TECHNICAL REPORT

TR-390

Performance Measurement from IP Edge to Customer Equipment using TWAMP Light

Issue: 1
Issue Date: May 2017

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 copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be 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 IS EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT.

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

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	8 May 2017	9 June 2017	Guiu Fabregas Nokia	Original

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

Editor	Guiu Fabregas	Nokia	guiu.fabregas@nokia.com
Work Area Director(s)	David Allan	Ericsson	david.i.allan@ericsson.com
	David Thorne	BT	david.j.thorne@bt.com

TABLE OF CONTENTS

List of Figures

List of Tables

Executive Summary

In today's demanding broadband service delivery environment, the industry is lacking the ability to use standardized mechanisms for broadband access network service monitoring and performance measurement 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 TWAMP Light (TWL) performance measurement, including architectural and nodal requirements.

1 Purpose and Scope

1.1 Purpose

Reliable and performant 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 currently lack the ability to use standardized mechanisms for performance measurement of the access network, which provides service to residential and business subscribers.

TR-304 [10] 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 builds on these TRs and defines architectural and nodal requirements to enable Service Providers (SPs) to monitor the performance of the access network, between the IP Edge (MS-BNG, PE, etc.) and the Customer Equipment (CE) using TWAMP Light (TWL) performance measurement.

Therefore, the main goals for this document are to:

- Describe how to use TWL performance measurement in the MSBN. Resulting metrics include latency, jitter and packet loss
- Give service providers a tool to gain insight on how their access network is performing
- Facilitate the use of already specified IP performance measurement tools, not currently deployed in the MSBN

1.2 Scope

This Technical Report describes in-service performance measurement tests. The focus of TR-390 is on-demand performance measurement using TWL, but the same test tools can be used for 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. However, scaling considerations of continuous proactive testing are out of scope of TR-390.

TR-390 covers access network performance measurement for the broad spectrum of BBF defined MSBN architectures, including but not limited to:

- IPoE and PPPoX models (TR-101 [2] / TR-178 [5] / TR-146 [4])
- Wholesaling scenarios (L2, L3, LAC/LNS)
- WLAN access networks (TR-203 [7] / TR-291 [9]/ TR-321 [12])
- Network Enhanced Residential Gateway (TR-317 [11])
- Virtual Business Gateway (WT-328 [13])

Note that for all these use cases, the prerequisite is to have IP connectivity between the two end points for performance monitoring. As such, in L2 wholesaling scenario, TR-390 capabilities apply only to the retailer.

The performance measurement toolkit defined in TR-390, using TWL, can be re-used for network-wide performance measurement as described in TR-304, that is performance measurement between any point in the network to the CE, but no specific nodal requirements for this are covered in TR-390.

The scope of this Technical Report covers:

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

The following are outside of the scope of TR-390:

- Other test endpoint combinations, e.g. CE to CE, network-wide performance measurement
- 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 [19])
- Usage and processing of collected performance measurement data
- 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 [16].

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 5	*CPE WAN Management Protocol*	BBF	2013
[2]	TR-101 Issue 2	*Migration to Ethernet-Based Broadband Aggregation*	BBF	2011

[3]	TR-143	*Enabling Network Throughput Performance Tests and Statistical Monitoring*	BBF	2008
[4]	TR-146	*Subscriber Sessions*	BBF	2013
[5]	TR-178	*Multi-service Broadband Network Architecture and Nodal Requirements*	BBF	2014
[6]	TR-181 Issue 2 Amendment 11	*Device data Model for TR-069*	BBF	2016
[7]	TR-203	*Interworking between Next Generation Fixed and 3GPP Wireless Networks*	BBF	2012
[8]	TR-242 Issue 2	*IPv6 Transition Mechanisms for Broadband Networks*	BBF	2015
[9]	TR-291	*Nodal Requirements for Interworking between Next Generation Fixed and 3GPP Wireless*	BBF	2014
[10]	TR-304	*Broadband Access Service Attributes and Performance Metrics*	BBF	2015
[11]	TR-317	*Network Enhanced Residential Gateway*	BBF	2016
[12]	TR-321	*Public Wi-Fi Access in Multi-service Broadband Networks*	BBF	2015
[13]	WT-328	*Virtual Business Gateway*	BBF	2017
[14]	TR-345	*Broadband Network Gateway and Network Function Virtualization*	BBF	2016
[15]	TR-348	*Hybrid Access Broadband Network Architecture*	BBF	2016
[16]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[17]	RFC 4656	*A One-way Active Measurement Protocol (OWAMP)*	IETF	2006
[18]	RFC 5357	*A Two-Way Active Measurement Protocol (TWAMP)*	IETF	2008
[19]	Y.1564	*Ethernet service activation test methodology*	ITU-T	2016

