Technical Report

TR-390.2a1

Quality Attenuation Measurement in Broadband Access Network using STAMP

Issue: 1 Amendment 1

Issue Date: March 2024

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Technical Report has been approved by members of the Forum. This Technical Report is subject to change. This Technical Report is owned and copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be owned and/or copyrighted by Broadband Forum members.

Intellectual Property

Recipients of this Technical Report are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Technical Report, or use of any software code normatively referenced in this Technical Report, and to provide supporting documentation.

Terms of Use

1. License

Broadband Forum hereby grants you the right, without charge, on a perpetual, non-exclusive and worldwide basis, to utilize the Technical Report for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, products complying with the Technical Report, in all cases subject to the conditions set forth in this notice and any relevant patent and other intellectual property rights of third parties (which may include members of Broadband Forum). This license grant does not include the right to sublicense, modify or create derivative works based upon the Technical Report except to the extent this Technical Report includes text implementable in computer code, in which case your right under this License to create and modify derivative works is limited to modifying and creating derivative works of such code. For the avoidance of doubt, except as qualified by the preceding sentence, products implementing this Technical Report are not deemed to be derivative works of the Technical Report.

2. NO WARRANTIES

THIS TECHNICAL REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT AND ANY IMPLIED WARRANTIES ARE EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE USER'S OR IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY USER, IMPLEMENTER, OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT, INCLUDING BUT NOT LIMITED TO, ANY CONSEQUENTIAL, SPECIAL, PUNITIVE, INCIDENTAL, AND INDIRECT DAMAGES.

3. THIRD PARTY RIGHTS

Without limiting the generality of Section 2 above, BROADBAND FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE TECHNICAL REPORT IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH RIGHTS ARE DESCRIBED ON THE TECHNICAL REPORT, BROADBAND FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

All copies of this Technical Report (or any portion hereof) must include the notices, legends, and other provisions set forth on this page.

Issue History

Issue Number	Issue Date	Issue Editor	Changes
1 a1	March 2024	Gregory Mirsky, Ericsson	Original

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

Editor: Gregory Mirsky, Ericsson

Work Area Director(s): David Sinicrope, Ericsson
Jonathan Newton, Vodafone

Project Stream Leader(s): Gregory Mirsky, Ericsson

Table of Contents

Table of Figures

Table of Tables

Executive Summary

In today's demanding broadband service delivery environment, the industry can benefit from 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 extends use cases discussed in TR-390.2 and defines the capabilities required in the User Equipment, 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 to differentiate their services from the competition. One of the opportunities is optimizing users' quality of experience based on the quality attenuation measurements of the access network, which provides service to residential and business subscribers. TR-452.1 [2] has described the architecture and requirements for the measurement of Quality Attenuation. TR-452.2 [3] provided further detailed information on using active performance measurement protocols to measure quality attenuation.

TR-304 [4] specifies a performance measurement framework for measuring performance in Multi-Service Broadband Networks (MSBN). TR-143 defines an Active Monitoring test suite that can be used for network performance measurement from the RG to a Network Test Server. TR-390.2 [1] 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 a subset of functionalities of Simple Two-way Active Measurement Protocol (STAMP) [7]. This Technical Report extends the model to perform performance measurement described in TR-390.2 as it applies STAMP and its extensions [8] to measure Quality Attenuation accurately.

Therefore, the main goals for this document are to:

- Describe how to use STAMP in measuring Quality Attenuation. The resulting metrics include but are not limited to latency, jitter, and packet loss.
- Give service providers a standards-based tool to gain insight into 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 Quality Attenuation measurement tests in the on-demand and proactive testing, including continuous monitoring. Service providers may use one, the other or both modes, depending on their business objectives and dimensioning criteria.

TR-390.2a1 covers the measurement of the Quality Attenuation in the access network for the broad spectrum of BBF defined MSBN architectures, including but not limited to:

- IPoE and PPPoX models (TR-101 [10] / TR-178 [11])
- Wholesaling scenarios (L2, L3, LAC/LNS)
- WLAN access networks (TR-203 [12] / TR-291 [13] / TR-321 [14])
- Network Enhanced Residential Gateway (TR-317 [15])
- Virtual Business Gateway (TR-328 [16])

The performance measurement toolkit defined in TR-390.2a1 can be re-used for network-wide performance measurement as described in TR-304 [4], that is performance measurement between any point in the network, but no specific nodal requirements for this are covered in TR-390.2a1.

