



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

MEF Draft Standard
MEF 67 Draft (R1)

Service Activation Testing for IP Services
Technical Specification

February 2019

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

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

21 Disclaimer

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

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

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

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

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

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

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

48 © MEF Forum 2019. All Rights Reserved.

49

Table of Contents

50		
51	1	List of Contributing Members..... 1
52	2	Abstract..... 1
53	3	Release Notes 1
54	4	Terminology and Abbreviations..... 2
55	5	Compliance Levels 5
56	6	Numerical Prefix Conventions..... 5
57	7	Introduction..... 6
58	7.1	Terminology and SAT Use Cases 7
59	7.2	Service Activation Testing Use Cases..... 10
60	8	SAMP and THCP Locations 23
61	8.1	Service Activation Measurement Point Locations 23
62	9	Service Attributes..... 28
63	9.1	Configuration Testing..... 28
64	9.1.1	Subscriber UNI Service Attributes..... 28
65	9.1.2	Subscriber UNI Access Link..... 30
66	9.1.3	Subscriber IPVC Service Attributes..... 33
67	9.1.4	Subscriber IPVC End Point..... 35
68	9.2	Performance Testing..... 37
69	10	Service Activation Testing Methodologies..... 39
70	10.1	Common Methodology Requirements..... 40
71	10.1.1	Test Packet Format and Length..... 40
72	10.1.2	Common IP Test Equipment Requirements 41
73	10.1.3	Test Measurements..... 42
74	10.2	Service Acceptance Criteria 44
75	10.3	Service Configuration Tests 44
76	10.3.1	UNI Access Link Service Configuration Test..... 46
77	10.3.2	IPVC Configuration Tests..... 52
78	10.3.3	IPVC EP Configuration Tests 57
79	10.4	Service Performance Tests 66
80	10.4.1	Service Performance Test Duration 67
81	10.4.2	Service Performance Service Loss and Delay..... 67
82	11	Results 70
83	11.1	Monitoring Test 70
84	11.1.1	Test Report 70
85	12	References 71
86	Appendix A	Test Report Content Example 73
87	Appendix B	Information Rate Comparison..... 79
88		

List of Figures

89		
90	Figure 1 IPVC and UNI	9
91	Figure 2 IPVC with IPTEs	10
92	Figure 3 Use Case 1: New IPVC Activation using IPTE-Is with Subscriber Managed CE	12
93	Figure 4 Use Case 2: New IPVC Activation IPTE-A to IPTE-A Testing from the Service	
94	Provider Side of the UNI, IPVC and IPVC EP Service Attributes	13
95	Figure 5 Use Case 3: New IPVC Activation using IPTE-A and IPTE-TH to Verify IPVC and	
96	IPVC EP Service Attributes	14
97	Figure 6 Use Case 4: New UNI adding New IPVC EP to Existing IPVC Testing from Subscriber	
98	Side of UNI using IPTE-I	15
99	Figure 7 Use Case 5: New IPVC EP Activation of an IPVC Testing from the Service Provider	
100	Side of the UNI Using IPTE-A	16
101	Figure 8 Use Case 6: New IPVC EP Activation using IPTE-TH to IPTE-TH to Verify IPVC and	
102	IPVC EP Service Attributes	17
103	Figure 9 Use Case 7: New UNI Adding a New IPVC EP to Existing IPVC using IPTE-I Testing	
104	UNI and UNI Access Link Service Attributes	18
105	Figure 10 Use Case 8: New IPVC EP Activation IPTE-A to IPTE-I Testing Across UNI to	
106	Verify UNI and UNI Access Link Service Attributes	19
107	Figure 11 Use Case 9: New IPVC Activation IPTE-A to IPTE-I Testing Across UNI to Test UNI	
108	and UNI Access Link Service Attributes	20
109	Figure 12 Use Case 10: New IPVC Activation using IPTE-I and IPTE-TH to Verify UNI and	
110	UNI Access Link Service Attributes	21
111	Figure 13 Use Case 11: New IPVC EP Activation using IPTE-I and IPTE-TH to Verify UNI and	
112	UNI Access Link Service Attributes	22
113	Figure 14 THCP Location to Verify IPVC and IPVC EP Service Attributes	23
114	Figure 15 THCP Location to Verify UNI and UNI Access Link Service Attributes	24
115	Figure 16 Up SAMP Location in IPTE-A to Verify IPVC and IPVC EP Service Attributes	25
116	Figure 17 SAMP Location in IPTE-A to Verify UNI and UNI Access Link Service Attributes	26
117	Figure 18 SAMP Location in IPTE-I to Verify IPVC, IPVC EP, UNI, and UNI Access Link	
118	Service Attributes	27
119	Figure 19 Service Activation Test Process	39
120	Figure 20 Responder Processing Packet	42
121	Figure 21 Responder Looping Back Packet	43
122	Figure 22 UNI Access Link Service Configuration Tests	45
123	Figure 23 IPVC Service Configuration Tests	46
124	Figure 24 IPVC EP Service Configuration Tests	46
125	Figure 25 Service Performance Flow	67
126		

127

List of Tables

128	Table 1 – Terminology and Abbreviations	4
129	Table 2 – Numerical Prefix Conventions.....	5
130	Table 3 Use Case Overview.....	11
131	Table 4 Per UNI Configuration Service Attributes.....	30
132	Table 5 Per UNI Access Link Configuration Service Attributes.....	33
133	Table 6 Per IPVC Configuration Service Attributes.....	35
134	Table 7 Per IPVC EP Configuration Service Attributes.....	37
135	Table 8 Performance Attributes	38
136	Table 9 IMIX Values	40
137	Table 10 UNI Access Link BFD Test Methodology	48
138	Table 11 UNI Access Link BFD Test Methodology	50
139	Table 12 UNI Access Link IP MTU Test Methodology.....	51
140	Table 13 IPVC DSCP Preservation Test Methodology.....	53
141	Table 14 IPVC MTU Test Methodology.....	54
142	Table 15 IPVC Path MTU Discovery Test Methodology	56
143	Table 16 IPVC Fragmentation Test Methodology.....	57
144	Table 17 IPVC EP Profile Mapping Test Methodology.....	59
145	Table 18 IPVC Ingress BWP Envelope Aggregate Test Methodology.....	60
146	Table 19 IPVC Ingress BWP Envelope per Flow Test Methodology	61
147	Table 20 IPVC Ingress BWP Envelope for all Flows within the Envelope Test Methodology...	62
148	Table 21 IPVC Egress BWP Envelope Aggregate Test Methodology.....	64
149	Table 22 IPVC Egress BWP Envelope per Flow Test Methodology	65
150	Table 23 IPVC Egress BWP Envelope for all Flows within the Envelope Test Methodology....	66
151	Table 24 Service Performance Loss and Delay Test Methodology.....	69
152	Table 25 Test Report Contents	78

153

154 **1 List of Contributing Members**

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

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

- 161 • ABC Networks
- 162 • XYZ Communications

163 **2 Abstract**

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

175 **3 Release Notes**

176 Appendix B, a comparison of Layer 1 to Layer 2 to Layer 3 throughput will be provided in a lat-
177 ter release of this document.

178 **4 Terminology and Abbreviations**

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

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

184

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

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

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

Table 1 – Terminology and Abbreviations

185

186

187 **5 Compliance Levels**

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

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

197 A paragraph preceded by [CRa]< specifies a conditional mandatory requirement that **MUST** be
 198 followed if the condition(s) following the "<" have been met. For example, "[CR1]<[D38]" in-
 199 dicates that Conditional Mandatory Requirement 1 must be followed if Desirable Requirement
 200 38 has been met. A paragraph preceded by [CDb]< specifies a Conditional Desirable Require-
 201 ment that **SHOULD** be followed if the condition(s) following the "<" have been met. A para-
 202 graph preceded by [COc]< specifies a Conditional Optional Requirement that **MAY** be followed
 203 if the condition(s) following the "<" have been met.

