Network Working Group	A. Morton	
Internet-Draft	AT&T Labs	
Updates: 5357 (if approved)	M. Chiba	
Intended status: Standards Track	Cisco Systems	
Expires: September 1, 2010	February 28, 2010	

TOC

Individual Session Control Feature for TWAMP
draft-ietf-ippm-twamp-session-cntrl-04

Abstract

The IETF has completed its work on the core specification of TWAMP - the Two-Way Active Measurement Protocol. This memo describes an OPTIONAL feature for TWAMP, that gives the controlling host the ability to start and stop one or more individual test sessions using Session Identifiers. The base capability of the TWAMP protocol requires all test sessions previously requested and accepted to start and stop at the same time.

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

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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/1id-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 September 1, 2010.

Copyright Notice

Copyright (c) 2010 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 BSD License.
This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction
2. Purpose and Scope
3. TWAMP Control Extensions
    3.1. Connection Setup with Individual Session Control
    3.2. Start-N-Sessions Command with Individual Session Control
    3.3. Start-N-Ack Command with Individual Session Control
    3.4. Stop-N-Sessions Command with Individual Session Control
    3.5. Stop-N-Ack Command with Individual Session Control
    3.6. SERVWAIT Timeout Operation
    3.7. Additional considerations
4. TWAMP Test with Individual Session Control
    4.1. Sender Behavior
    4.2. Reflector Behavior
5. Security Considerations
6. IANA Considerations
    6.1. Registry Specification
    6.2. Registry Management
    6.3. Experimental Numbers
    6.4. Registry Contents
7. Acknowledgements
8. References
    8.1. Normative References

8.2. Informative References
§ Authors' Addresses

---

1. Introduction

TOC

The IETF has completed its work on the core specification of TWAMP - the Two-Way Active Measurement Protocol [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, “A Two-Way Active Measurement Protocol (TWAMP),” October 2008.). TWAMP is an extension of the One-way Active Measurement Protocol, OWAMP [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, “A One-way Active Measurement Protocol (OWAMP),” September 2006.). 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 of 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 an OPTIONAL feature for TWAMP. TWAMP (and OWAMP) start all previously requested and accepted test sessions at once. This feature allows the Control-Client to control individual test sessions on the basis of their Session Identifier (SID). This feature permits a short duration TWAMP test to start (and/or stop) during a longer test. This feature permits a specific diagnostic test to begin if intermediate results indicate that the test is warranted, for example. This feature requires a Mode bit position assignment and the assignment of two new TWAMP command numbers (for the augmented Start and Stop commands). This feature also specifies a new Stop-ACK Server response, to complete the symmetry of the session stopping process in the same way as the Start-ACK response.

Implementers of this feature MAY also wish to implement the "Reflect Octets" feature, described in [I-D.ietf-ippm-twamp-reflect-octets] (Morton, A. and L. Ciavattone, “TWAMP Reflect Octets and Symmetrical Size Features,” April 2010.), once it has been published as an RFC. This feature allows a Control-Client to insert a locally-specified request number into the Request-TW-Session command (in octets originally designated MBZ=Must Be Zero), and a compliant Server will return the request number in its reply (Accept message).

This memo is intended to be an update to the TWAMP core protocol specified in [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, “A Two-Way Active Measurement Protocol (TWAMP),” October 2008.). It is not required to implement the feature described in this memo to claim compliance with [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, “A Two-Way Active Measurement Protocol (TWAMP),” October 2008.).

Throughout this memo, the bits marked MBZ (Must Be Zero) MUST be set to zero by senders and MUST be ignored by receivers.

---

2. Purpose and Scope

TOC

The purpose of this memo is to describe an additional OPTIONAL function and feature for TWAMP [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.). The feature needs a clear description so it can be discussed and (hopefully) adopted in the IP Performance Metrics Charter.
The scope of the memo is currently limited to specifications of the following features:

1. Extension of the modes of operation through assignment of a new value in the Mode field to communicate feature capability and use,

2. the definitions of augmented start session and stop session commands (with corresponding acknowledgements), and

3. the definition of related procedures for TWAMP entities.

The motivation for this feature is the ability to start and stop individual test sessions at will, using a single TWAMP-control connection.
When the Server and Control-Client have agreed to use the Individual Session Control 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. The original TWAMP-Control Start and Stop commands MUST NOT be used.

---

3. TWAMP Control Extensions

TOC

TWAMP-Control protocol is a derivative of the OWAMP-Control protocol, and provides two-way measurement capability. TWAMP [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.) 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 Individual Session Control

TOC

TWAMP-Control connection establishment follows the procedure defined in section 3.1 of [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.) OWAMP. The Individual Session Control mode requires one new bit position (and value) to identify the ability of the Server/Session-Reflector to start and stop specific sessions (according to their Session Identifier, or SID). This new feature requires an additional TWAMP mode bit assignment 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, Auth. CONTROL	RFC5618, Section 3.1
zzz	Individual Session Control	this memo, bit position (Z)

In the original OWAMP mode 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] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.)). In the [RFC5618] (Morton, A. and K. Hedayat, "Mixed Security Mode for the Two-Way Active Measurement Protocol (TWAMP)," August 2009.) memo, bit position (3) allows a different security mode in the Test protocol and uses the unauthenticated test packet format.
If the Server sets the new bit position (bit position Z) in the Server Greeting message to indicate its capabilities, then the Server and Session-Reflector MUST comply with the requirements of this memo to control sessions on an individual basis if desired.
If the Control-Client intends to control sessions on an individual basis (according to the requirements in this memo), it MUST set the mode bit (Z, corresponding to the new mode) in the Setup Response message. This means that:

1. The Control-Client and the Server MUST use the start and stop commands intended for individual session control and the corresponding acknowledgements, as defined in the sections that follow.

2. The Control-Client and the Server MUST NOT use the start and stop commands (2 and 3) and the acknowledgement defined in

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

The Control-Client MUST also set one mode bit to indicate the chosen security mode (currently bits 0, 1, 2, or 3), consistent with the modes offered by the Server. The Control-Client MAY also set Modes bit Z with other features and bit positions (such as the reflect octets feature). If the Control-Client has selected the Reflect Octets feature [I-D.ietf-ippm-twamp-reflect-octets] (Morton, A. and L. Ciavattone, “TWAMP Reflect Octets and Symmetrical Size Features,” April 2010.) in combination with the Individual Session Control feature (after the Server identified its capability), AND utilizes the feature to insert a locally-specified request number in the Request-TW-Session command, THEN the Control Client MAY send more than one Request-TW-Session command to a given Server without waiting for the corresponding Accept-Session message. In such a case the Access-Session response reflects the locally-specified request number. Note that when the Reflect Octets feature is being used all Request-TW-Session command and Accept-Session responses MUST include the locally-specified request number.

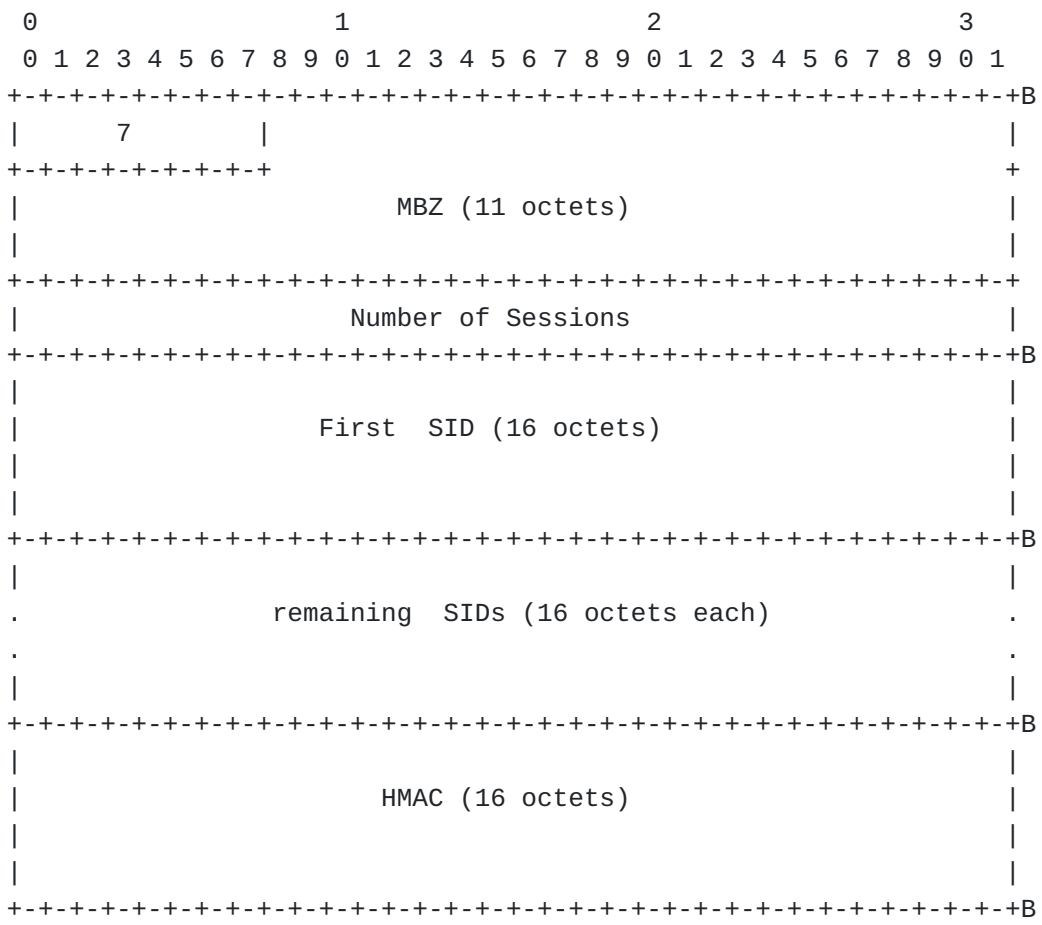
3.2. Start-N-Sessions Command with Individual Session Control

TOC

Having

- *initiated Individual Session Control mode in the Setup Response,
- *requested one or more test sessions, and
- *received affirmative Accept-Session response(s),

a TWAMP Client MAY start the execution of one or more test sessions by sending a Start-N-Sessions message to the Server (note that "N" indicates that this command is applicable to one or more sessions, and does not change with the number of sessions identified in the command). The format of the Start-N-Sessions message is as follows:



The Command Number value of 7 indicates that this is a Start-N-Sessions command. The Control-Client MUST compose this command, and the Server MUST interpret this command, according to the field descriptions below. The Number of Sessions field indicates the count of sessions that this Start command applies to, and must be one or greater. The number of SID fields that follow MUST be equal to the value in the Number of Sessions field (otherwise, the command MUST NOT be affirmed with a zero Accept field in the Start-N-Ack response).

All SID fields are constructed as defined in the last paragraph of OWAMP section 3.5 [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.) (and referenced in TWAMP). Note that the SID is assigned by the Server during the session request exchange.

The message is terminated with a single block HMAC, as illustrated above.

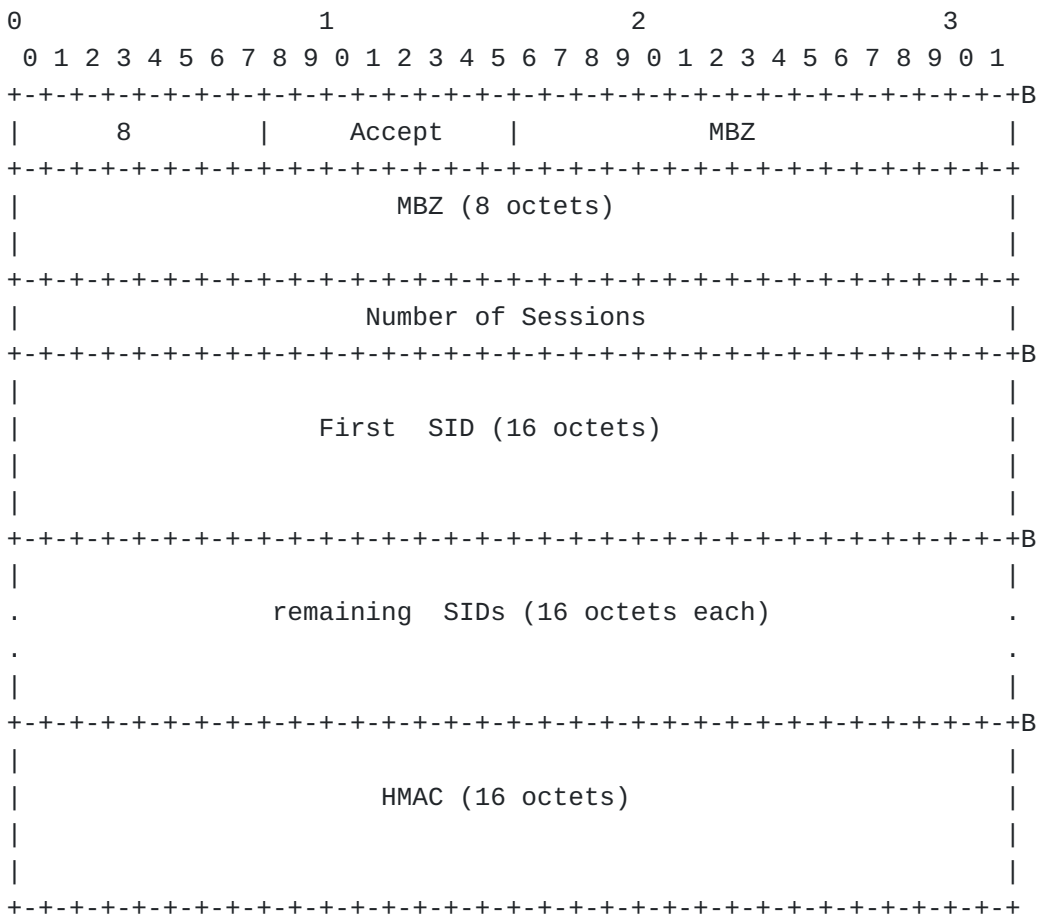
The Server MUST respond with one or more Start-N-Ack messages (which SHOULD be sent as quickly as possible). Start-N-Ack messages SHALL have the format defined in the next session.

When using Individual Session Control mode and its Start-N-Ack command as described in the next section, multiple Start-N-Sessions commands MAY be sent without waiting for acknowledgement, and the Start-N-sessions commands MAY arrive in any order.

3.3. Start-N-Ack Command with Individual Session Control

TOC

The Server responds to the Start-N-Sessions command (for one or more specific sessions referenced by their SIDs) with one or more Start-N-Ack commands with Accept fields corresponding to one or more of the SIDs. This allows for the possibility that a Server cannot immediately start one or more the sessions referenced in a particular Start-N-Sessions command, but can start one or more of the sessions.
The format of the message is as follows.



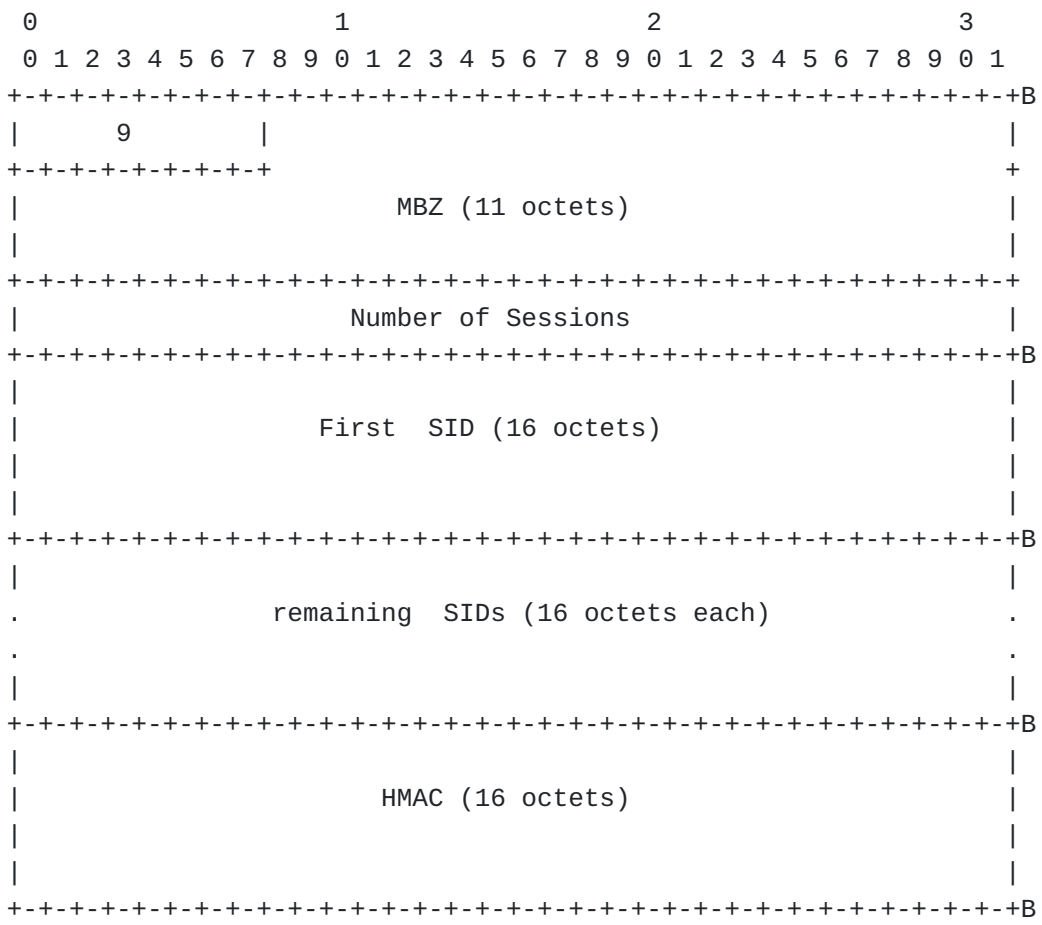
The Command Number value of 8 indicates that this is a Start-N-Ack message. The Server MUST compose this command, and the Control-Client MUST interpret this command, according to the field descriptions below. The Accept Field values are defined in OWAMP section 3.3 [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.).
The Number of Sessions field indicates the count of sessions that this Start-N-Ack command applies to, and must be one or greater. The number

of SID fields that follow MUST be equal to the value in the Number of Sessions field.
All SID fields are constructed as defined in the last paragraph of OWAMP section 3.5 [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, “A One-way Active Measurement Protocol (OWAMP),” September 2006.) (and referenced in TWAMP). Note that the SID is assigned by the Server during the session request exchange.
The message is terminated with a single block HMAC, as illustrated above.
Note that the SIDs for all Sessions with the same 'Accept' code can be acknowledged using the same Start-N-Ack message.
For example, say that the Server receives a Start-N-Sessions command for SIDs 1, 2, 3, and 4. The Server determines that the resources for SID=3 are temporarily unavailable. The Server responds with two Start-N-Ack commands with fields as follows:
Accept = 0 Number of Sessions = 3 SIDs 1, 2, 4
Accept = 5 Number of Sessions = 1 SID 3

3.4. Stop-N-Sessions Command with Individual Session Control

TOC

The Stop-N-Sessions command can only be issued by the Control-Client. The command MUST contain at least one SID.
The TWAMP Stop-N-Sessions command for use in Individual Session Control mode is formatted as follows:



The Command Number value of 9 indicates that this is a Stop-N-Sessions command. The Control-Client MUST compose this command, and the Server MUST interpret this command, according to the field descriptions below. The Number of sessions field indicates the count of sessions that this Stop-N-Sessions command applies to. The SID is as defined in OWAMP (and TWAMP) section 3.5 [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, “A One-way Active Measurement Protocol (OWAMP),” September 2006.) and the value must be one or greater. The number of SID fields that follow MUST be equal to the value in the Number of Sessions field.

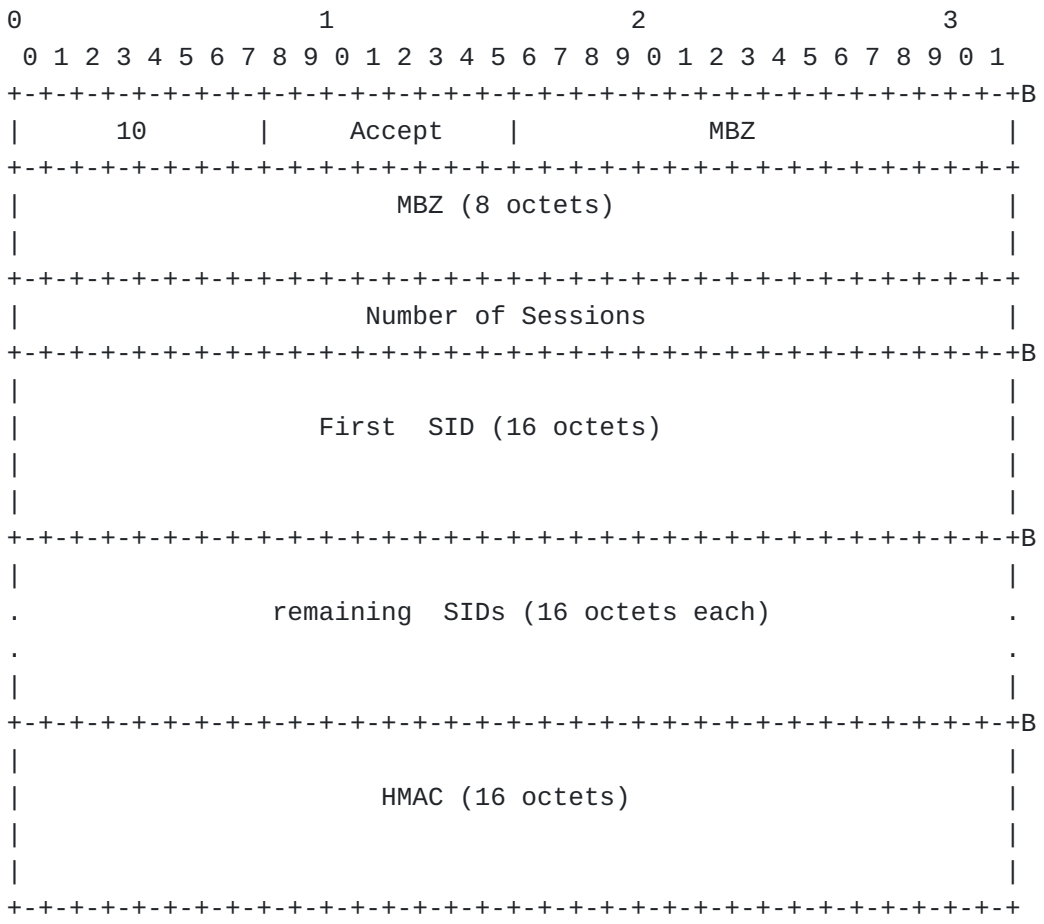
The message is terminated with a single block HMAC, as illustrated above.

The Server MUST respond with one or more Stop-N-Ack messages (which SHOULD be sent as quickly as possible). Stop-N-Ack messages SHALL have the format defined in the next session.

TOC

3.5. Stop-N-Ack Command with Individual Session Control

In response to the Stop-N-Sessions command (for one or more specific sessions referenced by their SIDs), the Server MUST reply with one or more Stop-N-Ack commands with Accept fields corresponding to one or more of the SIDs. This allows for the possibility that a Server cannot immediately stop one or more the sessions referenced in a particular Stop-N-Sessions command, but can stop one or more of the sessions.
The format for the Stop-N-Ack command is as follows:



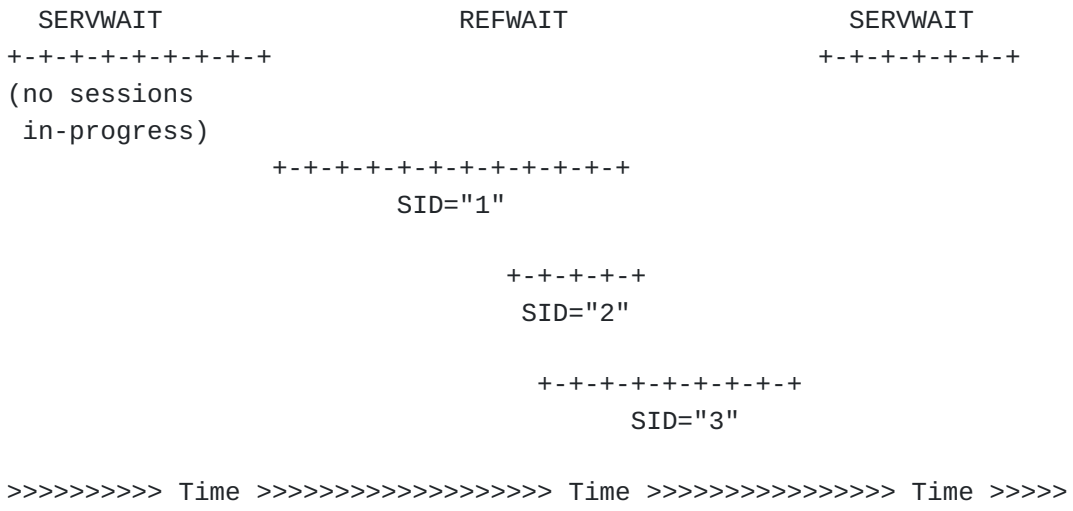
The Command Number value of 10 indicates that this is a Stop-N-Ack message. The Server MUST compose this command, and the Control-Client MUST interpret this command, according to the field descriptions below.
The Accept Field values are defined in OWAMP section 3.3 [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.).
The Number of Sessions field indicates the count of sessions that this Stop-N-Ack command applies to, and must be one or greater. The number of SID fields that follow MUST be equal to the value in the Number of Sessions field.
All SID fields are constructed as defined in the last paragraph of OWAMP section 3.5 [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol

(OWAMP)," September 2006.) (and referenced in TWAMP). Note that the SID is assigned by the Server during the session request exchange.
The message is terminated with a single block HMAC, as illustrated above.
Note that the SIDs for all Sessions with the same 'Accept' code can be acknowledged using the same Stop-N-Ack message.

3.6. SERVWAIT Timeout Operation

TOC

Section 3.1 of [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.) describes the operation of the optional SERVWAIT timer. In normal TWAMP operation, the Server suspends monitoring the SERVWAIT timer while test sessions are in progress. When the Individual Session Control feature is utilized, this suspension is extended to cover the time when ANY test session is in progress.
Thus, the Server SHALL suspend monitoring control connection activity after receiving any Start-N-Sessions command, and after receiving a Stop-N-Sessions command for all corresponding SIDs (and no test sessions are in-progress), OR when REFWAIT expires on ALL test sessions initiated by a TWAMP-Control connection, then the SERVWAIT monitoring SHALL resume (as though a Stop-N-Sessions command had been received).
An implementation which supports the SERVWAIT timeout option SHOULD also implement the REFWAIT timeout option.
The diagram below illustrates the operation of timers SERVWAIT and REFWAIT.



TOC

3.7. 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.
With the publication of this feature, bit positions 0 through (Z=4) of the Modes 32-bit field are used. A Control-Client MAY ignore bit positions greater than 2 in the Modes Field, or it MAY support OPTIONAL features that are communicated in bit positions 3 and higher. (The unassigned bits are available for future protocol extensions.)
Other ways in which TWAMP extends OWAMP are described in [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.).

---

4. TWAMP Test with Individual Session Control

TOC

The TWAMP test protocol is similar to the OWAMP [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.) 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 [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.) defines two different test packet formats, one for packets transmitted by the Session-Sender and one for packets transmitted by the Session-Reflector. As with OWAMP-Test protocol there are three security modes: unauthenticated, authenticated, and encrypted. Unauthenticated mode has one test packet format, while authenticated and encrypted modes use another (common) format.

4.1. Sender Behavior

TOC

The individual session control feature requires that the sender MUST manage test sessions according to their SID. Otherwise, the sender behavior is as described in section 4.1 of [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.).

TOC

4.2. Reflector Behavior

The TWAMP Reflector follows the procedures and guidelines in section 4.2 of [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.), with the following additional functions required by this feature:

- *The Session-Reflector MUST manage all test sessions accepted according to their SID.

- *Upon receipt of a TWAMP-Control Stop-N-Sessions command referencing a specific session/SID, the Session-Reflector MUST ignore TWAMP-Test packets (in the same session/SID) that arrive at the current time plus the Timeout (in the Request-TW-Session command and assuming subsequent acknowledgement). The Session-Reflector MUST NOT generate a test packet to the Session-Sender for packets that are ignored.

- *If the RECOMMENDED REFWAIT timer is implemented, it SHOULD be enforced when any test session is in-progress (started and not stopped).

---

5. Security Considerations

TOC

The security considerations that apply to any active measurement of live networks are relevant here as well. See the security considerations in[RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.) and [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.).