The scope of this Technical Report covers:

- Definition of in-service Quality Attenuation measurement tests
- Support for multiple CoS, for per traffic class performance measurements
- Resulting requirements for systems that participate in the Quality Attenuation measurement test
- Aspects of proactive Quality Attenuation monitoring in MSBN

The following are outside of the scope of TR-390.2a1:

- 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 [18] 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 [5] and RFC 8174 [6].

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-390.2	Performance Measurement from Customer Equipment to IP Edge using STAMP	BBF	2020
[2] TR-452.1	Quality Attenuation Architecture and Requirements	BBF	2020
[3] TR-452.2	Quality Attenuation Measurements Using Active Measurement Protocols	BBF	2022
[4] TR-304	Broadband Access Service Attributes and Performance Metrics	BBF	2015

[5]	RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997
[6]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words	IETF	2017
[7]	RFC 8762	Simple Two-way Active Measurement Protocol	IETF	March 2020
[8]	RFC 8972	Simple Two-way Active Measurement Protocol Optional Extensions	IETF	January 2021
[9]	STAMP TLV Types registry	STAMP Timestamping Methods sub-registry	IANA	2021
[10]	TR-101 Issue 2	Migration to Ethernet-Based Broadband Aggregation	BBF	2011
[11]	TR-178	Multi-service Broadband Network Architecture and Nodal Requirements	BBF	2014
[12]	TR-203	Interworking between Next Generation Fixed and 3GPP Wireless Networks	BBF	2012
[13]	TR-291	Nodal Requirements for Interworking between Next Generation Fixed and 3GPP Wireless Access	BBF	2014
[14]	TR-321	Public Wi-Fi Access in Multi-service Broadband Networks	BBF	2015
[15]	TR-317	Network Enhanced Residential Gateway	BBF	2016
[16]	TR-328	Virtual Business Gateway	BBF	2017
[17]	Y.1564	Ethernet service activation test methodology	ITU-T	2016
[18]	TR-069 Issue 1 Amendment 2	CPE WAN Management Protocol v1.1	BBF	2007
[19]	TR-242	IPv6 Transition Mechanisms for Broadband Networks	BBF	2015
[20]	TR-348	Hybrid Access Broadband Network Architecture	BBF	2016
[21]	TR-369a1	TR-369 Amendment 1: User Service Platform (USP)	BBF	October 2019
[22]	TR-181 Issue 2 Amendment 12	Device Data Model for TR-069	BBF	February 2010
[23]	RFC 8545	Well-Known Port Assignments for the One-Way Active Measurement Protocol (OWAMP) and the Two-Way Active Measurement Protocol (TWAMP)	IETF	March 2019

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-390.2a1, the following are considered to be IP Edge: MS-BNG, PE, vG, vBG, LNS, TWAG.

CE	Customer Equipment. In the context of TR-390.2a1, 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 []. 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:

TR	Technical Report
WA	Work Area

3 Technical Report Impact

3.1 Energy Efficiency

WT-390.2a1 has no significant impact on energy efficiency. Although performance measurement mechanisms defined in WT-390.2a1 will make use of additional computational cycles in the User Equipment, Customer Equipment and IP Edge nodes, these will cause a minimal contribution to the overall energy consumption.

3.2 Security

Enabling a STAMP Session-Reflector function at the UE, CE, and IP Edge 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 using spoofed STAMP test packets.

• 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 timestamping. Instead, TR-390.2a1 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 or IPv6 link-local addressing for STAMP tests, which makes a UE or CE unreachable for STAMP outside of the domain.
- Setting a filtering rule at the IP Edge preventing any STAMP test traffic towards the UE or CE other than that originated by the IP Edge.
- A Session-Reflector implementation MUST provide control to limit the rate of STAMP test packets punted from the data to control plane.
- A Session-Reflector implementation MUST provide control to limit the rate of STAMP test packets reflected to the Session-Sender.

3.3 Privacy

TR-390.2a1 has no impact on privacy.

