Network Working Group
Internet-Draft
Updates: 5357 (if approved)
Intended status: Standards Track
Expires: January 1, 2012

A. Morton
L. Ciavattone
AT&T Labs

June 30, 2011

TWAMP Burst Rate Measurement Features
draft-morton-ippm-twamp-rate-00

Abstract

This memo describes two rate-measurement features for the core specification of TWAMP - the Two-Way Active Measurement Protocol: an optional capability where the reflector host responds with a controlled burst of test-session packets (instead of a single packet), and an optional test mode that requires the responder to measure a burst of test packets and communicate the results in truncated packet(s). Both features add the ability to control packet size in the tested direction, enabling asymmetrical packet size testing.

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].

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 January 1, 2012.

Copyright Notice

Table of Contents

1. Introduction 3
2. Purpose and Scope 3
3. TWAMP Control Extensions 4
3.1. Connection Setup with New Features 5
3.2. Burst Generation: Request-TW-Session Packet Format 5
3.3. Burst Measurement: Request-TW-Session Packet Format . . . 7
3.4. Burst Gen and Meas: Accept Session Packet Format 8
3.5. Burst Gen and Meas: Stopping Test Sessions 8
3.6. Additional considerations 8
4. Burst Generation in TWAMP Test 9
4.1. Sender Behavior 9
4.1.1. Packet Timings 9
4.1.2. Packet Formats and Contents 9
4.2. Reflector Behavior 10
4.2.1. Session-Reflector Burst Packet Format and Contents . . 10
5. Burst Measurement in TWAMP Test 12
5.1. Sender Behavior 12
5.1.1. Packet Timings 12
5.1.2. Packet Formats and Contents 12
5.2. Reflector Behavior 13
5.2.1. Session-Reflector Burst Measurement Response Packet Format and Contents 14
6. Special Case of One-packet Bursts 16
7. Security Considerations 16
8. IANA Considerations 16
8.1. Registry Specification 16
8.2. Registry Contents 17
9. Acknowledgements 17
10. References 17
10.1. Normative References 17
10.2. Informative References 18
Authors' Addresses 18

1. Introduction

TWAMP - the Two-Way Active Measurement Protocol [RFC5357] is an extension of the One-way Active Measurement Protocol, OWAMP [RFC4656]. The TWAMP specification gathered wide review as it was deployed, resulting in recommendations for new features.

This memo describes two closely-related features for TWAMP. When measuring packet delivery rate to end-systems, unique control and measurement capabilities become useful, especially when the path tested includes asymmetrical link speeds (as are often deployed in consumer Internet access services).

One feature is the OPTIONAL capability for the responder host to return a controlled burst of test-session packets (instead of a single packet).

Another is an optional sender packet format that requires the responder to measure a burst of test packets and communicate the results in a single packet.

Both features add the ability to control packet size in each direction, enabling asymmetrical packet size testing. Although TWAMP [RFC5357] recommends padding truncation to achieve symmetrical sizes (to compensate for the Session-Reflector's larger test packet header), these features configure test packet sizes when the test session is requested using the TWAMP-Control protocol.

We note that [draft-baillargeon-ippm-twamp-value-added-octets-01.txt] addresses a similar measurement problem, but places different requirements on the reflector host and does not include the asymmetrical size aspect.

This memo is an update to the TWAMP core protocol specified in [RFC5357]. Measurement systems are not required to implement the features described in this memo to claim compliance with [RFC5357].

Throughout this memo, the bits marked MBZ (Must Be Zero) MUST be set to zero by senders and MUST be ignored by receivers. Also, the HMAC (Hashed Message Authentication Code) MUST be calculated as defined in Section 3.2 of [RFC4656].

2. Purpose and Scope

The purpose of this memo is to define two OPTIONAL closely-related features for TWAMP [RFC5357]. The features enhance the TWAMP responder's capabilities to perform a simple operations on test

packets, and the capability to demand asymmetrical size TWAMP-Test packets.

The scope of the memo is limited to specifications of the following features:

- Burst Generation: the capability of the Session-Reflector to generate a burst of packets for return to the Session-Sender, and the corresponding TWAMP-Control messages to activate the capability between compliant hosts.

- Burst Measurement: the capability of the Session-Reflector to measure a burst of packets from the Session-Sender, report the key information (receive timestamps) in the response packet(s), and the corresponding TWAMP-Control messages to activate the capability between compliant hosts.

