Network Working Group
Internet-Draft
Updates: 8762 (if approved)
Intended status: Standards Track
Expires: January 9, 2021

G. Mirsky
X. Min
ZTE Corp.
H. Nydell
Accedian Networks
R. Foote
Nokia
A. Masputra
Apple Inc.
E. Ruffini
OutSys

July 8, 2020

# Simple Two-way Active Measurement Protocol Optional Extensions
# draft-ietf-ippm-stamp-option-tlv-07

## Abstract

This document describes optional extensions to Simple Two-way Active Measurement Protocol (STAMP) that enable measurement of performance metrics, in addition to ones supported by the STAMP base specification. The document also defines a STAMP Test Session Identifier and thus updates RFC 8762.

## 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 https://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 9, 2021.

## Copyright Notice

Table of Contents



## 1. Introduction

Simple Two-way Active Measurement Protocol (STAMP) [RFC8762] supports the use of optional extensions that use Type-Length-Value (TLV) encoding. Such extensions enhance the STAMP base functions, such as measurement of one-way and round-trip delay, latency, packet loss, packet duplication, and out-of-order delivery of test packets. This specification defines optional STAMP extensions, their formats, and

the theory of operation. Also, a STAMP Test Session Identifier is defined as an update of the base STAMP specification [RFC8762].

## 2. Conventions Used in This Document

### 2.1. Acronyms

BDS BeiDou Navigation Satellite System

BITS Building Integrated Timing Supply

CoS Class of Service

DSCP Differentiated Services Code Point

ECN Explicit Congestion Notification

GLONASS Global Orbiting Navigation Satellite System

GPS Global Positioning System [GPS]

HMAC Hashed Message Authentication Code

LORAN-C Long Range Navigation System Version C

MBZ Must Be Zero

NTP Network Time Protocol [RFC5905]

PMF Performance Measurement Function

PTP Precision Time Protocol [IEEE.1588.2008]

TLV Type-Length-Value

SSID STAMP Session Identifier

SSU Synchronization Supply Unit

STAMP Simple Two-way Active Measurement Protocol

### 2.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 3. STAMP Test Session Identifier

The STAMP Session-Sender transmits test packets to the STAMP Session-Reflector. The STAMP Session-Reflector receives the Session-Sender's packet and acts according to the configuration and optional control information communicated in the Session-Sender's test packet. STAMP defines two different test packet formats, one for packets transmitted by the STAMP Session-Sender and one for packets transmitted by the STAMP Session-Reflector. STAMP supports two modes: unauthenticated and authenticated. Unauthenticated STAMP test packets are compatible on the wire with unauthenticated TWAMP-Test [RFC5357] packets.

By default, STAMP uses symmetrical packets, i.e., the size of the packet transmitted by the Session-Reflector equals the size of the packet received by the Session-Reflector.

A STAMP Session is identified by the 4-tuple (source and destination IP addresses, source and destination UDP port numbers). A STAMP Session-Sender MAY generate a locally unique STAMP Session Identifier (SSID). SSID is a two-octet-long non-zero unsigned integer. A Session-Sender MAY use SSID to identify a STAMP test session. If SSID is used, it MUST be present in each test packet of the given test session. In the unauthenticated mode, SSID is located as displayed in Figure 1.

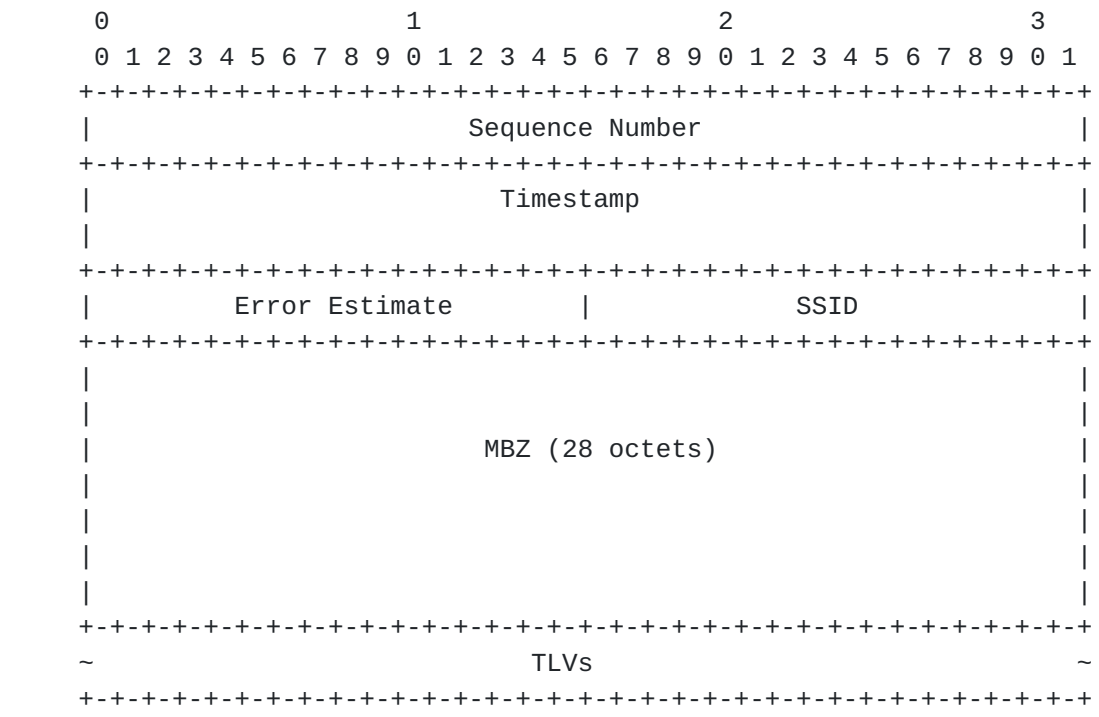



Figure 1: An example of an extended STAMP Session-Sender test packet format in unauthenticated mode

An implementation of the STAMP Session-Reflector that supports this specification SHOULD identify a STAMP Session using the SSID in combination with elements of the usual 4-tuple for the session. Before a test session commences, a Session-Reflector MUST be provisioned with all the elements that identify the STAMP Session. A STAMP Session-Reflector MUST discard non-matching STAMP test packet(s). The means of provisioning the STAMP Session identification is outside the scope of this specification. A conforming implementation of STAMP Session-Reflector MUST copy the SSID value from the received test packet and put it into the reflected packet, as displayed in Figure 2.

