

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 29, 2009

A. Morton
L. Ciavattone
AT&T Labs
October 26, 2008

TWAMP Reflect Octets Feature
draft-ietf-ippm-twamp-reflect-octets-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on April 29, 2009.

Abstract

The IETF has completed its work on the core specification of TWAMP - the Two-Way Active Measurement Protocol. This memo describes a new feature for TWAMP: an optional capability where the responder host returns some of the command octets or padding octets to the controller, and/or ensures that the same test packet sizes are used in both directions.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

Internet-Draft

TWAMP Reflect Octets

October 2008

Table of Contents

1.	Introduction	3
2.	Purpose and Scope	3
3.	TWAMP Control Extensions	4
3.1.	Connection Setup with Reflect Padding Feature	4
3.2.	Request-TW-Session Packet Format	5
3.3.	Accept Session Packet Format	7
3.4.	Additional considerations	7
4.	Extended TWAMP Test	8
4.1.	Sender Behavior	8
4.1.1.	Packet Timings	8
4.1.2.	Packet Formats and Contents	8
4.1.3.	Padding Truncation	9
4.2.	Reflector Behavior	10
4.2.1.	Packet Format and Contents	10
4.2.2.	Padding Truncation	11
5.	Possible Alternative	12
6.	Security Considerations	14
7.	IANA Considerations	14
7.1.	Registry Specification	15
7.2.	Registry Management	15
7.3.	Experimental Numbers	15
7.4.	Registry Contents	15
8.	Acknowledgements	16
9.	References	16
9.1.	Normative References	16
9.2.	Informative References	16
	Authors' Addresses	16
	Intellectual Property and Copyright Statements	18

Internet-Draft

TWAMP Reflect Octets

October 2008

1. Introduction

The IETF has completed its work on the core specification of TWAMP - the Two-Way Active Measurement Protocol [[RFC5357](#)]. TWAMP is an extension of the One-way Active Measurement Protocol, OWAMP [[RFC4656](#)]. The TWAMP specification gathered wide review as it approached completion, and the by-products were several recommendations for new features in TWAMP. There are a growing number TWAMP implementations at present, and wide-spread usage is expected. There are even devices that are designed to test implementations for protocol compliance.

This memo describes a new feature for TWAMP. This feature adds the OPTIONAL capability for the responder host to return a limited number of unassigned (padding) octets to the Control-Client or Session-Sender entities. With this capability, the Control-Client or Session-Sender can embed octets of information it deems useful and have the assurance that the corresponding reply/test packet will contain that information when it is reflected and returned (by the Server or Session-Reflector). The feature also adds the Session-Reflector capability to assure that reflected test packets SHALL have their padding octets truncated, so that TWAMP-Test protocol uses the same packet size in both directions of transmission.

The relationship between this memo and TWAMP is intended to be an update to [[RFC5357](#)] when published.

2. Purpose and Scope

The purpose of this memo is to describe a new feature for TWAMP [[RFC5357](#)]. The feature enhances the TWAMP responder's capabilities to perform simple operations on control and test packets: the reflection of octets or padding and the guaranteed truncation of padding to compensate for the different sizes of TWAMP fields in the test packets. Motivations include permitting the controller host to

tag packets with an index for simplified identification, and/or assert that the same size test packets MUST be used in each direction.

The scope of the memo is currently limited to specifications of the following feature:

- o Extension of the modes of operation through assignment of new values in the Mode Field (see [section 3.1 \[RFC4656\]](#) for the format of the Server Greeting message), while retaining backward compatibility with the core TWAMP [\[RFC5357\]](#) implementations. These two values identify the ability of the Server/

Session-Reflector to reflect specific octets back to the Client/Session-Sender, and/or to truncate padding octets and ensure that TWAMP-Test protocol uses the same packet size in both directions.

[3.](#) TWAMP Control Extensions

TWAMP-Control protocol [\[RFC5357\]](#) uses the Modes Field to identify and select specific communication capabilities, and this field is a recognized extension mechanism. The following sections describe one such extension.

