

Internet Engineering Task Force (IETF)  
Request for Comments: 8972  
Updates: 8762  
Category: Standards Track  
ISSN: 2070-1721

G. Mirsky  
X. Min  
ZTE Corp.  
H. Nydell  
Accedian Networks  
R. Foote  
Nokia  
A. Masputra  
Apple Inc.  
E. Ruffini  
OutSys  
January 2021

## Simple Two-Way Active Measurement Protocol Optional Extensions

Необязательные расширения протокола STAMP

### Аннотация

Этот документ описывает необязательные расширения для протокола STAMP), позволяющего измерять параметры производительности. Документ также определяет идентификатор тестовой сессии (STAMP Test Session Identifier) обновляя тем самым RFC 8762.

### Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF<sup>1</sup> и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG<sup>2</sup>. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке <https://www.rfc-editor.org/info/rfc8972>.

### Авторские права

Copyright (c) 2021. Авторские права принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

## Оглавление

1. Введение.....	2
2. Используемые соглашения.....	2
2.1. Сокращения.....	2
2.2. Уровни требований.....	2
3. Идентификатор сессии STAMP.....	2
4. TLV-расширения для STAMP.....	4
4.1. TLV дополнительного заполнения.....	5
4.2. TLV местоположения.....	5
4.2.1. Суб-TLV местоположения.....	6
4.2.2. Теория работы Location TLV.....	7
4.3. TLV характеристик временных меток.....	7
4.4. TLV класса обслуживания.....	8
4.5. TLV прямого измерения.....	8
4.6. TLV отчета о сети доступа.....	9
4.7. Follow-Up Telemetry TLV.....	9
4.8. HMAC TLV.....	10
5. Взаимодействие с IANA.....	11
5.1. Субреестр STAMP TLV Types.....	11
5.2. Субреестр STAMP TLV Flags.....	11
5.3. Субреестр STAMP Sub-TLV Types.....	11
5.4. Субреестр STAMP Synchronization Sources.....	11
5.5. Субреестр STAMP Timestamping Methods.....	12
5.6. Субреестр STAMP Return Codes.....	12
6. Вопросы безопасности.....	12

<sup>1</sup>Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

<sup>2</sup>Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

7. Литература.....	13
7.1. Нормативные документы.....	13
7.2. Дополнительная литература.....	13
Благодарности.....	13
Участники работы.....	13
Адреса авторов.....	13

## 1. Введение

Простой протокол активных двухсторонних измерений (Simple Two-way Active Measurement Protocol или STAMP) [RFC8762] задает базовую функциональность STAMP. В этом документе описаны необязательные расширения, использующие кодирование TLV. Такие расширения дополняют базовые функции STAMP, такие как измерение односторонней или круговой задержки, задержки при обработке, потери пакетов, их дублирование и нарушение порядка доставки. Спецификация определяет необязательные расширения STAMP, их формат и теорию работы. Определен также идентификатор тестовых сессий (STAMP Test Session Identifier) в качестве обновления [RFC8762].

## 2. Используемые соглашения

### 2.1. Сокращения

<b>BDS</b>	BeiDou Navigation Satellite System (навигационная система BeiDou).
<b>BITS</b>	Building Integrated Timing Supply (устройство синхронизации здания).
<b>CoS</b>	Class of Service (класс обслуживания).
<b>DSCP</b>	Differentiated Services Code Point (код дифференцированного обслуживания).
<b>ECN</b>	Explicit Congestion Notification (явное уведомление о перегрузке).
<b>GLONASS</b>	Global Orbiting Navigation Satellite System (глобальная орбитальная спутниковая система навигации).
<b>GPS</b>	Global Positioning System (глобальная система позиционирования) [GPS].
<b>HMAC</b>	Hashed Message Authentication Code (хэшированный код аутентификации сообщения).
<b>LORAN-C</b>	Long Range Navigation System Version C (система навигации дальнего действия, версия C).
<b>MBZ</b>	Must be Zero (должно быть 0).
<b>NTP</b>	Network Time Protocol (протокол сетевого времени) [RFC5905].
<b>PMF</b>	Performance Measurement Function (функция измерения производительности).
<b>PTP</b>	Precision Time Protocol (протокол точного времени) [IEEE.1588.2008].
<b>RP</b>	Reverse Path (обратный путь).
<b>SMI</b>	Structure of Management Information (структура информации управления).
<b>SSID</b>	STAMP Session Identifier (идентификатор сессии STAMP).
<b>SSU</b>	Synchronization Supply Unit (блок синхронизации).
<b>STAMP</b>	Simple Two-way Active Measurement Protocol (простой протокол активного двухстороннего измерения).
<b>TLV</b>	Type-Length-Value (тип, размер, значение).

### 2.2. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

## 3. Идентификатор сессии STAMP

STAMP Session-Sender передает тестовые пакеты рефлектору STAMP Session-Reflector. Рефлектор принимает пакеты от Session-Sender и действует в соответствии со своей конфигурацией и необязательными управляющими сигналами в тестовых пакетах от Session-Sender. Протокол STAMP определяет два формата пакетов - один для STAMP Session-Sender, другой для STAMP Session-Reflector и может работать в режиме с аутентификацией или без нее. Тестовые пакеты STAMP без аутентификации совместимы в линии с пакетами TWAMP-Test без аутентификации [RFC5357].

По умолчанию STAMP использует симметричные пакеты, т. е. размер пакетов, переданных Session-Reflector, совпадает с размером пакетов, полученных рефлектором.

Сессия STAMP идентифицируется четвертом (4-tuple) из IP-адресов отправителя и получателя, а также портов UDP на той и другой стороне). STAMP Session-Sender **может** создавать уникальный для него идентификатор сессии SSID,

представляющий собой 2-октетное положительное целое число. Правила генерации SSID определяются реализацией. В [NUM-IDS-GEN] тщательно проанализированы базовые алгоритмы для генерации идентификаторов и их уязвимости. Например, реализация может использовать алгоритмы, описанные в параграфе 7.1 [NUM-IDS-GEN]. Реализации **недопустимо** назначать один идентификатор разным тестовым сессиям STAMP. Session-Sender **может** применять SSID для идентификации тестовых сессий STAMP. При использовании SSID идентификатор **должен** включаться в каждый тестовый пакет данной сессии. Расположение SSID в режиме без аутентификации показано на рисунке 1.