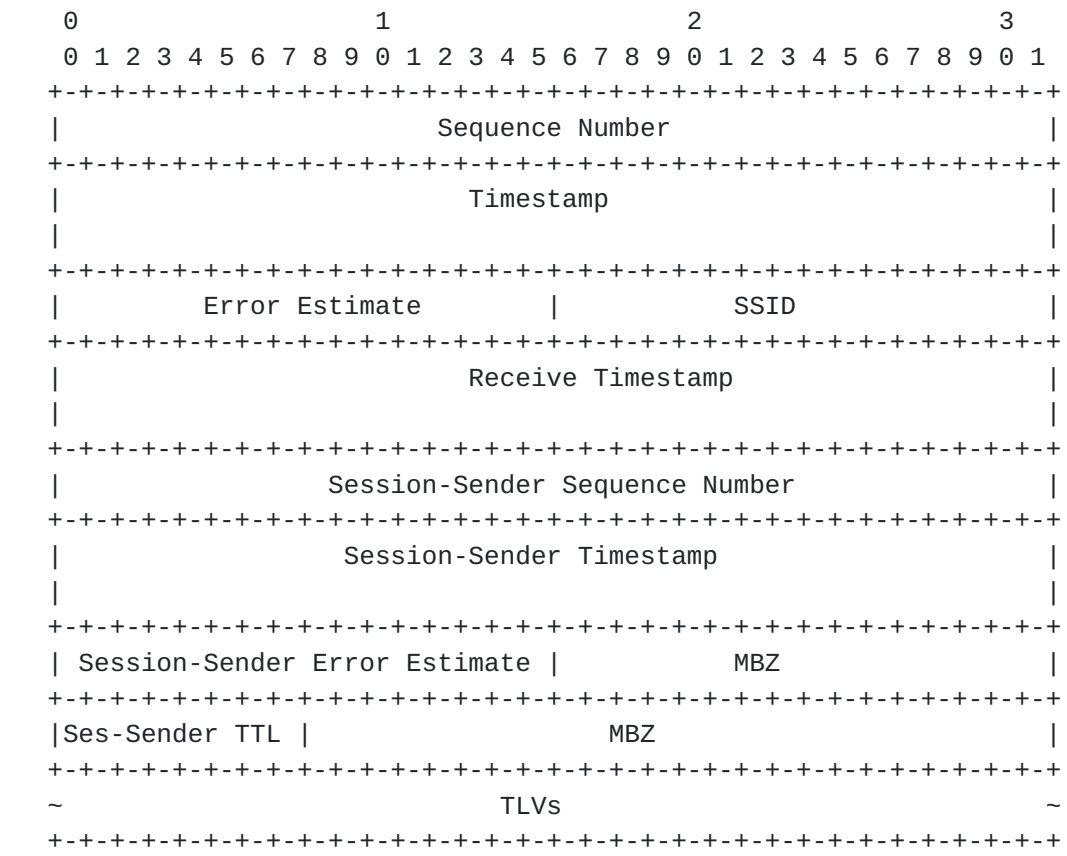



Figure 2: An example of an extended STAMP Session-Reflector test packet format in unauthenticated mode

A STAMP Session-Reflector that does not support this specification will return the zeroed SSID field in the reflected STAMP test packet. The Session-Sender MAY stop the session if it receives a zeroed SSID field. An implementation of a Session-Sender MUST support control of its behavior in such a scenario. If the test session is not stopped, the Session-Sender, can, for example, send a base STAMP packet [RFC8762].

Location of the SSID field in the authenticated mode is shown in Figure 3 and Figure 4.

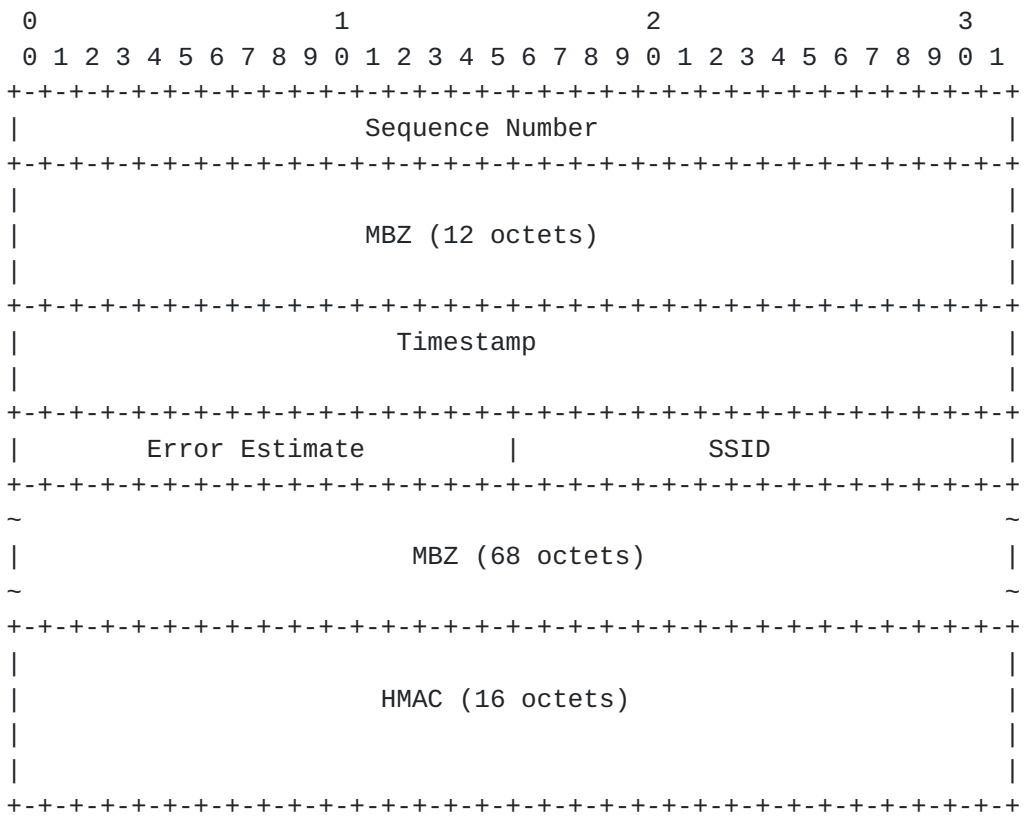
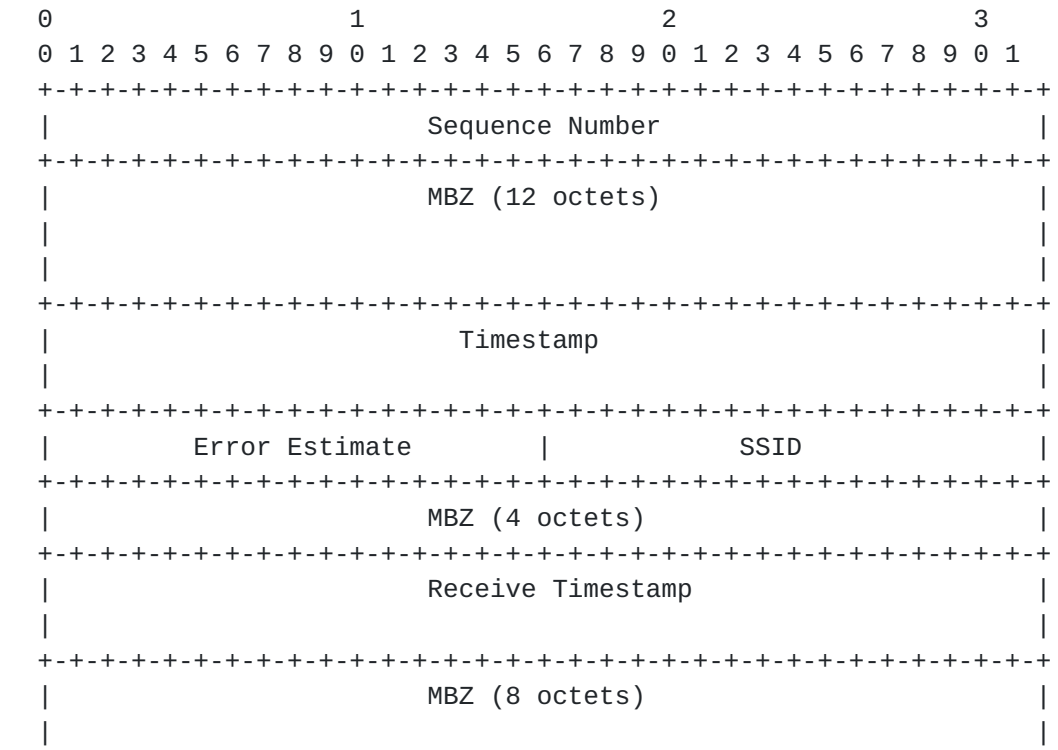



