

Internet Engineering Task Force (IETF)
Request for Comments: 8545
Updates: 4656, 5357
Category: Standards Track
ISSN: 2070-1721

A. Morton, Ed.
AT&T Labs
G. Mirsky, Ed.
ZTE Corp.
March 2019

Well-Known Port Assignments for the One-Way Active Measurement Protocol (OWAMP) and the Two-Way Active Measurement Protocol (TWAMP)

Назначение общеизвестных портов для протоколов OWAMP и TWAMP

Аннотация

Этот документ содержит мотивацию и описание переназначения общеизвестных портов для протоколов односторонних (One-Way Active Measurement Protocol или OWAMP) и двухсторонних активных измерений (Two-Way Active Measurement Protocol или TWAMP) при управлении и выполнении измерений. Документ разъясняет также состав и смысл названий для этих стандартов в отрасли.

Этот документ обновляет RFC 4656 и RFC 5357 в части назначения общеизвестных портов UDP, а также уточняет полный состав протоколов OWAMP и TWAMP для отрасли.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF¹ и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG². 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 <https://www.rfc-editor.org/info/rfc8545>.

Авторские права

Copyright (c) 2019. Авторские права 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 Revised BSD License).

Оглавление

1. Введение.....	1
2. Уровни требований.....	2
3. Область действия.....	2
4. Определения и основы.....	2
5. Общеизвестные номера портов.....	2
5.1. Влияние на протокол TWAMP-Control.....	2
5.2. Влияние на протокол OWAMP-Control.....	3
5.3. Влияние на протоколы OWAMP-Test и TWAMP-Test.....	3
6. Вопросы безопасности.....	3
7. Взаимодействие с IANA.....	3
8. Литература.....	3
8.1. Нормативные документы.....	3
8.2. Дополнительная литература.....	4
Приложение А. Основы TWAMP Light.....	4
Благодарности.....	4
Участники работы.....	4
Адреса авторов.....	4

1. Введение

Рабочая группа IETF IPPM (IP Performance Metrics — параметры производительности IP) разработала исходный протокол OWAMP, описанный в [RFC4656]. Продолжение работы по поддержке тестирования привело к разработке протокола TWAMP, описанного в [RFC5357]. Оба протокола OWAMP и TWAMP требуют реализации протоколов управления и согласования режима (OWAMP-Control и TWAMP-Control) на основе надёжного транспорта TCP (включая настройку защиты и вывод ключей). Протоколы управления обеспечивают настройку и поддержку сеансов тестирования с применением связанных протоколов тестирования (OWAMP-Test и TWAMP-Test) с транспортом UDP.

IETF признает значимость выделения общеизвестного порта UDP для протоколов OWAMP-Test и TWAMP-Test, а также возможность выполнить это путём переназначения портов.

¹Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

²Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

2. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

3. Область действия

У этого документа две задачи (1) заново выделить общеизвестные порты UDP для протоколов тестирования и соответствующих документов Standards Track (OWAMP и TWAMP) и (2) уточнить назначение и состав названий протоколов для отрасли. Документ обновляет [RFC4656] и [RFC5357] в части назначения общеизвестных портов UDP.

4. Определения и основы

В этом документе определены основные требования и уточнён требуемый состав протоколов OWAMP и TWAMP Standards Track.

OWAMP-Control

Протокол, заданный в разделе 3 [RFC4656].

OWAMP-Test

Протокол, заданный в разделе 4 [RFC4656].

Описание OWAMP приведено в выдержке из параграфа 1.1 в [RFC4656]: «OWAMP фактически состоит из двух связанных протоколов – OWAMP-Control и OWAMP-Test». Похожее предложение приведено в разделе 2 [RFC4656]. Во избежание сомнений реализация OWAMP-Control и OWAMP-Test является **обязательной** для Standards Track OWAMP, как указано в [RFC4656] (в согласованной трактовке термина «состоит» в разных словарях).

TWAMP-Control

Протокол, заданный в разделе 3 [RFC5357].