2.3 Definitions

The following terminology is used throughout this Technical Report.

IP Edge	This Technical Report expands the definition of IP Edge in TR-146 to broaden its scope. In the context of TR-390, IP Edge is a generic term to refer to the logical function that is the first IP hop from the point of view of the customer traffic. As such, the following are considered to be IP Edge functions: MS-BNG, PE, vG, vBG, LNS, TWAG, HAG.
CE	Customer Equipment. In the context of TR-390, CE is a generic term to refer to network equipment placed in the customer premises and includes the following: RG, BG, BRG, pBG, AP, HCPE.
TWL Session-Sender	TWAMP Light Session-Sender. Logical function that transmits test packets to one or more TWL Session-Reflectors, and determines performance metrics from the reflected test packets.
TWL Session-Reflector	TWAMP Light Session-Reflector. Logical function that acts as a test point in the network, following the Session-Reflector behavior of TWAMP, as per Section 4.2/RFC 5357. The TWL Session-Reflector does not need to have knowledge of the session state.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

3GPP	3rd Generation Partnership Project
AFTR	DS-Lite Address Family Transition Router
AP	Wi-Fi Access Point
BG	Business Gateway
BNG	Broadband Network Gateway
BR	6rd Border Relay
BRG	Bridged Residential Gateway
CoS	Class of Service
CPE	Customer Premises Equipment
CPU	Computer Processing Unit
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service

DSCP	Differentiated Services Code Point
GPS	Global Positioning System
HAG	Hybrid Access Gateway
HCPE	Hybrid CPE
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPoE	IP over Ethernet
LAC	L2TP Access Concentrator
LAN	Local Area Network
LNS	L2TP Network Server
LSL	Logical Subscriber Link
MS-BNG	Multi Service BNG
MSBN	Multi-Service Broadband Network
NERG	Network Enhanced Residential Gateway
NTP	Network Time Protocol
pBG	Physical Business Gateway
PD	Prefix Delegation
PE	Provider Edge Router
PGW	Packet Data Network Gateway
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PTP	Precision Time Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RG	Residential Gateway
SLAAC	Stateless Address AutoConfiguration
TR	Technical Report
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
WA	Work Area
WAN	Wide Area Network
WLAN	Wireless LAN

3 Technical Report Impact

3.1 Energy Efficiency

TR-390 has no significant impact on energy efficiency. Although performance measurement mechanisms defined in TR-390 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 TWAMP Light Session-Reflector function at the CE opens an additional potential door for attackers to use, as the port used for TWL testing must be opened in the CE firewall. Potential security risks include:

- Denial-of-service (DoS) attacks, especially in the case where TWL timestamping is done in software
- Man-in-the-middle attacks, where the attacker may modify the TWL test packets and alter the measurement results

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

While TWAMP supports options for authentication and privacy (encryption), this Technical Report does not rely on these mechanisms, as they increase the implementation complexity and may cause inaccuracies in time-stamping. Instead, TR-390 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 TWL tests, which makes the CPE unreachable for TWL outside of the domain
- Setting a filtering rule at the IP Edge preventing any TWL test traffic towards the CE other than that originated by the IP Edge

3.3 Privacy

This Technical Report does not have an impact on subscriber privacy.