- Asymmetrical Size: the capability to ensure that TWAMP-Test protocol uses a specific packet size in each direction. This feature is combined with the Burst features, and essentially adds a third simple capability when the Burst size = 1.

This memo extends the modes of operation through assignment of two new values in the Modes Field (see section 3.1 of[RFC4656] for the format of the Server Greeting message), while retaining backward compatibility with the core TWAMP [RFC5357] implementations. The two new values correspond to the two features defined in this memo.

When the Server and Control-Client have agreed to use the Burst Generation mode during control connection setup, then the Control-Client, the Server, the Session-Sender, and the Session-Reflector MUST all conform to the requirements of that mode, as identified below.

When the Server and Control-Client have agreed to use the Burst Measurement mode during control connection setup, then the Control-Client, the Server, the Session-Sender, and the Session-Reflector MUST all conform to the requirements of that mode, as identified below.

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 two such extensions.

3.1. Connection Setup with New Features

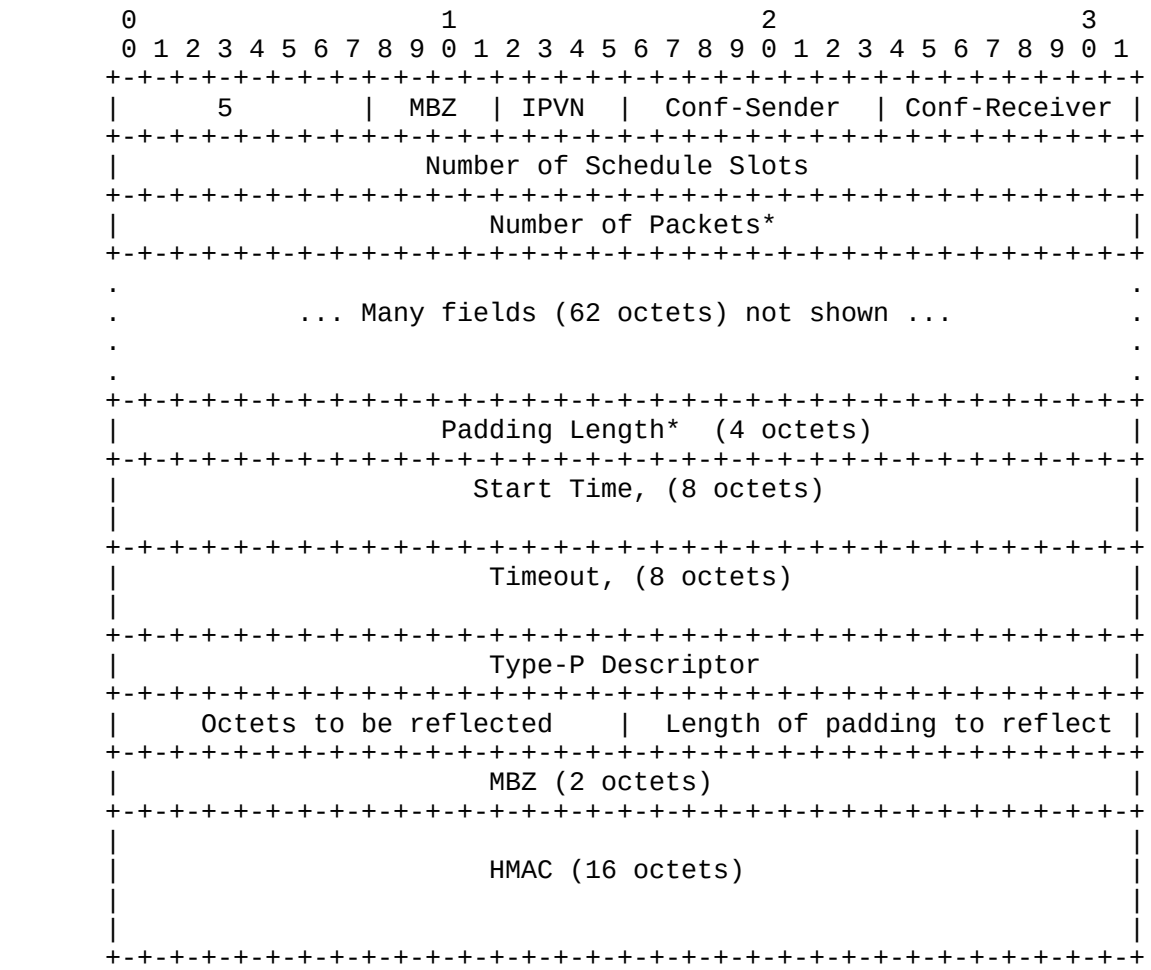
TWAMP connection establishment follows the procedure defined in section 3.1 of [RFC4656] and section 3.1 of [RFC5357]. The new features require two new bit positions (and values). See the IANA section for details on the assigned values and bit positions.