TWAMP-Test

Протокол, заданный в разделе 4 [RFC5357].

Описание TWAMP приведено в выдержке из параграфа 1.1 в [RFC5357]: «Подобно OWAMP [RFC4656], протокол TWAMP фактически состоит из двух связанных протоколов – TWAMP-Control и TWAMP-Test». Во избежание сомнений реализация TWAMP-Control и TWAMP-Test является **обязательной** для Standards Track TWAMP, как указано в [RFC5357] (в согласованной трактовке термина «состоит» в разных словарях).

Идея TWAMP Light описана в Приложении I ("TWAMP Light (Informative)") к [RFC5357]. TWAMP Light включает неуказанный протокол управления в сочетании с протоколом TWAMP-Test protocol. В [RFC5357] идея TWAMP Light была представлена в Приложении I, поскольку TWAMP Light не соответствует требованиям к протоколам IETF (нет спецификации для согласования форм работы и обязательных для реализации функций защиты), как указано в Приложении A к этому документу. См. также [LarsAD] и [TimDISCUSS].

Поскольку идея TWAMP Light включает TWAMP-Test, считается разумным в будущих версиях TWAMP-Test применять общеизвестный порт UDP (указан в этом документе). Очевидно, что идея TWAMP Light предусматривает множество компонентов и коммуникационных возможностей за рамками TWAMP-Test (например, реализацию требований безопасности), иначе Приложение I к [RFC5357] состояло бы из одного предложения (приравнивание TWAMP Light к TWAMP-Test).

5. Общеизвестные номера портов

Исходно для протоколов управления, являющихся важными компонентами Standards Track OWAMP и TWAMP, были выделены общеизвестные порты TCP и UDP. Поскольку для OWAMP-Control и TWAMP-Control требуется транспорт TCP, эти протоколы не могут работать с назначенными изначально портами UDP. Однако сессии OWAMP-Test и TWAMP-Test используют транспорт UDP.

В соответствии с этим документом агентство IANA переназначило общеизвестный порт UDP для протокола тестирования вместо протокола управления (см. раздел 7). Использование этого порта UDP **необязательно** для Standards Track OWAMP и TWAMP. Оно может упростить некоторые операции за счёт доступности общеизвестного порта для протоколов тестирования или при использовании этого порта по умолчанию в будущих спецификациях, включающих TWAMP-Test. Например, спецификация [TR-390] определяет тестирование на пользовательских границах (customer edge) сетей IP и соответствующие реализации выиграют от предоставления общеизвестного порта UDP.

5.1. Влияние на протокол TWAMP-Control

В параграфе 3.5 [RFC5357] подробно описан процесс согласования номера Receiver Port, через который TWAMP Session-Reflector будет передавать и принимать пакеты TWAMP-Test (см. цитату ниже). Control-Client, действующий от имени Session-Sender, предлагает номер Receiver Port из диапазона Dynamic range [RFC6335].

Receiver Port указывает желаемый порт UDP, в который Session-Sender будет направлять пакеты TWAMP-Test (порт, запрошенный у Session-Reflector для приёма пакетов). Receiver Port также является портом UDP, из которого Session-Reflector будет передавать пакеты TWAMP-Test (Session-Reflector использует один порт UDP для передачи и приёма).

Возможно, что предложенный номер Receiver Port будет недоступен, например, выделен для другой сессии. Для таких случаев этот документ обновляет последний абзац параграфа 3.5 в [RFC5357] в соответствии с Erratum ID 1587 (<https://www.rfc-editor.org/errata/eid1587>), как показано ниже.

... Server на стороне Session-Reflector **может** предложить для этой сессии доступный порт в поле Port. Control-Client воспринимает этот порт и создаёт сообщение Session-Request с подходящими параметрами или не принимает его и использует поле Accept для информирования Control-Client об отказе или ошибке (в этом случае серверу **недопустимо** предлагать другой порт и поле Port **должно** иметь значение 0).