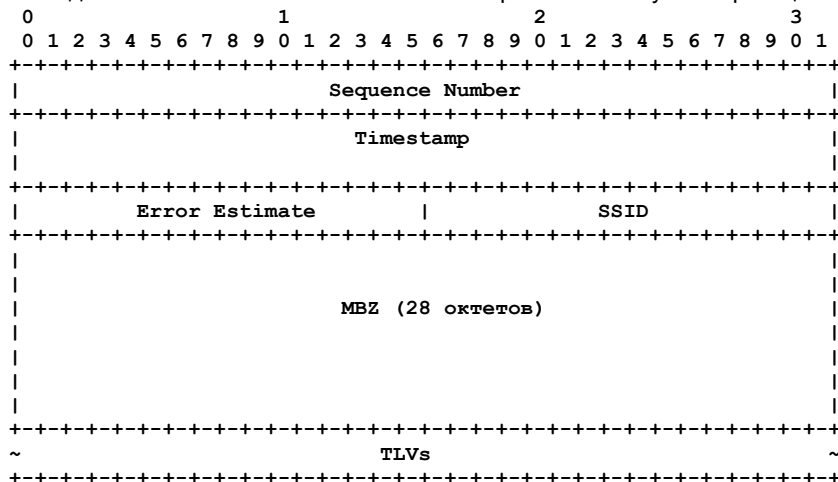


Рисунок 1. Формат расширенного пакета без аутентификации.

Реализация STAMP Session-Reflector, поддерживающая эту спецификацию, **должна** идентифицировать сессию STAMP по SSID в комбинации с обычным квартетом для сессии. Перед началом тестовой сессии рефлектору **должны** быть предоставлены все элементы, идентифицирующие сессию. STAMP Session-Reflector **должен** отбрасывать не соответствующие сессии пакеты STAMP. Способ предоставления идентификационных данных сессии выходит за рамки документа. Соответствующая спецификации реализации STAMP Session-Reflector **должна** копировать значение SSID из полученных тестовых пакетов в отражаемые пакеты, как показано на рисунке 2.

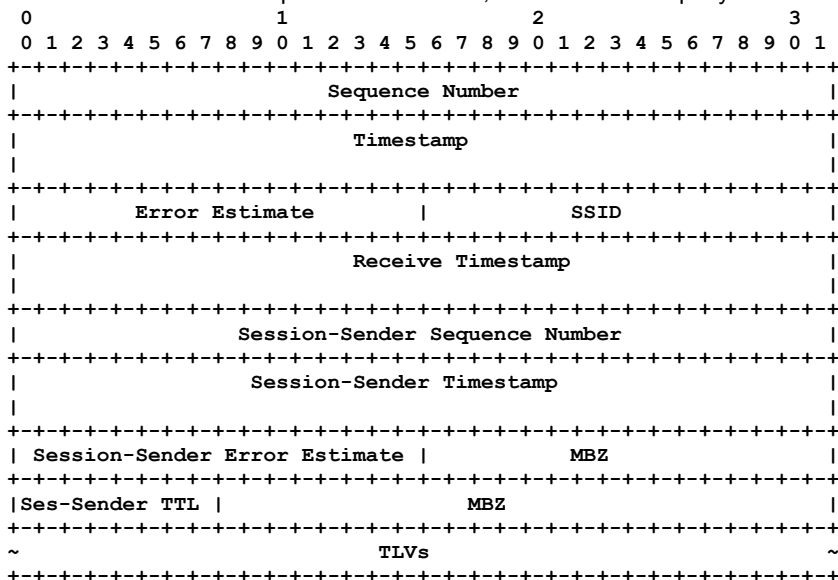


Рисунок 2. Формат отраженного расширенного пакета без аутентификации.

Не поддерживающий эту спецификацию STAMP Session-Reflector будет возвращать нулевое значение поля SSID в отраженных пакетах STAMP и Session-Sender **может** прервать сессию при получении такого поля SSID. Реализация Session-Sender **должна** поддерживать управление поведением в таких случаях. Если тестовая сессия не прерывается, Session-Sender может передавать базовые пакеты STAMP [RFC8762] или продолжить передачу пакетов с SSID.

Размещение поля SSID в режиме с аутентификацией показано на рисунках 3 и 4.

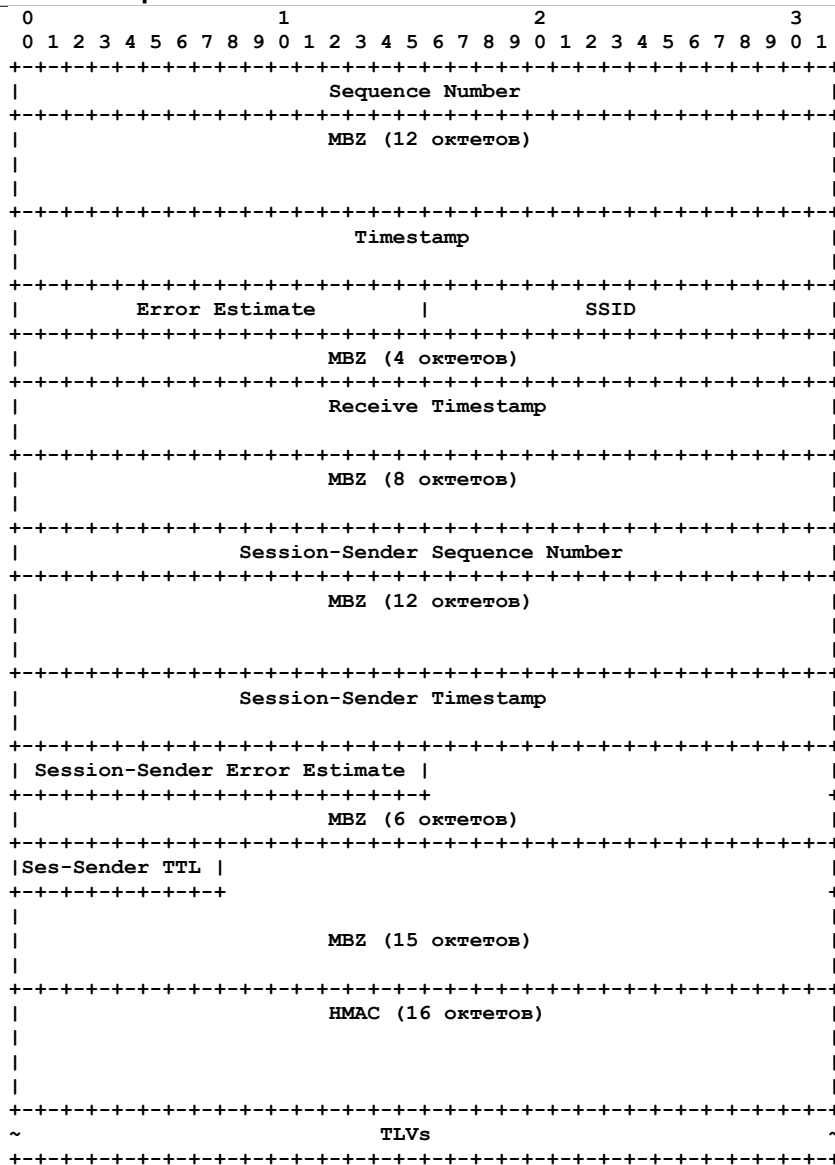


Рисунок 4. Формат отраженного расширенного пакета с аутентификацией.

