Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 3, 2015

J. Hedin
G. Mirsky
S. Baillargeon
Ericsson

September 30, 2014

Differentiated Service Code Point and Explicit Congestion Notification Monitoring in Two-Way Active Measurement Protocol (TWAMP) draft-hedin-ippm-type-p-monitor-04

Abstract

This document describes an OPTIONAL feature for TWAMP [RFC5357] allowing the monitoring of the Differentiated Service Code Point and Explicit Congestion Notification fields with the TWAMP-Test protocol.

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 April 3, 2015.

Table of Contents

1. Introduction

One-Way Active Measurement Protocol (OWAMP) [RFC4656] defines Type-P descriptor and negotiation of its value in OWAMP-Control protocol. Two-Way Active Measurement Protocol (TWAMP) [RFC5357] states that only Differentiated Service Code Point (DSCP) value can be defined by Type-P descriptor and the negotiated value must be used by both Session-Sender and Session-Reflector. The TWAMP specification also states that the same value of DSCP (found in the Session-Sender packet) MUST be used in the test packet reflected by the Session-Reflector. However the TWAMP-Test protocol does not specify any methods to determine or report when the DSCP value has changed or is different than expected in the forward or reverse direction. Re-marking the DSCP (changing its original value) in IP networks is possible and often accomplished by a Diffserv policy configured o a single node along the IP path. In many cases, a change of the DSCP value of indicates an unintentional or errorneous behavior. At best, the Session-Sender can detect a change of the DSCP reverse direction assuming such change is actually detectable.

This document describes an OPTIONAL feature for TWAMP. It is called the DSCP and ECN monitoring feature. This feature allows the

Session-Sender to know the actual DSCP value received at the Session-Reflector. Furthermore this OPTIONAL feature also tracks the Explicit Congestion Notification (ECN) value received at the Session-Reflector. This is helpful to determine if ECN is actually operating

or if an ECN-capable node has detected congestion in the forward direction.

1.1. Conventions used in this document

1.1.1. Terminology

DSCP: Differentiated Service Codepoint

ECN: Explicit Congestion Notification

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 DSCP and ECN values 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 DSCP and ECN

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

2.2. TWAMP-Test Extension

Monitoring of DSCP and ECN requires support by Session-Reflector and changes format of its test packet format both in unauthenticated, authenticated and encrypted modes. Monitoring of DSCP and ECN 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 DSCP and ECN Monitoring

When Session-Reflector supports DSCP and ECN Monitoring it MUST construct Sender DSCP and ECN (S-DSCP-ECN) field for each test packet it sends to Session-Sender according to the following procedure:

- first six bits MUST be copied Differentiated Service field from received Session-Sender test packet into Sender DSCP (S-DSCP) field;

- following two bits MUST be copied ECN field from received Session-Sender test packet into Sender ECN (S-ECN) field.