Control-Client, поддерживающий выделенный TWAMP-Test Receiver Port (раздел 7), **может** использование этого порта в команде Request-TW-Session. Если Server не поддерживает выделенный TWAMP-Test Receiver Port, он передаёт доступный номер порта в сообщении Accept-Session с полем Accept = 0. таким образом, применение выделенного порта TWAMP Receiver Port совместимо с имеющимися решениями TWAMP-Control на основе [RFC5357]. Разумеется, использование порта UDP из диапазона Dynamic Ports [RFC6335] поможет избежать ситуаций, когда Control-Client или Server уже использует предложенный порт.

5.2. Влияние на протокол OWAMP-Control

Как указано выше, клиент OWAMP-Control поддерживающий использование выделенного OWAMP-Test Receiver Port (раздел 7), **может** запросить применение этого порта в команде Request-Session. Если Server не поддерживает выделенный OWAMP-Test Receiver Port (или порт недоступен), он передаёт другой номер порта в сообщении Accept-Session с полем Accept = 0. Дальнейший обмен происходит в соответствии со спецификацией.

5.3. Влияние на протоколы OWAMP-Test и TWAMP-Test

Протоколы OWAMP-Test и TWAMP-Test могут служить для измерения параметров производительности IP в средах с несколькими равноценными путями (Equal-Cost Multipath или ECMP). Хотя алгоритмы распределения потоков IP по доступным путям не стандартизованы, чаще всего для этого используется квинтет из адресов IP отправителя и получателя, типа протокола и номеров портов у отправителя и получателя. При попытке отслеживать разные пути в сети ECMP достаточно менять лишь один из этих параметров. Таким образом, повторное выделение порта не окажет негативного влияния на возможность организации одновременных тестовых сессий OWAMP/TWAMP между одной парой точек для разных путей в сети ECMP с выделенным заново номером порта UDP в качестве Receiver Port, так как использование этого порта является необязательным.

6. Вопросы безопасности

Вопросы безопасности, связанные с активными измерениями на «живых» путях, применимы и здесь (см. [RFC4656] и [RFC5357]).

В части приватности вовлечённых в тестирование (в том числе тех, чей трафик измеряется) объем доступных для отслеживания конфиденциальных сведений существенно сокращается при использовании активных методов, рассматриваемых здесь. С пассивными наблюдениями пользовательского трафика в измерительных целях связано много рисков приватности. Читателям рекомендуется обратиться к рассмотрению вопросов безопасности при крупномасштабных измерениях производительности широкополосных сетей (Large-Scale Measurement of Broadband Performance или LMAP) [RFC7594], где рассмотрены активные и пассивные измерения.

Зарегистрированный порт UDP в качестве Receiver Port для OWAMP-Test и TWAMP-Test может стать целью атак с отказом в обслуживании (denial of service или DoS) или перехвата и изменения с участием человека (man-in-the-middle или MITM). Для повышения защиты от DoS-атак рекомендуется:

- фильтровать доступ к OWAMP/TWAMP Receiver Port с помощью списков контроля доступа;
- использовать не маршрутизируемые (глобально) адреса IP для OWAMP/TWAMP Session-Reflector.

В MITM-атаке злоумышленник пытается изменять пакеты OWAMP-Test/TWAMP-Test для искажения результатов измерений. Однако реализация может использовать режим с проверкой подлинности (authenticated mode) для обнаружения подмены данных. Кроме того, реализация может использовать режим с шифрованием (encrypted mode) для предотвращения просмотра и незаметного изменения пакетов OWAMP-Test и TWAMP-Test.

Существует также опасность того, что тестируемая сеть (зная или не зная адресов отправителя и получателя в измерительной системе) будет уделять особое внимание пакетам с общеизвестным портом UDP, искажая результаты за счёт ускорения или замедления обработки таких пакетов.

7. Взаимодействие с IANA

Агентство IANA заново выделило два номера портов UDP из диапазона System Ports в реестре Service Name and Transport Protocol Port Number Registry [RFC6335]. В частности, заново выделены порты UDP 861 и 862, как показано ниже, с сохранением выделенных портов TCP. Для этих портов также изменены назначившее и контактное лицо (как для UDP, так и для TCP) с указанием IESG и IETF Chair, соответственно.

