MEF Standard

MEF 67

Service Activation Testing for IP Services

December 2020

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.

Table of Contents

List of Figures

List of Tables

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.

Member
Bell Canada
Cisco
Iometrix
Spirent
ZTE

Table 1 – Contributing Members

2 Abstract

This document specifies Service Activation Testing (SAT) of IP Service Attributes as defined in MEF 61.1 [15]. The document addresses activation of Internet Protocol Virtual Connections (IPVCs), IPVC End Points (IPVC EPs), User Network Interfaces (UNIs), and UNI Access Links. 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 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 61.1 [15] are included in this document by reference and are not repeated in the table below.

Term	Definition	Reference
BFD	Bidirectional Forwarding Detection	IETF RFC 5880 [7]
Bidirectional 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 [7]
Collector Test Function	A logical function for counting and discarding received IP Packets, which can include test packets.	This document derived from MEF 48.1 [14]
CTF	Collector Test Function	MEF 48.1 [14]
DSCP	Differentiated Services Code Point	IETF RFC 2474 [5]
Generator Test Function	A logical function for generating and transmitting IP Packets which can include test packets.	This document derived from MEF 48.1 [14]
GTF	Generator Test Function	MEF 48.1 [14]
ICMP	Internet Control Management Protocol	IETF RFC 792 [2]
IMIX	Internet Mix	IETF RFC 6985 [9]
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 Packet sizes used to emulate real-world traffic scenarios in a testing environment.	IETF RFC 6985 [9]
Internet Protocol Conditioning Function	Processing entity responsible for implementing behavior associated with certain IPVC and IPVC EP Service Attributes. In some cases, the IPCF also implements behavior associated with the UNI and UNI Access Link BWP Envelopes.	This document

Internet Protocol Loopback Function	A function that receives IP Test Packets, swaps the IP Addresses and Port Numbers on these packets, and retransmits these packets back towards the Source Address of the received IP Test Packets.	This document
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
Internet Protocol Test Packet	An IP packet that is used to perform test measurements.	This document
IPCF	Internet Protocol Conditioning Function	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
IP Loopback Function	Internet Protocol Loopback Function	This document
IP Test Packet	Internet Protocol Test Packet	This document
IR	Information Rate	This document
L2	Layer 2	ISO OSI [12]
Packet Loss Ratio	The ratio of the packets lost versus the total number of packets sent.	This document
SAC	Service Acceptance Criteria	ITU-T Y.1564 [13]
SAMP	Service Activation Measurement Point	MEF 48.1 [14]
SAT	Service Activation Testing	MEF 48.1 [14]
Service Acceptance 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 [13]
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. A Service Activation Measurement Point contains both a Generator Test Function and a Collector Test Function.	This document derived from MEF 48.1 [14]

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 48.1 [14]
Test End Point	A pseudo IPVC EP that is created within the Service Provider's network to perform IPVC and IPVC EP verification when a new IPVC EP is added to an existing IPVC.	This document
UNICF	User Network Interface Conditioning Function	This document
User Network Interface Conditioning Function	Processing entity responsible for implementing behavior associated with certain UNI or UNI Access Link Service Attributes.	This document

Table 2 – Terminology and Abbreviations

4 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 [3], RFC 8174 [10]) 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.

5 Numerical Prefix Conventions

This document uses the prefix notation to indicate multiplier values as shown in Table 3.

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 3 – Numerical Prefix Conventions

6 Introduction

Service Activation Testing (SAT) is the process of testing an IP Service in order to collect behavioral information about the service and compare this with the intended behavior before the service is handed off to the Subscriber. Both the configuration of the service and its performance can be verified. Configuration tests, normally short in duration (under 30 seconds), are used to take a "snap-shot" of the service.

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, such as congestion or errors, and these issues can be intermittent. Performance tests are not expected to detect all extremes of degradations. The duration of the Performance tests is a compromise between the probability of detecting degradations and the length of time needed to perform SAT. Service Providers and Subscribers must determine the acceptable length of the performance tests.

Configuration testing verifies that Service Attributes are configured per the service order for: IP Virtual Connection (IPVC), IPVC End Point (IPVC EP), User Network Interface (UNI), and UNI Access Link. The Service Attributes verified are shown in section 10.

Performance testing verifies that the service is performing acceptably and that the performance-related Service Acceptance Criteria (SAC) are met. See section 11.2 for the description of SAC and how they differ from a Service Level Specification (SLS). The measurements that are performed include Packet Delay and Packet Loss. Packet Delay can be measured using timestamps present in the IP Test Packets. If used, these timestamps indicate the time an IP Test Packet was transmitted or received by an Internet Protocol Test Equipment (IPTE). The specific implementation within an IPTE to measure Packet Delay is outside the scope of this document. Packet Loss can be measured by comparing the number of IP Test Packets generated to those received. Sequence numbers within the IP Test Packets can be used to identify gaps in the received packets. The number of received IP Test Packets is subtracted from the number of generated IP Test Packets. If the IP Test Packets contain sequence numbers, they can be used to identify lost, misordered, or duplicated packets. The use of sequence numbers requires that any packet re-ordering be identified and addressed. Additional metrics that are calculated based on these measurements are Packet Delay Percentile, Mean Packet Delay, Inter-Packet Delay Variation, Packet Delay Range, and Packet Loss Ratio.

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 metrics used for the SAC for each test methodology.

Before an IP Service is turned over to a Subscriber, the Service Provider normally tests the service. 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 61.1 [15] 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 are expected, resulting in fewer complaints from Subscribers.

Service configuration tests are performed on a UNI and its UNI Access Links at the time the UNI is activated. Service configuration tests are performed on an IPVC and its initial set of IPVC EPs at the time they are activated. Additional IPVC EPs that are later added to the IPVC are tested at the time they are activated. If the UNI and UNI Access Links are activated at the same time as the first IPVC EPs at that UNI, it is suggested that the UNI and the UNI Access Link are tested before the IPVC EP.

Note that there are two distinct ways that an IPVC EP is tested. For IPVC EPs that are part of a new IPVC, SAT is performed between some or all of the IPVC EPs in the new IPVC. If an IPVC EP is being added to an existing IPVC, SAT is performed on the new IPVC EP to a Test End Point and testing between all IPVC EPs in the IPVC is not required. This avoids impact on the service at the existing IPVC EPs in the IPVC.

The standardized test methodologies defined in this document provide measurable objectives for service activation that can be used internally within a Service Provider or shared externally to Subscribers. 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 which tests they can request from their Service Provider.

An IP service might have an SLS that defines objectives for some performance metrics but not others. 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 shorter time periods such as seconds for Configuration tests and 15 minutes, 2 hours, or 24 hours for Performance tests. SAC 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. SAC do not need to be agreed on for each performance metric that has an SLS objective. SAC can be agreed on for metrics that do not have an SLS performance objective. As an example, SAC can be agreed on for one-way Packet Delay even if the SLS provides no performance objective for Packet Delay. The definitions of SAC 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 Terms and Components (section 7)
- A definition of Service Activation Measurement Points (SAMPs) and Test Head Connection Points (THCPs) including defining where SAMPs and THCPs are located (section 8)
- SAT Use Cases and Test Cases (section 9)
- Verification of IP Service Attributes per Use Case including which are tested and which are reported (section 10)
- SAT Methodologies for Configuration and Performance tests (section 11)
- Test Result reporting (section 12)

Note: the reader of this document is assumed to be familiar with MEF 61.1 [15].

7 SAT Terms and Components

This section of the document describes terms and components used to perform SAT. Where possible, these are aligned with MEF 48.1 [14]. SAT is performed using IP Test Equipment (IPTE). There are three types of IPTE: IP Test Equipment – Instrument (IPTE-I), IP Test Equipment – Application (IPTE-A), and IP Test Equipment – Test Head (IPTE-TH). An IPTE-I is a hand-held portable device that can be useful for dispatches to the Subscriber's premises or similar locations. An IPTE-I might be limited in the number of interfaces it has and the number of flows it can generate/receive packets on simultaneously. An IPTE-A is 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. An IPTE-A can reside in a Physical Network Function (PNF) or be a Virtual Network Function (VNF) that can be loaded as needed. It is useful for tests from managed or non-managed routers and CE. An IPTE-A can help Providers avoid dispatches to Subscriber premises and might have the ability to test multiple flows simultaneously. An IPTE-TH is a type of IPTE that contains multiple interfaces, is typically rack-mounted, is normally installed at a location in the Service Provider's network, and usually contains multiple interfaces and the ability to perform tests on multiple flows simultaneously. An IPTE-TH connects to the Service Under Test via a Test Head Connection Point (THCP). An IPTE-TH is especially useful for testing from a network device to other IPTEs in the service.

An IPTE contains at least one 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 away from the IPTE. An IPTE-I normally contains a single Downward facing SAMP, whereas an IPTE-TH can contain one or more Downward facing SAMPs that connect to THCPs that are either Upward or Downward facing. An IPTE-A can contain one or more SAMPs which can be Upward facing or Downward facing. A SAMP contains both a Generator Test Function (GTF) and a Collector Test Function (CTF). A GTF generates IP Test Packets used for test measurements. A CTF either counts and discards IP Test Packets coming from a GTF or counts and processes IP Test Packets from a GTF.

A THCP is within the Service Provider's network and is where the IPTE-TH connects to the service to be tested. 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 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, service type, test objective, test procedure, variables used in the methodology, results, and remarks. The tables in section 10 identify the test methodology used to verify the Service Attribute. SAT Methodologies are specified in section 11. SAT is performed from one SAMP to another SAMP (GTF-CTF) or from a SAMP to an IP Loopback Function and back to the originating SAMP. An IP Loopback Function swaps the IP Addresses and Port Numbers but does not otherwise process the IP Test Packets.

Figure 1 shows an example IPVC connecting three UNIs together.

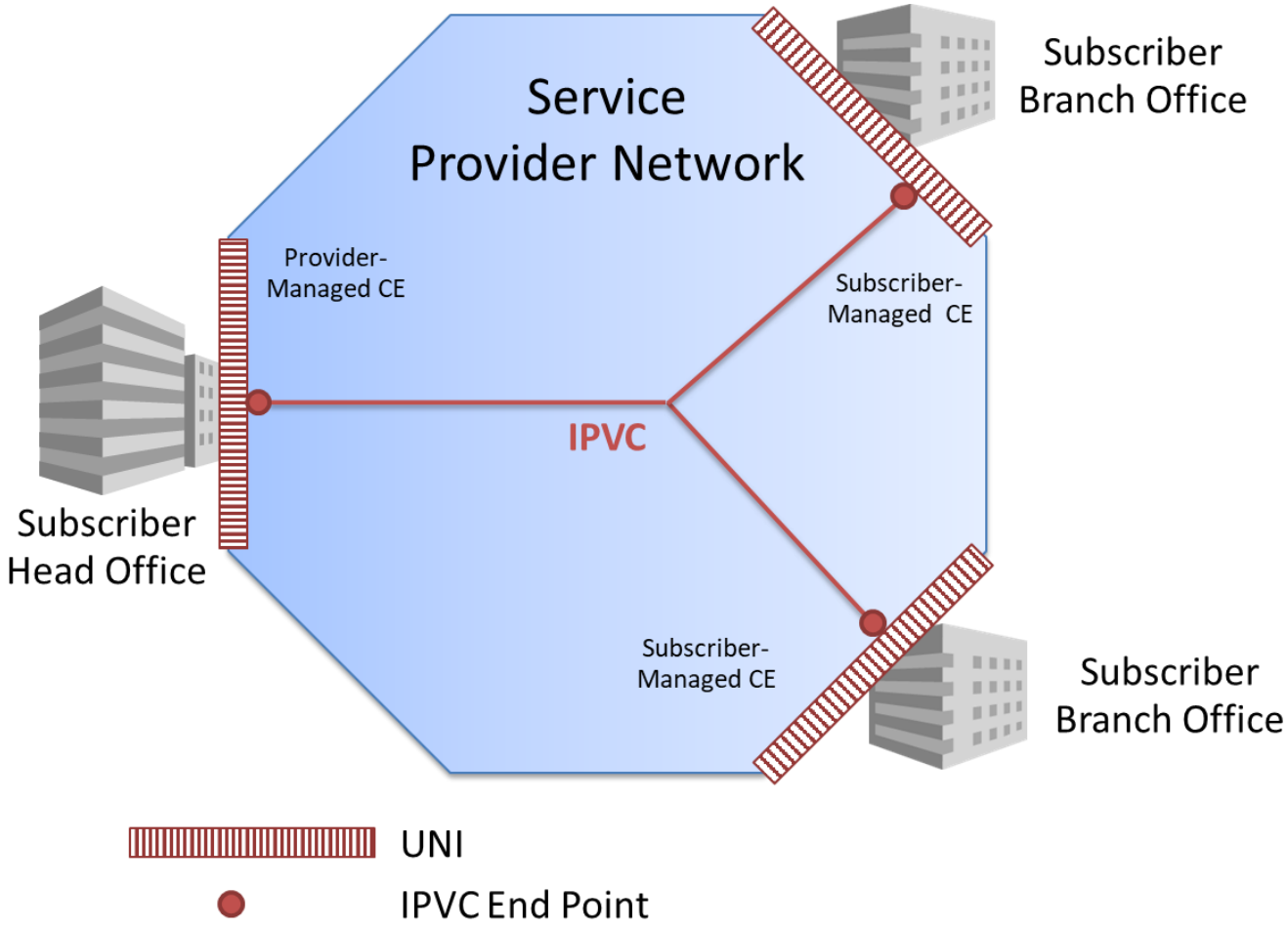

Figure 1 – Example of an IPVC and UNI

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.

Figure 2 shows the example IPVC with IPTEs. Similar to Figure 1, the two UNIs on the right-hand side of Figure 2 connect to Subscriber-Managed CEs. The UNI on the left-hand side of Figure 2 connects to a Provider-Managed CE.

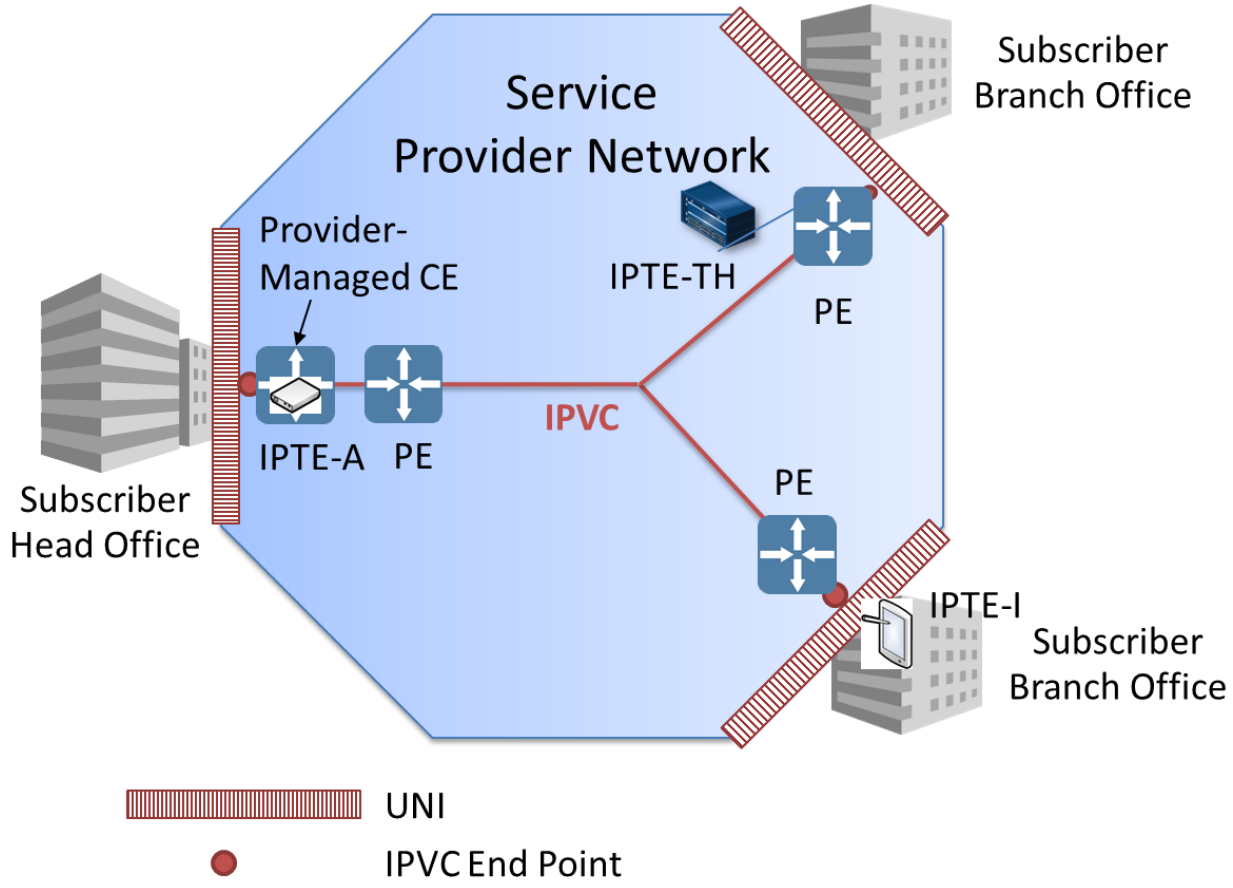

Figure 2 – Example of IPTE locations

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 connected to the UNI in place of a Subscriber-managed CE, and can perform test measurements to the IPTE-TH or IPTE-A. The IPTE-A is shown in the Provider-Managed Customer Edge (CE) at the Subscriber Head Office. This application can perform test measurements to the IPTE-TH or the IPTE-I.

8 SAMP and THCP Locations

The logical location of SAMPs and of THCPs within the Service Provider Network is described in this section. This is provided as guidance for SAMP and THCP implementations. The SAMPs and THCPs are located so that packets generated and received pass through the appropriate processing functions - i.e. either Internet Protocol Conditioning Functions (IPCFs) or User Network Interface Conditioning Functions (UNICFs), as specified below. How and where these functions are implemented is outside the scope of this document; however, an implementation must ensure that IP Test Packets generated or received by a SAMP or THCP have passed through the processing functions as shown.

Note: The tools used to generate and receive packets, and the specific implementation of the SAMPs and THCPs, is beyond the scope of this document.

8.1 Internet Protocol Conditioning Function and User Network Interface Conditioning Function

The IP Conditioning Function (IPCF) and the UNI Conditioning Function (UNICF) are responsible for implementing behavior associated with certain of the Service Attributes defined in MEF 61.1 [15]. The IPCF implements behavior associated with the following Service Attributes:

- IPVC
    - DSCP Preservation
    - IPVC MTU
    - MTU Discovery
    - Fragmentation
- IPVC EP
    - Prefix Mapping
    - Ingress BWP Envelope
    - Egress BWP Envelope
- UNI (if not implemented in UNICF)
    - Ingress BWP Envelope
    - Egress BWP Envelope
- UNI Access Link (if not implemented in UNICF)
    - Ingress BWP Envelope

- Egress BWP Envelope

The UNICF implements behavior associated with the following Service Attributes:

- UNI (if not implemented in IPCF)
  - Ingress BWP Envelope
  - Egress BWP Envelope
- UNI Access Link
  - BFD
  - MTU
  - Ingress BWP Envelope (if not implemented in IPCF)
  - Egress BWP Envelope (if not implemented in IPCF)

As shown above, the UNI and UNI Access Link BWP Envelopes can be implemented in either the IPCF or the UNICF. If the BWP Envelope contains per IPVC EP BWP flows, the BWP Envelope must be implemented in the IPCF and cannot be implemented in the UNICF. IPVC EP BWP Envelopes can only contain per-IPVC EP BWP Flows, and hence can only be implemented in the IPCF. The SAMPs or THCPs might need to be placed differently for verification of the IPVC EP BWP Envelope and the UNI or UNI Access Link BWP Envelope depending on which conditioning function implements the BWP Envelope. Implementation specific details are outside the scope of this document.

8.2 SAMP and THCP Locations for an IPTE-TH

The following figures show the location of SAMPs and THCPs associated with an IPTE-TH in relationship to processing functions within the SP Network. The specific way that the THCPs and processing functions are implemented is outside the scope of this document, so long as the overall behavior is consistent with the arrangement specified below. In particular, it is not specified whether the functions are all implemented within a single device or distributed over multiple devices.

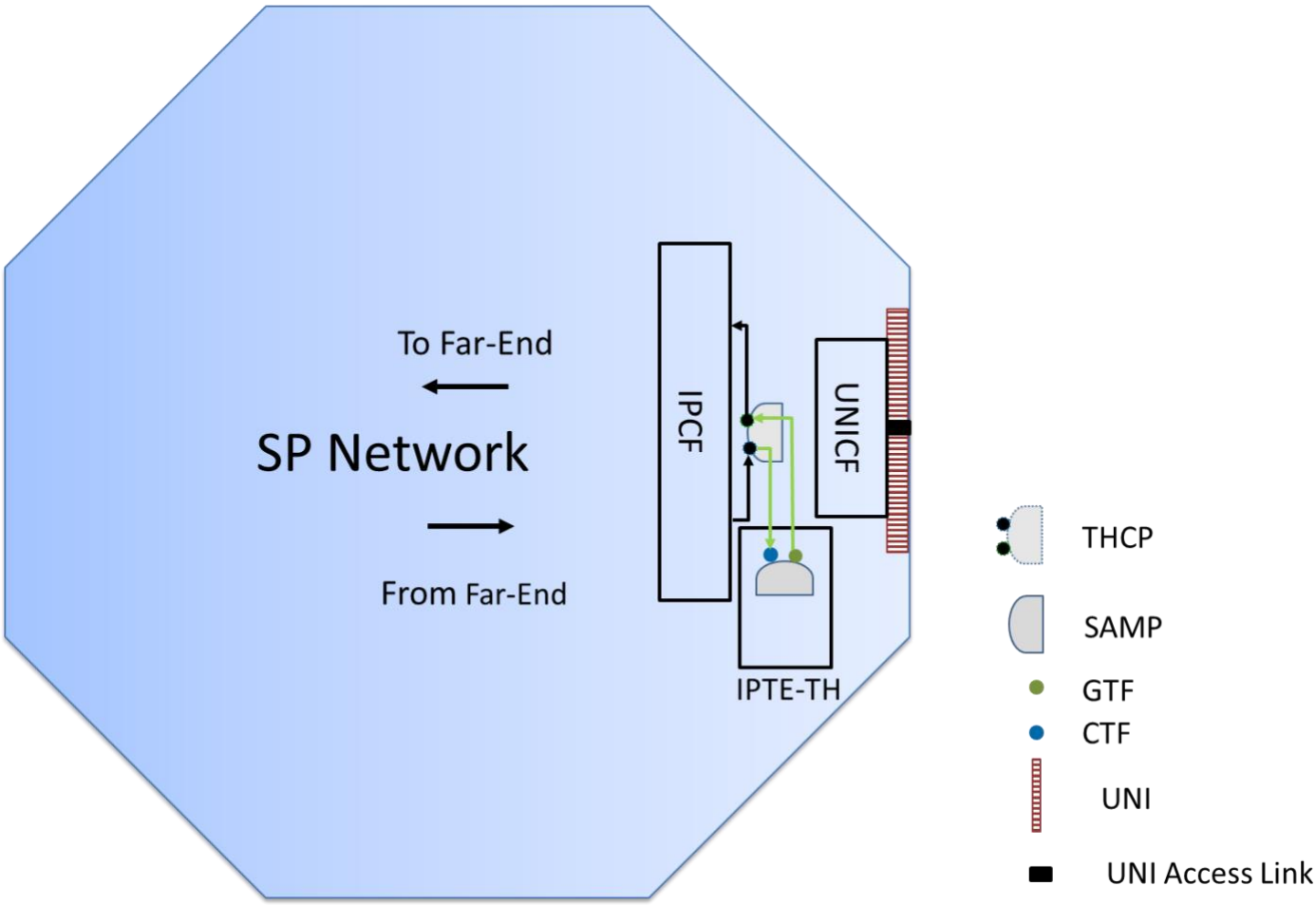

Figure 3 – Upward Facing THCP at a UNI

Figure 3 shows the location of the Upward facing THCP at a UNI. Packets generated by the GTF in the IPTE-TH pass through the THCP and the IPCF and continue to the far-end. Packets from the far-end pass through the IPCF and the THCP and continue to the CTF in the IPTE-TH.

