MEF Draft Standard
MEF 67 Draft (R1)

Service Activation Testing for IP Services Technical Specification

February 2019

This draft represents MEF work in progress and is subject to change.

This draft document represents MEF work in progress, has not achieved full MEF standardization and is subject to change. There are known unresolved issues that are likely to result in changes before this becomes a fully endorsed MEF Standard. The reader is strongly encouraged to review the Release Notes when making a decision on adoption. Additionally, because this document has not been adopted as a Final Specification in accordance with MEF's Bylaws, Members are not obligated to license patent claims that are essential to implementation of this document under MEF's Bylaws.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Disclaimer

The information in this publication is freely available for reproduction and use by any recipient and is believed to be accurate as of its publication date. Such information is subject to change without notice and MEF Forum (MEF) is not responsible for any errors. MEF does not assume responsibility to update or correct any information in this publication. No representation or warranty, expressed or implied, is made by MEF concerning the completeness, accuracy, or applicability of any information contained herein and no liability of any kind shall be assumed by MEF as a result of reliance upon such information.

The information contained herein is intended to be used without modification by the recipient or user of this document. MEF is not responsible or liable for any modifications to this document made by any other party.

The receipt or any use of this document or its contents does not in any way create, by implication or otherwise:

a) any express or implied license or right to or under any patent, copyright, trademark or trade secret rights held or claimed by any MEF member which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

b) any warranty or representation that any MEF members will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor

c) any form of relationship between any MEF member and the recipient or user of this document.

Implementation or use of specific MEF standards or recommendations and MEF specifications will be voluntary, and no Member shall be obliged to implement them by virtue of participation in MEF Forum. MEF is a non-profit international organization to enable the development and worldwide adoption of agile, assured and orchestrated network services. MEF does not, expressly or otherwise, endorse or promote any specific products or services.

© MEF Forum 2019. All Rights Reserved.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Table of Contents

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

List of Figures

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

List of Tables

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

1 List of Contributing Members

The following members of the MEF participated in the development of this document and have requested to be included in this list.

Editor Note 1: *This list will be finalized before Letter Ballot. Any member that comments in at least one CfC is eligible to be included by opting in before the Letter Ballot is initiated. Note it is the MEF member that is listed here (typically a company or organization), not their individual representatives.*

- ABC Networks
- XYZ Communications

2 Abstract

This document specifies Service Activation Testing (SAT) of IP Service Attributes as defined in MEF 61 [24]. The document addresses activation of Internet Protocol Virtual Connections (IPVCs), IPVC End Points (IPVC EPs), User Network Interfaces (UNIs), and UNI Access Links (UNI ALs). It provides both configuration and performance testing methodologies. Access to the service under test is gained via Service Activation Measurement Points (SAMPs) or Test Head Connection Points (THCPs). SAT is performed using various types of IP Test Equipment (IPTE) to generate and collect test packets. Packet Delay and Loss measurements are performed on these test packets. Additional metrics are then calculated based on these measurements. Service Activation Criteria (SAC) are agreed to by the Subscriber and Service Provider and are used to determine if a given test methodology passes or fails. Upon completion of the SAT methodologies, a Test Report can be provided to the Subscriber.

3 Release Notes

Appendix B, a comparison of Layer 1 to Layer 2 to Layer 3 throughput will be provided in a later release of this document.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

4 Terminology and Abbreviations

This section defines the terms used in this document. In many cases, the normative definitions to terms are found in other documents. In these cases, the third column is used to provide the reference that is controlling, in other MEF or external documents.

In addition, terms defined in MEF 61 [24] are included in this document by reference, and are not repeated in the table below.

Term	Definition	Reference
BFD	Bi-Directional Forwarding Detection	IETF RFC 5880 [10]
Bi-Direction Forwarding Detection	A protocol intended to detect faults in the bidirectional path between two forwarding engines, including interfaces, data link(s), and to the extent possible the forwarding engines themselves, with potentially very low latency.	IETF RFC 5880 [10]
Collector Test Function	A logical function for counting and discarding received IP Packets, which can include test packets.	MEF 48 [23]

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Term	Definition	Reference
CTF	Collector Test Function	MEF 48 [23]
DHCP	Dynamic Host Configuration Protocol	IETF RFC 2131 [5]
DSCP	Differentiated Services Code Point	IETF RFC 2474 [6]
Generator Test Function	A logical function for generating and transmitting Packets which can include test packets.	This document derived from MEF 48 [23]
GTF	Generator Test Function	MEF 48 [23]
ICMP	Internet Control Management Protocol	IETF RFC 792 [4]
IMIX	Internet Mix	IETF RFC 6985 [12]
Information Rate	The average bit rate of IP Packets passing a Measurement Point, where each IP Packet is measured from the start of the IP Version field to the end of the IP Data field.	This document
Internet Mix	A traffic pattern consisting of a preset mixture of IP-Layer IP Packet sizes used to emulate real-world traffic scenarios in a testing environment.	IETF RFC 6985 [12]
Internet Protocol Test Equipment	Test measurement equipment that generates and collects IP packets.	This document
Internet Protocol Test Equipment - Application	A type of IPTE that is an application that resides on a device in the Service Provider's network or at the Subscriber's location.	This document
Internet Protocol Test Equipment – Instrument	A type of IPTE that is a hand held or portable device that is connected directly to the UNI.	This document
Internet Protocol Test Equipment – Test Head	A type of IPTE that contains multiple interfaces, is normally rack mounted, and is normally installed at a location in the Service Provider's network. An Internet Protocol Test Equipment – Test Head (IPTE-TH) connects to the Service Under Test via a Test Head Connection Point.	This document
IPTE	Internet Protocol Test Equipment	This document
IPTE-A	IPTE-Application	This document
IPTE-I	IPTE-Instrument	This document
IPTE-TH	IPTE-Test Head	This document
IPv4	Internet Protocol version 4	IETF RFC 791[3]
IPv6	Internet Protocol version 6	IETF RFC 8200 [13]
IR	Information Rate	This document
L2	Layer 2	ISO OSI [14]

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Term	Definition	Reference
MTU	Maximum Transmission Unit	This document
Packet Loss Ratio	The ratio of total packets sent versus packets received.	This document
SAC	Service Activation Criteria	ITU-T Y.1564 [21]
SAMP	Service Activation Measurement Point	MEF 48 [23]
SAT	Service Activation Testing	MEF 48 [23]
Service Activation Criteria	A set of criteria used to ensure that a service meets its functionality and quality requirement and that the service is ready to operate when it has been deployed.	ITU-T Y.1564 [21]
Service Activation Measurement Point	A Service Activation Measurement Point is a reference point in the Service Provider's network where events can be observed and measured during the Service Activation Testing process.	This document derived from MEF 48 [23]
Service Activation Testing	The process of executing a collection of test procedures to be applied to a given traffic entity (e.g., IPVC) in order to collect behavioral information about the traffic and compare this with predefined expectations.	MEF 48 [23]
Virtual Router Identifier	The identifier of a VRRP virtual router	IETF RFC 5798 [9]
Virtual Router Redundancy Protocol	An election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.	IETF RFC 5798 [9]
VRID	Virtual Router Identifier	IETF RFC 5798 [9]
VRRP	Virtual Router Redundancy Protocol	IETF RFC 5798 [9]

Table 1 – Terminology and Abbreviations

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

5 Compliance Levels

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 (RFC 2119 **Error! Reference source not found.**, RFC 8174 **Error! Reference source not found.**) when, and only when, they appear in all capitals, as shown here. All key words must be in bold text.

Items that are **REQUIRED** (contain the words **MUST** or **MUST NOT**) are labeled as **[Rx]** for required. Items that are **RECOMMENDED** (contain the words **SHOULD** or **SHOULD NOT**) are labeled as **[Dx]** for desirable. Items that are **OPTIONAL** (contain the words **MAY** or **OPTIONAL**) are labeled as **[Ox]** for optional**.**

A paragraph preceded by **[CRa]<** specifies a conditional mandatory requirement that **MUST** be followed if the condition(s) following the “<” have been met. For example, “**[CR1]<**[D38]” indicates that Conditional Mandatory Requirement 1 must be followed if Desirable Requirement 38 has been met. A paragraph preceded by **[CDb]<** specifies a Conditional Desirable Requirement that **SHOULD** be followed if the condition(s) following the “<” have been met. A paragraph preceded by **[COc]<** specifies a Conditional Optional Requirement that **MAY** be followed if the condition(s) following the “<” have been met.

6 Numerical Prefix Conventions

Editor Note 2: This section will be deleted if no numerical prefixes are used in the document.

This document uses the prefix notation to indicate multiplier values as shown in Table 2.

Decimal		**Binary**	
Symbol	**Value**	**Symbol**	**Value**
k	10^{3}	Ki	2^{10}
M	10^{6}	Mi	2^{20}
G	10^{9}	Gi	2^{30}
T	10^{12}	Ti	2^{40}
P	10^{15}	Pi	2^{50}
E	10^{18}	Ei	2^{60}
Z	10^{21}	Zi	2^{70}
Y	10^{24}	Yi	2^{80}

Table 2 – Numerical Prefix Conventions

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

7 Introduction

As is discussed in section 2, SAT verifies both the proper configuration and performance of the service. Configuration tests are normally short in duration (<30 seconds). Performance tests are longer in duration (15 minutes, 2 hours, and 24 hours) since they are trying to identify issues with the performance of a service and these issues can be intermittent.

Configuration testing verifies IP Virtual Connection (IPVC), IPVC End Point (IPVC EP), User Network Interface (UNI), and per UNI Access Link Service Attributes are configured per the service order. The Service Attributes verified are shown in section 9.

Performance testing verifies that the Service Acceptance Criteria (SAC) are met. See section 10.2 for the description of SAC and how they differ from a Service Level Specification (SLS). The measurements that are performed include Packet Delay (PD) and Packet Loss (PL). Additional metrics that are calculated based on these measurements are Mean Packet Delay (MPD), Inter-Packet Delay Variation (IPDV), Packet Delay Range (PDR), and Packet Loss Ratio (PLR).

Test methodologies are defined for both Configuration and Performance tests. These test methodologies provide step by step processes for performing a specific test or measurement. They also include the attributes used for the SAC for each test methodology.

Before IP Services are turned over to Subscribers, Service Providers perform some type of SAT. This can range from ICMP pings to a Subscriber router to extensive connectivity and throughput testing. While IP Services are widely implemented, standard methods of performing SAT have not been clearly defined. This document builds upon the IP Service Attributes defined in MEF 61 [24] to provide methodologies for verifying the Service Attributes defined by that document. If these Service Attributes are verified, a smaller number of failures after installation is expected, resulting in fewer complaints from Subscribers.

There are two distinct ways that IP Services can be activated. The first is when a new IPVC containing several IPVC End Points (IPVC EP) is activated. In this case, SAT is performed for each IPVC EP and tests are performed between the IPVC EPs. The second case is when a new IPVC EP is added to an existing IPVC. In this case, SAT is performed on the new IPVC EP and testing between all IPVC EPs in the IPVC is not required.

Service Providers can set Subscriber expectations by using the test methodologies defined within this document. Subscribers can use the methodologies within this document to understand what tests they can request from their Service Provider.

The test methodologies defined in this document cover two general areas, configuration and performance. Configuration methodologies verify that Service Attributes are correctly configured. As discussed previously, these include IP Service Attributes which include IPVC Attributes, IPVC EP Attributes, UNI Attributes, and UNI Access Link Attributes. . These standardized Configuration test methodologies provide measurable objectives for service activation that can be used internally within a Service Provider or shared externally to Subscribers.

Performance methodologies define how the performance of new services is verified. Since intermittent issues like network congestion can impact the performance of a service, the perfor-

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

mance methodologies perform longer-term tests that measure performance over a period of time rather than just a single snapshot. As with the configuration methodologies, standardized performance methodologies allow Subscribers and Service Providers to have certain expectations of testing that is performed before the service is activated.

An IP Service might have an SLS even if that SLS provides no guarantee of service performance. These SLSs are normally stated over a period of a month. It is not realistic for service activation to measure performance for a month before turning the service over to the customer. Instead, SAT uses Service Acceptance Criteria (SAC) which are set for short time periods. SACs can be as simple as the number of packets received during a test or can be as complex as the combination of multiple performance measurements like delay and loss. The definitions of SACs allow Subscribers and Service Providers to understand the acceptance criteria for each methodology.

The remainder of the document contains the following:

- A discussion of SAT Use Cases
- A discussion of SAT Terminology
- A description of SAMPs and THCPs
- A description of where SAMPs and THCPs are located
- Tables that define what IP Service Attributes are tested
- Tables that define what IP Service Attributes are reported
- SAT Methodologies for Configuration and Performance tests
- Test Result reporting
- Requirements are specified for devices and applications including SAMPs, THCPs, and IPTEs

7.1 Terminology and SAT Use Cases

This section of the document describes terms and components used to perform SAT. Where possible these are aligned with MEF 48 [23]. SAT is performed using some type of IP Test Equipment (IPTE). Types of an IPTE are an IP Test Equipment – Instrument (IPTE-I), an IP Test Equipment – Application (IPTE-A), and an IP Test Equipment- Test Head (IPTE-TH). IPTEs contain at least one Service Activation Measurement Point (SAMP). The SAMP location depends on the type of IPTE used for testing. If the IPTE is a Test Head or an Instrument, the SAMP is located at a physical point in the network. If the IPTE is an Application, then the SAMP is located at a logical point inside a Network Element. A SAMP is either Upward facing, meaning it faces into the Service Provider’s Network, or Downward facing, meaning it faces toward an External Interface.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

An IPTE-I and an IPTE-TH always contain a Down SAMP. An IPTE-A can contain either an Up or Down SAMP.

A Test Head Connection Point (THCP) is similar to a SAMP. It is where the IPTE-TH connects to the service to be tested. A THCP exists in a device within the Service Provider's network or within an application within the Service Provider's network. A THCP is either Upward facing, meaning it faces into the Service Provider's Network, or Downward facing, meaning it faces toward an External Interface (UNI).

A SAMP contains a Generator Test Function (GTF), a Collector Test Function (CTF), or both. A GTF generates packets used for test measurements. A CTF counts and discards or counts and responds to packets used for test measurements. For Unicast services a GTF is paired with a CTF so that the packets generated by the GTF are collected by a particular CTF. The GTF and CTF might be located within the same IPTE (e.g. if test packets are looped back by a remote reflector) or might be in two different IPTEs.

A SAT Methodology is defined to verify the configuration of specific Service Attributes. Each of these Service Attributes has its own SAT Methodology. Additional SAT Methodology(s) are used to verify the performance of the service. Each SAT Methodology identifies the test name, test type, service type, test status, test objective, test procedure, variables used in the methodology, results, and remarks. The SAT Methodology used to verify the Service Attribute is shown in the tables in section 9 and the SAT Methodologies are shown in section 10.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

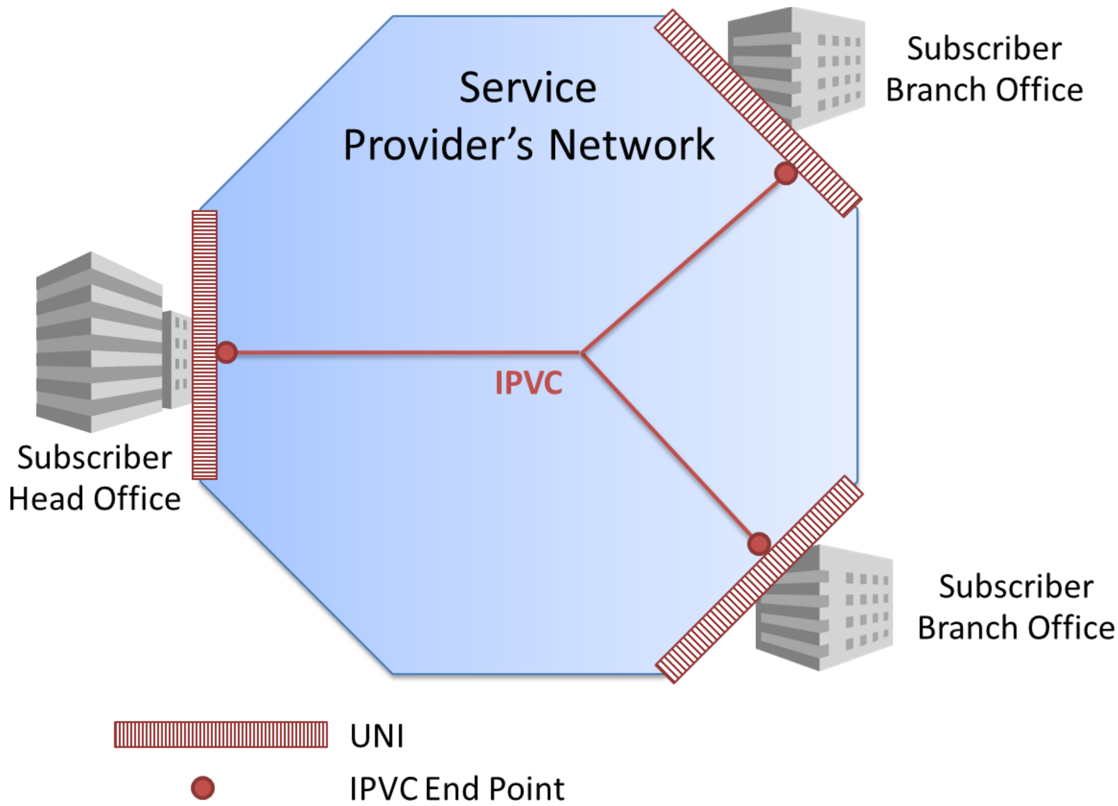

Figure 1 IPVC and UNI

Figure 1 shows an example IPVC connecting three UNIs together. As this service is activated, SAT is performed to ensure that it meets Subscriber expectations. This example will be used to discuss where IPTEs are located for SAT.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

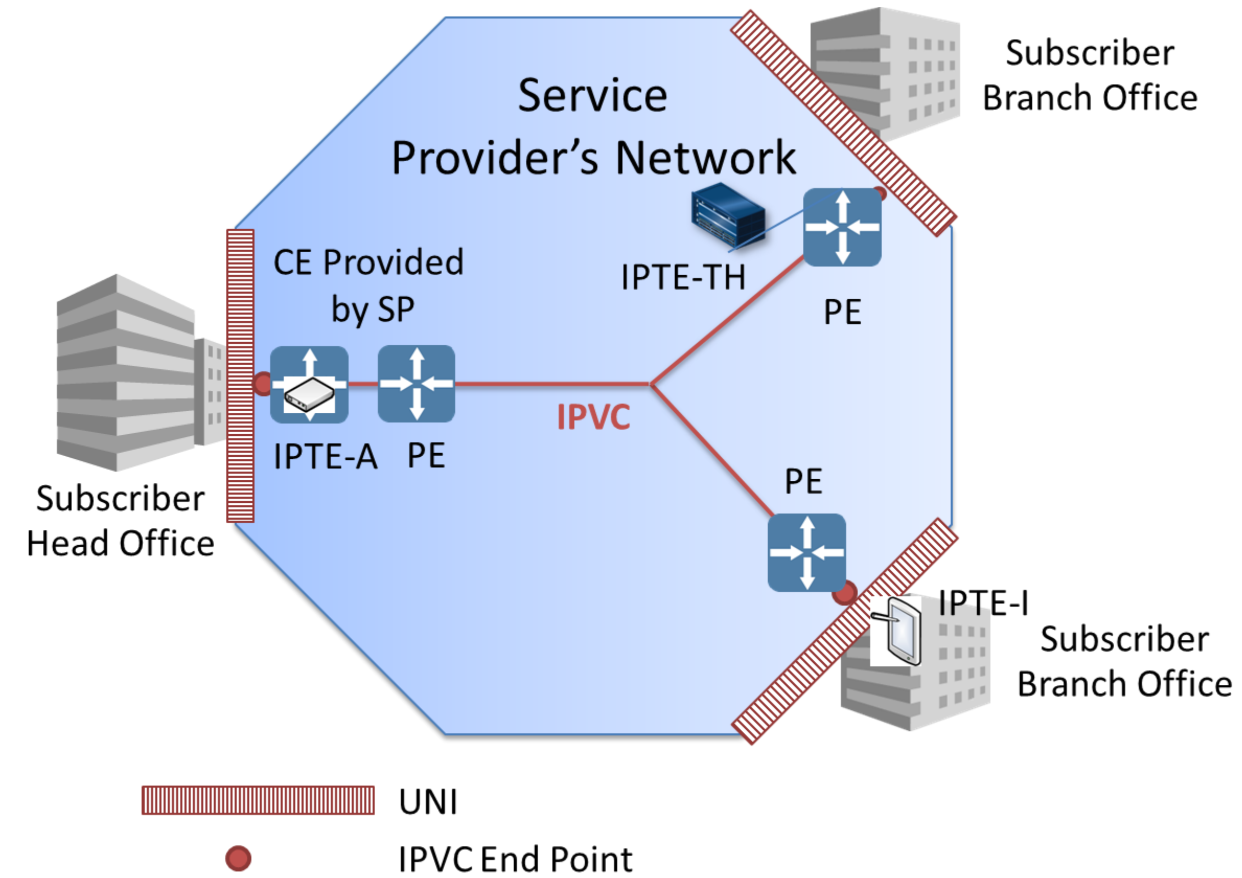

Figure 2 IPVC with IPTEs

Figure 2 shows the example IPVC with IPTEs. The IPTE-TH is connected to a Provider Edge (PE) at the UNI at the upper Subscriber Branch Office. The IPTE-I is shown on the Subscriber side of the UNI at the lower Subscriber Branch Office. It is inserted in the UNI and can perform test measurements to the IPTE-TH or IPTE-A. The IPTE-A is shown in the SP provided Customer Edge (CE) at the Subscriber Head Office. This application is able to perform test measurements to the IPTE-TH or the IPTH-I.