The Server sets one or both of the new bit positions in the Modes Field of the Server Greeting message to indicate its capabilities and willingness to operate in either of these modes if desired.

If the Control-Client intends to operate all test sessions invoked with this control connection using one of the new modes, it MUST set the Mode Field bit corresponding to each function in the Setup Response message. With this and other extensions, the Control-Client MAY set multiple Mode Field bits in the Setup Response message, but these new features are mutually exclusive, and MUST NOT be used together.

3.2. Burst Generation: Request-TW-Session Packet Format

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



* = re-interpreted field

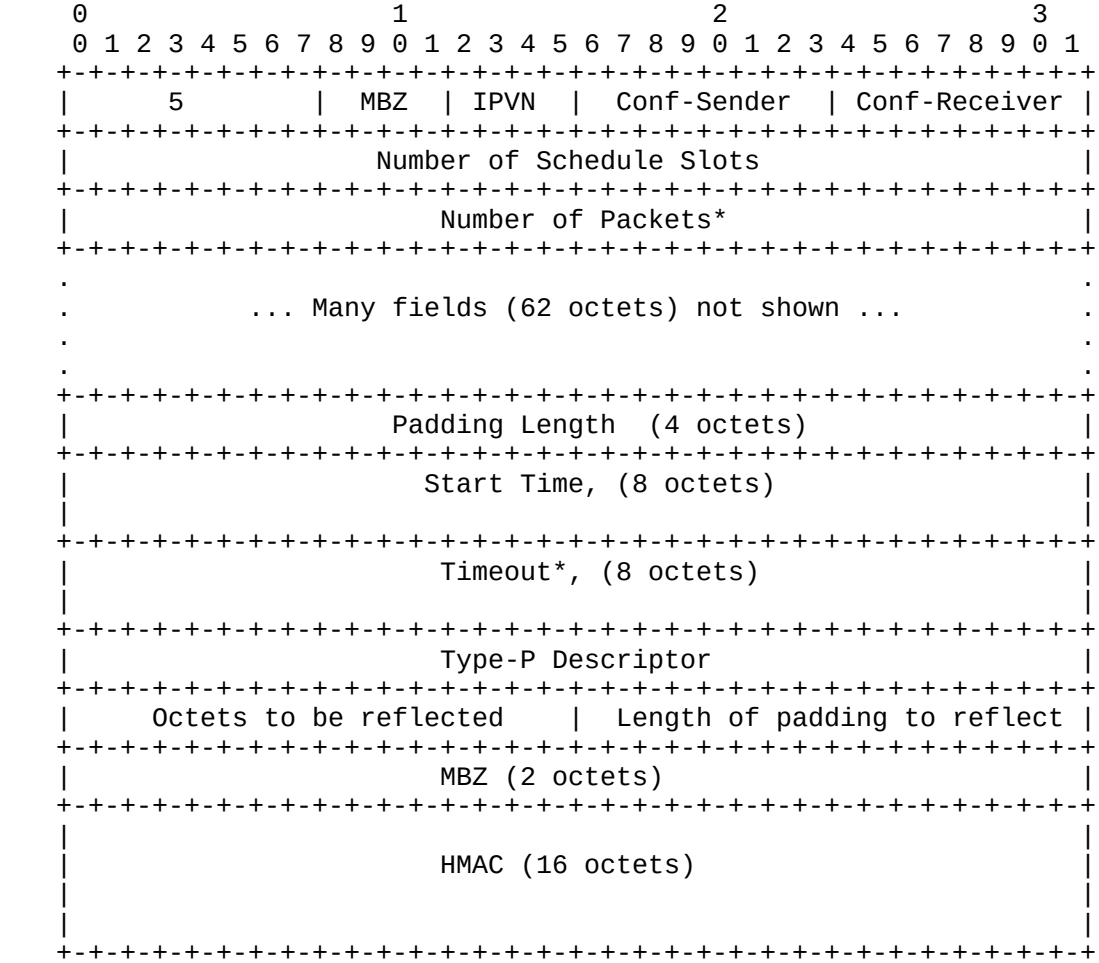
Two re-interpreted fields appear in the Request-TW-Session command when using Burst Generation mode:

1. Number of Packets: In this mode, re-interpreted as the number of packets that the Session-Reflector MUST generate in each Burst.