Figure 3: Base STAMP Session-Sender test packet format in authenticated mode



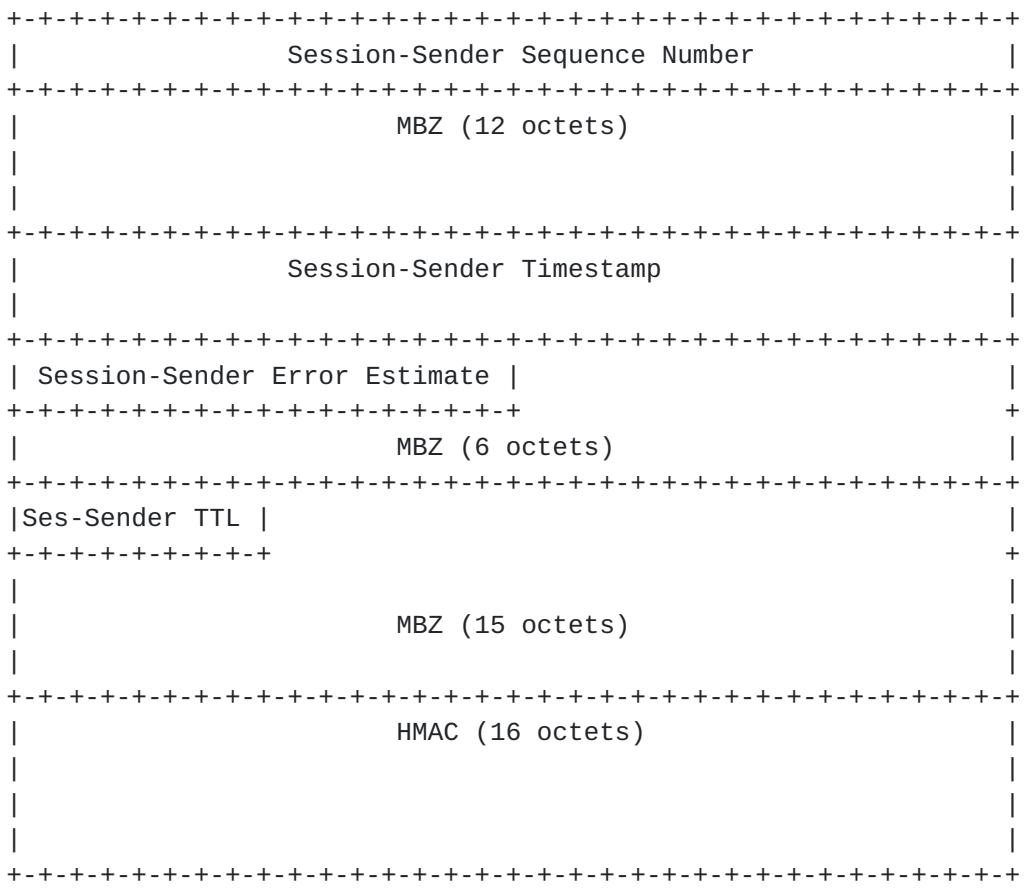



Figure 4: Base STAMP Session-Reflector test packet format in authenticated mode

## 4. TLV Extensions to STAMP

The Type-Length-Value (TLV) encoding scheme provides a flexible extension mechanism for optional informational elements. TLV is an optional field in the STAMP test packet. Multiple TLVs MAY be placed in a STAMP test packet. A TLV MAY be enclosed in a TLV. TLVs have a one-octet-long STAMP TLV Flags field, one-octet-long Type field, and two-octet-long Length field that is equal to the length of the Value field in octets. If a Type value for TLV or sub-TLV is in the range for Vendor Private Use, the Length MUST be at least 4, and the first four octets MUST be that vendor's the Structure of Management Information (SMI) Private Enterprise Code, as recorded in IANA's SMI Private Enterprise Codes sub-registry, in network octet order. The rest of the Value field is private to the vendor. The following sections describe the use of TLVs for STAMP that extend STAMP capability beyond its base specification.

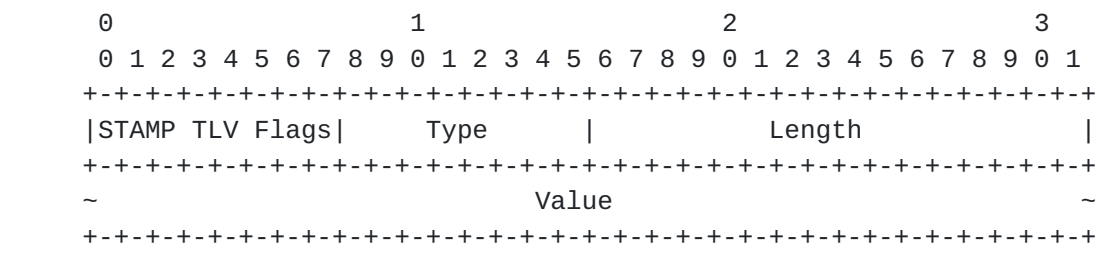



Figure 5: TLV Format in a STAMP Extended Packet

where fields are defined as the following:

- STAMP TLV Flags - eight-bit-long field. Detailed format and interpretation of flags defined in this specification is below.

- Type - one-octet-long field that characterizes the interpretation of the Value field. It is allocated by IANA, as specified in Section 5.1.

- Length - two-octet-long field equal to the length of the Value field in octets.

- Value - a variable-length field. Its interpretation and encoding is determined by the value of the Type field.

The format of the STAMP TLV Flags displayed in Figure 6 and the location of flags is according to Section 5.2.

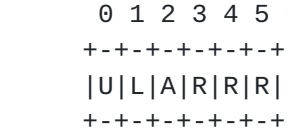



Figure 6: STAMP TLV Flags Format

where fields are defined as the following:

- U - a one-bit flag. A Session-Sender MUST set the U flag to 0 before transmitting an extended STAMP test packet. A Session-Reflector MUST set the U flag to 1 if the Session-Reflector has not understood the TLV.