4 Introduction

In typical Service Provider networks, the access and aggregation network has a high impact on service quality. The reasons are typically specific to the access technology and include limited QoS capabilities and a relatively high aggregation factor, so-called 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 delay, delay variation (jitter) and frame loss ratio.

4.1 Performance measurement using TWAMP Light

TWAMP, defined in RFC 5357, is a well-defined protocol to measure network performance. TWAMP Light (TWL) is described in Appendix I of RFC 5357 and provides a light weight architecture, mitigating the need for TWAMP-Control protocol, where the responder only implements the TWAMP Session-Reflector function reflecting incoming TWAMP test packets back to the Session-Sender.

Two functions are required in a TWL architecture:

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

By removing the control component of the architecture, TWL requires less resources (e.g. CPU, memory), making it more effective to run at scale in the IP Edge rather than requiring external dedicated probing devices, while still supporting the ability to derive delay, delay variation and loss performance metrics.

The CE implements the TWL Session-Reflector function while the IP Edge performs the TWL Session-Sender functions. The TWL test session is run between the IP Edge and the CE as shown in Figure 1:

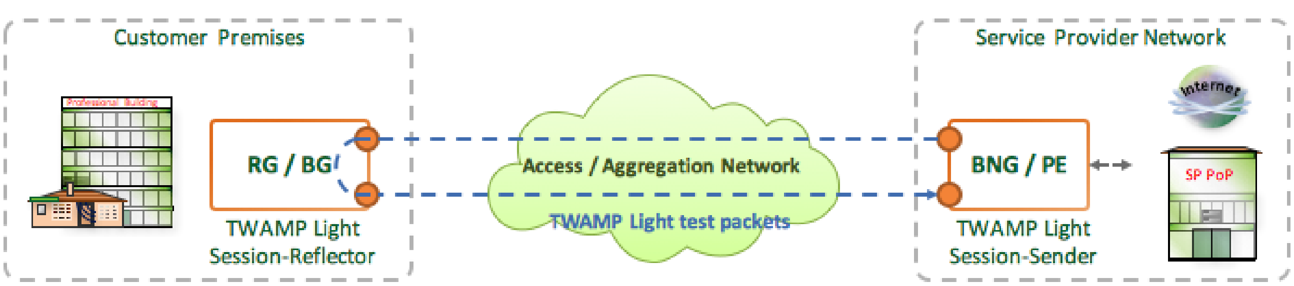

Figure 1 – BNG/PE to RG/BG performance measurement with TWAMP Light

The figure below 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 WT-328 (VBG).

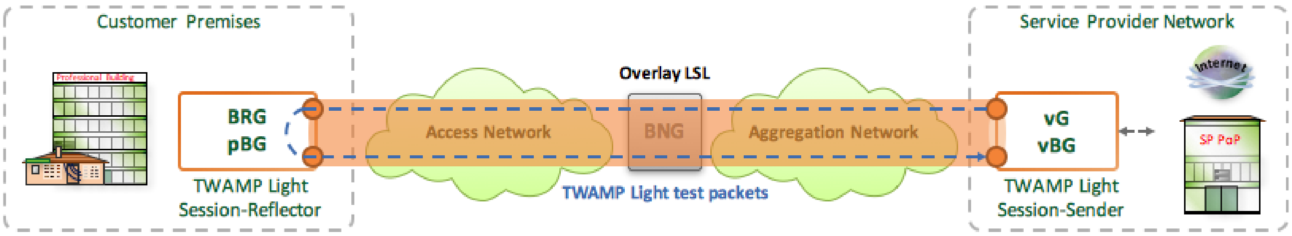

Figure 2 – TWAMP Light performance measurement in the context of TR-317/WT-328

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

BBF TR	TWL Session-Sender	TWL Session-Reflector
TR-101	MS-BNG	RG
TR-101 (LAC/LNS)	LNS	RG
TR-178 / TR-345 [14]	Edge BNG / Service BNG	RG / BG
TR-242 [8] (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
WT-328	vBG	pBG
TR-348 [15]	HAG	HCPE

Table 1 TWL test endpoints in BBF architectures

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

- In L2 wholesaling scenario, TR-390 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, TWL 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, TWL 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 TWL 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 scope of TR-390.