#### 4. TLV-расширения для STAMP

Кодирование TLV обеспечивает гибкий механизм расширения для необязательных информационных элементов за счет включения необязательного поля TLV в тестовый пакет STAMP. Это поле TLV **может** содержать другие TLV в зависимости от семантики (внешнего) TLV. TLV имеют однооктетное поле STAMP TLV Flags, однооктетное поле Type и двухоктетное поле Length, указывающее размер поля Value в октетах. Если поле Type для TLV или суб-TLV имеет значение из диапазона Private Use [RFC8126], размер **должен** быть не меньше 4 и первые четыре октета **должны** содержать фирменный код SMI (Private Enterprise Code), как указано в субреестре IANA SMI Network Management Private Enterprise Codes, с сетевым порядком байтов. Остальная часть поля Value определяется производителем. В последующих параграфах описано применение TLV для STAMP, расширяющее базовую спецификацию STAMP.

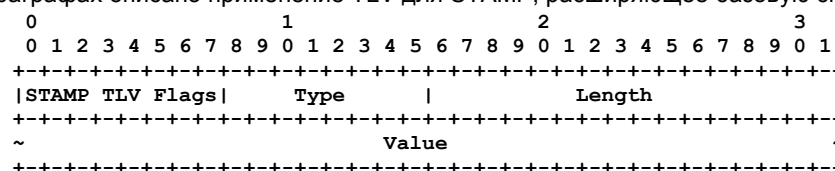


Рисунок 5. Формат TLV в расширенном пакете STAMP.

##### STAMP TLV Flags

8-битовое поле. Формат и интерпретация описаны ниже.

##### Type

1-октетное поле, определяющее интерпретацию поля Value. Значения выделяются IANA (параграф 5.1).

##### Length

2-октетное поле, указывающее размер поля Value в октетах.

##### Value

Поле переменного размера, кодирование и интерпретация которого определяются значением поля Type.

Для всех многобайтовых полей в TLV, определенных этой спецификацией, используется сетевой порядок байтов.

Формат поля STAMP TLV Flags показан на рисунке 6, а флаги местоположения определены в параграфе 5.2.

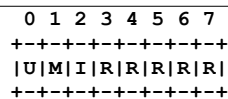


Рисунок 6. Формат поля флагов.

**U (Unrecognized)**

Session-Sender **должен** устанавливать U = 1 перед отправкой расширенного пакета STAMP, а Session-Reflector **должен** устанавливать U = 1, если он не понимает данный TLV. Для известных TLV рефлексор **должен** указывать в отраженных пакетах U = 0.

**M (Malformed)**

Session-Sender **должен** устанавливать M = 1 перед отправкой расширенного пакета STAMP, а Session-Reflector **должен** устанавливать M = 1, если считает формат TLV некорректным (поле Length не соответствует типу или оставшаяся часть пакета STAMP меньше размера данного TLV). В остальных случаях рефлексор **должен** указывать в отраженных пакетах M = 0.

**I (Integrity)**

Session-Sender **должен** устанавливать I = 0 перед отправкой расширенного пакета STAMP, а Session-Reflector **должен** устанавливать I = 1, если расширения STAMP не прошли проверку HMAC (параграф 4.8). В остальных случаях рефлексор **должен** указывать в отраженных пакетах I = 0.

**R**

Зарезервированные на будущее флаги, которые **должны** содержать 0 при передаче и игнорироваться при получении.

Узел STAMP (Session-Sender или Session-Reflector), получивший тестовый пакет, должен проверить, является пакет базовым или содержит TLV. Узел **должен** сравнить значение поля Length в заголовке UDP и размер базового пакета STAMP в режиме (с аутентификацией или без нее), заданном конфигурацией сессии STAMP. Если разница превышает размер заголовка UDP, тестовый пакет включает STAMP TLV, следующие сразу за базовым пакетом STAMP. Рефлексор, не поддерживающий принятые расширения, не будет обрабатывать их, а просто скопирует в отраженный пакет, как указано в параграфе 4.3 [RFC8762]. Поддерживающий TLV рефлексор укажет необработанные им TLV установкой для них флага U = 1.

STAMP Session-Sender, получающий отраженные пакеты STAMP с TLV, **должен** проверить все TLV как указано ниже.

- При установленном флаге U система STAMP **должна** пропустить обработку соответствующего TLV.
- При установленном флаге M система STAMP **должна** прекратить обработку оставшейся части пакета STAMP.
- При установленном флаге I система STAMP **должна** отбросить все TLV и **должна** прекратить обработку оставшейся части пакета STAMP.
- Если реализация Session-Reflector не распознает значение поля Type, она **должна** включить копию TLV в отраженный пакет STAMP и **должна** установить для нее U = 1. Рефлексор **должен** пропускать обработку неизвестных TLV.
- При нарушении формата TLV обработка TLV расширений **должна** прекращаться. Session-Reflector **должен** скопировать оставшуюся часть полученного пакета STAMP в отраженный пакет и **должен** установить M = 1.

**4.1. TLV дополнительного заполнения**

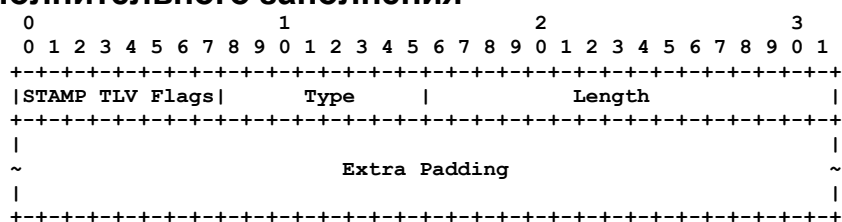


Рисунок 7. TLV дополнительного заполнения.

**STAMP TLV Flags**

8-битовое поле флагов, формат которого показан на рисунке 6.

**Type**

1-октетное поле, определяющее интерпретацию поля Value. Значения выделяются IANA (параграф 5.1).

**Length**

2-октетное поле, указывающее размер поля Value в октетах.

**Extra Padding**

Это поле **следует** заполнять псевдослучайными значениями, но **можно** заполнить нулями. Реализация **должна** контролировать поле Extra Padding.

Блок Extra Padding TLV похож на поле Packet Padding в пакетах TWAMP-Test [RFC5357]. Применение Extra Padding TLV **рекомендуется** для тестов STAMP, использующих пакеты, размер которых превышает базовый [RFC8762] размер, составляющий 44 октета в режиме без аутентификации и 112 - в режиме с аутентификацией. Extra Padding TLV **может** присутствовать в пакете STAMP в нескольких экземплярах.

**4.2. TLV местоположения**

STAMP Session-Sender **может** включать Location TLV переменного размера для запроса информации о местоположении рефлексора. Отправителю **недопустимо** заполнять в этом случае какие-либо поля, за исключением STAMP TLV Flags, Type и Length. Рефлексор **должен** проверять корректность формата TLV и следовать описанной в разделе 4 процедуре при обнаружении несоответствия.