- L - a one-bit flag. A Session-Sender MUST set the L flag to 0 before transmitting an extended STAMP test packet. A Session-Reflector MUST set the L flag to 1 if the Session-Reflector determined the TLV is malformed, i.e., the Length field value of the fixed-size TLV is not equal to the value defined for the

particular type, or the remaining length of the extended STAMP packet is less than the size of the TLV.

- A - a one-bit flag. A Session-Sender MUST set the A flag to 0 before transmitting an extended STAMP test packet. A Session-Reflector MUST set the A flag to 1 if the STAMP extensions have failed HMAC verification (Section 4.8).

- R - reserved flags for future use. These flags MUST be zeroed on transmit and ignored on receipt.

A STAMP node, whether Session-Sender or Session-Reflector, receiving a test packet MUST determine whether the packet is a base STAMP packet or includes one or more TLVs. The node MUST compare the value in the Length field of the UDP header and the length of the base STAMP test packet in the mode, unauthenticated or authenticated based on the configuration of the particular STAMP test session. If the difference between the two values is larger than the length of the UDP header, then the test packet includes one or more STAMP TLVs that immediately follow the base STAMP test packet. A Session-Reflector that does not support STAMP extensions is not expected to compare the value in the Length field of the UDP header and the length of the STAMP base packet. Hence the Session-Reflector will transmit the base STAMP packet. It is the local policy on the Session-Sender (similar to the handling of SSID == 0 scenario described in Section 3) that will control the sender's behavior.

A system that has received a STAMP test packet with extension TLVs MUST validate each TLV:

If the U flag is set, the STAMP system MUST skip the processing of the TLV. The implementation MUST try to process the next TLV if present in the extended STAMP packet.

If the L flag is set, the STAMP system MUST stop processing the remainder of the extended STAMP packet.

If the A flag is set, the STAMP system MUST discard all TLVs and MUST stop processing the remainder of the extended STAMP packet.

If an implementation of a Session-Reflector does not recognize the Type field value, it MUST include a copy of the TLV into the reflected STAMP packet. The Session-Reflector MUST set the U flag to 1. The Session-Reflector MUST try to process the next TLV in the extended STAMP packet.

If a TLV is malformed, the processing of extension TLVs MUST be stopped. The Session-Reflector MUST copy the remainder of the

received extended STAMP packet into the reflected STAMP packet. The Session-Reflector MUST set the L flag to 1.

Detected error events MUST be logged. Note that rate of logging MUST be controlled.

## 4.1. Extra Padding TLV

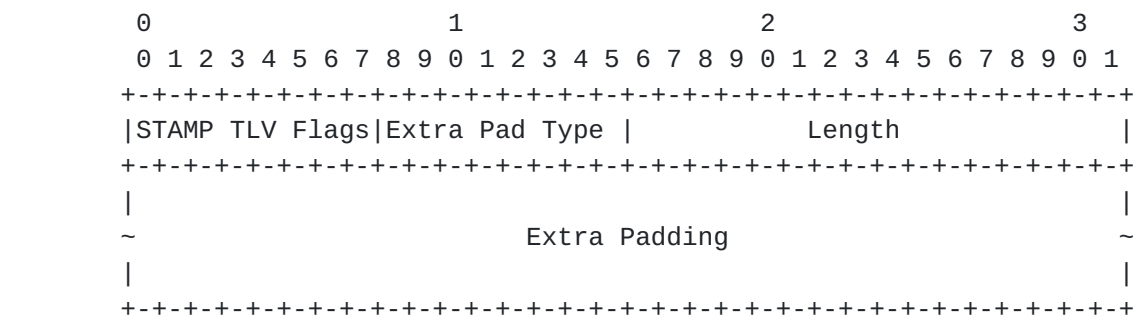



Figure 7: Extra Padding TLV

where fields are defined as the following:

- STAMP TLV Flags - is an eight-bit-long field. Its format is presented in Figure 6.

- Extra Padding Type - is a one-octet-long field, value TBA1 allocated by IANA Section 5.1.

- Length - two-octet-long field equal to the length of the Extra Padding field in octets.

- Extra Padding - a pseudo-random sequence of bits. The field MAY be filled with all zeros.

The Extra Padding TLV is similar to the Packet Padding field in a TWAMP-Test packet [RFC5357]. The use of the Extra Padding TLV is RECOMMENDED to perform a STAMP test using test packets of larger size than the base STAMP packet [RFC8762]. The length of the base STAMP packet is 44 octets in the unauthenticated mode or 112 octets in the authenticated mode. The Extra Padding TLV MAY be present more than one time in an extended STAMP test packet.

## 4.2. Location TLV

STAMP Session-Senders MAY include the Location TLV to request information from the Session-Reflector. The Session-Sender SHOULD NOT fill any information fields except for STAMP TLV Flags, Type, and Length. The Session-Reflector MUST validate the Length value against

the address family of the transport encapsulating the STAMP test packet. If the Length field's value is invalid, the Session-Reflector MUST zero all fields and MUST NOT return any information to the Session-Sender. The Session-Reflector MUST ignore all other fields of the received Location TLV.

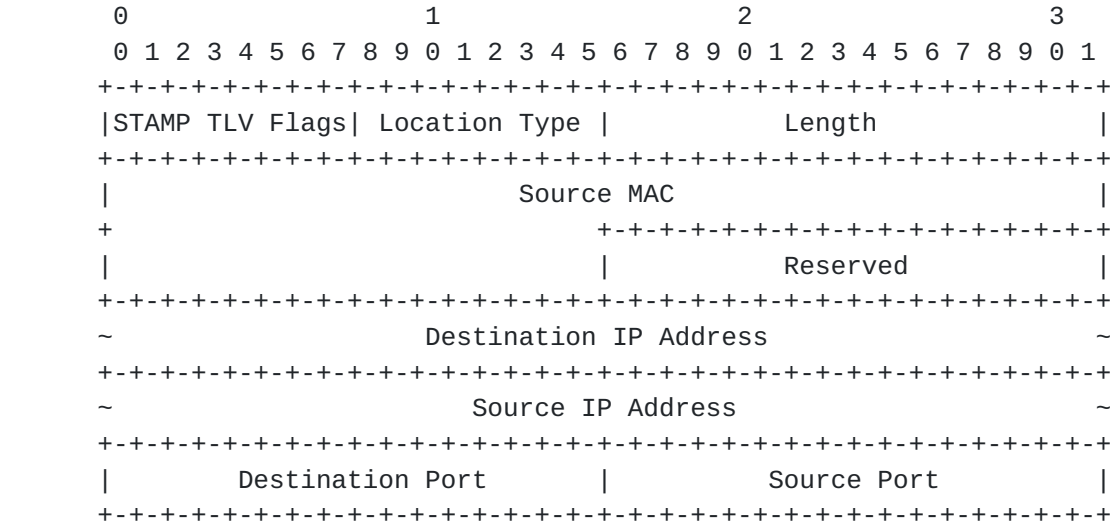



Figure 8: Session-Reflector Location TLV

where fields are defined as the following:

- STAMP TLV Flags - is an eight-bit-long field. Its format is presented in Figure 6.

