Technical Report

TR-390.2
Performance Measurement from IP Edge to Customer Equipment using STAMP

Issue: 1
Issue Date: November 2020

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	5 November 2016	5 November 2016	Gregory Mirsky, ZTE	Original

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editor: Gregory Mirsky, ZTE

Work Area Director(s): David Sinicrope, Ericsson

Project Stream Leader(s): Gregory Mirsky, ZTE

Table of Contents

Table of Figures

Table of Tables

Executive Summary

In today’s demanding broadband service delivery environment, the industry is lacking the ability to use standardized mechanisms to monitor service quality and measure performance in the broadband access network for residential and business subscribers.

This Technical Report defines the capabilities required in the Customer Equipment and the IP Edge for service assurance of broadband subscribers using Simple Two-way Active Measurement Protocol (STAMP) performance measurement, including architectural and nodal requirements.

1 Purpose and Scope

1.1 Purpose

Reliable and well-performing network services are becoming critical for broadband subscribers, as more and more their lives rely on a "connected world". In this demanding and competitive environment, Service Providers are looking for insight on how their networks are performing but cannot currently use standardized mechanisms for performance measurement of the access network, which provides service to residential and business subscribers.

TR-304 [8] specifies a performance measurement framework for measuring performance in Multi-Service Broadband Networks (MSBN). TR-143 [3] defines an Active Monitoring test suite that can be used for network performance measurement from the RG to a Network Test Server. TR-390 [19] has built on these TRs and defined architectural and nodal requirements to enable Service Providers (SPs) to monitor the performance of the access network, between the Customer Equipment (CE) and the IP Edge (MS-BNG, PE, etc.) using subset of functionalities of Two-Way Active Measurement Protocol (TWAMP) [15] known as TWAMP Light (TWL). Though TWL described in the body of RFC 5357 it is contained in Appendix I, thus not obtaining the standard but only informational status. Resulting from that, interoperability issues among numerous implementations exist despite the massive deployment of TWL. This Technical Report extends the model to perform performance measurement described in TR-390 as it applies it to the new standard performance measurement protocol, Simple Two-way Active Measurement Protocol (STAMP) [20].

Therefore, the main goals for this document are to:

- Describe how to use STAMP performance measurement in the MSBN. Resulting metrics include but not limited to latency, jitter and packet loss
- Give service providers a standards-based tool to gain insight on how their access network is performing
- Facilitate the use of existing but not currently deployed tools

1.2 Scope

This Technical Report describes in-service performance measurement tests in the on-demand as well as in proactive testing, including continuous monitoring. Service providers may decide to use one, the other or both modes, depending on their business objectives and dimensioning criteria.

TR-390.2 covers performance measurement in the access network for the broad spectrum of BBF defined MSBN architectures, including but not limited to:

- IPoE and PPPoX models (TR-101 [2] /TR-178 [4])
- Wholesaling scenarios (L2, L3, LAC/LNS)
- WLAN access networks (TR-203 [5] / TR-291 [7]/ TR-321 [10])
- Network Enhanced Residential Gateway (TR-317 [9])
- Virtual Business Gateway (WT-328 [11])

The performance measurement toolkit defined in TR-390.2 can be re-used for network-wide performance measurement as described in TR-304, that is performance measurement between any point in the network and the CE, but no specific nodal requirements for this are covered in TR-390.2.

The scope of this Technical Report covers:

- Definition of in-service performance measurement tests between the Customer Equipment and IP Edge
- Support for multiple CoS, for per traffic class performance measurements
- Resulting requirements for the CE and IP Edge
- Aspects of proactive performance monitoring between the Customer Equipment and IP Edge

- Backward compatibility with the devices conforming to TR-390

The following are outside of the scope of TR-390.2:

- Scaling impact of in-service, proactive, continuous monitoring
- Out-of-service tests, like service activation, which typically involve throughput measurement (such as ITU-T Y.1564 [17])
- Network-wide performance measurement
- TR-069 [1] extensions in support of the defined solution

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [14] and RFC 8174 [18].

MUST This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification.

MUST NOT This phrase means that the definition is an absolute prohibition of the specification.

SHOULD This word, or the term “RECOMMENDED”, means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.

SHOULD NOT This phrase, or the phrase “NOT RECOMMENDED” means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.

MAY This word, or the term “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

	Document	Title	Source	Year
[1]	TR-069 Amendment 6	CPE WAN Management Protocol	BBF	March 2018
[2]	TR-101 Issue 2	Migration to Ethernet-Based Broadband Aggregation	BBF	2011
[3]	TR-143 Issue:1 Amendment 1 Corrigendum 1	Enabling Network Throughput Performance Tests and Statistical Monitoring	BBF	August 2015
[4]	TR-178	Multi-service Broadband Network Architecture and Nodal Requirements	BBF	2014
[5]	TR-203	Interworking between Next Generation Fixed and 3GPP Wireless Networks	BBF	2012
[6]	TR-242	IPv6 Transition Mechanisms for Broadband Networks	BBF	2015

	Issue 2			
[7]	TR-291	Nodal Requirements for Interworking between Next Generation Fixed and 3GPP Wireless	BBF	2014
[8]	TR-304	Broadband Access Service Attributes and Performance Metrics	BBF	2015
[9]	TR-317	Network Enhanced Residential Gateway	BBF	2016
[10]	TR-321	Public Wi-Fi Access in Multi-service Broadband Networks	BBF	2015
[11]	WT-328	Virtual Business Gateway	BBF	2017
[12]	TR-345	Broadband Network Gateway and Network Function Virtualization	BBF	2016
[13]	TR-348	Hybrid Access Broadband Network Architecture	BBF	2016
[14]	RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997
[15]	RFC 5357	A Two-Way Active Measurement Protocol (TWAMP)	IETF	2008
[16]	RFC 8545	OWAMP and TWAMP Well-Known Port Assignments	IETF	2019
[17]	Y.1564	Ethernet service activation test methodology	ITU-T	2016
[18]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words	IETF	2017
[19]	TR-390	Performance Measurement from IP Edge to Customer Equipment Using TWAMP Light	BBF	2017
[20]	RFC 8762	Simple Two-way Active Measurement Protocol	IETF	March 2020
[21]	draft-ietf-ippm-stamp-yang-06	Simple Two-way Active Measurement Protocol (STAMP) Data Model	IETF	September 2020
[22]	RFC 7820	UDP Checksum Complement in OWAMP and TWAMP	IETF	2016
[23]	draft-ietf-ippm-stamp-option-tlv-09	Simple Two-way Active Measurement Protocol Optional Extensions	IETF	October 2020
[24]	PORTREG	Service Name and Transport Protocol Port Number Registry	IANA	N/A
[25]	TR-369a1	TR-369 Amendment 1: User Service Platform (USP)	BBF	October 2019
[26]	RFC 2865	Remote Authentication Dial In User Service (RADIUS)	IETF	June 2000
[27]	RFC 3576	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)	IETF	July 2003
[28]	TR-181 Issue 2 Amendment 12	Device Data Model for TR-069	BBF	February 2010

2.3 Definitions

The following terminology is used throughout this Technical Report.

IP Edge A generic term to refer to the logical function that is the first IP hop from the point of view of the customer traffic. In the context of TR-390.2, the following are considered to be IP Edge: MS-BNG, PE, vG, vBG, LNS, TWAG.

CE Customer Equipment. In the context of TR-390.2, CE is a generic term to refer to network equipment placed in the customer premises and includes the following: RG, BG, BRG, pBG, AP.

STAMP Session-Sender A logical function that transmits test packets to one or more STAMP Session-Reflectors, and determines performance metrics from the reflected test packets.

STAMP Session-Reflector A logical function that acts as a test point in the network, following the Session-Reflector behavior of STAMP, as per Section 4.2 of [20]. The STAMP Session-Reflector MAY do not know of the session state, i.e., be in stateless mode.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

AFTR	DS-Lite Address Family Transition Router
AP	Wi-Fi Access Point
BG	Business Gateway
BNG	Broadband Network Gateway
BRG	Bridged Residential Gateway
CoA	Change-of-Authorization
CoS	Class of Service
CPE	Customer Premises Equipment
CPU	Computer Processing Unit
DSCP	Differentiated Services Code Point
GPS	Global Positioning System
HAG	Hybrid Access Gateway
HCPE	Hybrid CPE
IETF	Internet Engineering Task Force
IP	Internet Protocol
LAC	L2TP Access Concentrator
LAN	Local Area Network
LNS	L2TP Network Server
MSBN	Multi-Service Broadband Network
NTP	Network Time Protocol
OAM	Operations Administration and Maintenance
pBG	Physical Business Gateway
PE	Provider Edge Router
PGW	Packet Data Network Gateway
PTP	Precision Time Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RTT	Round-Trip Time
SLA	Service Level Agreement
STAMP	Simple Two-way Active Measurement Protocol

TTL	Time-To-Live
TWAG	Trusted WLAN Access Gateway
TWAMP	Two-Way Active Measurement Protocol
TWL	TWAMP Light (RFC 5357, Appendix I)
UDP	User Datagram Protocol
vBG	Virtual Business Gateway
vG	Virtual Gateway
VLAN	Virtual Local Area Network
WA	Work Area
WAN	Wide Area Network
WT	Working Text

3 Technical Report Impact

3.1 Energy Efficiency

TR-390.2 has no significant impact on energy efficiency. Although performance measurement mechanisms defined in TR-390.2 will make use of additional computational cycles in the Customer Equipment and IP Edge nodes, these will cause a minimal contribution to energy consumption.

3.2 Security

Enabling a STAMP Session-Reflector function at the CE opens an additional potential door for attackers to use, as the port used for STAMP testing (UDP port 862) must be opened in the CE firewall. Potential security risks include:

- Denial-of-service (DoS) attacks, especially in the case where time-stamping, i.e., reading the value of the wall clock and storing this value into a STAMP test packet, is done in software
- Man-in-the-middle attacks, where the attacker may modify the STAMP test packets and alter the measurement results

Using a well-known port at the STAMP Session-Reflector could allow it to be more easily targeted by attackers.

While STAMP supports an authentication option, this Technical Report does not require its use, as it increases the implementation complexity and may cause inaccuracies in time-stamping. Instead, TR-390.2 makes use of prefix-lists and TTL-based filtering.

In addition to these measures, the following options will also help mitigate the opportunities for attack:

- Using private IPv4 addressing for STAMP tests, which makes the CPE unreachable for STAMP outside of the domain
- Setting a filtering rule at the IP Edge preventing any STAMP test traffic towards the CE other than that originated by the IP Edge

3.3 Privacy

TR-390.2 has no impact on privacy.

4 Introduction

In typical Service Provider networks, the access and aggregation network has a high impact on service quality. The reasons are often specific to the access technology and include limited QoS capabilities and a relatively high aggregation factor, also referred to as overbooking or oversubscription.

To help Service Providers better understand the service impact of the access network, this Technical Report defines a test method to measure service performance between the IP Edge and the CE. The key performance attributes of interest are packet delay (latency), packet delay variation (jitter) and packet loss ratio.

4.1 Simple Two-way Active Measurement Protocol (STAMP)

STAMP, defined in draft-ietf-ippm-stamp [20], is a new standard-based protocol to measure network performance. STAMP provides light-weight architecture, mitigating the need for a control protocol. To control and manage STAMP test sessions, the use of YANG data model, defined in draft-ietf-ippm-stamp-yang [21], is RECOMMENDED. Alternatively, the control MAY be provided using proprietary management solution, e.g., Command Line Interface (CLI) system or a Network Management System.

Two functions are required in STAMP architecture:

- STAMP Session-Sender: Owns the test session. Generates outgoing STAMP test packets and derives metrics of the test session based on returning test packets from the Session-Reflector.
- STAMP Session-Reflector: Reflects incoming packets to the STAMP Session-Sender while:
  - copying the necessary information received in the PDU (e.g., Sequence Number, received timestamp, etc.);
  - recording the number of received packets and time stamping upon receiving;
  - and, finally, recording the number of reflected packets and time stamping the packets transmission back to the source.

The CE is expected to implement, at the minimum, the STAMP Session-Reflector function while the IP Edge performs the STAMP Session-Sender functions. The STAMP test session is run between the IP Edge and the CE as shown in Figure 1:

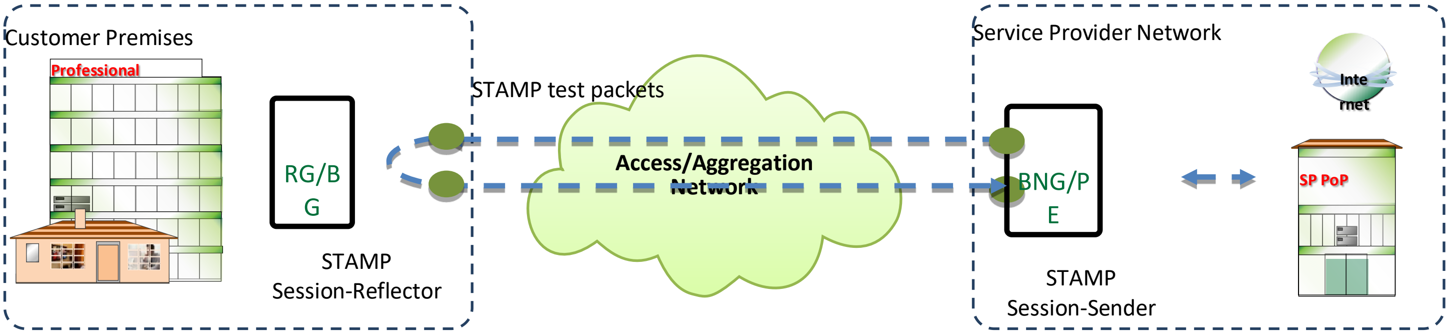

Figure 1 – BNG/PE to RG/BG performance measurement with STAMP

The Figure 2 shows the case where the transport network between the CE and the IP Edge (from the point of view of the end devices) is not a Layer 2 network, using the example of the Overlay LSL architecture described in TR-317 (NERG) and TR-328 (VBG).

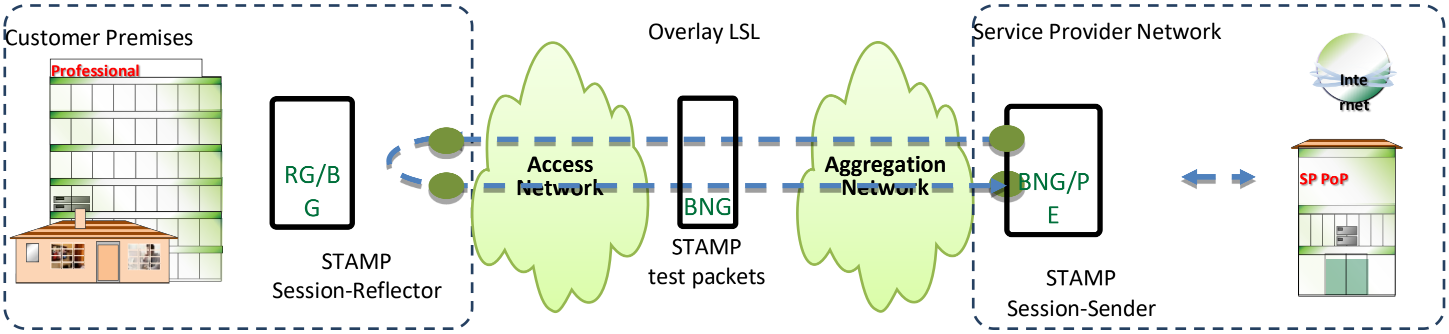

Figure 2 – STAMP-based performance measurement in the context of TR-317/TR-328

Performance measurement using STAMP can be operated over the broad spectrum of BBF defined MSBN architectural options:

BBF TR	STAMP Session-Sender	STAMP Session-Reflector
TR-101	MS-BNG	RG
TR-101 (LAC/LNS)	LNS	RG
TR-178 / TR-345 [12]	Edge BNG / Service BNG	RG / BG
TR-242 [6] (DS-Lite)	AFTR	RG
TR-242 (6rd)	6rd BR	RG
TR-291	TWAG	RG / AP
TR-291 (S2 extension)	PGW	RG / AP
TR-317	vG	BRG
TR-321	BNG	RG / AP
TR-321 (3GPP routed)	PGW	RG / AP
TR-328	vBG	pBG
TR-348 [13]	HAG	HCPE

Table 1 STAMP test endpoints in BBF architectures

For all these use cases, the prerequisite is to have IP connectivity between the two endpoints for performance monitoring. As such, the following considerations apply for the specific MSBN architectures:

- In L2 wholesaling scenario, TR-390.2 capabilities apply only to the retailer.
- In Wi-Fi architectures described in TR-291 and TR-321, in addition to its regular functions, the RG/AP request an IP address for itself as it if were a UE.
- In NERG, defined in TR-317, STAMP testing is done over the LSL. The BRG must request an IP address within the LAN domain.
- In the VBG System architecture, defined in WT-328, STAMP testing is done over the LSL. The pBG must request or be configured with an IP address for use over the LSL:
  - Bridged pBGs must have an IP address within the LAN domain
  - Routed and Routing & Bridging pBGs can use the pBG LSL IP address

Note that STAMP Session-Sender functions could also be run from a test platform beyond the IP Edge, allowing measurement of performance from different points within the service provider's network to the CE. However, definition and requirements for this scenario are out of the scope of TR-390.2.

4.1.1 STAMP test session modes

Proactive monitoring permits timely reporting of the fault and/or performance status. It can be carried on continuously as a single test session unbound in time. Such mode is referred to as Continuous monitoring [21]. Another proactive monitoring mode is referred to as Periodic [21], when an unlimited number of consecutive test sessions with each session transmitting the specified number of test packets repeated over at the specified intervals. On-demand monitoring is usually used to collect performance metrics in networks after the detection of a problem, report of the degradation of the quality of experience by a subscriber. It is carried only in Periodic mode with a limited number of the test sessions.

4.1.1.1Continuous test

In a Continuous mode [21], a STAMP Session-Sender is configured with the rate of the test packets and the value of a Measurement Interval. The Measurement Interval defines the periodicity at which the STAMP Session-Sender reports the required performance metrics.

4.1.1.2Periodic test

In the Periodic mode [21], a STAMP Session-Sender is provisioned with the rate of the test packets and the number of the packets for one test session, number of the test sessions, and the time interval between the consecutive test sessions. Also, the Test Collection timer is configured by which value the STAMP Session-Sender delays the calculation of the performance metrics for the completed test session after the last test packet in the session was transmitted. Hence, the Measurement Interval in the Periodic mode is from when the STAMP Session-Sender transmits the first test packet in the test session until the Test Collection timer expires.

4.1.2 STAMP Session-Reflector modes

Stateful Packet Loss measurements [21] require that the STAMP Session-Reflector maintains test state determining forward loss, gaps recognized in the received sequence number. That implies that the STAMP Session-Reflector keeps a state for each test session, uniquely identifying which test packets belong to one such test session instance, and enabling adding a sequence number in the reflected test packet that is individually incremented on a per-session basis. The method used by the STAMP Session-Reflector to keep a state for each test session is beyond the scope of this document.

Stateless Packet Loss measurements [21] do not require the STAMP Session-Reflector to maintain test state, and the Session-Reflector will reflect the received sequence number without modification.
Stateful Packet Loss measurement allows one-way packet loss to be measured. Stateless Packet Loss measurement allows only two-way packet loss to be measured.

Also, the Session-Reflector can be either Stateless (does not maintain test state) or Stateful (maintains test state). A Stateful STAMP Session-Reflector can be used to measure one-way packet loss. A Stateless STAMP Session-Reflector can be used to measure two-way packet loss only.

5 Solution description

This Technical Report describes the procedures and requirements for performance measurement of the Access / Aggregation Network using STAMP. In this scenario, the equipment located at the customer premises (e.g., RG, BG) performs STAMP Session-Reflector function, and the IP Edge node (e.g., BNG, PE, etc.) implements the STAMP Session-Sender role.

Using STAMP as a performance measurement tool requires that the STAMP Session-Reflector, the CE in the context of TR-390.2, has an IP address that is reachable from the STAMP Session-Sender. This IP address must be reachable by the IP Edge platform and is either bound to the WAN interface or a loopback interface at the CE.

STAMP can be used over IPv4 and IPv6 networks natively. It uses unicast IP addressing. For IPv4, in most cases, tests will be directed at the CE WAN interface IP address, with the exceptions described in Table 2.

CE type	IPv4 address in use at CPE for STAMP
General case	CE WAN interface IPv4 address, e.g., DHCP/PPPoE/static.
TR-291/TR-321	The CE will use DHCP to obtain an address for itself, allocated by the BNG/TWAG/PGW.
TR-317/WT-328	The CE will use DHCP over the LSL to obtain an address for itself, allocated by the vG/vBG. Alternatively, static IP addressing over the LSL may be used.

Table 2 CE IPv4 addresses to use for STAMP

In the IPv6 case, different addressing models may be used. TR-390.2 mandates the use of the IPv6 addresses listed in Table 3 for the respective models.

IPv6 Addressing Mode	IPv6 address in use at CPE for STAMP
Numbered WAN – DHCPv6	DHCPv6 IA_NA
Numbered WAN – SLAAC	SLAAC WAN address. In the case an IPv6 Temporary Address (TA) is used by the CE, the CE must reflect STAMP test packets using newest TA
Unnumbered WAN + PD	A preassigned address within the PD prefix. *For example, always use ::10 address in the PD. If the PD assigned is 2000::, then 2000::10 would be for the STAMP Session-Reflector function)*
TR-291/TR-321	The CE will use SLAAC to obtain an IP address for itself, allocated by the BNG/TWAG/PGW. Same notes as above for SLAAC apply.
TR-317/WT-328	The CE will use either SLAAC or DHCPv6 over the LSL to obtain an IP address for itself, allocated by the vG/vBG. Same notes as above for SLAAC/DHCPv6 apply.

Table 3 CE IPv6 addresses to use for STAMP

While STAMP could make use of any UDP port in the Dynamic and/or Private Ports range (49152-65535) as the Destination UDP port by a Session-Sender, the use of a well-known port TWAMP-Test Receiver Port (862) [16] as the default is required to simplify the provisioning and testing workflows.

Although it is possible to use STAMP in multiple modes, including those allowing for authentication of test packets, TR-390.2 does not rely on these mechanisms, as they increase the implementation complexity and may cause inaccuracies in time-stamping, especially in lower-end platforms.

Instead, TR-390.2 makes use of prefix-lists and TTL-based filtering for protection of the STAMP Session-Reflector at the CE, and not allowing the IP Edge to accept and process any STAMP test packets from any non-active STAMP test sessions. TTL filtering at the CE is set to a single hop to allow testing only from the IP Edge.

STAMP performance measurement can be used in either on-demand or continuous modes. Running STAMP on-demand allows its use for reactive testing and troubleshooting whereas continuous measurement allows proactive detection of performance issues on customer service (e.g., for premium enterprise customers). Service providers can decide to use one, the other or both modes, depending on their business objectives and dimensioning criteria.

Since multiple Classes of Service will typically be transported over the access and aggregation networks, TR-390.2 supports running multiple test sessions between a given pair of testing endpoints for per traffic class performance measurements. In this case, packets of each test session are marked with the DSCP value of the corresponding session at the STAMP Session-Sender and processed appropriately by the STAMP Session-Reflector. The 4-tuple Source IP, Destination IP, Source UDP Port, and Destination UDP Port provide a unique index for each test session. A different UDP source port is used for each test session.

Activation and configuration of STAMP in the MSBN is simplified as much as possible, by making use of default parameters as listed in Section 6 as well as by having the STAMP Session-Reflector function enabled by default on the CE. By doing this, the activation workflow for a test session is constrained to the IP Edge platform. For those cases where the default values are not sufficient, management and provisioning of STAMP attributes in the CE could also be supported by TR-390.2, e.g., utilizing TR-069 [1] or TR-369 (USP) [25]. At the time of this writing, work is ongoing on a TR-181 Issue 2 Amendment 12 [28] data model for TR-069 management of the STAMP client in the CE. Meanwhile, vendor-specific extensions can be used.

This Technical Report recommends the support of hardware-based time-stamping to improve the accuracy of the delay and delay variation measurements. It is recognized that this will not be possible in all cases, e.g., where the IP Edge is deployed as a VNF. It is also expected that lower-end CE devices will not be capable of hardware-based time-stamping. It is essential that implementations not supporting such mechanisms apply measures in software to prevent high CPU load conditions or other high priority tasks to affect the quality of the timestamps.

In the event the STAMP timestamp application for IPv6 occurs after the computation of the original UDP Checksum, the UDP checksum must be re-calculated, as the UDP Checksum field cannot be set to zero in IPv6 packets, which is allowed only for IPv4. RFC 7820 [22] proposes an alternative that consists of modifying the last two octets of the STAMP test packet payload (padding) and use them as a Checksum Complement, to reflect checksum change caused by the new timestamp. Implementations may choose to either re-calculate the UDP checksum or use the Checksum Complement approach. To allow both approaches for IPv6, TR-390.2 mandates that both the Session-Sender and Session-Reflector must send STAMP packets with an additional two octets-long Payload (padding) field, beyond the minimum requirement for symmetrical packet handling (27 bytes).

Even though STAMP test packets could be reassembled at the receiving end if fragmentation has occurred along the path, this would have a significant impact on the accuracy of the measurements. The proper operation of TR-390.2 depends on the STAMP test packets not having been fragmented. In order to avoid the fragmentation of STAMP test packets, the IP Edge is required to use a Path Maximum Transmission Unit Discovery protocol.

For performance measurement to be meaningful, statistics need to be collected and processed to gain insight into how the network is performing. TR-390.2 mandates the collection of delay, delay variation, packet loss ratio, and service availability performance metrics. More complex metrics such as minimum, maximum, average, and percentile values over a period of time; statistics for one-way, in forward and reverse directions, and round-trip could be derived locally at the IP Edge or provided by external platforms. The use of an external clock reference (e.g., NTP, PTP, GPS, …) in both the IP Edge and the CE will allow for calculation of useful one-way delay metrics.

6 Nodal Requirements

6.1 CE Requirements

[R-1] The CE MUST support STAMP Session-Reflector in the Unauthenticated mode as defined in Section 4.2.1 [1] **Error! Bookmark not defined.**[20].
[R-2] The CE MUST support STAMP Session-Reflector in the Authenticated mode as defined in Section 4.2.2 [20].
[R-3] When STAMP is enabled, the CE MUST use TWAMP-Test Receiver Port [24], as the default STAMP Session-Reflector receive port.
[R-4] The CE MUST support STAMP with IPv4 encapsulation,
[R-5] The CE MUST support STAMP with IPv6 encapsulation
[R-6] The CE MUST support symmetrical packet size, i.e., STAMP Session-Reflector transmits reflected packets of the same packet size as the received packets.
[R-7] The CE MUST support access-list filtering of IP ranges for the source address of STAMP test packets it receives.

According to the base STAMP specification [RFC8762] a Session-Sender and a Session-Reflector always use symmetrical test packets.

[R-8] The CE SHOULD support access-list filtering of source UDP port ranges for STAMP test packets it receives.
[R-9] The CE MUST support at least eight access-lists to comply with [R-14] in Section IP Edge Requirements.
[R-10] The CE MUST support configurable STAMP values for the parameters listed in Table 4.

Attribute	Default	Description
Administrative State	Disabled (IPv4+IPv6)	Controls the administrative state of the STAMP Session-Reflector
STAMP IP Address	IPv4: As per Table 2	IP address that the STAMP Session-Reflector listens on
	IPv6: As per Table 3	
STAMP Destination UDP Port	TWAMP-Test Receiver Port	UDP Port to listen for STAMP Test Packets
TTL/Hop Limit Security	Enabled	Check against IP TTL/Hop Limit
TTL/Hop Limit	1 hop	The value expected in a received STAMP test packet
IP Security	Disabled (0.0.0.0/0)	Check against IP Source Address
UDP Security	Disabled	Check against UDP Source Port
Timestamp format	NTP	Timestamp encoding (NTP or PTPv2)

Table 4 CE STAMP configurable parameters

[R-11] The CE MUST silently discard any fragmented STAMP test packets received.
[R-12] The CE SHOULD support hardware-based time-stamping of STAMP test packets.
[R-13] The CE MUST support NTP timestamp format.
[R-14] The CE SHOULD support PTPv2 timestamp format.
[R-15] The CE SHOULD support management using Netconf or RESTCONF with STAMP YANG data model.
[R-16] The CE SHOULD support STAMP management using TR-069 [1] or TR-369 (USP) [25].
[R-17] The CE SHOULD support STAMP Extensions as described in [23].
[R-18] If the CE supports Unauthenticated STAMP mode, it MUST support the Extra Padding TLV [23].
Timestamp Information TLV [23] helps to evaluate the accuracy of a timestamp and, as a result, the accuracy of the delay measurement, and calculation of performance metrics using the delay measurement.

[R-19] If the CE supports Unauthenticated STAMP mode, it MUST support the Timestamp Information TLV [23].

Class of Service TLV [1] allows testing of CoS marking.

[R-20] If the CE supports Unauthenticated STAMP mode, it MUST support the Class of Service TLV [23].

One-way metrics, delay in particular, require, clock synchronization (e.g., NTP, PTP, GPS, …).

[R-21] The CE MUST support clock synchronization.

6.2 IP Edge Requirements

[R-22] The IP Edge MUST support STAMP Session-Sender in the Unauthenticated mode as defined in Section 4.1.1 [20].

[R-23] The IP Edge MUST support STAMP Session-Sender in the Authenticated mode as defined in Section 4.1.2 [20].

[R-24] The IP Edge MUST support STAMP with IPv4 encapsulation.

[R-25] The IP Edge MUST support STAMP with IPv6 encapsulation.

[R-26] The IP Edge MUST transmit base STAMP test packets as its default behavior

[R-27] The IP Edge MUST support NTP timestamp format.

[R-28] The IP Edge MUST support PTPv2 timestamp format.

[R-29] The IP Edge MUST support on-demand STAMP test sessions.

[R-30] The IP Edge MUST support continuous STAMP test sessions.

[R-31] The IP Edge SHOULD support STAMP Extensions, as described in [23].

[R-32] If the IP Edge supports Unauthenticated STAMP mode it MUST support Extra Padding TLV [23].

Timestamp Information TLV helps to evaluate the accuracy of a timestamp and, as a result, the accuracy of the delay measurement, and calculation of performance metrics using the delay measurement.

[R-33] If the IP Edge supports Unauthenticated STAMP mode, it MUST support Timestamp Information TLV.

Class of Service TLV allows testing of CoS marking.

[R-34] If the IP Edge supports [1], it MUST support Class of Service TLV.

[R-35] The IP Edge MUST support at least eight concurrent STAMP test sessions for a given endpoint.

[R-36] The IP Edge MUST support configurable values per STAMP test session for the parameters listed in Table 5.

[R-37] The IP Edge MUST NOT accept or process STAMP test packets that are not associated with active test sessions.

[R-38] The IP Edge SHOULD support reporting of discarded STAMP test packets for invalid sessions.

[R-39] The IP Edge MUST silently discard any fragmented test packets received.

[R-40] The IP Edge SHOULD support reporting of discarded STAMP test packets due to fragmentation.

One-way metrics, delay in particular, require clock synchronization (e.g., NTP, PTP, GPS, …).

[R-41] The IP Edge MUST support clock synchronization (both frequency and time).

[R-42] The IP Edge SHOULD support management according to STAMP YANG data model Section x.y.z [21].

Other methods of managing the STAMP protocol and related functionality are outside the scope of this document.

[R-43] The IP Edge MUST support collection and reporting of performance metric statistics per test session according to STAMP YANG data model in Section x.y.z [21].

For IP Edge implementations supporting IP Sessions as defined in TR-146, e.g., BNG, vG, the following requirements apply:

[R-44] The IP Edge MUST support the activation of STAMP test sessions during initial IP session setup, utilizing a RADIUS [26] Access-Accept message

[R-45] The IP Edge MUST support the activation of STAMP test sessions during the life of an IP session, utilizing a RADIUS [27] Change-of-Authorization (CoA) message

[R-46] The IP Edge MUST support de-activation of STAMP test sessions during the life of an IP session, utilizing a RADIUS [27] CoA message

Attribute	**Default**	**Description**
Source IP	-	Source IP address of the STAMP test session
Destination IP	-	Destination IP address of the STAMP test session
Source UDP port	Auto-generate	Source UDP port of the STAMP test session
Destination UDP port	TWAMP-Test Receiver Port	Destination UDP port of the STAMP test session
Packet size	44 bytes in Unauthenticated mode 112 bytes in Authenticated mode	Size of the STAMP test packets
TTL or Hop Limit	1	TTL/Hop Limit field of the IP header of the test packets
DSCP	0x000 (Best Effort)	DSCP field of the IP header of the test packets
Timestamp format	NTP	Timestamp encoding (NTP or PTPv2)
Interval	1 second	Amount of time between STAMP test packet transmission
Test duration	5 minutes	Amount of time the STAMP test will run before stopping automatically

Table 5 IP Edge STAMP test session configurable parameters

7 STAMP interoperability with TR-390 TWAMP Light-based system

The ability for a STAMP system to interwork with a TWAMP Light (TWL) system in performance measurement from IP Edge to a Customer Equipment is one of the key requirements for STAMP protocol. Because STAMP and TWAMP use different algorithms in Authenticated mode (HMAC-SHA-256 vs. HMAC-SHA-1), interoperability is only considered for the Unauthenticated mode. Throughout this text, a TWL system is the system that conforms to the TR-390 specification. Also, “ability to interwork” and “interoperability” used interchangeably throughout this section.

There are two possible scenarios of STAMP and TWL interworking considered below.

7.1 STAMP Session-Sender at IP Edge and TWL Session-Reflector at Customer Equipment side

This case, presented in Figure 1, does not introduce any new requirements in addition to those listed in 6.2 because:

- A TWL system by default is listening on UDP port 862 ([R-2] Section 6.1 TR-390)
- A TWL system is required to generate reflected test packet of the symmetrical size by adding TWAMP padding ([R-6] Section 6.1 TR-390). As a result, the Session-Sender will receive from the TWL system the reflected packet indistinguishable from a STAMP base Session-Reflector packet in the Unauthenticated mode.

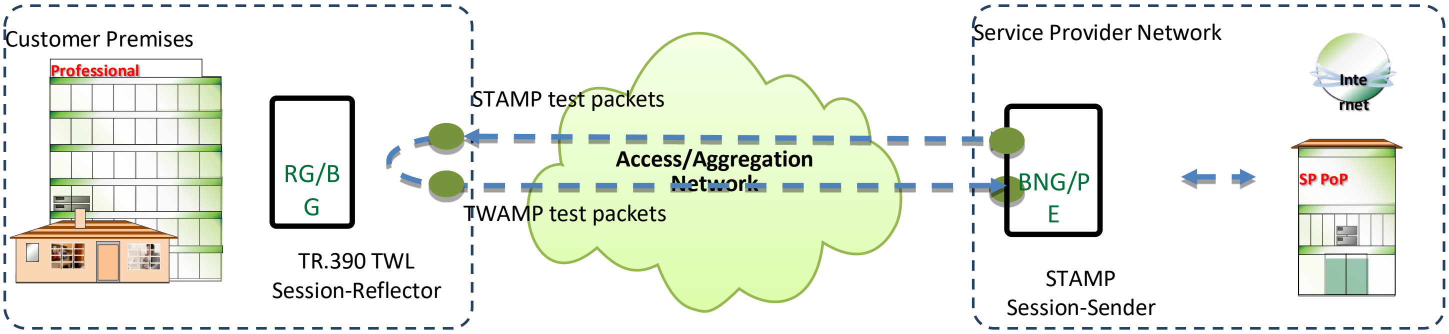

Figure 3 - Performance measurement from STAMP-based PE with TR.390-based CE

- A STAMP system can interpret NTP and PTPv2 timestamp formats, and it MAY use any of them. Calculation of the delay is performed by the Session-Sender, which, in this case, is a STAMP system. Thus, since the STAMP system can identify and interpret both formats, TWL using only NTP format does not cause a problem.

7.2 TWL Session-Sender at IP Edge and STAMP Session-Reflector at Customer Equipment side

In this scenario, (presented in Figure 2), a STAMP system, acting as a Session-Reflector, can interwork with TWL system acting as Session-Sender using its default values:

- UDP port to listen for test packets - 862;
- timestamp encoding format - NTP.

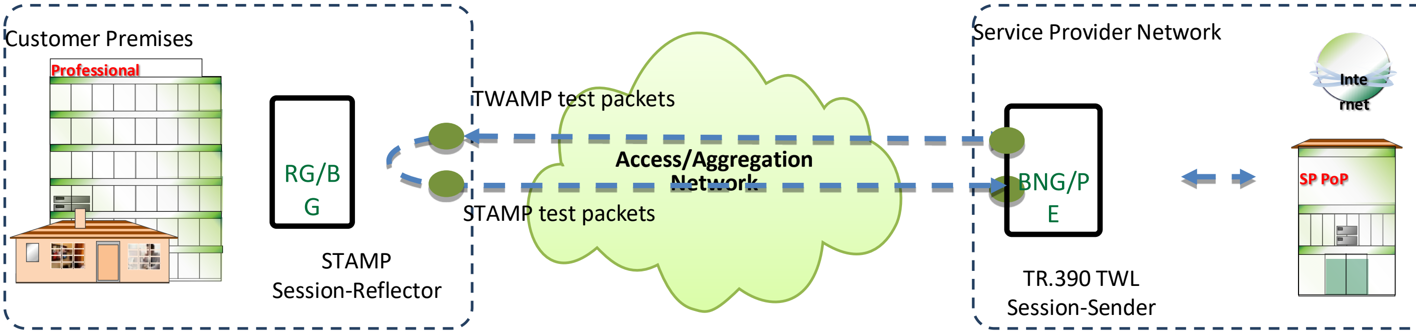

Figure 4 - Performance measurement from TR.390-based PE with STAMP-based CE

A STAMP Session-Reflector will respond to the minimal size of the TWL test packet, transmitted by the Session-Sender, with the STAMP base packet, according to Section 4.6 [draft-ietf-ippm-stamp]. TWL Session-Sender will interpret the received reflected packet as TWL's reflected packet with three octets of TWAMP padding.

Also, a TWL Session-Sender will be able to calculate packet delay because both systems, TWL and STAMP, use the same timestamp format for all timestamps collected in the course of the test.

End of Broadband Forum Technical Report TR-390.2