204 **6 Numerical Prefix Conventions**

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

206 This document uses the prefix notation to indicate multiplier values as shown in Table 2.
 207

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

208 **Table 2 – Numerical Prefix Conventions**
 209

210 7 Introduction

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

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

218 Performance testing verifies that the Service Acceptance Criteria (SAC) are met. See section
219 10.2 for the description of SAC and how they differ from a Service Level Specification (SLS).
220 The measurements that are performed include Packet Delay (PD) and Packet Loss (PL). Addi-
221 tional metrics that are calculated based on these measurements are Mean Packet Delay (MPD),
222 Inter-Packet Delay Variation (IPDV), Packet Delay Range (PDR), and Packet Loss Ratio (PLR).

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

226 Before IP Services are turned over to Subscribers, Service Providers perform some type of SAT.
227 This can range from ICMP pings to a Subscriber router to extensive connectivity and throughput
228 testing. While IP Services are widely implemented, standard methods of performing SAT have
229 not been clearly defined. This document builds upon the IP Service Attributes defined in MEF
230 61 [24] to provide methodologies for verifying the Service Attributes defined by that document.
231 If these Service Attributes are verified, a smaller number of failures after installation is expected,
232 resulting in fewer complaints from Subscribers.

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

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

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

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

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

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

261 The remainder of the document contains the following:

- 262 • A discussion of SAT Use Cases
- 263 • A discussion of SAT Terminology
- 264 • A description of SAMPs and THCPs
- 265 • A description of where SAMPs and THCPs are located
- 266 • Tables that define what IP Service Attributes are tested
- 267 • Tables that define what IP Service Attributes are reported
- 268 • SAT Methodologies for Configuration and Performance tests
- 269 • Test Result reporting
- 270 • Requirements are specified for devices and applications including SAMPs, THCPs, and
271 IPTEs

272 7.1 Terminology and SAT Use Cases

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

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

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

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

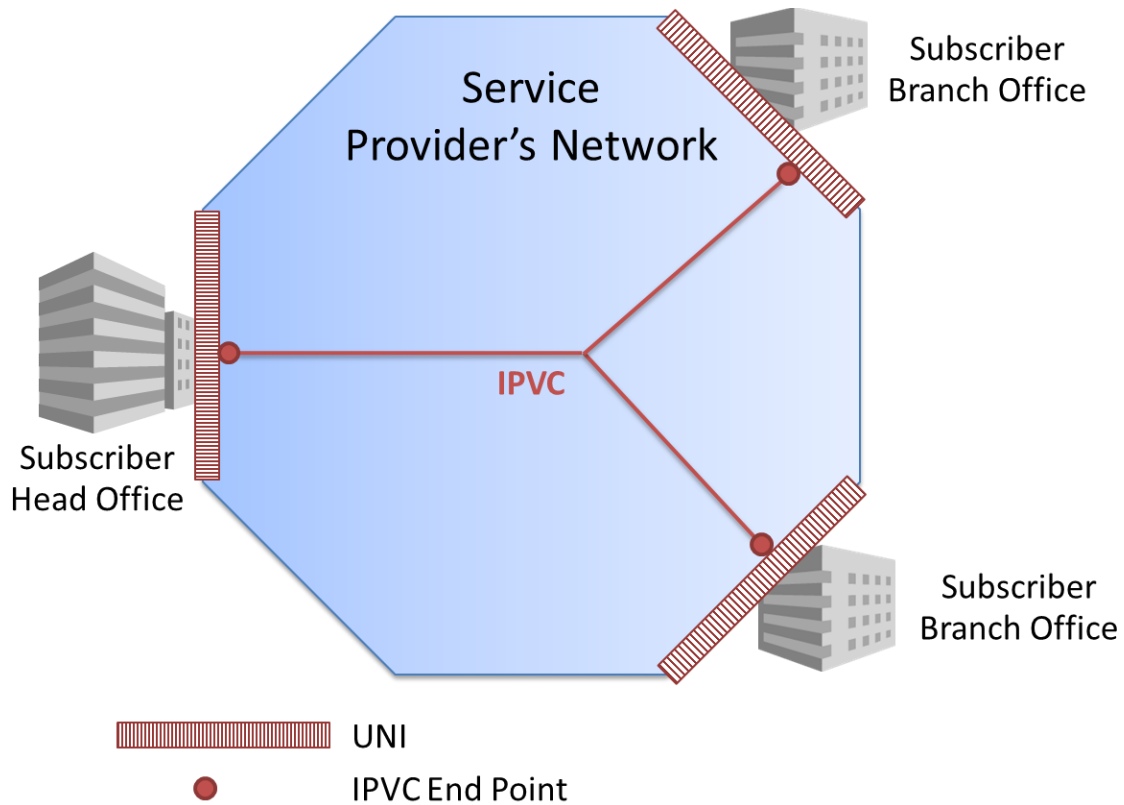
296 A SAT Methodology is defined to verify the configuration of specific Service Attributes. Each of
297 these Service Attributes has its own SAT Methodology. Additional SAT Methodology(s) are
298 used to verify the performance of the service. Each SAT Methodology identifies the test name,
299 test type,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

