Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 21, 2015

J. Hedin
G. Mirsky
S. Baillargeon
Ericsson

December 18, 2014

Differentiated Service Code Point and Explicit Congestion Notification Monitoring in Two-Way Active Measurement Protocol (TWAMP)
draft-ietf-ippm-type-p-monitor-01

Abstract

This document describes an OPTIONAL extension for Two-Way Active Measurement Protocol (TWAMP) 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 June 21, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
1.1. Conventions used in this document 3
1.1.1. Terminology 3
1.1.2. Requirements Language 3
2. TWAMP Extensions 3
2.1. Setting Up Connection to Monitor DSCP and ECN 3
2.2. TWAMP-Test Extension 4
2.2.1. Session-Reflector Packet Format for DSCP and ECN Monitoring 4
2.2.2. DSCP and ECN Monitoring with RFC 6038 extensions . . 7
2.2.3. Consideration for TWAMP Light mode 8
3. IANA Considerations 8
4. Security Considerations 8
5. Acknowledgements 8
6. Normative References 9
Authors' Addresses 9

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) values 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 DSCP value (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 on a single node along the IP path. In many cases, a change of the DSCP value indicates an unintentional or erroneous 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 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 Measurement 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 is used to identify and select specific communication capabilities. At the same time the Modes field been recognized and used as an extension mechanism [RFC6038]. The new feature requires a 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 the Modes field in the Setup Response message.

2.2. TWAMP-Test Extension

Monitoring of DSCP and ECN requires support by the Session-Reflector and changes the format of its test packet format both in unauthenticated, authenticated and encrypted modes. Monitoring of DSCP and ECN does not alter the 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 the Session-Reflector supports DSCP and ECN Monitoring it MUST construct the Sender DSCP and ECN (S-DSCP-ECN) field for each test packet it sends to Session-Sender according to the following procedure:

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

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

```
 0     1     2     3     4     5     6     7     8
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |               S-DSCP               |   S-ECN   |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Sender DSCP and ECN field format

For unauthenticated mode:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Sequence Number                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Timestamp                            |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Error Estimate        |             MBZ                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Receive Timestamp                         |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Sender Sequence Number                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Sender Timestamp                          |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Sender Error Estimate    |             MBZ                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Sender TTL  |  S-DSCP-ECN   |             MBZ                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
.                                                               .
.                        Packet Padding                         .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

For authenticated and encrypted modes:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Sequence Number                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                     MBZ (12 octets)                           |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Timestamp                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Error Estimate        |                                 |
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                        MBZ (6 octets)                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Receive Timestamp                        |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       MBZ (8 octets)                          |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Sender Sequence Number                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                      MBZ (12 octets)                          |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Sender Timestamp                         |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Sender Error Estimate    |                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                       MBZ (6 octets)                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Sender TTL  |  S-DSCP-ECN   |                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                                                               |
+                                                               +
|                       MBZ (14 octets)                         |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                      HMAC (16 octets)                         |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                                                               .
.                    Packet Padding                             .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 Extension, the Session-Reflector handles DSCP as following:

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

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

- o 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 are 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].

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Sequence Number                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Timestamp                           |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Error Estimate        |                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                                +
|                                                               |
|                       MBZ (28 octets)                         |
|                                                               |
+                             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             |                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                                +
|                                                               |
.                                                               .
.                        Packet Padding                         .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 the value of the Type-P descriptor is synchronized between Session-Sender and Session-Reflector and whether different values are considered as error condition and SHOULD be reported. We assume that by some means the Session-Sender and the Session-Reflector of the given TWAMP-Test session been 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 Bill Cerveny, Christofer Flinta and Samita Chakrabarti.

6. Normative References

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

[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.

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