Оператор с помощью функции настройки или управления **может** задать использование усеченного формата меток PTPv2 (Z = 1). Отметим, что поддерживающую эту спецификацию реализацию Session-Sender **можно** настроить на использование формата PTPv2, даже когда в Session-Reflector задан формат NTP.

MBZ

В пакетах Session-Sender без аутентификации имеет размер 30 октетов. Поле **должно** быть заполнено нулями при передаче и **должно** игнорироваться на приемной стороне.

4.2.2. Формат пакетов в режиме с аутентификацией

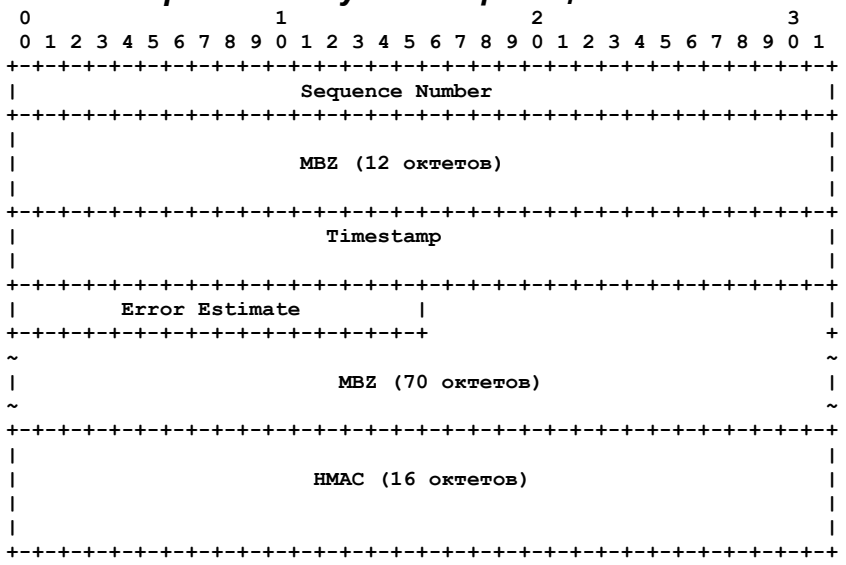

Рисунок 4. Формат пакета отправителя в режиме с аутентификацией.

Определения полей совпадают с режимом без аутентификации, как указано в параграфе 4.2.1. Поля MBZ служат для выравнивания пакетов по размеру, кратному 16 октетам. Поля **должны** заполняться нулями при передаче и **должны** игнорироваться при получении. Оба поля MBZ учитываются при расчете HMAC [RFC2104]. Пакет включает также хэш-код HMAC в конце PDU. Принятое по умолчанию использование поля HMAC описано в параграфе 4.4.

4.3. Поведение и формат пакетов рефлектора

Session-Reflector принимает пакет STAMP-Test и проверяет его. Если базовый пакет STAMP-Test действителен, поддерживающая эту спецификацию реализация Session-Reflector готовит и передает отраженный тестовый пакет, симметричный полученному от Session-Sender, копируя в него содержимое за пределами размера базового пакета STAMP (параграф 4.2).

4.3.1. Формат пакетов в режиме без аутентификации

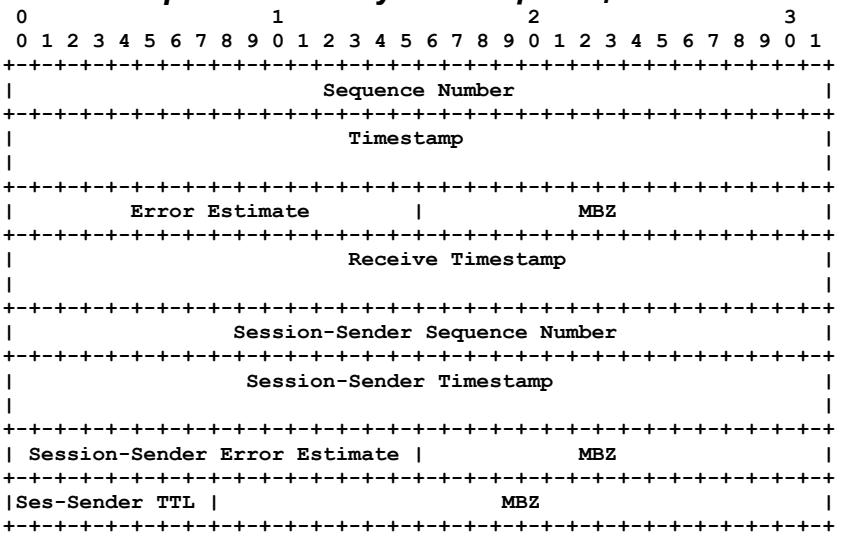

Рисунок 5. Формат пакета рефлектора в режиме без аутентификации.