- Location Type - is a one-octet-long field, value TBA2 allocated by IANA Section 5.1.

- Length - two-octet-long field equal to the length of the Value field in octets. The Length field value MUST equal 20 octets for the IPv4 address family. For the IPv6 address family, the value of the Length field MUST equal 44 octets. All other values are invalid.

- Source MAC - 6-octet-long field. The Session-Reflector MUST copy the Source MAC of the received STAMP packet into this field.

- Reserved - two-octet-long field. MUST be zeroed on transmission and ignored on reception.

- Destination IP Address - IPv4 or IPv6 destination address of the packet received by the STAMP Session-Reflector.

- Source IP Address - IPv4 or IPv6 source address of the packet received by the STAMP Session-Reflector.

- Destination Port - two-octet-long UDP destination port number of the received STAMP packet.

- Source Port - two-octet-long UDP source port number of the received STAMP packet.

The Location TLV MAY be used to determine the last-hop IP addresses, ports, and last-hop MAC address for STAMP packets. The MAC address can indicate a path switch on the last hop. The IP addresses and UDP ports will indicate if there is a NAT router on the path. It allows the Session-Sender to identify the IP address of the Session-Reflector behind the NAT, and detect changes in the NAT mapping that could cause sending the STAMP packets to the wrong Session-Reflector.

### 4.3. Timestamp Information TLV

The STAMP Session-Sender MAY include the Timestamp Information TLV to request information from the Session-Reflector. The Session-Sender SHOULD NOT fill any information fields except for STAMP TLV Flags, Type, and Length. The Session-Reflector MUST validate the Length value of the TLV. If the value of the Length field is invalid, the Session-Reflector MUST zero all fields and MUST NOT return any information to the Session-Sender.

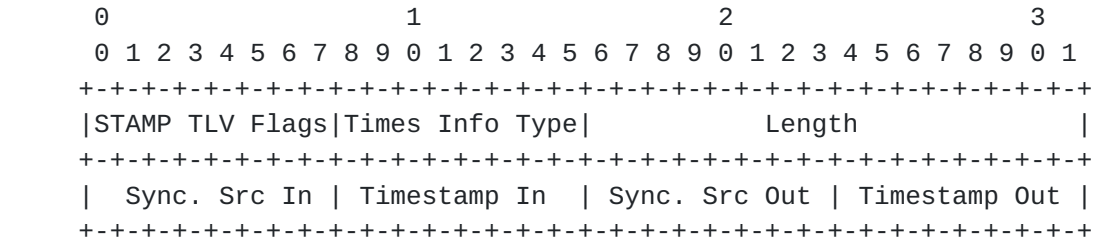



Figure 9: Timestamp Information TLV

where fields are defined as the following:

- STAMP TLV Flags - is an eight-bit-long field. Its format is presented in Figure 6.

- Timestamp Information Type - is a one-octet-long field, value TBA3 allocated by IANA Section 5.1.

- Length - two-octet-long field, set equal to the value 4.

- Sync Src In - one-octet-long field that characterizes the source of clock synchronization at the ingress of a Session-Reflector. There are several methods to synchronize the clock, e.g., Network Time Protocol (NTP) [RFC5905]. The value is one of those listed in Table 5.

- Timestamp In - one-octet-long field that characterizes the method by which the ingress of the Session-Reflector obtained the timestamp T2. A timestamp may be obtained with hardware assistance, via software API from a local wall clock, or from a remote clock (the latter is referred to as "control plane"). The value is one of those listed in Table 7.

- Sync Src Out - one-octet-long field that characterizes the source of clock synchronization at the egress of the Session-Reflector. The value is one of those listed in Table 5.

- Timestamp Out - one-octet-long field that characterizes the method by which the egress of the Session-Reflector obtained the timestamp T3. The value is one of those listed in Table 7.

### 4.4. Class of Service TLV

The STAMP Session-Sender MAY include a Class of Service (CoS) TLV in the STAMP test packet. The format of the CoS TLV is presented in Figure 10.

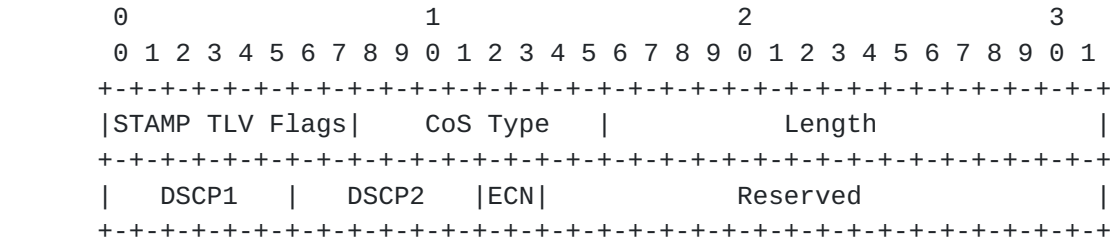



Figure 10: Class of Service TLV

where fields are defined as the following:

- STAMP TLV Flags - is an eight-bit-long field. Its format is presented in Figure 6.

- CoS (Class of Service) Type - is a one-octet-long field, value TBA4 allocated by IANA Section 5.1.

- Length - two-octet-long field, set equal to the value 4.

- DSCP1 - The Differentiated Services Code Point (DSCP) intended by the Session-Sender to be used as the DSCP value of the reflected test packet.

- DSCP2 - The received value in the DSCP field at the Session-Reflector in the forward direction.

- ECN - The received value in the ECN field at the Session-Reflector in the forward direction.

- Reserved - 18-bit-long field, MUST be zeroed on transmission and ignored on receipt.

A STAMP Session-Reflector that receives a test packet with the CoS TLV MUST include the CoS TLV in the reflected test packet. Also, the Session-Reflector MUST copy the value of the DSCP and ECN fields of the IP header of the received STAMP test packet into the DSCP2 field in the reflected test packet. Finally, the Session-Reflector MUST set the DSCP field's value in the IP header of the reflected test packet equal to the value of the DSCP1 field of the received test packet. Upon receiving the reflected packet, the Session-Sender will save the DSCP and ECN values for analysis of the CoS in the reverse direction.

Re-mapping of CoS can be used to provide multiple services (e,g., 2G, 3G, LTE in mobile backhaul networks) over the same network. But if it is misconfigured, then it is often difficult to diagnose the root cause of excessive packet drops of higher-level service while packet drops for lower service packets are at a normal level. Using a CoS TLV in STAMP testing helps to troubleshoot the existing problem and also verify whether DiffServ policies are processing CoS as required by the configuration.

### 4.5. Direct Measurement TLV

The Direct Measurement TLV enables collection of the number of in-profile packets that had been transmitted and received by the Session-Sender and Session-Reflector, respectively. The definition of "in-profile packet" is outside the scope of this document and is left to the test operators to determine.