[R1] An implementation of an Upward facing THCP at a UNI **MUST** be located such that IP Test Packets are processed by the IPCF and not by the UNICF.

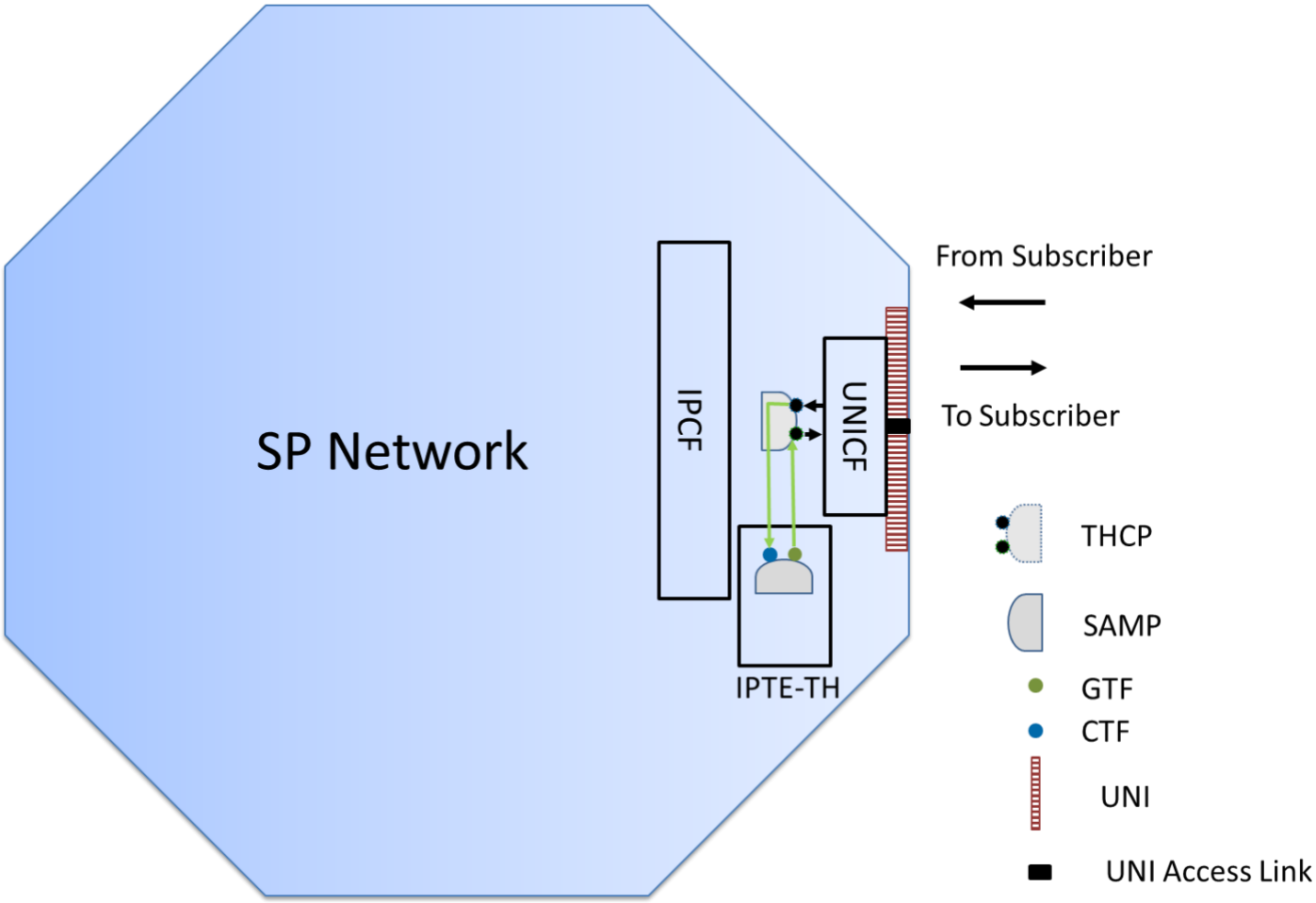

Figure 4 – Downward Facing THCP at a UNI

Figure 4 shows the location of a Downward facing THCP at a UNI. The THCP is placed so that packets generated and received by the IPTE-TH are processed by the UNICF. Packets generated by the GTF pass through the UNICF towards the Subscriber's equipment. Packets come from the Subscriber's equipment and pass through the UNICF before being received by the CTF. This example can be used to verify a new UNI or new UNI Access Link even if there are no IPVC EPs at the UNI.

[R2] An implementation of a Downward facing THCP at a UNI **MUST** be located such that IP Test Packets are processed by the UNICF and not by the IPCF.

8.3 SAMP Locations for an IPTE-A

The following figures show the location of SAMPs associated with an IPTE-A in relationship to processing functions within the SP Network. The specific way that the SAMPs and processing functions are implemented is outside the scope of this document, so long as the overall behavior is consistent with the arrangement specified below. In particular, it is not specified whether the processing functions are all implemented within a single device or distributed over multiple devices.

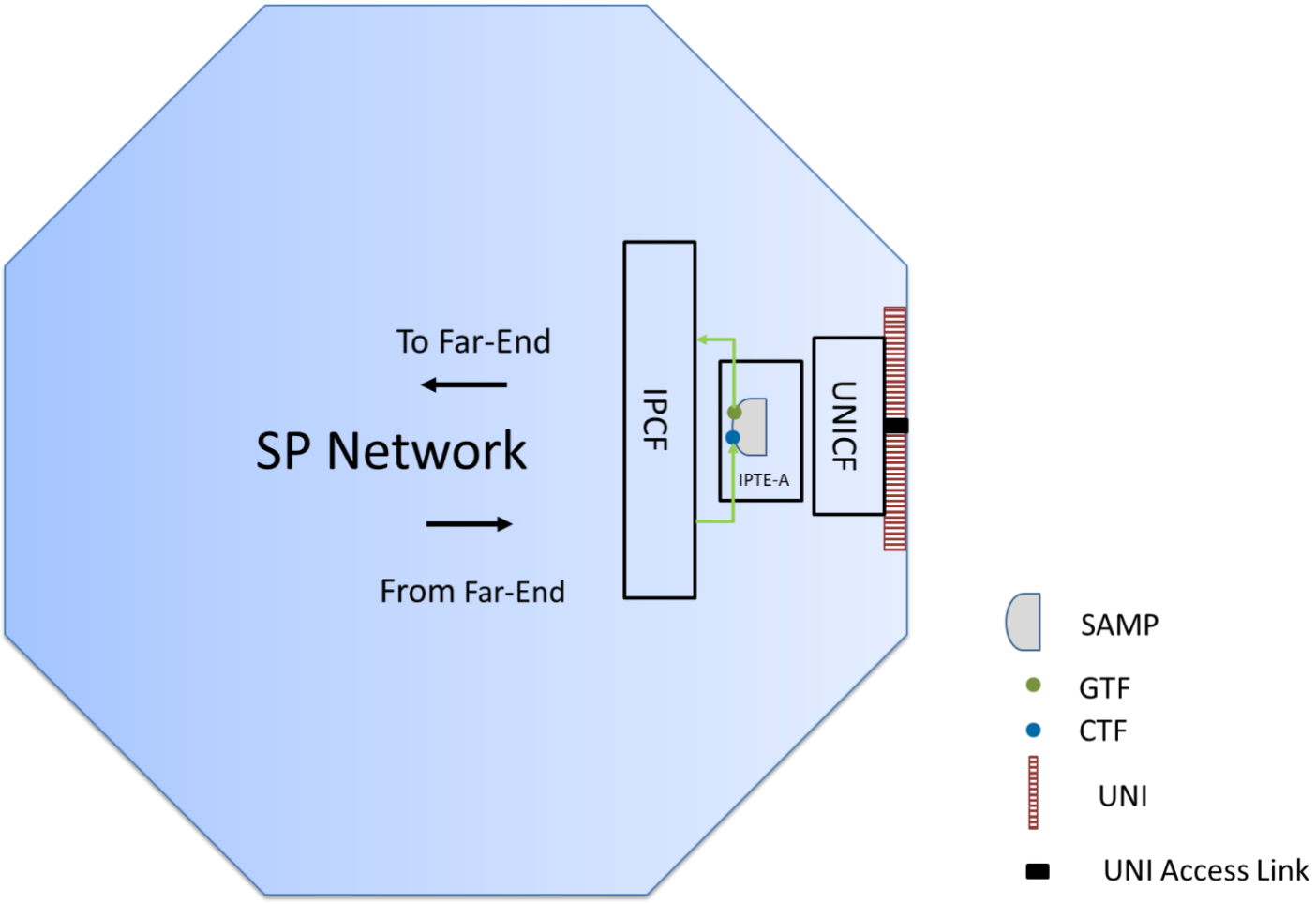

Figure 5 – Upward facing SAMP Location in IPTE-A

Figure 5 shows the Upward facing SAMP location using an IPTE-A on the SP's side of the UNI. The SAMP is located so that packets generated by the GTF pass through the IPCF to the far-end and packets received from the far-end pass through the IPCF before being counted by the CTF .

[R3] An implementation of an Up SAMP in an IPTE-A on the SP's side of the UNI **MUST** be located such that IP Test Packets are processed by the IPCF and not by the UNICF.

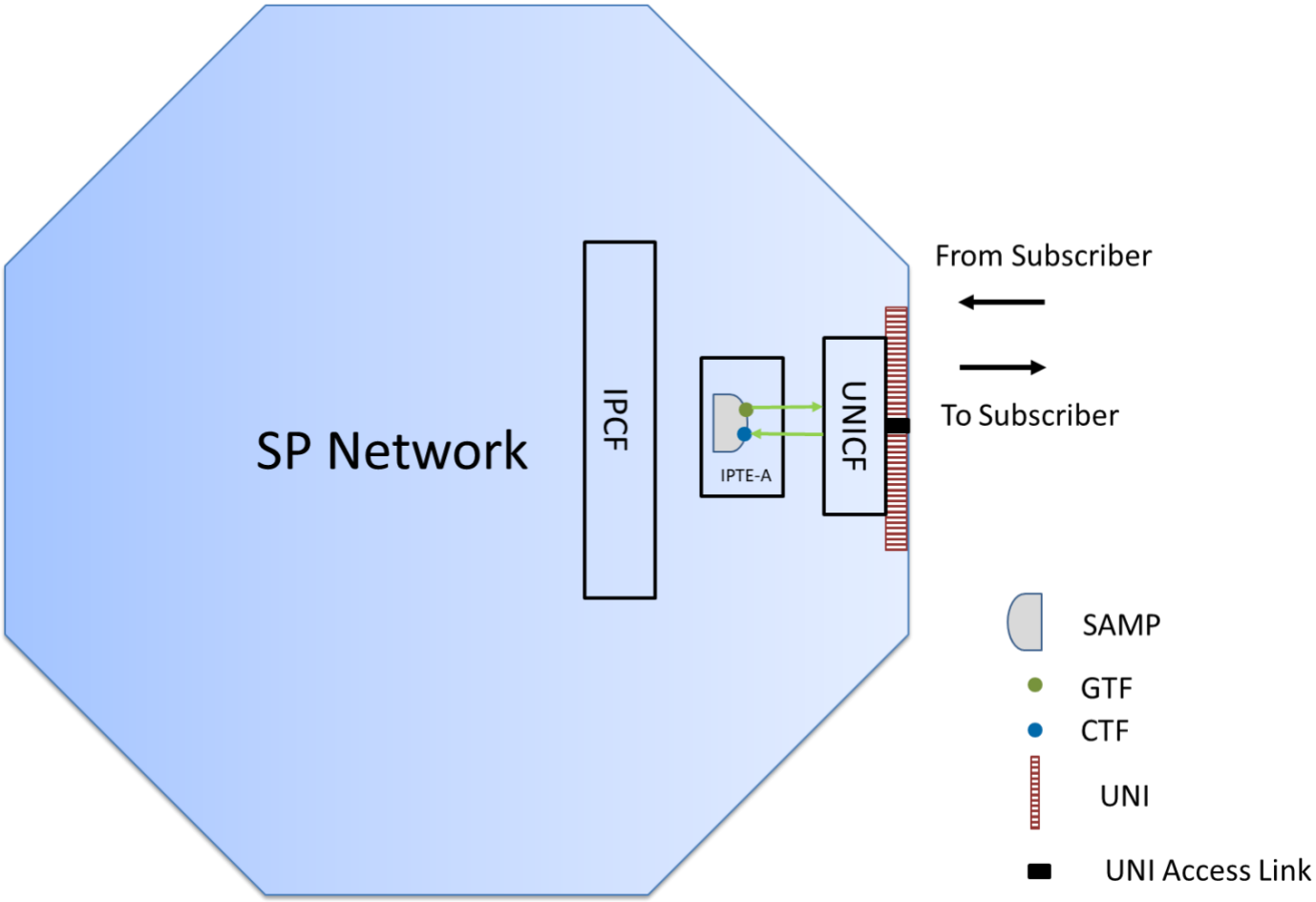

Figure 6 – Downward Facing SAMP Location in IPTE-A on the SP's side of the UNI

Figure 6 shows the location of a Downward facing SAMP in an IPTE-A on the SP's side of the UNI. Packets generated by the GTF pass through the UNICF and to the Subscriber's equipment and packets received from the Subscriber's equipment pass through the UNICF before being counted by the CTF.

[R4] An implementation of a Down SAMP in an IPTE-A on the SP's side of the UNI **MUST** be located such that IP Test Packets are processed by the UNICF and not by the IPCF.

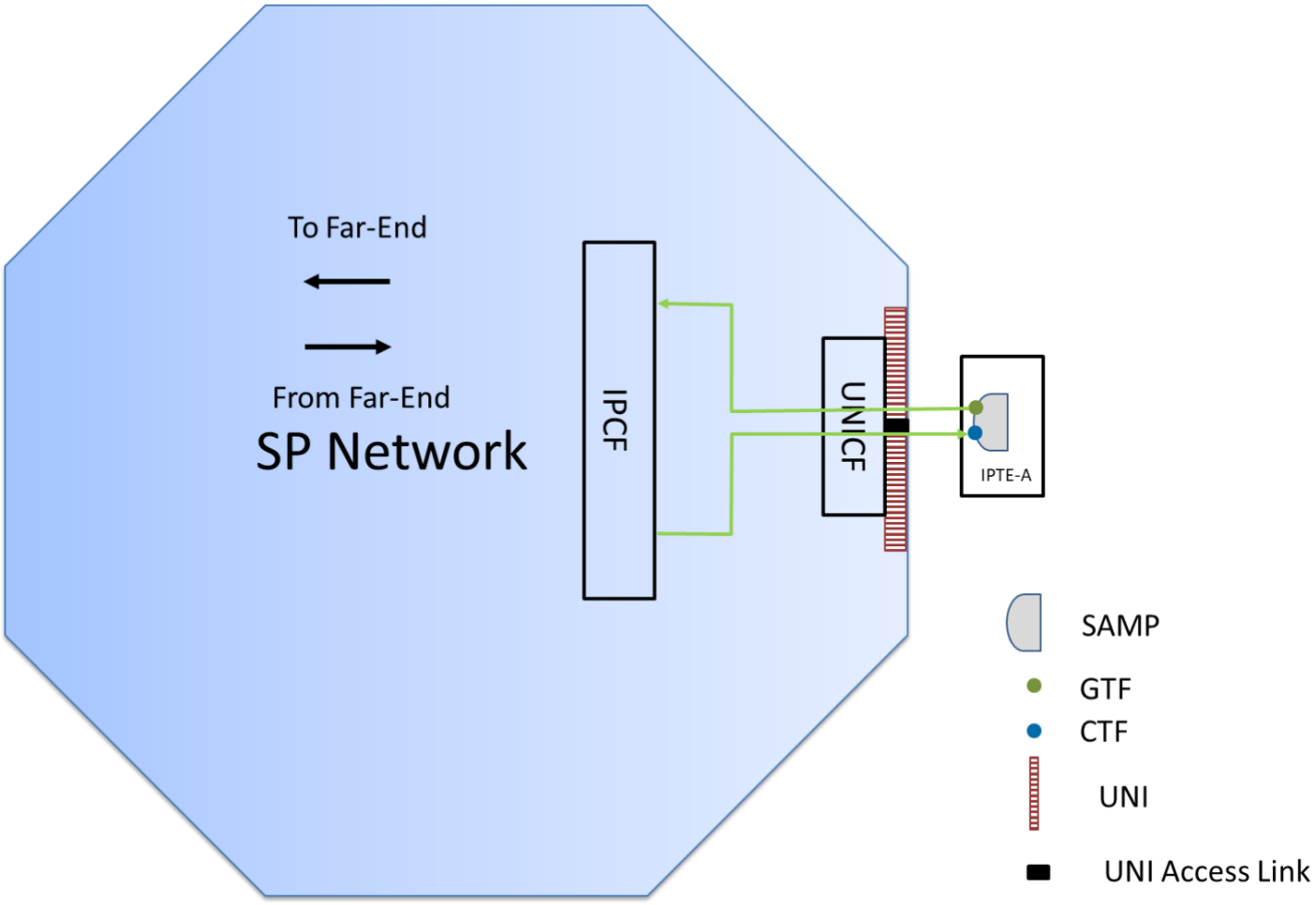

Figure 7 – Downward Facing SAMP Location in IPTE-A on the Subscriber's Side of the UNI

Figure 7 shows the location of a Down SAMP in an IPTE-A on the Subscriber's side of the UNI. The IPTE-A is instantiated within the Subscriber's equipment in coordinated testing between the SP and the Subscriber. Packets generated by the GTF pass through the UNI, UNI Access Link, the UNICF and may pass through the IPCF and to the far-end. Packets received from the far-end pass through the IPCF, UNICF, UNI Access Link, and UNI before being counted by the CTF.

8.4 SAMP Locations for an IPTE-I

The following figures show the location of SAMPs associated with an IPTE-I in relationship to processing functions within the SP Network. The specific way that the SAMPs and processing functions are implemented is outside the scope of this document, so long as the overall behavior is consistent with the arrangement specified below. In particular, it is not specified whether the processing functions are all implemented within a single device or distributed over multiple devices.

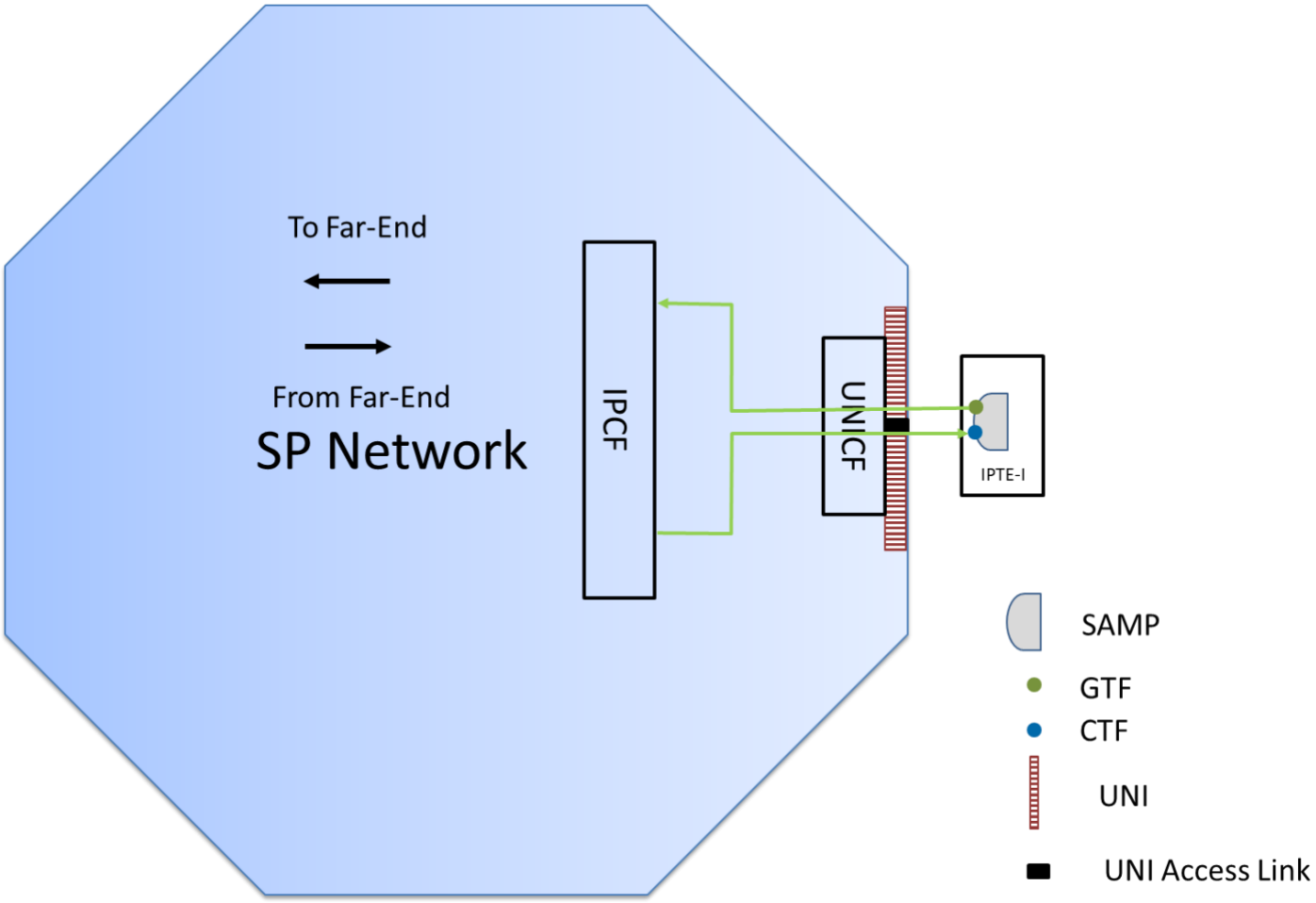

Figure 8 – Downward Facing SAMP Location in IPTE-I

Figure 8 shows the location of a Downward facing SAMP in an IPTE-I on the Subscriber's side of the UNI. The SAMP is located so that packets generated by the GTF pass through the UNI, UNI Access Link, UNICF, and may pass through the IPCF to the far-end. Packets received from the far-end pass through the IPCF, UNICF, UNI Access Link, and UNI before being counted by the CTF.