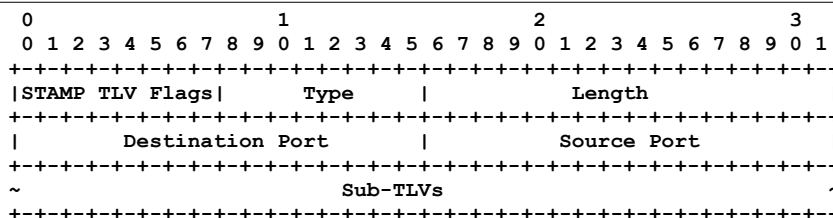


Рисунок 8. Location TLV.

**STAMP TLV Flags**

8-битовое поле флагов, формат которого показан на рисунке 6.

**Type**

1-октетное поле, определяющее интерпретацию поля Value. Значения выделяются IANA (параграф 5.1).

**Length**

2-октетное поле, указывающее размер поля Value в октетах.

**Destination Port**

2-октетное поле с номером целевого порта UDP в принятом пакете STAMP.

**Source Port**

2-октетное поле с номером порта отправителя UDP в принятом пакете STAMP.

**Sub-TLVs**

Последовательность суб-TLV, определенная ниже, которые Session-Sender использует для запроса информации о местоположении. Session-Reflector отвечает на них соответствующими суб-TLV для типа адреса (например, IPv4 или IPv6), используемого им.

Отметим, что все поля, не заполненные отправителем или рефлектором, передаются с заполнением нулями.

**4.2.1. Суб-TLV местоположения**

Location TLV использует формат, показанный на рисунке 5. Обработка флагов U и M для этого суб-TLV выполняется в соответствии с разделом 4. Для флага I отправитель и рефлектор **должны** устанавливать значение 0 до передачи, а на приемной стороне флаг игнорируется. Ниже приведены типы суб-TLV для Location TLV, определенные этой спецификацией (таблица 5).

**Source MAC Address**

12-октетный блок суб-TLV с Type = 1. Поле Length **должно** иметь значение 8, поле Value является 8-октетным MBZ, которое **должно** заполняться нулями при передаче и игнорироваться при получении.

**Source EUI-48 Address**

12-октетный блок суб-TLV MAC-адресом отправителя EUI-48 и Type = 2. Поле Length **должно** иметь значение 8.

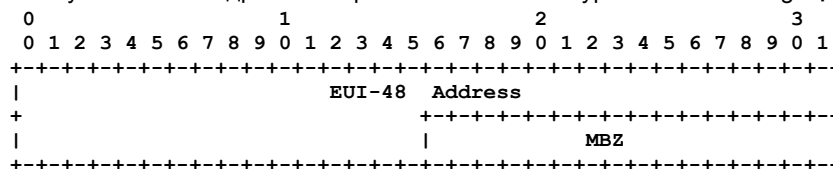


Рисунок 9. Поле Value в суб-TLV Source EUI-48 Address.

**EUI-48 Address**

6-октетное поле.

**MBZ**

2-октетное поле, которое **должно** заполняться нулями при передаче и игнорироваться при получении.

**Source EUI-64 Address**

12-октетный блок суб-TLV, содержащий MAC-адрес EUI-64 для отправителя и Type = 3. Поле Length **должно** иметь значение 8, а Value содержит 8-октетный адрес EUI-64.

**Destination IP Address**

20-октетный блок суб-TLV с Type = 4. Поле Length **должно** иметь значение 16, а 16-октетное поле MBZ **должно** заполняться нулями при передаче и игнорироваться при получении.

**Destination IPv4 Address**

20-октетный блок суб-TLV с адресом получателя IPv4 и Type = 5. Поле Length **должно** иметь значение 16.

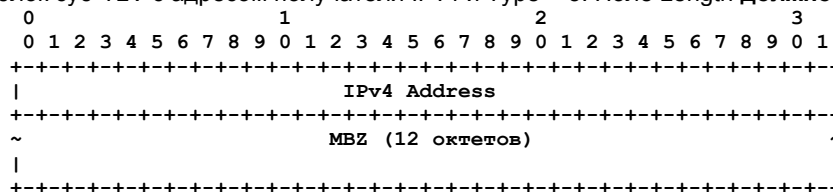


Рисунок 10. Поле Value в суб-TLV IPv4 Address.

**IPv4 Address**

4-октетное поле.

**MBZ**

12-октетное поле, которое **должно** заполняться нулями при передаче и игнорироваться при получении.

**Destination IPv6 Address**

20-октетный блок суб-TLV с адресом получателя IPv6 и Type = 6. Поле Length **должно** иметь значение 16, а Value содержит 16-октетный адрес IPv6.

**Source IP Address**

20-октетный блок суб-TLV с Type = 7. Поле Length **должно** иметь значение 16, а Value содержит 16-октетное поле MBZ, которое **должно** заполняться нулями при передаче и игнорироваться при получении.

**Source IPv4 Address**

20-октетный блок суб-TLV с адресом отправителя IPv4 и Type = 8. Поле Length **должно** иметь значение 16, а Value содержит показанные ниже поля (рисунок 10).

**IPv4 Address**

4-октетное поле.

**MBZ**

12-октетное поле, которое **должно** заполняться нулями при передаче и игнорироваться при получении.

**Source IPv6 Address**

20-октетный блок суб-TLV с адресом отправителя IPv6 и Type = 9. Поле Length **должно** иметь значение 16, а Value содержит 16-октетный адрес IPv6.

**4.2.2. Теория работы Location TLV**

Session-Reflector, принимающий расширенный пакет STAMP с Location TLV, **должен** включить в отраженный пакет Location TLV, размер которого совпадает с размером Location TLV в полученном пакете. В соответствии с локальной политикой Session-Reflector **может** не сообщать значения некоторых полей, заполнив их нулями. Реализация Session-Reflector с учетом состояния **должна** обеспечивать управление политикой заполнения полей.

Session-Sender **может** включить суб-TLV Source MAC Address в Location TLV. Рефлектор, получивший Location TLV с суб-TLV Source MAC Address, **должен** включить суб-TLV Source EUI-48 Address, если MAC-адрес отправителя тестового пакета имеет формат EUI-48. Session-Reflector **должен** копировать MAC-адрес отправителя в поле EUI-48. В противном случае Session-Reflector **должен** использовать суб-TLV Source EUI-64 Address и **должен** копировать значение Source MAC Address из полученного пакета в поле EUI-64. Если полученный пакет STAMP не имеет поля Source MAC Address, рефлектор **должен** заполнить поле EUI-64 нулями до передачи отраженного пакета.

Session-Sender **может** включить суб-TLV Destination IP Address в Location TLV. Рефлектор, получивший Location TLV с суб-TLV Destination IP Address, **должен** включить суб-TLV Destination IPv4 Address, если IP-адрес отправителя полученного пакета относится к семейству IPv4. Session-Reflector **должен** копировать значение IP-адреса получателя в поле IPv4 Address. В противном случае Session-Reflector **должен** использовать суб-TLV Destination IPv6 Address и **должен** копировать значение IP-адреса получателя в поле IPv6 Address.