5 Solution description

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

Using TWL as a performance measurement tool requires that the TWL Session-Reflector, the CE in the context of TR-390, has an IP address that is reachable from the TWL Session-Sender. This IP address must be reachable by the IP Edge platform and is either bound to the WAN interface or to a loopback interface at the CE.

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

CE type	**IPv4 address in use at CPE for TWL**
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 TWL

In the IPv6 case, different addressing models may be used. TR-390 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 TWL**
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 TWL 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 TWL 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 TWL

While TWAMP could make use of any UDP port, this Technical Report proposes the use of a well-known port (862), to simplify the provisioning and testing work flows.

Although it is possible to run TWL in multiple modes, including those allowing for authentication and encryption of test packets, TR-390 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 makes use of prefix-lists and TTL-based filtering for protection of the TWL Session-Reflector at the CE, and not allowing the IP Edge to accept and process any TWL test packets from any non-active TWL test sessions. TTL filtering at the CE is set to a single hop to allow testing only from the IP Edge.

TWL performance measurement can be run on-demand or in continuous mode. Running TWL on-demand allows its use for reactive testing and troubleshooting whereas continuous measurement allows proactive detection of performance issues on a 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 normally be transported over the access / aggregation network, TR-390 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 TWL Session-Sender and processed appropriately by the TWL Session-Reflector. The 4-tuple Source IP, Destination IP, Source UDP, and Destination UDP provide a unique index for each test session. A different UDP source port is used for each test session.

Activation and configuration of TWL 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 TWL Session-Reflector function enabled by default on the CE. By doing this, the activation work flow 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 TWL attributes in the CE could also be supported by TR-390, e.g. by means of TR-069. At the time of this writing, work is ongoing on a TR-181i2 [6] data model for TR-069 management of the TWL 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 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 TWL 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 proposes an alternative that consists in modifying the last two octets of the TWAMP 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 mandates that both the Session-Sender and Session-Reflector must send TWL packets with an additional 2 octets-long Payload (padding) field, beyond the minimum requirement for symmetrical packet handling (27 bytes).

Even though TWL test packets could be reassembled at the receiving end if fragmentation has occurred along the path, this would have significant impact on the accuracy of the measurements. The proper operation of TR-390 depends on the TWL test packets not having been fragmented.

For performance measurement to be meaningful, statistics need to be collected and processed to gain insight on how the network is performing. TR-390 mandates the collection of latency, jitter, and packet loss statistics per test session. More complex metrics such as minimum, maximum, average values over a period of time, statistics for inbound, outbound and round-trip directions, etc. 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 one-way metrics.

6 Nodal requirements

6.1 CE Requirements

[R-1] The CE MUST support TWL Session-Reflector in unauthenticated mode.
[R-2] The CE MUST have the TWL Session-Reflector enabled by default, listening on UDP port 862.
[R-3] The CE MUST support TWL with IPv4 encapsulation, supporting reflection in the addresses listed in Table 2.
[R-4] The CE MUST support TWL with IPv6 encapsulation, supporting reflection at least in the addresses listed in Table 3.
[R-5] The CE MUST reflect back the received CoS parameters of the incoming TWL packet.
[R-6] The CE MUST send TWL response packets with the same packet size as the request packets received, by adjusting the padding.
[R-7] The CE MUST discard TWL test packets with a TTL greater than 1.
[R-8] The CE MUST support access-list filtering of IP ranges for the source address of TWL test packets it receives.
[R-9] The CE SHOULD support access-list filtering of source UDP port ranges for TWL test packets it receives.
[R-10] The CE access-list SHOULD be disabled (i.e. allow all, 0.0.0.0/0) by default.
[R-11] The CE MUST support configurable TWL values for the parameters listed in Table 4.
[R-12] The CE MUST silently discard any fragmented test packets received.
[R-13] The CE MUST implement the Error Estimate field properly as described in Section 4.1.2/RFC 4656 [17], to allow the TWL Session-Sender to understand the quality of the timestamps provided.
[R-14] The CE SHOULD support hardware based timestamping of TWAMP test packets.
[R-15] The CE MUST prevent high CPU load or other high priority tasks from having an adverse impact on the quality of any software generated timestamps.
[R-16] The CE SHOULD support TWL management using TR-069.