302

303

304

305



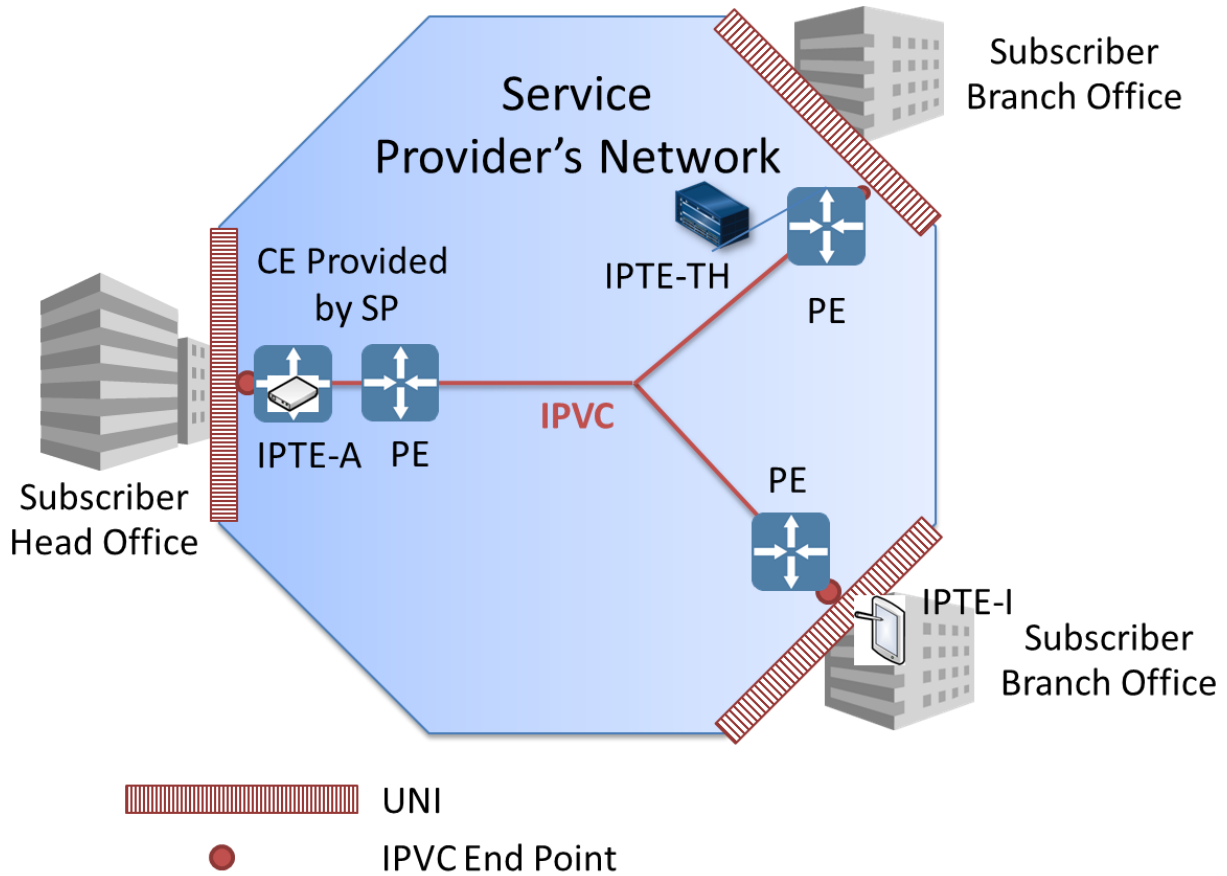
306

307

Figure 1 IPVC and UNI

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

311



312

313

Figure 2 IPVC with IPTEs

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

320

321 **7.2 Service Activation Testing Use Cases**

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

326

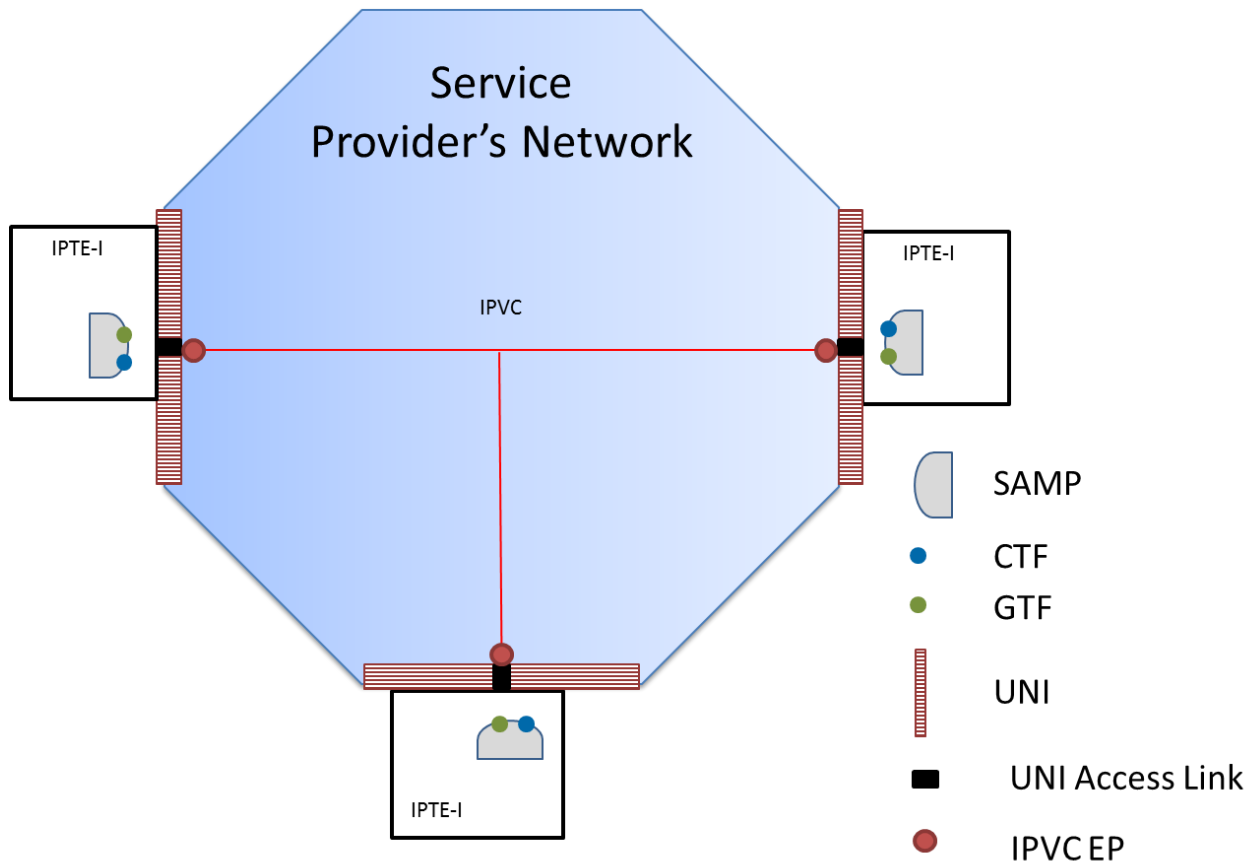
327

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

328

Table 3 Use Case Overview

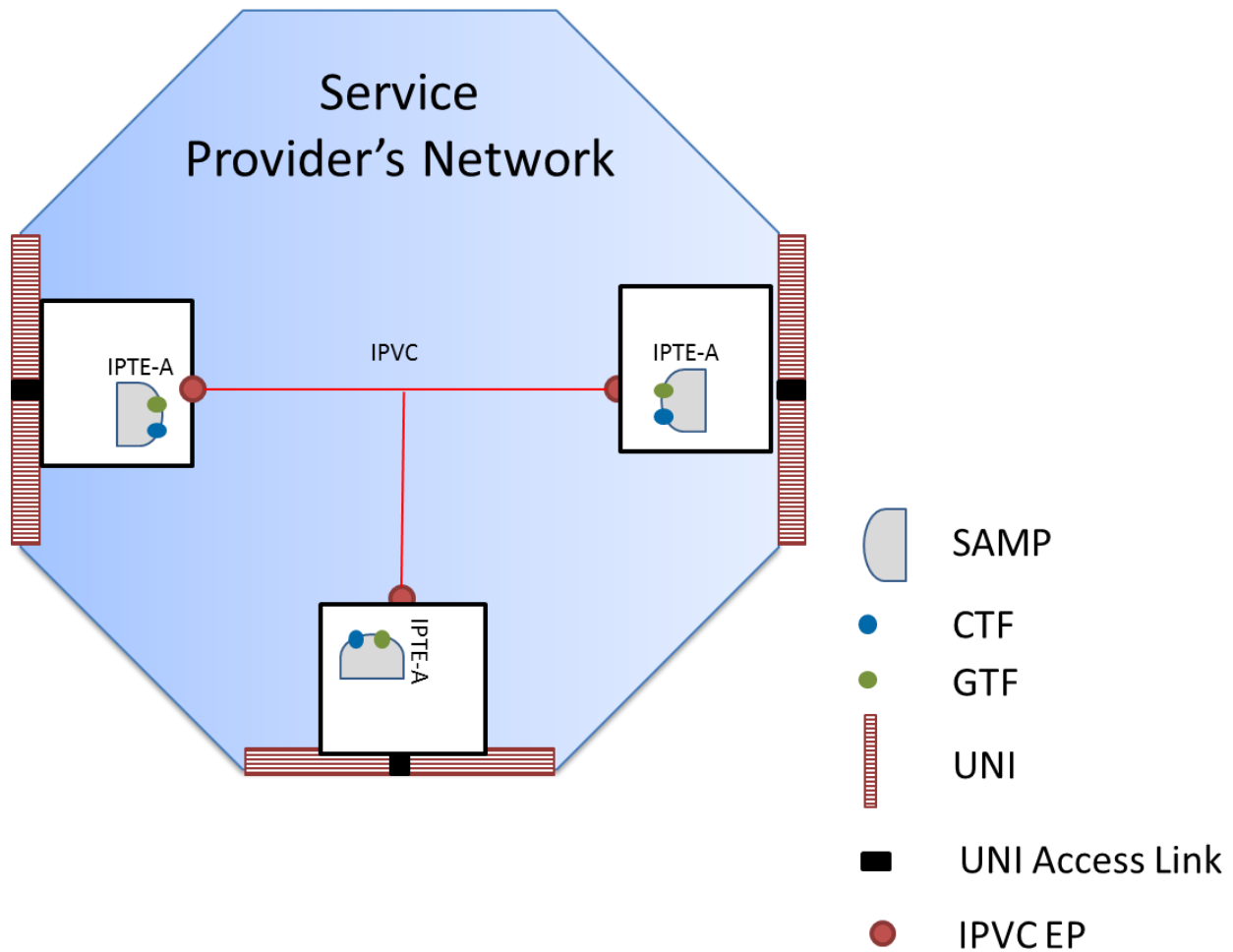
329 SAT use cases are shown below. These figures and associated text describe the use cases, the
 330 type of IPTE used, the type of SAMP and/or THCP used, the type of service tested, and the ser-
 331 vice attributes tested. These use cases are also referenced in the testing methodologies section.