Session-Sender **может** включить суб-TLV Source IP Address в Location TLV. Рефлектор, получивший Location TLV с суб-TLV Source IP Address, **должен** включить суб-TLV Source IPv4 Address, если IP-адрес отправителя в полученном пакете относится к семейству IPv4. Session-Reflector **должен** копировать значение IP-адреса отправителя в поле IPv4 Address. В противном случае Session-Reflector **должен** использовать суб-TLV Source IPv6 Address и **должен** копировать значение IP-адреса отправителя в поле IPv6 Address.

Location TLV **можно** применять для определения IP-адреса и порта и MAC-адреса последнего интервала (last-hop) для пакета STAMP. MAC-адрес может указывать переключение пути на последнем интервале, адрес IP и порт UDP покажут наличие на пути маршрутизаторов NAT. Это позволяет отправителю узнать IP-адрес рефлектора, расположенного за транслятором NAT и обнаружить изменения в отображении NAT, которые могут приводить к отправке пакетов STAMP не тому рефлектору.

**4.3. TLV характеристик временных меток**

STAMP Session-Sender **может** включать Timestamp Information TLV для запроса информации у рефлектора. Отправителю **недопустимо** указывать информационные поля, за исключением STAMP TLV Flags, Type и Length. Все остальные поля **должны** заполняться нулями. Session-Reflector **должен** проверять поле Length в TLV и при некорректном значении выполнять процедуру, описанную в разделе 4 для TLV с ошибкой формата.

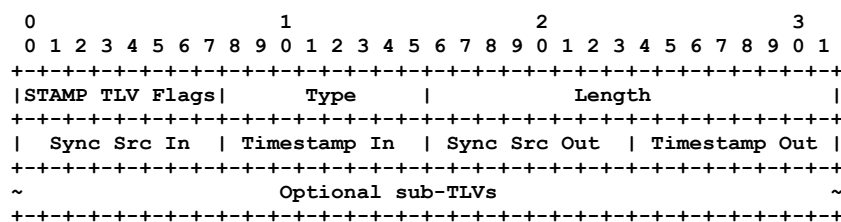


Рисунок 11. Timestamp Information TLV.

**STAMP TLV Flags**

8-битовое поле флагов, формат которого показан на рисунке 6.

**Type**

1-октетное поле, определяющее интерпретацию поля Value. Значения выделяются IANA (параграф 5.1).

**Length**

2-октетное поле, указывающее размер поля Value в октетах (рисунок 5).

**Sync Src In**

1-октетное поле, указывающее источник синхронизации часов на входе Session-Reflector. Имеется несколько методов синхронизации, например, протокол NTP (Network Time Protocol) [RFC5905] (таблица 7).

**Timestamp In**

1-октетное поле, указывающее метод, с помощью которого Session-Reflector получает временную метку T2. Это может быть аппаратный источник, подключенный через API к местным часам (wall clock) или удаленный источник (через плоскость управления). Возможные источники синхронизации указаны в таблице 9.

**Sync Src Out**

1-октетное поле, указывающее источник синхронизации часов на выходе Session-Reflector. Имеется несколько методов синхронизации выхода Session-Reflector (таблица 7).

**Timestamp Out**

1-октетное поле, указывающее метод, с помощью которого Session-Reflector получает временную метку T3 (таблица 9).

**Optional sub-TLVs**

Необязательное поле переменного размера.

## 4.4. TLV класса обслуживания

STAMP Session-Sender **может** включать CoS TLV в тестовые пакеты STAMP. Формат CoS TLV показан на рисунке 12.

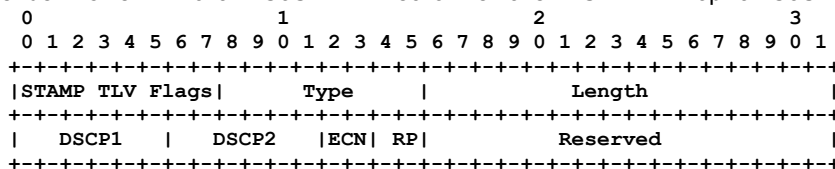


Рисунок 12. TLV класса обслуживания.

### STAMP TLV Flags

8-битовое поле флагов, формат которого показан на рисунке 6.

### Type

1-октетное поле, определяющее интерпретацию поля Value. Значения выделяются IANA (параграф 5.1).

### Length

2-октетное поле со значением 4.

### DSCP1

Код дифференцированного обслуживания (DSCP), назначенный отправителем для указания а поле DSCP отраженных пакетов.

### DSCP2

Значение поля DSCP во входных пакетах рефлектора.

### ECN

Значение поля ECN во входных пакетах рефлектора.

### RP (Reverse Path)

2-октетное поле, для которго Session-Sender **должен** устанавливать значение 0.

### Reserved

16-битовое поле, которое **должно** заполняться нулями при передаче и игнорироваться при получении.

STAMP Session-Reflector, получающий пакет с CoS TLV, **должен** включить CoS TLV в отраженный пакет. От также **должен** копировать значения полей DSCP и ECN из заголовка IP в принятом пакете STAMP в поле DSCP2 отраженного пакета. Кроме того, Session-Reflector **должен** использовать локальные правила для проверки соответствия CoS значению поля DSCP1, разрешенному в домене. При соответствии Session-Reflector **должен** установить поле DSCP в заголовке IP отраженного пакеты в соответствии с полем DSCP1 в полученном пакете. В противном случае Session-Reflector **должен** использовать значение DSCP из полученного пакета STAMP и установить RP = 1. При получении отраженного пакета с RP = 0 Session-Sender будет сохранять значения DSCP и ECN для анализа CoS в обратном направлении. Если в отраженном пакете RP = 1, CoS анализируется лишь для прямого направления.

Можно использовать перемаркировку CoS для разных сценариев (например, 2G, 3G, LTE в мобильных сетях) в одной сети. Однако при некорректной настройке будет сложно определить причину избыточной потери пакетов служб верхних уровней, тогда как для нижележащего уровня уровень потерь будет нормальным. использование CoS TLV в тестах STAMP помогает в поиске неполадок, а также проверке правил Diffserv при обработке CoS, требуемой конфигурацией.

## 4.5. TLV прямого измерения

Direct Measurement TLV позволяет собирать пакеты по профилю, т. е. из определенного потока данных, передаваемого от Session-Sender к Session-Reflector. Определение относящихся к профилю пакетов выходит за рамки документа и отдается на откуп оператору.

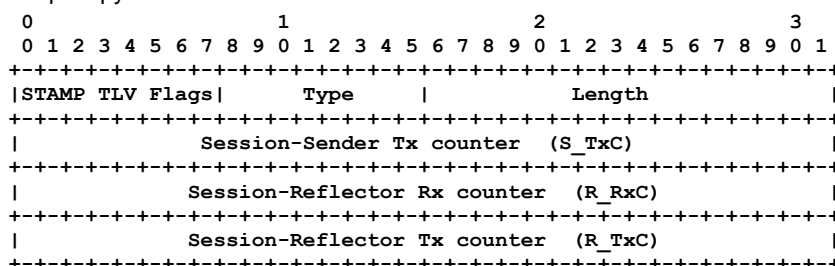


Рисунок 13. Direct Measurement TLV.

### STAMP TLV Flags

8-битовое поле флагов, формат которого показан на рисунке 6.

### Type

1-октетное поле, определяющее интерпретацию поля Value. Значения выделяются IANA (параграф 5.1).

### Length

2-октетное поле, указывающее размер поля Value в октетах. Поле **должно** иметь значение 12.

### Session-Sender Tx counter (S\_TxC)

4-октетное поле, к котором Session-Sender **должен** указывать число передаваемых по профилю пакетов.

### Session-Reflector Rx counter (R\_RxC)

4-октетное поле, которое Session-Sender **должен** устанавливать в 0, а Session-Reflector - игнорировать при получении. Рефлектор **должен** указывать в отраженных пакетах число принятых по профилю пакетов.

### Session-Reflector Tx counter (R\_TxC)

4-октетное поле, которое Session-Sender **должен** устанавливать в 0, а Session-Reflector - игнорировать при получении. Рефлектор **должен** указывать число переданных по профилю пакетов.

Session-Sender **может** включать Direct Measurement TLV в пакеты STAMP. При получении пакета STAMP с Direct Measurement TLV рефлектор **должен** включать этот блок TLV в отраженный пакет. Session-Reflector **должен** копировать значение поля S\_TxC из полученного пакета в то же поле отраженного пакета.



## 4.6. TLV отчета о сети доступа

STAMP Session-Sender **может** включать Access Report TLV (рисунок 14) для индикации рефлектору изменения статуса сети доступа. Определение сети доступа выходит за рамки документа.

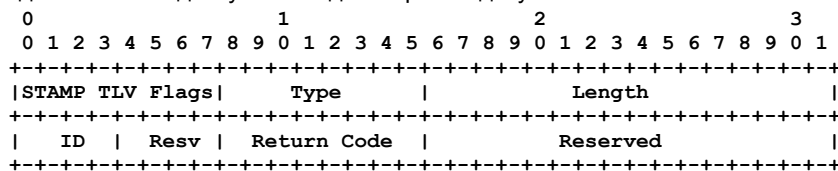


Рисунок 14. Access Report TLV.

### STAMP TLV Flags

8-битовое поле флагов, формат которого показан на рисунке 6.

### Type

1-октетное поле, определяющее интерпретацию поля Value. Значения выделяются IANA (параграф 5.1).

### Length

2-октетное поле со значением 4.

### ID (Access ID)

4-битовый идентификатор сети доступа, например, 3GPP (технологии радиодоступа, заданные 3GPP) или не-3GPP (доступ, не описанный 3GPP) [TS23501].

1

Сеть 3GPP.

2

Другая сеть (не-3GPP).

Другие значения недействительны и TLV с такими значениями **должны** отбрасываться.

### Resv

4-битовое поле, которое **должно** заполняться нулями при передаче и игнорироваться при получении.

### Return Code

1-октетное поле, идентифицирующее сигнал отчета, например, доступность или недоступность. Значение предоставляется конечной точке STAMP, механизмом, выходящим за рамки этого документа. Возможные значения приведены в параграфе 5.6.

### Reserved

2-октетное резервное поле, которое **должно** заполняться нулями при передаче и игнорироваться при получении.

STAMP Session-Sender, включающий Access Report TLV, устанавливает в поле Access ID значение, соответствующее типу сети, для которого передается отчет. Отправитель также указывает значение поля Return Code в соответствии с рабочим состоянием сети доступа. Механизм определения этого состояния выходит за рамки спецификации. Рефлектор, получивший тестовый пакет с Access Report TLV, должен включить такой TLV в отраженный пакет. Рефлектор **должен** скопировать в поля Access ID и Return Code значения из соответствующих полей принятого пакета.

Session-Sender **должен** запустить таймер повторной передачи после отправки тестового пакета с Access Report TLV. Таймер **должен** быть остановлен при получении отраженного пакета STAMP с Access Report TLV. Если отсчет таймера завершается до приема такого пакета, Session-Sender **должен** повторить тестовый пакет с Access Report TLV. Этот повтор **следует** выполнять до 4 раз, после чего процедуру нужно прервать. Установка значения таймера определяется локальной политикой и сетевым окружением. По умолчанию для таймера повтора Access Report TLV **следует** устанавливать значение 3 секунды. Реализация **должна** обеспечивать управления значением таймера и числом повторов.

Access Report TLV используется функцией измерения производительности (Performance Measurement Function или PMF) в системе управления доступом, коммутацией и разделением для сети 5G networks [TS23501]. PMF в пользовательском оборудовании выступает как STAMP Session-Sender, а PMF в пользовательской плоскости (User Plane) - как STAMP Session-Reflector.

## 4.7. Follow-Up Telemetry TLV

Session-Reflector может оказаться способным поместить в поле Follow-Up Timestamp лишь временную метку типа SW Local (таблица 9). Однако система хостинга может предоставлять временную метку ближе к началу реальной передачи пакета, даже если невозможно доставить информацию отправителю (Session-Sender) вовремя для самого пакета. Тем не менее, эта метка может быть важна для Session-Sender, поскольку она повышает точность измерения задержки в сети за счет минимизации влияния задержки в выходных очередях.

STAMP Session-Sender **может** включать Follow-Up Telemetry TLV для запроса информации у рефлектора. Session-Sender **должен** указать в полях Follow-Up Telemetry Type и Length подходящие для него значения. Поля Sequence Number и Follow-Up Timestamp **должны** заполняться отправителем нулями и игнорироваться рефлектором при получении пакета STAMP с Follow-Up Telemetry TLV. Рефлектор **должен** проверить значение поля Length в тестовом пакете STAMP. Если это значение недействительно, рефлектор **должен** обнулить поля Sequence Number и Follow-Up Timestamp, а также установить флаг M в поле STAMP TLV Flags отраженного пакета. Если рефлектор работает без поддержки состояния (параграф 4.2 в [RFC8762]), он **должен** обнулять поля Sequence Number и Follow-Up Timestamp.

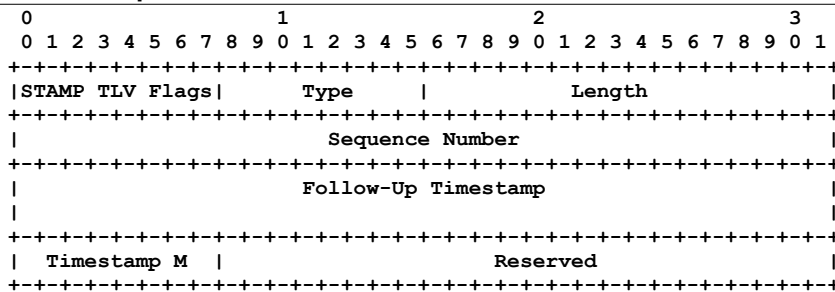


Рисунок 15. Follow-Up Telemetry TLV.

**STAMP TLV Flags**

8-битовое поле флагов, формат которого показан на рисунке 6.

**Type**

1-октетное поле, определяющее интерпретацию поля Value. Значения выделяются IANA (параграф 5.1).

**Length**

2-октетное поле со значением 16.

**Sequence Number**

4-октетное поле, указывающее порядковый номер последнего пакета, отраженного в данной сессии STAMP. Поскольку Session-Reflector работает в режиме с поддержкой состояния (параграф 4.2 в [RFC8762]), это будет порядковый номер Session-Reflector из предыдущего отраженного пакета.

**Follow-Up Timestamp**

8-октетное поле, формат которого задает флаг Z в поле Error Estimate базового пакета STAMP, который содержится в этом отраженном пакете от Session-Reflector, как описано в параграфе 4.2.1 [RFC8762]. Поле содержит временную метку момента передачи отраженного пакета с указанным номером.

**Timestamp M(ode)**

1-октетное поле, указывающее метод получения Follow-Up Timestamp элементом, передающим отраженный пакет STAMP (см. таблицу 9).

**Reserved**

2-октетное резервное поле, которое **должно** заполняться нулями при передаче и игнорироваться при получении.

**4.8. HMAC TLV**

STAMP в режиме с аутентификацией защищает целостность данных в базовом пакете STAMP. Расширения STAMP предназначены для предоставления дополнительных сведений об условиях в сети и их целостность тоже важна. Все базовые пакеты STAMP с аутентификацией (параграфы 4.2.2 и 4.3.2 в [RFC8762]), совместимые с этой спецификацией, **должны** также аутентифицировать дополнительные TLV путем включения HMAC TLV, за исключением случаев наличия лишь Extended Padding TLV. Блок HMAC TLV **должен** помещаться после всех TLV, включенных в пакет STAMP, за исключением Extra Padding TLV. Включение HMAC TLV в другое место расширенного тестового пакета STAMP **должно** считаться отказом при проверке HMAC, как указано ниже. HMAC TLV **можно** применять для защиты целостности расширений STAMP в режиме без аутентификации. Реализация расширений STAMP **должна** обеспечивать элементы управления для включения защиты целостности расширений в режиме без аутентификации.

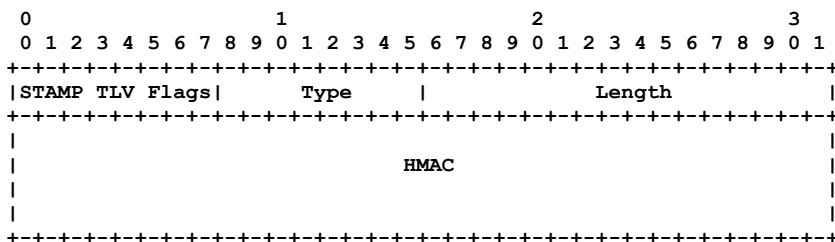


Рисунок 16. HMAC TLV.

**STAMP TLV Flags**

8-битовое поле флагов, формат которого показан на рисунке 6.

**Type**

1-октетное поле, определяющее интерпретацию поля Value. Значения выделяются IANA (параграф 5.1).

**Length**

2-октетное поле со значением 16.

**HMAC**

16-октетное поле с кодом HMAC для всех предшествующих TLV.

Как определено в [RFC8762], STAMP использует HMAC-SHA-256 с отсечкой до 128 битов (см. [RFC4868]). Все вопросы использования ключей, рассмотренные в параграфе 4.4 [RFC8762], полностью применимы к HMAC TLV. Управление ключами HMAC и механизмы их распространения выходят за рамки этой спецификации. Предполагается, что HMAC TLV будет отслеживать изменения базового протокола STAMP [RFC8762], включая применение более совершенных криптографических алгоритмов. Расчет HMAC выполняется в соответствии с [RFC2104] для конкатенации поля Sequence Number в стандартном пакете STAMP и всех предшествующих TLV. Подпись **должна** отсекается до 128 битов и помещаться в поле HMAC. Если HMAC TLV имеется в расширенном пакете STAMP, например, в режиме с аутентификацией, значение HMAC **должно** проверяться до использования данных, включенных в STAMP TLV. Если проверка HMAC рефлектором завершается отказом, Session-Reflector **должен** прекратить обработку полученного расширенного пакета STAMP. В этом случае рефлектор **должен** копировать TLV из полученного пакета STAMP в отраженный пакет и **должен** устанавливать флаг I = 1 в каждом TLV, копируемом в отраженный пакет, до отправки отраженного пакета. Если Session-Sender получает расширенный пакет STAMP с I = 1, он **должен** прервать обработку TLV в отраженном пакете. Если проверка HMAC у Session-Sender завершилась отказом, Session-Sender **должен** прервать обработку TLV в расширенном отраженном пакете STAMP.

## 5. Взаимодействие с IANA

Агентство IANA создало в реестре Simple Two-way Active Measurement Protocol (STAMP) TLV Types перечисленные в следующих параграфах субреестры.

### 5.1. Субреестр STAMP TLV Types

В IANA создан субреестр STAMP TLV Types, коды в котором выделяются в соответствии с [RFC8126], как указано в таблице 1.

Таблица 1. Процедуры регистрации для субреестров типов STAMP TLV.

Диапазон	Процедура регистрации
1 - 175	IETF Review
176 - 239	First Come First Served
240 - 251	Experimental Use
252 - 254	Private Use

В соответствии с этим документом в IANA создан субреестр STAMP TLV Types (таблица 2).

Таблица 2. Типы STAMP TLV.

Значение	Название	Документ
0	Резерв	RFC 8972
1	Extra Padding	RFC 8972
2	Location	RFC 8972
3	Timestamp Information	RFC 8972
4	Class of Service	RFC 8972
5	Direct Measurement	RFC 8972
6	Access Report	RFC 8972
7	Follow-Up Telemetry	RFC 8972
8	HMAC	RFC 8972
255	Резерв	RFC 8972

### 5.2. Субреестр STAMP TLV Flags

В IANA создан субреестр STAMP TLV Flags, коды в котором выделяются по процедуре IETF Review [RFC8126]. Флаги занимают 8 битов. В соответствии с этим документом в IANA создан субреестр STAMP TLV Flags (таблица 3).

Таблица 3. Флаги STAMP TLV.

Бит	Символ	Название	Документ
0	U	Unrecognized TLV	RFC 8972
1	M	Malformed TLV	RFC 8972
2	I	Integrity check failed	RFC 8972

### 5.3. Субреестр STAMP Sub-TLV Types

В IANA создан субреестр STAMP Sub-TLV Types, значения в котором выделяются в соответствии с [RFC8126], как указано в таблице 4.

Таблица 4. Процедуры регистрации для субреестров типов STAMP суб-TLV.

Диапазон	Процедура регистрации
1 - 175	IETF Review
176 - 239	First Come First Served
240 - 251	Experimental Use
252 - 254	Private Use

В соответствии с этим документом в IANA создан субреестр STAMP Sub-TLV Types (таблица 5).

Таблица 5. Типы STAMP суб-TLV.