2. Packet Padding Length: In the mode, re-interpreted as the number of octets the Session-Reflector MUST append to the Test packet header of each packet it generates as part of the burst. The Session-Reflector MUST NOT assume that the Session-Sender will use any packet padding, and MUST be prepared to generate the padding itself.

3.3. Burst Measurement: Request-TW-Session Packet Format

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



* = re-interpreted field

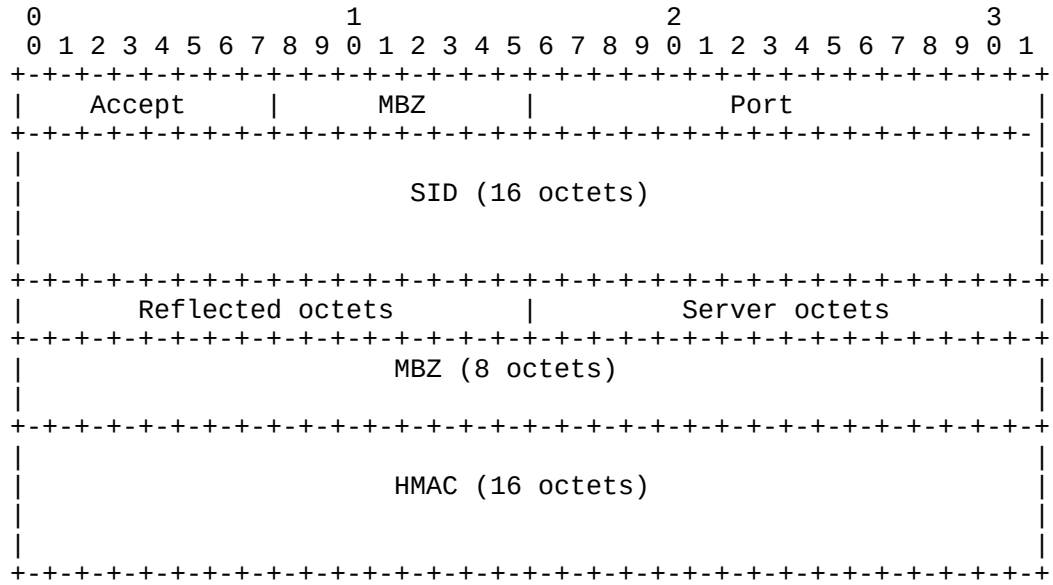
Two re-interpreted fields appear in the Request-TW-Session command when using Burst Measurement mode:

1. Number of Packets: In this mode, re-interpreted as the number of packets that the Session-Reflector MUST expect to measure as part of each Burst.

2. Timeout: In this mode, re-interpreted as the time to wait for all packets in a burst to arrive, expressed in the existing timestamp format used in TWAMP and OWAMP. In the case of lost packets, the Session-Reflector is commanded to wait through this time-out for packets in a burst to arrive.

3.4. Burst Gen and Meas: Accept Session Packet Format

The Accept Session command for the Burst feature is as shown in the packet format below (assuming the Reflect Octets feature is also in use).



3.5. Burst Gen and Meas: Stopping Test Sessions

The Control-Client SHALL stop in-progress test sessions using any standardized methods, including section 3.8 of [RFC5357] or the optional capability of [RFC5938].

3.6. 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.

We note that Burst Generation and Measurement features are incompatible with each other, and with the Symmetrical Size feature

described in [RFC6038], and MUST NOT be used in combination with those features.

With the publication of this memo as an RFC, the last 9 bit positions of the Modes 32-bit Field are used. A Control-Client conforming to this extension of [RFC5357] MAY ignore the values in the higher bits of the Modes Field, or it MAY support other features that are communicated in those bit positions. The other bits are available for future protocol extensions.

4. Burst Generation in 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. The Burst Generation feature modifies the behavior of TWAMP section 4[RFC5357]. This mode requires the Session-Sender to send a Burst-Initiation packet, and the Session-Reflector generates test session packets according to the configuration agreed using the TWAMP-Control protocol.