[3.1.](#) Connection Setup with Reflect Padding Feature

TWAMP connection establishment follows the procedure defined in [section 3.1 of \[RFC4656\]](#) and [section 3.1 of \[RFC5357\]](#). The new feature requires two new bit positions (and values) to identify the ability of the Server/Session-Reflector to reflect specific octets back to the Control-Client/Session-Sender, and to truncate padding octets when required. With this added feature, the complete set of TWAMP Modes Field bit positions and values would be as follows:

Value	Description	Reference/Explanation
0	Reserved	
1	Unauthenticated	RFC4656, Section 3.1
2	Authenticated	RFC4656, Section 3.1
4	Encrypted	RFC4656, Section 3.1
8	Unauth. TEST protocol, Encrypted CONTROL	draft-ietf-more-twamp (3)

```

-----
xxx   Reflect Octets           new bit position (X)
      Capability
yyy   Truncate Padding        new bit position (Y)
      Capability

```

In the original OWAMP Modes Field, setting bit positions 0, 1 or 2 indicated the security mode of the Control protocol, and the Test protocol inherited the same mode (see [section 4 of \[RFC4656\]](#)). In the memo [\[I-D.ietf-ippm-more-twamp\]](#), bit position 3 allows unauthenticated TWAMP Test protocol to be used with encryption on the TWAMP-Control protocol.

The Server sets one or both of the new bit positions (X and Y) in the Modes Field of the Server Greeting message to indicate its capabilities and willingness to operate in these modes if desired.
 >>>IANA: change X and Y to the assigned values <<<

If the Control-Client intends to operate all test sessions invoked with this control connection using one or both of the new modes, it MUST set the Modes Field bit corresponding to that function in the Setup Response message.

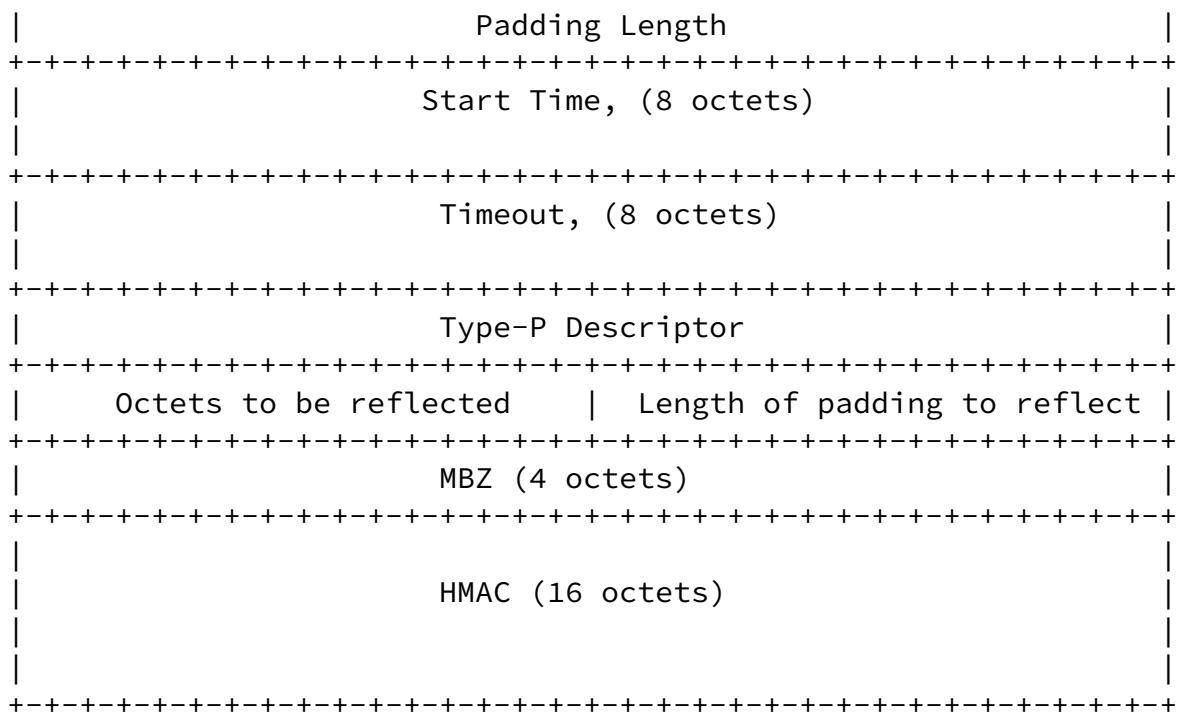
[3.2.](#) Request-TW-Session Packet Format