7.2 Service Activation Testing Use Cases

SAT Use Cases are shown in this section. They include the use of various IPTEs for verification of IPVC, IPVC EP, UNI, and UNI Access Link Service Attributes for both new IPVCs and new IPVC EPs. The following table provides a brief view of the Use Cases, the IPTEs that they cover and if they address new IPVCs, new UNIs, or new IPVC EPs.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Use Case Number	New Service Type	IPTE Type(s)	Service Attributes Tested
Use Case 1	New IPVC	IPTE-I	IPVC, IPVC EP, UNI, UNI Access Link
Use Case 2	New IPVC	IPTE-A	IPVC, IPVC EP
Use Case 3	New IPVC	IPTE-A, IPTE-TH	IPVC, IPVC EP
Use Case 4	New IPVC EP, New UNI	IPTE-I, IPTE-A/TH	IPVC, IPVC EP, UNI, UNI Access Link
Use Cases 5	New IPVC EP	IPTE-A, IPTE-A/TH	IPVC, IPVC EP
Use Case 6	New IPVC EP	IPTE-TH	IPVC, IPVC EP
Use Case 7	New UNI	IPTE-I	UNI, UNI Access Link
Use Case 8	New UNI	IPTE-A, IPTE-I	UNI, UNI Access Link
Use Case 9	New UNI	IPTE-A, IPTE-I	UNI, UNI Access Link
Use Case 10	New UNI	IPTE-TH, IPTE-I	UNI, UNI Access Link
Use Case 11	New UNI	IPTE-TH, IPTE-I	UNI, UNI Access Link

Table 3 Use Case Overview

SAT use cases are shown below. These figures and associated text describe the use cases, the type of IPTE used, the type of SAMP and/or THCP used, the type of service tested, and the service attributes tested. These use cases are also referenced in the testing methodologies section.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

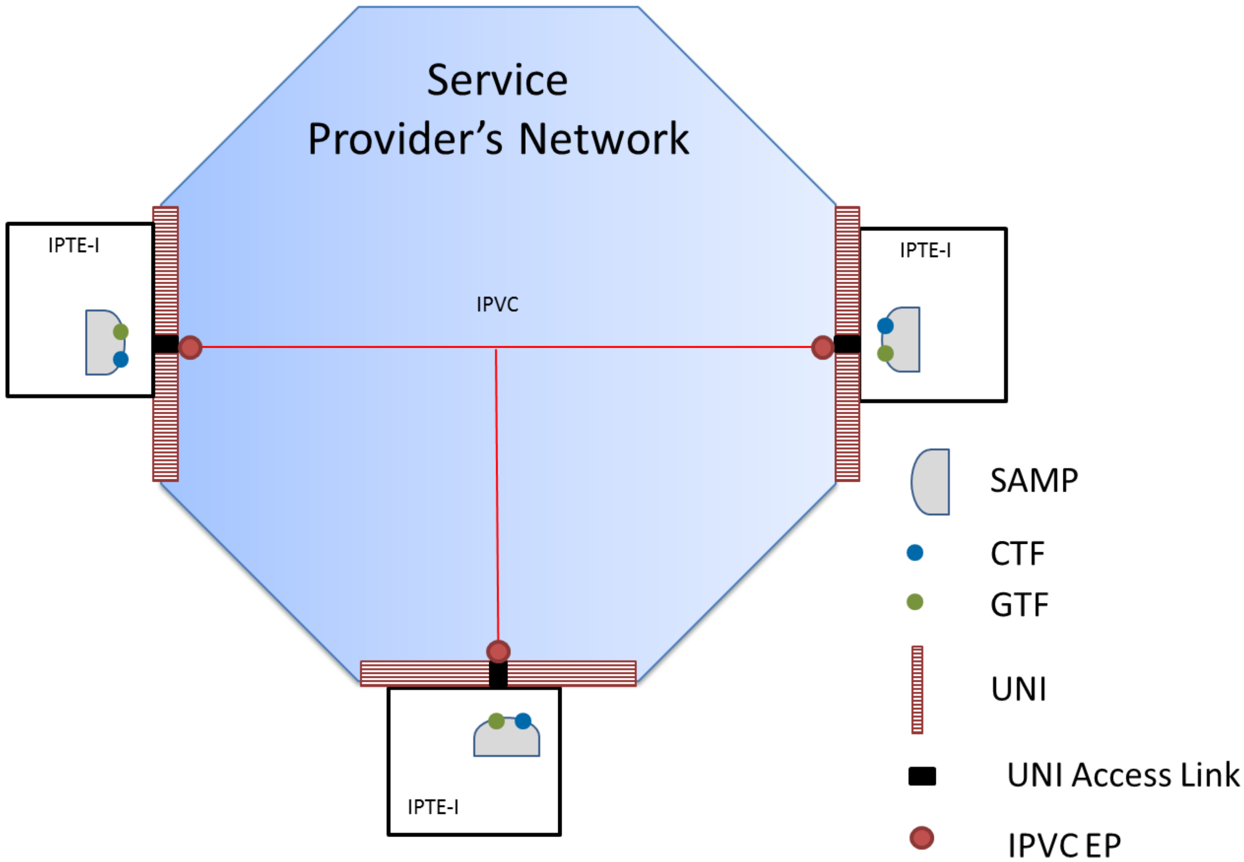

Figure 3 Use Case 1: New IPVC Activation using IPTE-Is with Subscriber Managed CE

Figure 3 Use Case 1, shows SAT being done on a new IPVC with three IPVC EPs and Subscriber managed CE. Testing is done from each IPVC EP to each of the other IPVC EPs meaning that each IPTE-I tests to each of the other IPTE-Is. This use case shows the SAMP, GTF, and CTF within the IPTE-I. The SAMP is a Down SAMP. The IPTE-I replaces the CE and connects to the Subscriber side of the UNI. Test packets are passed across the UNI and UNI Access Link in the same way that Subscriber packets would be passed from the Subscriber managed CE. Measurements are made between the IPTE-Is and results are either manually collected or are uploaded to a management system. In this case UNI, UNI Access Link, IPVC and IPVC EP Service Attributes can be verified.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

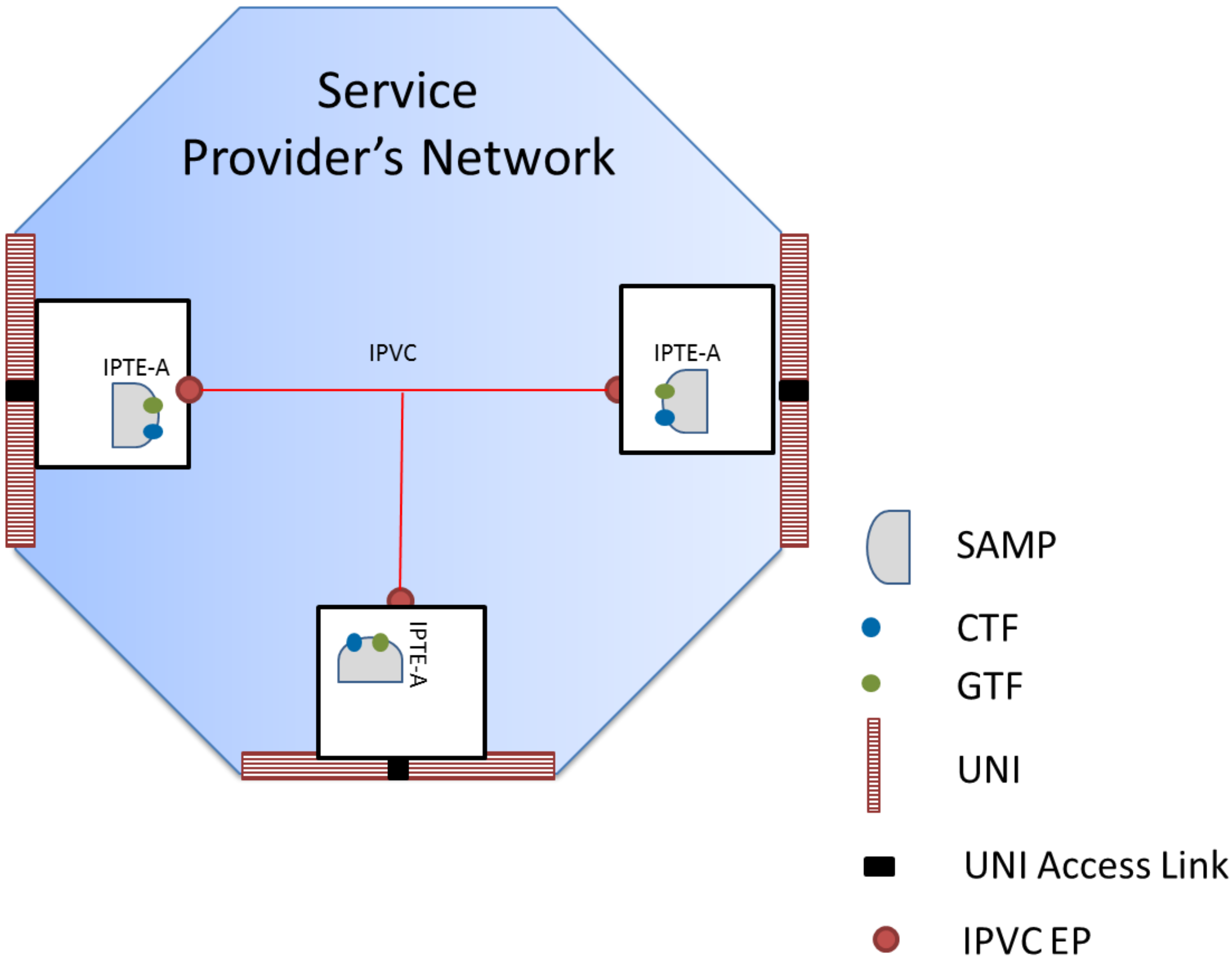

Figure 4 Use Case 2: New IPVC Activation IPTE-A to IPTE-A Testing from the Service Provider Side of the UNI, IPVC and IPVC EP Service Attributes

Figure 4 Use Case 2, reflects the activation of a new IPVC containing three IPVC EPs. At each IPVC EP an IPTE-A which is contained within a device managed by the Service Provider is present. Each IPTE-A uses an Up SAMP. SAT is performed between all the IPVC EPs of this new IPVC with each IPTE-A exchanging measurement packets with each of the other two IPTE-As. Because the device is on the Service Provider side of the UNI, test packets do not pass across the UNI and UNI Access Link. For details on testing the UNI and UNI Access Link please see Figure 11.

Note: The IPTE-A is shown between the UNI Access Link and the IPVC EP so that packets generated by the IPTE-A pass through the IPVC EP and any IPVC/IPVC EP Service Attributes are verified.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

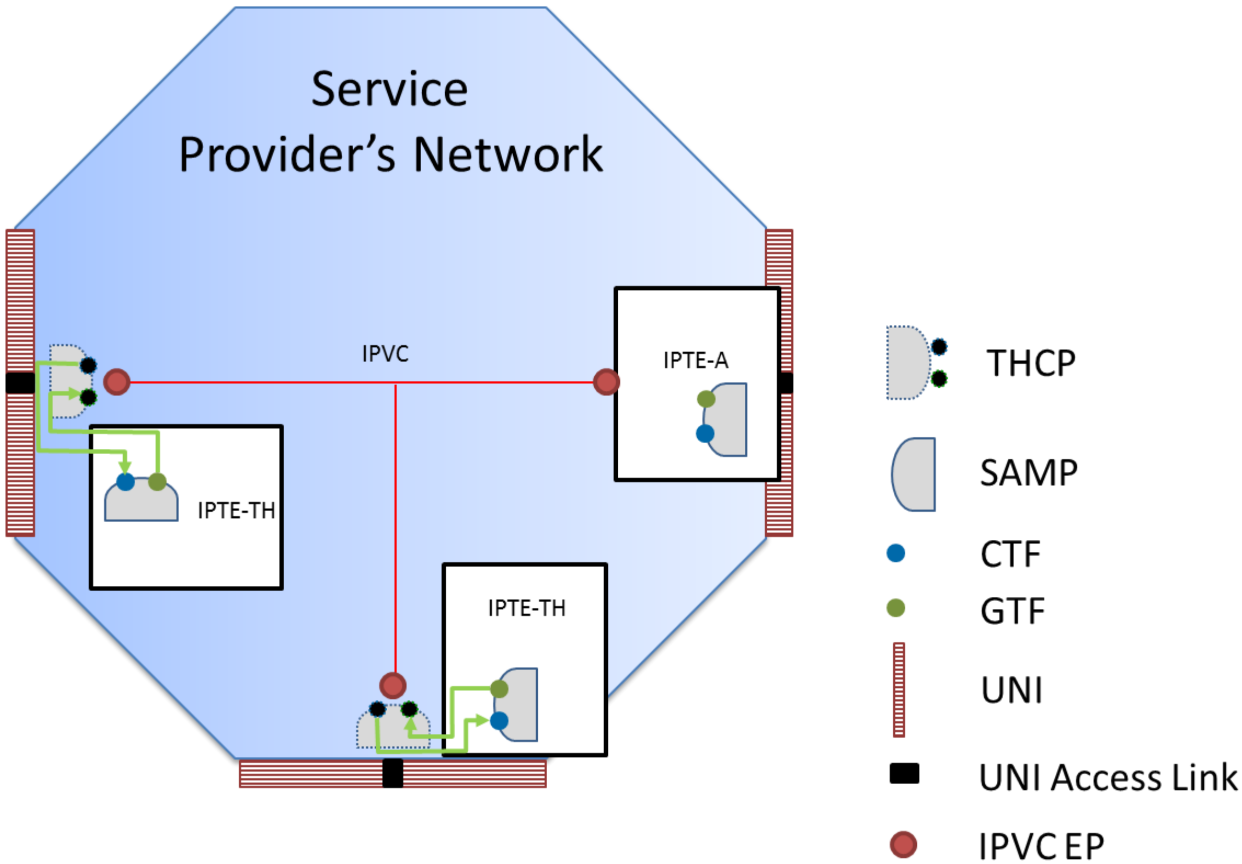

Figure 5 Use Case 3: New IPVC Activation using IPTE-A and IPTE-TH to Verify IPVC and IPVC EP Service Attributes

Figure 5 Use Case 3, shows SAT being performed on a new IPVC using an IPTE-A and IPTE-THs. The IPTE-A uses a Up SAMP. The IPTE-THs use Down SAMPs and Up THCPs. Tests are performed between the IPTE-A and each of the IPTE-THs and between each of the IPTE-THs. This configuration is used to verify the IPVC and IPVC EP Service Attributes. The THCPs are located so that packets generated by the GTF in the IPTE-TH pass through the IPVC EP onto the IPVC and that packets received from the IPVC are passed through the IPVC EP to the CTF in the IPTE-TH. The IPTE-A SAMP is located so that the GTF generates packets through the IPVC EP onto the IPVC and that packets received by the IPVC EP pass to the CTF.

This configuration is not used to test the UNI or UNI Access Link Service Attributes. To see this detail please see Figure 12 .

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

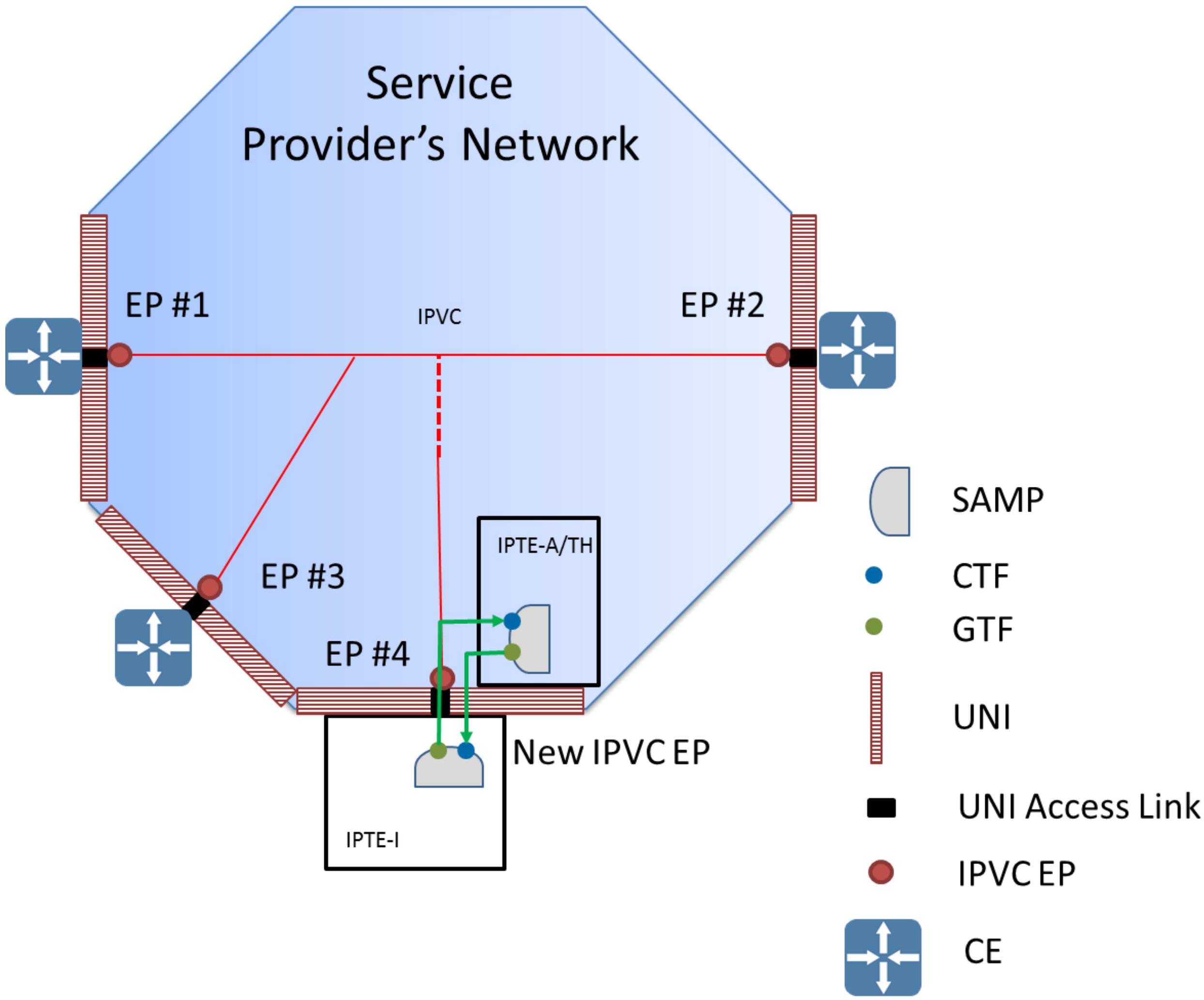

Figure 6 Use Case 4: New UNI adding New IPVC EP to Existing IPVC Testing from Subscriber Side of UNI using IPTE-I

Figure 6 Use Case 4, shows SAT being performed on a new IPVC EP (EP #4) being added to an existing IPVC from the Subscriber side of the UNI. This configuration can be used with Service Provider or Subscriber managed CEs. SAT is only performed between the IPTE-I located at the Subscriber's location and the IPTE-A or IPTE-TH located within the Service Provider's network near the new IPVC EP (EP #4). The IPTE-I as always uses a Down SAMP. The IPTE-A uses a Down SAMP. The IPTE-TH uses a Down SAMP and a Down THCP. Test packets pass over the UNI and UNI Access Link in the same manner as Subscriber packets. If the IPVC EP is being activated on a UNI without any existing IPVC EPs then all IPVC, IPVC EP, UNI, and UNI Access Link Service Attributes are verified. If the IPVC EP is being activated on an UNI that has existing IPVC EPs, then an IPTE-I cannot be inserted in the UNI without impacting existing IPVC EPs at that location. Either downtime is scheduled with the Subscriber for that location to activate the new IPVC EP or the IPVC EP is only tested as shown in Figure 7.

Service between existing IPVC EPs (EP #1, EP #2, EP #3) is not disrupted. The new IPVC EP is not added to the IPVC until after it has passed SAT. If the PE that the new IPVC EP connects to is new to the IPVC, that is no other IPVC EPs (EP #1, EP #2, EP #3) for that IPVC exist on the

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

PE, SAT can be performed between the PE and other PEs with IPVC EPs in the IPVC to ensure that routing updates are complete.

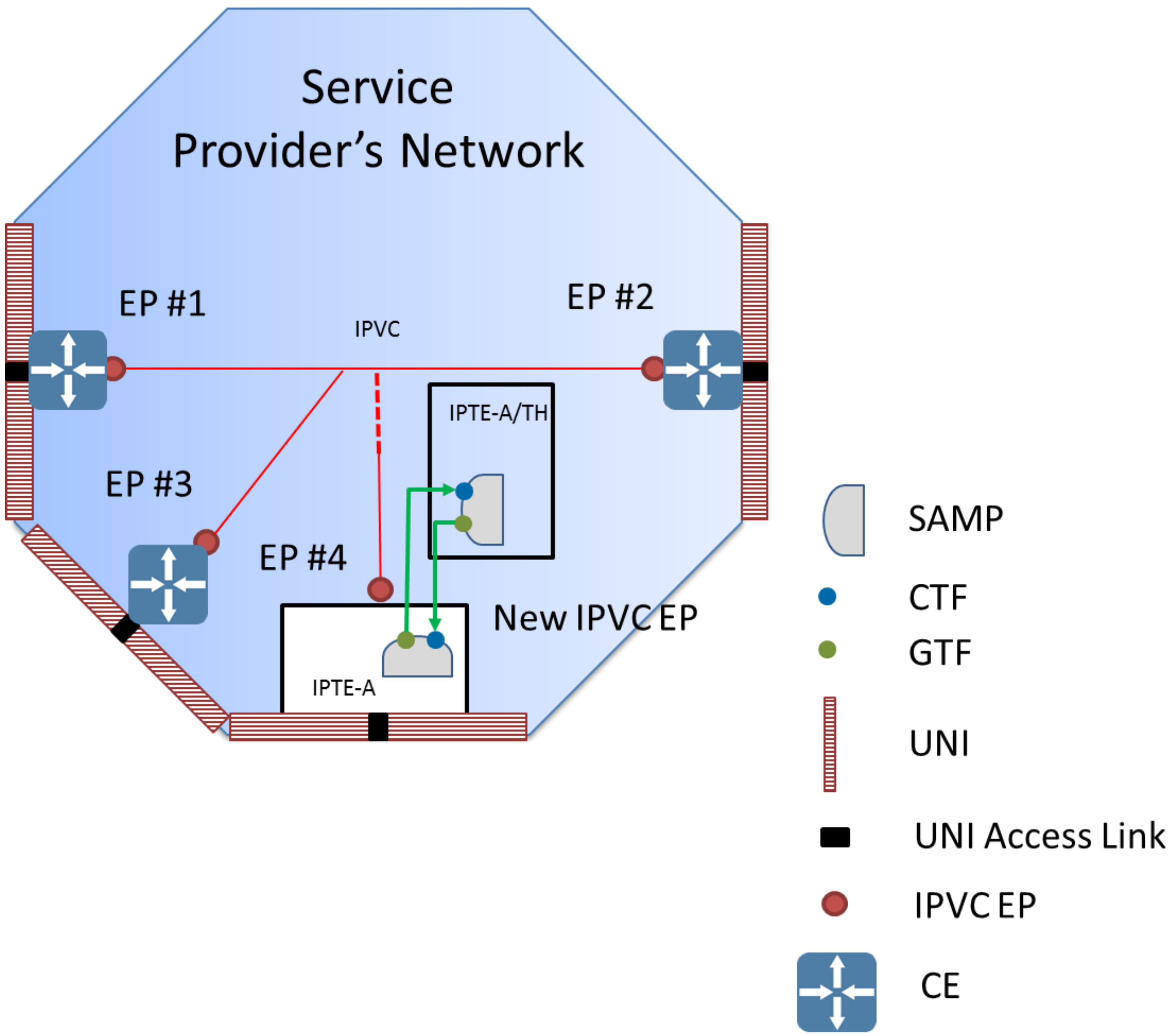

Figure 7 Use Case 5: New IPVC EP Activation of an IPVC Testing from the Service Provider Side of the UNI Using IPTE-A

Figure 7 Use Case 5, shows an example of a new IPVC EP (EP #4) being added to an existing IPVC where the Service Provider is testing from the Service Provider side of the UNI. The IPTE-A resides as an application or set of applications in the device or applications that make up the Managed CE or other device in the Service Provider's network. The IPTE-A at EP #4 uses an Up SAMP. The test packets do not pass over the UNI or UNI Access Link. The SAT is performed between the IPTE-A and an IPTE-A or IPTE-TH that is located near the IPVC EP in the Service Provider's network. The IPTE-A or IPTE-TH uses a Down SAMP and a Down THCP as applicable. UNI and UNI Access Link Service Attributes are not verified using this configu-

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

ration. See Figure 10 for the configuration used for verifying UNI and UNI Access Link Service Attributes for a new UNI.

