Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 27, 2013

J. Hedin
G. Mirsky
Ericsson

June 25, 2013

Type-P Descriptor Monitoring in Two-Way Active Measurement Protocol (TWAMP)
draft-hedin-ippm-type-p-monitor-01

Abstract

This document specifies how optional monitoring of Type-P Descriptor can be negotiated and performed by TWAMP [RFC5357] Control and Test protocols.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 27, 2013.

Copyright Notice

Table of Contents

1. Introduction

Re-marking of Type-P Descriptor, i.e. change in value, might be demonstration of intentional or errorneous behavior. Monitoring of Type-P Descriptor can provide valuable information for network operators. One-Way Active Measurement Protocol [RFC4656] and Two-Way Active Measurement Protocol [RFC5357] define negotiation of TypeP Descriptor value that must be used by Session-Sender and Session-Reflector. But there's not means for Session-Sender to know whether Type-P Descriptor was received by Session-Reflector unchanged. Opional monitoring of Type-P Descriptor between Session-Sender and Session-Reflector requires extensions to TWAMP [RFC5357] that are described in this document.

1.1. Conventions used in this document

1.1.1. Terminology

DSCP: Differentiated Service Codepoint

IPPM: IP Performance Measurement

TWAMP: Two-Way Active Measuremnt Protocol

OWAMP: One-Way Active Measurement Protocol

1.1.2. 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 [RFC2119].

2. TWAMP Extensions

TWAMP connection establishment follows the procedure defined in Section 3.1 of [RFC4656] and Section 3.1 of [RFC5357] where the Modes field been used to identify and select specific communication capabilities. At the same time the Modes field been recognized and used as extension mechanism [RFC6038]. The new feature requires new bit position to identify the ability of a Session-Reflector to return value of received Type-P Descriptor back to a Session-Sender, and to support the new Session-Reflector packet format in the TWAMP-Test protocol. See the Section 3 for details on the assigned value and bit position.

2.1. Setting Up Connection to Monitor Type-P Descriptor

The Server sets Type-P Descriptor Monitoring flag in Modes field of the Server Greeting message to indicate its capabilities and willingness to monitor Type-P. If the Control-Client agrees to monitor Type-P Descriptor on some or all test sessions invoked with this control connection, it MUST set the Type-P Descriptor Monitoring flag in Modes field in the Setup Response message.

2.2. TWAMP-Test Extension

Monitoring of Type-P Descriptor requires support by Session-Reflector and changes format of its test packet format both in unauthenticated, authenticated and encrypted modes. Monitoring of Type-P Descriptor does not alter Session-Sender test packet format but certain considerations must be taken when and if this mode is accepted in combination with Symmetrical Size mode[RFC6038].

2.2.1. Session-Reflector Packet Format for Type-P Descriptor Monitoring

When Session-Reflector supports Type-P Descriptor Monitoring in MUST construct Sender Type-P Descriptor for each test packet it sends to Session-Sender according to the following procedure:

- first two bits MUST be the same as two first bits of Type-P Descriptor field Request-Session control packet;

- remaining bits MUST be copied from received Session-Sender test packet according to two first bits:

Section 3.5 in [RFC5357] states that Type-P Descriptor capability supported in TWAMP is to set Differentiated Services Codepoint (DSCP) value, as defined in [RFC2474]. Thus first two bits MUST be set to 00. Then DSCP value copied into subsequent six bits. For a Session-Sender, upon receiving reflected TWAMP-Test packet, If the first two bits are not 00, then subsequent value should be ignored.