332

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

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



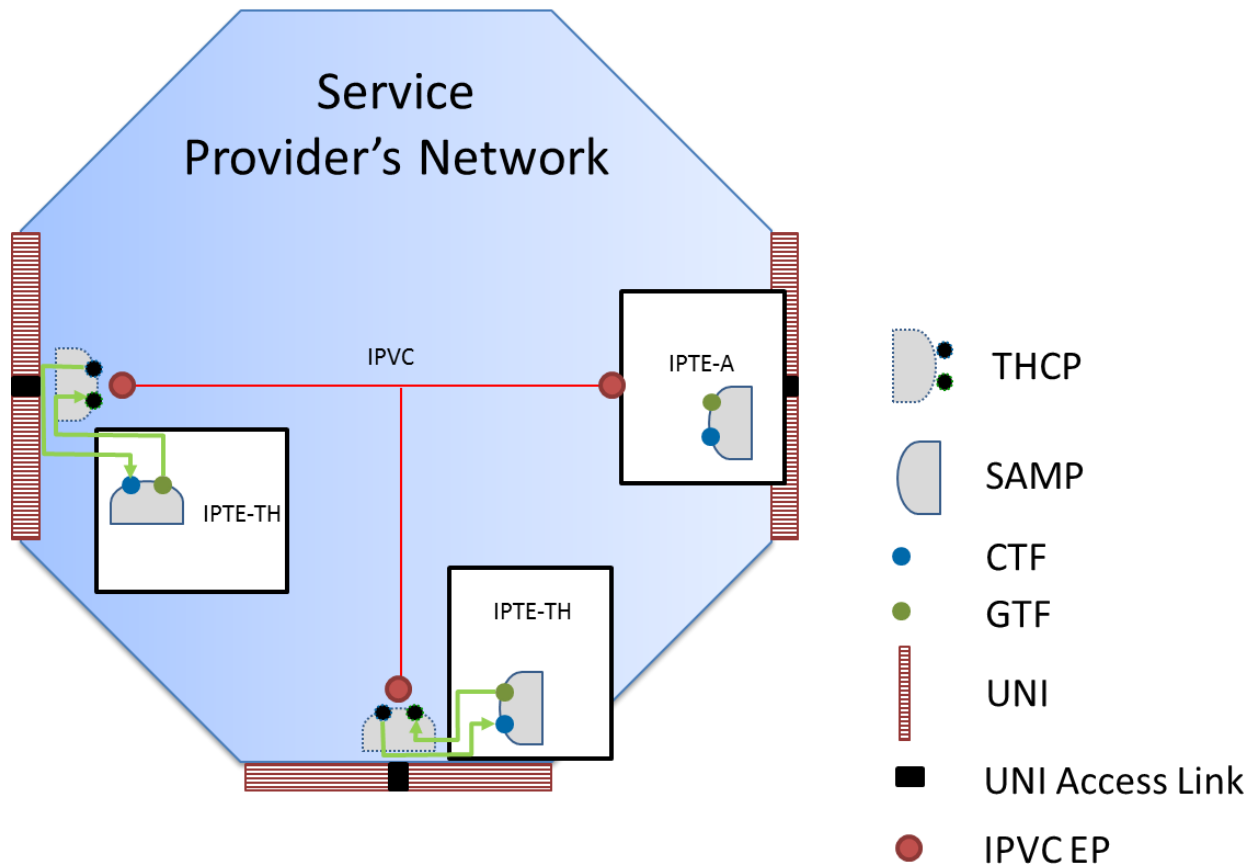
343

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

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

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

356



357

358

359

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

360

361

362

363

364

365

366

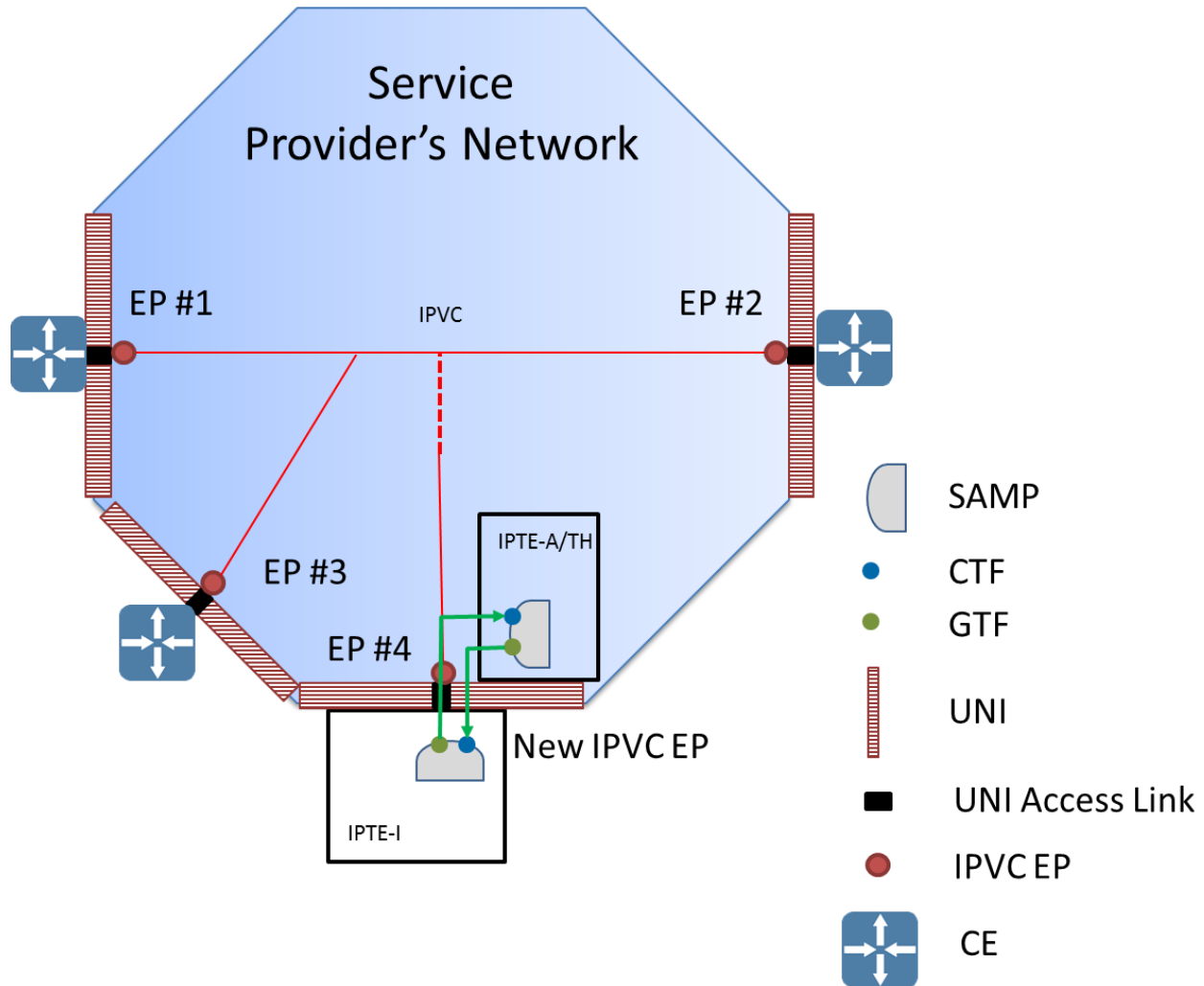
367

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

368

369