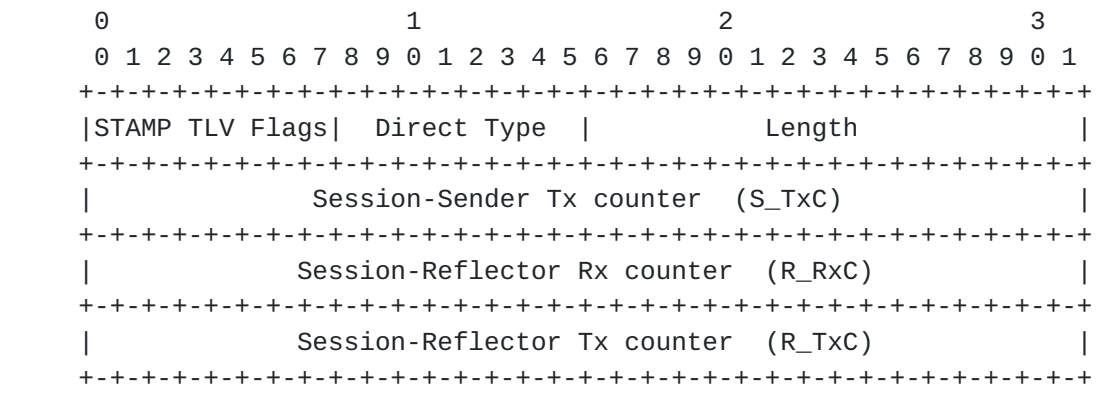



Figure 11: Direct Measurement TLV

where fields are defined as the following:

- STAMP TLV Flags - is an eight-bit-long field. Its format is presented in Figure 6.

- Direct (Measurement) Type - is a one-octet-long field, value TBA5 allocated by IANA Section 5.1.

- Length - two-octet-long field equals length of the Value field in octets. The Length field value MUST equal 12 octets.

- Session-Sender Tx counter (S_TxC) is a four-octet-long field. The Session-Sender MUST set its value equal to the number of the transmitted in-profile packets.

- Session-Reflector Rx counter (R_RxC) is a four-octet-long field. MUST be zeroed by the Session-Sender on transmit and ignored by the Session-Reflector on receipt. The Session-Reflector MUST fill it with the value of in-profile packets received.

- Session-Reflector Tx counter (R_TxC) is a four-octet-long field. MUST be zeroed by the Session-Sender and ignored by the Session-Reflector on receipt. The Session-Reflector MUST fill it with the value of the transmitted in-profile packets.

A Session-Sender MAY include the Direct Measurement TLV in a STAMP test packet. The Session-Sender MUST zero the R_RxC and R_TxC fields before the transmission of the STAMP test packet. If the received STAMP test packet includes the Direct Measurement TLV, the Session-Reflector MUST include it in the reflected test packet. The Session-Reflector MUST copy the value from the S_TxC field of the received test packet into the same field of the reflected packet before its transmission.

### 4.6. Access Report TLV

A STAMP Session-Sender MAY include an Access Report TLV (Figure 12) to indicate changes to the access network status to the Session-Reflector. The definition of an access network is outside the scope of this document.

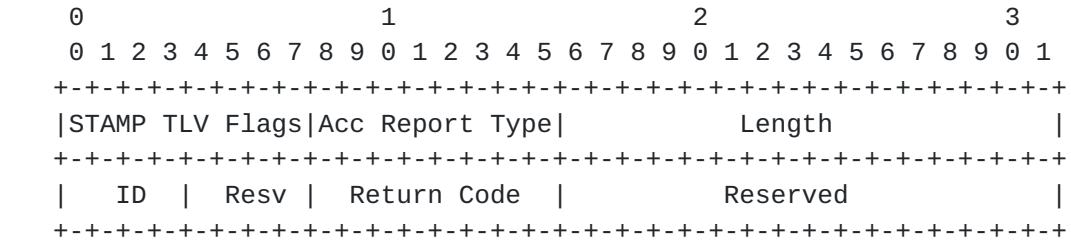



Figure 12: Access Report TLV

where fields are defined as follows:

- STAMP TLV Flags - is an eight-bit-long field. Its format presented in Figure 6.

- Access Report Type - is a one-octet-long field, value TBA6 allocated by IANA Section 5.1.

- Length - two-octet-long field, set equal to the value 4.

- ID (Access ID) - four-bit-long field that identifies the access network, e.g., 3GPP (Radio Access Technologies specified by 3GPP) or Non-3GPP (accesses that are not specified by 3GPP) [TS23501]. The value is one of those listed below:

  * 1 - 3GPP Network

  * 2 - Non-3GPP Network

  All other values are invalid and the TLV that contains it MUST be discarded.

- Resv - four-bit-long field, MUST be zeroed on transmission and ignored on receipt.

- Return Code - one-octet-long field that identifies the report signal, e.g., available or unavailable. The value is supplied to the STAMP end-point through some mechanism that is outside the scope of this document. The value is one of those listed in Section 5.5.

- Reserved - two-octet-long field, MUST be zeroed on transmission and ignored on receipt.

The STAMP Session-Sender that includes the Access Report TLV sets the value of the Access ID field according to the type of access network it reports on. Also, the Session-Sender sets the value of the Return Code field to reflect the operational state of the access network. The mechanism to determine the state of the access network is outside the scope of this specification. A STAMP Session-Reflector that received the test packet with the Access Report TLV MUST include the Access Report TLV in the reflected test packet. The Session-Reflector MUST set the value of the Access ID and Return Code fields equal to the values of the corresponding fields from the test packet it has received.

The Session-Sender MUST also arm a retransmission timer after sending a test packet that includes the Access Report TLV. This timer MUST be disarmed upon reception of the reflected STAMP test packet that includes the Access Report TLV. In the event the timer expires before such a packet is received, the Session-Sender MUST retransmit the STAMP test packet that contains the Access Report TLV. This retransmission SHOULD be repeated up to four times before the procedure is aborted. Setting the value for the retransmission timer is based on local policies and network environment. The default value of the retransmission timer for the Access Report TLV SHOULD be three seconds. An implementation MUST provide control of the retransmission timer value and the number of retransmissions.

The Access Report TLV is used by the Performance Measurement Function (PMF) components of the Access Steering, Switching and Splitting feature for 5G networks [TS23501]. The PMF component in the User Equipment acts as the STAMP Session-Sender, and the PMF component in the User Plane Function acts as the STAMP Session-Reflector.

## 4.7. Follow-up Telemetry TLV

A Session-Reflector might be able to put in the Timestamp field only an "SW Local" (see Table 7) timestamp. But the hosting system might provide a timestamp closer to the start of the actual packet transmission even though it is not possible to deliver the information to the Session-Sender in time for the packet itself. This timestamp might nevertheless be important for the Session-Sender, as it improves the accuracy of measuring network delay by minimizing the impact of egress queuing delays on the measurement.