Service between existing IPVC EPs (EP #1, EP #2, EP #3) is not disrupted. The new IPVC EP is not added to the IPVC until after it has passed SAT. If the PE that the new IPVC EP connects to is new to the IPVC, that is no other IPVC EPs for that IPVC exist on the PE, SAT can be performed between the PE and other PEs with IPVC EPs in the IPVC to ensure that routing updates are complete.

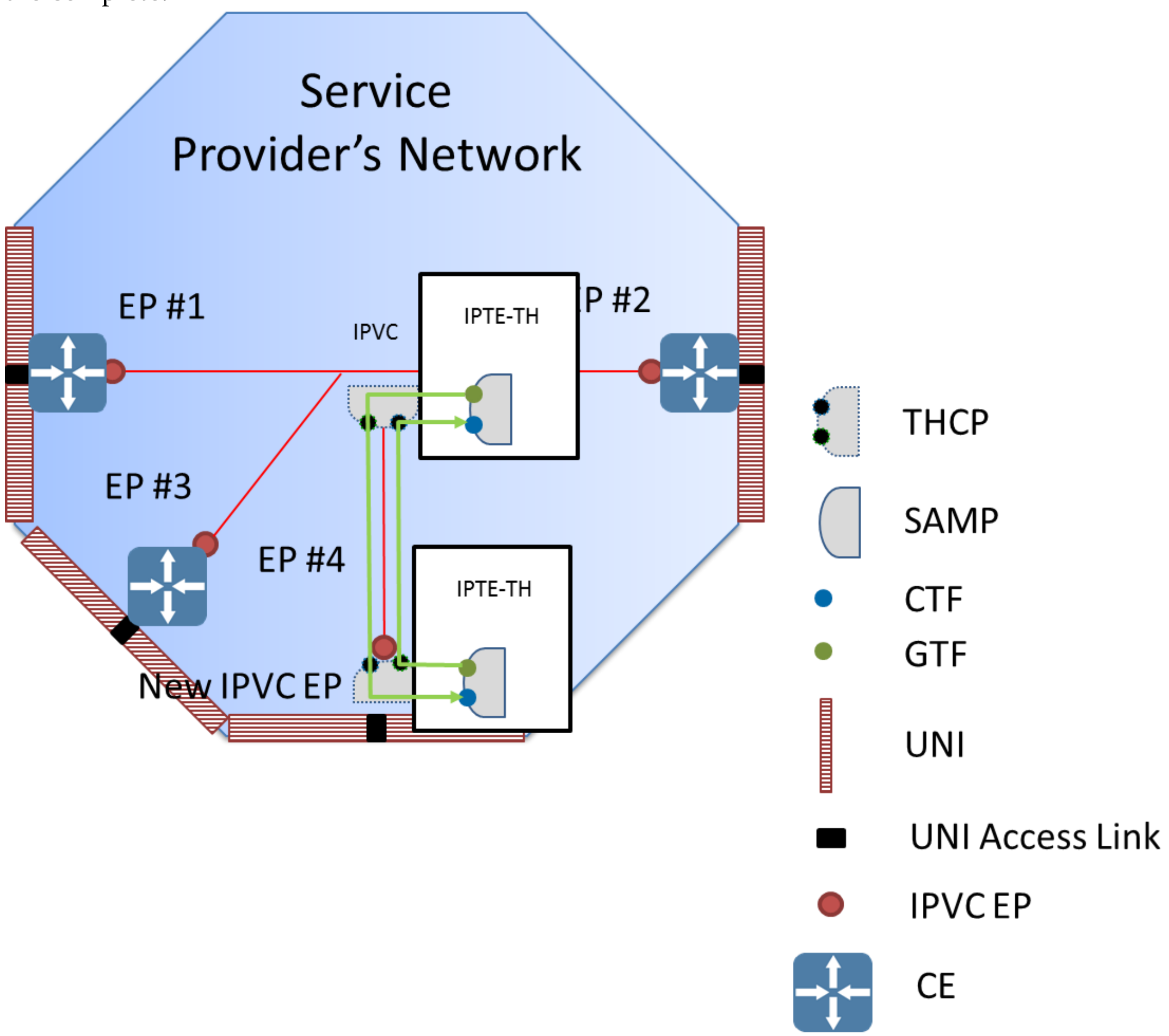

Figure 8 Use Case 6: New IPVC EP Activation using IPTE-TH to IPTE-TH to Verify IPVC and IPVC EP Service Attributes

Figure 8 Use Case 6, shows SAT being performed on a new IPVC using two IPTE-THs. Tests are performed between the IPTE-THs. The IPTH-TH at EP #4 uses a Down SAMP and a Up THCP. The other IPTE-TH uses a Down SAMP and a Down THCP. This configuration is used to verify the IPVC and IPVC EP Service Attributes. The THCPs are located so that packets gen-

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

erated by the GTF in the IPTE-TH pass through the IPVC EP onto the IPVC and that packets received from the IPVC are passed through the IPVC EP to the CTF in the IPTE-TH.

Note: Depending on the Service Provider's Network configuration, the same IPTE-TH using different test or interface applications or cards could be connected to two different THCPs to perform the testing rather than using two IPTE-THs as shown in the figure.

This configuration is not used to test the UNI or UNI Access Link Service Attributes. To see this detail please see Figure 13.

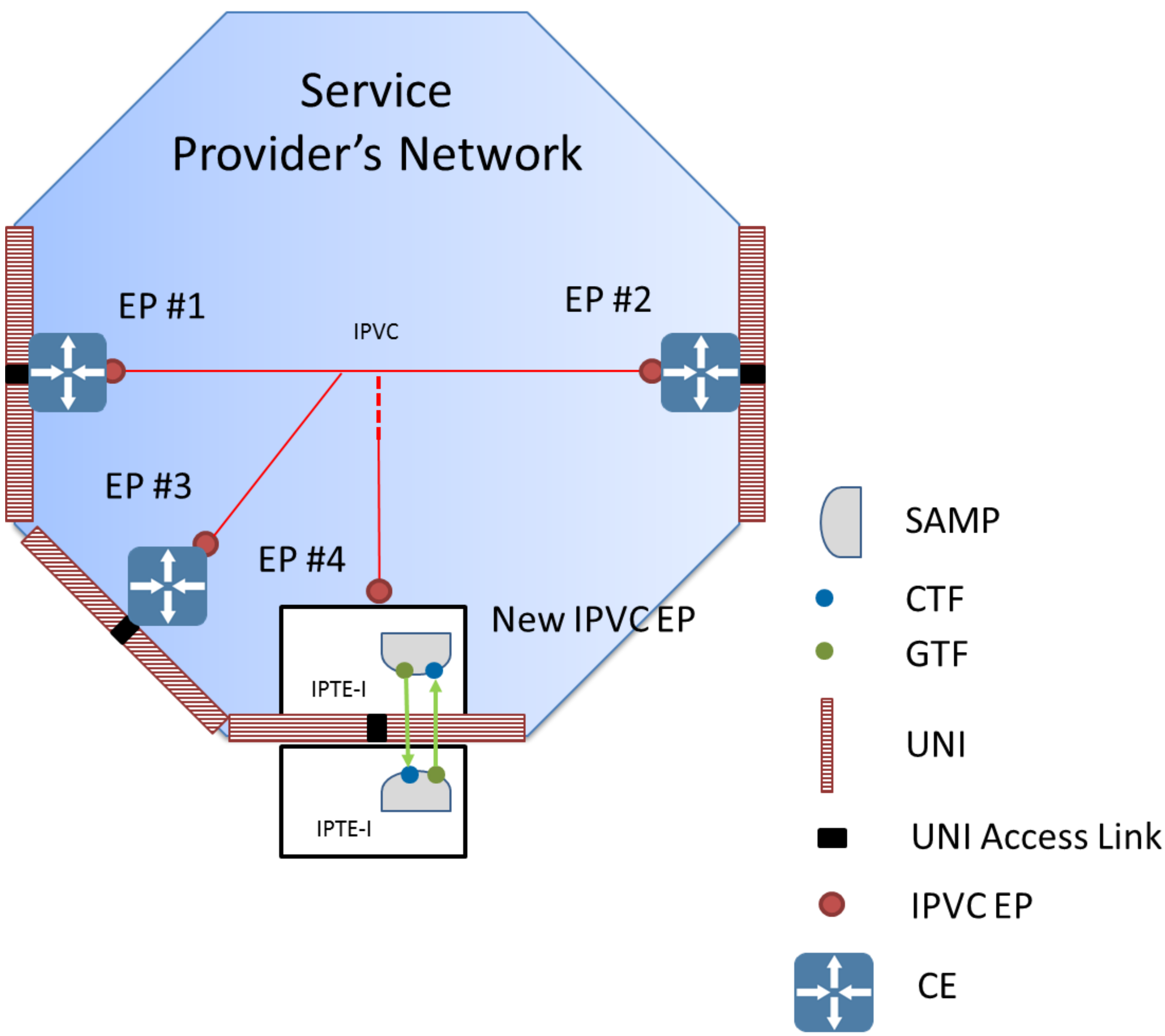

Figure 9 Use Case 7: New UNI Adding a New IPVC EP to Existing IPVC using IPTE-I Testing UNI and UNI Access Link Service Attributes

Figure 9 Use Case 7, shows an example of a new IPVC EP (EP #4) being added to an existing IPVC. Two IPTE-Is are used to perform UNI and UNI Access Link Service Attribute Verifica-

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

tion. The SAT is performed between the IPTE-Is. Both IPTE-Is use Down SAMPs. This configuration is only used when the UNI has no existing IPVCs configured on it. If the UNI has IPVCs configured on it, the UNI Service Attributes have already been tested. As UNI Access Links are added it might not be possible to verify the UNI Access Link Service Attributes since performing tests in them could impact other UNI Access Links or IPVCs.

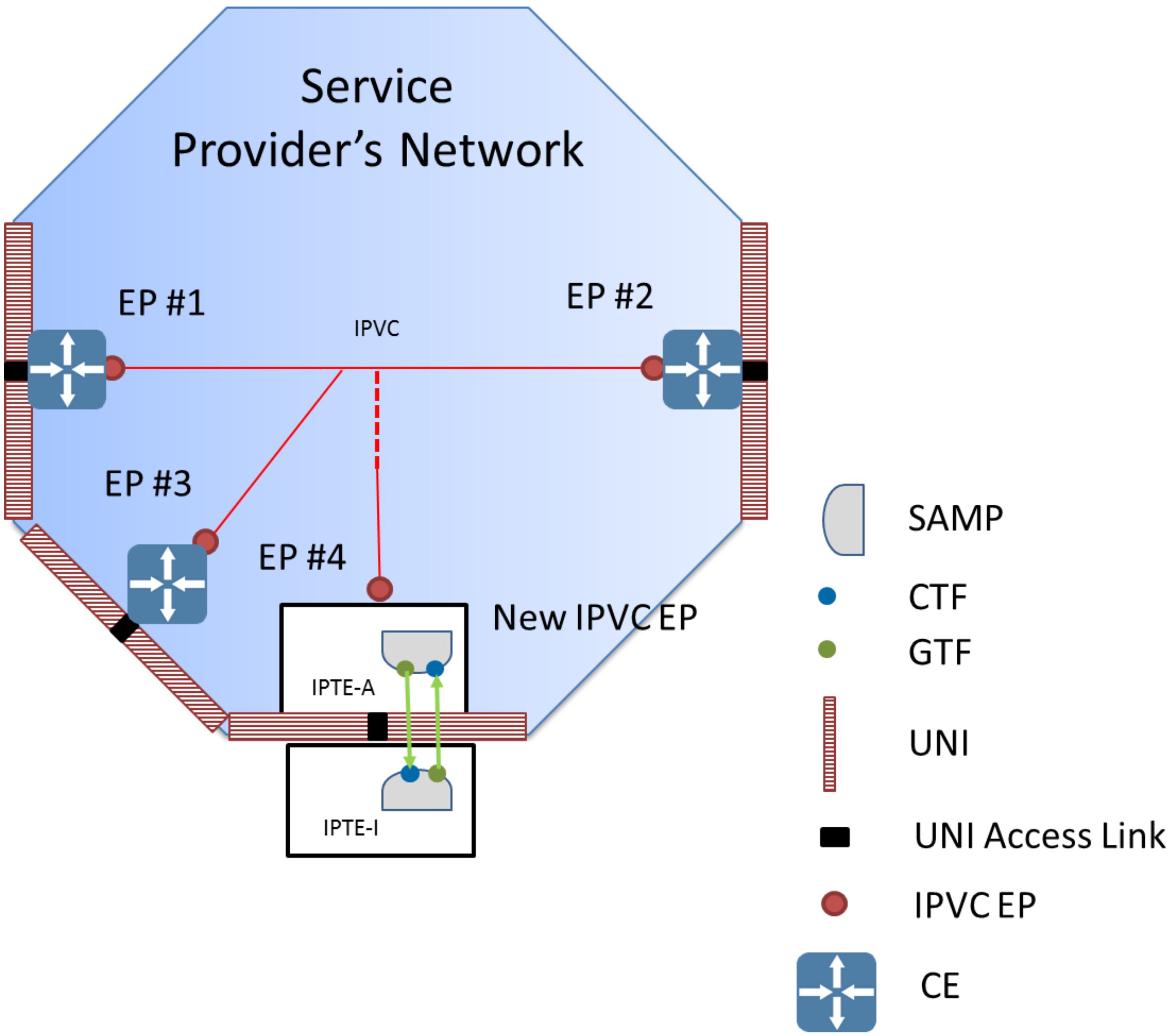

Figure 10 Use Case 8: New IPVC EP Activation IPTE-A to IPTE-I Testing Across UNI to Verify UNI and UNI Access Link Service Attributes

Figure 10 Use Case 8, shows an example of a new IPVC EP being activated where the Service Provider is testing across the UNI. An IPTE-A and an IPTE-I are used to perform UNI and UNI Access Link Service Attribute Verification. The IPTE-A and IPTE-I both use Down SAMPs. The SAT is performed between the IPTEs. This configuration is only used when the UNI has no existing IPVCs configured on it. If the UNI has IPVCs configured on it, the UNI Service Attributes have already been tested. As UNI Access Links are added it might not be possible to verify

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

the UNI Access Link Service Attributes since performing tests in them could impact other UNI Access Links or IPVCs.

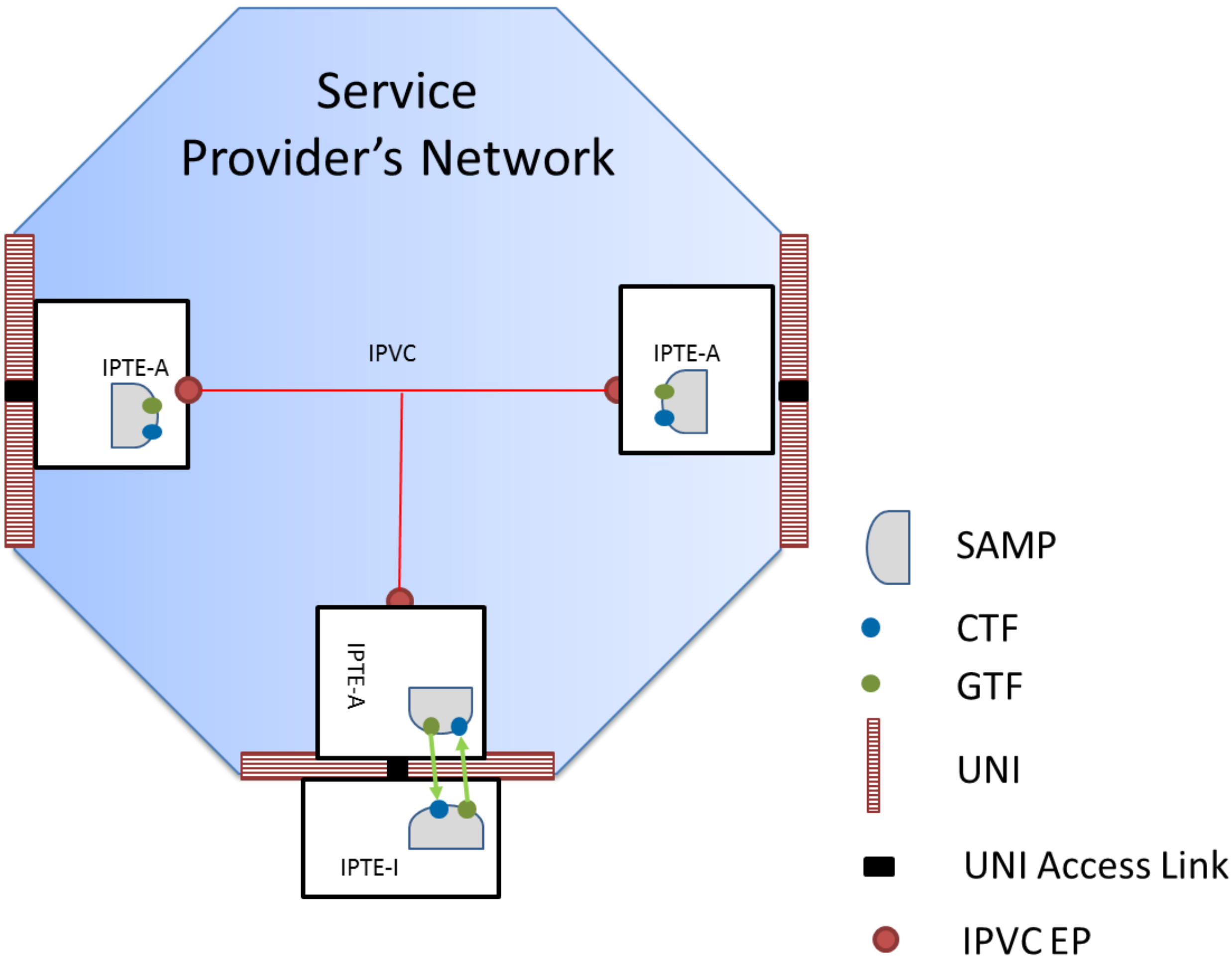

Figure 11 Use Case 9: New IPVC Activation IPTE-A to IPTE-I Testing Across UNI to Test UNI and UNI Access Link Service Attributes

Figure 11 Use Case 9, shows an example of a new IPVC being activated where the testing is being done by the Service Provider across the UNI. An IPTE-A and an IPTE-I are used to perform UNI and UNI Access Link Service Attribute Verification. The IPTE-I uses a Down SAMP. The IPTE-A uses a Down SAMP. The SAT is performed between the IPTEs. This configuration is only used when the UNI has no existing IPVCs configured on it. If the UNI has IPVCs configured on it, the UNI Service Attributes have already been tested. As UNI Access Links are added it might not be possible to verify the UNI Access Link Service Attributes since performing tests in them could impact other UNI Access Links or IPVCs.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

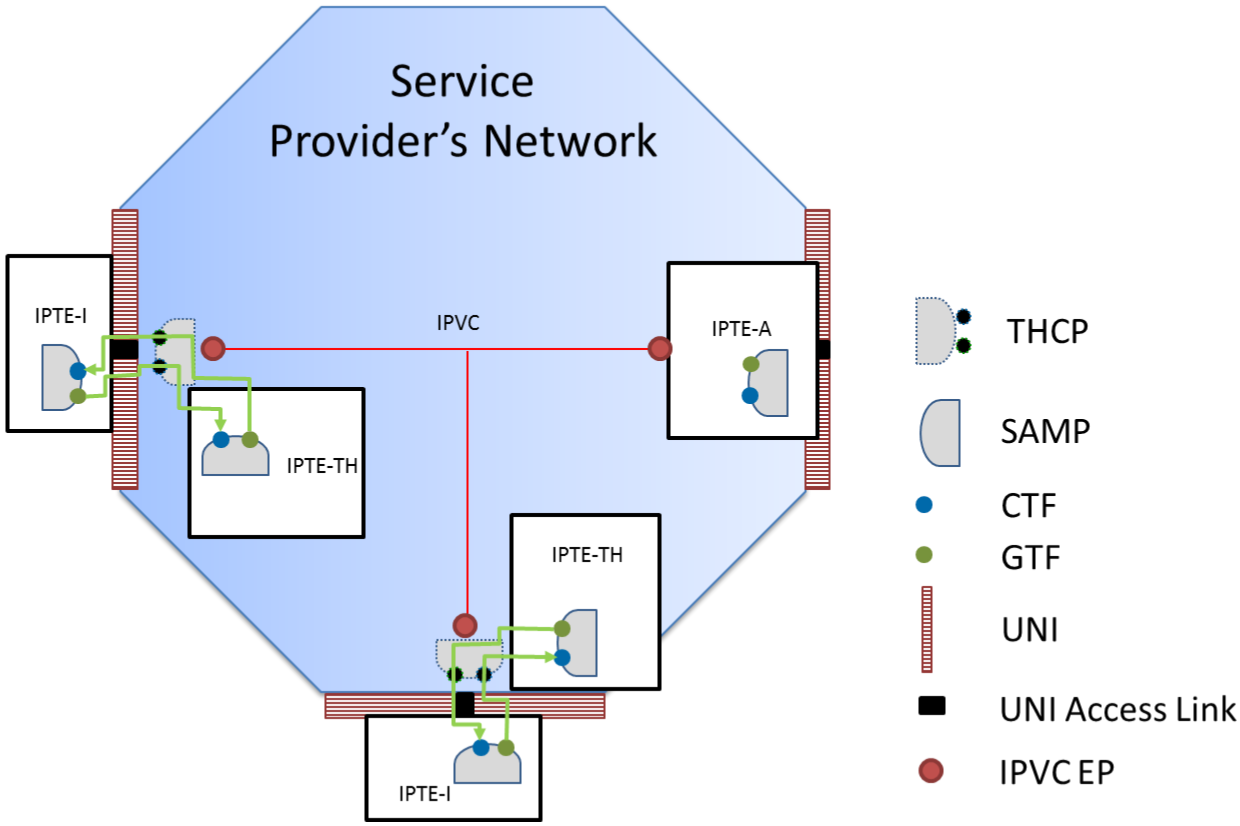

Figure 12 Use Case 10: New IPVC Activation using IPTE-I and IPTE-TH to Verify UNI and UNI Access Link Service Attributes