4 Introduction

4.1 Simple Two-way Active Measurement Protocol (STAMP)

The use of STAMP, as defined in **[7]** and **[8]**, for the performance measurement from IP Edge to Customer Equipment is described in **[1]**. In the use case for measuring performance in the access network, a CE device (RG/BG) is required to implement, at the minimum, the functionality of a STAMP Session-Reflector while the IP Edge system performs the STAMP Session-Sender functions. That case of STAMP deployment can be used to measure Quality Attenuation. Additionally, using the existing STAMP support by a CE, the Quality Attenuation measurement may be performed on the home network if a User Equipment (UE), a handset (Figure 1), or an access device (Figure 2) supports the STAMP Session-Sender functions.

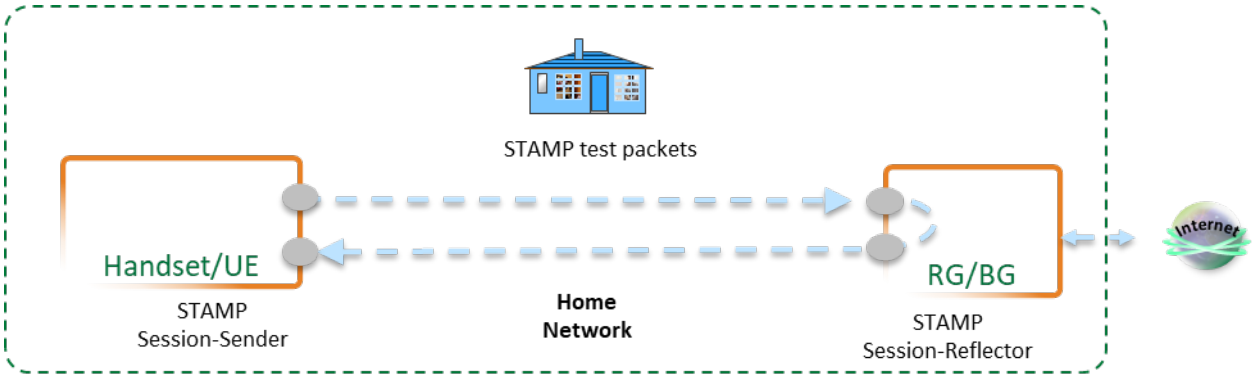

Figure 1 QED measurement on a home network between UE and CE in the upload direction

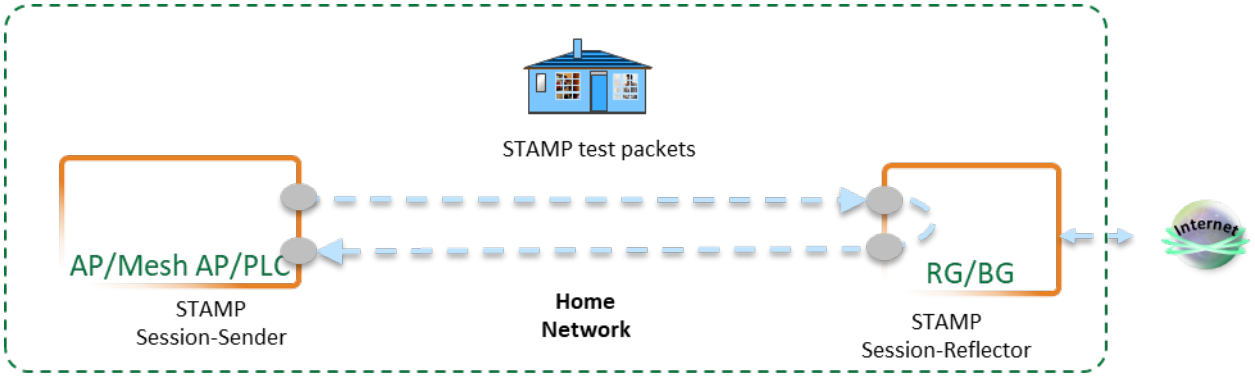

Figure 2 QED measurement on a home network between an access device and CE in the upload direction

In a home network, it is often the case that the available upload and download bandwidth are maintained at different values. As a result, it might be beneficial to a customer and the operator if the performance of download and upload directions can be measured separately in a test session by a system acting as STAMP Session-Sender. Figure 1 and Figure 2 depict the measurement of the upload direction in a home network. To test the download direction, CE system needs to support the STAMP Session-Sender functions and

UE/handset or access point – STAMP Session-Reflector functions, as displayed in Figure 3 and Figure 4, respectively.