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



370

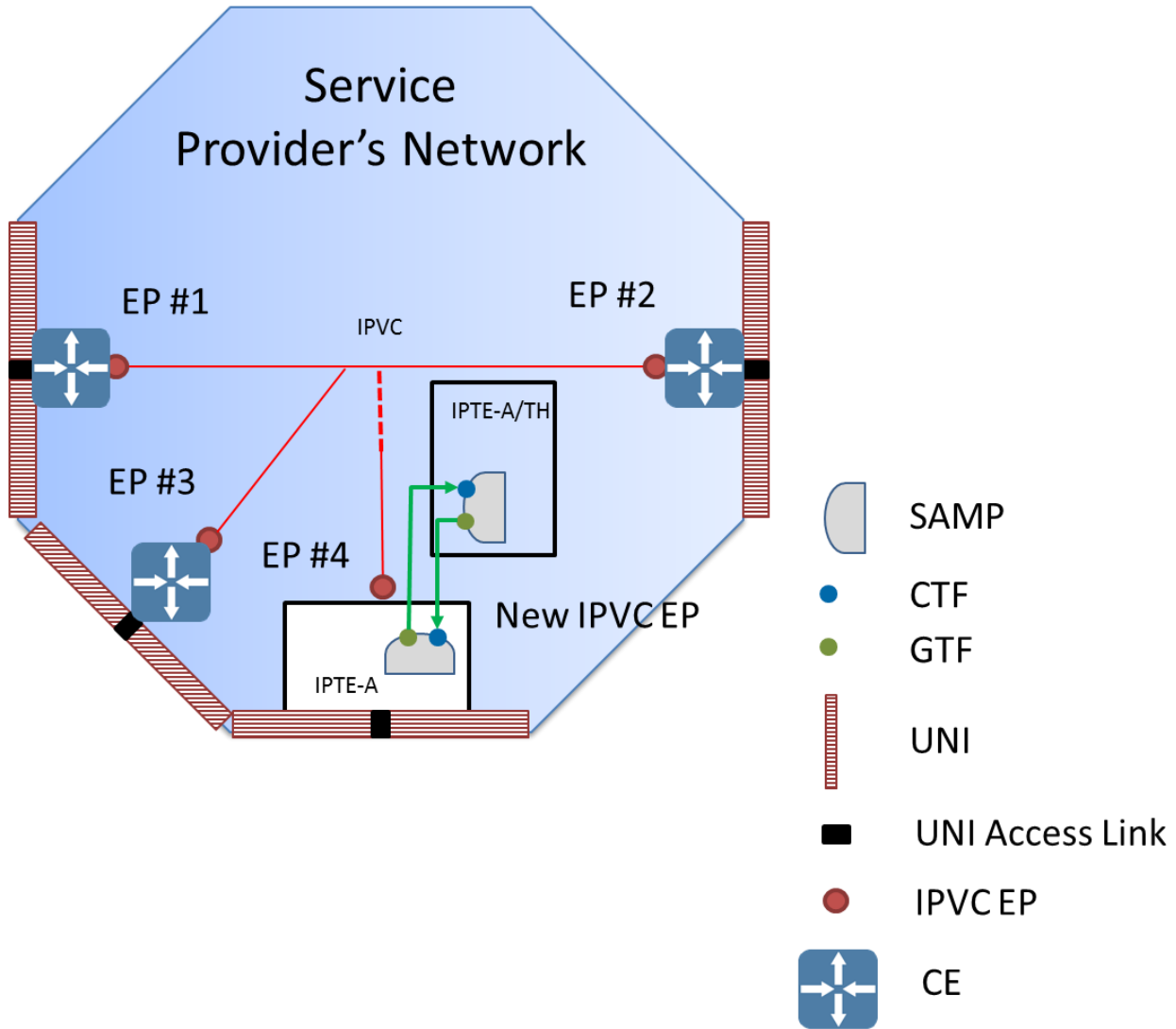
371 **Figure 6 Use Case 4: New UNI adding New IPVC EP to Existing IPVC Testing from Sub-**
 372 **scriber Side of UNI using IPTE-I**

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

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

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

390



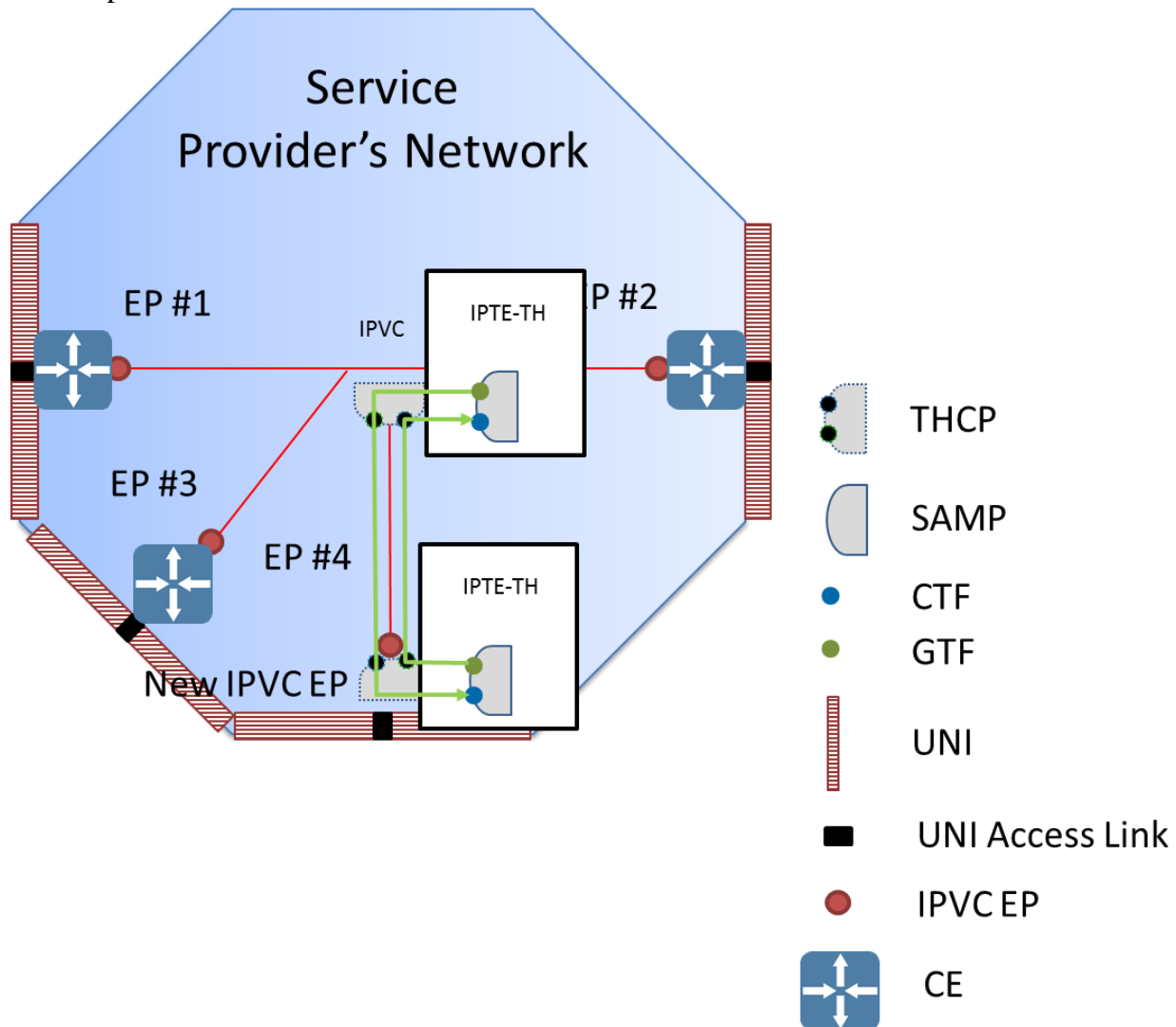
391

392 **Figure 7 Use Case 5: New IPVC EP Activation of an IPVC Testing from the Service Pro-**
 393 **vider Side of the UNI Using IPTE-A**