A STAMP Session-Sender MAY include the Follow-up Telemetry TLV to request information from the Session-Reflector. The Session-Sender MUST set the Follow-up Telemetry Type and Length fields to their

appropriate values. The Sequence Number and Timestamp fields MUST be zeroed on transmission by the Session-Sender and ignored by the Session-Reflector upon receipt of the STAMP test packet that includes the Follow-up Telemetry TLV. The Session-Reflector MUST validate the Length value of the STAMP test packet. If the value of the Length field is invalid, the Session-Reflector MUST zero the Sequence Number and Timestamp fields and set the L flag in the STAMP TLV Flags field in the reflected packet. If the Session-Reflector is in stateless mode (defined in Section 4.2 [RFC8762]), it MUST zero the Sequence Number and Timestamp fields.

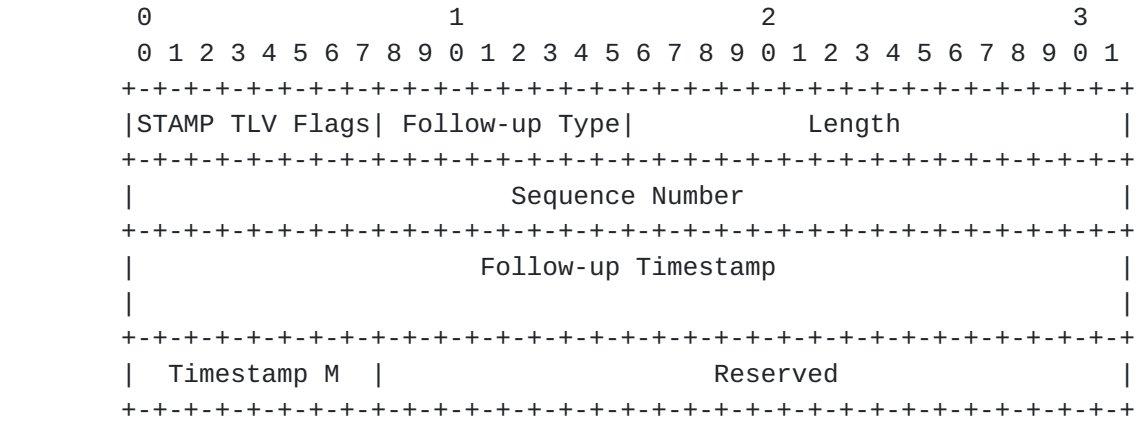



Figure 13: Follow-up Telemetry TLV

where fields are defined as follows:

- STAMP TLV Flags - is an eight-bit-long field. Its format presented in Figure 6.

- Follow-up (Telemetry) Type - is a one-octet-long field, value TBA7 allocated by IANA Section 5.1.

- Length - two-octet-long field, set equal to the value 16 octets.

- Sequence Number - four-octet-long field indicating the sequence number of the last packet reflected in the same STAMP-test session. Since the Session-Reflector runs in the stateful mode (defined in Section 4.2 [RFC8762]), it is the Session-Reflector's Sequence Number of the previous reflected packet.

- Follow-up Timestamp - eight-octet-long field, with the format indicated by the Z flag of the Error Estimate field of the packet transmitted by a Session-Reflector, as described in Section 4.1 [RFC8762]. It carries the timestamp when the reflected packet with the specified sequence number was sent.

- Timestamp M(ode) - one-octet-long field that characterizes the method by which the entity that transmits a reflected STAMP packet obtained the Follow-up Timestamp. The value is one of those listed in Table 7.

- Reserved - three-octet-long field. Its value MUST be zeroed on transmission and ignored on receipt.

## 4.8. HMAC TLV

The STAMP authenticated mode protects the integrity of data collected in the STAMP base packet. STAMP extensions are designed to provide valuable information about the condition of a network, and protecting the integrity of that data is also essential. The keyed Hashed Message Authentication Code (HMAC) TLV MUST be included in a STAMP test packet in the authenticated mode, excluding when the only TLV present is Extra Padding TLV. The HMAC TLV MUST follow all TLVs included in a STAMP test packet, except for the Extra Padding TLV. The HMAC TLV MAY be used to protect the integrity of STAMP extensions in STAMP unauthenticated mode.

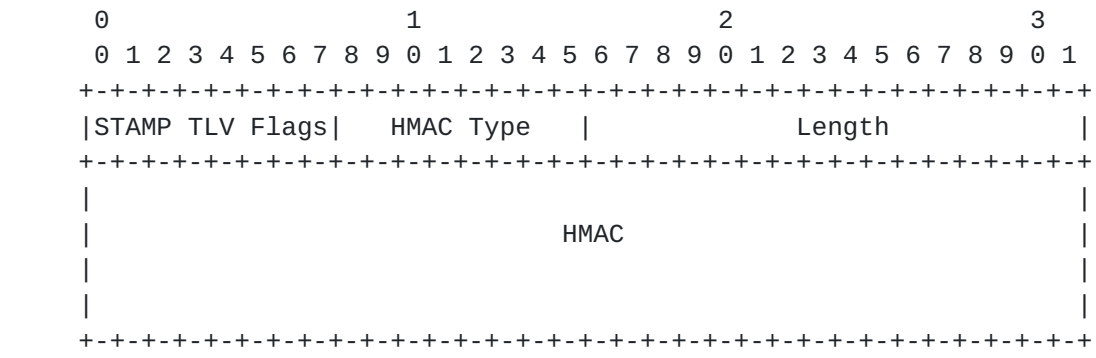



Figure 14: HMAC TLV

where fields are defined as follows:

- STAMP TLV Flags - is an eight-bit-long field. Its format is presented in Figure 6.

- HMAC Type - is a one-octet-long field, value TBA8 allocated by IANA Section 5.1.

- Length - two-octet-long field, set equal to 16 octets.

- HMAC - is a 16-octet-long field that carries HMAC digest of the text of all preceding TLVs.

As defined in [RFC8762], STAMP uses HMAC-SHA-256 truncated to 128 bits ([RFC4868]). All considerations regarding using the key and key distribution and management listed in Section 4.4 of [RFC8762] are fully applicable to the use of the HMAC TLV. HMAC is calculated as defined in [RFC2104] over text as the concatenation of all preceding TLVs. The digest then MUST be truncated to 128 bits and written into the HMAC field. In the authenticated mode, HMAC MUST be verified before using any data in the included STAMP TLVs. If HMAC verification by the Session-Reflector fails, then the Session-Reflector MUST stop processing the received extended STAMP test packet. The Session-Reflector MUST copy the remainder of the extended STAMP test packet into the reflected packet. The Session-Reflector MUST set the A flag in the copy of the HMAC TLV in the reflected packet to 1 before transmitting the reflected test packet. Also, both the Session-Sender and Session-Reflector SHOULD log the notification that HMAC verification of STAMP TLVs failed.