Figure 12 Use Case 10, shows an example of a new IPVC being activated where the Service Provider is testing from the Service Provider side of the UNI. An IPTE-TH and an IPTE-I are used to perform UNI and UNI Access Link Service Attribute Verification. The IPTE-I uses a Down SAMP. The IPTE-TH uses a down SAMP and a Down THCP. The SAT is performed between the IPTEs. This configuration is only used when the UNI has no existing IPVCs configured on it. If the UNI has IPVCs configured on it, the UNI Service Attributes have already been tested. As UNI Access Links are added it might not be possible to verify the UNI Access Link Service Attributes since performing tests in them could impact other UNI Access Links or IPVCs.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

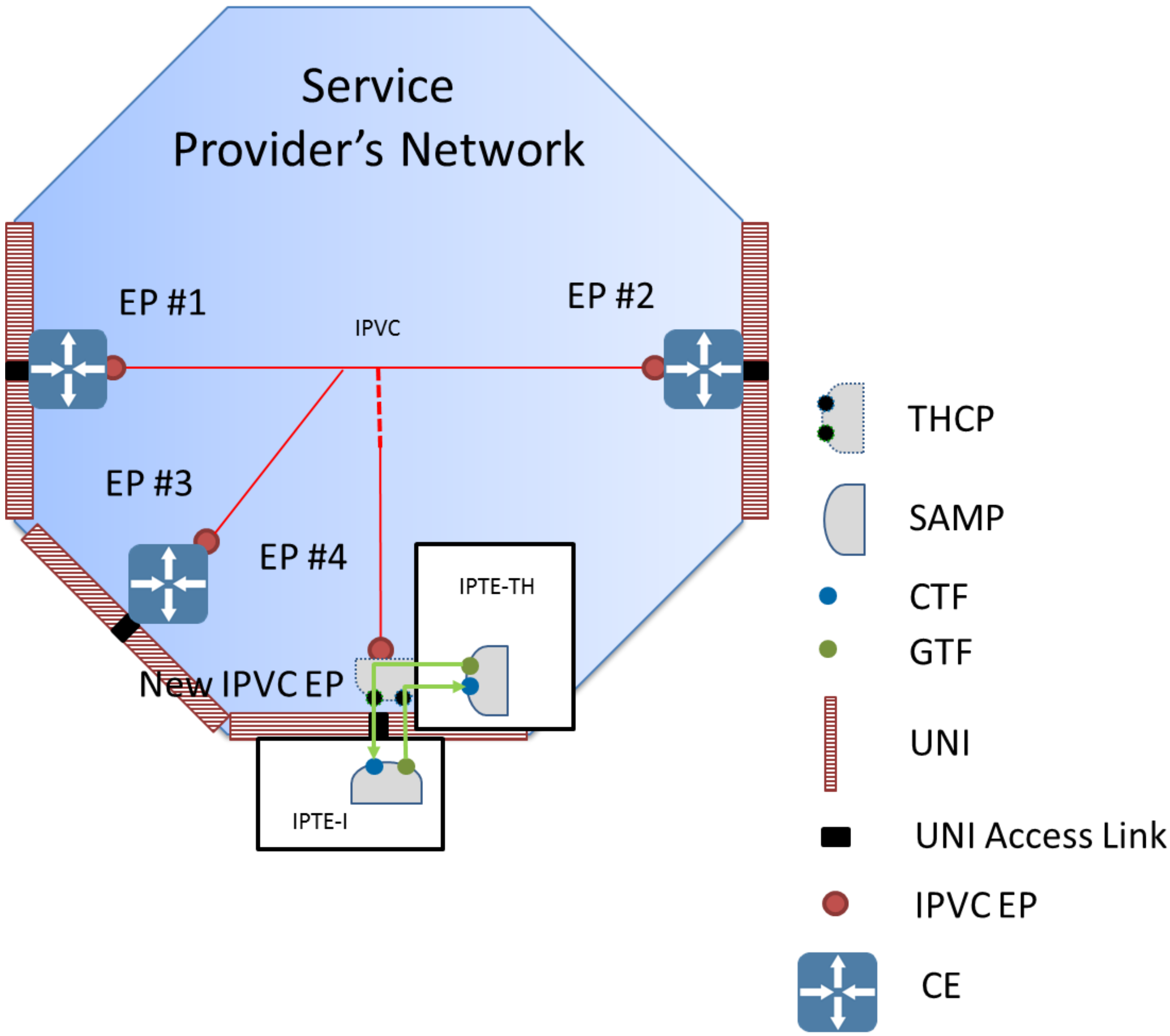

Figure 13 Use Case 11: New IPVC EP Activation using IPTE-I and IPTE-TH to Verify UNI and UNI Access Link Service Attributes

Figure 13 Use Case 11, shows an example of a new IPVC EP being activated where the Service Provider is testing from the Service Provider side of the UNI. An IPTE-TH and an IPTE-I are used to perform UNI and UNI Access Link Service Attribute Verification. The IPTE-TH uses a Down SAMP and a Down THCP. The IPTE-I uses a Down SAMP. The SAT is performed between the IPTEs. This configuration is only used when the UNI has no existing IPVCs configured on it. If the UNI has IPVCs configured on it, the UNI Service Attributes have already been tested. As UNI Access Links are added it might not be possible to verify the UNI Access Link Service Attributes since performing tests on them could impact other UNI Access Links or IPVCs on the UNI.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

8 SAMP and THCP Locations

The logical location of SAMPs and THCPs within the network is shown in this section. These examples are provided as guidance for SAMP and THCP implementations. These examples represent single-ended tests performing one-way or two-way measurements. One-way measurements might be possible depending on the measurement tool used. The tool used is beyond the scope of this document.

8.1 Service Activation Measurement Point Locations

The following figures show the location of SAMPs and THCPs in relationship to logical functions within the network.

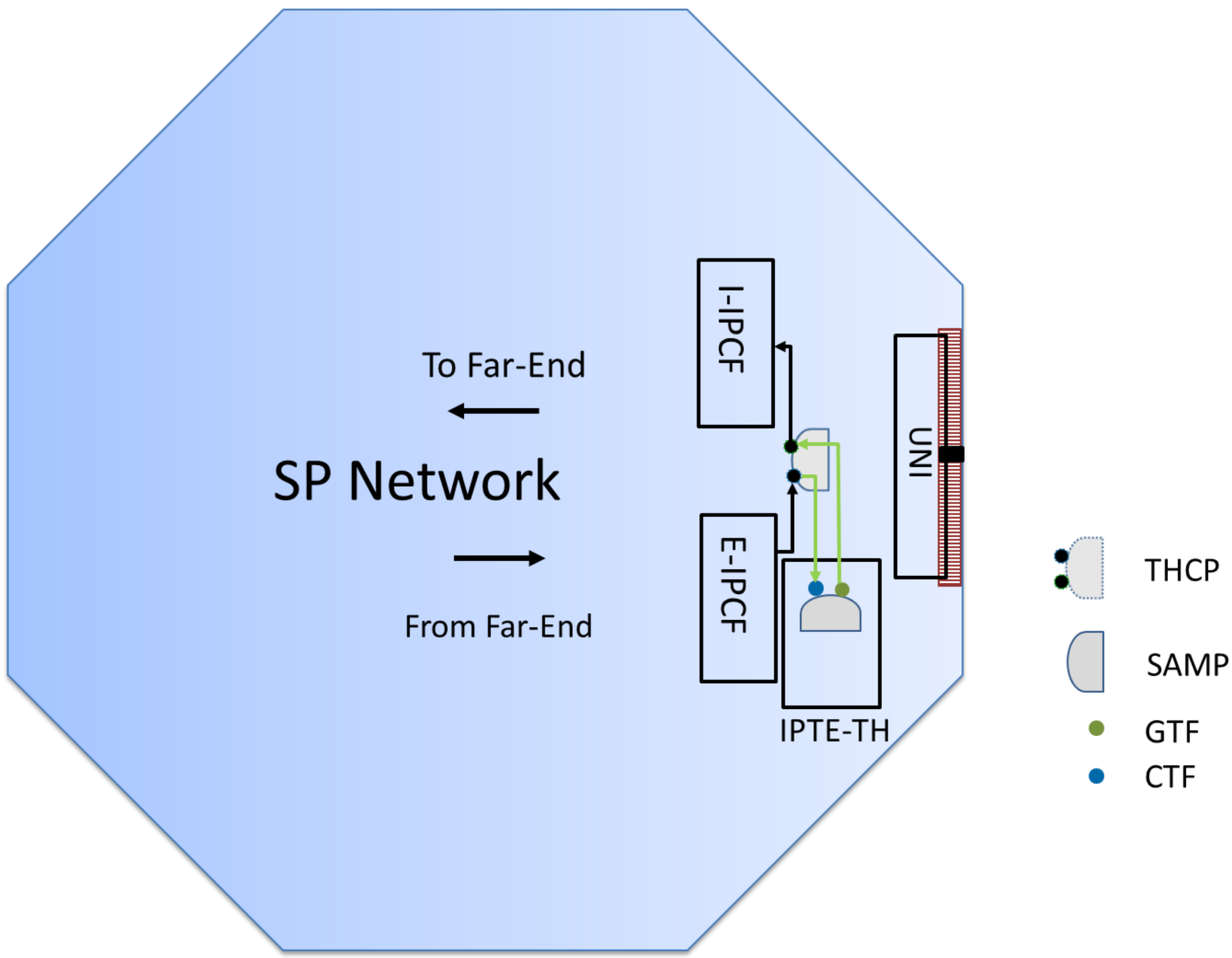

Figure 14 THCP Location to Verify IPVC and IPVC EP Service Attributes

Figure 14 shows the location of the Up THCP and Down SAMP when verifying IPVC and IPVC EP Service Attributes. Packets generated by the GTF pass through the Ingress – IP Conditioning Function (I-IPCF) and continue to the far-end. Packets from the far-end pass through the Egress – IP Conditioning Function (E-IPCF) and continue to the CTF. The Ingress and Egress IP Conditioning Functions support the Service Attributes through functions like:

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

- Service Packet classification into one or more flows
- Service Packet conditioning as per Ingress or Egress BWP

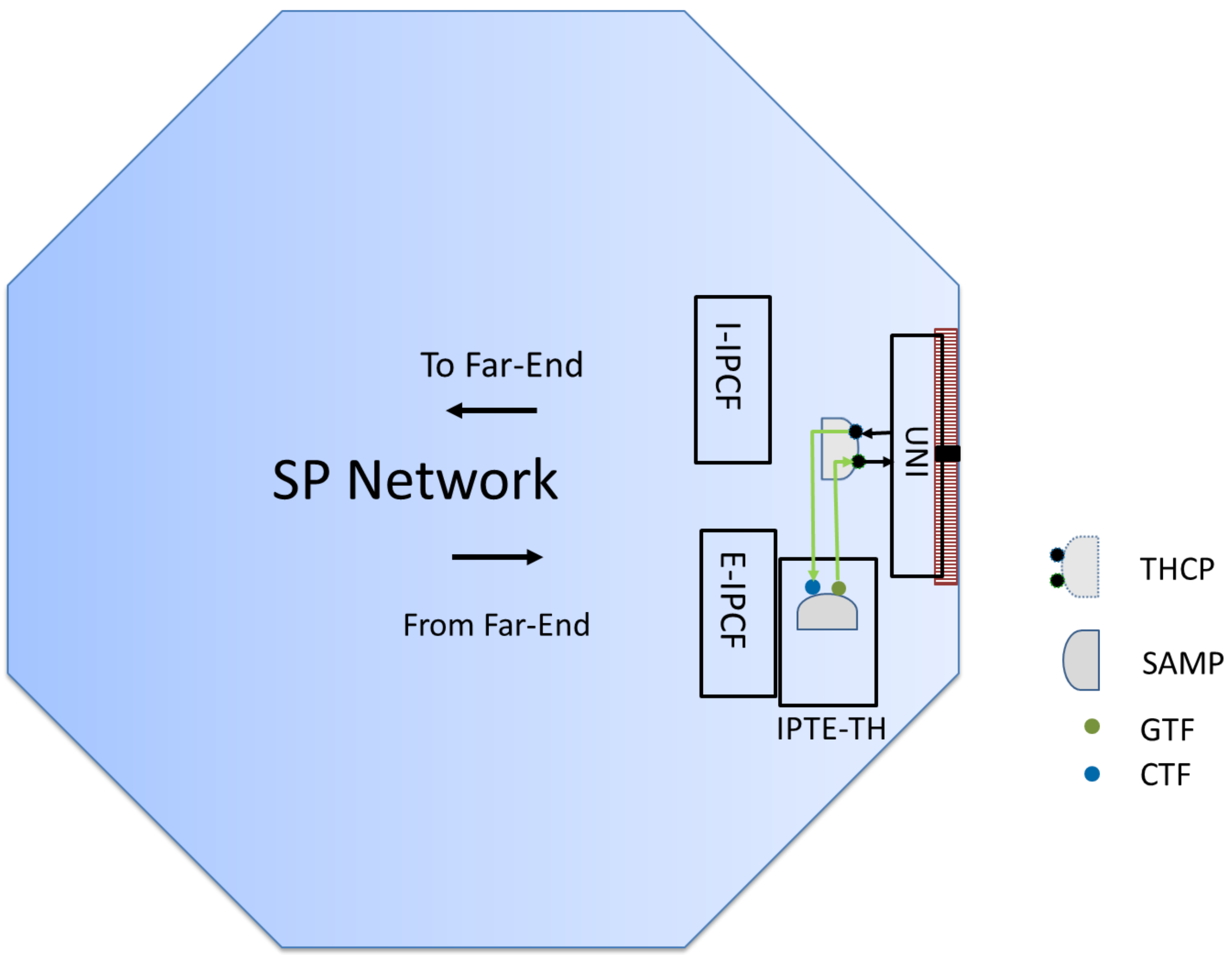

Figure 15 THCP Location to Verify UNI and UNI Access Link Service Attributes

Figure 15 shows the location of a Down THCP and Down SAMP used to verify the UNI and UNI Access Link Service Attributes. The THCP is placed so that packets generated and received by the IPTE-TH are processed by the UNI

[R1] This example can be used to verify a new UNI or new UNI Access Link if no IPVCs exist on the UNI already. When being used to verify IPVC and IPVC EP Service Attributes, a THCP implementation **MUST** locate the THCP as shown in Figure 14.

[R2] When being used to verify UNI and UNI Access Link Service Attributes a THCP implementation **MUST** locate the THCP as shown in Figure 15.

Note: The specific implementation is beyond the scope of this document.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

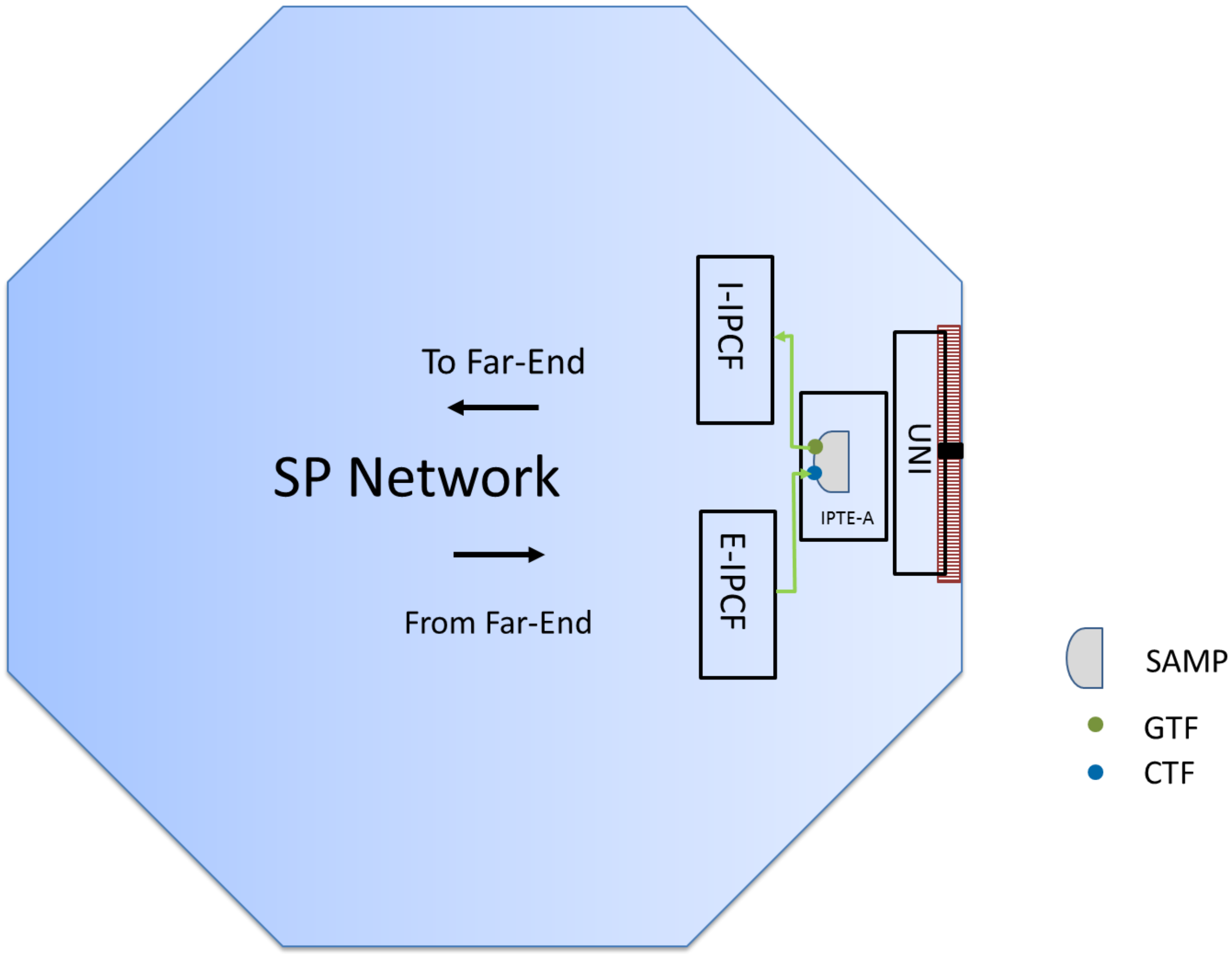

Figure 16 Up SAMP Location in IPTE-A to Verify IPVC and IPVC EP Service Attributes

Figure 16 shows the SAMP location used to verify the IPVC and IPVC EP Service Attributes using an IPTE-A. The SAMP is located so that packets generated by the GTF pass through the I-IPCF and packets counted by the CTF pass through the E-IPCF.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

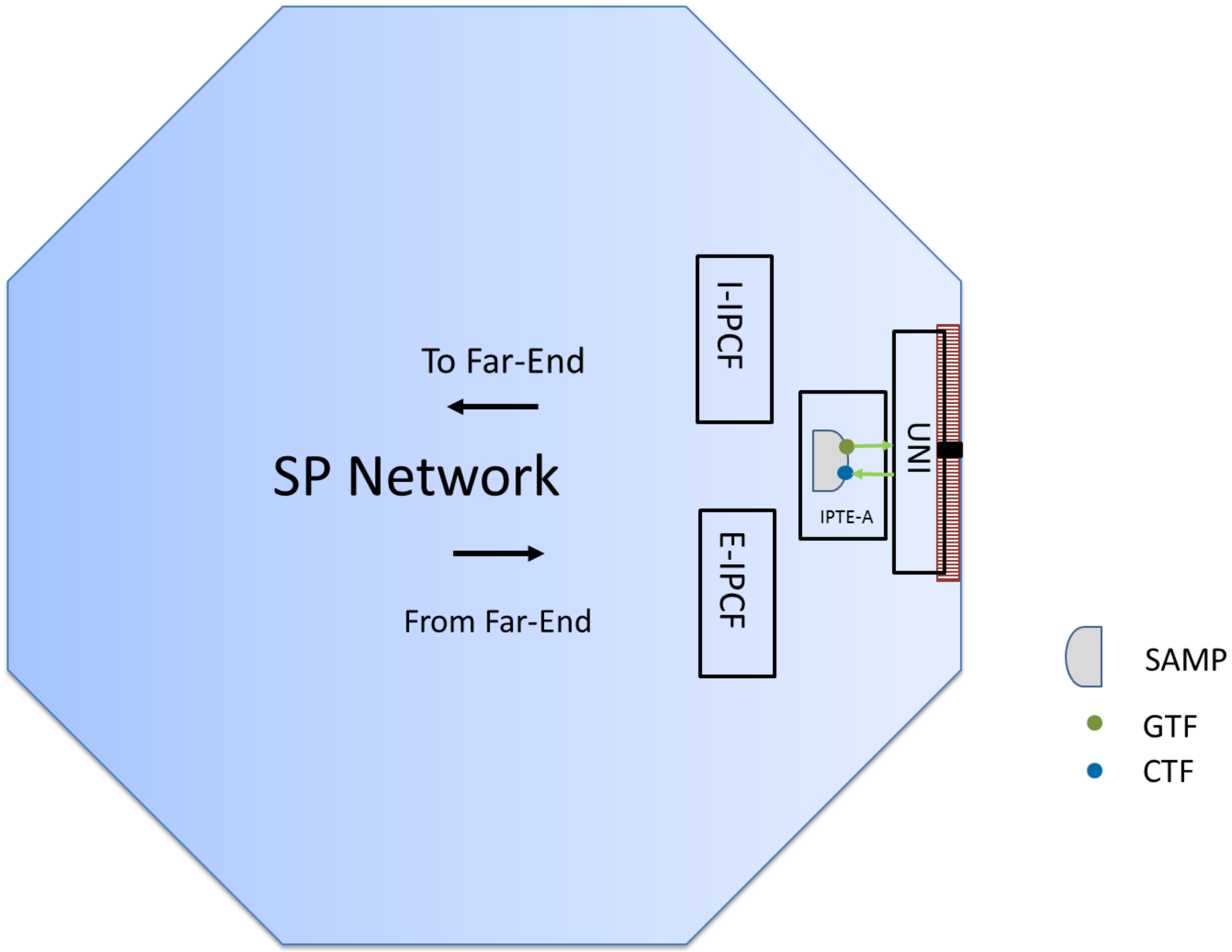

Figure 17 SAMP Location in IPTE-A to Verify UNI and UNI Access Link Service Attributes

Figure 17 shows the IPTE-A SAMP location used to verify the UNI and UNI Access Link Service Attributes. Packets generated by the GTF pass through the UNI and packets counted by the CTF pass through the UNI.

[R3] A SAMP implementation supporting an IPTE-A used to verify IPVC and IPVC EP Service Attributes **MUST** be implemented as shown in Figure 16.

[R4] A SAMP implementation supporting an IPTE-A used to verify UNI and UNI Access Link Service Attributes **MUST** be implemented as shown in Figure 17.