For unauthenticated mode:

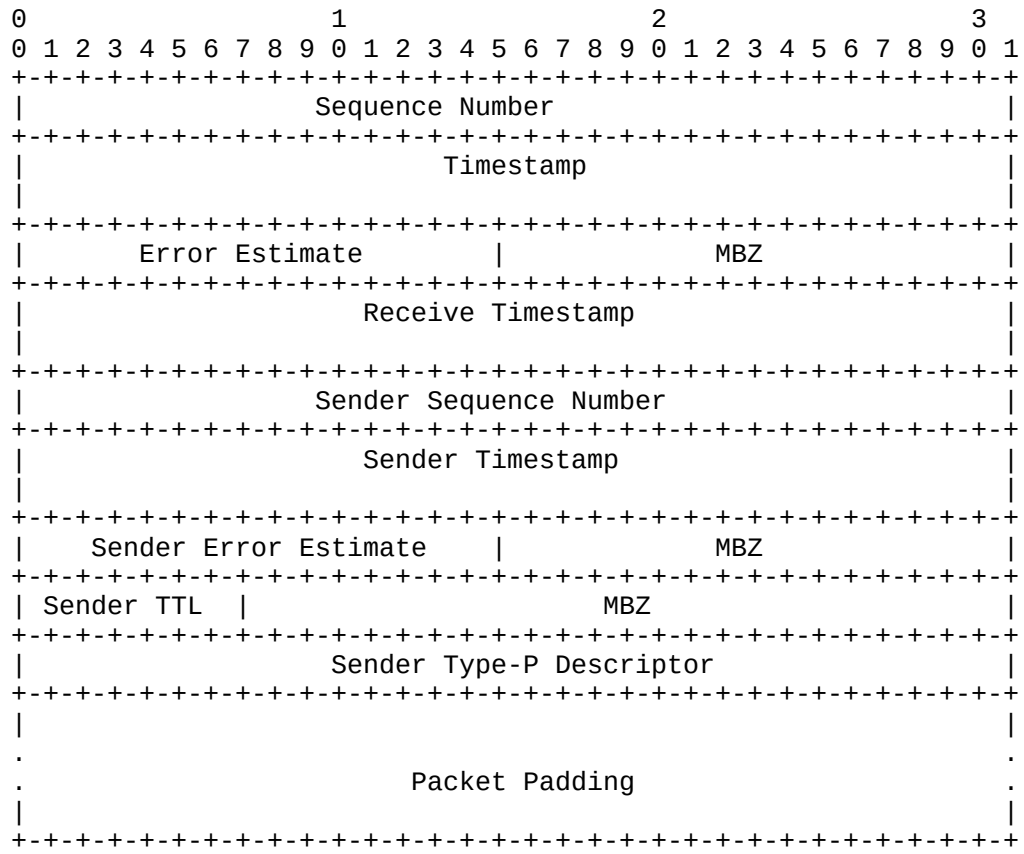
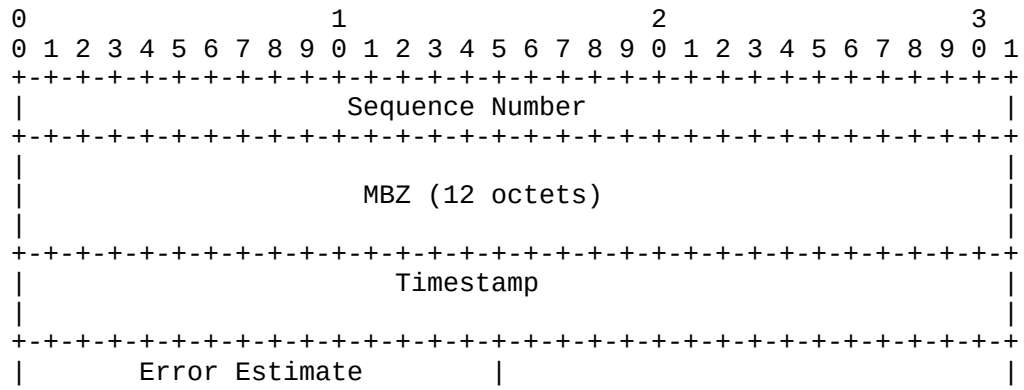


Figure 1: Session-Reflector test packet format with Type-P Descriptor monitoring in unauthenticated mode

For authenticated and encrypted modes:



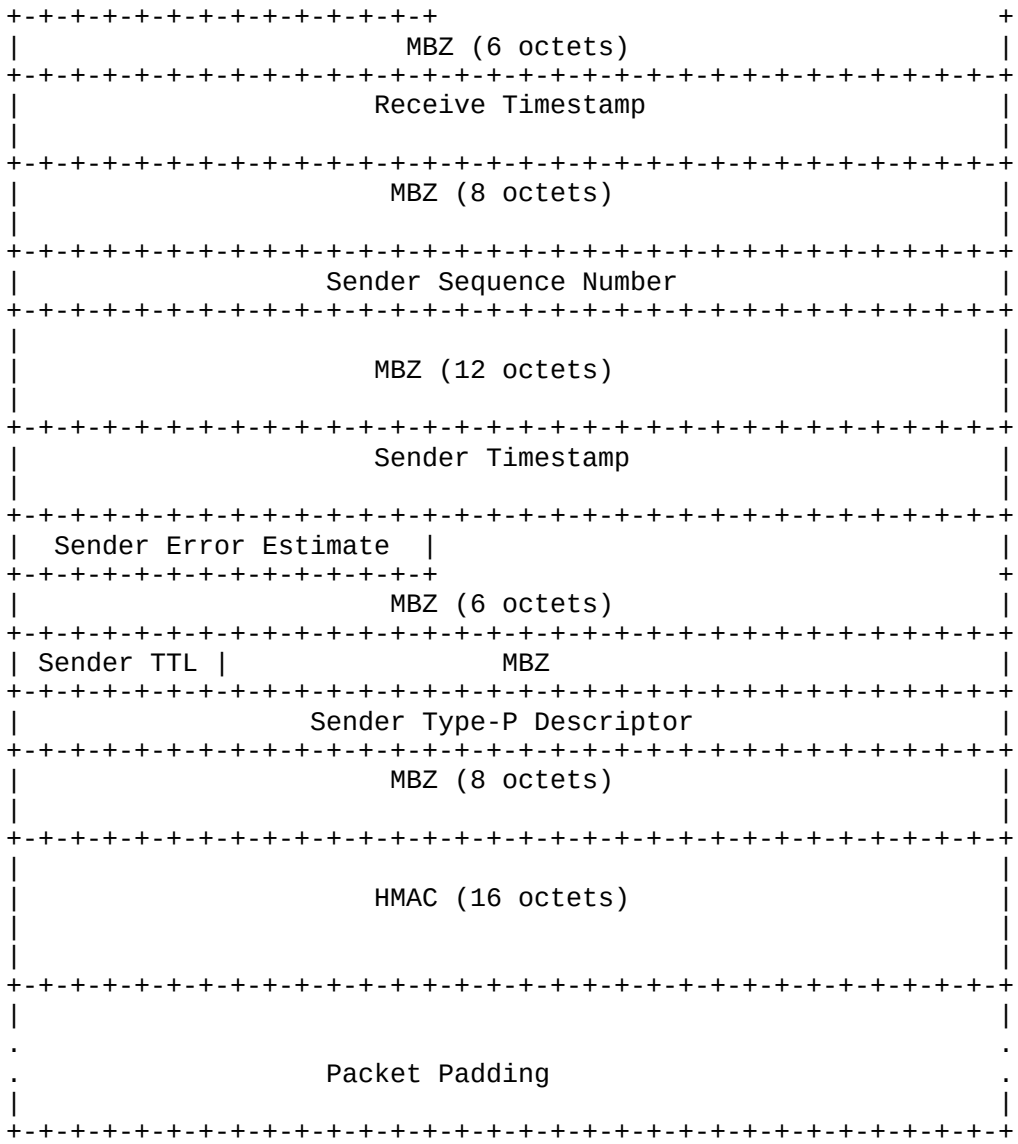


Figure 2: Session-Reflector test packet format with Type-P Descriptor monitoring in authenticated or encrypted modes

2.2.2. Type-P Descriptor Monitoring with RFC 6038 extensions

[RFC6038] defined two extensions to TWAMP. First, to ensure that Session-Sender and Session-Reflector exchange TWAMP-Test packets of equal size. Second, to specify number of octets to be reflected by

Session-Reflector. If Type-P Descriptor monitoring and Symmetrical Size and/or Reflects Octets modes being negotiated between Server and Control-Client in Unauthenticated mode, then because Sender Type-P Descriptor increases size of unauthenticated Session-Reflector packet by 4 octets the Padding Length value SHOULD be >= 31 octets to allow for the truncation process that TWAMP recommends in Section 4.2. 1 of [RFC5357].