## 5. IANA Considerations

### 5.1. STAMP TLV Registry

IANA is requested to create the STAMP TLV Type registry. All code points in the range 1 through 175 in this registry shall be allocated according to the "IETF Review" procedure as specified in [RFC8126]. Code points in the range 176 through 239 in this registry shall be allocated according to the "First Come First Served" procedure as specified in [RFC8126]. The remaining code points are allocated according to Table 1:

| Value | Description | Reference |
|---|---|---|
| 0 | Reserved | This document |
| 1- 175 | Unassigned | IETF Review |
| 176 - 239 | Unassigned | First Come First Served |
| 240 - 251 | Experimental | This document |
| 252 - 254 | Private Use | This document |
| 255 | Reserved | This document |

Table 1: STAMP TLV Type Registry

This document defines the following new values in the STAMP Extension TLV range of the STAMP TLV Type registry:

| Value | Description | Reference |
|---|---|---|
| TBA1 | Extra Padding | This document |
| TBA2 | Location | This document |
| TBA3 | Timestamp Information | This document |
| TBA4 | Class of Service | This document |
| TBA5 | Direct Measurement | This document |
| TBA6 | Access Report | This document |
| TBA7 | Follow-up Telemetry | This document |
| TBA8 | HMAC | This document |

Table 2: STAMP Types

## 5.2. STAMP TLV Flags Sub-registry

IANA is requested to create the STAMP TLV Flags sub-registry as part of the STAMP TLV Type registry. The registration procedure is "IETF Review" [RFC8126]. Flags are 8 bits. This document defines the following bit positions in the STAMP TLV Flags sub-registry:

| Bit position | Symbol | Description | Reference |
|---|---|---|---|
| 0 | U | Unrecognized TLV | This document |
| 1 | L | Malformed TLV | This document |
| 2 | A | Authentication failed | This document |

Table 3: STAMP TLV Flags

## 5.3. Synchronization Source Sub-registry

IANA is requested to create the Synchronization Source sub-registry as part of the STAMP TLV Type registry. All code points in the range 1 through 127 in this registry shall be allocated according to the "IETF Review" procedure as specified in [RFC8126]. Code points in the range 128 through 239 in this registry shall be allocated according to the "First Come First Served" procedure as specified in [RFC8126]. Remaining code points are allocated according to Table 4:

| Value | Description | Reference |
|---|---|---|
| 0 | Reserved | This document |
| 1- 127 | Unassigned | IETF Review |
| 128 - 239 | Unassigned | First Come First Served |
| 240 - 249 | Experimental | This document |
| 250 - 254 | Private Use | This document |
| 255 | Reserved | This document |

Table 4: Synchronization Source Sub-registry

This document defines the following new values in the Synchronization Source sub-registry:

| Value | Description | Reference |
|---|---|---|
| 1 | NTP | This document |
| 2 | PTP | This document |
| 3 | SSU/BITS | This document |
| 4 | GPS/GLONASS/LORAN-C/BDS | This document |
| 5 | Local free-running | This document |

Table 5: Synchronization Sources

## 5.4. Timestamping Method Sub-registry

IANA is requested to create the Timestamping Method sub-registry as part of the STAMP TLV Type registry. All code points in the range 1 through 127 in this registry shall be allocated according to the "IETF Review" procedure as specified in [RFC8126]. Code points in the range 128 through 239 in this registry shall be allocated according to the "First Come First Served" procedure as specified in [RFC8126]. Remaining code points are allocated according to Table 6:

| Value | Description | Reference |
|---|---|---|
| 0 | Reserved | This document |
| 1- 127 | Unassigned | IETF Review |
| 128 - 239 | Unassigned | First Come First Served |
| 240 - 249 | Experimental | This document |
| 250 - 254 | Private Use | This document |
| 255 | Reserved | This document |

Table 6: Timestamping Method Sub-registry

This document defines the following new values in the Timestamping Methods sub-registry:

| Value | Description | Reference |
|---|---|---|
| 1 | HW Assist | This document |
| 2 | SW local | This document |
| 3 | Control plane | This document |

Table 7: Timestamping Methods

## 5.5. Return Code Sub-registry

IANA is requested to create the Return Code sub-registry as part of the STAMP TLV Type registry. All code points in the range 1 through 127 in this registry shall be allocated according to the "IETF Review" procedure as specified in [RFC8126]. Code points in the range 128 through 239 in this registry shall be allocated according to the "First Come First Served" procedure as specified in [RFC8126]. Remaining code points are allocated according to Table 8:

| Value | Description | Reference |
|---|---|---|
| 0 | Reserved | This document |
| 1- 127 | Unassigned | IETF Review |
| 128 - 239 | Unassigned | First Come First Served |
| 240 - 249 | Experimental | This document |
| 250 - 254 | Private Use | This document |
| 255 | Reserved | This document |

Table 8: Return Code Sub-registry

This document defines the following new values in the Return Code sub-registry:

| Value | Description | Reference |
|---|---|---|
| 1 | Network available | This document |
| 2 | Network unavailable | This document |

Table 9: Return Codes

## 6. Security Considerations

This document defines extensions to STAMP [RFC8762] and inherits all the security considerations applicable to the base protocol. Additionally, the HMAC TLV is defined in this document to protect the integrity of optional STAMP extensions. The use of HMAC TLV is discussed in detail in Section 4.8.

## 7. Acknowledgments

Authors much appreciate the thorough review and thoughtful comments received from Tianran Zhou, Rakesh Gandhi, Yuezhong Song and Yali Wang. The authors express their gratitude to Al Morton for his comments and the most valuable suggestions. The authors greatly appreciate comments and thoughtful suggestions received from Martin Duke.

## 8. Contributors

The following people contributed text to this document:

Guo Jun
ZTE Corporation
68# Zijinghua Road
Nanjing, Jiangsu 210012
P.R.China

Phone: +86 18105183663
Email: guo.jun2@zte.com.cn

## 9. References

### 9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, DOI 10.17487/RFC5357, October 2008, <https://www.rfc-editor.org/info/rfc5357>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8762] Mirsky, G., Jun, G., Nydell, H., and R. Foote, "Simple Two-Way Active Measurement Protocol", RFC 8762, DOI 10.17487/RFC8762, March 2020, <https://www.rfc-editor.org/info/rfc8762>.

[TS23501] 3GPP (3rd Generation Partnership Project), "Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2 (Release 16)", 3GPP TS23501, 2019.

### 9.2. Informative References

[GPS] "Global Positioning System (GPS) Standard Positioning Service (SPS) Performance Standard", GPS SPS 5th Edition, April 2020.

[IEEE.1588.2008] "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE Standard 1588, March 2008.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <https://www.rfc-editor.org/info/rfc2104>.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, DOI 10.17487/RFC4868, May 2007, <https://www.rfc-editor.org/info/rfc4868>.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <https://www.rfc-editor.org/info/rfc5905>.

## Authors' Addresses

Greg Mirsky
ZTE Corp.

Email: gregimirsky@gmail.com

Xiao Min
ZTE Corp.

Email: xiao.min2@zte.com.cn

Henrik Nydell
Accedian Networks

Email: hnydell@accedian.com

Richard Foote
Nokia

Email: footer.foote@nokia.com

Adi Masputra
Apple Inc.
One Apple Park Way
Cupertino, CA 95014
USA

Email: adi@apple.com

Ernesto Ruffini
OutSys
via Caracciolo, 65
Milano 20155
Italy

Email: eruffini@outsys.org