Note: The specific implementation is beyond the scope of this document.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

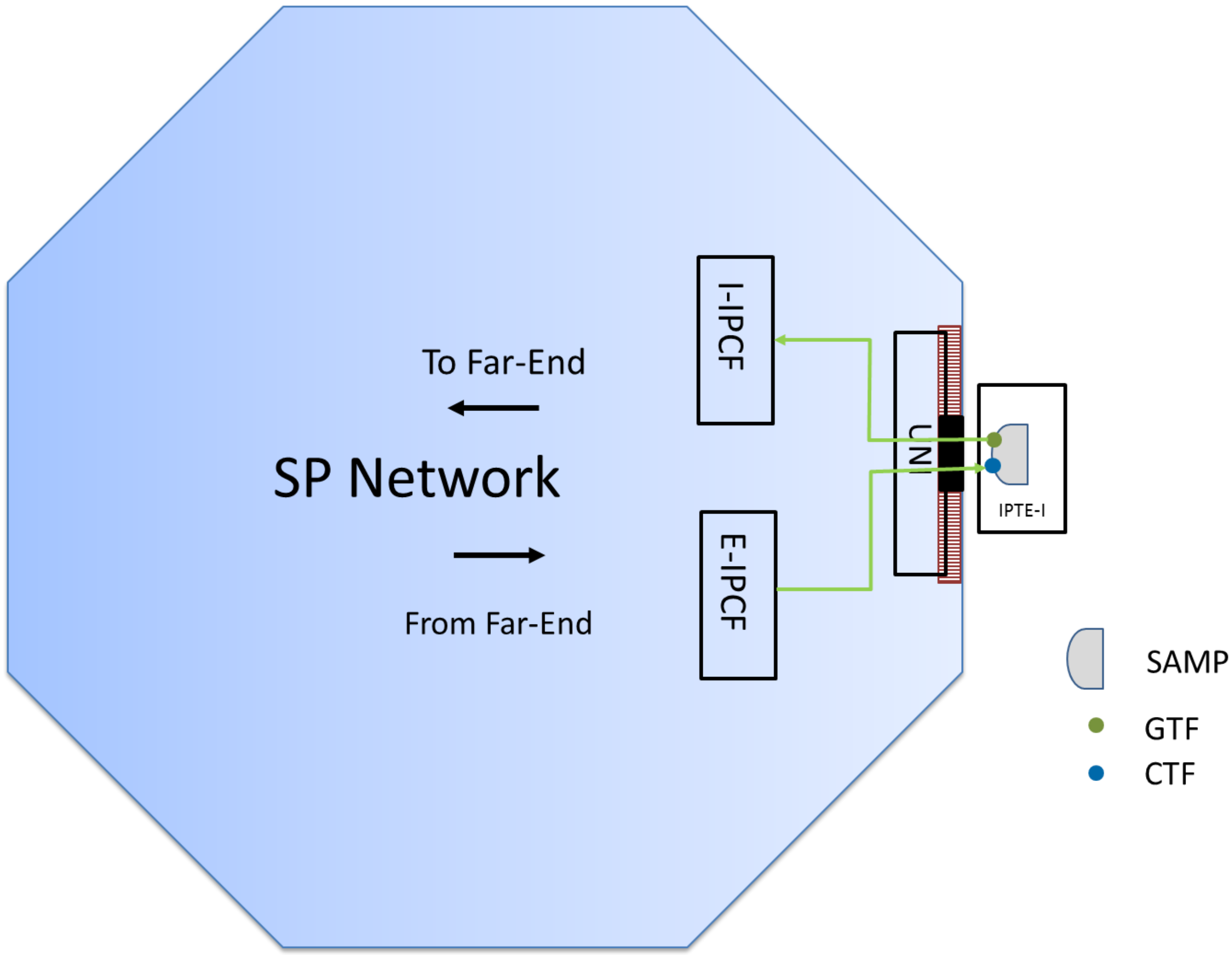

Figure 18 SAMP Location in IPTE-I to Verify IPVC, IPVC EP, UNI, and UNI Access Link Service Attributes

Figure 18 shows the SAMP location used to verify the IPVC, IPVC EP, UNI, and UNI Access Link Service Attributes simultaneously using an IPTE-I. The SAMP is located so that packets generated by the GTF pass through the UNI, UNI Access Link, I-IPCF and packets counted by the CTF pass through the E-IPCF, UNI Access Link and UNI.

[R5] A SAMP implementation supporting an IPTE-I used to verify IPVC, IPVC EP, UNI, and UNI Access Link Service Attributes **MUST** be implemented as shown in Figure 18.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

9 Service Attributes

IP Service Attributes are defined in MEF 61 [24]. This section defines how those Service Attributes are verified.

- For a specific service, each Service Attribute can either be 1) ***Tested*** using one of the test methodologies defined in section 10 of this document, and the test result reported in the SAT record, or 2) ***Reported***, meaning that Service Attribute is not tested but the value of the configured Service Attribute has to be reported in the SAT record or 3) ***Not applicable*** in the context of SAT meaning that the Service Attribute is not tested nor its value reported in the SAT record.
- The first column of each table specifies the Service Attribute.
- When a Service Attribute has to be ***reported*** , the second column, Report Status, of the Service Attribute tables indicates if it is mandatory, optional, or NA to report the Service Attribute.
    - There are two sub-columns under Report Status. The sub-column on the left is for new IPVCs, UNIs, etc. as shown in Table 3. The sub-column on the right is for new IPVC EPs being added to existing IPVCs as shown in Table 3.
- When a Service Attribute has to be ***tested*** , the third column, Testing Status, of the Service Attribute tables indicates if it is mandatory, optional, or NA to test the Service Attribute.
    - There are two sub-columns under Testing Status. The sub-column on the left is for new IPVCs, UNIs, etc. as shown in Table 3. The sub-column on the right is for new IPVC EPs being added to existing IPVCs as shown in Table 3.
- The fourth column of the Service Attribute tables specifies which SAT methodology has to be utilized to verify the Service Attribute.
- The fifth column of the Service Attribute tables is used for comments and notes.

9.1 Configuration Testing

The Service Attributes described in the following tables are verified as a part of Configuration testing.

9.1.1 Subscriber UNI Service Attributes

Table 4 shows the Subscriber UNI Service Attributes.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Subscriber UNI Service Attribute	Report Status		Testing Status		SAT Methodology	Comments
	New UNI, New IPVC EP	Existing UNI, New IPVC EP	New UNI, New IPVC EP	Existing UNI, New IPVC EP		
UNI Identifier	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI Management Type	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI List of UNI Access Links	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI Ingress Bandwidth Profile Envelope	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI Egress Bandwidth Profile Envelope	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI List of Control Protocols	Mandatory	Optional	NA	NA	NA	

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Subscriber UNI Service Attribute	Report Status		Testing Status		SAT Methodology	Comments
	New UNI, New IPVC EP	Existing UNI, New IPVC EP	New UNI, New IPVC EP	Existing UNI, New IPVC EP		
	for new UNI	for existing UNI				
UNI Routing Protocols	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI Reverse Path Forwarding	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	

Table 4 Per UNI Configuration Service Attributes

[R6] The Service Provider **MUST** report the UNI Service Attributes as shown in Table 4 for a new UNI or for an existing UNI that has a new IPVC or IPVC EP activated on it.

Note: The UNI Ingress and Egress Bandwidth Profile Envelope are not tested for new UNIs since there are no IPVC EPs configured on the UNI at the time the UNI is tested. Therefore no bandwidth flow can be tested. These Service Attributes are not tested on existing UNIs to avoid impacting other IPVCs sharing the envelope.

9.1.2 Subscriber UNI Access Link

Table 5 shows the Subscriber UNI Access Link Service Attributes. Testing of UNI Access Link Service Attributes can only be accomplished with the first UNI Access Link activated on a UNI. Subsequent UNI Access Links are not tested since that might impact active traffic on the existing UNI Access Links. Testing UNI Access Link Service Attributes requires using an IPTE-I placed on the Subscriber side of the UNI as shown in the use cases in section 7.2. This means that it might not be desirable to test the UNI Access Link Service Attributes even with the first UNI Access Link since it will require a dispatch to the Subscriber's premises.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Subscriber UNI Access Link Service Attribute	Report Status		Testing Status		SAT Methodology	Comments
	New UNI, New IPVC EP	Existing UNI, New IPVC EP	New UNI, New IPVC EP	Existing UNI, New IPVC EP		
UNI Access Link Identifier	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI Access Link Connection Type	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI Access Link L2 Technology	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI Access Link IPv4 Connection Addressing	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI Access Link IPv6 Connection Addressing	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI Access Link DHCP Relay	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Subscriber UNI Access Link Service Attribute	Report Status		Testing Status		SAT Methodology	Comments
	New UNI, New IPVC EP	Existing UNI, New IPVC EP	New UNI, New IPVC EP	Existing UNI, New IPVC EP		
UNI Access Link Prefix Delegation	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI Access Link BFD	Mandatory for new UNI	Optional for existing UNI	Tested for new UNI AL	NA	10.3.1.1 10.3.1.2	Test if not None.
UNI Access Link IP MTU	Mandatory for new UNI	Optional for existing UNI	Tested for new UNI AL	NA	10.3.1.3	
UNI Access Link Ingress Bandwidth Profile Envelope	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI Access Link Egress Bandwidth Profile Envelope	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	
UNI Access Link Reserved VRIDs Service Attribute	Mandatory for new UNI	Optional for existing UNI	NA	NA	NA	

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Table 5 Per UNI Access Link Configuration Service Attributes

[R7] The Service Provider **MUST** test or report the UNI Access Link Service Attributes as shown in Table 5 for a new UNI or for an existing UNI that has a new IPVC or IPVC EP activated on it.

Note: The UNI Access Link Ingress and Egress Bandwidth Profile Envelope are not tested for new UNI Access Links since there are no IPVC EPs configured on the UNI Access Link at the time the UNI Access Link is tested. Therefore no bandwidth flow can be tested. These Service Attributes are not tested on existing UNI Access Links to avoid impacting other IPVCs sharing the envelope.

9.1.3 Subscriber IPVC Service Attributes

Table 6 shows the Subscriber IPVC Service Attributes.

Subscriber IPVC Service Attributes	Report Status		Testing Status		SAT Methodology	Comments
	New IPVC	New IPVC EP	New IPVC	New IPVC EP		
IPVC Identifier	Mandatory for new IPVC	Optional for new IPVC EP	NA	NA	NA	
IPVC Topology	Mandatory for new IPVC	Optional for new IPVC EP	NA	NA	NA	
IPVC End Point List	Mandatory for new IPVC	Optional for new IPVC EP	NA	NA	NA	
IPVC Packet Delivery	Mandatory for	Optional for	NA	NA	NA	

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Subscriber IPVC Service Attributes	Report Status		Testing Status		SAT Methodology	Comments
	New IPVC	New IPVC EP	New IPVC	New IPVC EP		
	new IPVC	new IPVC EP				
IPVC Maximum Number of IPv4 Routes	Mandatory for new IPVC	Optional for new IPVC EP	NA	NA	NA	Report whether unlimited or value.
IPVC Maximum Number of IPv6 Routes	Mandatory for new IPVC	Optional for new IPVC EP	NA	NA	NA	Report whether unlimited or value.
IPVC DSCP Preservation	Mandatory for new IPVC	Mandatory for new IPVC EP	Tested between all IPVC EPs	Tested for new IPVC EP only	9.3.2.1	Report if Enabled or Disabled. Test when enabled
IPVC List of Class of Service Names	Mandatory for new IPVC	Optional for new IPVC EP	NA	NA	NA	
IPVC Service Level Specification	NA	NA	NA	NA	NA	
IPVC MTU	Mandatory for new IPVC	Mandatory for new IPVC EP	Tested between all IPVC EPs	Optional for new IPVC EP only	9.3.2.2	To avoid congestion IPVC MTU is not tested on new IPVC EPs when the new EP

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Subscriber IPVC Service Attributes	Report Status		Testing Status		SAT Methodology	Comments
	New IPVC	New IPVC EP	New IPVC	New IPVC EP		
						shares a UNI or UNI AL envelope with another IPVC EP
IPVC Path MTU Discovery	Mandatory for new IPVC	Optional for new IPVC EP	Tested for all IPVC EPs	NA	9.3.2.3	Tested only when enabled
IPVC Fragmentation	Mandatory for new IPVC	Mandatory for new IPVC EP	Tested for all IPVC EPs	Tested for new IPVC EP only	9.3.2.4	Reported when enabled, tested when disabled.
IPVC Cloud	Mandatory for new IPVC	Optional for new IPVC EP	NA	NA	NA	None or as described in section 9.1.2 of MEF 61 [24]
IPVC Reserved Prefixes	Mandatory for new IPVC	Optional for new IPVC EP	NA	NA	NA	

Table 6 Per IPVC Configuration Service Attributes

[R8] The Service Provider **MUST** test or report IPVC Service Attributes as shown in Table 6 for new IPVCs or new IPVC IPs added to an existing IPVC.

9.1.4 Subscriber IPVC End Point

Table 7 shows the Subscriber IPVC End Point (EP) Service Attributes.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

618

Subscriber IPVC EP Service Attribute	Report Status		Testing Status		SAT Methodology	Comments
	New IPVC	New IPVC EP	New IPVC	New IPVC EP		
IPVC EP Identifier	Mandatory for each IPVC EP	Mandatory for new IPVC EP only	NA	NA	NA	
IPVC EP UNI	Mandatory for each IPVC EP	Mandatory for new IPVC EP only	NA	NA	NA	
IPVC EP Prefix Mapping	Mandatory for each IPVC EP	Mandatory for new IPVC EP only	Tested for each IPVC EP	Tested for new IPVC EP only	9.3.3.1	Test only when non-empty
IPVC EP Maximum Number of IPv4 Routes	Mandatory for each IPVC EP	Mandatory for new IPVC EP only	NA	NA	NA	
IPVC EP Maximum Number of IPv6 Routes	Mandatory for each IPVC EP	Mandatory for new IPVC EP only	NA	NA	NA	
IPVC EP Ingress Class of Service Map	Mandatory for each IPVC EP	Mandatory for new IPVC EP only	NA	NA	NA	
IPVC EP Egress Class of Service	NA	NA	NA	NA	NA	Deferred to a later revision of MEF 61

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Subscriber IPVC EP Service Attribute	Report Status		Testing Status		SAT Methodology	Comments
	New IPVC	New IPVC EP	New IPVC	New IPVC EP		
Map						[24]
IPVC EP Ingress Bandwidth Profile Envelope	Mandatory for each IPVC EP	Mandatory for new IPVC EP only	Tested for each new IPVC EP	Tested for new IPVC EP only	9.3.3.2	Test if not None.
IPVC EP Egress Bandwidth Profile Envelope	Mandatory for each IPVC EP	Mandatory for new IPVC EP only	Tested for each new IPVC EP	Tested for new IPVC EP only	9.3.3.3	Test if not None.

Table 7 Per IPVC EP Configuration Service Attributes

[R9] The Service Provider **MUST** test or report IPVC EP Service Attributes as shown in Table 7 for new IPVCs or new IPVC IPs added to an existing IPVC.

9.2 Performance Testing

Performance testing is done after configuration testing. The purpose of performance testing is to verify that the service meets performance expectations. Performance testing does not verify the service meets the SLS, instead, it verifies that the service meets the SAC. The performance attributes are shown in Table 8. Two measurements are performed, Packet Delay and Packet Loss. The other delay Performance Attributes (Packet Delay Percentile, Mean Packet Delay, Inter-Packet Delay Variation, Packet Delay Range) are calculated from Packet Delay. The loss Performance Attribute (Packet Loss Ratio) is calculated from Packet Loss.

Performance Attribute	Tested/Reported	SAT Methodology	Comments
Packet Delay Percentile	Tested		The SAC for Packet Delay Percentile can be as high as 100% due to short test period. Note 2
Mean Packet Delay	Tested		Note 2

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Inter-Packet Delay Variation	Tested		Note 3
Packet Delay Range	Tested		Note 3
Packet Loss Ratio	Tested		
Note 1: These Performance Attributes are derived from MEF 61 [24].			
Note 2: Packet Delay and Mean Packet Delay performance form a pair for which this technical specification requires at least one be supported.			
Note 3: Inter-Packet Delay Variation and Packet Delay Range performance form a pair for which this technical specification requires at least one be supported.			

Table 8 Performance Attributes

[R10] The Service Provider **MUST** test the performance attributes as shown in Table 8 for all new IPVCs and all new IPVC EPs being added to existing IPVCs.

[R11] All Delay Performance Attribute calculations **MUST** be based on Packet Delay measurements.

[R12] All Packet Loss Performance Attribute calculations **MUST** be based on Packet Loss measurements.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

10 Service Activation Testing Methodologies

The purpose of Service Activation Testing (SAT) is to validate the configuration and performance of the service. For IP Services, this includes the IPVC, IPVC EP, UNI, and UNI Access Link. The SAT process that is defined for configuration and performance contain subsections or methodologies that define the method used to verify a specific configuration Service Attribute or the performance of a service. The validation of the configuration or performance is performed by sending pre-defined test traffic and verifying the behavior is according to the Service Description. The test methodologies to perform this testing are detailed within this section.

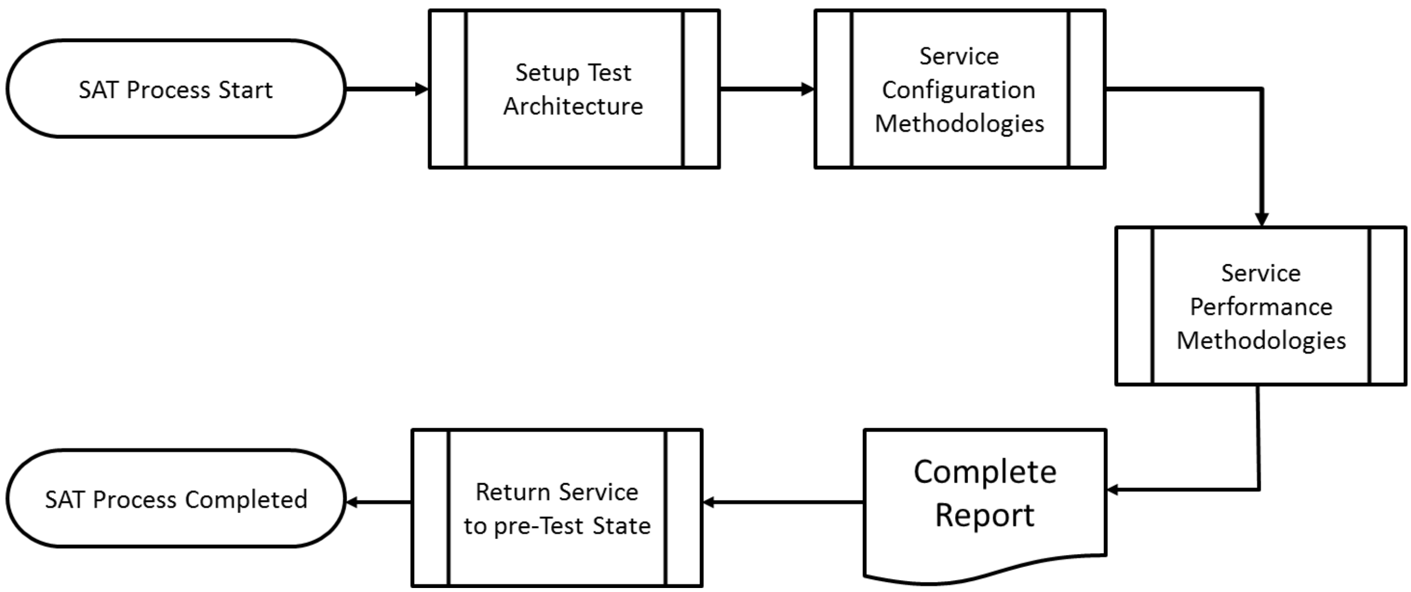

Figure 19 Service Activation Test Process

Figure 19**Error! Reference source not found.** shows a high-level view of the SAT process. It does not contain details on steps to be taken in the event of a test failure. These are discussed later in the document.

The first step in the SAT process is to establish the test architecture. This means creating and activating any IPTEs required to test the service. This process can be done once for the device and not repeated for SAT for each service.

The second step in the SAT process is to perform Service Configuration methodologies. The methodologies define short measurements that are used to verify that the service has been configured as per the Service Description.

The third step in the SAT process is to perform Service Performance methodologies. The performance testing methodology defines a longer term test period that is used to verify if the service meets the SAC.

The fourth step in the SAT process is to report the results of the tests. This report, sometimes called the “birth certificate”, includes the attributes shown in section 9. Both reported and tested

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

attributes are included in the report. A pass or fail indication can be provided with this report and attributes that are tested and fail can be identified.

The fifth and final step in the SAT process is to restore the service to its pre-test configuration. This step is accomplished regardless of whether the tests pass or fail.

SAT within a single Service Provider's network does not require that there be interoperability. The Service Provider can easily determine if the IPTEs are compatible. Since the scope of SAT for IP services is currently a single Service Provider network, interoperability is not a major concern. If/when this scope expands to multiple providers' networks interoperability becomes a major concern. If standardized protocols like TWAMP or STAMP are used to perform the measurements, interoperability is not an issue. If proprietary packet formats or measurement protocols are used, then interoperability becomes a challenge. To be interoperable, both IPTEs need to understand where time stamps, sequence numbers, etc. are located within an IP Packet so that they can perform measurements.

10.1 Common Methodology Requirements

There are some requirements that are common to all test methodologies. These are detailed in the following sections.

10.1.1 Test Packet Format and Length

The packets generated by an IPTE for SAT methodology need to comply with standards so that they are treated similarly to traffic packets.

[R14] An implementation of an IPTE **MUST** generate packets that comply with IETF RFC 791 [3] for IPv4 packets or IETF RFC 8200 [13] for IPv6.

[R15] An implementation of an IPTE **MUST** be able to generate single length packets.

[R16] An implementation of an IPTE **MUST** be configurable to generate packets of a single length within the range of 64-9000 bytes.

[D1] An implementation of an IPTE **SHOULD** be configurable to generate packets of a single length within the range of 9001-16000 bytes.

IETF RFC 6985 [12] describes an IMIX Genome. This RFC describes a pattern of different length packets that is intended to emulate the normal traffic mix on the internet.

a	b	c	d	e	f	g	h	i	j	z
64	128	256	512	1024	1280	1518	2112	9000	16000	MTU

Table 9 IMIX Values

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

The numerical values in Table 9 represent IP Packet lengths in bytes. Using the values in Table 9 a test pattern can be specified with different length packets sent. As an example aaagg specifies a pattern of 64 64 64 1518 1518 byte packets. This pattern is repeated for the duration of the test.

[D2] An implementation of an IPTE **SHOULD** support the use of an IMIX for variable length packets as specified in IETF RFC 6985 [12].

[CR1]< [D2] Packet lengths specified in IETF RFC 6985 section 4 **MUST** be supported.

Note: these IP Packet lengths are shown in Table 9.

Packet lengths other than those specified in IETF RFC 6985 section 4 can be supported by an IPTE implementation.

[CR2]< [D2] An implementation of an IPTE supporting an IMIX **MUST** support a repeating pattern of up to eight different IP Packet lengths.

[CD1]< [D2] An implementation of an IPTE supporting an IMIX **SHOULD** support a repeating pattern of up to 32 different IP Packet lengths.

[CR3]< [D2] An implementation of an IPTE **MUST** repeat the variable length pattern as long as necessary during the test procedure from the first to the last IP Packet length starting at the beginning of each test procedure.

[CD2]< [D2] The default IMIX pattern **SHOULD** be a pattern of IP Packet lengths of abcdefgh.

10.1.2 Common IP Test Equipment Requirements

As previously discussed, there are three types of IP test equipment that can be used to complete SAT. These are the IPTE-I, the IPTE-A, and the IPTE-TH. While the packaging and interfaces to these IPTEs can be different, there are some requirements that are common across all of these devices. These requirements are discussed in this section.

[R17] An IPTE implementation **MUST** support measurement of one-way Packet Delay and a count of sent and received test packets.

[R18] An IPTE implementation **MUST** support the calculation of one-way Packet Delay Percentile, one-way MPD, one-way IPDV, one-way PDR, PLR and IR.

[D3] An IPTE implementation **SHOULD** be capable of generating and receiving packets on multiple flows in an envelope at the same time.

The delay performance metrics defined in MEF 61 [24] use a percentile of packets measured over a period of time T. The method used by a particular IPTE implementation (timestamp location, packet format, etc.) to perform delay measurements is outside the scope of this document.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

The goal of SAT is to reproduce IP Data Packets behavior in the network. To accomplish this, test packets are sent in both directions between two IPTEs simultaneously. It is understood that starting or stopping the generation of packets between two different IPTEs at the same instant in time is difficult if not impossible. For this reason, the word simultaneously means within the same 2 second period within the context of this document.

[R19] SAT **MUST** be performed in both the forward and backward directions between two IPTEs simultaneously.

10.1.3 Test Measurements

Test measurements are performed from the Controller end of the service to the Responder end of the service and from the Responder end of the service to the Controller end of the service. The Controller end initiates the Test measurement. The Responder end either processes the packet and then sends it to the Controller or simply swaps the source and destination addresses and sends it to the Controller. The Controller then processes the packet that is received from the Responder. Examples are shown in Figure x.

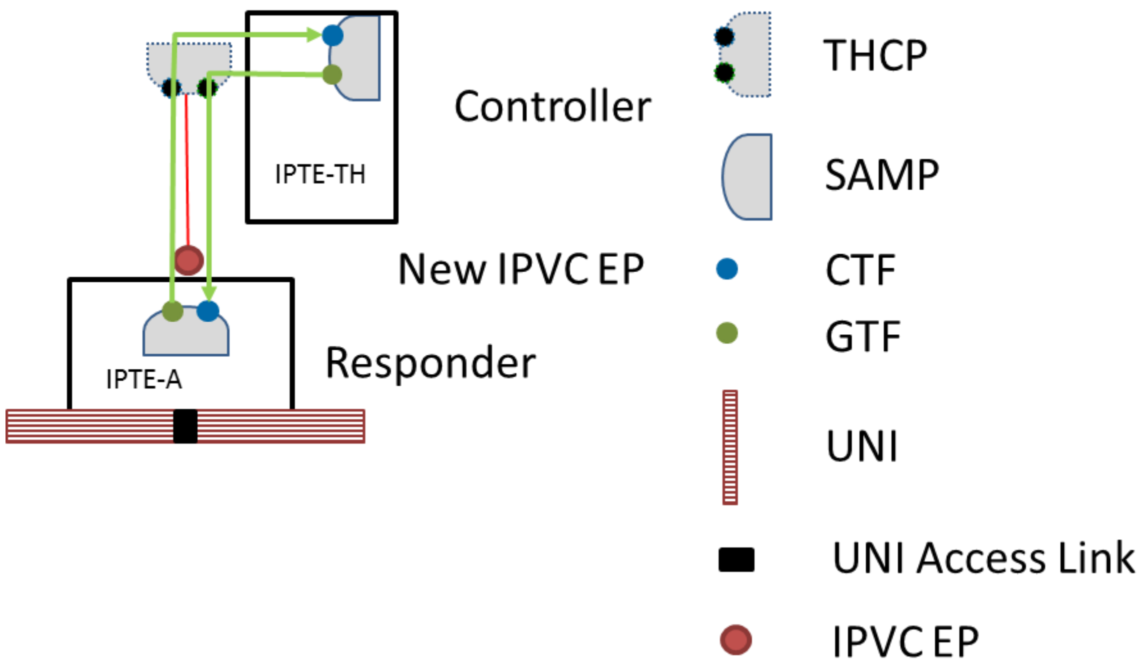

Figure 20 Responder Processing Packet

Figure 20 shows an example of an IPTE-TH as a Controller and an IPTE-A as a Responder testing a new IPVC EP. The IPTE-TH generates IP Data Service test packets. The IPTE-A receives these and processes these. This processing might include adding time stamps when the packets are received and transmitted, adding sequence numbers to measure packet loss, or other mechanisms that might be useful by IPTE vendors. When this type of packet processing is performed by the Responder, one-way measurements are possible in the Forward (Controller to Responder) and Backward (Responder to Controller) directions. Two-way measurements (Controller to Controller) are also possible if desired.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

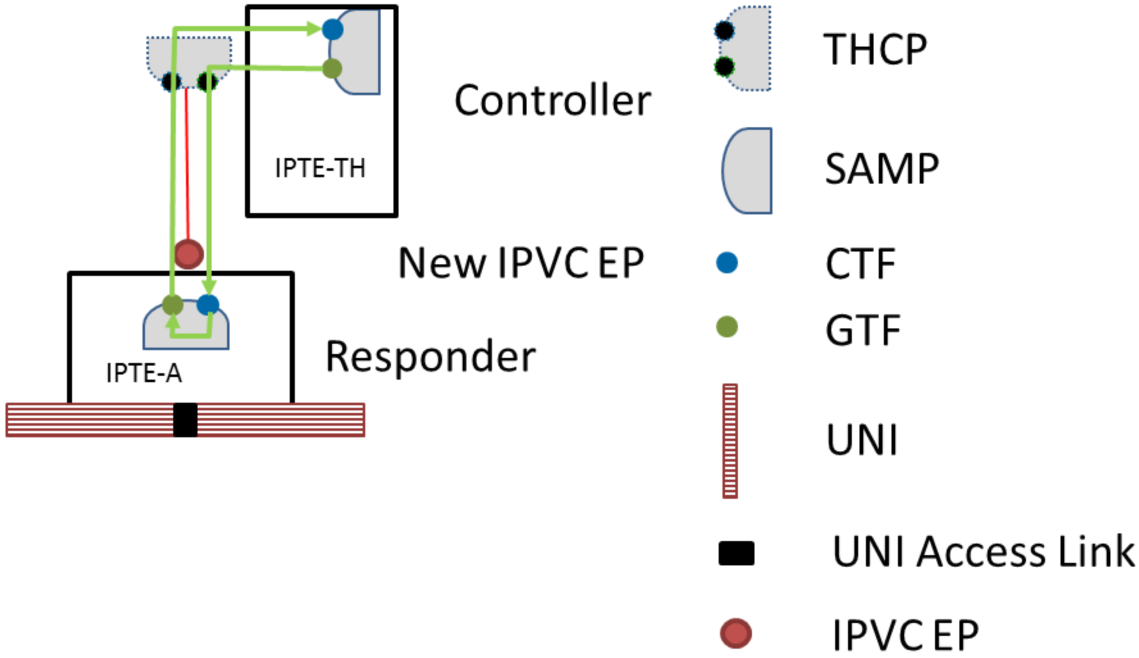

Figure 21 Responder Looping Back Packet

Figure 21 shows an example of the same test configuration with the IPTE-A Responder simply looping back the IP Data Service test packets. The IPTE-A does not process these packets in any way except to swap the source and destination IP Address and Ports. This simple functionality in the IPTE-A might be due to limited functionality in the IPTE-A or in incompatible test packet formats between the IPTE-TH and the IPTE-A. In this case only two-way (Controller to Controller) measurements are possible.

The ability to perform accurate one-way packet delay measurements without Time of Day (ToD) clock synchronization can be difficult. ToD clock differences can lead to measurements that result in negative delay or excessive delay. It is recommended that these issues be taken into account when deciding what type delay measurements and delay Service Attributes are used in SAT.

To overcome this, two-way Packet Delay and Packet Loss measurements are performed and the results are divided in half to obtain approximated one-way Packet Delay and Packet Loss measurements. This is acceptable as long as the results indicate that this was how the one-way Packet Delay and Packet Loss measurement was determined.

[R20] An IPTE implementation acting as a Controller end **MUST** perform one-way Packet Delay and Packet Loss measurements.

[R21] An IPTE implementation acting as a Controller end **MUST** calculate one-way Performance Attributes as shown in section 9.2.

[D4] An IPTE implementation acting as a Controller end **SHOULD** perform two-way Packet Delay measurements.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

[R22] Where two-way Packet Delay measurements are performed and one-way Packet Delay results are reported the results **MUST** indicate that the result was measured as two-way.

[R23] An IPTE implementation acting as a Responder end **MUST** either process IP Data Service test packets as shown in Figure 20 or loopback IP Data Service test packets as shown in Figure 21.

The methods used by the IPTE implementation acting as a Responder are beyond the scope of this document.

10.2 Service Acceptance Criteria

Service Acceptance Criteria (SAC) are used to determine if a test passes or fails. SAC are agreed to by the Subscriber and the Service Provider. As discussed in section 7, SAC are defined for short periods of time, versus a 30 day period that can be used for an SLS.

A SAC is specified for each tested Service Attribute and direction of a test. SAC are for the Forward and Backward directions of a service do not have to be the same for both directions although they are normally. The value specified for a SAC is defined to ensure that the Service Attribute being measured meets Subscriber expectations. Due to the shorter duration measurements used by SAT, a direct correlation between SLS values and SAC values does not need to be done. Examples of SAC that can be used for Configuration or Performance tests are IR_{SAC}, PD/MPD_{SAC}, $IPDV/PDR_{SAC}$, and $PLR_{SAC.}$ The use of these SAC are shown in the test methodologies in section 10.3 and 10.4.

[R24] A SAC **MUST** be defined for each Service Attribute that is tested.

[R25] The SAC **MUST** be agreed to by the Subscriber and Service Provider.

10.3 Service Configuration Tests

Service configuration tests are performed to verify that the IP Service has been correctly configured and that tested Service Attributes are set per the service agreement between the Subscriber and the Service Provider. Service configuration tests are normally of a short duration, long enough to verify that the Service Attribute is correctly configured but not so long that they make the SAT a time intensive exercise. Normally configuration tests are performed for a period of 30 seconds or less.

Service configuration tests include tests on the configuration of the IPVC, the IPVC EP, the UNI, and the UNI Access Link. There are no UNI configuration tests. The UNI Access Link configuration tests include two sub-processes, UNI Access Link BFD and UNI Access Link IP MTU. The IPVC configuration tests include four sub-processes, IPVC DSCP Preservation, IPVC MTU, IPVC Path MTU Discovery, and IPVC Fragmentation. The IPVC EP configuration tests include two sub-processes, IPVC EP Prefix Mapping, IPVC EP Ingress and Egress Bandwidth Profile.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

MEF 61 [24] states that there is no direct correlation between an IPVC and IPVC EP and an UNI Access Link. For this reason, the service configuration tests for an IPVC and IPVC EP and an UNI Access Link are not linked to one another.

Service configuration tests are performed on a UNI at the time it is activated. Service configuration tests are performed on an UNI Access Link at the time that it is activated as described in section 7.2. The service configuration tests are performed on an IPVC and IPVC EP at the time they are activated as described in section 7.2. If the UNI, the UNI Access Link, the IPVC, and IPVC EP are being activated at the same time, it is suggested that the UNI and the UNI Access Link are tested first.

Figure 22, Figure 23, and Figure 24 show high level views of the service configuration test processes. The order that these test processes appear in the figures is the recommended order that they be performed.

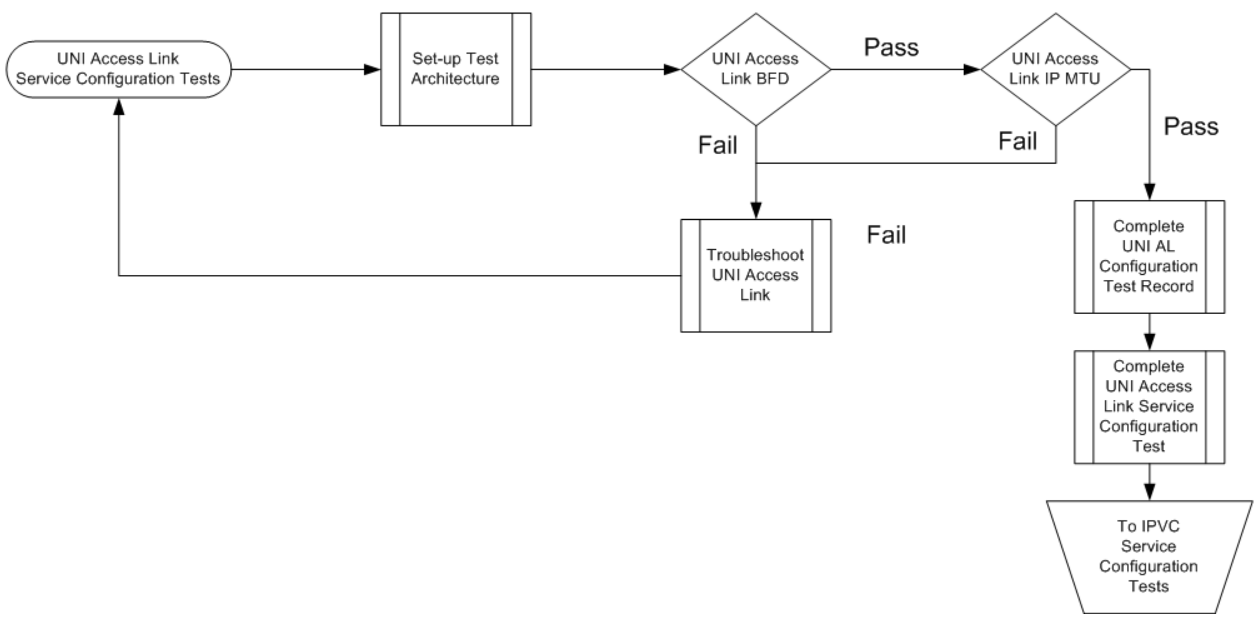

Figure 22 UNI Access Link Service Configuration Tests

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

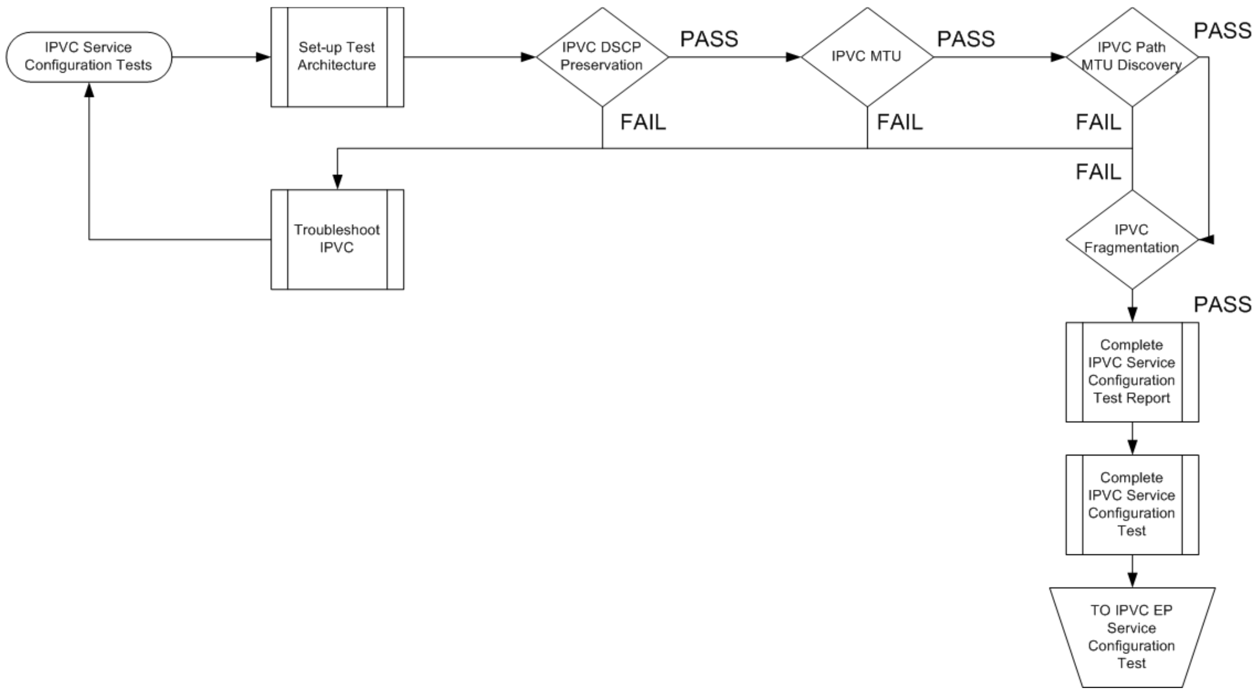

Figure 23 IPVC Service Configuration Tests

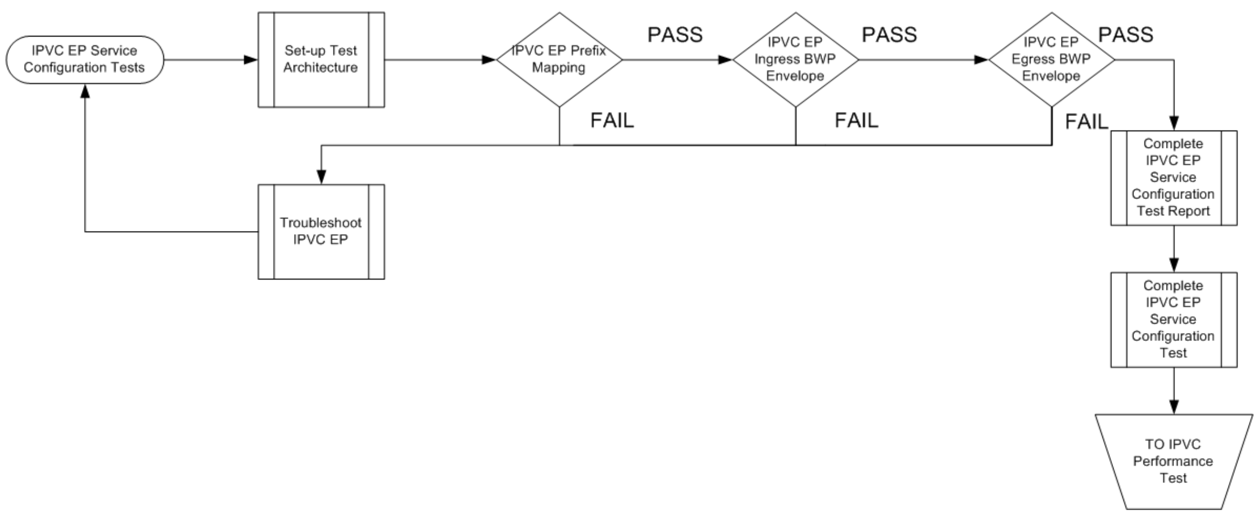

Figure 24 IPVC EP Service Configuration Tests

10.3.1 UNI Access Link Service Configuration Test

The UNI Access Link Service Configuration test methodologies are included in the following sections. UNI Access Link Service Configuration tests are performed when a UNI Access Link is initially configured after the UNI has been activated. Figure 9, Figure 10, Figure 11, Figure 12, and Figure 13 show the configuration used to test the UNI Access Link.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

10.3.1.1 UNI Access Link BFD Service Provider Active

The correct operation of BFD on the UNI Access Link when the Service Provider is Active is verified with this test methodology.

[R26] If the UNI Access Link BFD Service Attribute is not *None* and the Active End Service Attribute is *SP* or *Both* the UNI Access Link BFD Service Attribute **MUST** be tested as specified in Table 10.

Service Activation Test Methodology	
Test Name	UNI Access Link BFD
Test Type	Service Activation
Service Type	IP UNI Access Link
Test Status	Mandatory if UNI Access Link BFD Service Attribute is not *None* and the Active End Service Attribute is *SP* or *Both*
Test Objective	Verify that if the UNI Access Link BFD attribute is not *None* that the following are configured correctly in the Service Provider's equipment: • Connection Address Family • Transmission Interval • Detect Multiplier • Active End • Authentication Type
Test Procedure	• $IPTE_1$ located within SP network takes on the Active role of a BFD session as defined in IETF RFC 5880 [10] and sends BFD Control Packets encapsulated within IPv4 packets (when Connection Address Family = *IPv4* or *Both*) using attributes as defined in the service definition to the device (either Subscriber CE or Service Provider IPTE-I) at the Subscriber end of the UNI Access Link when Active End = *SP*. • $IPTE_1$ sends BFD Control Packets for period T_{BFD} or until the BFD session state is *Up* as defined in IETF RFC 5880 [10] . • $IPTE_1$ located within the SP network takes on the Active role of a BFD session as defined in IETF RFC 5880 [10] and sends BFD

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

	Control Packets encapsulated within IPv6 packets (when Connection Address Family = *IPv6* or *Both*) using attributes as defined in the service definition to the device (either Subscriber CE or Service Provider IPTE-I) at the Subscriber end of the UNI Access Link when Active End = *SP*. • IPTE$_1$ sends BFD Control Packets for period T_{BFD} or until the BFD session state is *Up* as defined in IETF RFC 5880 [10].
Variables	Connection Address Family, Transmission Interval, Detect Multiplier, Active End, Authentication Type, BFD Session State, T_{BFD}
Results	Pass = BFD session is UP with transmission interval and detect multiplier as per the service definition. Fail = BFD session is not up when T_{BFD} expires or the transmission interval or detect multiplier is not as per the service definition.
Remarks	**1.** This test does not use PL or PLR as a unit. Instead it uses the BFD session state of UP and the correct transmission interval and detect multiplier as the indicators of the test. **2.** This testing is only possible if there is a device connected to the UNI that is acting as a BFD peer. **3.** Testing is done for IPv4, IPv6, or Both depending on the value of Connection Address Family

Table 10 UNI Access Link BFD Test Methodology

[R27] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R28] The methodology **MUST** report the state of the Connection Address Family, BFD session, Active End, and T_{BFD}.

[R29] The methodology **MUST** report pass or fail for the methodology.

10.3.1.2 UNI Access Link BFD Subscriber Active

The correct operation of BFD on the UNI Access Link when the Subscriber is Active is verified with this test methodology.

[R30] If the UNI Access Link BFD Service Attribute is not *None* and the Active End Service Attribute is *Subscriber* the UNI Access Link BFD Service Attribute **MUST** be tested as specified in Table 11.