Sequence Number

4-октетное поле, значение которого устанавливается в соответствии с режимом STAMP Session-Reflector:

- в режиме без поддержки состояний копируется одноименное поле из принятого пакета STAMP-Test;
- в режиме с учетом состояния Session-Reflector считает переданные пакеты STAMP-Test, начиная с 0 и увеличивая на 1 номер в каждом последующем пакете для каждой сессии. Значение счетчика помещается в поле Sequence Number.

Timestamp

Receive Timestamp

8-октетные поля в формате NTP или PTPv2, указанном флагом Z в поле Error Estimate, как указано в параграфе 4.2.1. Receive Timestamp указывает время приема тестового пакета рефлектором, Timestamp - время начала передачи рефлектором ответного тестового пакета.

Error Estimate

Размер и описание полей соответствуют указанным в параграфе 4.2.1. Поле относится к Timestamp и Receive Timestamp.

Session-Sender Sequence Number, Session-Sender Timestamp, Session-Sender Error Estimate

Копии соответствующих полей из пакета STAMP-Test от Session-Sender.

Session-Sender TTL

1-октетное значение, содержащее копию поля IPv4 TTL (или IPv6 Hop Limit) из принятого пакета STAMP-Test.

MBZ

Служит для выравнивания полей по 4-октетной границе. Поля **должны** заполняться нулями при передаче и **должны** игнорироваться при получении.

4.3.2. Формат пакетов в режиме с аутентификацией

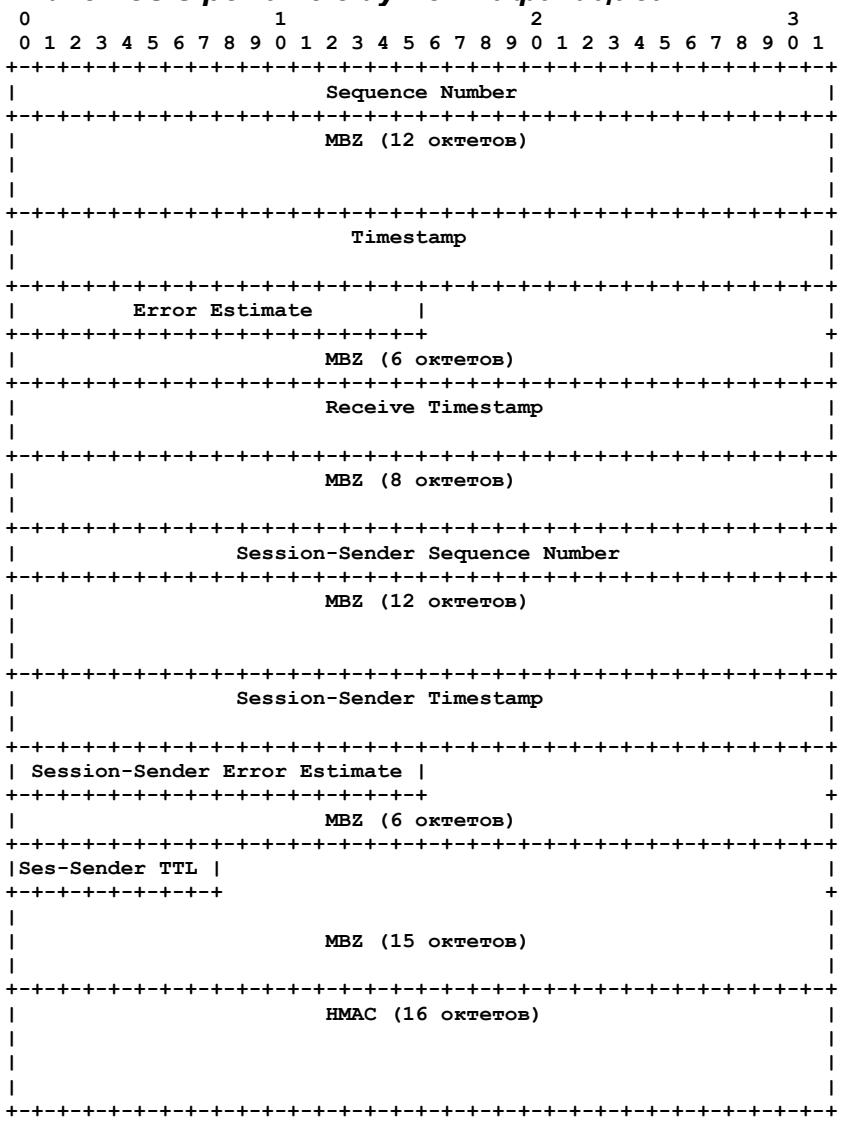

Рисунок 6. Формат пакета рефлектора в режиме с аутентификацией.