4.1. Sender Behavior

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

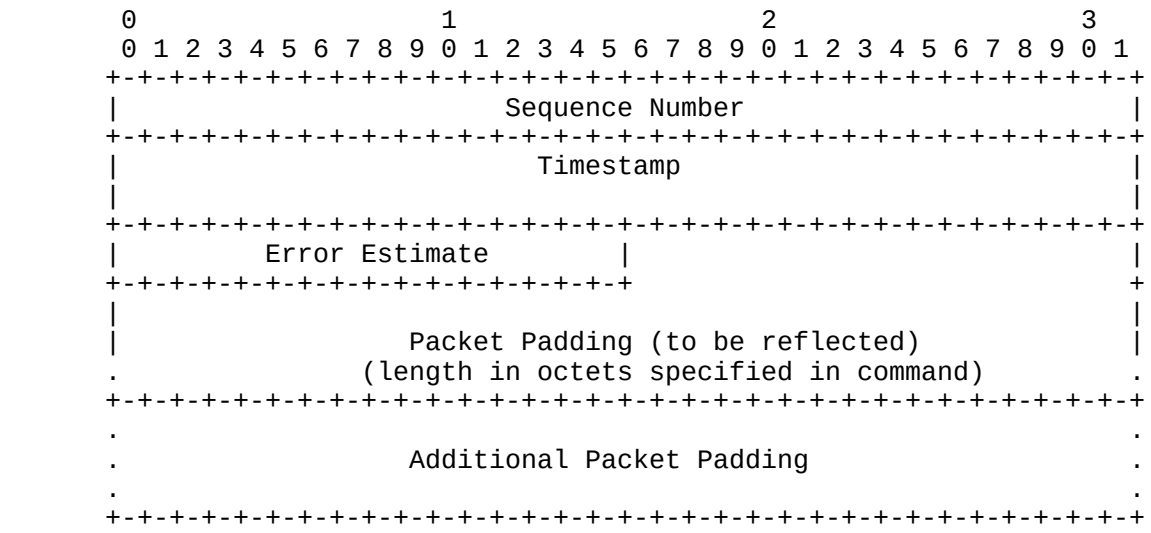
4.1.1. Packet Timings

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]).

This mode uses the original TWAMP-Test Packet Padding Field (see section 4.1.2 of [RFC4656]), or can be used with Reflect Octets feature as shown below for unauthenticated mode:



Burst Initiation Packet Format

The Sequence Number, Timestamp, and Error Estimate fields are the same as specified in section 4.1.2 of [RFC4656] in OWAMP.

We note that the format of the Burst Initiation packet has not been changed from the usual Session-Sender test packet format, to simplify adoption.

4.2. Reflector Behavior

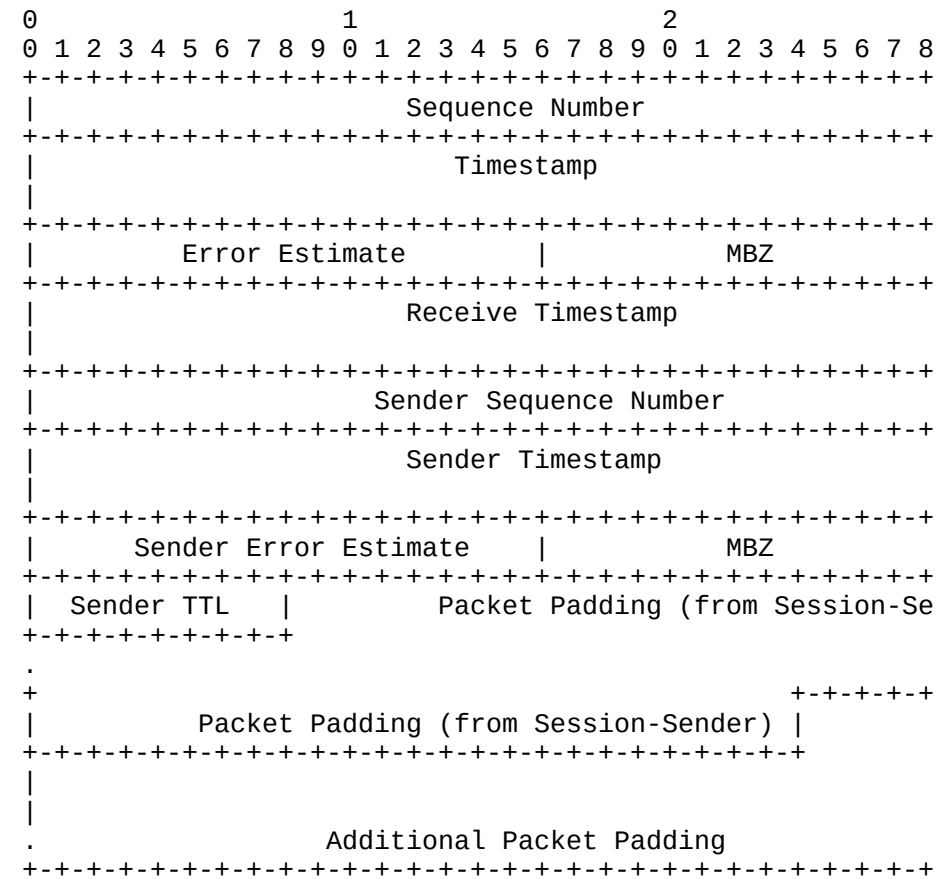
The TWAMP Reflector differs significantly from the procedures and guidelines in section 4.2 of [RFC5357]. The following new functions MUST be performed:

- o Recognition of the function of the Burst Initiation Packet used in this mode.

- o Generation of the required burst of test session packets, according to the configuration agreed in Request-TW-Session command, with the agreed number of packets in each burst and size of each packet in the burst.

4.2.1. Session-Reflector Burst Packet Format and Contents

The Burst Generation feature retains the usual Reflector packet fields, as shown below. When the Burst Generation mode is selected, the Session-Reflector SHALL use the following TWAMP-Test Packet Format in Unauthenticated mode (shown with Reflect Octets feature activated):



Section 4.2.1 of [RFC5357] describes the above fields as used in TWAMP, with one exception.

The Sequence Number field SHALL indicate the sequence number of each packet sent throughout the test session. The Sequence Number SHALL be increased by 1 for each packet. The initial Sequence Number SHALL be 0.

When one burst is complete, the Sequence Numbers SHALL continue to increment by 1 in the packets generated in response to the next burst.

The total Packet Padding octets SHALL have the length specified in the TWAMP-Control request for the appropriate test session. The Session-Reflector MAY need to generate its own packet padding, if the Burst Request packet does not include this field (or contains insufficient padding).

In any case, the Session-Reflector MAY re-use the Sender's Packet Padding (since the requirements for padding generation are the same for each) when possible.

The Session-Reflector SHALL send a series of TWAMP-Test Packets in response to reception of the Burst Initiation Packet, according to the configuration agreed in the Request-TW-Session command (number of packets and padding), and as immediately as possible. The Session-Reflector SHALL send all packets in a burst as close to back-to-back as possible (recognizing that lower layers may have spacing requirements that take precedence).

5. Burst Measurement in TWAMP Test

The Burst Measurement feature modifies the behavior of TWAMP section 4[RFC5357]. This mode requires the Session-Sender to send a Burst of test packets, and the Session-Reflector measures the burst of packets and reports the results in the Burst Response packet format(s), as described below.

5.1. Sender Behavior

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

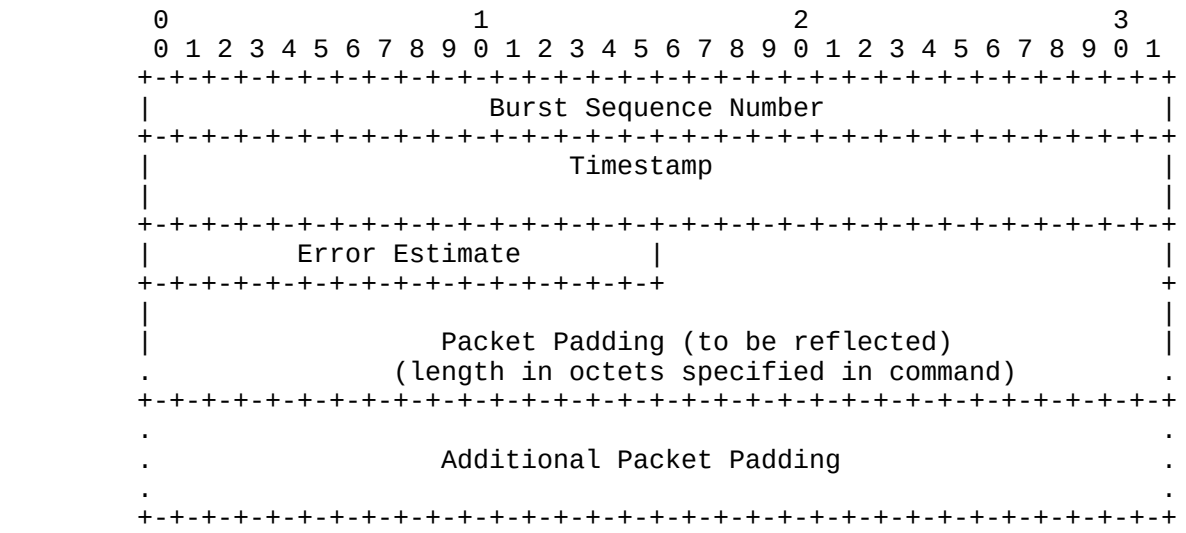
5.1.1. Packet Timings

The Session-Sender SHALL send all packets in a burst as close to back-to-back as possible (recognizing that lower layers may have spacing requirements that take precedence).