9 Service Activation Testing Use Cases and Test Cases

SAT Use Cases and Test Cases are described in this section.

Use Cases describe the scenario in which SAT is carried out, in terms of which elements of the service are being activated. There are four Use Cases for SAT:

- Use Case 1 - Testing a new UNI and its UNI Access Links
- Use Case 2 - Testing a new UNI Access Link being added to an existing UNI
- Use Case 3 - Testing a new IPVC and its initial set of IPVC EPs
- Use Case 4 - Testing a new IPVC EP being added to an existing IPVC.

In Use Case 1, the new UNI and UNI Access Links are tested at the same time since UNI Service Attributes cannot be verified until a UNI Access Link is active. In Use Case 2, the UNI Access Link is tested by itself. In Use Case 3, the IPVC Service Attributes and IPVC EP Service Attributes are tested from UNI to UNI for a set of IPVC EPs agreed to by the Subscriber and the Service Provider. In Use Case 4, the IPVC EP Service Attributes for the new IPVC EP are tested from the UNI to the Test End Point within the Service Provider's network, before the IPVC EP is joined to the IPVC. Test Cases describe the location of various types of IPTEs or equipment in reference to the UNICF and IPCFs. The following Test Cases are described in this document:

- Test Case 1 - UNI Access Link MTU; and UNI Ingress/Egress Bandwidth Profile Envelopes or UNI Access Link Ingress/Egress Bandwidth Profile Envelopes, if they are implemented in the UNICF
- Test Case 2 - UNI Access Link BFD
- Test Case 3 - New IPVC from Service Provider side of UNI
- Test Case 4 - New IPVC from Subscriber side of UNI
- Test Case 5 - New IPVC EP from Service Provider side of UNI
- Test Case 6 - New IPVC EP from Subscriber side of UNI

The relationships between Use Cases and Test Cases are shown in Table 4.

Use Case	Test Cases	Comments
Use Case 1 - New UNI/UNI Access Link	Test Case 1 (UNI/UNI Access Link) Test Case 2 (UNI Access Link BFD)	UNI or UNI Access Link BWP Envelopes are tested with Test Case 1 if implemented in the UNICF.
Use Case 2 - New UNI Access Link for an existing UNI	Test Case 1, (UNI/UNI Access Link) Test Case 2 (UNI Access Link BFD)	UNI or UNI Access Link BWP Envelopes are tested with Test Case 1 if implemented in the UNICF.
Use Case 3 - New IPVC and initial IPVC EPs	Test Case 3 or 4	UNI or UNI Access Link BWP Envelopes are tested with Test Case 3 or 4 if implemented in the IPCF.
Use Case 4 - New IPVC EP for an existing IPVC	Test Case 5 or 6	UNI or UNI Access Link BWP Envelopes are tested with Test Case 5 or 6 if implemented in the IPCF.

Table 4 – Use Case/Test Case Overview

Note: If a UNI Access Link is being added to an existing UNI with a UNI BWP Envelope enabled, testing of the UNI BWP Envelope is service affecting and should be coordinated with the Subscriber.

Verification of UNI and UNI Access Link Service Attributes is done using Test Cases 1 and 2. If the UNI or UNI Access Link BWP Envelopes are implemented in the IPCF, testing of the BWP Envelopes is done using Test Cases 3, 4, 5, or 6.

When testing UNI Access Link Service Attributes, the IPTE or THCP is connected so that IP Test Packets generated by the GTF and received by the CTF pass through the UNI Access Link under test. The method used to do this depends on how the UNI Access Link is configured. As an example, when the UNI Access Link is identified by a VLAN ID, the IP Test Packets generated by the IPTEs are configured with that VLAN ID. When multiple UNI Access Links exist on a single UNI, it might not be possible to ensure that all IP Test Packets pass on the correct UNI Access Link. In this case, the UNI Access Link Service Attributes are not tested.

The six Test Cases are described in the following sections. Figures are provided describing the location of SAMPs and THCPs and the IPCFs and UNICFs.

9.1 Test Case 1 - New UNI or UNI Access Link

Figure 9 Test Case 1, shows SAT being done on a new UNI or UNI Access Link.

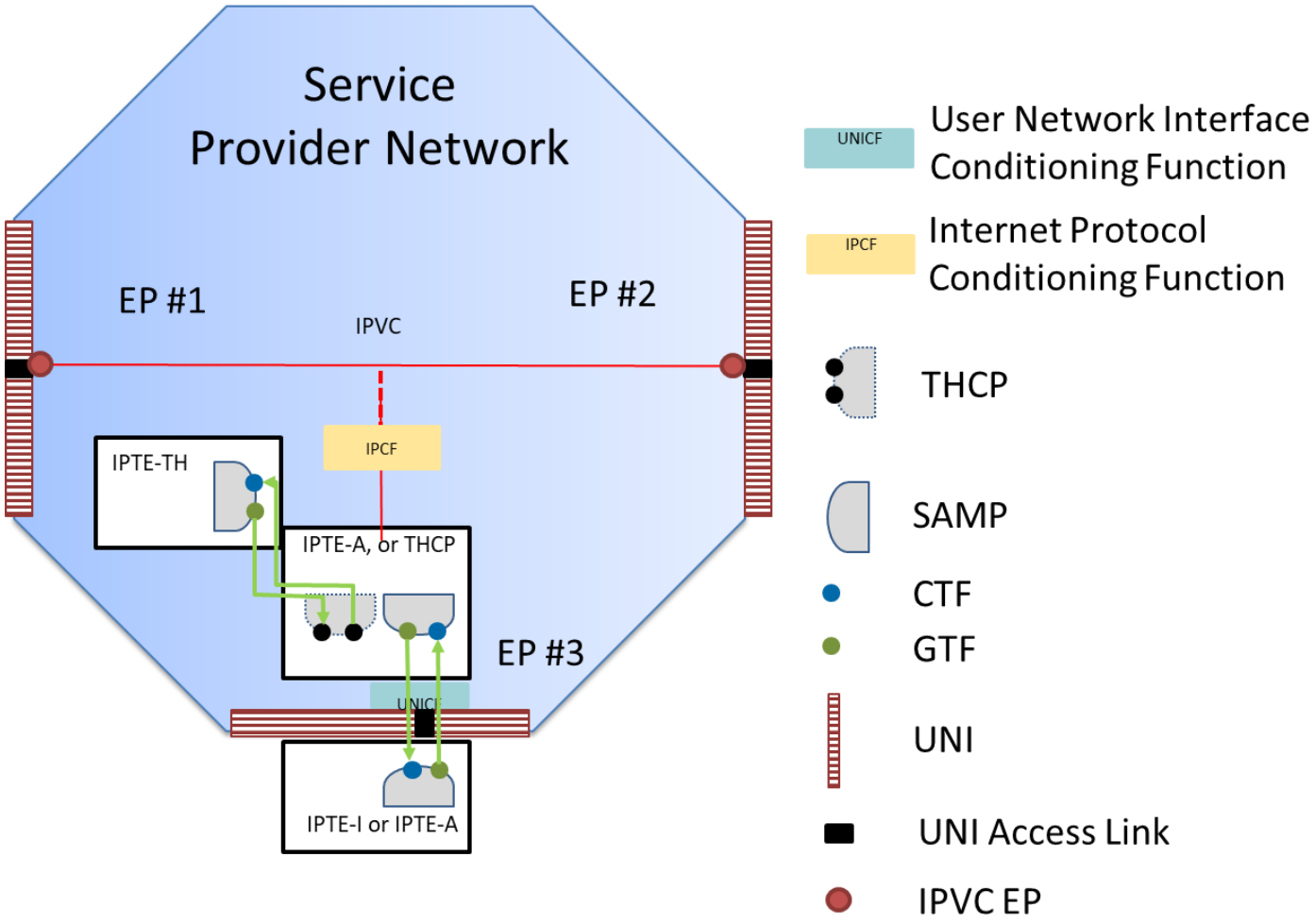

Figure 9 – Test Case 1: New UNI/UNI Access Link Service Attributes except BFD

Test Case 1 can be used to test the UNI Access Link MTU, and, if implemented in the UNICF, the UNI Ingress Bandwidth Profile Envelope, UNI Egress Bandwidth Profile Envelope, UNI Access Link Ingress Bandwidth Profile Envelope and UNI Access Link Egress Bandwidth Profile Envelope. An IPTE-A or IPTE-I is placed on the Subscriber side of the UNI. An IPTE-A, or a THCP/IPTE-TH is used on the Service Provider side of UNI between the UNICF and the IPCF. Test packets pass across the UNI/UNI Access Link but do not pass further into the Service Provider's network.

9.2 Test Case 2 - UNI Access Link BFD

Figure 10 Test Case 2, shows the testing of UNI Access Link BFD Service Attributes.

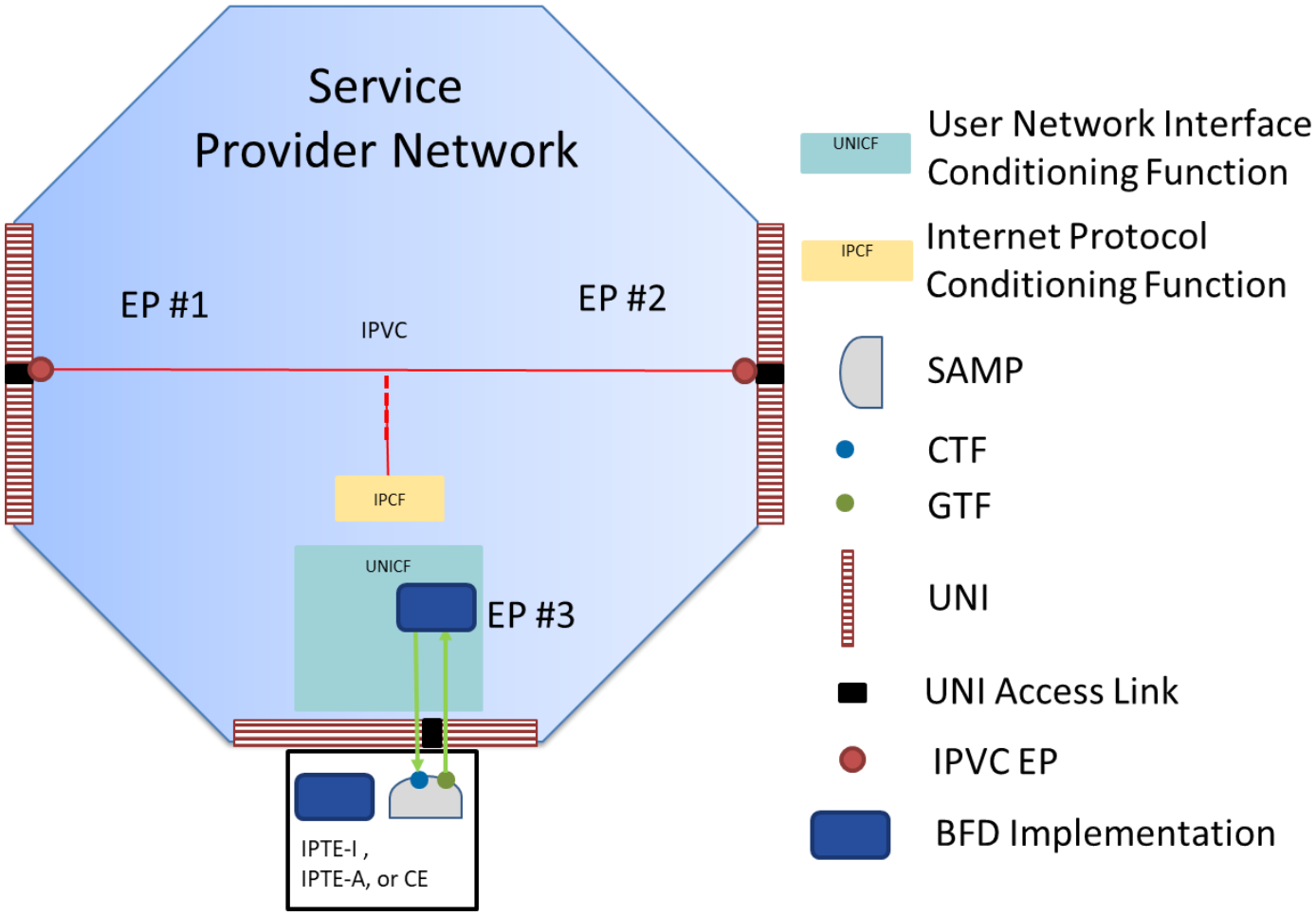

Figure 10 – Test Case 2: New UNI Access Link BFD Service Attribute

Test Case 2 performs testing on the UNI Access Link BFD Service Attribute. Instead of using an IPTE on the Service Provider's side of the UNI, the actual SP equipment that is a part of the service configuration is used to test that BFD is correctly configured and operating. On the Subscriber's side of the UNI the Service Provider may use an IPTE-I or an IPTE-A if the Subscriber's equipment is not present. If the Subscriber's equipment is present and configured, the test is performed using it.

9.3 Test Case 3 - New IPVC and IPVC EPs from Service Provider's Side of UNI

Figure 11 Test Case 3, shows SAT being performed on a new IPVC.

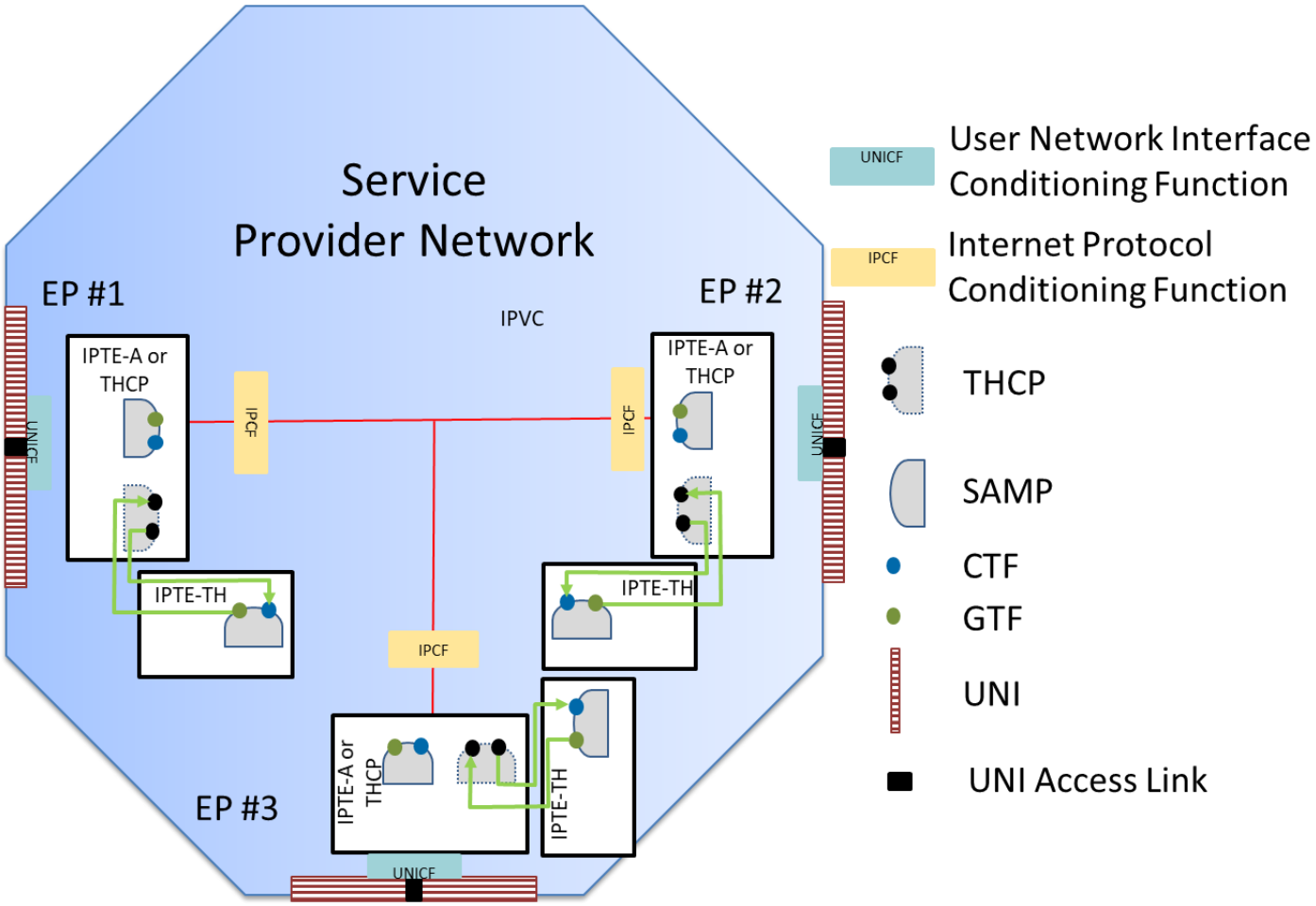

Figure 11 – Test Case 3: New IPVC Activation to Verify IPVC and IPVC EP Service Attributes

Test Case 3 places IPTE-As or THCP/IPTE-THs on the Service Provider side of the UNI. All packets generated and received pass through the appropriate IPCF. This Test Case is used to test IPVC and IPVC EP Service Attributes. Packets are exchanged between each pair of IPTEs (e.g. EP 1 - EP 2, EP 1 – EP 3, EP 2 – EP 3) agreed to between the Service Provider and the Subscriber. UNI and UNI Access Link BWP Envelopes may be tested with this Test Case if they are implemented in the IPCFs.

Note: in this Test Case and others where multiple IPTE-THs are shown, the actual configuration might be a single IPTE-TH with multiple interfaces that are connected to multiple THCPs in the Service Provider's network. If this is the case, Packet Delay and Packet Loss between the THCP and the IPTE-TH must be considered for all measurements.

9.4 Test Case 4 - New IPVC and IPVC EPs from the Subscriber's Side of the UNI

Figure 12 Test Case 4, shows SAT being performed on a new IPVC from the Subscriber's side of the UNI.

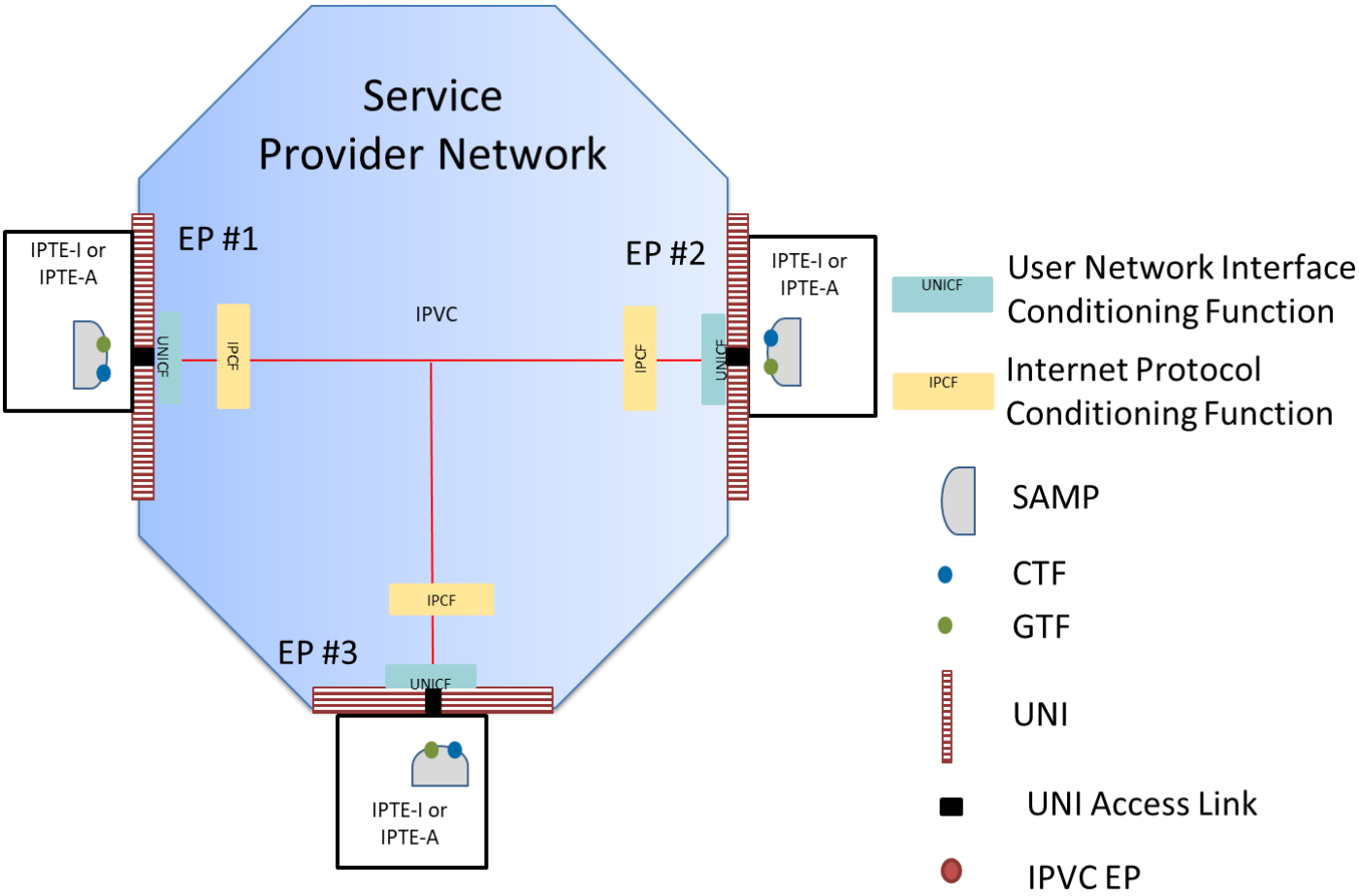

Figure 12 – Test Case 4: New IPVC Activation to Verify IPVC and IPVC EP Service Attributes from the Subscriber side of the UNI

Test Case 4 places IPTE-Is or IPTE-As on the Subscriber's side of the UNI. All packets generated and received pass through the UNICF and appropriate IPCF. This Test Case is used to test IPVC and IPVC EP Service Attributes. Packets are exchanged between each pair of IPTEs (e.g. EP 1 - EP 2, EP 1 – EP 3, EP 2 – EP 3) agreed to by the Service Provider and Subscriber. All Bandwidth Profile Envelopes can be tested using this test case, regardless of whether the behavior is implemented in the UNICF or IPCF.

9.5 Test Case 5 - New IPVC EP to an existing IPVC from Service Provider's Side of the UNI

Figure 13 Test 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.