Определения полей совпадают с режимом без аутентификации, как указано в параграфе 4.3.1. Поля MBZ служат для выравнивания пакетов по размеру, кратному 16 октетам. Поля **должны** заполняться нулями при передаче и **должны** игнорироваться при получении. Оба поля MBZ учитываются при расчете HMAC [RFC2104]. Пакет включает также хэш-код HMAC в конце PDU. Принятое по умолчанию использование поля HMAC описано в параграфе 4.4.

4.4. Защита целостности в STAMP

Режим с аутентификацией обеспечивает защиту каждого сообщения STAMP путем добавления хэш-кода HMAC. STAMP использует HMAC-SHA-256 с отсечкой до 128 битов (как в IPsec [RFC4868]), поэтому поле HMAC имеет размер 16 октетов. При расчете HMAC используются первые 6 блоков (96 октетов). В HMAC применяются свои ключи, которые могут быть уникальными для каждой сессии STAMP-Test. Механизм распространения ключей и управления ими выходит за рамки спецификации. Одним из вариантов является использование оркестратора для настройки ключей HMAC на основе модели данных YANG STAMP [STAMP-YANG]. Значение HMAC **должно** проверяться как можно раньше, чтобы предотвратить распространение поврежденных данных.

В будущих спецификациях может быть задано применение более совершенных криптографических алгоритмов и возможно обновление модели данных YANG STAMP [STAMP-YANG].

4.5. Защита конфиденциальности в STAMP

Если нужна конфиденциальность STAMP, в сессии STAMP-Test **должен** применяться защищенный транспорт. Например, пакеты STAMP могут передаваться через выделенный туннель IPsec или использовать общий туннель с потоком, для которого выполняется мониторинг. Защиту конфиденциальности может также обеспечить протокол Datagram Transport Layer Security (DTLS).

4.6. Взаимодействие с TWAMP Light

Одним из важных требований к STAMP является возможность взаимодействия с устройствами TWAMP Light. Поскольку в STAMP и TWAMP применяются разные алгоритмы для режима с аутентификацией (HMAC-SHA-256 и HMAC-SHA-1), такое взаимодействие возможно лишь в режиме без аутентификации. Здесь возможны два варианта:

- STAMP Session-Sender и TWAMP Light Session-Reflector;
- TWAMP Light Session-Sender и STAMP Session-Reflector.

В первом случае Session-Sender может не знать, что рефлектор не поддерживает STAMP. Например, TWAMP Light Session-Reflector может не поддерживать работу через порт UDP 862, как указано в [RFC8545]. Поэтому раздел 4 позволяет применять иной порт в STAMP Session-Sender. Если используется какое-либо из расширений STAMP, рефлектор TWAMP Light будет видеть его как поле Packet Padding.

Во втором варианте, если TWAMP Light Session-Sender не поддерживает использование порта UDP 862, система управления тестом **должна** задать для STAMP Session-Reflector другой порт UDP в соответствии с разделом 4. Рефлектор **должен** использовать принятый по умолчанию формат временных меток NTP.

STAMP Session-Reflector, поддерживающий эту спецификацию, будет передавать базовый пакет (рисунок 5) при получении пакета, размер которого меньше принятой в STAMP базы. Если принятый от TWAMP Session-Sender пакет больше базового пакета STAMP, поддерживающий эту спецификацию рефлектор будет копировать оставшуюся часть пакета для передачи отраженного пакета симметричного размера.

5. Вопросы эксплуатации

Протокол STAMP предназначен для использования в действующих сетях, чтобы позволить оператору оценить соглашения об уровне обслуживания на основе задержки пакетов, ее вариаций и потери пакетов. При использовании STAMP через Internet, особенно при передаче пакетов STAMP-Test с номером целевого порта UDP из диапазона User Ports, **должно** быть тщательно проанализировано возможное влияние пакетов STAMP-Test. Каждый случай использования STAMP **должен** согласовываться между пользователями узлов Session-Sender и Session-Reflector до начала сессии STAMP-Test.

Использование общеизвестного номера целевого порта UDP в пакетах STAMP-Test, передаваемых от Session-Sender, не будет препятствовать измерениям в среде с множеством равноценных путей (ECMP) и приведенный в параграфе 5.3 [RFC8545] анализ полностью применим к STAMP.

6. Взаимодействие с IANA

Этот документ не требует действий IANA.

7. Вопросы безопасности

[RFC5357] не указывает вопросы безопасности, связанные с TWAMP-Test, но ссылается на вопросы безопасности, отмеченные для OWAMP в [RFC4656]. Поскольку OWAMP и TWAMP включают компоненты плоскостей данных и управления, для STAMP применимы лишь вопросы безопасности, рассмотренные для OWAMP-Test в параграфах 6.2 и 6.3 [RFC4656].