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

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

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



409
 410

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

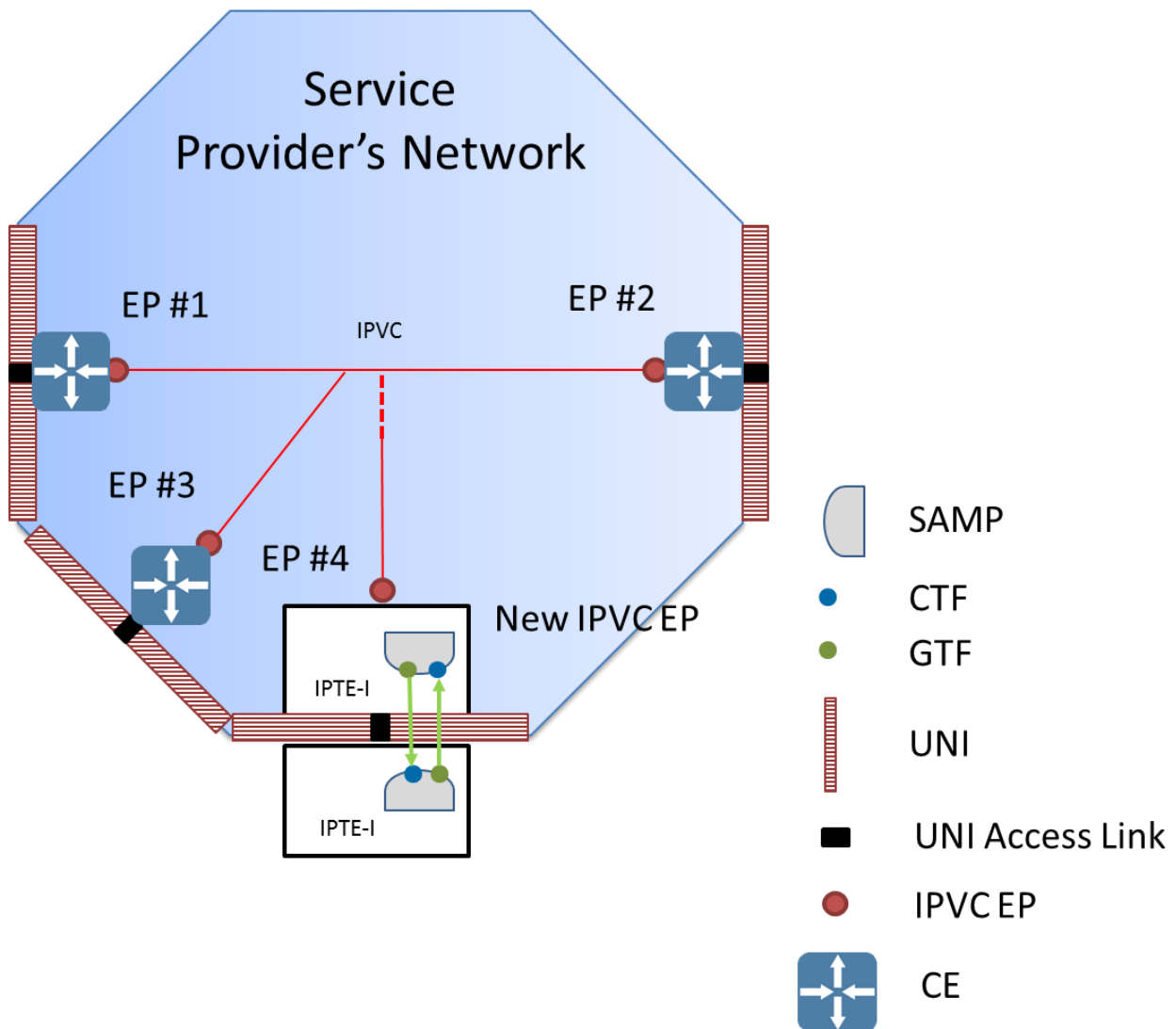
413 Figure 8 Use Case 6, shows SAT being performed on a new IPVC using two IPTE-THs. Tests
 414 are performed between the IPTE-THs. The IPTE-TH at EP #4 uses a Down SAMP and a Up
 415 THCP. The other IPTE-TH uses a Down SAMP and a Down THCP. This configuration is used
 416 to verify the IPVC and IPVC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