Имя службы	Номер порта	Транспортный протокол	Описание	Документ
owamp-control	861	tcp	OWAMP-Control	RFC 4656
owamp-test	861	udp	OWAMP-Test Receiver Port	RFC 8545
twamp-control	862	tcp	TWAMP-Control	RFC 5357
twamp-test	862	udp	TWAMP-Test Receiver Port	RFC 8545

8. Литература

8.1. Нормативные документы

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](https://www.rfc-editor.org/info/rfc2119), 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](https://www.rfc-editor.org/info/rfc4656), 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](https://www.rfc-editor.org/info/rfc5357), DOI 10.17487/RFC5357, October 2008, <<https://www.rfc-editor.org/info/rfc5357>>.
- [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>>.

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

[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>>.

8.2. Дополнительная литература

[IPPM-TWAMP-06] Hedayat, K., Krzanowski, R., Yum, K., Morton, A., and J. Babiarz, "A Two-way Active Measurement Protocol (TWAMP)", Work in Progress¹, draft-ietf-ippm-twamp-06, December 2007.

[LarsAD] Eggert, L., "Subject: [ippm] AD review: draft-ietf-ippm-twamp-06.txt", message to the ippm mailing list, April 2008, <<https://mailarchive.ietf.org/rch/msg/ippm/LzcTPYhPhWhbb5-ncR046XKpnzo>>.

[TimDISCUSS] "Tim Polk's Ballot discuss", July 2008, <<https://datatracker.ietf.org/doc/rfc5357/history>>.

[TR-390] Broadband Forum, "TR-390: Performance Measurement from IP Edge to Customer Equipment using TWAMP Light", Issue: 1, May 2017, <<https://www.broadband-forum.org/technical/download/TR-390.pdf>>.

Приложение А. Основы TWAMP Light

В этом информационном приложении указаны основания перевода идеи TWAMP Light в статус информационного приложения к [RFC5357].

Как отмечено в разделе 4, идея TWAMP Light была помещена в Приложение I к [RFC5357] по причине её несоответствия требованиям к протоколам IETF (нет спецификации согласования этой формы работы и обязательных для реализации свойств защиты), как указано ниже.

- Lars Eggert (Area Director) в рецензии [LarsAD] отметил, что наличие двух вариантов TWAMP (TWAMP Light и Complete TWAMP) требует протокольного механизма для согласования используемого варианта. Отметим, что в этом документе Complete TWAMP называется Standards Track TWAMP. См. комментарий Lars Section 5.2, paragraph 0 в [LarsAD] со ссылкой на [IPPM-TWAMP-06]. Рабочая группа согласилась поместить описание TWAMP Light в Приложение I и упоминать его как «путь поэтапной адаптации TWAMP с реализацией сначала TWAMP-Test».
- Tim Polk в Ballot discuss от 16.07.2008 [TimDISCUSS] отметил, что TWAMP Light является неполной спецификацией, поскольку ключ, требуемый для режимов с аутентификацией и шифрованием, зависит от ключа TWAMP-Control Session. В Приложение I добавлены требования, учитывающие замечание Tim (см. три последних абзаца Приложения I к [RFC5357]).

Поскольку идея TWAMP Light явно включает протокол TWAMP-Test и другие не определённые средства, Приложение I к [RFC5357] просто описывает идеи об использовании TWAMP-Test вне контекста Standards Track TWAMP.

Благодарности

Авторы признательны рабочей группе IPPM за быстрые отклики. Спасибо также Muthu Arul Mozhi Perumal и Luay Jalil за их участие и предложения.

Участники работы

Richard Foote и Luis M. Contreras внесли заметный вклад в этот документ.

Адреса авторов

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

Greg Mirsky (editor)
ZTE Corp.
Email: gregimirsky@gmail.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

¹Опубликовано в RFC 5357. Прим. перев.