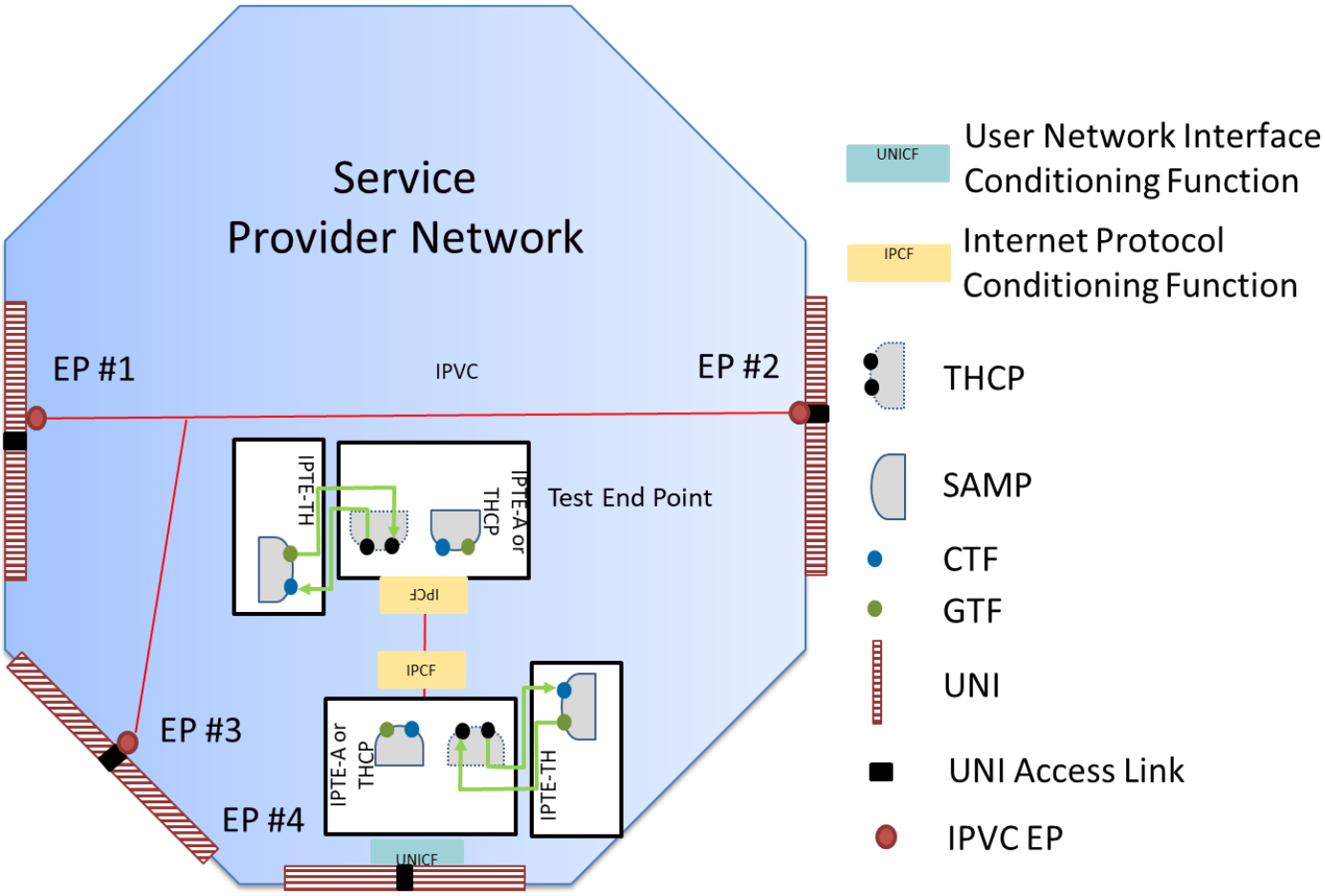

Figure 13 – Test Case 5: New IPVC EP Activation Testing from the Service Provider Side of the UNI

Test Case 5 places an IPTE-A or THCP/IPTE-TH at the UNI of the new IPVC EP and an IPTE-A or THCP/IPTE-TH at a Test End Point within the Service Provider's network. These are placed so that packets generated and received by the IPTEs pass through the appropriate IPCF. Any Bandwidth Profile Envelopes implemented in the IPCF can be tested in this configuration. In the case of the IPTE placed at the Test End Point in the Service Provider's network, an IPCF is configured to resemble an IPVC EP within the service under test. The IPCF located at the Test End Point within the Service Provider's network is intended to function as if it were at a UNI within the IPVC. The Service Provider determines which Service Attributes are configured identically to the Service and which are modified to function correctly with the point in the network that is selected. As an example, the UNI Access Link may be identified by something other than a VLAN ID at this point. Testing is performed between the new IPVC EP and the Test End Point simulating an IPVC EP at a UNI in the service.

9.6 Test Case 6 - New IPVC EP to an Existing IPVC from the Subscriber's Side of the UNI

Figure 14 Test Case 6, shows an example of a new IPVC EP (EP #4) being added to an existing IPVC where the Service Provider is testing from the Subscriber side of the UNI.

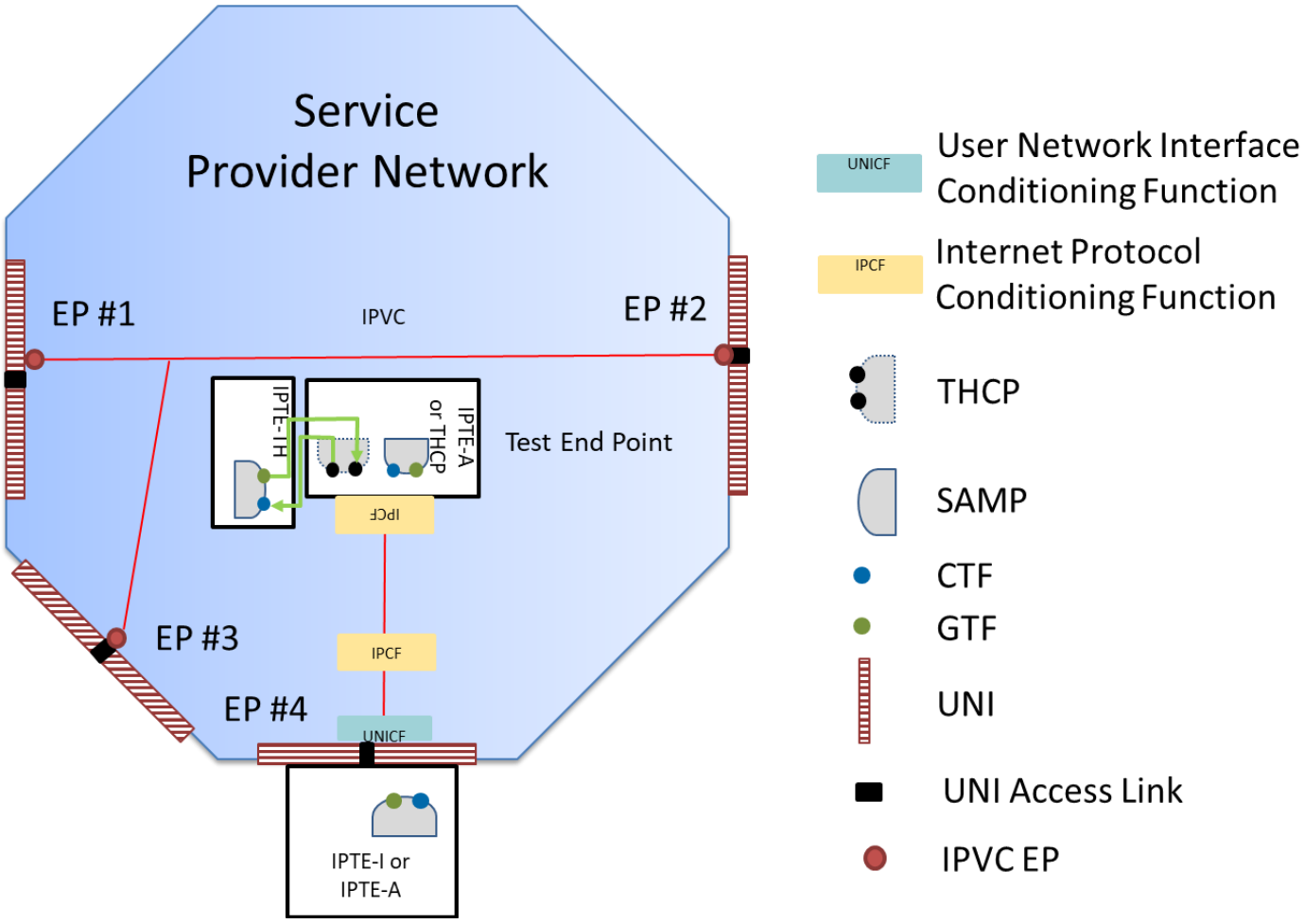

Figure 14 – Test Case 6: New IPVC EP Activation Testing from the Subscriber side of the UNI

Test Case 6 places an IPTE-A or IPTE-I at the Subscriber's side of the UNI of the new IPVC EP and an IPTE-A or THCP/IPTE-TH at the Test End Point within the Service Provider's network. The IPTE-I or IPTE-A located at the Subscriber's side of the UNI is placed so that packets generated and received by the IPTE pass through the UNICF and the IPCF. In the case of the IPTE placed at the Test End Point in the Service Provider's network, an IPCF is configured to resemble the IPVC and IPVC EP Service Attributes of the service under test. The IPCF located at the Test End Point within the Service Provider's network is intended to function as if it were at a UNI within the IPVC. The Service Provider determines which Service Attributes are configured identically to the Service and which are modified to function correctly with the point in the network that is selected. As an example, the UNI Access Link may be identified by something other than a VLAN ID at this point. Testing is performed between the new IPVC EP and the Test End Point simulating an IPVC EP at a UNI in the service. The IPTE-A or THCP is located so that packets generated and received by the IPTE pass through the appropriate IPCF. All Bandwidth Profile Envelopes can be tested using this test case, regardless of whether the behavior is implemented in the UNICF or IPCF.

10 Verification of Service Attribute Values

IP Service Attributes are defined in MEF 61.1 [15]. This section defines how those Service Attribute values are verified.

For a specific service, each Service Attribute can either be 1) ***Tested*** using one of the test methodologies defined in section 11 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 following bullets explain the columns in tables.

- The first column of each table specifies the Service Attribute.
- The second column of the Service Attribute tables, Report or Test, indicates if it is mandatory, optional, or Not Applicable (N/A) to report or test the Service Attribute. There are sub-columns under Report or Test header that reflect separate use cases and if the Service Attribute is reported, tested, or N/A. These cover different Use Cases as identified in the table and as shown in section 9. N/A indicates that no Report or Test is required. Reporting or Testing of the Service Attribute is mandatory unless otherwise noted.
- The third column of the Service Attribute tables specifies which SAT methodology is utilized to verify the Service Attribute.
- The fourth column of the Service Attribute tables is used for comments and notes.

10.1 Configuration Testing

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

10.1.1 SAT Configuration Verification Requirements for the UNI Service Attributes

Table 5 shows the SAT configuration verification requirements for the UNI Service Attributes.

UNI Service Attribute	Report or Test		SAT Methodology	Comments
	New UNI and New UNI Access Link	Existing UNI: New UNI Access Link, New IPVC and IPVC EPs or New IPVC EP in an existing IPVC		
UNI Identifier	Report	Report Optional	N/A	
UNI Management Type	Report	Report Optional	N/A	
UNI List of UNI Access Links	Report	Report Optional	N/A	
UNI Ingress Bandwidth Profile Envelope	Report, Test (see comments)	Report Optional, Test (see comments)	11.3.4	If *None* report, if not *None* see below.
UNI Egress Bandwidth Profile Envelope	Report, Test (see comments)	Report Optional, Test (see comments)	11.3.4	If *None* report, if not *None* see below.
UNI List of Control Protocols	Report	Report Optional	N/A	
UNI Routing Protocols	Report	Report Optional	N/A	
UNI Reverse Path Forwarding	Report	Report Optional	N/A	

Table 5 – Per UNI Configuration Service Attributes

Note: If a BWP Envelope Service Attributes is not *None*, testing is mandatory and is performed either for a new UNI (if the behavior is implemented in the UNICF) or when the first IPVC EPs are added at the UNI (if the behavior is implemented in the IPCF). If there are existing IPVC EPs at the UNI, they could be impacted by testing of this Service Attribute; therefore, testing is optional when subsequent IPVC EP(s) are activated at the UNI or when a new UNI Access Link is added to a UNI that has existing IPVC EPs. In these cases, maintenance time with the Subscriber must be arranged for any existing services before testing is performed.

[R5] The Service Provider **MUST** execute actions not indicated as optional for new UNIs as shown in Table 5.

[R6] The Service Provider **MUST** test the UNI Ingress Bandwidth Profile Envelope Service Attribute value (if the value is not None) and the UNI Egress

Bandwidth Profile Envelope Service Attribute value (if the value is not None) either:

- for a new UNI; or
- when the first IPVC EPs are activated at a UNI

The Service Provider may execute actions indicated as Optional in Table 5.

Note: If the UNI Ingress/Egress BWP Envelope is not *None* it may require an IPVC EP being configured on the UNI before the BWP Envelope can be tested.

10.1.2 SAT Configuration Verification Requirements for the UNI Access Link Service Attributes

Table 6 shows the SAT configuration verification requirements for the UNI Access Link Service Attributes. For the case where a Subscriber UNI Access Link is brought into service at the same time as the UNI, testing of both sets of Service Attributes is done at the same time. For the case where a Subscriber UNI Access Link is added to an existing UNI, the Subscriber UNI Access Link Service Attributes may or may not be tested, since there could be impacts to service on the existing Subscriber UNI Access Link. It is left up to the Service Provider and Subscriber to determine the need for testing. Testing UNI Access Link Service Attributes requires using an IPTE placed as shown in Figure 9 or BFD implementation as shown in Figure 10.

UNI Access Link Service Attribute	Report or Test			SAT Methodology	Comments
	New UNI, New UNI Access Link	Existing UNI, New UNI Access Link	Existing UNI Access Link, New IPVC and New IPVC EPs or New IPVC EP added to existing IPVC		
UNI Access Link Identifier	Report	Report	Report Optional	N/A	
UNI Access Link Connection Type	Report	Report	Report Optional	N/A	
UNI Access Link L2 Technology	Report	Report	Report Optional	N/A	
UNI Access Link IPv4 Connection Addressing	Report	Report	Report Optional	N/A	
UNI Access Link IPv6 Connection Addressing	Report	Report	Report Optional	N/A	
UNI Access Link DHCP Relay	Report	Report	Report Optional	N/A	
UNI Access Link Prefix Delegation	Report	Report	Report Optional	N/A	
UNI Access Link BFD	Report, Test	Report, Test Optional	Report Optional, Test Optional	11.3.1.3 11.3.1.4	Test if not *None*.
UNI Access Link IP MTU	Report, Test Optional	Report, Test Optional	Report Optional, Test Optional	11.3.1.5	
UNI Access Link Ingress Bandwidth Profile Envelope	Report, Test (see comments)	Report, Test Optional	Report Optional, Test (see comments)	11.3.4	If *None* report, if not *None* see below.
UNI Access Link Egress Bandwidth Profile Envelope	Report, Test (see comments)	Report, Test Optional	Report Optional, Test (see comments)	11.3.4	If *None* report, if not *None* see below.
UNI Access Link Reserved VRIDs Service Attribute	Report	Report	Report Optional	N/A	

Table 6 – Per UNI Access Link Configuration Service Attributes

Note: If a UNI Access Link BWP Envelope Service Attribute is not *None*, testing is mandatory and can be performed either for a new UNI Access Link (if the behavior is implemented in the UNICF) or when the first IPVC EPs are added at the UNI (if the behavior is implemented in the IPCF). If there are existing IPVC EPs at the UNI, they could be impacted by testing of this Service Attribute; therefore. testing is optional when subsequent IPVC EP(s) are activated at the UNI or when a new UNI Access Link is added to a UNI that has existing IPVC EPs. In these cases, maintenance time with the Subscriber must be arranged for any existing services before testing is performed.

[R7] The Service Provider **MUST** execute actions not indicated as optional for the Service Attribute values on a new UNI Access Link as specified in Table 6.

[R8] The Service Provider **MUST** test the UNI Access Link Ingress Bandwidth Profile Envelope Service Attribute value (if the value is not *None*) and the UNI

Access Link Egress Bandwidth Profile Envelope Service Attribute value (if the value is not *None*) either:

- for all UNI Access Links in a new UNI; or
- for all UNI Access Links in a UNI when the first IPVC EPs are activated at the UNI.

The Service Provider may execute actions indicated as optional on UNI Access Link Service Attribute values as specified in Table 6.

10.1.3 SAT Configuration Verification Requirements for the IPVC Service Attributes

Table 7 shows the SAT configuration verification requirements for the IPVC Service Attributes.

IPVC Service Attributes	Report or Test		SAT Methodology	Comments
	New IPVC and New IPVC EPs	New IPVC EP to an existing IPVC		
IPVC Identifier	Report	Report	N/A	
IPVC Topology	Report	Report	N/A	
IPVC End Point List	Report	Report	N/A	
IPVC Packet Delivery	Report	Report	N/A	
IPVC Maximum Number of IPv4 Routes	Report	Report	N/A	
IPVC Maximum Number of IPv6 Routes	Report	Report	N/A	
IPVC DSCP Preservation	Report, Test	Report, Test	11.3.2.1	Report if *Enabled* or *Disabled*. Test when *Enabled*.
IPVC List of Class of Service Names	Report	Report	N/A	
IPVC Service Level Specification	Report	Report	N/A	Performance is tested separately
IPVC MTU	Report, Test	Report, Test	11.3.2.2	
IPVC Path MTU Discovery	Report, Test	Report	11.3.2.3	Test when *Enabled*
IPVC Fragmentation	Report, Test	Report, Test	11.3.2.4	Report *Enabled* or *Disabled*. Test when *Disabled* and IPVC Max IPv4 routes $\neq 0$
IPVC Cloud	Report	Report	N/A	
IPVC Reserved Prefixes	Report	Report	N/A	

Table 7 – Per IPVC Configuration Service Attributes

[R9] The Service Provider **MUST** execute actions on IPVC Service Attribute values as specified in Table 7.

Note: To avoid causing disruption to existing IPVC EPs, testing of a new IPVC EP being added to an existing IPVC is performed to the Test End Point within the Service Provider's network. IPVC Service Attributes are verified between the new IPVC EP and the Test End Point.

10.1.4 SAT Configuration Verification Requirements for the IPVC End Point Service Attributes

Table 8 shows the SAT configuration verification requirements for the IPVC End Point (IPVC EP) Service Attributes.

IPVC EP Service Attribute	Report or Test New IPVC EP for new or existing IPVC	SAT Methodology	Comments
IPVC EP Identifier	Report	N/A	
IPVC EP UNI	Report	N/A	
IPVC EP Prefix Mapping	Report, Test	11.3.3.1	Test only when non-empty
IPVC EP Maximum Number of IPv4 Routes	Report	N/A	
IPVC EP Maximum Number of IPv6 Routes	Report	N/A	
IPVC EP Ingress Class of Service Map	Report	N/A	
IPVC EP Egress Class of Service Map	N/A	N/A	
IPVC EP Ingress Bandwidth Profile Envelope	Report, Test	11.3.4	Test if not *None*.
IPVC EP Egress Bandwidth Profile Envelope	Report, Test	11.3.4	Test if not *None*.

Table 8 – Per IPVC EP Configuration Service Attributes

[R10] The Service Provider **MUST** execute actions on IPVC EP Service Attribute values as specified in Table 8.

10.2 Performance Testing

Performance testing is done after configuration testing to ensure that performance of the final configuration is tested. The purpose of performance testing is to verify that the service meets performance expectations. Performance testing does not verify that the service meets the SLS. Instead, it verifies that the service meets the SAC. SLS objectives are normally expressed over a long time period (e.g. one month) whereas SAT performance tests are performed over a shorter time period (e.g. 15 minutes). Therefore, the SP and Subscriber might agree to SAC that reflects better performance than the objectives in the SLS, so as to ensure a high likelihood of the SLS

objectives being met if the SAT tests pass. Two measurements are performed, Packet Delay and Packet Loss. The delay Performance Metrics (Packet Delay Percentile, Mean Packet Delay, Inter-Packet Delay Variation, Packet Delay Range) are calculated from Packet Delay. The loss Performance Metric (Packet Loss Ratio) is calculated from Packet Loss.

The Performance Metrics used for SAT are defined as follows. In each case, the Performance Metric applies either to one-way measurements between an ordered pair of SAMPs, or to two-way measurements between the GTF and CTF of a single SAMP (see section 11.1.3). In the latter case, a single SAMP can be thought of as being both the source SAMP and the destination SAMP. Performance Metrics are evaluated over a time period equal to the duration of the service performance test denoted T_{SP} (see section 11.4.1).

Note that in all cases, the definitions are equivalent to the corresponding definitions in MEF 61.1 [15] if the set S defined in MEF 61.1 [15] were to contain a single ordered pair of SLS-RPs corresponding to the source and destination SAMPs, and the time period T_k defined in MEF 61.1 [15] was equal to the test duration T_{SP}.

Packet delay for an IP Test Packet is defined as the time elapsed from the transmission of the first bit of the packet by the GTF in the source SAMP until the reception of the last bit of the packet by the CTF in the destination SAMP. In the case of an IPTE-TH, an adjustment may be made to account for the delay between the IPTE-TH SAMP and the THCP.

The Packet Delay Percentile over T_{SP} for given source and destination SAMPs, a given CoS Name, and a given percentile p is the p_{th} percentile of packet delay for Qualified IP Test Packets for that CoS Name that are sent by the source SAMP during time T_{SP} and are delivered to the destination SAMP. If there are no such packets, the Packet Delay Percentile is 0.

The Mean Packet Delay over T_{SP} for given source and destination SAMPs and a given CoS Name is the arithmetic mean of packet delay for Qualified IP Test Packets for that CoS Name that are sent by the source SAMP during time T_{SP} and are delivered to the destination SAMP. If there are no such packets, the Mean Packet Delay is 0.

The Inter-Packet Delay Variation over T_{SP} for given source and destination SAMPs, a given CoS Name, a given difference in packet transmission time x, and a given percentile v is the v_{th} percentile of the absolute differences between the packet delays of pairs of Qualified IP Test Packets for that CoS Name that are sent by the source SAMP during time T_{SP}, at times that differ by x, and that are delivered to the destination SAMP. If there are no such pairs of packets, the Inter-Packet Delay Variation is 0.

The Packet Delay Range over T_{SP} for given source and destination SAMPs, a given CoS Name, and a given Percentile r is the difference between the r_{th} Percentile of packet delay and the minimum packet delay for Qualified IP Test Packets for that CoS Name that are sent by the source SAMP during time T_{SP} and are delivered to the destination SAMP. If there are no such packets, the Packet Delay Range is 0.

The Packet Loss Ratio over T_{SP} for given source and destination SAMPs and a given CoS Name is the ratio (expressed as a percentage) of the number of lost Qualified IP Test Packets to the number of transmitted Qualified IP Test Packets, for Qualified IP Test Packets for that CoS Name that are sent by the source SAMP during time T_{SP}. If there are no such packets transmitted, the Packet Loss Ratio

is 0. The number of lost packets is the number of packets transmitted by the source SAMP less the number of packets received by the destination SAMP.

Table 9 lists the Performance Metrics used for SAT.