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

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

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

424



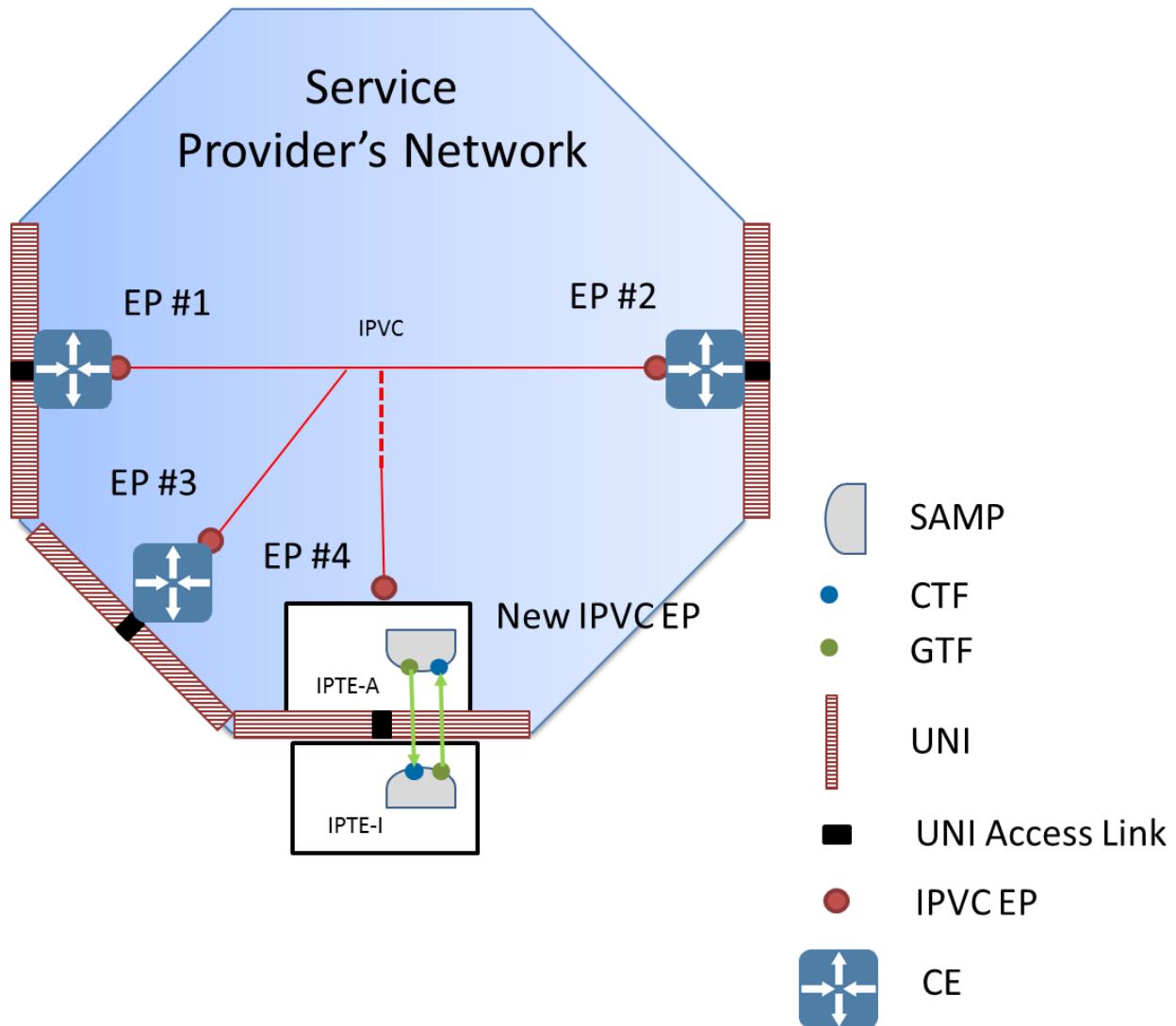
425

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

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

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

435

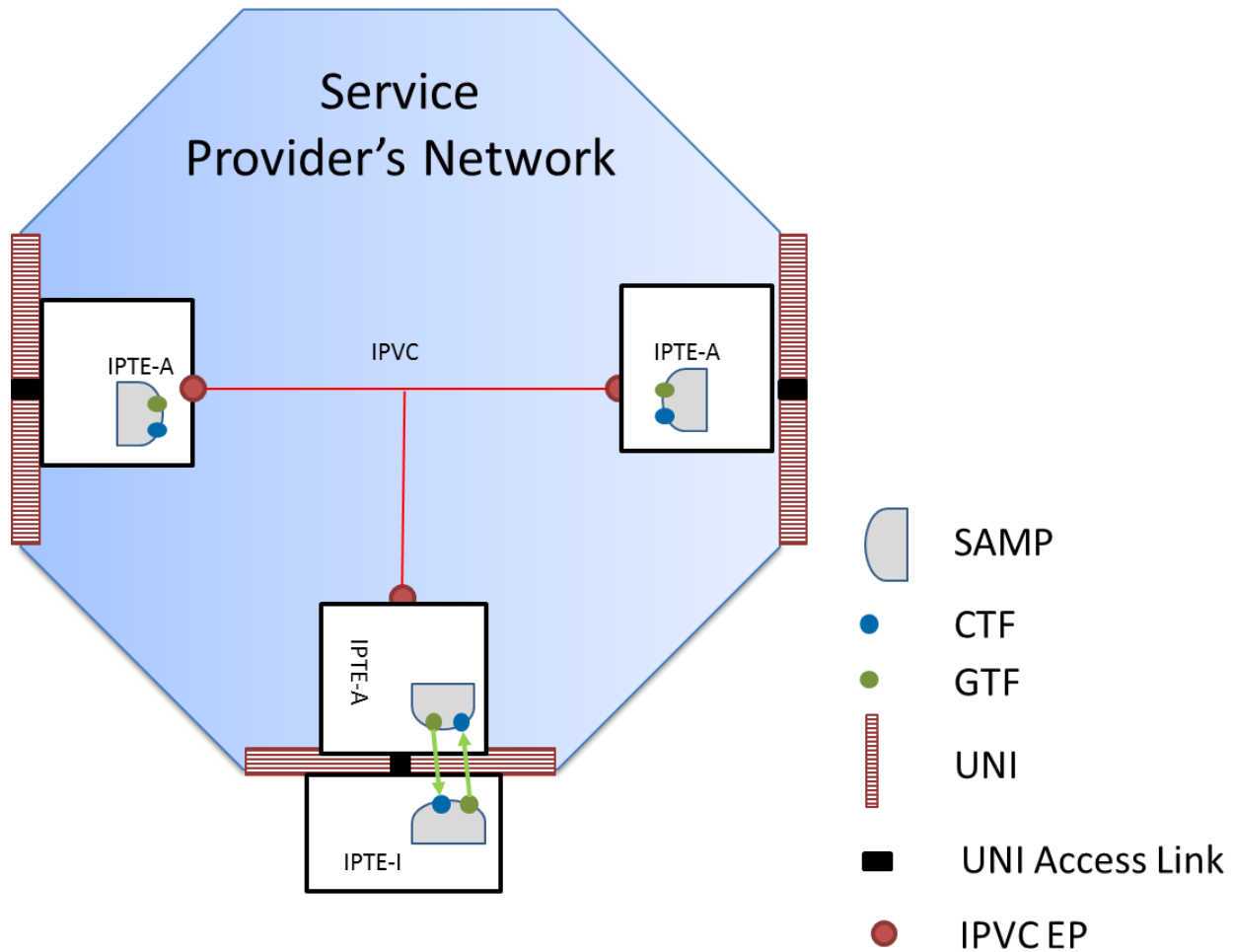


436

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

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

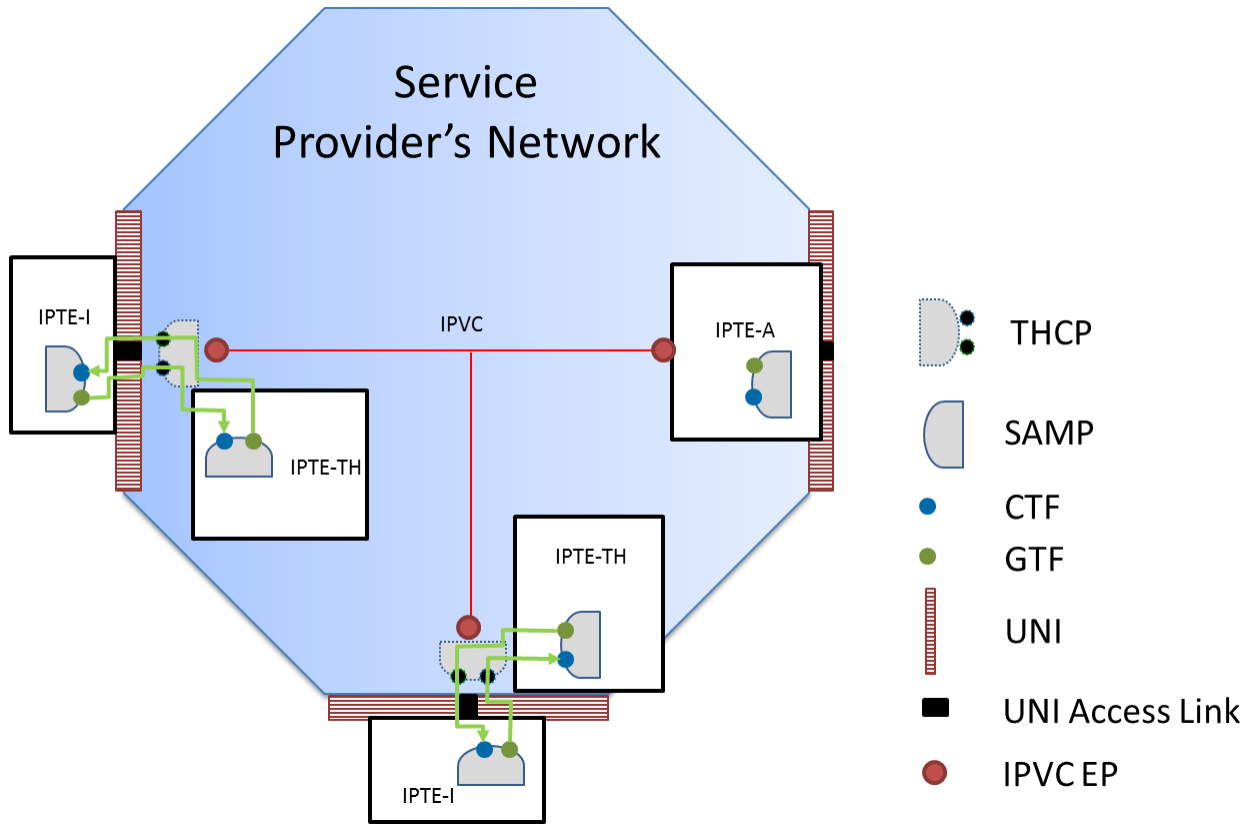
445 the UNI Access Link Service Attributes since performing tests in them could impact other UNI
 446 Access Links or IPVCs.



