Internet Engineering Task Force (IETF)
Request for Comments: 8545
Updates: 4656, 5357
Category: Standards Track
ISSN: 2070-1721
March 2019

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

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

Abstract

This memo explains the motivation and describes the reassignment of well-known ports for the One-Way Active Measurement Protocol (OWAMP) and the Two-Way Active Measurement Protocol (TWAMP) for control and measurement. It also clarifies the meaning and composition of these Standards Track protocol names for the industry.

This memo updates RFCs 4656 and 5357, in terms of the UDP well-known port assignments, and it clarifies the complete OWAMP and TWAMP protocol composition for the industry.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8545.

Copyright Notice

Table of Contents

1. Introduction

The IETF IP Performance Metrics (IPPM) Working Group first developed the One-Way Active Measurement Protocol (OWAMP), as specified in [RFC4656]. Further protocol development to support testing resulted in the Two-Way Active Measurement Protocol (TWAMP), as specified in [RFC5357].

Both OWAMP and TWAMP require the implementation of a control and mode negotiation protocol (OWAMP-Control and TWAMP-Control) that employs the reliable transport services of TCP (including security configuration and key derivation). The control protocols arrange for the configuration and management of test sessions using the associated test protocol (OWAMP-Test or TWAMP-Test) on UDP transport.

The IETF recognizes the value of assigning a well-known UDP port to the OWAMP-Test and TWAMP-Test protocols and also recognizes that this goal can be easily arranged through port reassignments.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Scope

The scope of this memo is twofold: (1) to reallocate the well-known ports for the UDP test protocols that compose necessary parts of their respective Standards Track protocols (OWAMP and TWAMP) and (2) to clarify the meaning and composition of these Standards Track protocol names for the industry.

This memo updates [RFC4656] and [RFC5357], in terms of the UDP well-known port assignments.

4. Definitions and Background

This section defines key terms and clarifies the required composition of the OWAMP and TWAMP Standards Track protocols.

"OWAMP-Control" is the protocol defined in Section 3 of [RFC4656].

"OWAMP-Test" is the protocol defined in Section 4 of [RFC4656].

OWAMP is described in this direct quote from Section 1.1 of [RFC4656]: "OWAMP actually consists of two inter-related protocols: OWAMP-Control and OWAMP-Test." A similar sentence appears in Section 2 of [RFC4656]. For avoidance of doubt, the implementation of both OWAMP-Control and OWAMP-Test is REQUIRED for Standards Track OWAMP as specified in [RFC4656] (applying the consensus of many dictionary definitions of "consist").

"TWAMP-Control" is the protocol defined in Section 3 of [RFC5357].

"TWAMP-Test" is the protocol defined in Section 4 of [RFC5357].

TWAMP is described in this direct quote from Section 1.1 of [RFC5357]: "Similar to OWAMP [RFC4656], TWAMP consists of two inter-related protocols: TWAMP-Control and TWAMP-Test." For avoidance of doubt, the implementation of both TWAMP-Control and TWAMP-Test is REQUIRED for Standards Track TWAMP as specified in [RFC5357] (applying the consensus of many dictionary definitions of "consist").

"TWAMP Light" is an idea described in Appendix I ("TWAMP Light (Informative)") of [RFC5357]; TWAMP Light includes an unspecified control protocol combined with the TWAMP-Test protocol. In [RFC5357], the TWAMP Light idea was relegated to Appendix I because TWAMP Light failed to meet the requirements for IETF protocols (there are no specifications for negotiating this form of operation and no specifications for mandatory-to-implement security features), as described in Appendix A of this memo. See also [LarsAD] and [TimDISCUSS].

Since the idea of TWAMP Light clearly includes the TWAMP-Test component of TWAMP, it is considered reasonable for future systems to use the TWAMP-Test well-known UDP port (whose reallocated assignment is specified in this document). Clearly, the TWAMP Light idea envisions many components and communication capabilities beyond TWAMP-Test (implementing the security requirements, for example); otherwise, Appendix I of [RFC5357] would be one sentence long (equating TWAMP Light with TWAMP-Test only).

5. New Well-Known Ports

Originally, both TCP and UDP well-known ports were assigned to the control protocols that are essential components of Standards Track OWAMP and TWAMP.

Since OWAMP-Control and TWAMP-Control require TCP transport, they cannot make use of the UDP ports that were originally assigned. However, test sessions using OWAMP-Test or TWAMP-Test operate on UDP transport.

Per this memo, IANA has reassigned the UDP well-known port from the control protocol to the test protocol (see Section 7 ("IANA Considerations")). The use of this UDP port is OPTIONAL in Standards Track OWAMP and TWAMP. It may simplify some operations to have a well-known port available for the test protocols or for future specifications involving TWAMP-Test to use this port as a default port. For example, [TR-390] is a specification for testing at the customer edge of IP networks, and conforming implementations will benefit from reallocation of the well-known UDP port to the test protocol.

5.1. Impact on TWAMP-Control Protocol

Section 3.5 of [RFC5357] describes the detailed process of negotiating the Receiver Port number, on which the TWAMP Session-Reflector will send and receive TWAMP-Test packets; see the quoted text below. The Control-Client, acting on behalf of the Session-Sender, proposes the Receiver Port number from the Dynamic Ports range [RFC6335]:

> The Receiver Port is the desired UDP port to which TWAMP-Test packets will be sent by the Session-Sender (the port where the Session-Reflector is asked to receive test packets). The Receiver Port is also the UDP port from which TWAMP-Test packets will be sent by the Session-Reflector (the Session-Reflector will use the same UDP port to send and receive packets).

It is possible that the proposed Receiver Port may not be available, e.g., the port is in use by another test session or another application. In this case, we update the last paragraph of Section 3.5 of [RFC5357] per Erratum ID 1587 (see <https://www.rfc-editor.org/errata/eid1587>) as follows:

> ... the Server at the Session-Reflector MAY suggest an alternate and available port for this session in the Port field. The Control-Client either accepts the alternate port or composes a new Session-Request message with suitable parameters. Otherwise, the

Server uses the Accept field to convey other forms of session rejection or failure to the Control-Client and MUST NOT suggest an alternate port; in this case, the Port field MUST be set to zero.

A Control-Client that supports the use of the allocated TWAMP-Test Receiver Port (Section 7) MAY request to use that port number in the Request-TW-Session command. If the Server does not support the allocated TWAMP-Test Receiver Port, then it sends an alternate port number in the Accept-Session message with Accept field = 0. Thus, the deployment of the allocated TWAMP Receiver Port number is backward compatible with existing TWAMP-Control solutions that are based on [RFC5357]. Of course, using a UDP port number chosen from the Dynamic Ports range [RFC6335] will help avoid the situation where the Control-Client or Server finds that the proposed port is already in use.

5.2. Impact on OWAMP-Control Protocol

As described above, an OWAMP-Control client that supports the use of the allocated OWAMP-Test Receiver Port (Section 7) MAY request to use that port number in the Request-Session command. If the Server does not support the allocated OWAMP-Test Receiver Port (or does not have the port available), then it sends an alternate port number in the Accept-Session message with Accept field = 0. Further exchanges proceed as already specified.

5.3. Impact on OWAMP-Test/TWAMP-Test Protocols

OWAMP-Test/TWAMP-Test may be used to measure IP performance metrics in an Equal-Cost Multipath (ECMP) environment. Though algorithms to balance IP flows among available paths have not been standardized, the most common is the five-tuple that uses destination IP address, source IP address, protocol type, destination port number, and source port number. When attempting to monitor different paths in an ECMP network, it is sufficient to vary only one of five parameters, e.g., the source port number. Thus, there will be no negative impact on the ability to arrange concurrent OWAMP/TWAMP test sessions between the same test points to monitor different paths in the ECMP network when using the reallocated UDP port number as the Receiver Port, as using the port is optional.