Performance Metric	Tested/Reported	SAT Methodology	Comments
Packet Delay Percentile	Tested	11.4.2	The SAC for Packet Delay Percentile can be as high as the 100th Percentile due to short test period. Note 1, Note 3
Mean Packet Delay	Tested	11.4.2	Note 1
Inter-Packet Delay Variation	Tested	11.4.2	Note 2, Note 3
Packet Delay Range	Tested	11.4.2	Note 2, Note 3
Packet Loss Ratio	Tested	11.4.2	
Note 1: Packet Delay Percentile and Mean Packet Delay performance form a pair for which this technical specification requires at least one be tested.			
Note 2: Inter-Packet Delay Variation and Packet Delay Range performance form a pair for which this technical specification requires at least one be tested.			
Note 3: Percentiles are calculated by the IPTE performing the Delay measurement or within the Element Control and Management (ECM) that manages the IPTE.			

Table 9 – Performance Metrics

[R11] When testing a new IPVC and new IPVC EPs as shown in Figure 11 and Figure 12, the Service Provider **MUST** test that the performance is within the applicable SAC per CoS Name between IPVC EPs agreed to by the Service Provider and Subscriber.

[R12] When testing a new IPVC EP being added to an existing IPVC as shown in Figure 13 and Figure 14, the Service Provider **MUST** test that the performance is within the applicable SAC per CoS Name between the IPVC EP and the Test End Point within the Service Provider's network.

[R13] When testing a new IPVC and new IPVC EPs or a new IPVC EP being added to an existing IPVC and verifying that the performance is within the applicable SAC per CoS Name, the Service Provider **MUST** test at least one of Packet Delay Percentile and Mean Packet Delay as specified in Table 9.

[R14] When testing a new IPVC and new IPVC EPs and verifying that the performance is within the applicable SAC per CoS Name, the Service Provider **MUST** test at least one of Packet Delay Range and Inter-Packet Delay Variation as specified in Table 9.

[O1] When testing a new IPVC EP being added to an existing IPVC and verifying that the performance is within the applicable SAC per CoS Name, the Service Provider **MAY** test at least one of Packet Delay Range and Inter-Packet Delay Variation, as specified in Table 9.

Note: An IPVC EP being added to an existing IPVC is not tested to existing IPVC EPs in the IPVC as shown in Test Cases 5 and 6. Thus, determining a valid SAC for Inter-Packet Delay Variation or Packet Delay Range is difficult, since only a segment of the IPVC is tested.

[D1] If the SAC for a CoS Name includes Performance Objectives for Mean Packet Delay but not Packet Delay Percentile, the SAC for that CoS Name **SHOULD** include objectives for Packet Delay Range.

[R15] When testing a new IPVC and new IPVC EPs or when testing a new IPVC EP being added to an existing IPVC and verifying that the performance is within the applicable SAC per CoS Name, the Service Provider **MUST** test Packet Loss Ratio as specified in Table 9.

11 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 contains subsections or methodologies that define the method used to verify a specific Service Attribute value configuration or the performance of a service. The validation of the configuration or performance is performed by sending pre-defined test traffic and verifying that the behavior is according to the Service Description. The test methodologies to perform this testing are detailed within this section.

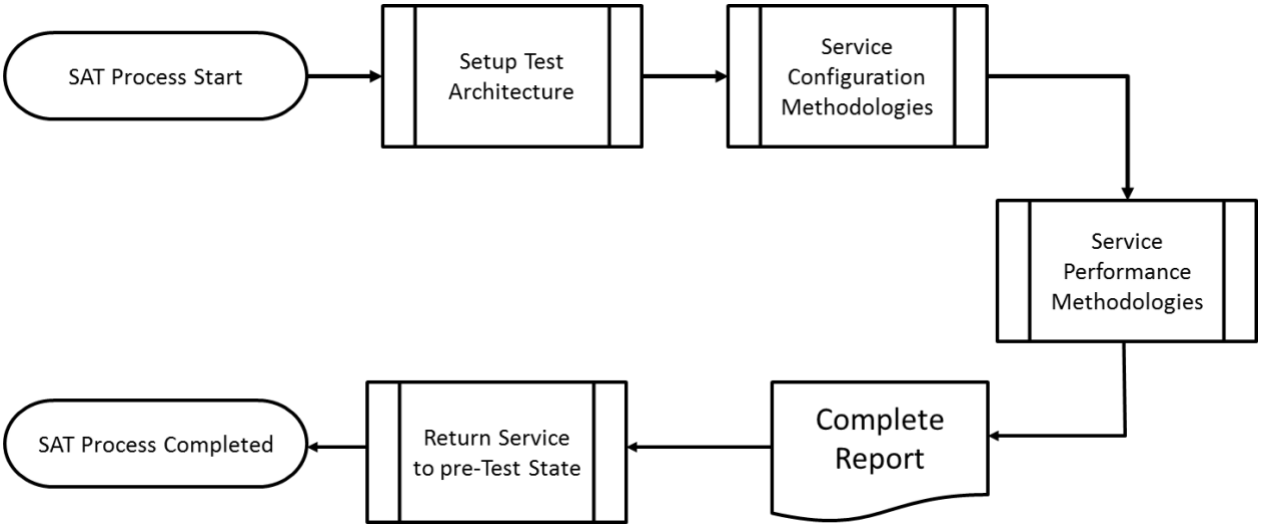

Figure 15 – Service Activation Test Process

Figure 15 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 step in the process can be done once for the device and not repeated for SAT for each service or may need to be done each time the IPTE is used.

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 Service Attributes described in section 10. Both reported and tested Service Attributes are included in the report. A Pass or Fail indication is provided per Service Attribute with this report.

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.

Note: When testing a new IPVC and new IPVC EPs, Configuration and Performance tests are performed between a set of IPVC EPs agreed to by the Subscriber and the Service Provider. This may mean that tests are not performed between all IPVC EPs within an IPVC. As an example, the Subscriber might require the Service Provider to test between their data center locations and all branch offices but not between branch offices since IP Data Packets do not normally pass from one branch office to another branch office.

11.1 Common Methodology Requirements

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

11.1.1 Test Packet Format and Length

The IP Test Packets generated by an IPTE for a SAT methodology need to comply with standards so that they are treated similarly to Subscriber Data Packets.

[R16] An implementation of an IPTE **MUST** generate packets that comply with IETF RFC 791 [3] for IPv4 Test Packets or IETF RFC 8200 [13] for IPv6 Test Packets.

[R17] An implementation of an IPTE **MUST** be able to generate a stream of packets with a single packet length.

[R18] An implementation of an IPTE **MUST** be configurable to generate packets within the range of 46-8982 bytes.

[D2] An implementation of an IPTE **SHOULD** be configurable to generate packets within the range of 8983-15,982 bytes.

IETF RFC 6985 [9] 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
46	110	238	494	1006	1262	1500	2094	8982	15,982	MTU

Table 10 – IMIX Values

The numerical values in Table 10 are modified from the values in RFC 6985 [9]. The RFC specifies values that appear to be Ethernet frame lengths at the wire. The values from RFC 6985 [9] have been reduced by 18 bytes to remove the Ethernet overhead from the value and to provide the IP Packet length. Using the values in Table 10 a test pattern can be specified with different length packets sent. As an example, ‘aaagg’ specifies a sequence of five IP Test Packets with lengths of 46 46 46 1500 1500 bytes. This pattern is repeated for the duration of the test.

[D3] An implementation of an IPTE **SHOULD** be capable of generating an IMIX for variable length packets as specified in IETF RFC 6985 [9] with modified values as shown in Table 10.

[CR1]<[D3] An implementation of an IPTE supporting an IMIX **MUST** be capable of generating a repeating pattern of at least eight elements as specified in Table 10.

[CR2]<[D3] An implementation of an IPTE supporting an IMIX **MUST** be capable of generating a repeating pattern of at least two different IP Packet lengths.

[CD1]<[D3] An implementation of an IPTE supporting an IMIX **SHOULD** be capable of generating a repeating pattern of up to 32 elements as specified in Table 10 containing at least eight different IP Packet lengths.

[CR3]<[D3] An implementation of an IPTE capable of generating an IMIX **MUST** repeat the variable length pattern as long as necessary during the test procedure from the first to the last IP Packet starting at the beginning of each test procedure.

[CD2]<[D3] An implementation of an IPTE capable of an IMIX **SHOULD** use a default IMIX pattern of IP Packet lengths of abcdefgh.

Packet lengths other than those specified in Table 10 can be supported by an IPTE implementation.

11.1.2 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 these devices. These requirements are specified in this section.

[R19] An IPTE implementation **MUST** maintain counts of sent and received IP Test Packets during the measurement period of a test.

[R20] When testing between two IPTEs, one-way packet delay **MUST** be measured.

[R21] When testing between two IPTEs, the one-way PLR **MUST** be calculated based on the sent and received packet counts.

[R22] When testing to a Loopback Function, the two-way PLR **MUST** be calculated based on the sent and received packet counts

See section 11.1.3 for a discussion on Time of Day clock synchronization and Time of Day clock accuracy.

[R23] An IPTE implementation **MUST** measure two-way packet delay when testing to an IP Loopback Function.

[R24] An IPTE implementation **MUST** be capable of calculating the following, as specified in section 10.2, based on the packet delay measurements performed during a test:

- Packet Delay Percentile
- Mean Packet Delay
- Inter-Packet Delay Variation
- Packet Delay Range.

SLS Objectives for Packet Delay Percentile, Inter-Packet Delay Variation and Packet Delay Range are specified using percentiles. This helps to eliminate extreme outliers when Performance Monitoring measurements are performed. Within this document the idea of SAT using percentiles has been identified as useful to align the SAT measurements with Subscriber expectations based on an SLS. Unlike Performance Monitoring, SAT might use percentiles of 100 or 0 to ensure that outliers are not eliminated during the SAT.

[D4] An IPTE implementation **SHOULD** be capable of the calculation of IR of received IP Test Packets.

[D5] An IPTE implementation **SHOULD** be capable of generating and receiving packets on multiple flows in a BWP Envelope at the same time.

The method used by a particular IPTE implementation (timestamp location, packet format, etc.) to perform delay measurements is outside the scope of this document.

The goal of SAT is to ensure that IP Test Packets meet the applicable SAC for each Test Methodology. This ensures that when the service is delivered to the Subscriber the Subscriber IP Data Packets meet agreed upon behavior. To accomplish this, IP Test Packets are sent in both directions between two IPTEs simultaneously, or between an IPTE and an IP Loopback Function. It is understood that starting or stopping the generation of IP Test 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.

[R25] When SAT is being performed between two IPTEs, the start of the test measurements in each direction **MUST** be simultaneous, i.e. within two seconds.

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.

[R26] An IPTE-TH, IPTE-A, or IPTE-I **MUST** allow a user or system to monitor the status of a test.

An IPTE can either send notifications of test status changes to the SP's support systems, can respond to queries about the test status from the SP's support systems, or both.

11.1.3 Test Measurements

A SAMP initiates a test by sending IP Test Packets from its GTF to either another SAMP, or to an IP Loopback Function, located at the far-end of the test. The far-end responds in one of the following ways:

- Has a SAMP that processes the IP Test Packet by adding additional time stamps, sequence numbers, or other information into a response IP Test Packet and sends the response IP Test Packet back to the near-end where the near-end CTF processes the packet and performs measurements, as shown in Figure 16
- Has a SAMP that processes the IP Test Packet received from the near-end SAMP, performs measurements on the IP Test Packet, and then discards it as shown in Figure 17
- Has an IP Loopback Function which swaps the source and destination IP Addresses and Port Numbers and returns the IP Test Packet to the near-end SAMP where the CTF processes, performs measurements on the IP Test Packet, and then discards it as shown in Figure 18.

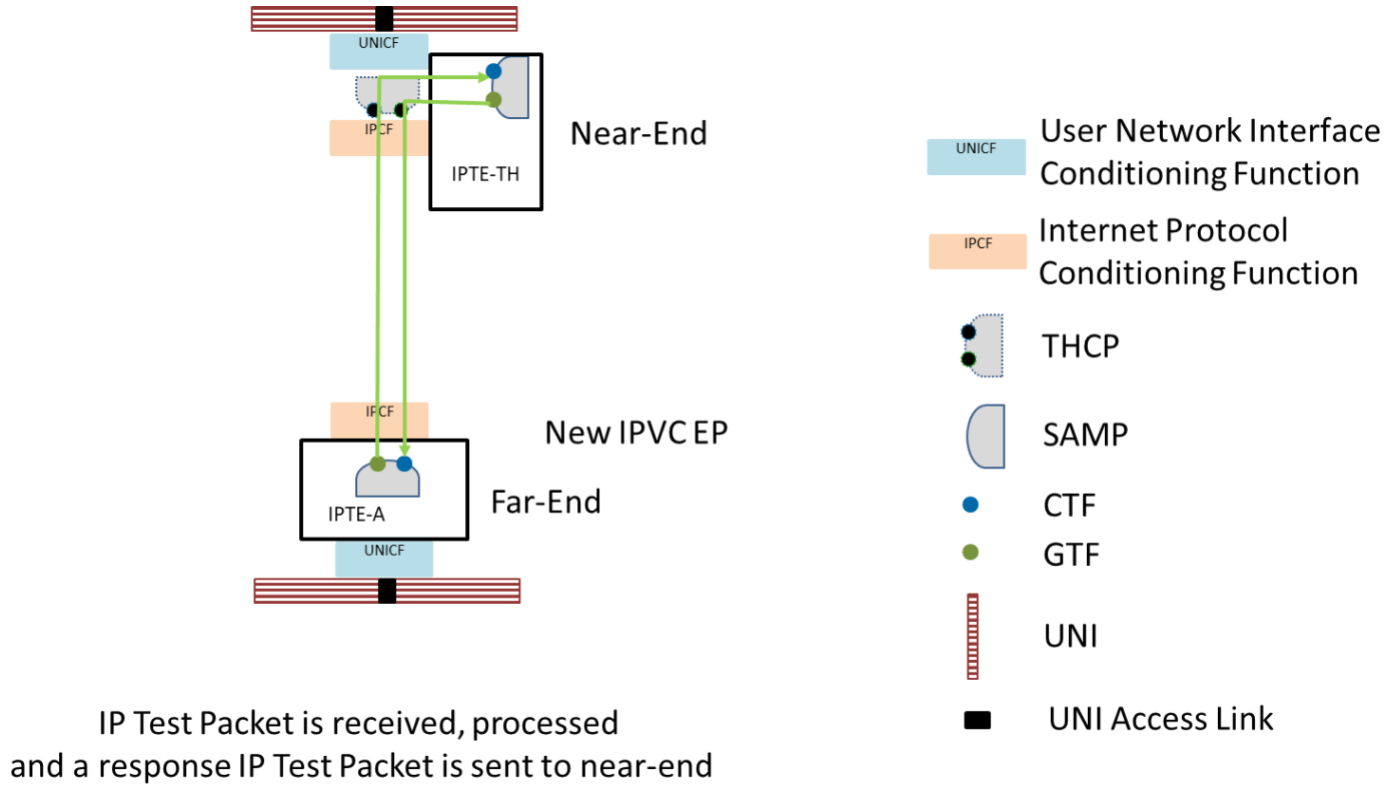

Figure 16 – Far-End SAMP Receives, Processes, and Sends Response IP Test Packet

Figure 16 shows an example of an IPTE-TH at the near-end and an IPTE-A at the far-end testing a new IPVC EP. The IPTE-TH generates IP Test Packets. The IPTE-A receives and processes the IP Test Packet. This processing might include adding time stamps when the IP Test Packets are received and are transmitted, adding sequence numbers to measure packet loss, or other mechanisms that might be useful by IPTE implementations. It then responds with a corresponding IP Test Packet. When this type of packet processing is performed by the far-end, one-way

measurements are possible in the Forward (near-end to far-end) and Backward (far-end to near-end) directions. Two-way measurements are also possible, if desired.

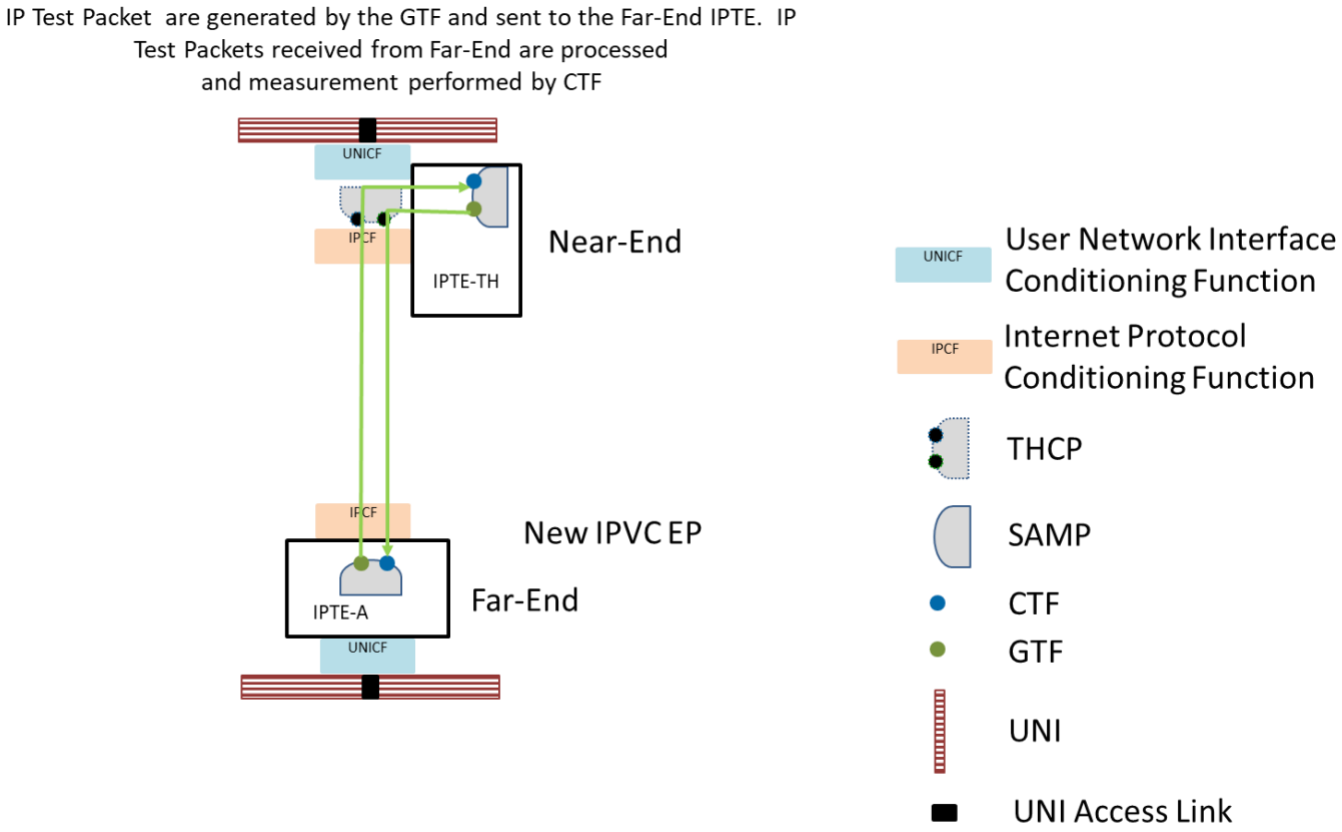

Figure 17 – Far-end SAMP Performs Measurements and Generates IP Test Packets

Figure 17 shows an example of an IPTE-TH at the near-end and an IPTE-A at the far-end testing a new IPVC EP. The IPTE-TH generates IP Test Packets. The IPTE-A CTF receives these packets, processes them, performs measurements on the IP Test Packets, and discards the packets. The IPTE-A GTF also generates IP Test Packets towards the near-end (IPTE-TH) where the near-end CTF processes the packets, measurements are performed, and the packets are discarded. One-way measurements are possible in the Forward (near-end to far-end) and Backward (far-end to near-end) directions.

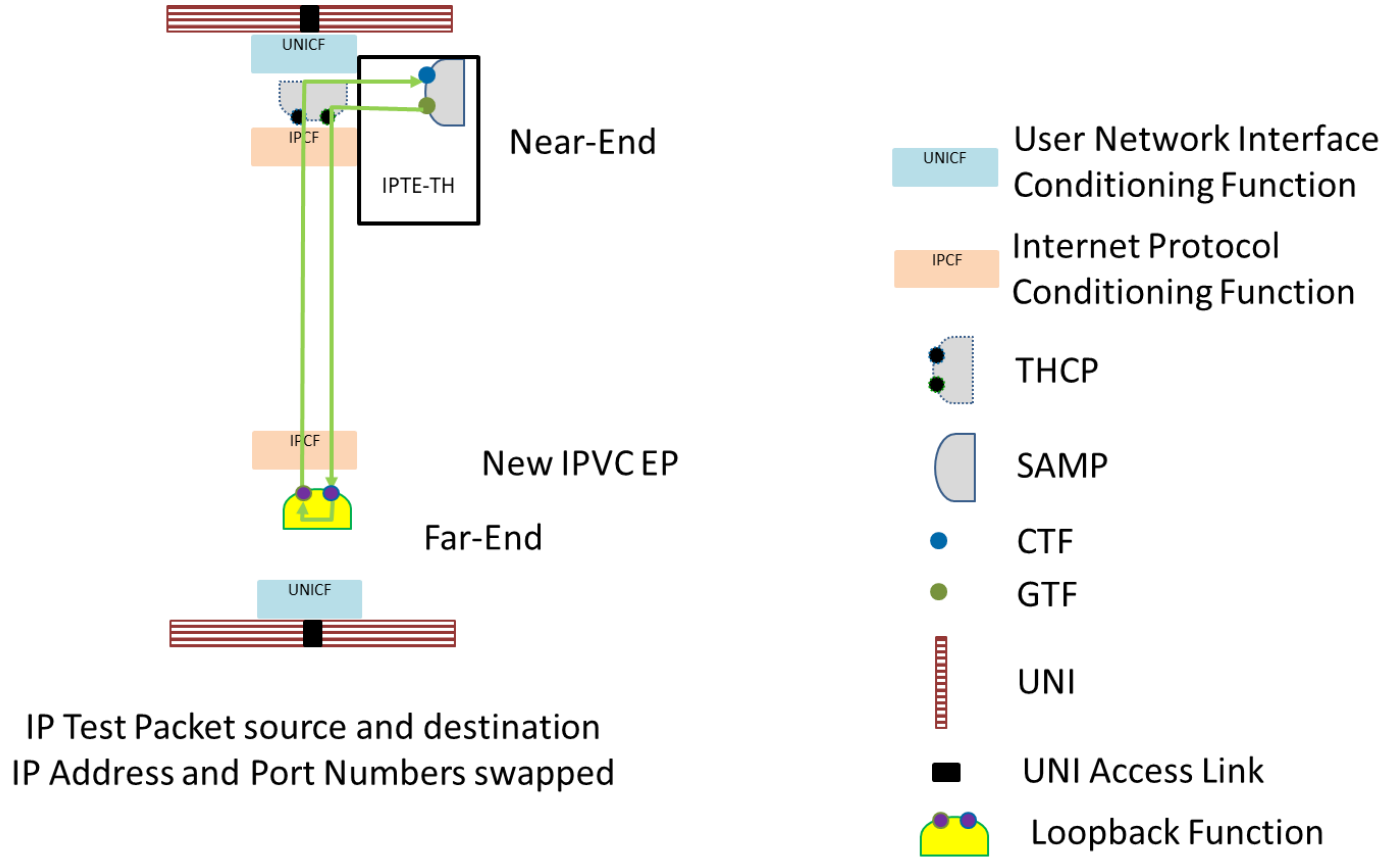

Figure 18 – Far-end Loopback Function Loops Back IP Test Packets

Figure 18 shows an example of the same test configuration with the far-end simply looping back the IP Test Packets. The IP Loopback Function does not process these packets in any way except to swap the source and destination IP Addresses and Port Numbers. This simple functionality at the far-end might be due to limited functionality at the far-end or in incompatible test packet formats between IPTEs. In this case, only two-way measurements are possible since the IP Loopback Function does not add any time stamps or sequence numbers to the IP Test Packets.