Service Activation Test Methodology

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Test Name	UNI Access Link BFD
Test Type	Service Activation
Service Type	IP UNI Access Link
Test Status	Mandatory if UNI Access Link BFD Service Attribute is not *None* and Active End Service Attribute is *Subscriber*
Test Objective	Verify that if the UNI Access Link BFD attribute is not *None* that the following are configured correctly in the Service Provider's equipment: • Connection Address Family • Transmission Interval • Detect Multiplier • Active End • Authentication Type
Test Procedure	• $IPTE_1$ located within the Service Provider network takes on the Passive role of a BFD session as defined in IETF RFC 5880 [10] and waits for BFD Control Packets from device (either Subscriber CE or Service Provider IPTE-I) at the Subscriber end of the UNI Access Link encapsulated in IPv4 (when Connection Address Family = IPv4 or Both) packets using attributes as defined in the service definition from the device at the Subscriber end of the UNI Access Link when Active End = Subscriber. • $IPTE_1$ waits for BFD Control Packets for period T_{BFD}, for a predetermined time, or until the BFD session state is *Up* as defined in IETF RFC 5880 [10]. • $IPTE_1$ located within the Service Provider network takes on the Passive role of a BFD session as defined in IETF RFC 5880 [10] and waits for BFD Control Packets from device (either Subscriber CE or Service Provider IPTE-I) at the Subscriber end of the UNI Access Link encapsulated in IPv6 (when Connection Address Family = IPv6 or Both) packets using attributes as defined in the service definition from the device at the Subscriber end of the UNI Access Link when Active End = Subscriber. • $IPTE_1$ waits for BFD Control Packets for period T_{BFD}, for a predetermined time, or until the BFD session state is *Up* as defined in IETF RFC 5880 [10].

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Variables	Connection Address Family, Transmission Interval, Detect Multiplier, Active End, Authentication Type, BFD Session State, T_{BFD}
Results	Pass = BFD session is up with transmission interval and detect multiplier as per the service definition. Fail = BFD session is not up when T_{BFD} expires or the transmission interval or detect multiplier is not as per the service definition.
Remarks	**1.** This test does not use PL or PLR as a unit. Instead it uses the BFD session state of UP and the correct transmission interval and detect multiplier as the indicators of the test. **2.** This testing is only possible if a device is connected to the UNI and is acting as a BFD peer. **3.** Testing is done for IPv4, IPv6, or Both depending on the value of Connection Address Family

Table 11 UNI Access Link BFD Test Methodology

[R31] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R32] The methodology **MUST** report the state of the Connection Address Family, BFD session, Active End, and T_{BFD}.

[R33] The methodology **MUST** report pass or fail for the methodology.

10.3.1.3 UNI Access Link IP MTU

The correct configuration of the UNI Access Link IP MTU is verified with this test methodology. Testing this is optional for a new UNI Access Link if there is one or more existing UNI Access Links on the UNI. Testing the new UNI Access Link IP MTU might impact the services on the existing UNI Access Links so the testing has been made optional. If there are no IPVC EPs active on the UNI or downtime can be arranged with the Subscriber testing could be performed. Otherwise it is recommended that testing the new UNI AL not be performed.

[R34] The UNI Access Link IP MTU Service Attribute value **MUST** be verified as described in Table 12.

Service Activation Test Methodology	
Test Name	UNI Access Link IP MTU
Test Type	Service Activation
Service Type	IP UNI Access Link

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Test Status	Optional for new UNI AL
Test Objective	Verify that the UNI Access Link IP MTU attribute is configured correctly.
Test Procedure	• $IPTE_1$ offers IP Data Service packets with the DA of $IPTE_2$ as per the Service Definition with a length equal to the UNI AL IP MTU at EI_1 with a rate up to IR_{SC} and for a time T_{SC} as specified by the Service Provider. • $IPTE_2$ verifies that the packets offered at EI_1 are received as defined in the Service Definition at EI_2. Packet Loss is acceptable up to PLR_{SAC}, where PLR_{SAC} is the SAC for Packet Loss Ratio. • Simultaneously, $IPTE_2$ offers IP Data Service packets with the DA of $IPTE_1$ as per the Service Definition with a length equal to the UNI AL IP MTU at EI_2 with a rate up to IR_{SC} and for a time T_{SC} as specified by the Service Provider. • $IPTE_1$ verifies that the packets offered at EI_2 are received as defined in the Service Definition at EI_1. Packet Loss is acceptable up to PLR_{SAC}, where PLR_{SAC} is the SAC for Packet Loss Ratio.
Variables	DA, IPVC MTU, IR_{SC}, T_{SC}, PL, and PLR_{SAC}
Results	Pass, Fail
Remarks	**1.** Testing is only possible if an IPVC is configured on the UNI. **2.** A range of IP Data Service packet lengths starting as small as 68B and increasing to the maximum length desired can be used instead of a single length **3.** This testing is only possible if there is an IPTE at the Subscriber end of the UNI. This could be an IPTE-A in the CE or an IPTE-I connected to the UNI.

Table 12 UNI Access Link IP MTU Test Methodology

[R35] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R36] The methodology **MUST** report the UNI AL IP MTU used for test packets.

[R37] The methodology **MUST** report the IR_{SC} and T_{SC} used for the test.

[R38] The methodology **MUST** report the PL result for the test.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

[R39] The methodology **MUST** report pass or fail for the test.

10.3.2 IPVC Configuration Tests

The IPVC Configuration test methodologies are included in the following sections. IPVC Configuration tests are performed when an IPVC is initially configured after the UNI and/or UNI Access Link has been activated. Use Cases 1-6 show examples of when these test methodologies are used. See Table 6 for more detail on which test methodologies are used for new IPVCs versus when new IPVC EPs are added to existing IPVCs.

10.3.2.1 IPVC DSCP Preservation

The correct configuration of the IPVC DSCP Preservation is verified with this test methodology.

[R40] The IPVC DSCP Preservation **MUST** be verified as described in Table 13 when IPVC DSCP Preservation is *Enabled*.

Service Activation Test Methodology	
Test Name	IPVC DSCP Preservation
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory when *Enabled*
Test Objective	Verify that the IPVC DSCP Preservation attribute is configured correctly.
Test Procedure	• $IPTE_1$ offers IP Data Service packets with the DA of $IPTE_2$ as per the Service Definition at EI_1 with a rate equal to IR_{SC} for a time T_{SC} and with a DSCP value in the below list. • $IPTE_2$ verifies that the packets received at EI_2 have the same DSCP as was offered at EI_1. An IP Data Service packet received with an incorrect DSCP value is considered lost. Packet Loss is acceptable up to PLR_{SAC}, where PLR_{SAC} is the SAC for Packet Loss Ratio. Note: The method used to communicate the DSCP value between $IPTE_1$ and $IPTE_2$ is beyond the scope of this document. • Simultaneously, $IPTE_2$ offers IP Data Service packets with the DA of $IPTE_1$ as per the Service Definition at EI_2 with a rate equal to IR_{SC} for a time T_{SC} and with the same DSCP value as bullet 1. • $IPTE_1$ verifies that the packets received at EI_1 have the same DSCP as was offered at EI_2. An IP Data Service packet received

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

	with an incorrect DSCP is considered lost. Packet Loss is acceptable up to PLR_{SAC}, where PLR_{SAC} is the SAC for Packet Loss Ratio. Note: The method used to communicate the DSCP value between $IPTE_1$ and $IPTE_2$ is beyond the scope of this document. • The above is repeated for each DSCP value that is included in the list for the IPVC that is agreed to by the Service Provider and Subscriber.
Variables	List of DSCP values, IR_{SC}, T_{SC}, PLR_{SAC}
Results	Pass or fail
Remarks	**1.** The DSCP value in packets is set per the Service Definition and is maintained in received packets for the test to pass. **2.** At minimum a sample of the 64 DSCP values is tested. The SP and Subscriber can determine how large a sample is sufficient to test. **3.** Figure 14, Figure 16, and Figure 18 show the SAMP location needed at each end of this Test Methodology to ensure that any DSCP manipulation points are included in the test. **4.** PLR_{SAC} for this test is recommended to be set at 0%.

Table 13 IPVC DSCP Preservation Test Methodology

[R41] The methodology **MUST** report the DSCP value(s) of test packets used in this methodology.

[R42] The methodology **MUST** report the IR_{SC} and T_{SC} used for the test.

[R43] The methodology **MUST** report the PL result for the test.

[R44] The methodology **MUST** report pass or fail for the test.

10.3.2.2 IPVC MTU

The correct configuration of the IPVC MTU is verified with this test methodology.

[R45] The IPVC MTU **MUST** be verified as described in Table 14.

Service Activation Test Methodology	
Test Name	IPVC MTU
Test Type	Service Activation

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Service Type	IPVC
Test Status	Mandatory for new IPVC, Mandatory for new IPVC EP on new UNI, Optional for new IPVC EP on UNI with existing IPVCs
Test Objective	Verify that the IPVC MTU attribute is configured correctly.
Test Procedure	• $IPTE_1$ offers IP Data Service packets with the DA of $IPTE_2$ as per the Service Definition with a length equal to the IPVC MTU at EI_1 with a rate equal to IR_{SC} and for a time T_{SC} as specified by the Service Provider. • $IPTE_2$ verifies that the packets offered at EI_1 are received as defined in the Service Definition at EI_2. Packet Loss is acceptable up to PLR_{SAC}, where PLR_{SAC} is the SAC for Packet Loss Ratio. • Simultaneously, $IPTE_2$ offers IP Data Service packets with the DA of $IPTE_1$ as per the Service Definition with a length equal to the IPVC MTU at EI_2 with a rate equal to IR_{SC} and for a time T_{SC} as specified by the Service Provider. • $IPTE_1$ verifies that the packets offered at EI_2 are received as defined in the Service Definition at EI_1. Packet Loss is acceptable up to PLR_{SAC}, where PLR_{SAC} is the SAC for Packet Loss Ratio.
Variables	IPVC MTU, IR_{SC}, Tsc, and PLR_{SAC}
Results	Pass, Fail
Remarks	**1.** A range of IP Data Service packet lengths starting as small as 68B and increasing to the maximum length desired can be used instead of a single length

Table 14 IPVC MTU Test Methodology

[R46] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R47] The methodology **MUST** report the IPVC MTU length of test packets used for the test.

[R48] The methodology **MUST** report the IR_{SC} and T_{SC} used for the test.

[R49] The methodology **MUST** report the PL result for the test.

[R50] The methodology **MUST** report pass or fail for the test.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

10.3.2.3 IPVC Path MTU Discovery

The correct configuration of the IPVC Path MTU Discovery attribute is verified with this test methodology.

[R51] The IPVC Path MTU Discovery attribute **MUST** be verified as described in Table 15 when *Enabled*.

Service Activation Test Methodology	
Test Name	IPVC Path MTU Discovery
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory for new IPVC when *Enabled*
Test Objective	Verify that the IPVC Path MTU Discovery attribute is configured correctly.
Test Procedure	• $IPTE_1$ offers IP Data Service packets with the DA of $IPTE_2$ in excess by 10% of the largest UNI AL IP MTU for UNIs in the IPVC with the DF bit set at rate IR_{SC} for period T_{SC}. • $IPTE_1$ collects ICMP Datagram Too Big messages for IPv4 or Packet Too Big messages for IPv6 received from the Service Provider network. If any messages are received test passes. If no messages are received the test fails. • Simultaneously, $IPTE_2$ offers IP Data Service packets with the DA of $IPTE_1$ in excess by 10% of the largest UNI AL IP MTU for UNIs in the IPVC with the DF bit set at rate IR_{SC} for period T_{SC}. • $IPTE_2$ collects ICMP Datagram Too Big messages for IPv4 or Packet Too Big messages for IPv6 received from the Service Provider network. If any messages are received test passes. If no messages are received the test fails.
Variables	IR_{SC}, T_{SC}, DA, ICMP messages
Results	Pass = Appropriate ICMP message received from SP network during time T_{SC} Fail = No ICMP message received from SP network during time T_{SC} for

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

	any IP Data Service packet size
Remarks	

Table 15 IPVC Path MTU Discovery Test Methodology

[R52] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R53] The methodology **MUST** report the length of test packets used for the test.

[R54] The methodology **MUST** report the IR_{SC} and T_{SC} used for the test.

[R55] The methodology **MUST** report the number of appropriate ICMP messages received for the test.

[R56] The methodology **MUST** report pass or fail for the test.

10.3.2.4 IPVC Fragmentation

The correct configuration of the IPVC Fragmentation attribute is verified with this methodology.

[R57] The IPVC Fragmentation attribute **MUST** be verified as described in Table 16.

Service Activation Test Methodology	
Test Name	IPVC Fragmentation
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory when *Disabled*
Test Objective	Verify that the IPVC Fragmentation Service Attribute is configured correctly.
Test Procedure	• $IPTE_1$ offers at EI_1 IP Data Service packets with the DA of $IPTE_2$ of a length 15% greater than the IPVC MTU with a rate equal to IR_{SC} for a time of T_{SC}. • $IPTE_2$ verifies at EI_2 that no fragmented IP Data Service packets are be received. • Simultaneously $IPTE_2$ offers at EI_2 IP Data Service packets with

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

	the DA of $IPTE_1$ of a length 15% greater than the IPVC MTU with a rate equal to IR_{SC} for a time of T_{SC}. • $IPTE_1$ verifies at EI_1 that no fragmented IP Data Service packets are be received.
Variables	IR_{SC}, T_{SC}, PLR_{SAC}, DA
Results	Pass = IP Data Service packets received with no fragmented packets received Fail = Any fragmented IP Data Service packets received during T_{SC}
Remarks	**1.** The Pass condition of no fragmented packets received includes no IP Data Service packets received. MEF 61 [24] allows packets greater than the MTU to be passed, fragmented, or discarded. If no packets are received they might have been discarded which means that the behavior is correct.

Table 16 IPVC Fragmentation Test Methodology

[R58] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R59] The methodology **MUST** report the length of test packets used for the test.

[R60] The methodology **MUST** report the IR_{SC} and T_{SC} used for the test.

[R61] The methodology **MUST** report the number of fragmented packets received.

[R62] The methodology **MUST** report pass or fail for the test.

10.3.3 IPVC EP Configuration Tests

The IPVC EP Configuration test methodologies are included in the following sections. IPVC EP Configuration tests are performed when an IPVC EP is initially configured after the IPVC has been tested. Use Cases 1-6 show examples of when these test methodologies are used. See Table 7 for more detail on which test methodologies are used for new IPVCs versus when new IPVC EPs are added to existing IPVCs.

10.3.3.1 IPVC EP Prefix Mapping

The correct configuration of the IPVC EP Prefix Mapping Service Attribute is verified with this test methodology.

[R63] The IPVC EP Prefix Mapping Service Attribute **MUST** be verified as described in Table 17.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Service Activation Test Methodology	
Test Name	IPVC EP Prefix Mapping
Test Type	Service Activation
Service Type	IPVC EP
Test Status	Mandatory when IPVC EP Prefix Mapping list in non-empty
Test Objective	Verify that the IPVC EP Prefix Mapping Service Attribute is configured correctly.
Test Procedure	• $IPTE_1$ offers IP Data Service packets with the DA for $IPTE_2$ at EI_1 at rate IR_{SC} for time T_{SC} using a SA for $IPTE_1$ that is not on the IPVC EP Prefix Mapping list. • $IPTE_2$ counts IP Data Service packets received at EI_2 from $IPTE_1$ for time T_{SC} and calculates PLR. • $IPTE_1$ then offers IP Data Service packets with the DA for $IPTE_2$ at EI_1 at rate IR_{SC} for time T_{SC} using a SA for $IPTE_1$ that is on the IPVC EP Prefix Mapping list. • $IPTE_2$ counts IP Data Service packets received at EI_2 from $IPTE_1$ for time T_{SC} and calculates PLR. • $IPTE_2$ then offers IP Data Service packets at EI_2 at rate IR_{SC} for time T_{SC} using a DA for $IPTE_1$ that is on the IPVC EP Prefix Mapping list. • $IPTE_1$ counts IP Data Service packets received at EI_1 from $IPTE_2$ for time T_{SC} and calculates PLR. • $IPTE_2$ then offers IP Data Service packets at EI_2 at rate IR_{SC} for time T_{SC} using a DA for $IPTE_1$ that is not on the IPVC EP Prefix Mapping list. • $IPTE_1$ counts IP Data Service packets received at EI_1 from $IPTE_2$ for time T_{SC} and calculates PLR.
Variables	IR_{SC}, T_{SC}, PLR_{SAC}, SA, DA
Results	Pass = From $IPTE_1$ to $IPTE_2$ with SA not in list PLR = 100% From $IPTE_1$ to $IPTE_2$ with SA in list PLR $\geq$ PLR_{SAC}

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

	From $IPTE_2$ to $IPTE_1$ with DA in list PLR ≥ PLR_{SAC} From $IPTE_2$ to $IPTE_1$ with DA not in list PLR = 100% Fail = From $IPTE_1$ to $IPTE_2$ with SA not in list PLR < 100% From $IPTE_1$ to $IPTE_2$ with SA in list PLR ≥ PLR_{SAC} From $IPTE_2$ to $IPTE_1$ with DA in list PLR ≥ PLR_{SAC} From $IPTE_2$ to $IPTE_1$ with DA not in list PLR < 100%
Remarks	

Table 17 IPVC EP Profile Mapping Test Methodology

[R64] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R65] The methodology **MUST** report the length of test packets used for the test.

[R66] The methodology **MUST** report the IR_{SC} and T_{SC} used for the test.

[R67] The methodology **MUST** report the SA and/or DA used for each step.

[R68] The methodology **MUST** report the number of packets received and the PL.

[R69] The methodology **MUST** report pass or fail for the test.

10.3.3.2 IPVC EP Ingress BWP Envelope

There are three tests that are performed to verify the IPVC EP Ingress BWP Envelope. The aggregate bandwidth of all flows within the envelope is tested, the bandwidth of each flow within the envelope is tested, the bandwidth of each flow simultaneously is tested. The test methodology for each of these is shown in the following sections.

10.3.3.2.1 IPVC EP Ingress BWP Envelope Aggregate Methodology

The correct configuration of the aggregate of all flows within the IPVC EP Ingress BWP Envelope attribute is verified with this test methodology.

[R70] The aggregate of all flows within the IPVC EP Ingress BWP Envelope attribute **MUST** be verified as described in Table 18.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Service Activation Test Methodology	
Test Name	IPVC EP Ingress BWP Envelope aggregate
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory if IPVC EP Ingress BWP Envelope not *None*
Test Objective	Verify that the IPVC EP Ingress BWP Envelope aggregate attribute is configured correctly.
Test Procedure	• $IPTE_1$ offers IP Data Service packets with the DA of $IPTE_2$ and a rate equal to $MaxIR_E$ for a time T_{SC} at EI_1 in accordance with the service description. • $IPTE_2$ counts the number of IP Data Service packets received at EI_2 determining the PL and measuring the *PLR*. Packet loss is acceptable up to PLR_{SAC}.
Variables	DA, $MaxIR_E$, T_{SC}, PL, PLR_{SAC}
Results	Pass = Packet loss is within $\mathrm{PLR}_{\mathrm{SAC}}$ Fail = Packet loss is not within $\mathrm{PLR}_{\mathrm{SAC}}$
Remarks	**1.** Ingress BWP Envelope test includes total aggregate information rate of traffic across all BWP Flows in the Envelope.

Table 18 IPVC Ingress BWP Envelope Aggregate Test Methodology

[R71] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R72] The methodology **MUST** report the length of test packets used for the test.

[R73] The methodology **MUST** report the $MAXIR_E$ and T_{SC} used for the test.

[R74] The methodology **MUST** report the PL.

[R75] The methodology **MUST** report pass or fail for the test.

10.3.3.2.2 IPVC EP Ingress BWP Envelope per Flow

The correct configuration of each flow within the IPVC EP Ingress BWP Envelope is verified using this test methodology.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

[R76] Each flow within the IPVC EP Ingress BWP Envelope **MUST** be verified as described in Table 19.

Service Activation Test Methodology	
Test Name	IPVC EP Ingress BWP Envelope per Flow
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory if IPVC EP Ingress BWP Envelope not *None*
Test Objective	Verify that the IPVC EP Ingress BWP Envelope attribute is configured correctly for each flow within the Envelope.
Test Procedure	• $IPTE_1$ offers IP Data Service packets with the DA of $IPTE_2$, a CoS marking equal to the IPVC EP Ingress Class of Service Map for the flow, a rate equal to $MaxIR_i$ for a time T_{SC} at EI_1 in accordance with the service description. • $IPTE_2$ counts the number of IP Data Service packets received at EI_2 determining the PL and measuring the *PLR*. Packet loss is acceptable up to PLR_{SAC}. • This is repeated for flows 1..n in the envelope.
Variables	DA, CoS Map, $MaxIR_i$, T_{SC}, PL, PLR_{SAC}
Results	Pass = Packet loss is within $\mathrm{PLR}_{\mathrm{SAC}}$ Fail = Packet loss is not within $\mathrm{PLR}_{\mathrm{SAC}}$
Remarks	**1.** A failure of any flow in the envelope represents a failure of all flows in the envelope.

Table 19 IPVC Ingress BWP Envelope per Flow Test Methodology

[R77] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R78] The methodology **MUST** report the length of test packets used for the test.

[R79] The methodology **MUST** report the $MAXIR_i$ and T_{SC} used for the test.

[R80] The methodology **MUST** report the PL.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

[R81] The methodology **MUST** report pass or fail for the test.

10.3.3.2.3 IPVC EP Ingress BWP Envelope All Flows Simultaneously

The correct configuration of all flows simultaneously within the IPVC EP Ingress BWP Envelope is verified using this test methodology.

[R82] All flows within the IPVC EP Ingress BWP Envelope **MUST** be verified simultaneously as described in Table 21.

Service Activation Test Methodology	
Test Name	IPVC EP Ingress BWP Envelope all Flows simultaneously
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory if IPVC EP Ingress BWP Envelope not *None*
Test Objective	Verify that the IPVC EP Ingress BWP Envelope attribute is configured correctly for all flows within the Envelope.
Test Procedure	• $IPTE_1$ offers IP Data Service packets with the DA of $IPTE_2$, a CoS marking equal to the IPVC EP Ingress Class of Service Map for each flow within the envelope simultaneously, a rate equal to $MaxIR_i$ for each flow, for a time T_{SC} at EI_1 in accordance with the service description. • $IPTE_2$ counts the number of IP Data Service packets received at EI_2 for each flow within the envelope determining the PL and calculating the *PLR*. Packet loss is acceptable up to PLR_{SAC}.
Variables	DA, CoS Map, $MaxIR_i$, T_{SC}, PL, PLR_{SAC}
Results	Pass = Packet loss is within PLR_{SAC} Fail = Packet loss is not within PLR_{SAC}
Remarks	**1.** A failure of any flow in the envelope represents a failure of all flows in the envelope.

Table 20 IPVC Ingress BWP Envelope for all Flows within the Envelope Test Methodology

[R83] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R84] The methodology **MUST** report the length of test packets used for the test.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

[R85] The methodology **MUST** report the $MAXIR_i$ and T_{SC} used for the test.

[R86] The methodology **MUST** report the PL.

[R87] The methodology **MUST** report pass or fail for the test.