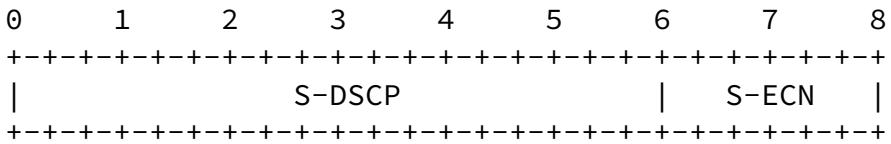
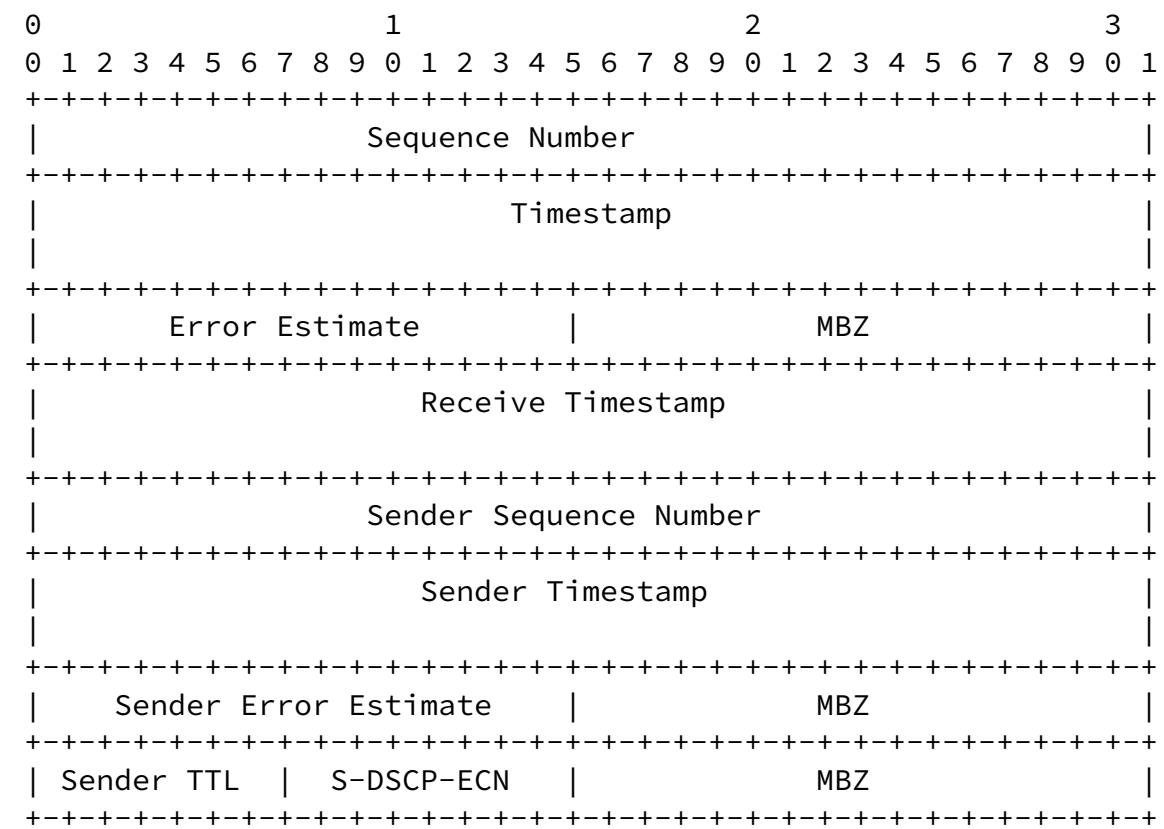


Figure 1: Sender DSCP and ECN field format

For unauthenticated mode:



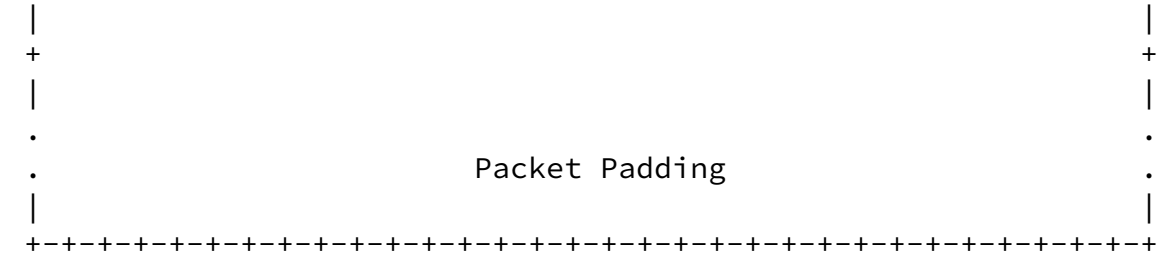
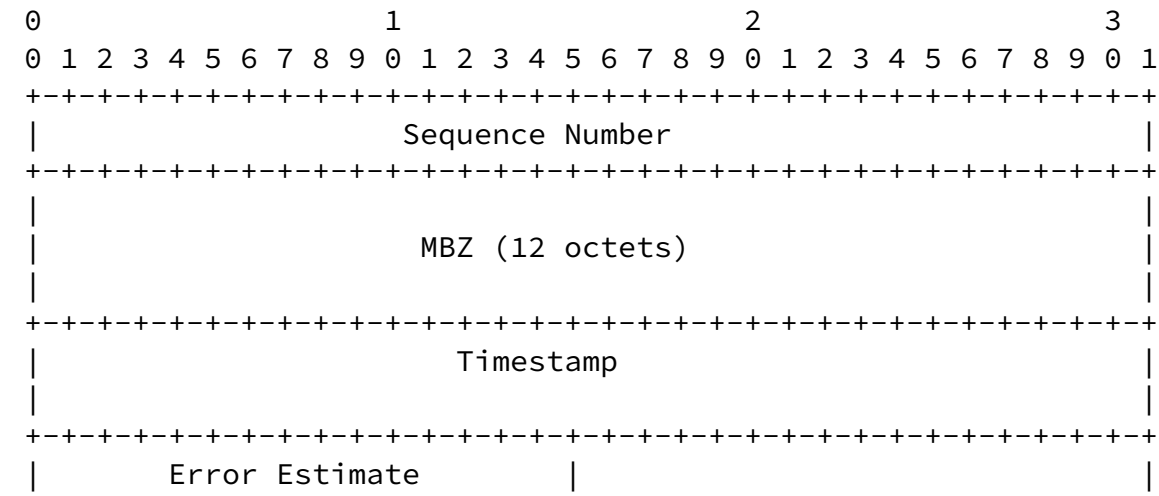
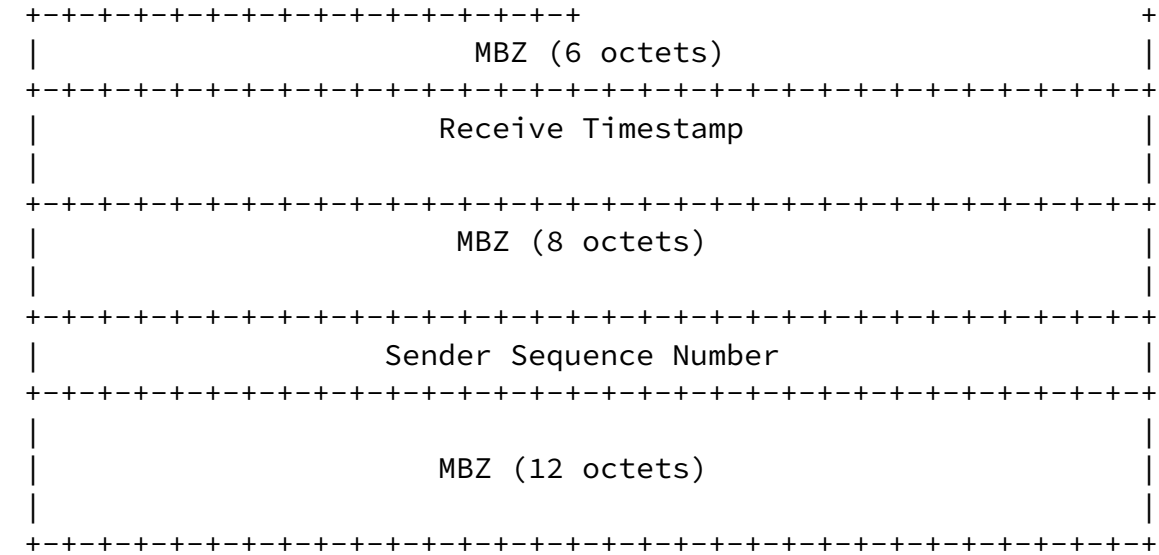


Figure 2: Session-Reflector test packet format with DSCP and ECN monitoring in unauthenticated mode

For authenticated and encrypted modes:





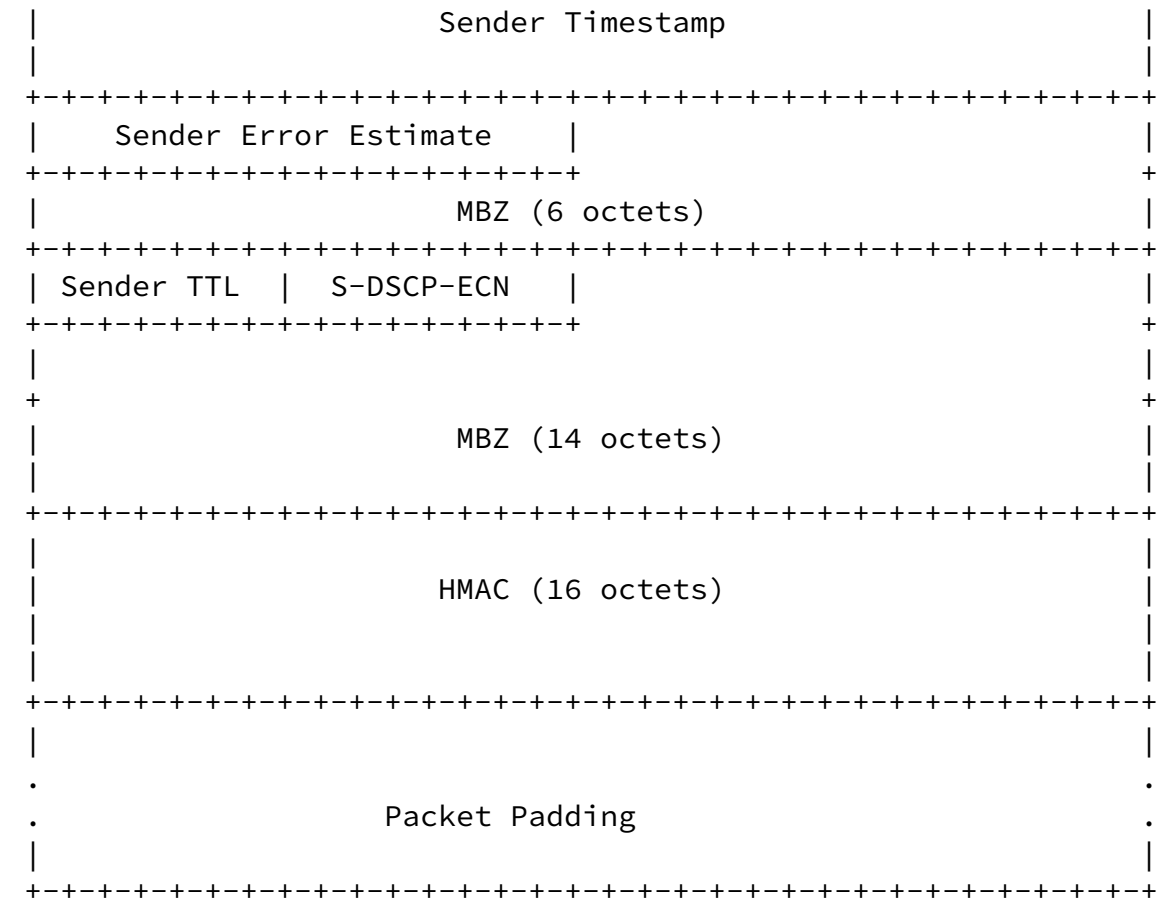


Figure 3: Session-Reflector test packet format with DSCP and ECN monitoring in authenticated or encrypted modes

The DSCP value is often copied into reflected test packets with current TWAMP implementations (with or without TWAMP-Control protocol). With DSCP and ECN Monitoring Extenstion Session-Reflector handles DSCP as following:

The Session-Reflector MUST extracts the S-DSCP-ECN value from the DSCP and ECN values of received packets;

The Session-Reflector MUST transmit each reflected test packet with DSCP set to the negotiated/provisioned value;

If the negotiated/provisioned DSCP value is not known (e.g. TWAMP Light), the choice of the DSCP is implementation specific. For

instance, Session-Reflector MAY copy the DSCP value from the received test packet and set it as DSCP in a reflected packet.

2.2.2. DSCP and ECN 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 DSCP and ECN monitoring and Symmetrical Size and/or Reflects Octets modes being negotiated between Server and Control-Client in Unauthenticated mode, then because Sender DSCP and Sender ECN increase size of unauthenticated Session-Reflector packet by 4 octets the Padding Length value SHOULD be >= 28 octets to allow for the truncation process that TWAMP recommends in Section 4.2. 1 of [RFC5357].

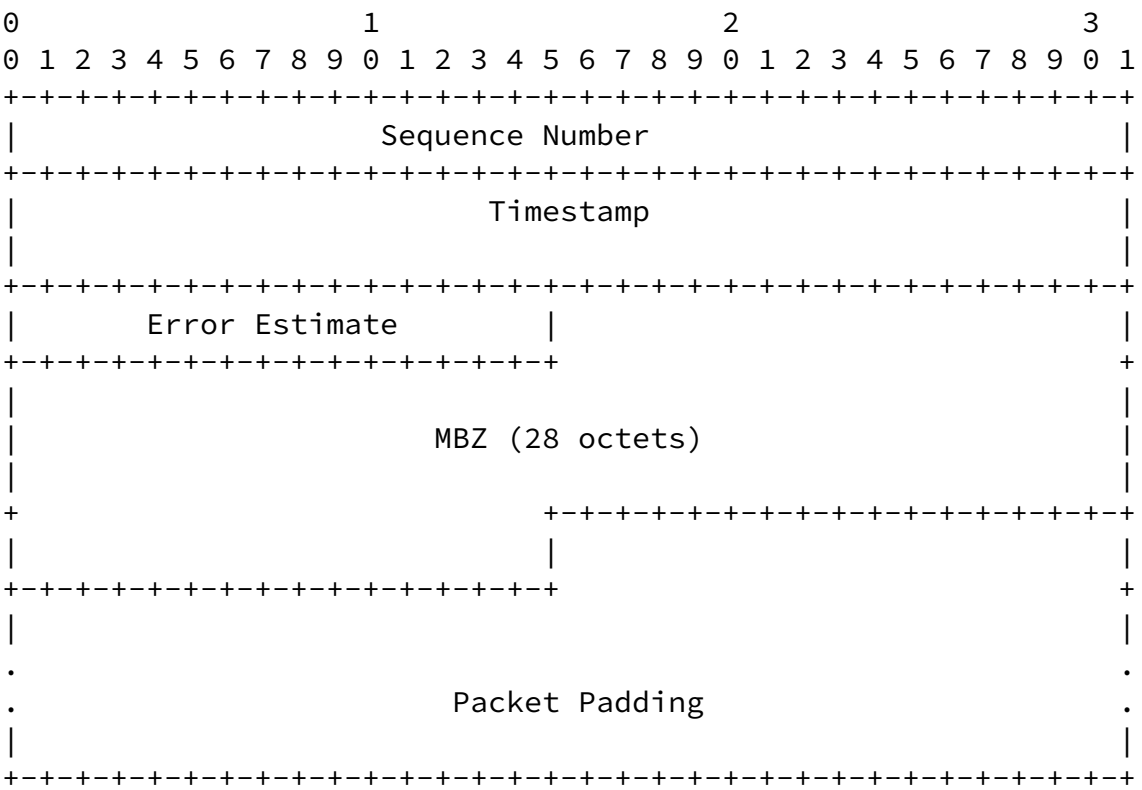


Figure 4: Session-Sender test packet format with DSCP and ECN monitoring and Symmetrical Test Packet in unauthenticated mode

2.2.3. Consideration for TWAMP Light mode

Appendix I of [RFC5357] does not explicitly state how value of Type-P descriptor synchronized between Session-Sender and Session-Reflector and whether different values considered as error condition and should be reported. We assume that by some means Session-Sender and Session-Reflector of given TWAMP-Test session informed to use the same DSCP value. Same means, i.e. configuration, could be used to inform Session-Reflector to support DSCP and ECN monitoring mode by copying data from received TWAMP test packets. Then Session-Sender may be informed to use Sender DSCP and ECN field in reflected TWAMP test packet.

3. IANA Considerations

The TWAMP-Modes registry defined in [RFC5618].

IANA is requested to reserve a new DSCP and ECN Monitoring Capability as follows:

Value	Description	Semantics	Reference
X (proposed 128)	DSCP and ECN Monitoring Capability	bit position Y (proposed 7)	This document

Table 1: New Type-P Descriptor Monitoring Capability

4. Security Considerations

Monitoring of DSCP and ECN 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

Authors greatly appreciate thorough review and thoughtful comments by Chritofer Flinta and Samita Chakrabarti.

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

Steve Baillargeon
Ericsson

Email: steve.baillargeon@ericsson.com