5.1.2. Packet Formats and Contents

The Session-Sender packet format and content SHALL comply with that defined in section 4.1.2 of [RFC4656] (as indicated in section 4.1.2 of TWAMP [RFC5357]).

This mode uses the original TWAMP-Test Packet Padding Field (see section 4.1.2 of [RFC4656]), or can be used with Reflect Octets feature as shown below for unauthenticated mode:



Session-Sender Burst Test Packet Format

The Burst Sequence Number field SHALL indicate the number of each burst. The Burst Sequence Number SHALL be increased by 1 for each burst, and remain the same for each packet in a burst. The initial number SHALL be 0.

When one burst is complete, the Burst Sequence Number used in the all packets of the next burst SHALL be increased by 1.

5.2. Reflector Behavior

The TWAMP Reflector differs slightly from the procedures and guidelines in section 4.2 of [RFC5357]. The following new functions MUST be performed:

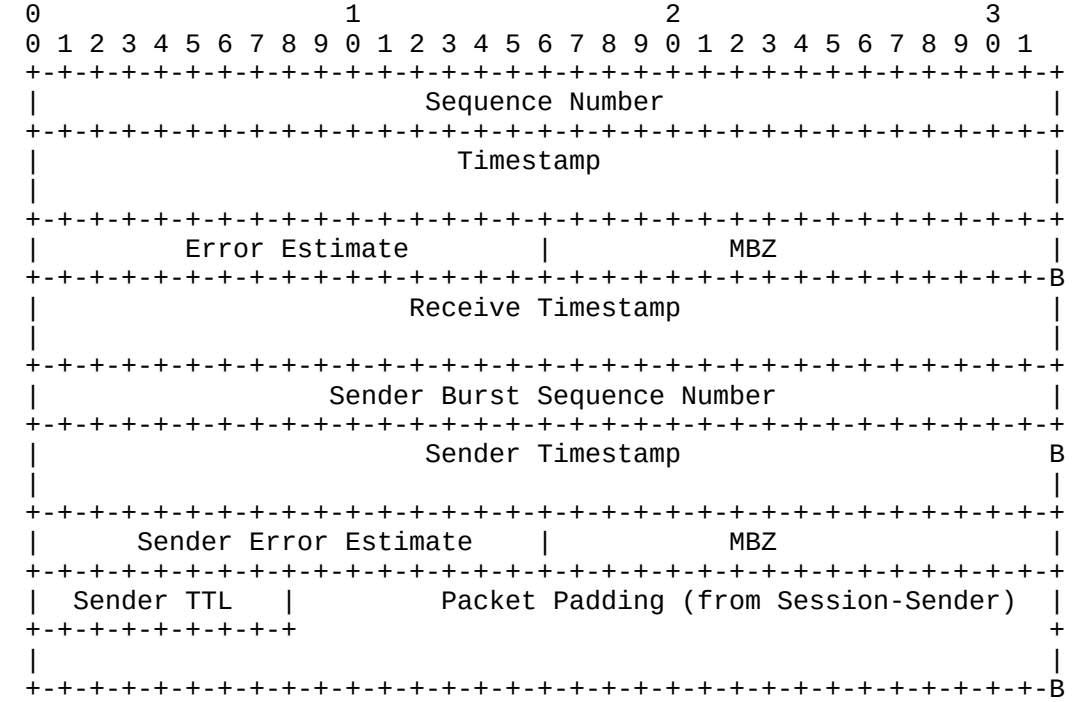
- o Recognition of the function of the Session-Sender Burst Test Packet Format used in this mode.
- o Processing the required bursts of test session packets, according to the configuration agreed in Request-TW-Session command, with the agreed length of the burst in packets and size of each packet in the burst, and the agreed Burst Time-out.
- o Response with an abbreviated Session-Reflector test packet as described below. For discussion, we will call this the 1-to-1 response.
- o OR - Response with the new Burst Measurement Response packet described below. For discussion, we will call this the

accumulated response.