Accurate one-way packet delay measurements cannot be performed without Time of Day clock synchronization. Time of Day clock differences can lead to measurements that result in negative delay or excessive delay.

However, one-way packet delay measurements can be used to calculate Packet Delay Range and Inter Packet Delay Variation even without clock synchronization, since these metrics are based on differences between delay measurements not on the absolute values. Therefore, taking one-way measurements is required except when testing to an IP Loopback Function. The two one-way measurements can be summed and divided by 2 to provide an approximated one-way measurement for the purpose of calculating Packet Delay Percentile and Mean Packet Delay.

When testing to an IP Loopback Function, one-way measurements can be approximated by performing two-way Packet Delay and Packet Loss measurements and the results divided in half to obtain approximated one-way Packet Delay and Packet Loss measurements.

In both cases discussed above, this approximation is acceptable as long as the results indicate that this was how the one-way Packet Delay and Packet Loss measurements were determined.

The methods used by the IPTE implementation acting as a far-end of the test to perform measurements are beyond the scope of this document.

[R27] When testing between two IPTEs with Time of Day clock synchronization, One-way Packet Delay measurements **MUST** be used to calculate One-way Packet Delay Percentile, One-way Mean Packet Delay, One-way Packet Delay Range and One-way Inter-Packet Delay Variation.

[R28] When testing between two IPTEs without Time of Day clock synchronization, One-way Packet Delay measurements **MUST** be used to calculate One-way Packet Delay Range and One-way Inter-Packet Delay Variation.

[R29] When testing between two IPTEs without Time of Day clock synchronization, the sum of the One-way Packet Delay measurements in each direction, divided by 2, **MUST** be used to approximate One-way Packet Delay Percentile and One-way Mean Packet Delay.

[R30] When testing between an IPTE and an IP Loopback Function, Two-way Packet Delay measurements, divided by 2, **MUST** be used to approximate One-way Packet Delay Percentile, One-way Mean Packet Delay, One-way Packet Delay Range and One-way Inter-Packet Delay Variation.

[R31] Where two one-way Packet Delay measurements are summed and divided by two or two-way Packet Delay measurements are performed, and one-way Packet Delay results are reported the Test Report **MUST** indicate that the result was approximated.

11.2 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. SAC are defined for short periods of time, versus a 30-day period that can be used for an SLS. SAC values can be stricter than the corresponding SLS objectives, due to the shorter time period. A direct correlation between SLS objectives and SAC values does not need to be done. The Configuration tests use a snap shot of the service and Performance tests use the minimum duration determined to meet Service Provider and Subscriber expectations.

SAC are specified for each tested Service Attribute, Performance Metric, CoS Name, and (unless testing to an IP Loopback Function) for each ordered pair of IPTEs. When testing between two IPTEs, the SAC for each direction do not have to be the same, although they normally are. Examples of SAC that can be used for Configuration or Performance tests are IR_{SAC}, *Packet Delay Percentile*$_{SAC}$, *Mean Packet Delay*$_{SAC}$, *Inter-Packet Delay Variation*$_{SAC}$, *Packet Delay Range*$_{SAC}$, and *Packet Loss Ratio*$_{SAC}$. The uses of these SAC are shown in the test methodologies in section

11.3 and 11.4. The SAC do not have to be the same for each Test Methodology. Instead they are defined for each methodology.

[R32] SAC **MUST** be defined for each Service Attribute and Performance Metric that is tested as described in the test methodologies in sections 11.3 and 11.4.

[R33] The SAC **MUST** be agreed to by the Subscriber and Service Provider.

11.3 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 per test.

Service configuration tests include tests on the configuration of the IPVC, the IPVC EP, the UNI, and the UNI Access Link. The UNI configuration tests include two sub-processes, Ingress Bandwidth Profile Envelope and Egress Bandwidth Profile Envelope. The UNI Access Link configuration tests include five sub-processes, UNI Access Link BFD with SP as Active, UNI Access Link BFD with SP as Passive, UNI Access Link IP MTU, UNI Access Link Ingress Bandwidth Profile Envelope, and UNI Access Link Egress Bandwidth Profile Envelope. 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 three sub-processes, IPVC EP Prefix Mapping, IPVC EP Ingress Bandwidth Profile Envelope, and IPVC EP Egress Bandwidth Profile Envelope.

In each of the test methodologies described in this Section, when it is said that test packets are sent from an IPTE, it means that the test packets that are sent are expected to conform to all of the Service Attribute values of the service under test, except if otherwise indicated in the test methodology.

MEF 61.1 [15] section 9 describes the relationship between an IPVC and IPVC EP and a UNI Access Link. That relationship is not static and an IPVC EP can have a relationship with more than one UNI Access Link. For this reason, the service configuration tests for an IPVC and IPVC EP and a UNI Access Link are not linked to one another.

Figure 19, Figure 20, and Figure 21 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.

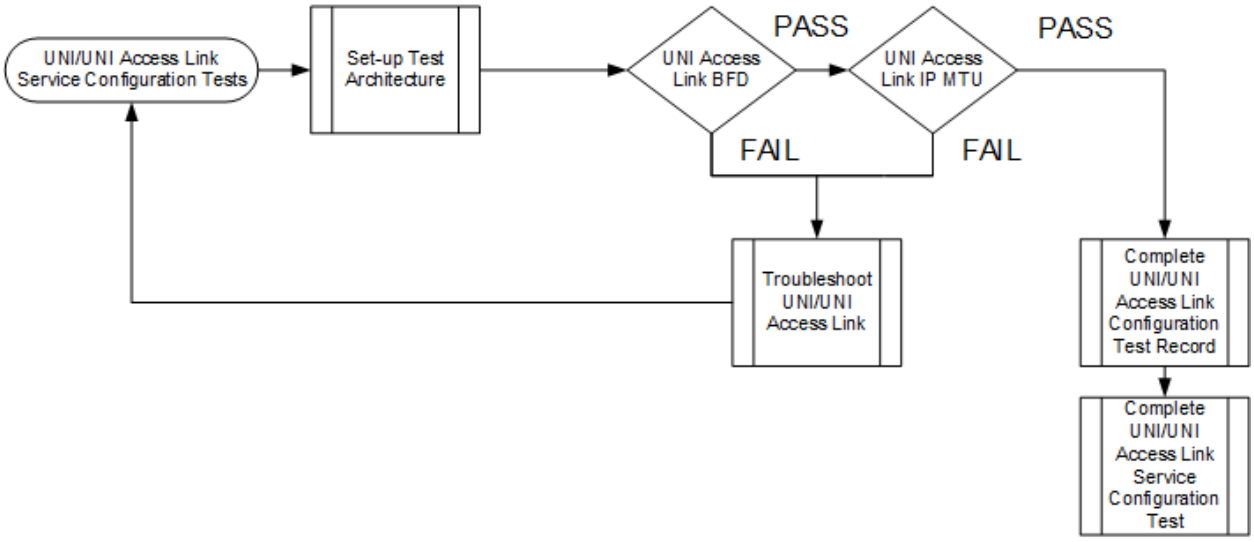

Figure 19 – UNI/UNI Access Link Service Configuration Tests

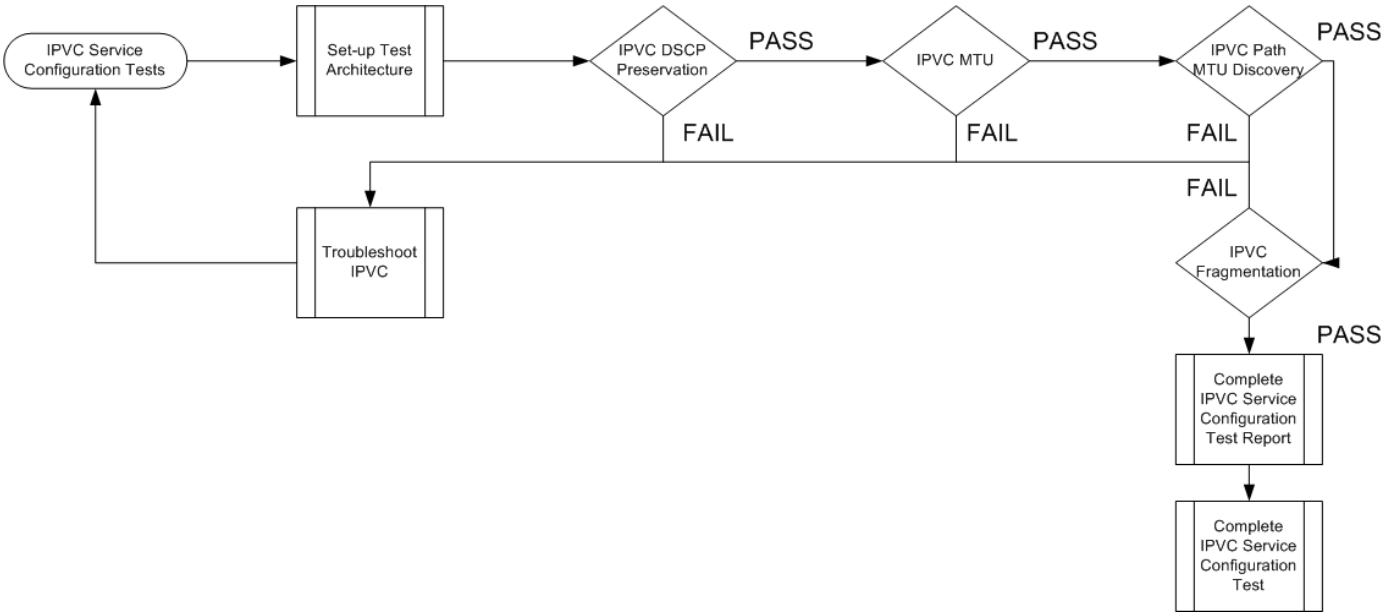

Figure 20 – IPVC Service Configuration Tests

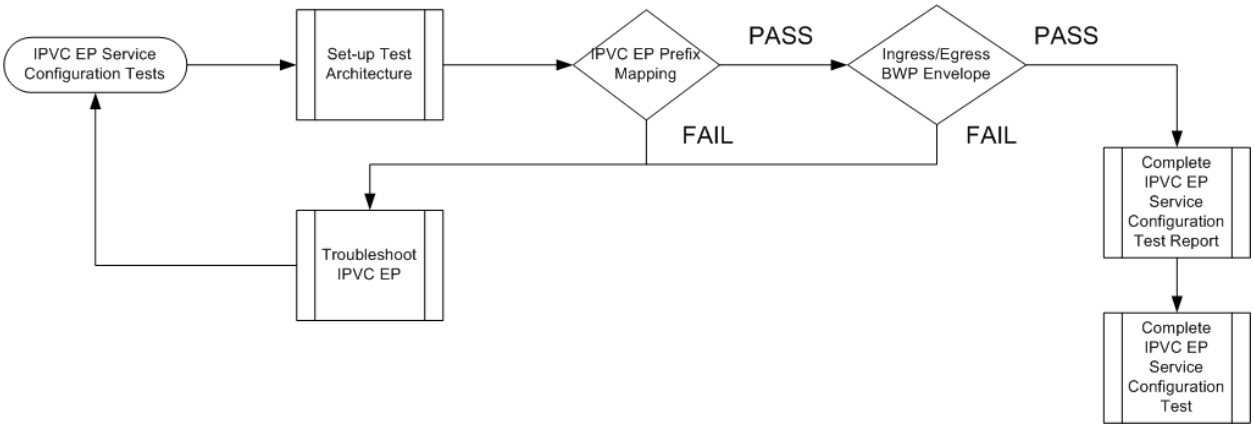

Figure 21 – IPVC EP Service Configuration Tests

The BWP Envelope tests for a UNI, UNI Access Link, or IPVC EP are all included in the Ingress/Egress BWP Envelope process step. The appropriate BWP Envelope test is performed at this time. The BWP Envelope tests are either performed in each direction, Ingress and Egress separately, or are performed in both directions, Ingress and Egress, at the same time. If performed separately, they can be performed in Ingress and then Egress or Egress and then Ingress directions.

[R34] When steps in a test methodology are repeated with different values of one of more parameters (e.g. some tests are repeated with different DSCP values, or for IPv4 and IPv6), the results - Pass or Fail - and the parameter values **MUST** be reported separately for each repetition.

[R35] When testing a new IPVC and its IPVC EPs, the results for each ordered pair of IPVC EPs that is tested **MUST** be reported separately.

[R36] When testing a UNI, UNI Access Link or a new IPVC EP in an existing IPVC, the results for each direction of the test **MUST** be reported separately.

[R37] The overall result of the Test Methodology **MUST** be reported as Pass or Fail.

[R38] If any repetition or direction tested fails, the result of the overall Test Methodology **MUST** be Fail.

[R39] When a new IPVC or IPVC EP is being added at a UNI that has existing IPVC EPs, the Information Rate used for tests other than BWP **MUST** be chosen to be the lowest rate sufficient for conducting the test.

This is to avoid impact to other IPVCs at the UNI.

11.3.1 UNI and UNI Access Link Service Configuration Test

The UNI and UNI Access Link Service Configuration test methodologies are included in the following sections. UNI and UNI Access Link Service Configuration tests are generally performed when the UNI and/or UNI Access Link are activated, except that the tests related to Bandwidth Profile Envelopes cannot be tested until at least one IPVC EP is enabled at the UNI if

the behavior associated with the Bandwidth Profiles is implemented in the IPCF. The test cases that can be used by each methodology are described in the following sections:

- Test Case 1 (section 9.1)
- Test Case 2 (section 9.2)
- Test Case 3 (section 9.3)
- Test Case 4 (section 9.4)
- Test Case 5 (section 9.5
- Test Case 6 (section 9.6)

11.3.1.1 UNI Ingress Bandwidth Profile Envelope

The correct configuration of the UNI Ingress Bandwidth Profile Envelope is verified with this test methodology as described in Test Case 1 (section 9.1), Test Case 4 (section 9.4), or Test Case 6 (section 9.6) if the BWP is implemented in the UNICF or Test Case 3 (section 9.3), Test Case 4 (section 9.4), Test Case 5 (section 9.5), or Test Case 6 (section 9.6) if the BWP is implemented in the IPCF.

[R40] When the UNI Ingress Bandwidth Profile Envelope is tested it **MUST** be tested as specified in Table 19 and Table 20 (in section 11.3.4) and associated requirements.

11.3.1.2 UNI Egress Bandwidth Profile Envelope

The correct configuration of the UNI Egress Bandwidth Profile Envelope is verified with this test methodology as described in Test Case 1 (section 9.1), Test Case 4 (section 9.4) , or Test Case 6 (section 9.6) if the BWP is implemented in the UNICF or Test Case 3 (section 9.3), Test Case 4 (section 9.4), Test Case 5 (section 9.5), or Test Case 6 (section 9.6) if the BWP is implemented in the IPCF.

[R41] When the UNI Egress Bandwidth Profile Envelope is tested it **MUST** be tested as specified in Table 21 and Table 22 (in section 11.3.4) and associated requirements.

11.3.1.3 UNI Access Link BFD when SP end of the BFD Session is Active

The correct operation of BFD on the UNI Access Link when the Service Provider end of the BFD session is in Active Mode is verified with this test methodology as described in Test Case 2 (section 9.2).

[R42] When the UNI Access Link BFD Service Attribute is tested and the Active End parameter is *SP* or *Both*, the UNI Access Link BFD Service Attribute **MUST** be tested as specified in Table 11.

Service Activation Test Methodology	
Test Name	UNI Access Link BFD
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	• The BFD implementations and/or IPTE is configured as shown in Test Case 2 (section 9.2). • When the SP end of the BFD session is in Active Mode and when Connection Address Family = *IPv4* or *Both*, the BFD peer located within the Service Provider network takes on the active role of a BFD session as defined in IETF RFC 5880 [7], and sends BFD Control Packets encapsulated within *IPv4* packets to the Subscriber's BFD peer located at the Subscriber end of the UNI Access Link. The Subscriber CE or $IPTE_2$ responds to the BFD Control Packets received from the SP equipment. • The SP sends BFD Control Packets for period T_{BFD} or until the BFD session state is *Up* as defined in IETF RFC 5880 [7] . • When the SP end of the BFD session is in Active Mode and when Connection Address Family = *IPv6* or *Both*, the BFD peer located within the Service Provider network takes on the active role of a BFD session as defined in IETF RFC 5880 [7], and sends BFD Control Packets encapsulated within *IPv6* packets to the Subscriber's BFD peer located at the Subscriber end of the UNI Access Link. The Subscriber CE or $IPTE_2$ responds to the BFD Control Packets received from the SP equipment. • The SP sends BFD Control Packets for period T_{BFD} or until the BFD session state is *Up* as defined in IETF RFC 5880 [7].
Variables	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 Packet Loss or Packet Loss Ratio as a measurement or calculation. 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 Subscriber BFD peer. This may require a dispatch to place an IPTE at the UNI to act as a BFD peer. 3. Testing is done for IPv4, IPv6, or Both depending on the value of Connection Address Family. 4. If the Subscriber has equipment at the UNI, this device is acting as an IPTE that only supports BFD Functionality.

Table 11 – UNI Access Link BFD Test Methodology Active End SP or Both

[R43] The SAT Record for the methodology shown in Table 11 **MUST** report the state of the BFD Session at the end of the test and the T_{BFD} used.

11.3.1.4 UNI Access Link BFD when Subscriber end of the BFD Session is Active

The correct operation of BFD on the UNI Access Link when the Subscriber end of the BFD session is in Active mode is verified with this test methodology as described in Test Case 2 (section 9.2).

[R44] When the UNI Access Link BFD Service Attribute is tested and the Active End parameter is *Subscriber* or *Both* the UNI Access Link BFD Service Attribute **MUST** be tested as specified in Table 12.

Service Activation Test Methodology	
Test Name	UNI Access Link BFD
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	• The BFD implementations and/or IPTE is configured as shown in Test Case 2 (section 9.2). • When the Subscriber end of the BFD session is in Active Mode and when Connection Address Family = *IPv4* or *Both*, the BFD peer located within the Service Provider network takes on the passive role of a BFD session as defined in IETF RFC 5880 [7], and waits for BFD Control Packets from a device (either Subscriber CE or Service Provider IPTE) at the Subscriber end of the UNI Access Link encapsulated within IPv4 packets. The SP equipment responds to BFD Control Packets received. • The SP equipment waits for BFD Control Packets for period T_{BFD}, for a pre-determined time, or until the BFD session state is UP as defined in IETF RFC 5880 [7]. • When the Subscriber end of the BFD session is in Active Mode and when Connection Address Family = *IPv6* or *Both*, the BFD peer located within the Service Provider network takes on the passive role of a BFD session as defined in IETF RFC 5880 [7], and waits for BFD Control Packets from a device (either Subscriber CE or Service Provider IPTE) at the Subscriber end of the UNI Access Link encapsulated within IPv6 packets. The SP equipment responds to BFD Control Packets received. • The SP equipment waits for BFD Control Packets for period T_{BFD}, for a pre-determined time, or until the BFD session state is UP as defined in IETF RFC 5880 [7].
Variables	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 testing is only possible if a device is connected to the UNI and is acting as a Subscriber BFD peer. This may require a dispatch to place an IPTE at the UNI to act as a BFD peer. 2. Testing is done for IPv4, IPv6, or Both depending on the value of Connection Address Family 3. If the Subscriber has equipment at the UNI this device is acting as an IPTE with limited functionality. 4. This test does not use Packet Loss 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.

Table 12 – UNI Access Link BFD Test Methodology, Active End Subscriber or Both

[R45] The SAT Record for the methodology shown in Table 12 **MUST** report the state of the BFD Session at the end of the test and the T_{BFD} used.

11.3.1.5 UNI Access Link IP MTU

The correct configuration of the UNI Access Link IP MTU is verified with this test methodology as described in Test Case 1 (section 9.1). This test verifies that IP Packets with size up to the value of the UNI Access Link MTU can be passed over the UNI Access Link. While this is not explicitly required in MEF 61.1 [15], a failure of this test can indicate a problem that could later cause the IPVC MTU test (section 11.3.2.2) to fail.

Note: MEF 61.1 [15] does not prohibit sending IP Data Packets in excess of the MTU. Packets that are greater than the MTU can be passed or discarded. For this reason, the MTU test does not require sending packets greater than the MTU. Packets in excess of the MTU can be sent if agreed to by the Service Provider and Subscriber.

[R46] When the UNI Access Link IP MTU Service Attribute value is tested it **MUST** be tested as described in Table 13.

Service Activation Test Methodology	
Test Name	UNI Access Link IP MTU
Test Objective	Verify that the UNI Access Link IP MTU attribute is configured correctly.
Test Procedure	• IPTEs are placed as shown in Test Case 1 (section 9.1). • $IPTE_1$ offers IP Test Packets with the DA for reaching $IPTE_2$ over the UNI Access Link under test with a length equal to the UNI Access Link IP MTU with a rate up to IR_{SC} and for a time T_{SC}. • $IPTE_2$ verifies that the IP Test Packets offered are received unfragmented. Packet Loss is acceptable up to *Packet Loss Ratio* $_{SAC2}$, where *Packet Loss Ratio*$_{SAC2}$ is the SAC for Packet Loss Ratio. • Simultaneously, $IPTE_2$ offers IP Test Packets with the DA for reaching $IPTE_1$ over the UNI Access Link under test with a length equal to the UNI Access Link IP MTU with a rate up to IR_{SC} and for a time T_{SC}. • $IPTE_1$ verifies that the IP Test Packets offered are received unfragmented. Packet Loss is acceptable up to *Packet Loss Ratio* $_{SAC1}$, where *Packet Loss Ratio*$_{SAC1}$ is the SAC for Packet Loss Ratio. • If both IPv4 and IPv6 are enabled the test is performed for each.
Variables	IR_{SC}, T_{SC}, *Packet Loss Ratio*$_{SAC1}$ and *Packet Loss Ratio*$_{SAC2}$
Results	Pass= IP Test Packets received unfragmented and within Packet Loss Ratio$_{SAC}$ Fail = IP Test Packets received fragmented or not within Packet Loss Ratio$_{SAC}$
Remarks	This testing is only possible if there is an IPTE at the Service Provider and Subscriber ends of where UNI Access Link Service Attributes are processed. At the Subscriber end this could be an IPTE-A in the CE or an IPTE-I connected to the UNI and might require a dispatch to the Subscriber's premises to place the IPTE-I as shown in Test Case 1 (section 9.1).

Table 13 – UNI Access Link IP MTU Test Methodology

[R47] The SAT Record for the methodology shown in Table 13 **MUST** report the IR_{SC}, T_{SC}, *Packet Loss Ratio*$_{SAC1}$, and *Packet Loss Ratio*$_{SAC2}$ used for the test.

[R48] The SAT Record for the methodology shown in Table 13 **MUST** report the *Packet Loss Ratio* results for each direction of the test and if any fragmented packets are received, for each IP version tested (*IPv4* and/or *IPv6*).

11.3.1.6 UNI Access Link Ingress Bandwidth Profile Envelope

The correct configuration of the UNI Access Link Ingress Bandwidth Profile Envelope specified in Test Case 1 (section 9.1), Test Case 4 (section 9.4), or Test Case 6 (section 9.6) is verified with this test methodology.

[R49] When the UNI Access Link Ingress Bandwidth Profile Envelope is tested it **MUST** be tested as specified in Table 19 and Table 20 (in section 11.3.4) and associated requirements.

11.3.1.7 UNI Access Link Egress Bandwidth Profile Envelope

The correct configuration of the UNI Access Link Egress Bandwidth Profile Envelope specified in Test Case 1 (section 9.1), Test Case 4 (section 9.4), or Test Case 6 (section 9.6) is verified with this test methodology.

[R50] When the UNI Access Link Egress Bandwidth Profile Envelope is tested it **MUST** be tested as specified in Table 21 and Table 22 (in section 11.3.4) and associated requirements.

11.3.2 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 tested and can also be tested when a new IPVC EP is added to the IPVC. 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. When testing IPVC Service Attributes on a new IPVC (Test Cases 3 and 4, sections 9.3 and 9.4) a list of IPVC EP pairs that are tested is agreed to by the Service Provider and Subscriber. Only these pairs are tested. When testing IPVC Service Attributes on a new IPVC EP being added to an existing IPVC (Test Cases 5 and 6, sections 9.5 and 9.6), testing is performed from the new IPVC EP to the Test End Point in the Service Provider's network.

11.3.2.1 IPVC DSCP Preservation

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

[R51] When the IPVC DSCP Preservation is tested it **MUST** be tested as described in Table 14.

Service Activation Test Methodology	
Test Name	IPVC DSCP Preservation
Test Objective	Verify that the IPVC DSCP Preservation attribute is configured correctly.
Test Procedure	• The following steps are repeated for each DSCP value in a list of DSCP values agreed between the Service Provider and the Subscriber. • IPTEs are placed as shown in Test Case 3 (section 9.3), Test Case 4 (section 9.4), Test Case 5 (section 9.5), or Test Case 6 (section 9.6). • $IPTE_1$ offers IP Test Packets with the DA of $IPTE_2$ with a rate equal to IR_{SC} for a time T_{SC} and with a DSCP value in the agreed upon list. • $IPTE_2$ counts the IP Test Packets received with the correct DSCP value and with the incorrect DSCP value. • Simultaneously, $IPTE_2$ offers IP Test Packets with the DA of $IPTE_1$ with a rate equal to IR_{SC} for a time T_{SC} and with the same DSCP value as $IPTE_1$. • $IPTE_1$ counts the IP Test Packets received with the correct DSCP value and with the incorrect DSCP value. • The above is repeated for each DSCP value that is included in the agreed upon list for the IPVC for each ordered pair within the set of ordered pairs being tested and for IPv4 and/or IPv6.
Variables	IR_{SC}, T_{SC}, list of agreed to DSCP values, ordered pairs of IPVC EPs being tested, if testing a new IPVC
Results	Pass = for each DSCP value in the list, the count of total packets received is equal to the count of packets received with the same DSCP value as offered packets. Fail = for any DSCP value in the list, the count of total packets received is not equal to the count of packets received with the same DSCP value as in offered packets.
Remarks	1. At minimum, a subset of the 64 DSCP values is tested. The SP and Subscriber can determine how large a subset is sufficient to test. 2. Figure 11, Figure 12, Figure 13, and Figure 14 show the SAMP location needed at each end of this Test Methodology to ensure that any DSCP manipulation points are included in the test. 3. The method used to communicate the DSCP value between IPTE1 and IPTE2 is beyond the scope of this document. 4. The IP Test Packet length must be less than or equal to the IP MTU specified for the service.

Table 14 – IPVC DSCP Preservation Test Methodology

[R52] The SAT Record for the methodology shown in Table 14 **MUST** report the DSCP value(s) of test packets used in this methodology.

[R53] The SAT Record for the methodology shown in Table 14 **MUST** report the IR_{SC}, T_{SC}, list of agreed to DSCP values, and ordered pairs of IPVC EPs being tested.

[R54] For each DSCP value in the agreed upon list and for each ordered pair of IPVC EPs being tested, the SAT Record for the methodology shown in Table 14 **MUST** report the count of packets received matching the DSCP value and the count of packets received not matching the DSCP value for the test.

11.3.2.2 IPVC MTU

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

Note: MEF 61.1 [15] does not prohibit sending IP Data Packets in excess of the MTU. Packets that are greater than the MTU can be passed or discarded. For this reason, the MTU test does not send packets greater than the MTU unless agreed to by the Service Provider and Subscriber.

[R55] When the IPVC MTU is tested it **MUST** be tested as described in Table 15.

Service Activation Test Methodology	
Test Name	IPVC MTU
Test Objective	Verify that the IPVC MTU attribute is configured correctly.

Test Procedure	• IPTEs are placed as shown in Test Case 3 (section 9.3), Test Case 4 (section 9.4), Test Case 5 (section 9.5), or Test Case 6 (section 9.6). • IPTE1 offers IP Test Packets with the DA of IPTE2 with a length equal to the IPVC MTU with a rate equal to IR_{SC} and for a time T_{SC}. • IPTE2 verifies that the packets offered are received unfragmented. Packet Loss is acceptable up to *Packet Loss Ratio*$_{SAC2}$, where *Packet Loss Ratio*$_{SAC2}$ is the SAC for Packet Loss Ratio. • Simultaneously, IPTE2 offers IP Test Packets with the DA of IPTE1 with a length equal to the IPVC MTU with a rate equal to IR_{SC} and for a time T_{SC}. • IPTE1 verifies that the packets offered are received unfragmented. Packet Loss is acceptable up to *Packet Loss Ratio*$_{SAC1}$, where *Packet Loss Ratio*$_{SAC1}$ is the SAC for Packet Loss Ratio. • This test is performed with IPv4 packets, IPv6 packets, or both depending on which are enabled. • The above is repeated for each ordered pair within the set of ordered pairs being tested.
Variables	IR_{SC}, *Tsc*, *Packet Loss Ratio*$_{SAC1}$, *Packet Loss Ratio*$_{SAC2}$ and Ordered pairs of IPVC EPs being tested, if testing a new IPVC
Results	Pass= IP Test Packets are received unfragmented and within *Packet Loss Ratio*$_{SAC}$ in each direction for each IP version tested (*IPv4*, *IPv6*, or *Both*). Fail = IP Test Packets are received fragmented or not within *Packet Loss Ratio*$_{SAC}$ in each direction for each IP version tested (*IPv4*, *IPv6*, or *Both*).
Remarks	The DSCP values used in IP Test Packets must be included in the values that are used for Qualified Packets.

Table 15 – IPVC MTU Test Methodology

[R56] The SAT Record for the methodology shown in Table 15 **MUST** report the agreed list of ordered pairs of IPVC EPs being tested, the IR_{SC}, T_{SC}, *Packet Loss Ratio*$_{SAC1}$ and *Packet Loss Ratio*$_{SAC2}$, used for the test.

[R57] For each ordered pair of IPVC EPs tested, the SAT Record for the methodology shown in Table 15 **MUST** report the *Packet Loss Ratio* results for each direction of the test, for each IP version tested (*IPv4* and/or *IPv6*,).

11.3.2.3 IPVC Path MTU Discovery

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

[R58] When the IPVC Path MTU Discovery attribute is tested it **MUST** be tested for new IPVCs as described in Table 16.

Service Activation Test Methodology	
Test Name	IPVC Path MTU Discovery
Test Objective	Verify that the IPVC Path MTU Discovery attribute is configured correctly.
Test Procedure	• IPTEs are placed as shown in Test Case 3 (section 9.3), Test Case 4 (section 9.4), Test Case 5 (section 9.5), or Test Case 6 (section 9.6). • $IPTE_1$ offers IP Test Packets with the DA of $IPTE_2$ starting with a length one byte greater than the IPVC MTU and increasing in length at some rate determined by the SP until the length is 10% greater than the largest UNI Access Link IP MTU for UNIs in the IPVC with the DF bit set for IPv4 packets 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 the test passes. If no messages are received and $IPTE_2$ counts no received IP Test Packets the test fails. • Simultaneously, $IPTE_2$ offers IP Test Packets with the DA of $IPTE_1$ starting with a length one byte greater than the IPVC MTU and increasing in length at some rate determined by the SP until the length is 10% greater than the largest UNI Access Link IP MTU for UNIs in the IPVC with the DF bit set for IPv4 packets 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 and $IPTE_1$ counts no received IP Test Packets the test fails. • This test is performed for IPv4 packets, IPv6 packets or both as enabled. • The above is repeated for each ordered pair within the set of ordered pairs being tested.
Variables	IR_{SC}, T_{SC}, ordered pairs of IPVC EPs being tested, if testing a new IPVC, packet lengths tested

Results	Pass = Appropriate ICMP message received from SP network during time T_{SC} for *IPv4*, *IPv6*, or *Both* as appropriate for each ordered pair. Fail = No ICMP message received from SP network and no IP Test Packets received during time T_{SC} for any IP Data Service packet size greater than IPVC MTU for *IPv4*, *IPv6*, or *Both* as appropriate for each ordered pair.
Remarks	The DSCP values used in IP Test Packets must be included in the values that are used for Qualified Packets.

Table 16 – IPVC Path MTU Discovery Test Methodology

[R59] The SAT Record for the methodology shown in Table 16 **MUST** report the length of test packets used for the test.

[R60] The SAT Record for the methodology shown in Table 16 **MUST** report the agreed list of ordered pairs of IPVC EPs being tested, the IR_{SC} and T_{SC} used for the test.

[R61] The SAT Record for the methodology shown in Table 16 **MUST** report the number of appropriate ICMP messages received, for each direction of the test, for each ordered pair of IPVC EPs tested, for each IP version tested (IPv4 and/or IPv6).

11.3.2.4 IPVC Fragmentation

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

[R62] When the IPVC Fragmentation attribute is tested it **MUST** be tested as described in Table 17.

Service Activation Test Methodology	
Test Name	IPVC Fragmentation
Test Objective	Verify that the IPVC Fragmentation Service Attribute is configured correctly.

Test Procedure	• IPTEs are placed as shown in Test Case 3 (section 9.3), Test Case 4 (section 9.4), Test Case 5 (section 9.5), or Test Case 6 (section 9.6). • $IPTE_1$ offers IPv4 Test Packets with the DA of $IPTE_2$ of a length one byte greater than the IPVC MTU and increasing in length at some rate determined by the SP until the length is 15% greater than the IPVC MTU with a rate equal to IR_{SC} for a time of T_{SC}. The DF bit is set to *Zero*. • $IPTE_2$ verifies that no fragmented IP Test Packets are received. • Simultaneously $IPTE_2$ offers IPv4 Test Packets with the DA of $IPTE_1$ of a length one byte greater than the IPVC MTU and increasing in length at some rate determined by the SP until the length is 15% greater than the IPVC MTU with a rate equal to IR_{SC} for a time of T_{SC}. The DF bit is set to *Zero*. • $IPTE_1$ verifies that no fragmented IP Test Packets are received. • The above is repeated for each ordered pair within the set of ordered pairs being tested.
Variables	IR_{SC}, T_{SC}, ordered pairs of IPVC EPs being tested, if testing a new IPVC, packet lengths tested
Results	Pass = IP Test Packets received with no fragmented packets received or no packets received during T_{SC} Fail = Any fragmented IP Test Packets received during T_{SC}
Remarks	1. The Pass condition of no fragmented packets received includes no IP Test Packets received. MEF 61.1 [15] 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. 2. This test is only used when IPVC Max IPv4 routes ≠ 0. 3. The DSCP values used in IP Test Packets must be included in the values that are used for Qualified Packets.

Table 17 – IPVC Fragmentation Test Methodology

[R63] The SAT Record for the methodology shown in Table 17 **MUST** report the length of test packets used for the test.

[R64] The SAT Record for the methodology shown in Table 17 **MUST** report the agreed list of ordered pairs of IPVC EPs being tested, the IR_{SC} and T_{SC} used for the test.

[R65] The SAT Record for the methodology shown in Table 17 **MUST** report the number of fragmented packets received for each direction of the test, for each ordered pair of IPVC EPs tested.

11.3.3 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 or when a new IPVC EP is added to an existing IPVC. See Table 8 for more detail on which test methodologies are used for new IPVCs versus when new IPVC EPs are added to existing IPVCs. A list of IPVC EP pairs to be tested is agreed to by the Service Provider and Subscriber on a new IPVC (Test Cases 3 and 4, sections 9.3 and 9.4). Only these pairs are tested. When testing IPVC Service Attributes on a new IPVC EP (Test Cases 5 and 6, sections 9.5 and 9.6) that is being added to an existing IPVC, testing is performed from the new IPVC EP to the Test End Point in the Service Provider's network.

11.3.3.1 IPVC EP Prefix Mapping

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

[R66] When the IPVC EP Prefix Mapping Service Attribute is tested it **MUST** be verified as described in Table 18.

Service Activation Test Methodology	
Test Name	IPVC EP Prefix Mapping
Test Objective	Verify that the IPVC EP Prefix Mapping Service Attribute is configured correctly.

Test Procedure	• IPTEs are placed as shown in Test Case 3 (section 9.3), Test Case 4 (section 9.4), Test Case 5 (section 9.5), or Test Case 6 (section 9.6). • This procedure tests the Prefix Mapping Service Attribute for one IPVC EP. This is represented by $IPTE_1$ located at the IPVC EP under test. $IPTE_2$ is located at another IPVC EP or the Test End Point in the Service Provider's network. • $IPTE_1$ offers IP Test Packets with the DA for $IPTE_2$ at rate IR_{SC} for time T_{SC} using a SA for $IPTE_1$ that is not on the IPVC EP Prefix Mapping list for the IPVC EP under test. • $IPTE_2$ counts IP Test Packets received from $IPTE_1$ for time T_{SC}. If any packets are received, the test fails. • $IPTE_1$ then offers IP Test Packets with the DA for $IPTE_2$ at rate IR_{SC} for time T_{SC} using a SA for $IPTE_1$ that is on the IPVC EP Prefix Mapping list for the IPVC EP under test. • $IPTE_2$ counts IP Test Packets received from $IPTE_1$ for time $T_{SC,}$ calculates Packet Loss Ratio and determines if Packet Loss Ratio ≤ $Packet\ Loss\ Ratio_{SAC2}$. • $IPTE_2$ then offers IP Test Packets at rate IR_{SC} for time T_{SC} using a DA for $IPTE_1$ that is on the IPVC EP Prefix Mapping list for the IPVC EP under test. • $IPTE_1$ counts IP Test Packets received from $IPTE_2$ for time $T_{SC,}$ calculates Packet Loss Ratio and determines if Packet Loss Ratio ≤ $Packet\ Loss\ Ratio_{SAC1}$. • $IPTE_2$ then offers IP Test Packets at rate IR_{SC} for time T_{SC} using a DA for $IPTE_1$ that is not on the IPVC EP Prefix Mapping list for the IPVC EP under test. • $IPTE_1$ counts IP Test Packets received from $IPTE_2$ for time TSC. If any packets are received, the test fails. • The above is repeated for each IPVC EP within the set of IPVC EPs being tested.

Variables	*IR$_{SC}$*, *T$_{SC}$*, *Packet Loss Ratio$_{SAC1}$*, *Packet Loss Ratio$_{SAC2}$*, List of IPVC EPs being tested, if testing a new IPVC
Results	Pass = From IPTE$_1$ to IPTE$_2$ with SA not in list for the IPVC EP under test, no packets received at IPTE$_2$, and From IPTE$_1$ to IPTE$_2$ with SA in list for the IPVC EP under test, Packet Loss Ratio ≤ *Packet Loss Ratio$_{SAC2}$*, and From IPTE$_2$ to IPTE$_1$ with DA in list for the IPVC EP under test, Packet Loss Ratio ≤ *Packet Loss Ratio$_{SAC1}$*, and From IPTE$_2$ to IPTE$_1$ with DA not in list for the IPVC EP under test no packets received at IPTE$_1$ Fail = From IPTE$_1$ to IPTE$_2$ with SA not in list for the IPVC EP under test, packets received at IPTE$_2$, or From IPTE$_1$ to IPTE$_2$ with SA in list for the IPVC EP under test Packet Loss Ratio > *Packet Loss Ratio$_{SAC2}$*, or From IPTE$_2$ to IPTE$_1$ with DA in list for the IPVC EP under test Packet Loss Ratio > *Packet Loss Ratio$_{SAC1}$*, or From IPTE$_2$ to IPTE$_1$ with DA not in list for the IPVC EP under test packets received at IPTE$_1$
Remarks	1. This Test Methodology requires that IPTE$_1$ be able to set the SA to an address in the list and to an address not in the list for the IPVC EP under test. 2. The DSCP values used in IP Test Packets must be included in the values that are used for Qualified Packets. 3. The IP Test Packet length must be less than or equal to the IPVC MTU specified for the service.

Table 18 – IPVC EP Prefix Mapping Test Methodology

[R67] The SAT Record for the methodology shown in Table 18 **MUST** report the agreed list of ordered pairs of IPVC EPs being tested, the *IR$_{SC}$*, *T$_{SC}$*, *Packet Loss Ratio$_{SAC1}$* and *Packet Loss Ratio$_{SAC2}$* used for the test.

[R68] For each ordered pair tested, the SAT Record for the methodology shown in Table 18 **MUST** report the SA and/or DA used for each step.

[R69] For each ordered pair of IPVC EPs being tested, the SAT Record for the methodology shown in Table 18 **MUST** report the number of packets received and the calculated Packet Loss Ratio for each step in the test.

11.3.4 BWP Envelope Tests

Ingress and Egress BWP Envelopes are possible at the UNI, the UNI Access Link, and the IPVC EP. If any of these is not *None*, the others must be *None*. There are two tests, aggregate bandwidth, and flow bandwidth, that are performed to verify the Ingress BWP Envelope and Egress BWP Envelope at a given point under test. The Ingress BWP Envelope and the Egress BWP Envelope

can be tested separately (as shown in Test Cases 5 and 6, sections 9.5 and 9.6) or at the same time (as shown in Test Cases 3 and 4, sections 9.3 and 9.4). In some cases, there are limitations to what BWPs can be tested depending on how the test is performed.

The aggregate bandwidth of all flows within the BWP Envelope is tested and the bandwidth of each flow within the BWP Envelope is tested. This ensures that the $MaxIR_E$ value is set correctly for the aggregate and that the $MaxIR_i$ value for each flow is set correctly. The test methodology for each of these is shown in the following sections.

Note that, depending on the service definition, it might not be possible to determine which BWP Flow an egress IP Packet was mapped to in the ingress or egress BWP. In this case, it is not possible to count the number of packets received, or calculate the Packet Loss Ratio, for each BWP Flow separately; only the total count and the aggregate Packet Loss Ratio can be determined. This limits the aspects of the BWP configuration that can be verified during SAT.

Note: The location of the IPTEs when testing Ingress BWP depends on how the BWP is implemented. See section 8 for details.

Note: If an Ingress BWP is implemented at one IPVC EP in the IPVC and an Egress BWP is implemented at another IPVC EP in the IPVC it is difficult to identify which BWP is being enforced on the IP Test Packets.

Note: It is recommended that BWP testing not be performed to an IP Loopback Function. An Ingress BWP will be enforced on the IP Test Packets at the GTF in the near-end to far-end direction. It is not possible to correctly test an Ingress BWP in the far-end to near-end direction after the near-end to far-end BWP has been enforced since *MaxIR* in the far-end to near-end direction may be set to a different value.

If the desire is to measure Packet Loss of packets of different lengths, the test methodologies below are repeated for each packet length. If an IMIX pattern is used, the Packet Loss reported reflects the total packet count and not counts of each packet length.

11.3.4.1 Ingress BWP Envelope Aggregate Methodology

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

[R70] When the aggregate of all flows within each Ingress BWP Envelope attribute is tested it **MUST** be tested as described in Table 19.

Service Activation Test Methodology	
Test Name	Ingress BWP Envelope aggregate
Test Objective	Verify that the Ingress BWP Envelope aggregate attribute is configured correctly.

Test Procedure	• IPTEs are placed as shown in Test Case 1 (section 9.1), Test Case 3 (section 9.3), Test Case 4 (section 9.4), Test Case 5 (section 9.5), or Test Case 6 (section 9.6). • $IPTE_1$ offers IP Test Packets on one or more flows with the DA of $IPTE_2$ and a rate equal to $MaxIR_E$ for a time T_{SC}. • $IPTE_2$ counts the number of IP Test Packets received. • The Packet Loss is measured, and the *Packet Loss Ratio* is calculated. Packet loss is acceptable up to *Packet Loss Ratio*$_{SAC}$. • The above is repeated for each ordered pair within the set of ordered pairs being tested.
Variables	T_{SC}, *Packet Loss Ratio*$_{SAC}$, ordered pairs of IPVC EPs being tested, if testing a new IPVC
Results	Pass = Packet loss is ≤ *Packet Loss Ratio*$_{SAC}$ Fail = Packet loss is > *Packet Loss Ratio*$_{SAC}$
Remarks	1. The Ingress BWP Envelope test involves the total aggregate information rate of traffic across all BWP Flows in the BWP Envelope. If there are one or more flows that have a *MaxIR* equal to $MaxIR_E$, one such flow is tested. If no single flow has a *MaxIR* that is equal to $MaxIR_E$, two or more flows are tested simultaneously such that the IR used for each flow is less than or equal to *MaxIR* for that flow, and the sum of IRs used for the flows equals $MaxIR_E$. 2. If the $MaxIR_E$ of the Egress BWP Envelope is less than the $MaxIR_E$ of the Ingress BWP Envelope this test does not apply. This test is either skipped or this case can be avoided by testing to a point within the SP's network verifying the I-BWP and E-BWP independently 3. The DSCP values used in IP Test Packets must be included in the values that are used for Qualified Packets. 4. The IP Test Packet length must be less than or equal to the IPVC MTU specified for the service.

Table 19 – Ingress BWP Envelope Aggregate Test Methodology

[R71] For each ordered pair of IPVC EPs tested, the SAT Record for the methodology shown in Table 19 **MUST** report the Flow Definition (as defined in MEF 61.1 [15]) and *IR* for each BWP Flow used in this methodology.

[R72] The SAT Record for the methodology shown in Table 19 **MUST** report the length of test packets used for the test.

[R73] The SAT Record for the methodology shown in Table 19 **MUST** report the agreed list of ordered pairs of IPVC EPs being tested, the T_{SC}, and *Packet Loss Ratio*$_{SAC}$ used for the test.

[R74] For each ordered pair of IPVC EPs tested, the SAT Record for the methodology shown in Table 19 **MUST** report the Packet Loss Ratio.