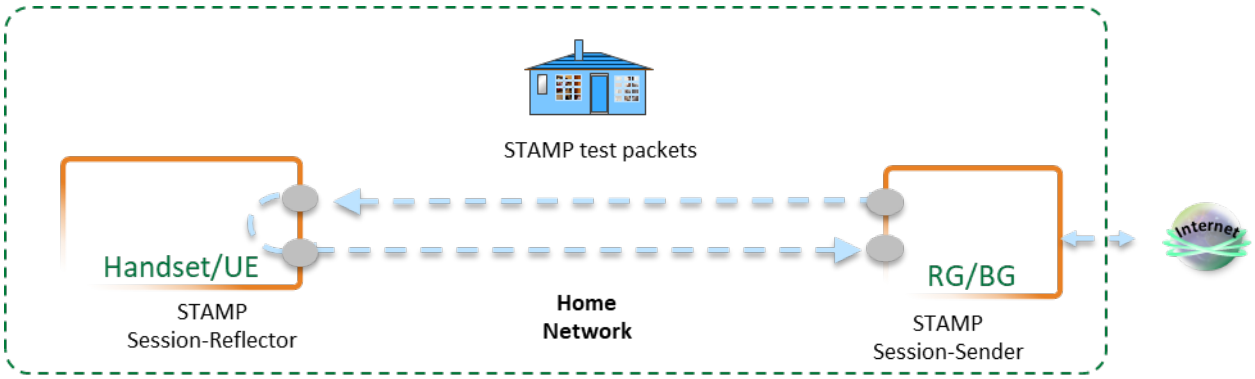

Figure 3 QED measurement on a home network between UE and CE in the download direction

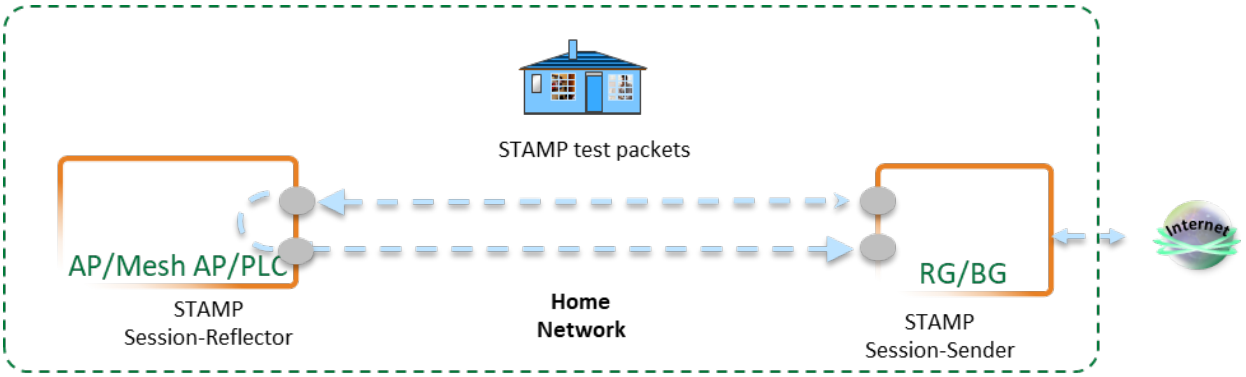

Figure 4 QED measurement on a home network between an access device and CE in the download direction

In addition to scenarios presented in Figure 3 and Figure 4, it is beneficial supporting the STAMP Session-Reflector functionality in the IP Edge device. Then a STAMP test sessions can be performed as presented in Figure 5 and Figure 6