We seek feedback from the IPPM working group on which of these two alternatives is preferable.

5.2.1. Session-Reflector Burst Measurement Response Packet Format and Contents

The Burst Measurement feature specifies a standard Session-Reflector packet to communicate the results, as shown below. When the Burst measurement mode is selected, the Session-Sender SHALL use the following Burst Measurement Response packet Format in Unauthenticated mode (shown with Reflect Octets feature also in use):



Session-Reflector Measurement Packet (1-to-1 response)

Section 4.2.1 of [RFC5357] describes the fields in the 1-to-1 response packet above; they are the same as used in TWAMP. The main difference is that Packet Padding SHALL be truncated on a 16 octet-word boundary, returning the minimum information to the Session-Sender.

All Timestamps SHALL be formatted according to the precedent set in section 4.1.2 of [RFC4656], which is to use [RFC1305] (and updated

version), as follows:

"The first 32 bits represent the unsigned integer number of seconds elapsed since 0h on 1 January 1900; the next 32 bits represent the fractional part of a second that has elapsed since then."

The Session-Reflector MUST truncate the Sender's Packet Padding, unless the Reflect Octets feature is also active in which case the Session_Reflector MAY re-use the Sender's Packet Padding (since the requirements for padding generation are the same for each) to reach a word boundary.

The Sender Timestamp field SHALL have the sender's timestamp from each packet received in the burst.

In 1-to-1 response mode, the Session-Reflector SHALL send a Session-Reflector Measurement Packet in response to every Session-Sender packet received, and as immediately as possible.

==========

In the accumulated response alternative, the Session-Reflector creates and holds all packet headers described above in a buffer, and sends them all at once in a single Session-Reflector test packet. The length of the burst and the path MTU MUST be coordinated to avoid fragmentation.

The first Session-Sender packet to arrive with a previously unseen Burst Sequence Number SHALL be designated as the "First" packet in that burst, and its timestamp is used in processing below.

As subsequent packets arrive, Session-Reflector SHALL:

- Maintain a count of packets with the same Burst Sequence Number (one burst).
- Time stamp each packet as it arrives and store the time stamp in a response packet structure with all fields complete, as in the 1-to-1 alternative.

When

- The count of packets with the same Burst Sequence Number equals the agreed Burst Length, OR
- The agreed Timeout expires (computed by a the time to the "First" Packet Timestamp), OR

- o The Burst Sequence Number increases from previous packets (indicating a new Burst is in progress),

then the current burst is determined to be complete.

When the Burst is complete, the Session-Reflector SHALL terminate the current burst processing as described above and send the Burst Measurement Response Packet to the Session-Sender as immediately as possible.

In Accumulated Response, the Burst Measurement Response Packet is a single packet with the concatenation of all previously-generated response packet formats in the information field.

6. Special Case of One-packet Bursts

When the Number of Packets field in the Request-TW-Session command equals 1, then the Burst Generation and Measurement modes are reduced to test sessions with controlled, asymmetrical packet sizes. A minimal size packet travels in one direction, and the measured direction uses a packet with all Packet Padding specified in the Request-TW-Session command.

7. 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].

8. IANA Considerations

This memo adds two modes 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.

8.1. Registry Specification

IANA has created a TWAMP-Modes registry (as requested in [RFC5618]). 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 that

correspond to values in the Modes registry. For the TWAMP-Modes registry, we expect that new features will be assigned increasing registry values that correspond to single bit positions, unless there is a good reason to do otherwise (more complex encoding than single bit positions may be used in the future, to access the 2^32 value space).

8.2. Registry Contents

TWAMP Modes Registry is recommended to be augmented as follows:

Value	Description	Semantics Definition
xxx	Burst Generation Capability	this memo, section 3.1 new bit position (X)
yyy	Burst Measurement	this memo, section 3.1 new bit position (Y)

>>>IANA: change xxx, yyy, X, Y, and RFC???? to the assigned values

The suggested values are

X=7, xxx=128

Y=8, yyy=256 <<<<

9. Acknowledgements

The authors thank folks for review and comment.

10. References

10.1. Normative References

[RFC1305] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

[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.

[RFC5938] Morton, A. and M. Chiba, "Individual Session Control Feature for the Two-Way Active Measurement Protocol (TWAMP)", RFC 5938, August 2010.

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

10.2. Informative References

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: