Internet Engineering Task Force (IETF)
Request for Comments: 5938
Updates: 5357
Category: Standards Track
ISSN: 2070-1721

A. Morton
AT&T Labs
M. Chiba
Cisco Systems

August 2010

Individual Session Control Feature for the Two-Way Active Measurement Protocol (TWAMP)

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 that were previously requested and accepted to start and stop at the same time.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5938.

Table of Contents

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 of TWAMP implementations at present, and widespread usage is expected. There are even devices that are designed to test implementations for protocol compliance.

This memo describes an OPTIONAL feature for TWAMP. [RFC5357] 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 Modes field bit position assignment and the use of two new TWAMP command numbers (for the augmented Start and Stop commands). This feature also specifies the use of a new Stop-N-ACK Server response, to complete the symmetry of the session-stopping process in the same way as the Start-ACK (Start-N-ACK when used with this feature) response.

The Individual Session Control feature gives the Control-Client new flexibility to manage any number of test sessions once they are established. However, [RFC5357] test sessions are established in serial order and the total establishment time grows with the number of sessions and the round-trip time. Therefore, implementers of this feature may also wish to implement the "Reflect Octets" feature, described in [REFLECT]. This feature allows a Control-Client to distinguish between parallel Request-TW-Session commands because a participating Server can return octets (e.g., the Control-Client's local index) in its reply to the request. Thus, the Reflect Octets feature supports the efficient establishment of many simultaneous test sessions that the Individual Session Control feature can then manage (start/stop).

This memo is an update to the TWAMP core protocol specified in [RFC5357]. Measurement systems are not required to implement the feature 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].

1.1. 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].

2. Purpose and Scope

The purpose of this memo is to describe an additional OPTIONAL function and feature for TWAMP [RFC5357].

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

1. extension of the modes of operation through assignment of a new value in the Modes 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

The TWAMP-Control protocol is a derivative of the OWAMP-Control protocol, and provides two-way measurement capability. TWAMP [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 Individual Session Control

TWAMP-Control connection establishment follows the procedure defined in Section 3.1 of [RFC4656] 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	RFC 4656, Section 3.1
2	Authenticated	RFC 4656, Section 3.1
4	Encrypted	RFC 4656, Section 3.1
8	Unauth. TEST protocol, Encrypted CONTROL	RFC 5618, Section 3.1
16	Individual Session Control	RFC 5938, bit position 4

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 [RFC5618] 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 4) 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 (4, 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].

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

field bit 4 with other features and bit positions (such as the reflect octets feature).

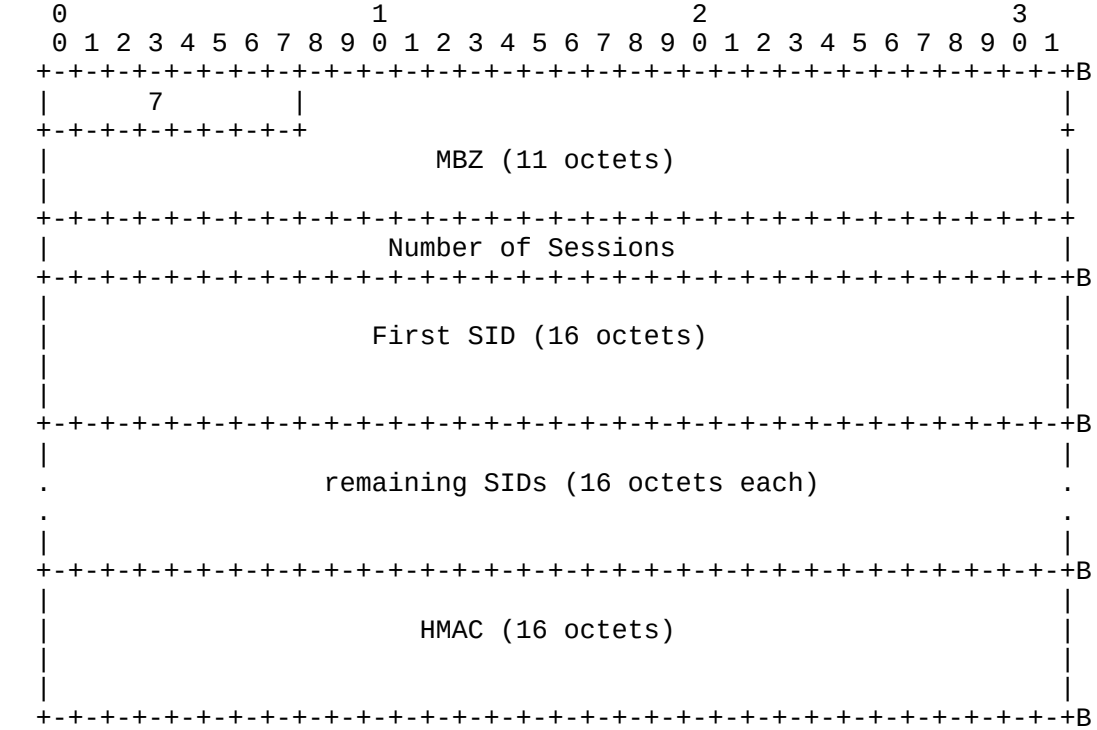
3.2. Start-N-Sessions Command with Individual Session Control

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:



Note: In figures, "B" indicates the boundary of a 16-octet word.

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 Section 3.5 of OWAMP [RFC4656] (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.

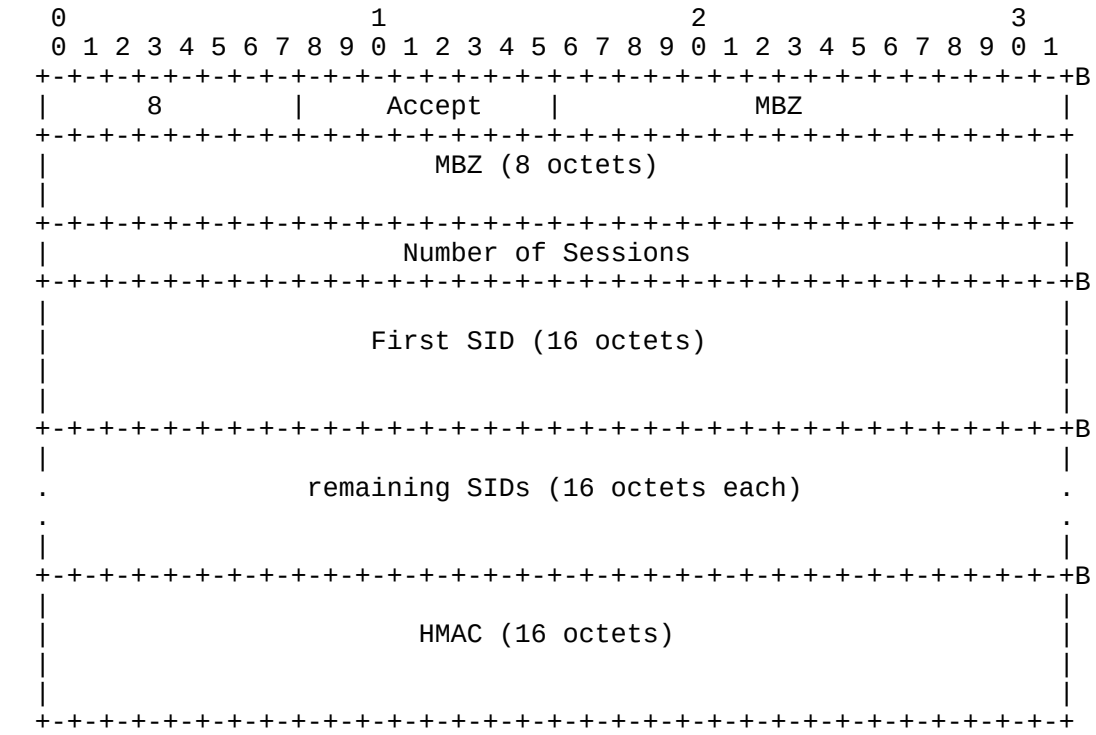
The Server MUST respond with one or more Start-N-Ack messages (which SHOULD be sent as quickly as possible). Start-N-Ack messages SHALL have the format defined in the next session.

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

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 of 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 Section 3.3 of OWAMP [RFC4656].

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 Section 3.5 of OWAMP [RFC4656] (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:

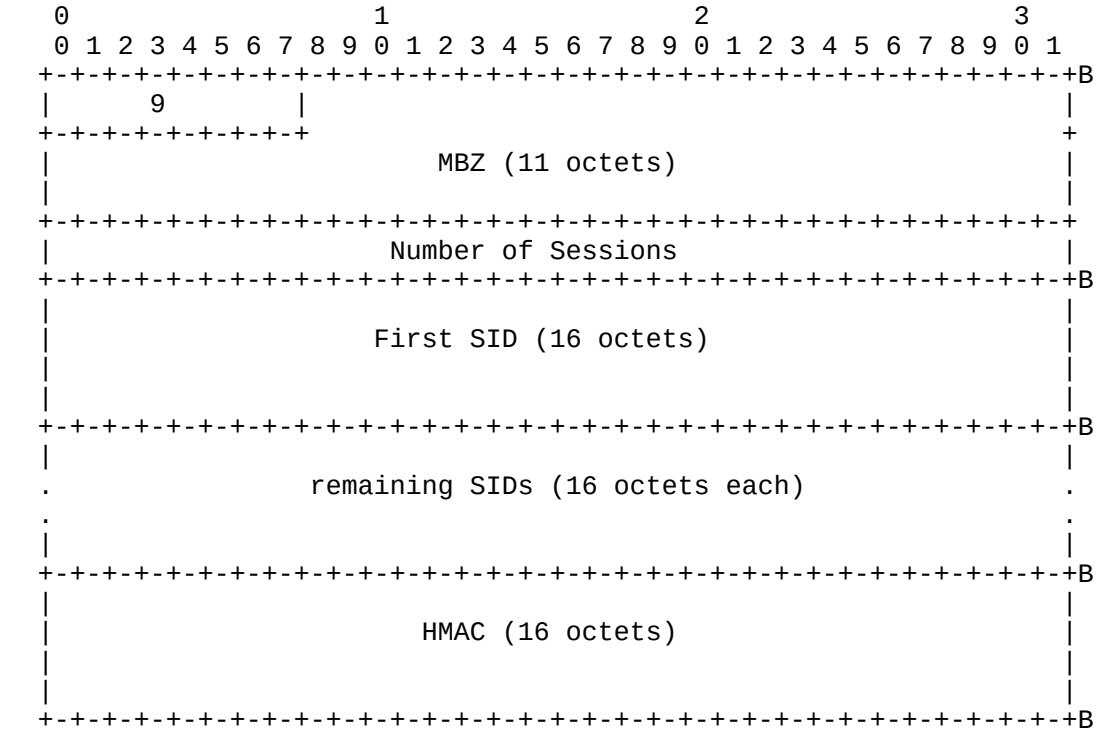
Accept = 0 Number of Sessions = 3 SIDs 1, 2, 4

Accept = 5 Number of Sessions = 1 SID 3

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

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 to which this Stop-N-Sessions command applies. The SID is as defined in Section 3.5 of OWAMP [RFC4656] (and TWAMP), 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.

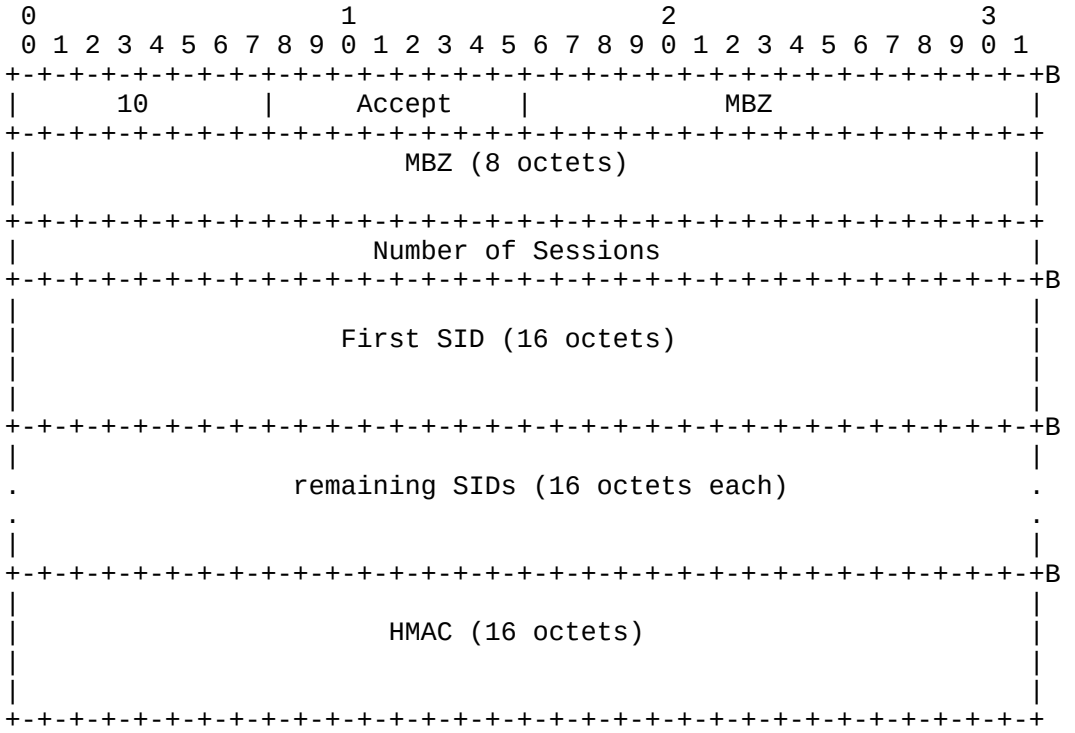
The message is terminated with a single block HMAC, as illustrated above.

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.

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 of 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 Section 3.3 of OWAMP [RFC4656].

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 Section 3.5 of OWAMP [RFC4656] (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.

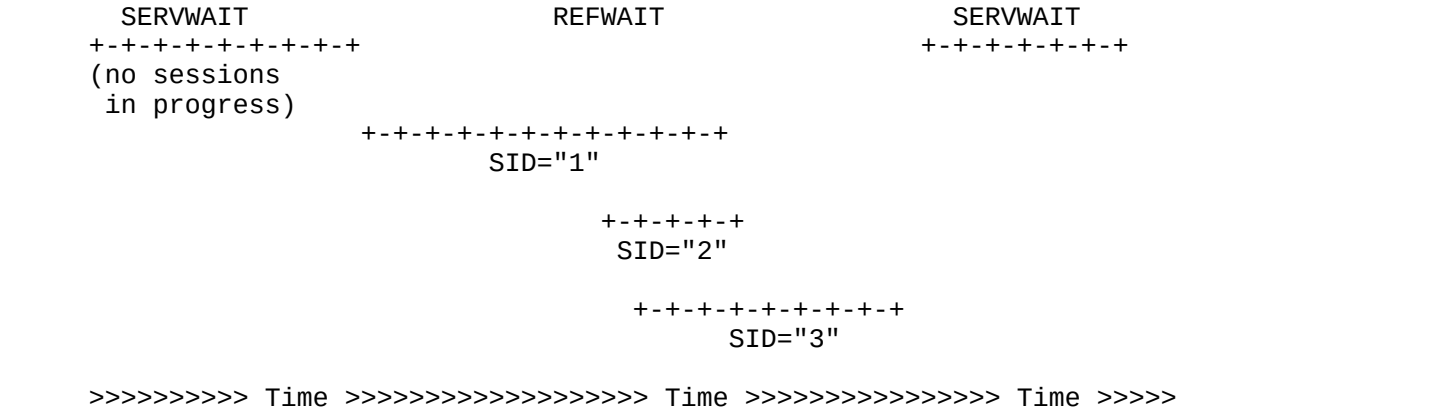
Note that the SIDs for all Sessions with the same 'Accept' code can be acknowledged using the same Stop-N-Ack message.

3.6. SERVWAIT Timeout Operation

Section 3.1 of [RFC5357] 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 that supports the SERVWAIT timeout option SHOULD also implement the REFWAIT timeout option.

The diagram below illustrates the operation of timers SERVWAIT and REFWAIT.



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 4 of the 32-bit Modes 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].

4. TWAMP Test with Individual Session Control

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 [RFC5357] 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 the OWAMP-Test protocol, there are three security modes: unauthenticated, authenticated, and encrypted. The unauthenticated mode has one test packet format, while the authenticated and encrypted modes use another (common) format.

4.1. Sender Behavior

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].

4.2. Reflector Behavior

The TWAMP Reflector follows the procedures and guidelines in Section 4.2 of [RFC5357], 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. (Note: The Request-TW-Session command includes sender address + port and receiver address + port, and this is usually sufficient to distinguish sessions.)

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

5. Security Considerations

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

6. IANA Considerations

As a result of this document, IANA has assigned one mode bit position/value for a mode in the IANA registry for the TWAMP Modes field, and this memo describes the behavior when the new mode is used. This field is a recognized extension mechanism for TWAMP.

As a result of this document, IANA has assigned four command numbers in the "TWAMP-Control Command Numbers" registry, and this memo describes the use of the new commands. The command number field is a recognized extension mechanism for TWAMP.

6.1. 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 "TWAMP-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).

IANA has also created the "TWAMP-Control Command Numbers" registry. TWAMP-Control commands are specified by the first octet in TWAMP-Control messages as specified in Section 3.5 of [RFC5357], and augmented by this memo. This registry may contain 256 possible values.

6.2. Registry Management

Because the "TWAMP-Control Command Numbers" registry can contain only 256 values and "TWAMP-Modes" are based on only 32 bit positions with a maximum of 2^32 values, and because TWAMP is an IETF protocol, these registries must be updated only by "IETF Consensus" as specified in [RFC5226] (an RFC that documents registry use and is approved by the IESG). Management of these registries is described in Section 8.2 of [RFC5357] and [RFC5618].

The values 7, 8, 9, and 10 have been assigned in the "TWAMP-Control Command Numbers" Registry. The value 16 corresponding to the next available bit position (4) (as described in Sections 3.1 and 3.7) has been assigned in the "TWAMP-Modes" registry.

6.3. Experimental Numbers

One experimental value has been assigned in the "TWAMP-Control Command Numbers" registry.

No additional experimental values are assigned in the TWAMP-Modes registry.

6.4. Registry Contents

TWAMP-Control Command Numbers Registry

Value	Description	Semantics Definition
0	Reserved	
1	Forbidden	
2	Start-Sessions	RFC 4656, Section 3.7
3	Stop-Sessions	RFC 4656, Section 3.8
4	Reserved	
5	Request-TW-Session	RFC 5357, Section 3.5
6	Experimentation	RFC 5357, Section 8.3
7	Start-N-Sessions	RFC 5938, Section 3.2
8	Start-N-Ack	RFC 5938, Section 3.3
9	Stop-N-Sessions	RFC 5938, Section 3.4
10	Stop-N-Ack	RFC 5938, Section 3.5

TWAMP-Modes Registry

Value	Description	Reference/Explanation
0	Reserved	
1	Unauthenticated	RFC 4656, Section 3.1
2	Authenticated	RFC 4656, Section 3.1
4	Encrypted	RFC 4656, Section 3.1
8	Unauth. TEST protocol, Encrypted CONTROL	RFC 5618, Section 3.1
16	Individual Session Control	RFC 5938, Section 3.1 bit position 4

7. Acknowledgements

The authors thank everyone who provided comments on this feature, especially Lars Eggert, Adrian Farrel, and Alexey Melnikov.

8. References

8.1. 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.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[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.

8.2. Informative References

[REFLECT] Morton, A. and L. Ciavattone, "TWAMP Reflect Octets and Symmetrical Size Features", Work in Progress, June 2010.

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/

Murtaza Chiba
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
USA

Phone: +1 800 553 NETS
EMail: mchiba@cisco.com