6. Security Considerations

The security considerations that apply to any active measurement of live paths are relevant here as well (see [RFC4656] and [RFC5357]).

When considering the privacy of those involved in measurement or those whose traffic is measured, the sensitive information available to potential observers is greatly reduced when using active techniques that are within this scope of work. Passive observations of user traffic for measurement purposes raise many privacy issues. We refer the reader to the security and privacy considerations described in the Large-Scale Measurement of Broadband Performance (LMAP) framework [RFC7594], which covers both active and passive techniques.

The registered UDP port as the Receiver Port for OWAMP-Test/TWAMP-Test could become a target of denial of service (DoS) or could be used to aid man-in-the-middle (MITM) attacks. To improve protection against DoS, the following methods are recommended:

- filtering access to the OWAMP/TWAMP Receiver Port via an access list.

- using a non-globally routable IP address for the OWAMP/TWAMP Session-Reflector address.

A MITM attacker may try to modify the contents of the OWAMP-Test/TWAMP-Test packets in order to alter the measurement results. However, an implementation can use authenticated mode to detect modification of data. In addition, an implementation can use encrypted mode to prevent eavesdropping and undetected modification of the OWAMP-Test/TWAMP-Test packets.

There is also the risk of a network under test giving special treatment to flows involving the well-known UDP port, with or without knowing source and destination addresses of measurement systems, and thus biasing the results through preferential or detrimental processing.

7. IANA Considerations

IANA has reallocated two UDP port numbers from the System Ports range of the "Service Name and Transport Protocol Port Number Registry" [RFC6335]. Specifically, IANA has reallocated UDP ports 861 and 862 as shown below, leaving the TCP port assignments as is. IANA has also updated the Assignee and Contact for these ports (both UDP and TCP) to be the IESG and the IETF Chair, respectively.

Service Name	Port Number	Transport Protocol	Description	Reference
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. References

8.1. Normative References

[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>.

[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. Informative References

[IPPM-TWAMP-06] Hedayat, K., Krzanowski, R., Yum, K., Morton, A., and J. Babiarz, "A Two-way Active Measurement Protocol (TWAMP)", Work in Progress, 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>.

Appendix A. Background on TWAMP Light

This informative appendix provides the background on the decision to move the TWAMP Light idea to an informative appendix in [RFC5357].

As also noted in Section 4, the TWAMP Light idea was relegated to Appendix I of [RFC5357] because it failed to meet the requirements for IETF protocols (there are no specifications for negotiating this form of operation and no specifications for mandatory-to-implement security features), as described in the references cited below:

- Lars Eggert's Area Director review [LarsAD], where he pointed out that having two variants of TWAMP (TWAMP Light and Complete TWAMP) requires a protocol mechanism to negotiate which variant will be used. Note that "Complete TWAMP" is called "Standards Track TWAMP" in this document. See Lars's "Section 5.2, paragraph 0" comment on [LarsAD], which refers to a section in [IPPM-TWAMP-06]. The working group consensus was to place the TWAMP Light description in Appendix I and to refer to that appendix only as an "incremental path to adopting TWAMP, by implementing the TWAMP-Test protocol first."

- Tim Polk's "Ballot discuss" of 2008-07-16 [TimDISCUSS], which points out that TWAMP Light was an incomplete specification because the key required for authenticated and encrypted modes depended on the TWAMP-Control Session key. Additional requirement statements were added in Appendix I to address Tim's Ballot discuss (see the last three paragraphs of Appendix I in [RFC5357]).

Since the idea of TWAMP Light clearly includes the TWAMP-Test protocol and other undefined facilities, Appendix I of [RFC5357] simply describes ideas for how TWAMP-Test might be used outside of the context of Standards Track TWAMP.

Acknowledgements

The authors thank the IPPM Working Group for their rapid review; thanks also to Muthu Arul Mozhi Perumal and Luay Jalil for their participation and suggestions.

Contributors

Richard Foote and Luis M. Contreras made notable contributions on this topic.

Authors' Addresses

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