10.3.3.3 IPVC EP Egress BWP Envelope

There are three tests that are performed to verify the IPVC EP Egress BWP Envelope. The aggregate bandwidth of all flows within the envelope is tested, the bandwidth of each flow within the envelope is tested, the bandwidth of each flow simultaneously is tested. The test methodology for each of these is shown in the following sections.

10.3.3.3.1 IPVC EP Egress BWP Envelope Aggregate Methodology

The correct configuration of the aggregate of all flows within the IPVC EP Egress BWP Envelope attribute is verified with this test methodology.

[R88] The aggregate of all flows within the IPVC EP Egress BWP Envelope attribute **MUST** be verified as described in Table 21.

Service Activation Test Methodology	
Test Name	IPVC EP Egress BWP Envelope aggregate
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory if IPVC EP Egress BWP Envelope not *None*
Test Objective	Verify that the IPVC EP Egress BWP Envelope aggregate attribute is configured correctly.
Test Procedure	• $IPTE_2$ offers IP Data Service packets with the DA of $IPTE_1$ and a rate equal to $MaxIR_E$ for a time T_{SC} at EI_2 in accordance with the service description. • $IPTE_1$ counts the number of IP Data Service packets received at EI_1 determining the PL and measuring the PLR_{SAC}. Packet loss is acceptable up to PLR_{SAC}.
Variables	DA, $MaxIR_E$, T_{SC}, PL, PLR_{SAC}
Results	Pass = Packet loss is within PLR_{SAC}

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

	Fail = Packet loss is not within PLR_{SAC}
Remarks	1. Egress BWP Envelope test includes total aggregate information rate of traffic across all BWP Flows in the Envelope.

Table 21 IPVC Egress BWP Envelope Aggregate Test Methodology

[R89] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R90] The methodology **MUST** report the length of test packets used for the test.

[R91] The methodology **MUST** report the $MAXIR_E$ and T_{SC} used for the test.

[R92] The methodology **MUST** report the PL.

[R93] The methodology **MUST** report pass or fail for the test.

10.3.3.3.2 IPVC EP Egress BWP Envelope per Flow

The correct configuration of each flow within the IPVC EP Egress BWP Envelope is verified using this test methodology.

[R94] Each flow within the IPVC EP Egress BWP Envelope **MUST** be verified as described in Table 22.

Service Activation Test Methodology	
Test Name	IPVC EP Egress BWP Envelope per Flow
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory if IPVC EP Egress BWP Envelope not *None*
Test Objective	Verify that the IPVC EP Egress BWP Envelope attribute is configured correctly for each flow within the Envelope.
Test Procedure	• $IPTE_2$ offers IP Data Service packets with the DA of $IPTE_1$, a CoS marking equal to the IPVC EP Ingress Class of Service Map for the flow, a rate equal to $MaxIR_i$ for a time equal to T_{SC} at EI_2 in accordance with the service description. • $IPTE_1$ counts the number of IP Data Service packets received at EI_1 determining the PL and measuring the PLR_{SAC}. Packet loss is acceptable up to PLR_{SAC}.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

	• This is repeated for flows 1..n in the envelope.
Variables	DA, CoS Map, $MaxIR_E$, T_{SC}, PL, PLR_{SAC}
Results	Pass = Packet loss is within PLR_{SAC} Fail = Packet loss is not within PLR_{SAC}
Remarks	**1.** A failure of any flow in the envelope represents a failure of all flows in the envelope.

Table 22 IPVC Egress BWP Envelope per Flow Test Methodology

[R95] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R96] The methodology **MUST** report the length of test packets used for the test.

[R97] The methodology **MUST** report the $MAXIR_i$ and T_{SC} used for the test.

[R98] The methodology **MUST** report the PL.

[R99] The methodology **MUST** report pass or fail for the test.

10.3.3.3.3 IPVC EP Egress BWP Envelope All Flows Simultaneously

The correct configuration of all flows simultaneously within the IPVC EP Egress BWP Envelope is verified using this test methodology.

[R100] All flows within the IPVC EP Egress BWP Envelope **MUST** be verified simultaneously as described in Table 23

Service Activation Test Methodology	
Test Name	IPVC EP Egress BWP Envelope all Flows simultaneously
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory if IPVC EP Egress BWP Envelope not *None*
Test Objective	Verify that the IPVC EP Egress BWP Envelope attribute is configured correctly for all flows within the Envelope.
Test Procedure	• $IPTE_2$ offers IP Data Service packets with the DA of $IPTE_1$, a CoS marking equal to the IPVC EP Egress Class of Service Map

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

	for each flow within the envelope simultaneously, a rate equal to $MaxIR_i$ for each flow, for a time T_{SC} at EI_2 in accordance with the service description. • $IPTE_1$ counts the number of IP Data Service packets received at EI_1 for each flow within the envelope determining the PL and calculating the *PLR*. Packet loss is acceptable up to PLR_{SAC}.
Variables	DA, CoS Map, $MaxIR_i$, T_{SC}, PL, PLR_{SAC}
Results	Pass = Packet loss is within PLR_{SAC} Fail = Packet loss is not within PLR_{SAC}
Remarks	**1.** A failure of any flow in the envelope represents a failure of all flows in the envelope.

Table 23 IPVC Egress BWP Envelope for all Flows within the Envelope Test Methodology

[R101] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R102] The methodology **MUST** report the length of test packets used for the test.

[R103] The methodology **MUST** report the $MAXIR_i$ and T_{SC} used for the test.

[R104] The methodology **MUST** report the PL.

[R105] The methodology **MUST** report pass or fail for the test.

10.4 Service Performance Tests

Service performance tests are used to ensure that the service meets performance expectations of the Subscriber. Service performance tests measure percentile of PD, MPD, IPDV, PDR, and PLR. To perform these measurements an IPTE generates and/or receives test packets. Timestamps within the packets are used to perform delay measurements and the count of packets is used to determine IP Packet loss. There are several mechanisms that can be used to measure delay and loss. Examples are TWAMP Light, STAMP, and TWAMP. Other methods are also acceptable. To calculate one-way Packet Delay Percentile or Mean Packet Delay, either Time of Day synchronization between the two IPTEs is supported (in which case one-way measurements can be used), or two-way measurements are taken and divided in half to approximate the one-way packet delay. If two-way measurements are divided in half, this is indicated in the report.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

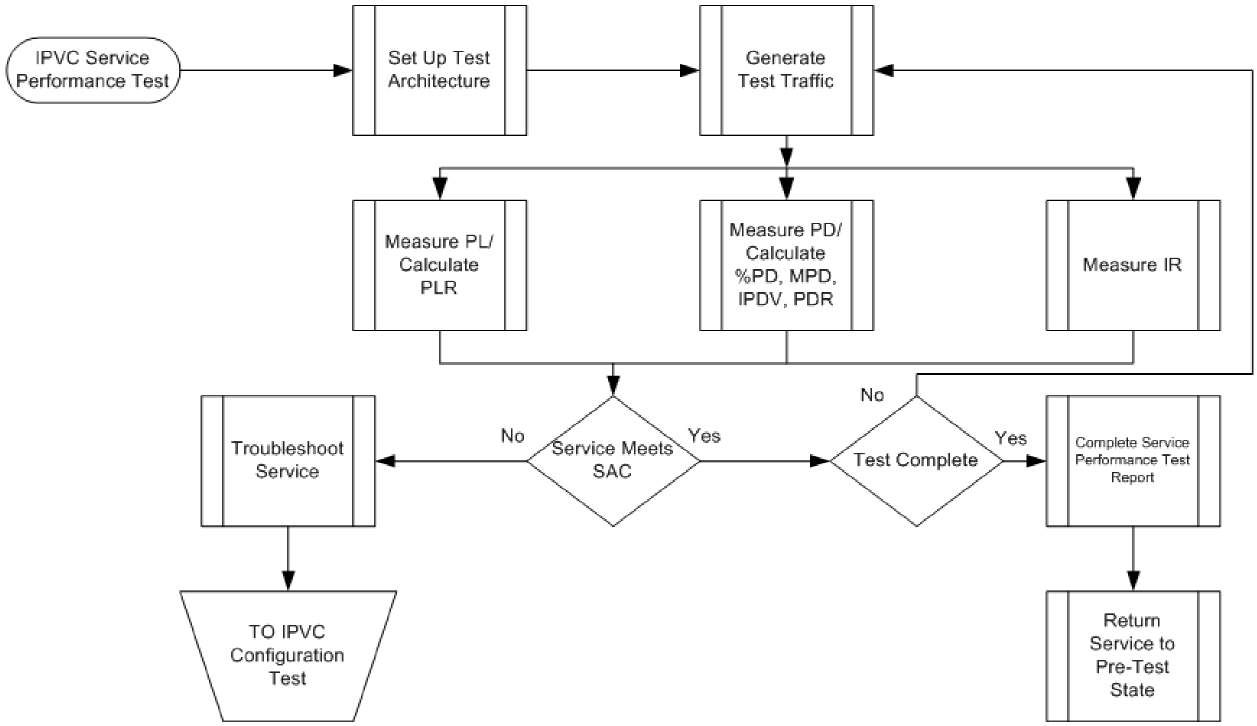

Figure 25 Service Performance Flow

10.4.1 Service Performance Test Duration

As discussed previously, the duration of the service performance test is significantly longer than the service configuration tests. To approximate the expected performance of the service, a longer test is required. There are three recommended test durations, 15 minutes, 2 hours, or 24 hours.

[D5] The Service Provider **SHOULD** support at least one of these test durations.

The duration of the performance test is agreed to between the Service Provider and the Subscriber.

[R106] The Service Performance test duration **MUST** be agreed to by the Service Provider and Subscriber from one of the three test durations above.

10.4.2 Service Performance Service Loss and Delay

When an IPVC is being activated, the performance of each CoS Name applicable to the IPVC is tested one CoS Name at a time between each set of IPVC EPs in the IPVC. The test methodology in Table 24 is used to perform loss and delay measurements between each set of IPVC EPs.

[R107] The loss and delay performance of each set of IPVC EPs in a new IPVC **MUST** be verified as specified in Table 24.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Test Name	Service Performance Loss and Delay
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory for new IPVC, Mandatory for new IPVC EP
Test Objective	Verify that the IPVC performance meets the SAC.
Test Procedure	• Packet length can be any single length or multiple lengths as specified in the IMIX pattern shown in section 10.1.1. • $IPTE_1$ offers packets with the DA of $IPTE_2$ at a constant rate equal to $MaxIR_i$ for the Bandwidth Profile Flow that the CoS Name and IPVC is mapped to for time T_{SP}. • $IPTE_2$ counts the packets received and transmitted. It measures the received IR_{MEAS}, PL_{MEAS}, and PD_{MEAS}. $IPTE_2$ calculates the MPD_{MEAS}, $IPDV_{MEAS}$ and/or PDR_{MEAS} from PD_{MEAS} and PLR_{MEAS} from PL_{MEAS}. • Simultaneously, $IPTE_2$ offers packets with the DA of $IPTE_1$ at a constant rate equal to $MaxIR_i$ for the Bandwidth Profile Flow that the CoS Name and IPVC is mapped to for time T_{SP}. • $IPTE_1$ counts the packets received and transmitted. It measures the received IR_{MEAS}, PL_{MEAS}, and PD_{MEAS}. $IPTE_1$ calculates the MPD_{MEAS}, $IPDV_{MEAS}$ and/or PDR_{MEAS} from PD_{MEAS} and PLR_{MEAS} from PL_{MEAS}. • IR_{SAC}, PD_{SAC} and/or MPD_{SAC}, $IPDV_{SAC}$ and/or PDR_{SAC}, and PLR_{SAC} are the limits specified by SAC. • This process is repeated for each Bandwidth Profile Flow contained in the IPVC and for packets that are not mapped to a particular Bandwidth Profile Flow. • If the IR_{MEAS}, PLR_{MEAS}, PD_{MEAS} and/or MPD_{MEAS}, and $IPDV_{MEAS}$ and/or PDR_{MEAS} are within the limits of SAC for each flow and for packets not mapped to a particular Bandwidth Profile Flow at $IPTE_1$ and $IPTE_2$ the result is Pass.
Variables	Packet lengths, T_{SP}, IR_{SAC}, PD_{SAC}, MPD_{SAC}, $IPDV_{SAC}$, PDR_{SAC}, PLR_{SAC}
Results	Pass = All Bandwidth Profile Flows and packets not mapped to a particular Bandwidth Profile Flow have to meet IR_{SAC}, PD_{SAC} and/or MPD_{SAC},

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

	$IPDV_{SAC}$ and/or PDR_{SAC}, and PLR_{SAC} for this test to pass. Fail = Any Bandwidth Profile Flow or packets not mapped to a particular Bandwidth Profile Flow fail to meet IR_{SAC}, PD_{SAC} and/or MPD_{SAC}, $IPDV_{SAC}$ and/or PDR_{SAC}, and PLR_{SAC} this test fails.
Remarks	**1.** T_{SP} is the Time of the Service Performance test. It is similar to the T_{SC} variable used in the Service Configuration tests.

Table 24 Service Performance Loss and Delay Test Methodology

[R108] The methodology **MUST** report the CoS Name of test packets used in this methodology.

[R109] The methodology **MUST** report the length of test packets used for the test.

[R110] The methodology **MUST** report the $MAXIR_i$ and T_{SP} used for the test.

[R111] The methodology **MUST** report the IR, PL, %PD, MPD, IPDV, PDR.

[R112] The methodology **MUST** report pass or fail for the test.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

11 Results

After all tests have been completed a SAT record is created. The SAT record contains the attribute and test result information described in section 9 and 10. The results from the different tests on a particular service are mapped into one SAT record for that service. The SAT record can be shared with the Subscriber and can be stored within Service Provider management systems. The format of the SAT record is not mandated by this document.

11.1 Monitoring Test

While a particular test is in progress, the ability to query the IPTE(s) for the status of the test is needed. This does not include interim measurement results but does include the test status.

[R113] An IPTE-TH, IPTE-A, or IPTE-I **MUST** allow a user or system to monitor the status of a test.

An IPTE can support autonomous reporting of test status or can support retrieving the status of the test through queries by the Service Provider's support systems.

11.1.1 Test Report

The test report format is not defined within this document. The expectation is that the test report contains all the attributes specified in section 9 and 10. The Test Report can be provided to the Subscriber by the Service Provider or can be maintained by the Service Provider for future reference. An example of the contents of a Test Report is shown in Appendix A.

Editor's Note: Upon the completion of this document, additional work will be performed that will define the IP Services SAT Test Report format and Interface Profile Specification.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

12 References

[1] BBF TR-143, *Enabling Network Throughput Performance Tests and Statistical Monitoring*, May 2008

[2] IEEE Std 1003.1-2017, *Draft Standard for Information Technology – Portable Operating System Interface (POSIX)*, 2017

[3] IETF RFC 791, *Internet Protocol DARPA Internet Program Protocol Specification*, September 1981

[4] IETF RFC 792, *Internet Control Message Protocol, DARPA Internet Program Protocol Specification*, September 1981

[5] IETF RFC 2131, *Dynamic Host Configuration Protocol*, March 1997

[6] IETF RFC 2474, *Definition of Differentiated Service Field (DS)*, December 1998

[7] IETF RFC 2544, *Benchmarking Methodology for Network Interconnect Devices*, March 1999

[8] IETF RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*, February 2006

[9] IETF RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*, March 2010

[10] IETF RFC 5880, *Bidirectional Forwarding Detection (BFD)*, June 2010

[11] IETF RFC 6349, *Framework for TCP Throughput Testing*, August 2011

[12] IETF RFC 6985, *IMIX Genome: Specification of Variable Packet Sizes for Additional Testing*, July 2013

[13] IETF RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*, July 2017

[14] International Standards Organisation ISO/IEC 7498-1, Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, November 1994

[15] ITU-T Recommendation Y.1540, *Internet protocol data communication service – IP IP Packet transfer and availability performance*, July 2016

[16] ITU-T Recommendation Y.1541, *Network performance objectives for IP-based services*, December 2011

[17] ITU-T Recommendation Y.1541 Amendment 1, *New Appendix XII – Considerations for low speed access networks*, December 2013

[18] ITU-T Recommendation Y.1542, *Framework for achieving end-to-end IP performance objectives*, June 2010

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

[19] ITU-T Recommendation Y.1544, *Multicast IP performance parameters*, July 2008

[20] ITU-T Recommendation Y.1560, *Parameters for TCP connection performance in the presence of middleboxes*, September 2003

[21] ITU-T Recommendation Y.1564, *Ethernet service activation test methodology*, February 2016

[22] MEF 10.3, *Ethernet Services Attributes Phase 3*, October 2013

[23] MEF 48/48.1, *Carrier Ethernet Service Activation Testing Phases 1 and 2*,

[24] MEF 61, *IP Service Attributes for Subscriber IP Services*, January 2018

[25] MEF z.a, *Service OAM for IP Services*, April 2018

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Appendix A Test Report Content Example

An example of the contents of a Test Report is shown in Table 25. This is shown as an example only. Normative text in sections 9 and 10 are used to specify exactly what Service Attributes are reported.

Editor Note 3: Should we keep this appendix in the document?

Attributes	Report Attribute	Comments
UNI		
UNI Identifier	Reported as per section 9	
UNI Management Type	Reported as per section 9	
UNI List of UNI Access Links	Reported as per section 9	
UNI Ingress Bandwidth Profile Envelope	Reported as per section 9	
UNI Egress Bandwidth Profile Envelope	Reported as per section 9	
UNI List of Control Protocols	Reported as per section 9	
UNI Routing Protocols	Reported as per section 9	
UNI Reverse Path Forwarding	Reported as per section 9	
UNI Access Link		
IPVC Identifier		
UNI Access Link Identifier	Reported as per section 9	
UNI Access Link Connection Type	Reported as per section 9	
UNI Access Link L2 Technology	Reported as per section 9	
UNI Access Link IPv4 Connection Addressing	Reported as per section 9	
UNI Access Link IPv6 Connection Addressing	Reported as per section 9	
UNI Access Link DHCP Relay	Reported as per section 9	

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Attributes	Report Attribute	Comments
UNI Access Link Prefix Delegation	Reported as per section 9	
UNI Access Link BFD Service Provider Active	Reported as per section 9 Tested as per section 10.3.1.1	
	BFD Session State	
	T_{BFD}	
	Connection Address Family	
	Transmission Interval	
	Detect Multiplier	
	Active End	
	Authentication Type	
	Pass/Fail	
UNI Access Link BFD Subscriber Active	Reported as per section 9 Tested as per section 10.3.1.2	
	BFD Session State	
	T_{BFD}	
	Connection Address Family	
	Transmission Interval	
	Detect Multiplier	
	Active End	
	Authentication Type	
	Pass/Fail	
UNI Access Link IP MTU	Reported as per section 9 Tested as per section 10.3.1.3	
	IR_{SC}	
	Tsc	
	PLR_{SAC}	

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Attributes	Report Attribute	Comments
	Pass/Fail	
UNI Access Link Ingress Bandwidth Profile Envelope	Reported as per section 9	
UNI Access Link Egress Bandwidth Profile Envelope	Reported as per section 9	
UNI Access Link Reserved VRIDs Service Attribute	Reported as per section 9	
UNI Access Link Reserved VRIDs Service Attribute	Reported as per section 9	
IPVC		
IPVC Identifier	Reported as per section 9	
IPVC Topology	Reported as per section 9	
IPVC End Point List	Reported as per section 9	
IPVC Packet Delivery	Reported as per section 9	
IPVC Maximum Number of IPv4 Routes	Reported as per section 9	
IPVC Maximum Number of IPv6 Routes	Reported as per section 9	
IPVC DSCP Preservation	Reported as per section 9 Tested as per section 10.3.2.1	
	List of DSCP values	
	IR_{SC} per DSCP value	
	T_{SC} per DSCP value	
	PLR_{SAC} per DSCP value	
	Pass/Fail	
IPVC List of Class of Service Names	Reported as per section 9	
IPVC Service Level Specification	NA	
IPVC MTU	Reported as per section 9 Tested as per section 10.3.2.2	
	IPVC MTU	

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Attributes	Report Attribute	Comments
	IR_{SC}	
	Tsc	
	PLR_{SAC}	
	Pass/Fail	
IPVC Path MTU Discovery	Reported as per section 9 Tested as per section 10.3.2.3	
	Packet length	
	IR_{SC}	
	Tsc	
	PLR_{SAC}	
	Pass/Fail	
IPVC Fragmentation	Reported as per section 9 Tested as per section 10.3.2.4	
	Packet length	
	IR_{SC}	
	Tsc	
	PLR_{SAC}	
	Pass/Fail	
IPVC Cloud	Reported as per section 9	
IPVC Reserved Prefixes	Reported as per section 9	
IPVC End Point		
IPVC EP Identifier	Reported as per section 9	
IPVC EP UNI	Reported as per section 9	
IPVC EP Prefix Mapping	Reported as per section 9 Tested as per section 10.3.3.1	
	IR_{SC}	
	Tsc	
	PLR_{SAC}	
	Pass/Fail	
IPVC EP Maximum Number of IPv4 Routes	Reported as per section 9	
IPVC EP Maximum Number of IPv6 Routes	Reported as per section 9	
IPVC EP Ingress Class of Service Map	Reported as per section 9	

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Attributes	Report Attribute	Comments
IPVC EP Egress Class of Service Map	NA	
IPVC EP Ingress Bandwidth Profile Envelope	Reported as per section 9 Tested as per section 10.3.3.2, 10.3.3.2.1, and 10.3.3.2.2	
	$MaxIR_n$	
	T_{SC}	
	PLR_{SAC}	
	Pass/Fail	
IPVC EP Egress Bandwidth Profile Envelope	Tested Reported as per section 9 Tested as per section 10.3.3.3, 0, and 10.3.3.3.2	
	$MaxIR_n$	
	T_{SC}	
	PLR_{SAC}	
	Pass/Fail	
Performance Test		
Packet Delay	IR	
	Delay: ms	
	Packet Length	
	T_{SP}	
	PD_{SAC}	
	Pass/Fail	
Mean Packet Delay	IR	
	Delay: ms	
	Packet Length	
	T_{SP}	
	MPD_{SAC}	
	Pass/Fail	
Inter-Packet Delay Variation	IR	
	Delay: ms	
	T_{SP}	
	$IPDV_{SAC}$	
	Packet Length	
	Pass/Fail	
Packet Delay Range	IR	
	Delay: ms	
	T_{SP}	
	PDR_{SAC}	
	Packet Length	
	Pass/Fail	

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Attributes	Report Attribute	Comments
Packet Loss Ratio	IR	
	IR_{SAC}	
	PLR_{SAC}	

Table 25 Test Report Contents

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.

Appendix B Information Rate Comparison

This appendix provides a comparison of the Information Rate (IR) between Layer 1 (L1), Layer 2 (L2), and Layer 3 (L3). For the purposes of this document L2 is assumed to be Ethernet and L3 is assumed to be IP.

Editor Note 4: This appendix will be provided in the next release of this document.

© MEF Forum 2019. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of MEF Forum." No user of this document is authorized to modify any of the information contained herein.