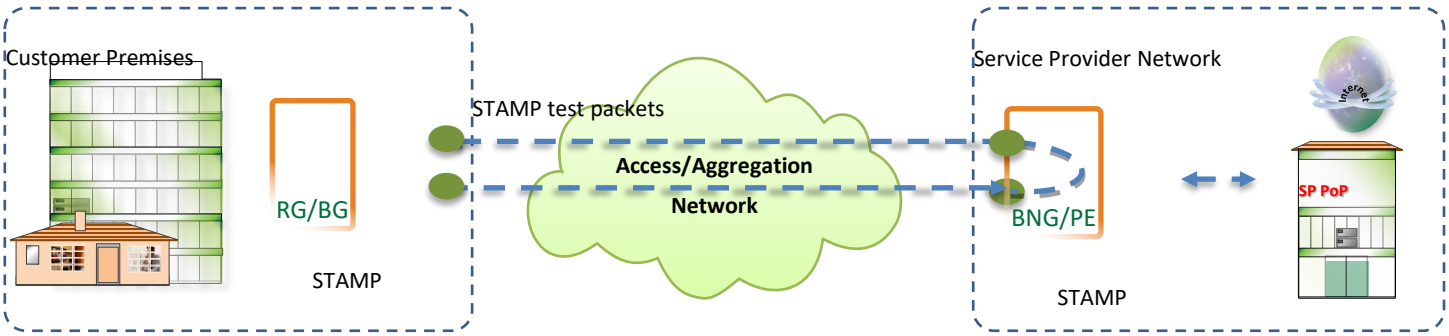

Figure 5 RG/BG to BNG/PE performance measurement with STAMP

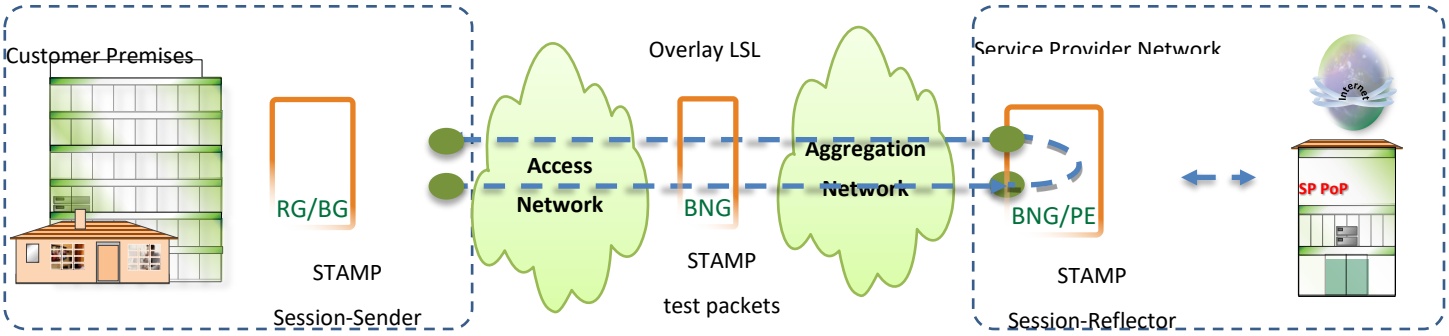

Figure 6 STAMP-based performance measurement in the context of TR-317/TR-328

As the result of supporting the STAMP Session-Reflector functionality in an IP Edge device, performance measurements using STAMP can be operated over the additional, to listed in Table 1 of TR-390.2 [1], spectrum of BBF defined MSBN architectural options:

BBF TR	STAMP Session-Sender	STAMP Session-Reflector
TR-101	RG	MS-BNG
TR-101 (LAC/LNS)	RG	LNS
TR-178 / TR-345 [11]	RG / BG	Edge BNG / Service BNG
TR-242 [19] (DS-Lite)	RG	AFTR
TR-242 (6rd)	RG	6rd BR
TR-291	RG / AP	TWAG
TR-291 (S2 extension)	RG / AP	PGW
TR-317	BRG	vG
TR-321	RG / AP	BNG
TR-321 (3GPP routed)	RG / AP	PGW
TR-328	pBG	vBG
TR-348 [20]	HCPE	HAG

Table 1 Additional STAMP test endpoints in BBF architectures

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) and the IP Edge node (e.g., BNG, PE, etc.) performs both STAMP Session-Reflector and STAMP Session-Sender functions.

Using STAMP as a performance measurement tool, in the context of TR-390.2, requires that the STAMP Session-Reflector has an IP address that is reachable from the STAMP Session-Sender.

When the CE acts as STAMP Session-Reflector, this functionality must be either bound to the WAN interface or a loopback interface and reachable by the STAMP Session-Sender platform.

When the IP Edge acts as STAMP Session-Reflector, this functionality must be [Editor's note: needs further clarification].

Instead, TR-390.2 makes use of prefix lists and TTL-based filtering for the protection of the STAMP Session-Reflector. It does not allow the STAMP Session-Sender to accept and process any STAMP test packets from non-active STAMP test sessions.

Activation and configuration of STAMP in the MSBN are simplified as much as possible by making use of default parameters as listed in Section 6 and by having the STAMP Session-Reflector function enabled by default on the CE. Doing this limits the activation workflow for a test session 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 [18] or TR-369 (USP) [21]. Data model for TR-069 management of the STAMP client (Session-Reflector) in the CE TR-181 Issue 2 Amendment 12 [22] or vendor-specific extensions can be used.

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

6 Nodal Requirements

6.1 CE Requirements

[R-1] The CE MUST support the STAMP Stateful mode of a Session-Reflector defined in Section 4 [7].
[R-2] The CE MUST support the STAMP Test Session Identifier as defined in Section 3 [8].
[R-3] The CE MUST support STAMP Session-Sender in the Unauthenticated mode as defined in Section 4.1.1 [7].
[R-4] The CE MUST support STAMP Session-Sender in the Authenticated mode as defined in Section 4.1.2 [7].
[R-5] The CE MUST transmit base STAMP test packets [7] as its default behavior.
[R-6] The CE MUST support on-demand STAMP test sessions.
[R-7] The CE MUST support continuous STAMP test sessions.
[R-8] The CE MUST support at least eight concurrent STAMP test sessions for a given endpoint.
[R-9] The CE MUST support configurable values per STAMP test session for the parameters listed in Table 5 of TR-390.2 [1].
[R-10] The CE MUST NOT accept or process STAMP test packets that are not associated with active test sessions.

[R-11] The CE SHOULD support reporting of discarded STAMP test packets for invalid sessions.
[R-12] The CE SHOULD support reporting of discarded STAMP test packets due to fragmentation.
[R-13] The CE MUST support collection and reporting of performance metric statistics per test session according to TR-069 [18] or TR-369 (USP) [21].
[R-14] The CE MUST support the Extra Padding TLV as defined in Section 4.1 [8].
[R-15] If the CE supports the Authenticated mode, it MUST support the HMAC TLV as defined in Section 4.8 [8].
[R-16] The CE MUST support Timestamp Information TLV as defined in Section 4.3 [8].

Using the Follow-up Telemetry TLV is intended to improve the packet delay calculation accuracy by communicating Session-Reflector timestamp value at the transmission of an earlier reflected timestamp packet.

[R-17] The CE SHOULD support the STAMP Follow-up Telemetry TLV as Session-Reflector as defined in Section 4.7 [8].
[R-18] If CE supports the STAMP Follow-up Telemetry TLV, the CE MUST support the values defined in the STAMP Timestamping Methods sub-registry [9] to characterize the method by which the value in the Follow-Up Timestamp field is obtained.

6.2 IP Edge Requirements

[R-19] The IP Edge MUST support STAMP Session-Reflector in the Unauthenticated mode as defined in Section 4.2.1 [7].
[R-20] The IP Edge support STAMP Session-Reflector in the Authenticated mode as defined in Section 4.2.2 [7].
[R-21] When STAMP is enabled, the IP Edge MUST use TWAMP-Test Receiver Port [23], as the default STAMP Session-Reflector receive port.
[R-22] The IP Edge MUST support symmetrical packet size, i.e., STAMP Session-Reflector transmits reflected packets of the same packet size as the received packets.
[R-23] The IP Edge MUST support access-list filtering of IP ranges for the source address of STAMP test packets it receives. According to the base STAMP specification [7], a Session-Sender and a Session-Reflector by default use symmetrical test packets.
[R-24] The IP Edge SHOULD support access-list filtering of source UDP port ranges for STAMP test packets it receives.
[R-25] The IP Edge MUST support at least eight access-lists to comply with [R-35] in Section IP Edge Requirements.
[R-26] The IP Edge MUST support configurable STAMP values for the parameters listed in Table 4 of TR-390.2 [1].
[R-27] The IP Edge SHOULD support hardware-based time-stamping of STAMP test packets.
[R-28] The IP Edge MUST support the use of STAMP Test Session Identifier as defined in Section 3 [8].
[R-29] The IP Edge MUST support the Extra Padding TLV as defined in Section 4.1 [8].
[R-30] If the IP Edge supports the Authenticated mode [7], it MUST support the HMAC TLV as defined in Section 4.8 [8].
[R-31] The IP Edge MUST support Timestamp Information TLV as defined in Section 4.3 [8].
[R-32] The IP Edge MUST support STAMP the Follow-up Telemetry TLV as Session-Reflector as defined in Section 4.7 [8].
[R-33] The IP Edge SHOULD report the original and recalculated, using the Follow-up Telemetry TLV, values of packet delay.

End of Broadband Forum Technical Report TR-390.2a1