STAMP использует общеизвестный номер порта UDP, выделенный для получателя OWAMP-Test и TWAMP-Test. Таким образом, вопросы безопасности и меры по снижению риска атак с использованием зарегистрированного порта, указанные в разделе 6 [RFC8545], полностью применимы для STAMP. Поскольку управление и поддержка STAMP-Test полностью выходят за рамки этой спецификации, задаются лишь базовые требования.

Для смягчения возможных атак при управлении и поддержке сессий STAMP-Test **должен** применяться защищенный транспорт.

Нагрузка сети пакетами STAMP-Test **должна** внимательно оцениваться, а возможное влияние на имеющиеся службы **должно** тщательно анализироваться до начала тестирования. В параграфе 3.1.5 [RFC8085] даны рекомендации по обработке сетевой нагрузки для протоколов на основе UDP. Хотя характеристики тестового трафика зависят от цели тестирования, настоятельно рекомендуется оставаться в пределах, заданных [RFC8085].

Использование HMAC-SHA-256 в режиме с аутентификацией защищает целостность данных в пакетах STAMP-Test.

8. Литература

8.1. Нормативные документы

[IEEE.1588.2008] IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE Standard 1588, July 2008.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <https://www.rfc-editor.org/info/rfc2104>.

[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>.

[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>.

[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>.

[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>.

[RFC6038] Morton, A. and L. Ciavattone, "Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features", RFC 6038, DOI 10.17487/RFC6038, October 2010, <https://www.rfc-editor.org/info/rfc6038>.

[RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", BCP 165, RFC 6335, DOI 10.17487/RFC6335, August 2011, <https://www.rfc-editor.org/info/rfc6335>.

[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>.

[RFC8186] Mirsky, G. and I. Meilik, "Support of the IEEE 1588 Timestamp Format in a Two-Way Active Measurement Protocol (TWAMP)", RFC 8186, DOI 10.17487/RFC8186, June 2017, <https://www.rfc-editor.org/info/rfc8186>.

[RFC8545] Morton, A., Ed. and G. Mirsky, Ed., "Well-Known Port Assignments for the One-Way Active Measurement Protocol (OWAMP) and the Two-Way Active Measurement Protocol (TWAMP)", RFC 8545, DOI 10.17487/RFC8545, March 2019, <https://www.rfc-editor.org/info/rfc8545>.

8.2. Дополнительная литература

[BBF.TR-390] Broadband Forum, "Performance Measurement from IP Edge to Customer Equipment using TWAMP Light", TR-390 Issue 1, May 2017.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, DOI 10.17487/RFC4868, May 2007, <https://www.rfc-editor.org/info/rfc4868>.

[RFC7750] Hedin, J., Mirsky, G., and S. Baillargeon, "Differentiated Service Code Point and Explicit Congestion Notification Monitoring in the Two-Way Active Measurement Protocol (TWAMP)", RFC 7750, DOI 10.17487/RFC7750, February 2016, <https://www.rfc-editor.org/info/rfc7750>.

[RFC8085] Eggert, L., Fairhurst, G., and G. Shepherd, "UDP Usage Guidelines", BCP 145, RFC 8085, DOI 10.17487/RFC8085, March 2017, <https://www.rfc-editor.org/info/rfc8085>.

[STAMP-OPTION] Mirsky, G., Xiao, M., Nydell, H., Foote, R., Masputra, A., and E. Ruffini, "Simple Two-way Active Measurement Protocol Optional Extensions", Work in Progress, Internet-Draft, draft-ietf-ippm-stamp-option-tlv-03[1], 21 February 2020, <https://tools.ietf.org/html/draft-ietf-ippm-stamp-option-tlv-03>.

[STAMP-YANG] Mirsky, G., Xiao, M., and W. Luo, "Simple Two-way Active Measurement Protocol (STAMP) Data Model", Work in Progress, Internet-Draft, draft-ietf-ippm-stamp-yang-05, 25 October 2019, <https://tools.ietf.org/html/draft-ietf-ippm-stamp-yang-05>.

Благодарности

Авторы выражают свою признательность Jose Ignacio Alvarez-Hamelin и Brian Weis за их глубокое понимание безопасности и защиты отождествлений, а также за множество полезных и важных предложений. Спасибо David Ball, Rakesh Gandhi и Xiao Min за их рецензии и полезные комментари.

Адреса авторов

Greg Mirsky
ZTE Corp.
Email: gregimirsky@gmail.com

Guo Jun
ZTE Corp.
68# Zijinghua Road
Nanjing
Jiangsu, 210012
China
Phone: +86 18105183663
Email: guo.jun2@zte.com.cn

Henrik Nydell
Accedian Networks
Email: hnydell@accedian.com

Richard Foote
Nokia
Email: footer.foote@nokia.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1]Работа опубликована в RFC 8972. *Прим. перев.*