---

6. IANA Considerations

TOC

This memo requests assignment of one mode bit position/value to the IANA registry for the TWAMP Mode field, and describes behavior when the new mode is used. This field is a recognized extension mechanism for TWAMP.

This memo also requests assignment of four command numbers in the TWAMP-Control Command Number registry, and describes the use of the new commands. The command number field is a recognized extension mechanism for TWAMP.

6.1. Registry Specification

TOC

IANA has created a TWAMP-Modes registry (as requested in [RFC5618] (Morton, A. and K. Hedayat, “Mixed Security Mode for the Two-Way Active Measurement Protocol (TWAMP),” August 2009.)). TWAMP-Modes are specified in TWAMP Server Greeting messages and Set-up Response messages, as described in section 3.1 of [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, “A Two-Way Active Measurement Protocol (TWAMP),” October 2008.), consistent with section 3.1 of [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, “A One-way Active Measurement Protocol (OWAMP),” September 2006.), 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.

IANA has also created a TWAMP-Control Command Number registry. TWAMP-Control commands are specified by the first octet in TWAMP-Control messages as specified in section 3.5 of [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, “A Two-Way Active Measurement Protocol (TWAMP),” October 2008.), and augmented by this memo. This registry may contain 256 possible values.

6.2. Registry Management

TOC

Because the TWAMP-Control Command Number registry can contain only 256 values and TWAMP-Modes can only contain thirty-two values, and because TWAMP is an IETF protocol, these registries must be updated only by "IETF Consensus" as specified in [RFC5226] (Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” May 2008.) (an RFC documenting registry use that is approved by the IESG). Management of these registries is described in section 8.2 of [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, “A Two-Way Active Measurement Protocol (TWAMP),” October 2008.) and [RFC5618] (Morton, A. and K. Hedayat, “Mixed Security Mode for the Two-Way Active Measurement Protocol (TWAMP),” August 2009.).

This memo proposes assignment of values 7, 8, 9 and 10 in the Command number Registry, and the next available bit position (indicated by "Z") and corresponding value (indicated by "zzz") in sections 3.1 and 3.7 above. Note that these values should be replaced by IANA or the RFC Editor when assigned.

6.3. Experimental Numbers

TOC

One experimental value has been assigned in the TWAMP-Control Command Number registry.
No additional experimental values are assigned in the TWAMP-Modes registry.

6.4. Registry Contents

TOC

TWAMP-Control Command Number Registry

Value	Description	Semantics Definition
0	Reserved	
1	Forbidden	
2	Start-Sessions	RFC4656, Section 3.7
3	Stop-Sessions	RFC4656, Section 3.8
4	Reserved	
5	Request-TW-Session	RFC5357, Section 3.5
6	Experimentation	RFC5357, Section 8.3
7	Start-N-Sessions	this memo, Section 3.2
8	Start-N-Ack	this memo, Section 3.3
9	Stop-N-Sessions	this memo, Section 3.4
10	Stop-N-Ack	this memo, Section 3.5

TWAMP-Modes Registry

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, Auth. CONTROL	RFC5618, Section 3.1
zzz	Individual Session Control	this memo, Section 3.1 bit position (Z)

The suggested values are:
Z=4 zzz=16

TOC

7. Acknowledgements

The authors thank everyone who provided comments on this feature.

---

8. References

TOC

8.1. Normative References

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC4656]	Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," RFC 4656, September 2006 (TXT).
[RFC5226]	Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," BCP 26, RFC 5226, May 2008 (TXT).
[RFC5357]	Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," RFC 5357, October 2008 (TXT).
[RFC5618]	Morton, A. and K. Hedayat, "Mixed Security Mode for the Two-Way Active Measurement Protocol (TWAMP)," RFC 5618, August 2009 (TXT).

8.2. Informative References

TOC

[I-D.ietf-ippm-twamp-reflect-octets]	Morton, A. and L. Ciavattone, "TWAMP Reflect Octets and Symmetrical Size Features," draft-ietf-ippm-twamp-reflect-octets-05 (work in progress), April 2010 (TXT).

Authors' Addresses

TOC

	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/
	Murtaza Chiba
	Cisco Systems
	170 W. Tasman Drive
	San Jose, 95134
	USA
Phone:	+1 800 553 NETS
Fax:	+1
Email:	mchiba@cisco.com
URI:	