The bits designated for the Reflect Octets feature in the Request-TW-Session command are as shown in the packet format below.

```

      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
+-----+-----+-----+-----+-----+-----+-----+-----+
|           5           | MBZ | IPVN | Conf-Sender | Conf-Receiver |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Number of Schedule Slots           |
+-----+-----+-----+-----+-----+-----+-----+-----+
.
.           ... Many fields (66 octets) not shown ...           .
.
.
+-----+-----+-----+-----+-----+-----+-----+-----+

```



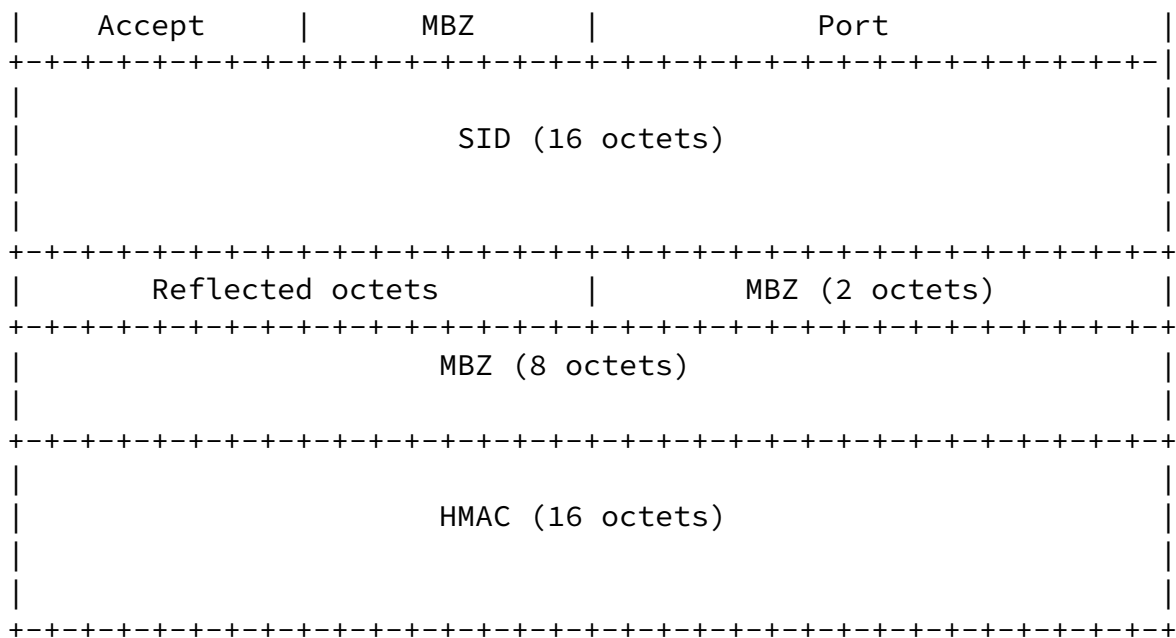
The "Padding Length" Field **continues** to specify the number of padding octets that the Session-Sender will append to ALL TWAMP-Test packets associated with this test session. See below for considerations on the minimum length of the padding octets, especially when complying with the options described in this memo, following the definitions of the two new fields that follow the

Type-P Descriptor.

Note that the number of padding octets appended to the Session-Reflector's test packet depends on support for the OPTIONAL Truncate Padding mode, or the RECOMMENDED truncation process in TWAMP [section 4.2.1 \[RFC5357\]](#).

The "Octets to be reflected" Field SHALL be 2 octets long, as shown and contains the octets that the Server MUST reflect in the Accept Session message as specified below.

The "Length of padding to reflect" Field SHALL be 2 octets long, and contain an unsigned binary value in units of octets. This field communicates the length of the padding in the TWAMP-Test Packet that the Session-Sender expects to be reflected, and the length of octets



The "Reflected octets" field SHALL contain the octets from the Request-TW-Session "Octets to be reflected" Field, and be 2 octets long, as shown.

In Truncate Padding mode, IF calculations on the Padding lengths reveal that there are insufficient octets supplied to produce equal-length Session-Sender and Session-Reflector test packets, then the Accept Field MUST be set to 3 = some aspect of the request is not supported.

3.4. Additional considerations

The value of the Modes Field sent by the Server in the Server Greeting message is the bit-wise OR of the mode values that it is willing to support during this session.

Thus, the last six bits of the Modes 32-bit Field are used. A client conforming to this extension of [\[RFC5357\]](#) MAY ignore the values in the first 24 bits of the Modes Field, or it MAY support other features that are communicated in these bit positions. (The first 24 bits are available for future protocol extensions.)

Other ways in which TWAMP extends OWAMP are described in [\[RFC5357\]](#).

[4.](#) Extended TWAMP Test

The TWAMP test protocol is similar to the OWAMP [[RFC4656](#)] test protocol with the exception that the Session-Reflector transmits test packets to the Session-Sender in response to each test packet it receives. TWAMP [section 4](#)[[RFC5357](#)] defines two additional test packet formats for packets transmitted by the Session-Reflector. The appropriate format depends on the security mode chosen. The new modes specified here utilize some of the padding octets within each test packet format, or require truncation of those octets depending on the security mode in use.

[4.1.](#) Sender Behavior

This section describes extensions to the behavior of the TWAMP Session-Sender.

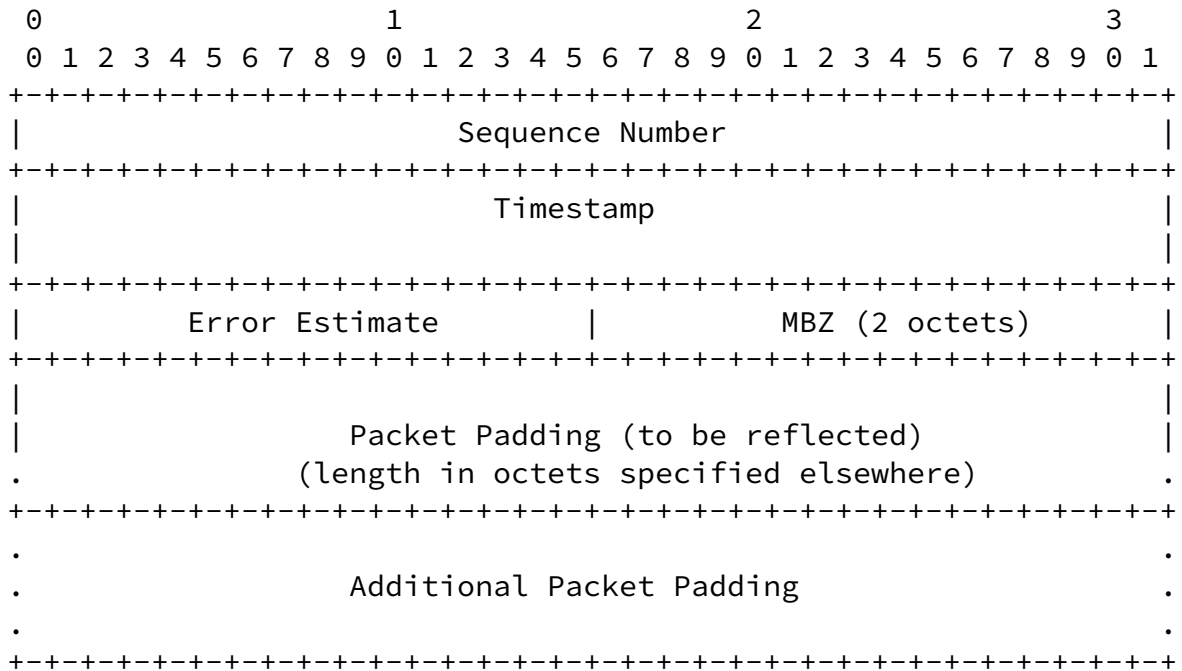
[4.1.1.](#) Packet Timings

The Send Schedule is not utilized in TWAMP, and this is unchanged in this memo.

[4.1.2.](#) Packet Formats and Contents

The Session-Sender packet format and content follow the same procedure and guidelines as defined in [section 4.1.2 of \[RFC4656\]](#) (as indicated in [section 4.1.2](#) of TWAMP [[RFC5357](#)]).

The Reflect octets mode re-designates the original TWAMP-Test (and OWAMP-Test) Packet Padding Field (see [section 4.1.2 of \[RFC4656\]](#)), as shown below for unauthenticated mode:



The "Packet Padding (to be reflected)" Field SHALL correspond to the length of octets specified in the Request-TW-Session "Length of padding to reflect" Field to this test session. These are the octets that the Session-Sender expects will be returned by the Session-Reflector.

The length of the "Additional Packet Padding" Field is the difference between two fields in the Request-TW-Session command, as follows:

$$\text{"Additional Packet Padding", in octets} = \text{"Padding Length"} - \text{"Length of padding to reflect"}$$

[4.1.3.](#) Padding Truncation

When the Truncate Padding mode is selected and communicated in the Setup Response message, the Session-Sender MUST anticipate a minimum padding required to achieve equal size test packets in both directions. The amount of padding needed depends on BOTH the security mode (Unauthenticated/Authenticated/Encrypted) and whether the Reflect Octets mode is selected simultaneously.

When using the Truncate Padding mode, the Session-Sender MUST append sufficient Packet Padding octets to allow the same IP packet payload lengths to be used in each direction of transmission (this is usually desirable). To compensate for the Session-Reflector's larger test packet format, the Session-Sender MUST append at least 27 octets of

padding in Unauthenticated mode, and at least 56 octets in Authenticated and Encrypted modes.

When using the Reflect Octets mode simultaneously with the Truncate Padding mode, the Session-Sender MUST append at least 27 octets of padding plus the "Length of the padding to reflect" octets when operating in Unauthenticated mode. The Session-Sender MUST append at least 56 octets of padding plus the "Length of the padding to reflect" octets when operating in Authenticated and Encrypted modes.

[4.2.](#) Reflector Behavior

The TWAMP Reflector follows the procedures and guidelines in [section 4.2 of \[RFC5357\]](#), with the following additional functions:

- o Reflect Octets mode: Designated octets in the "Packet Padding (to be reflected)" field of the Session-Sender's test packet MUST be included in the Session-Reflector's test packet.
- o Truncate Padding mode: Octets in the packet padding field of the Session-Sender's test packet MUST be truncated so that the length of the Session-Reflector's test packet equals the length of the Session-Sender's test packet.

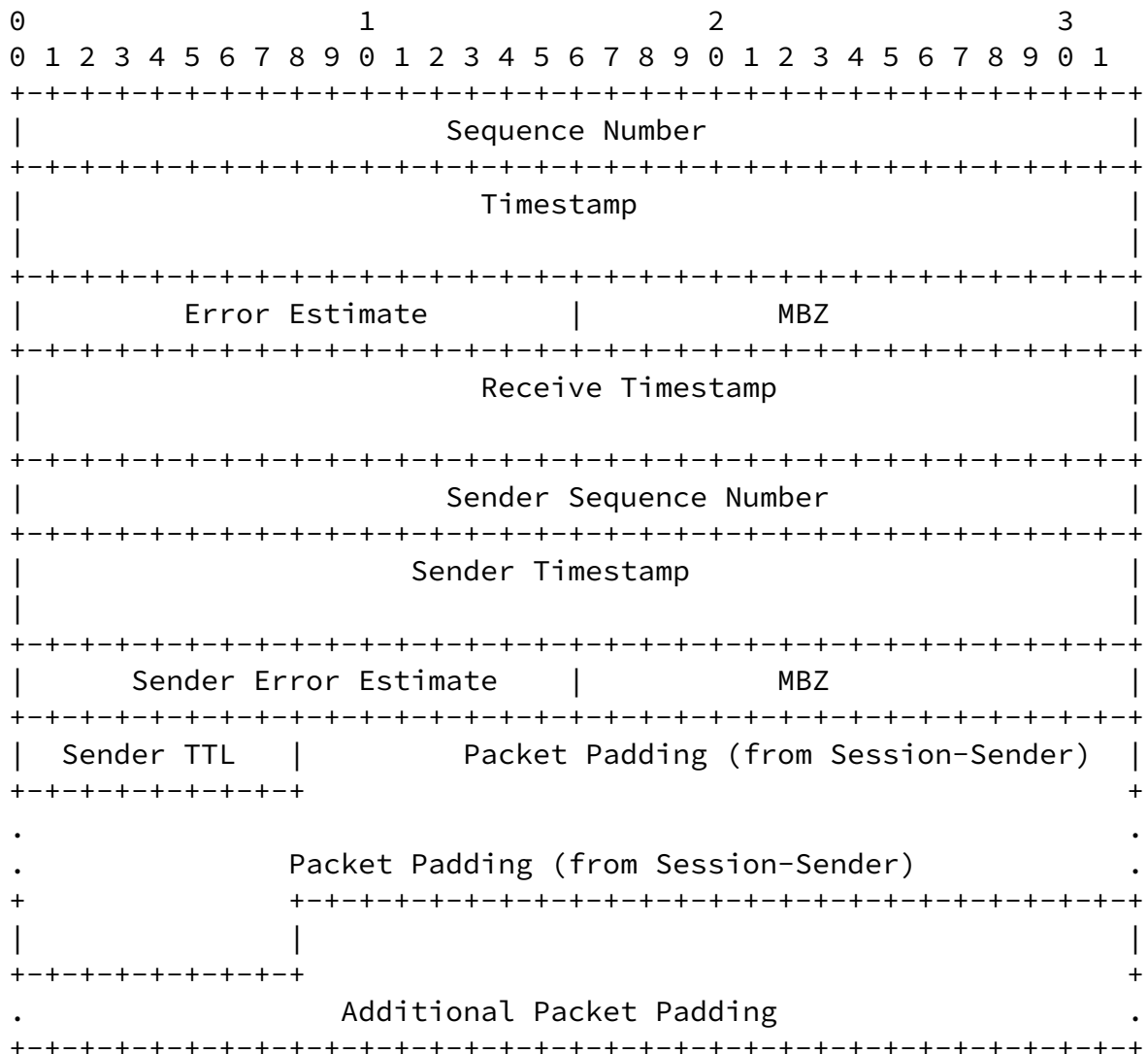
[4.2.1.](#) Packet Format and Contents

The Reflect Padding feature re-designates the packet padding field, as shown below for unauthenticated mode:

Internet-Draft

TWAMP Reflect Octets

October 2008



The "Packet Padding (from Session-Sender)" field MUST be the same octets as the "Packet Padding (to be reflected)" field in the Session-Sender's test packet, and therefore MUST conform to the

length specified in the Request-TW-Session message.

IF the test packet length is truncated within the padding fields in conformance with the RECOMMENDED truncation process in TWAMP [section 4.2.1 \[RFC5357\]](#), THEN ALL padding designated to be reflected MUST be reflected by Session-Reflectors using this feature.

[4.2.2](#). Padding Truncation

Note that the Session-Reflector Test Packet Formats are larger than the Sender's formats. When the Truncate Padding mode is selected and communicated in the Setup Response message, the Session-Reflector must truncate a specific number of padding octets to achieve equal size test packets in both directions. The number of octets truncated depends on BOTH the security mode (Unauthenticated/Authenticated/Encrypted) and whether the Reflect octets mode is selected

Morton & Ciavattone

Expires April 29, 2009

[Page 11]

Internet-Draft

TWAMP Reflect Octets

October 2008

simultaneously.

When using the Truncate Padding mode, the Session-Reflector MUST truncate exactly 27 octets of padding in Unauthenticated mode, and exactly 56 octets in Authenticated and Encrypted modes. The Session-Reflector MAY re-use the Sender's Packet Padding (since the requirements for padding generation are the same for each), and in this case the Session-Reflector MUST truncate the padding such that the highest number octets are discarded.

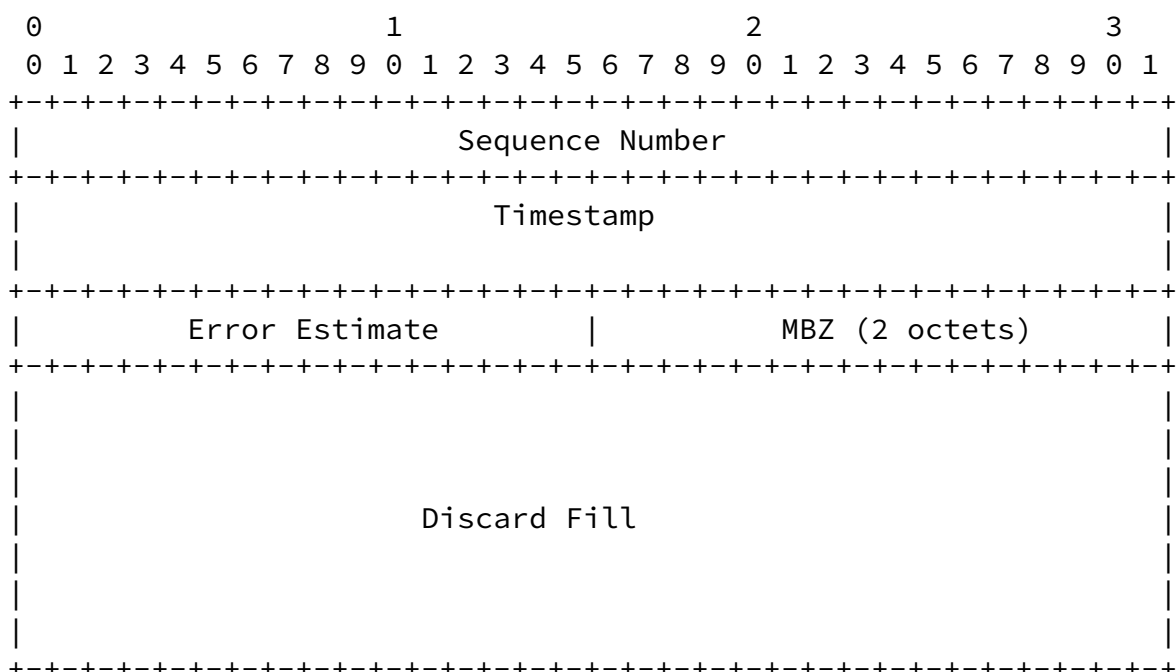
When simultaneously using the Truncate Padding mode AND Reflect octets mode, the Session-Reflector MUST reflect the designated octets from the Session-Sender's test packet in the "Packet Padding (from Session-Sender)" Field, and MAY re-use additional Packet Padding from the Session-Sender. The Session-Reflector MUST truncate the padding such that the highest number octets are discarded, and the test packet length equals the Session-Sender's packet length.

[5](#). Possible Alternative

If new TWAMP-Test packet formats are defined, the Reflect Octets and Truncate Padding modes could be folded into one new mode.

This Alternative is illustrated for discussion purposes.

New Session-Sender Test Packet Format:

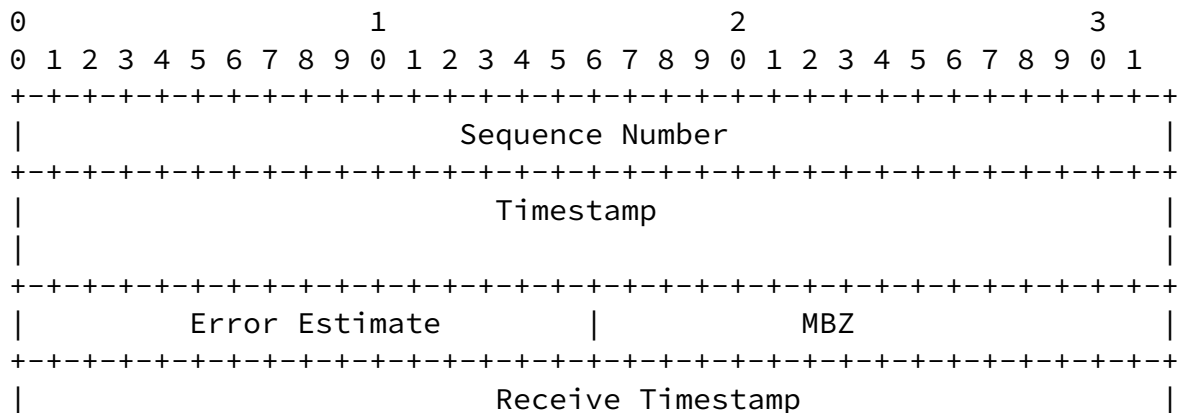


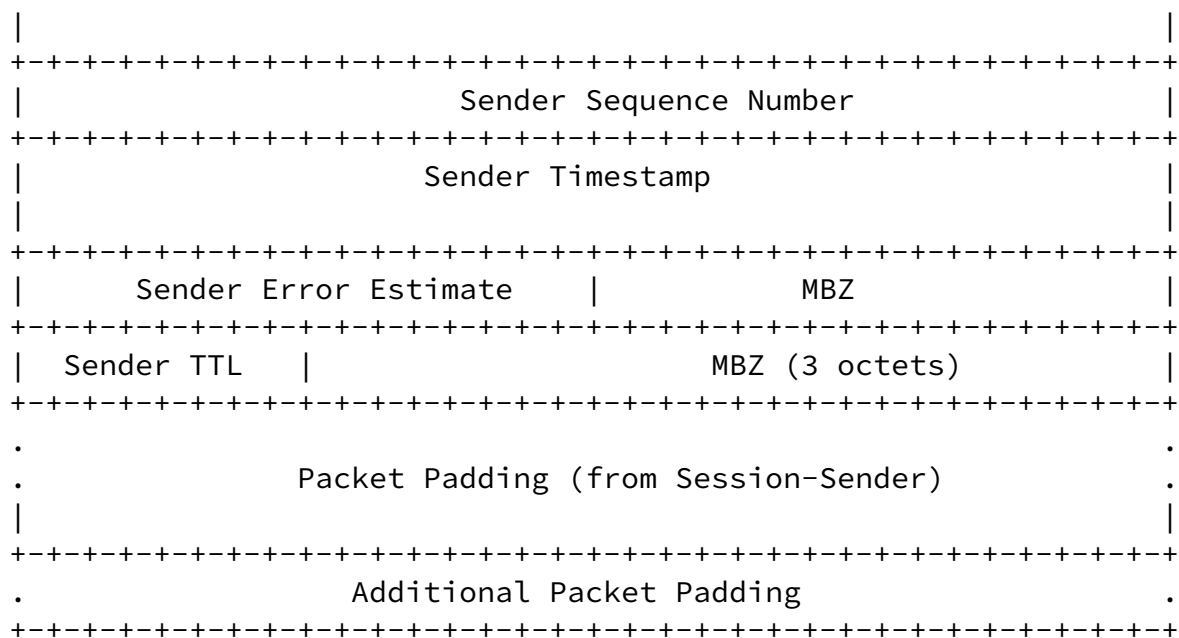
```

|
|           Packet Padding (to be reflected)           |
|           (length in octets specified elsewhere)     |
.-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
.
.           Additional Packet Padding                   .
.-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
The "Discard Fill" octets are discarded at the Session-Reflector.

```

New Session-Reflector Test Packet format:





6. Security Considerations

These extended modes of operation do not appear to permit any new attacks on hosts communicating with core TWAMP [[RFC5357](#)] ???

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

7. IANA Considerations

This memo adds two mode combinations to the IANA registry for the TWAMP Modes Field, and describes behavior when the new modes are used. This field is a recognized extension mechanism for TWAMP.

7.1. Registry Specification

IANA has created a TWAMP-Modes registry (as requested in [[I-D.ietf-ippm-more-twamp](#)]). TWAMP-Modes are specified in TWAMP

Server Greeting messages and Set-up Response messages, as described in [section 3.1 of \[RFC5357\]](#), consistent with [section 3.1 of \[RFC4656\]](#), and extended by this memo. Modes are indicated by setting bits in the 32-bit Modes field. Thus, this registry can contain a total of 32 possible values.

[7.2.](#) Registry Management

Because the Modes registry can contain only thirty-two values, and because TWAMP is an IETF protocol, this registry must be updated only by "IETF Consensus" as specified in [\[RFC2434\]](#) (an RFC documenting registry use that is approved by the IESG). For the Modes registry, we expect that new features will be assigned using monotonically increasing bit positions and in the range [0-31] and the corresponding values, unless there is a good reason to do otherwise.

[7.3.](#) Experimental Numbers

No experimental values are currently assigned for the Modes Registry.

[7.4.](#) Registry Contents

TWAMP Modes Registry is recommended to be augmented as follows:

Value	Description	Semantics Definition
0	Reserved	
1	Unauthenticated	RFC4656, Section 3.1
2	Authenticated	RFC4656, Section 3.1
4	Encrypted	RFC4656, Section 3.1
8	Unauth. TEST protocol, Auth. CONTROL	draft-ietf-more-twamp (3)

xxx	Reflect Octets Capability	this memo, section 3.1 new bit position (X)
yyy	Truncate Padding Capability	this memo, section 3.1 new bit position (Y)

The suggested values are

X=4, xxx=16

Y=5, yyy=32

8. Acknowledgements

The authors would like to thank Walt Steverson for helpful review and comments.

9. References

9.1. Normative References

[I-D.ietf-ippm-more-twamp]

Morton, A. and K. Hedayat, "More Features for TWAMP", [draft-ietf-ippm-more-twamp-00](#) (work in progress), October 2008.

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

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 2434](#), October 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.

9.2. Informative References

[x] "".

Internet-Draft

TWAMP Reflect Octets

October 2008

Authors' Addresses

Al Morton
AT&T Labs
200 Laurel Avenue South
Middletown,, NJ 07748
USA

Phone: +1 732 420 1571
Fax: +1 732 368 1192
Email: acmorton@att.com
URI: <http://home.comcast.net/~acmacm/>

Len Ciavattone
AT&T Labs
200 Laurel Avenue South
Middletown,, NJ 07748
USA

Phone: +1 732 420 1239
Fax:
Email: lencia@att.com
URI:

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at

<http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.