Значение	Название	TLV	Документ
0	Резерв		RFC 8972
1	Source MAC Address	Location	RFC 8972
2	Source EUI-48 Address	Location	RFC 8972
3	Source EUI-64 Address	Location	RFC 8972
4	Destination IP Address	Location	RFC 8972
5	Destination IPv4 Address	Location	RFC 8972
6	Destination IPv6 Address	Location	RFC 8972
7	Source IP Address	Location	RFC 8972
8	Source IPv4 Address	Location	RFC 8972
9	Source IPv6 Address	Location	RFC 8972
255	Резерв		RFC 8972

### 5.4. Субреестр STAMP Synchronization Sources

В IANA создан субреестр STAMP Synchronization Sources, значения в котором выделяются в соответствии с [RFC8126], как указано в таблице 6.

Таблица 6. Процедуры регистрации для источников синхронизации STAMP.

Диапазон	Процедура регистрации
----------	-----------------------

1 - 127  
128 - 239  
240 - 249  
250 - 254

IETF Review  
First Come First Served  
Experimental Use  
Private Use

В соответствии с этим документом в IANA создан субреестр STAMP Synchronization Sources (таблица 7).

Таблица 7. Источники синхронизации STAMP.

Значение	Название	Документ
0	Резерв	RFC 8972
1	NTP	RFC 8972
2	PTP	RFC 8972
3	SSU/BITS	RFC 8972
4	GPS/GLONASS/LORAN-C/BDS/Galileo	RFC 8972
5	Local free-running	RFC 8972
255	Резерв	RFC 8972

## 5.5. Субреестр STAMP Timestamping Methods

В IANA создан субреестр STAMP Timestamping Methods, значения в котором выделяются в соответствии с [RFC8126], как указано в таблице 8.

Таблица 8. Процедуры регистрации для методов указания временных меток STAMP.

Диапазон	Процедура регистрации
1 - 127	IETF Review
128 - 239	First Come First Served
240 - 249	Experimental Use
250 - 254	Private Use

В соответствии с этим документом в IANA создан субреестр STAMP Timestamping Methods (таблица 9).

Таблица 9. Методы получения временных меток STAMP.

Значение	Название	Документ
0	Резерв	RFC 8972
1	HW Assist	RFC 8972
2	SW Local	RFC 8972
3	Control Plane	RFC 8972
255	Резерв	RFC 8972

## 5.6. Субреестр STAMP Return Codes

В IANA создан субреестр STAMP Return Codes, коды в котором выделяются в соответствии с [RFC8126], как указано в таблице 10.

Таблица 10. Процедуры регистрации для кодов возврата STAMP.

Диапазон	Процедура регистрации
1 - 127	IETF Review
128 - 239	First Come First Served
240 - 249	Experimental Use
250 - 254	Private Use

В соответствии с этим документом в IANA создан субреестр STAMP Return Codes (таблица 11).

Таблица 11. Коды возврата STAMP.

Значение	Название	Документ
0	Резерв	RFC 8972
1	Network available	RFC 8972
2	Network unavailable	RFC 8972
255	Резерв	RFC 8972

## 6. Вопросы безопасности

Этот документ определяет расширения протокола STAMP [RFC8762] и наследует все вопросы безопасности, связанные с базовым протоколом. В документе также определен блок HMAC TLV, обеспечивающий защиту целостности расширения STAMP, но он не защищает от replay-атак (повторное использование пакетов). Использование HMAC TLV описано в параграфе 4.8.

Для защиты от TLV с некорректным форматом реализации Session-Sender и Session-Reflector **должны**:

- проверять значение флага M;
- проверять корректность значения поля Length.

Поскольку эта спецификация задает механизм тестирования отображений DSCP, документ наследует все вопросы безопасности, рассмотренные в [RFC2474]. Мониторинг т необязательное управление DSCP с помощью CoS TLV можно использовать через Internet так, что Session-Sender и Session-Reflector будут размещаться в доменах с разными профилями CoS. Поэтому важна проверка оператором набора значений CoS, применяемых в домене Session-Reflector. Реализации Session-Reflector также **следует** поддерживать локальную политику для подтверждения возможности использования значения поля DSCP, переданного Session-Sender (параграф 4.4).

## 7. Литература

### 7.1. Нормативные документы

- [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>>.
- [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>>.
- [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>>.

### 7.2. Дополнительная литература

- [GPS] "Global Positioning System (GPS) Standard Positioning Service (SPS) Performance Standard", GPS SPS 5th Edition, April 2020.
- [IEEE.1588.2008] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE Std. 1588-2008, DOI 10.1109/IEEESTD.2008.4579760, July 2008, <<https://doi.org/10.1109/IEEESTD.2008.4579760>>.
- [NUM-IDS-GEN] Gont, F. and I. Arce, "On the Generation of Transient Numeric Identifiers", Work in Progress, Internet-Draft, draft-irtf-pearg-numeric-ids-generation-06, 13 January 2021, <<https://tools.ietf.org/html/draft-irtf-pearg-numeric-ids-generation-06>>.
- [RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", [RFC 2474](#), DOI 10.17487/RFC2474, December 1998, <<https://www.rfc-editor.org/info/rfc2474>>.
- [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>>.
- [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>>.
- [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>>.
- [TS23501] 3GPP, "Technical Specification Group Services and System Aspects; System Architecture for the 5G System (5GS); Stage 2 (Release 16)", 3GPP TS 23.501, 2019.

## Благодарности

Авторы признательны за внимательное рецензирование и вдумчивые комментарии Tianran Zhou, Rakesh Gandhi, Yuezhong Song и Yali Wang. Спасибо Al Morton за его замечанию и ценные предложения. Авторы также признательны за комментарии и предложения, полученные от Martin Duke.

## Участники работы

Ниже указан человек, внесший вклад в текст этого документа.

### Guo Jun

ZTE Corporation  
68# Zijinghua Road  
Nanjing  
Jiangsu, 210012  
China  
Phone: +86 18105183663  
Email: [guo.jun2@zte.com.cn](mailto:guo.jun2@zte.com.cn)

## Адреса авторов

### Greg Mirsky

ZTE Corp.  
Email: [gregimirsky@gmail.com](mailto:gregimirsky@gmail.com)

### Xiao Min

ZTE Corp.

Email: [xiao.min2@zte.com.cn](mailto:xiao.min2@zte.com.cn)

**Henrik Nydell**

Accedian Networks

Email: [hnydell@accedian.com](mailto:hnydell@accedian.com)

**Richard Foote**

Nokia

Email: [footer.foote@nokia.com](mailto:footer.foote@nokia.com)

**Adi Masputra**

Apple Inc.

One Apple Park Way

Cupertino, CA 95014

United States of America

Email: [adi@apple.com](mailto:adi@apple.com)

**Ernesto Ruffini**

OutSys

via Caracciolo, 65

20155 Milan

Italy

Email: [eruffini@outsys.org](mailto:eruffini@outsys.org)

Перевод на русский язык

**Николай Малых**

[nmalykh@protokols.ru](mailto:nmalykh@protokols.ru)