11.3.4.2 Ingress BWP Envelope per Flow

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

[R75] When each flow within the Ingress BWP Envelope is tested, they **MUST** be tested as described in Table 20.

Service Activation Test Methodology	
Test Name	Ingress BWP Envelope per Flow
Test Objective	Verify that the Ingress BWP Envelope attribute is configured correctly for each flow within the BWP Envelope.
Test Procedure	• IPTEs are placed as shown in Test Case 1 (section 9.1), Test Case 3 (section 9.3), Test Case 4 (section 9.4), Test Case 5 (section 9.5), or Test Case 6 (section 9.6). • $IPTE_1$ offers IP Test Packets with the DA of $IPTE_2$ that are mapped to the BWP Flow under test, at a rate equal to *MaxIR* for the flow for a time T_{SC} in accordance with the service description. • $IPTE_2$ counts the number of IP Test Packets received. • The Packet Loss is measured, and the *Packet Loss Ratio* is calculated. Packet loss is acceptable up to *Packet Loss Ratio*$_{SAC}$. • This is repeated for flows 1..n in the BWP Envelope. • The above is repeated for each ordered pair within the set of ordered pairs being tested.
Variables	T_{SC}, *Packet Loss Ratio*$_{SAC}$ and Ordered pairs of IPVC EPs being tested, if testing a new IPVC
Results	Pass = Packet loss is within *Packet Loss Ratio*$_{SAC}$ Fail = Packet loss is not within *Packet Loss Ratio*$_{SAC}$
Remarks	1. A failure of any flow in the BWP Envelope represents a failure of all flows in the BWP Envelope. 2. The DSCP values used in IP Test Packets must be included in the values that are used for Qualified Packets. 3. The IP Test Packet length must be less than or equal to the IP MTU specified for the service.

Table 20 – Ingress BWP Envelope per Flow Test Methodology

[R76] The SAT Record for the methodology shown in Table 20 **MUST** report the length of test packets used for the test.

[R77] The SAT Record for the methodology shown in Table 20 **MUST** report the agreed list of ordered pairs of IPVC EPs being tested, the T_{SC} and *Packet Loss Ratio*$_{SAC}$ used for the test.

[R78] For each ordered pair of IPVC EPs being tested, and for each BWP Flow in the BWP Envelope, the SAT Record for the methodology shown in Table 20 **MUST** report the Packet Loss Ratio

11.3.4.3 Egress BWP Envelope Aggregate Methodology

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

[R79] When the aggregate of all flows within each Egress BWP Envelope attribute is tested it **MUST** be tested as described in Table 21.

Service Activation Test Methodology	
Test Name	Egress BWP Envelope aggregate
Test Objective	Verify that the Egress BWP Envelope aggregate attribute is configured correctly.
Test Procedure	• IPTEs are placed as shown in Test Case 1 (section 9.1), Test Case 3 (section 9.3), Test Case 4 (section 9.4), Test Case 5 (section 9.5), or Test Case 6 (section 9.6). • IPTE$_2$ offers IP Test Packets with the DA of IPTE$_1$, at a rate equal to $MaxIR_E$ for the flow for a time of T_{SC}. • IPTE$_1$ counts the number of IP Test Packets received. • The Packet Loss is measured, and the *Packet Loss Ratio* is calculated. Packet loss is acceptable up to *Packet Loss Ratio*$_{SAC}$. • The above is repeated for each ordered pair within the set of ordered pairs being tested.
Variables	T_{SC}, *Packet Loss Ratio* $_{SAC}$, ordered pairs of IPVC EPs being tested, if testing a new IPVC
Results	Pass = Packet loss is ≤ *Packet Loss Ratio*$_{SAC}$ Fail = Packet loss is > *Packet Loss Ratio*$_{SAC}$

Remarks	1. The Egress BWP Envelope test involves the total aggregate information rate of traffic across all BWP Flows in the BWP Envelope. If there are one or more flows that have a *MaxIR* equal to $MaxIR_E$, one such flow is tested. If no single flow has a *MaxIR* that is equal to $MaxIR_E$, two or more flows are tested simultaneously such that the IR used for each flow is less than or equal to *MaxIR* for that flow, and the sum of IRs used for the flows equals $MaxIR_E$. 2. If the $MaxIR_E$ of the Ingress BWP Envelope is less than the $MaxIR_E$ of the Egress BWP Envelope this test does not apply. This test is either skipped or this case can be avoided by testing to a point within the SP's network verifying the I-BWP and E-BWP independently 3. The DSCP values used in IP Test Packets must be included in the values that are used for Qualified Packets. 4. The IP Test Packet length must be less than or equal to the IP MTU specified for the service.

Table 21 – Egress BWP Envelope Aggregate Test Methodology

[R80] For each ordered pair of IPVC EPs tested, the SAT Record for the methodology shown in Table 21 **MUST** report the Flow Definition (as defined in MEF 61.1 [15]) and *IR* for each BWP Flow used in this methodology.

[R81] The SAT Record for the methodology shown in Table 21 **MUST** report the length of test packets used for the test.

[R82] The SAT Record for the methodology shown in Table 21 **MUST** report the agreed list of ordered pairs of IPVC EPs being tested, the T_{SC} and *Packet Loss Ratio* $_{SAC}$ used for the test.

[R83] For each ordered pair of IPVC EPs tested, the SAT Record for the methodology shown in Table 21 **MUST** report the Packet Loss Ratio.

11.3.4.4 Egress BWP Envelope per Flow

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

[R84] When each flow within an Egress BWP Envelope is tested, they **MUST** be tested as described in Table 22.

Service Activation Test Methodology	
Test Name	Egress BWP Envelope per Flow
Test Objective	Verify that the Egress BWP Envelope attribute is configured correctly for each flow within the BWP Envelope.

Test Procedure	• IPTEs are placed as shown in Test Case 1 (section 9.1), Test Case 3 (section 9.3), Test Case 4 (section 9.4), Test Case 5 (section 9.5), or Test Case 6 (section 9.6). • $IPTE_2$ offers IP Test Packets with the DA of $IPTE_1$ that are mapped to the BWP Flow under test at a rate equal to *MaxIR* for the flow for a time equal to T_{SC}. • $IPTE_1$ counts the number of IP Test Packets received. • The Packet Loss is measured, and the *Packet Loss Ratio* is calculated. Packet loss is acceptable up to *Packet Loss Ratio*$_{SAC}$. This is repeated for flows 1..n in the BWP Envelope. • The above is repeated for each ordered pair within the set of ordered pairs being tested.
Variables	T_{SC}, *Packet Loss Ratio*$_{SAC}$, ordered pairs of IPVC EPs being tested, if testing a new IPVC
Results	Pass = Packet loss is ≤ *Packet Loss Ratio*$_{SAC}$ Fail = Packet loss is > *Packet Loss Ratio*$_{SAC}$
Remarks	1. A failure of any flow in the BWP Envelope represents a failure of all flows in the BWP Envelope. 2. The DSCP values used in IP Test Packets must be included in the values that are used for Qualified Packets. 3. The IP Test Packet length must be less than or equal to the IP MTU specified for the service.

Table 22 – Egress BWP Envelope per Flow Test Methodology

[R85] The SAT Record for the methodology shown in Table 22 **MUST** report the length of test packets used for the test.

[R86] The SAT Record for the methodology shown in Table 22 **MUST** report the agreed list of ordered pairs of IPVC EPs being tested, the T_{SC} and *Packet Loss Ratio*$_{SAC}$ used for the test.

[R87] For each ordered pair of IPVCs being tested and for each BWP Flow in the BWP Envelope, the SAT Record for the methodology shown in Table 22 **MUST** report the measured Packet Loss Ratio.

11.4 Service Performance Tests

Service performance tests are used to ensure that the service meets performance expectations of the Subscriber. Service performance tests measure Packet Loss and Packet Delay. Performance metrics including Packet Delay Percentile, Mean Packet Delay, Inter-Packet Delay Variation, Packet Delay Range, and Packet Loss Ratio are calculated from these measurements. 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 as specified in 11.1.3.

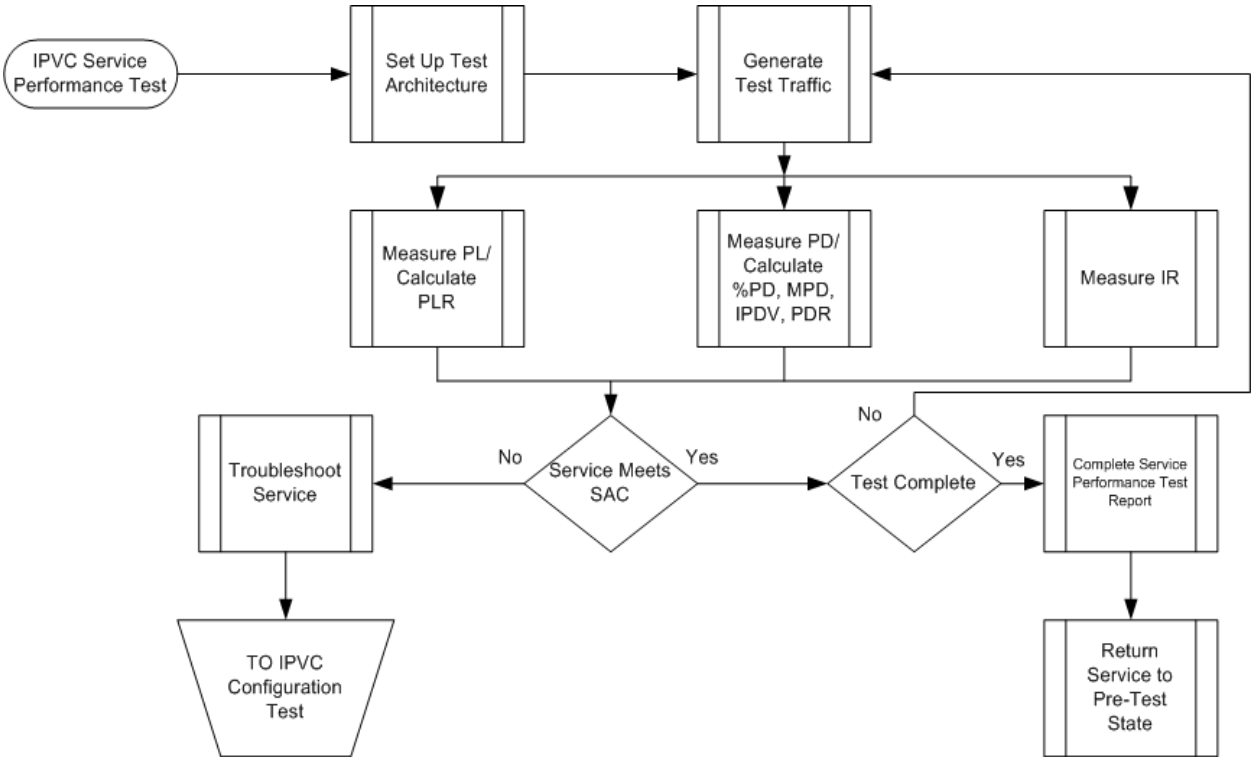

Figure 22 – Service Performance Flow

11.4.1 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.

[R88] An implementation of an IPTE **MUST** be capable of the following durations for performance tests: 15 minutes, 2 hours, 24 hours.

[R89] The Service Performance test duration **MUST** be agreed to by the Service Provider and Subscriber.

11.4.2 Service Performance 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. For new IPVCs this testing is performed between each IPVC EP pair in the list of IPVC EPs agreed to by the Service Provider and the Subscriber. For a new IPVC EP being added to an existing IPVC, the test is performed between the UNI with the new IPVC EP and the Test End Point within the Service Provider's network. When testing new IPVCs or

new IPVC EPs that are being installed on UNIs that have existing IPVC EP(s), the Service Provider must be aware that testing performance at or even near *MaxIR* for the new services can impact the existing services on the UNI. Test traffic generated for the new IPVC or IPVC EP may cause congestion and impact the Subscriber traffic at the UNI. For this reason, it is recommended that the Service Provider coordinate any performance testing on new services at UNIs with existing services with the Subscriber. The test methodology in Table 23 is used to perform loss and delay measurements between each set of UNIs.

[R90] When the loss and delay performance of each ordered pair of IPVC EPs in a list agreed to by the Service Provider and Subscriber in a new IPVC is tested, they **MUST** be tested as specified in Table 23.

[R91] When the loss and delay performance of a new IPVC EP being added to an existing IPVC is tested, they **MUST** be tested as specified in Table 23.

[D6] The Service Provider **SHOULD** coordinate any performance testing of new IPVCs or IPVC EPs on UNIs with existing services with the Subscriber.

Service Activation Test Methodology	
Test Name	Service Performance Loss and Delay
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 11.1.1. • IPTEs are placed as shown in Test Case 3 (section 9.3), Test Case 4 (section 9.4), Test Case 5 (section 9.5), or Test Case 6 (section 9.6). • $IPTE_1$ offers IP Test Packets with the DA of $IPTE_2$ at a constant rate less than the lowest *MaxIR* of the Ingress and Egress BWP Envelopes for the IPVC EP pair being tested for each Bandwidth Profile Flow that the CoS Name under test and IPVC EP are mapped to for time T_{SP}. If the CoS Name under test and IPVC EP are not mapped to a Bandwidth Profile, IP Test Packets are offered at a constant rate equal to the sum of the bandwidth of all UNI Access Links at the UNI. • $IPTE_1$ counts the IP Test Packets transmitted. • $IPTE_2$ counts the IP Test Packets received. • The received *Packet Loss*, and *Packet Delay* are measured and the *Packet Delay Percentile*, *Mean Packet Delay*, *Inter-Packet Delay Variation* and/or *Packet Delay Range* from *Packet Delay* and *Packet Loss Ratio* are calculated. • Simultaneously, $IPTE_2$ offers IP Test Packets with the DA of $IPTE_1$ at a constant rate less than the lowest *MaxIR* of the Ingress and Egress BWP Envelopes for the IPVC EP pair being tested for each Bandwidth Profile Flow that the CoS Name under test and IPVC EP are mapped to for time T_{SP}. If the CoS Name under test and IPVC EP are not mapped to a Bandwidth Profile, IP Test Packets are offered at a constant rate equal to the sum of the bandwidth of all UNI Access Links at the UNI. • $IPTE_2$ counts the IP Test Packets transmitted. • $IPTE_1$ counts the IP Test Packets received. • The received *Packet Loss*, and *Packet Delay* are measured and the *Packet Delay Percentile*, *Mean Packet Delay*, *Inter-Packet Delay Variation* and/or *Packet Delay Range* from *Packet Delay* and *Packet Loss Ratio* are calculated. • This process is repeated for each *CoS Name* in the *IPVC List of CoS Names* Service Attribute in the IPVC. • If the *Packet Loss Ratio*, *Packet Delay Percentile* and/or *Mean Packet Delay*, and *Inter-Packet Delay Variation* and/or *Packet Delay Range* are within the limits of SAC for CoS Name at $IPTE_1$ and $IPTE_2$ the result is Pass. • The above is repeated for each ordered pair within the set of ordered pairs being tested.

Variables	• T_{SP} • Percentile for Packet Delay Percentile • Percentile for Inter-Packet Delay Variation • Percentile for Packet Delay Range • Inter-Packet Delay Variation Separation Time • Ordered pairs of IPVC EPs being tested, if testing a new IPVC For each CoS Name and ordered pair of IPVC EPs • Packet Delay$_{SACCoSi}$ • Mean Packet Delay$_{SACCoSi}$ • Inter-Packet Delay Variation$_{SACCoSi}$ • Packet Delay Range$_{SACCoSi}$ • Packet Loss Ratio$_{SACCoSi}$ The variables might be different for each pair of IPVC EPs tested for a new IPVC.
Results	Pass = the SAC are met for every CoS Name, for every pair of IPVC EPs that is tested. Fail = there is at least one CoS Name and pair of IPVC EPs for which the SAC are not met.

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. 2. The SAC values are set for each CoS Name and each IPVC EP pair tested. Values between different IPVC EP pairs can be different. 3. If the BWP flow under test is not specific to a UNI Access Link and testing is being performed from the Subscriber side of the UNI, the BWP flow is tested over each UNI Access Link separately. This does not apply to testing performed from the Service Provider side of the UNI. 4. The percentiles and Inter-Packet Delay Variation Separation Time used for Packet Delay, Packet Delay Range, and Inter-Packet Delay Variation are agreed to by the Service Provider and Subscriber. The percentiles are determined by identifying the number of packets that must meet the SAC. As an example, the Packet Delay Percentile could be set to the 99th percentile meaning that almost all Packet Delay measurements must fall within the SAC or it could be set to the 50th percentile meaning that half the Packet Delay measurements must fall within the SAC. 5. The IP Test Packet length must be less than or equal to the IP MTU specified for the service.

Table 23 – Service Performance Loss and Delay Test Methodology

[R92] The SAT Record for the methodology shown in Table 23 **MUST** report the length of test packets used for the test.

If the desire is to test multiple length packets, the test methodology is repeated for each packet length. When the test methodology uses an IMIX pattern, the lengths are reported but Packet Loss is measured for all packets in the IMIX not for individual length packets.

[R93] The SAT Record for the methodology shown in Table 23 **MUST** report the T_{SP}, *Percentile for Packet Delay Percentile*, *Percentile for Inter-Packet Delay Variation*, *Percentile for Packet Delay Range*, and *Inter-Packet Delay Variation Separation Time*, used for the test.

[R94] For each ordered pair of IPVC EPs tested and for each CoS Name tested, the SAT Record for the methodology shown in Table 23 **MUST** report the *Packet Delay*$_{SACCoSi}$, *Mean Packet Delay*$_{SACCoSi}$, *Inter-Packet Delay Variation*$_{SACCoSi}$, *Packet Delay Range*$_{SACCoSi}$, and *Packet Loss Ratio*$_{SACCoSi}$ used for the test.

[R95] The SAT Record for the methodology shown in Table 23 **MUST** report the Packet Loss, Packet Delay Percentile, Mean Packet Delay, Inter-Packet Delay Variation, Packet Delay Range for each CoS Name, for each direction, and for each IPVC EP pair tested.

12 Test Report

After all tests have been completed a SAT Record is created. The SAT Record contains the attribute and test result information described in sections 10 and 11. 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.

13 References

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

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

[3] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, March 1997

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

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

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

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

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

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

[10] IETF RFC 8174, *Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words*, May 2017

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

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

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

[14] MEF 48.1, *Ethernet Service Activation Testing*, February 2020

[15] MEF 61.1, *IP Service Attributes*, May 2019

Appendix A 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. IR is defined as the number of bits transmitted in one second.

The IR of L1, L2, and L3 differs due to the number of bytes of overhead for each technology. As an example, an Ethernet MAC Frame has 20 bytes of overhead (12 Inter-Frame Gap and 8 bytes of Preamble and Start of Frame Delimiter), an Ethernet Frame has at least 18 bytes of overhead (14 bytes of Ethernet Header and 4 bytes of FCS), and an IPv4 Packet has 20 bytes of IP Header that is included in the IP packet length shown below. The IR must be higher at lower Layers to consider the additional overhead.

As an example, the IR at L3 for a given service is 50Mb/s. This is constant regardless of the packet length of the payload. The packet length of the payload is variable. A longer packet length results in fewer packets per second being transmitted. A constant payload of 1500 byte packets results in approximately 4100 packets per second being transmitted. A constant payload of 494-byte packets results in approximately 12650 packets per second. For a constant payload of 46-byte packets, the packet per second rate increases to approximately 140000 packets per second. It should be noted that all packet lengths include overhead.

The L1 and L2 IRs required to support an L3 IR of 50Mb/s are impacted by the number of packets transmitted per second at L3. The chart below shows an example of the required L2 and L1 IRs to meet the number of packets transmitted per second at L3.

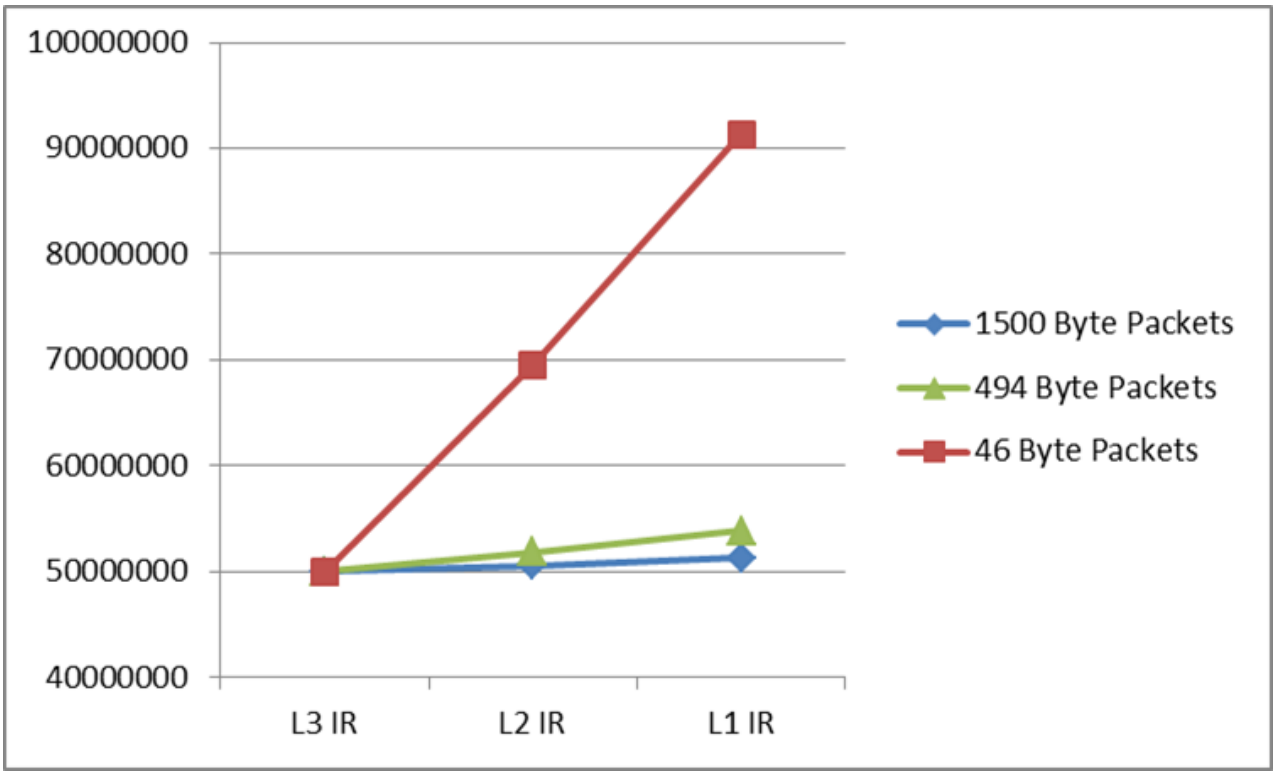

Figure 23 – IR and Packet Length Comparison

As seen in Figure 23, the L2 and L1 IR required can vary greatly depending on the number of packets transmitted per second at L3. This example is a worst-case view with a single packet length. If the lengths of packets are varied it is likely a less extreme IR at L2 and L1 will be seen.

When testing an IPVC the difference between the IR required at each layer should be considered. Failures of measurements at L3 can result from the L2 or L1 IR being configured too low.