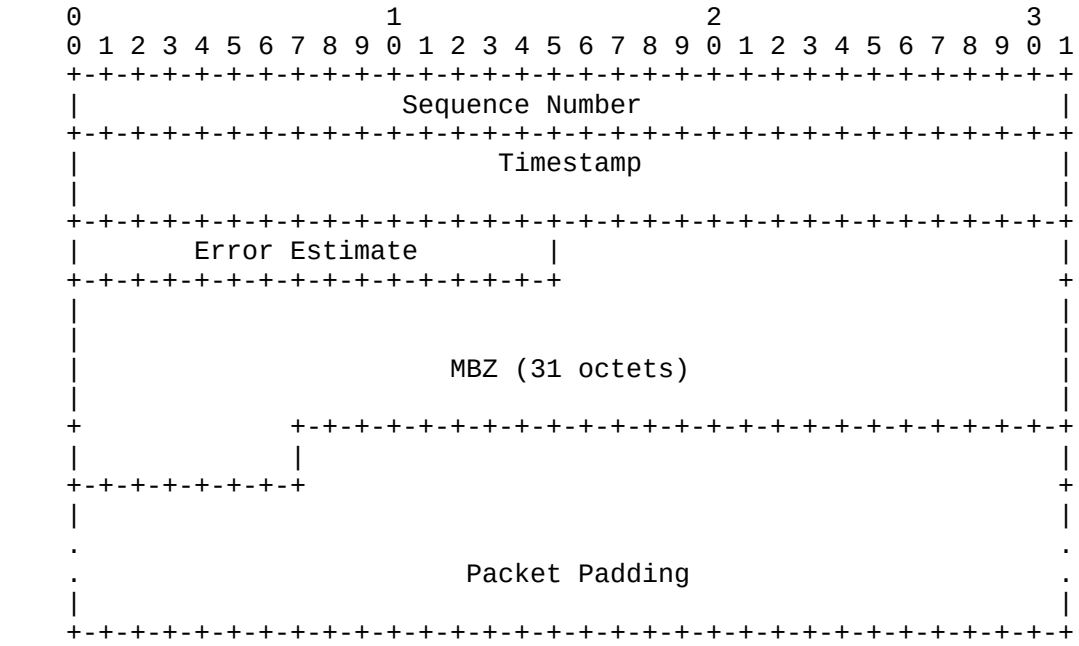


Figure 3: Session-Sender test packet format with Type-P Descriptor monitoring and Symmetrical Test Packet in unauthenticated mode

3. IANA Considerations

The TWAMP-Modes registry defined in [RFC5618].

IANA is requested to reserve a new Type-P Descriptor Monitoring Capability as follows:

Value	Description	Semantics	Reference
X (proposed 128)	Type-P Descriptor Monitoring Capability	bit position Y (proposed 7)	This document

Table 1: New Type-P Descriptor Monitoring Capability

4. Security Considerations

Monitoring of Type-P Descriptor does not appear to introduce any additional security threat to hosts that communicate with TWAMP as defined in [RFC5357], and existing extensions [RFC6038]. The security considerations that apply to any active measurement of live networks are relevant here as well. See the Security Considerations sections in [RFC4656] and [RFC5357].

5. Acknowledgements

TBD

6. References

6.1. Normative References

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

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, September 2006.

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

[RFC5618] Morton, A. and K. Hedayat, "Mixed Security Mode for the Two-Way Active Measurement Protocol (TWAMP)", RFC 5618,

August 2009.

[RFC6038] Morton, A. and L. Ciavattone, "Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features", RFC 6038, October 2010.

6.2. Informative References

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

Authors' Addresses

Jonas Hedin
Ericsson

Email: jonas.hedin@ericsson.com

Greg Mirsky
Ericsson

Email: gregory.mirsky@ericsson.com