Where one-way metrics are required, the following additional requirement applies:

[R-17] The CE MUST support external clocking (e.g. NTP, PTP, GPS, …).

Attribute	Default	Description
Administrative State	Enabled (IPv4+IPv6)	Controls the administrative state of the TWL Session-Reflector
TWL IP Address	IPv4: As per Table 2 IPv6: As per Table 3	IP address that the TWL Session-Reflector listens on
TWL UDP Port	862	UDP Port to listen for Test Packets
TTL Security	Enabled (1 hop)	Check against IP TTL
IP Security	Disabled (0.0.0.0/0)	Check against IP Source Address
UDP Security	Disabled	Check against UDP Source Port

Table 4 CE TWL configurable parameters

6.2 IP Edge Requirements

[R-18] The IP Edge MUST support TWL Session-Sender in unauthenticated mode.
[R-19] The IP Edge MUST support TWL with IPv4 encapsulation, sending TWL test packets to the CE IPv4 addresses listed in Table 2.
[R-20] The IP Edge MUST support TWL with IPv6 encapsulation, sending TWL test packets to the CE IPv6 addresses listed in Table 3.
[R-21] The IP Edge MUST send TWL test packets with Padding not smaller than 27 octets-long.
[R-22] For IPv6, the IP Edge MUST send TWL test packets with Padding not smaller than 29 octets-long.
[R-23] The IP Edge MUST support on-demand TWL test sessions.
[R-24] The IP Edge MUST support continuous TWL test sessions.
[R-25] The IP Edge MUST support at least 8 concurrent test sessions for a given endpoint.
[R-26] The IP Edge MUST support configurable values per TWL test session for the parameters listed in Table 5.
[R-27] The IP Edge MUST only accept and process TWL test packets for active test sessions.
[R-28] The IP Edge SHOULD support logging of discarded TWL test packets for invalid sessions.
[R-29] The IP Edge MUST silently discard any fragmented test packets received.
[R-30] The IP Edge SHOULD support logging of discarded TWL test packets due to fragmentation.
[R-31] The IP Edge MUST support external clocking (NTP, PTP, GPS, …).
[R-32] The IP Edge SHOULD support hardware based timestamping of TWL test packets.
[R-33] The IP Edge MUST prevent high CPU load or other high priority tasks from having an adverse impact on the quality of any software generated timestamps.
[R-34] The IP Edge MUST collect delay, jitter and packet loss statistics per test session.

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

[R-35] The IP Edge MUST support activation of TWL test sessions during initial IP session setup, by means of a RADIUS Access-Accept message
[R-36] The IP Edge MUST support activation of TWL test sessions during the life of an IP session, by means of a RADIUS CoA message

[R-37] The IP Edge MUST support de-activation of TWL test sessions during the life of an IP session, by means of a RADIUS CoA message

Attribute	**Default**	**Description**
Source IP	-	Source IP address of the TWL test session
Dest. IP	-	Destination IP address of the TWL test session
Source UDP port	Auto-generate	Source UDP port of the TWL test session
Dest. UDP port	862	Destination UDP port of the TWL test session
Packet size	Configurable. Default padding: • IPv4: 27 bytes • IPv6: 29 bytes	Size of the TWL test packets
TTL	1	TTL field of the IP header of the test packets
DSCP	00h (Best Effort)	DSCP field of the IP header of the test packets
Interval	1 second	Amount of time between TWL test packet transmission
Test duration	5 minutes	Amount of time the TWL test will run before stopping automatically

Table 5 IP Edge TWL test session configurable parameters

End of Broadband Forum Technical Report TR-390