447
 448 **Figure 11 Use Case 9: New IPVC Activation IPTE-A to IPTE-I Testing Across UNI to Test**
 449 **UNI and UNI Access Link Service Attributes**

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

458



459

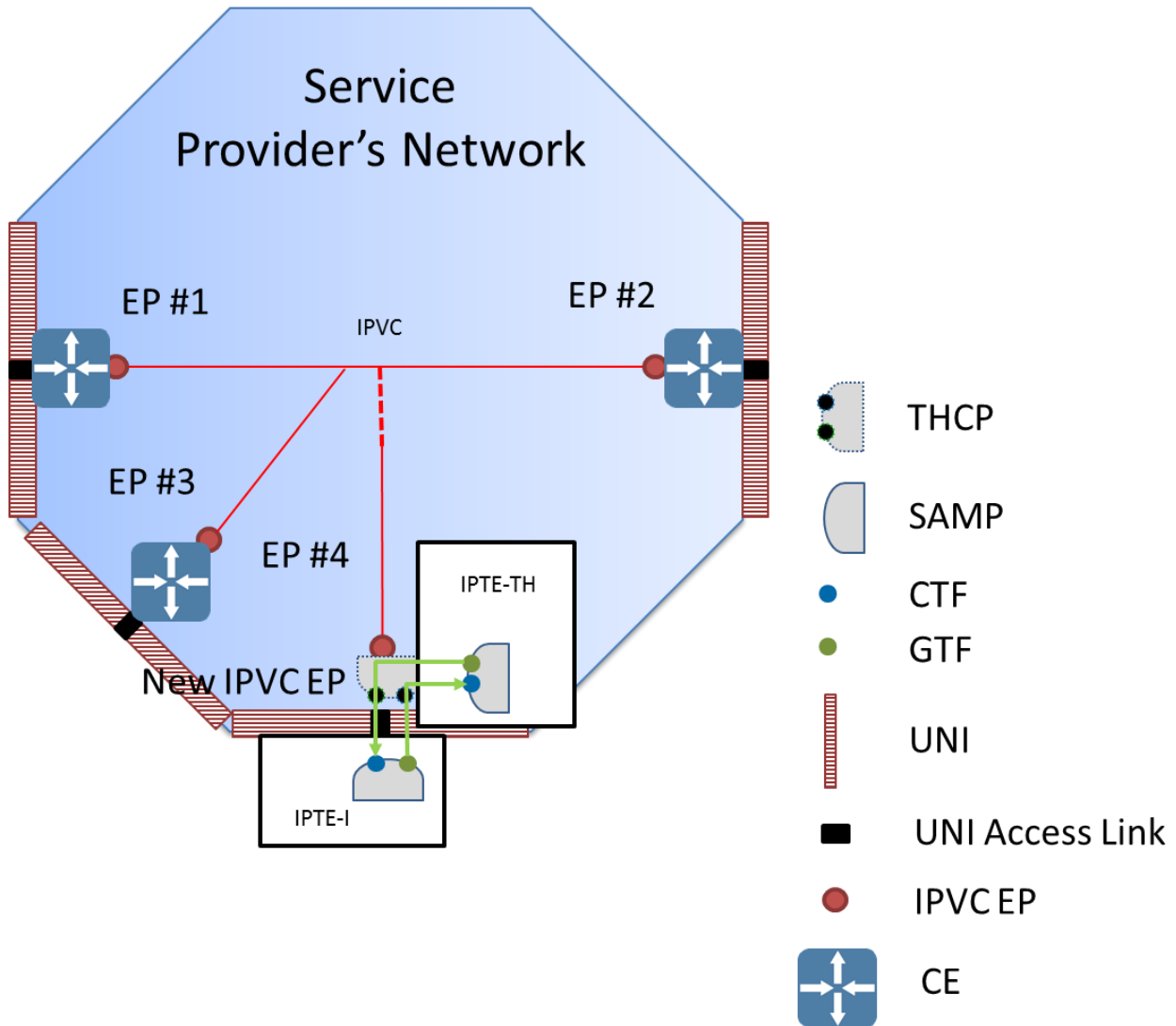
460

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

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

472

473



474
475
476
477

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

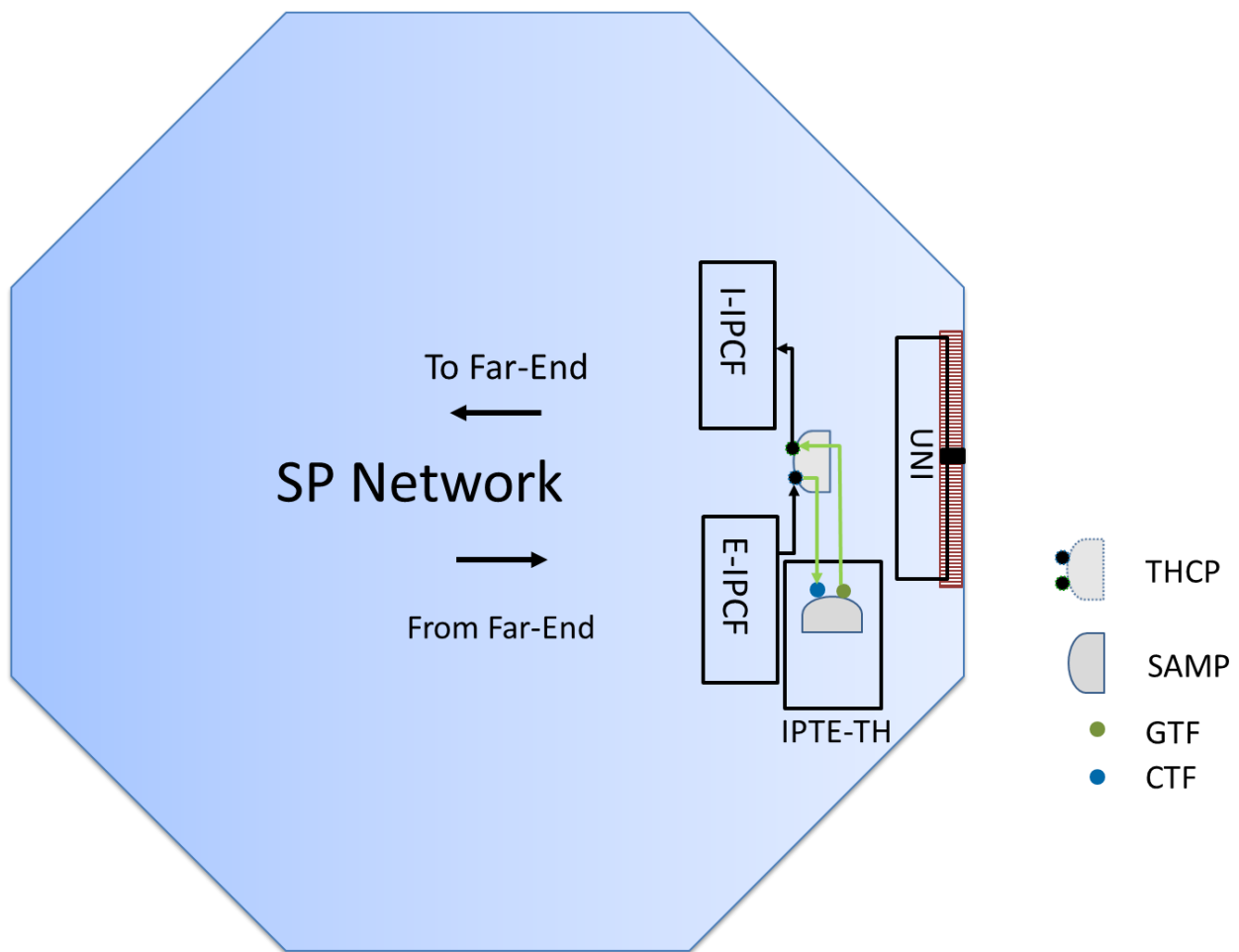
478 Figure 13 Use Case 11, shows an example of a new IPVC EP being activated where the Service
 479 Provider is testing from the Service Provider side of the UNI. An IPTE-TH and an IPTE-I are
 480 used to perform UNI and UNI Access Link Service Attribute Verification. The IPTE-TH uses a
 481 Down SAMP and a Down THCP. The IPTE-I uses a Down SAMP. The SAT is performed be-
 482 tween the IPTEs. This configuration is only used when the UNI has no existing IPVCs config-
 483 ured on it. If the UNI has IPVCs configured on it, the UNI Service Attributes have already been
 484 tested. As UNI Access Links are added it might not be possible to verify the UNI Access Link
 485 Service Attributes since performing tests on them could impact other UNI Access Links or
 486 IPVCs on the UNI.
 487

488 **8 SAMP and THCP Locations**

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

494 **8.1 Service Activation Measurement Point Locations**

495 The following figures show the location of SAMPs and THCPs in relationship to logical func-
 496 tions within the network.

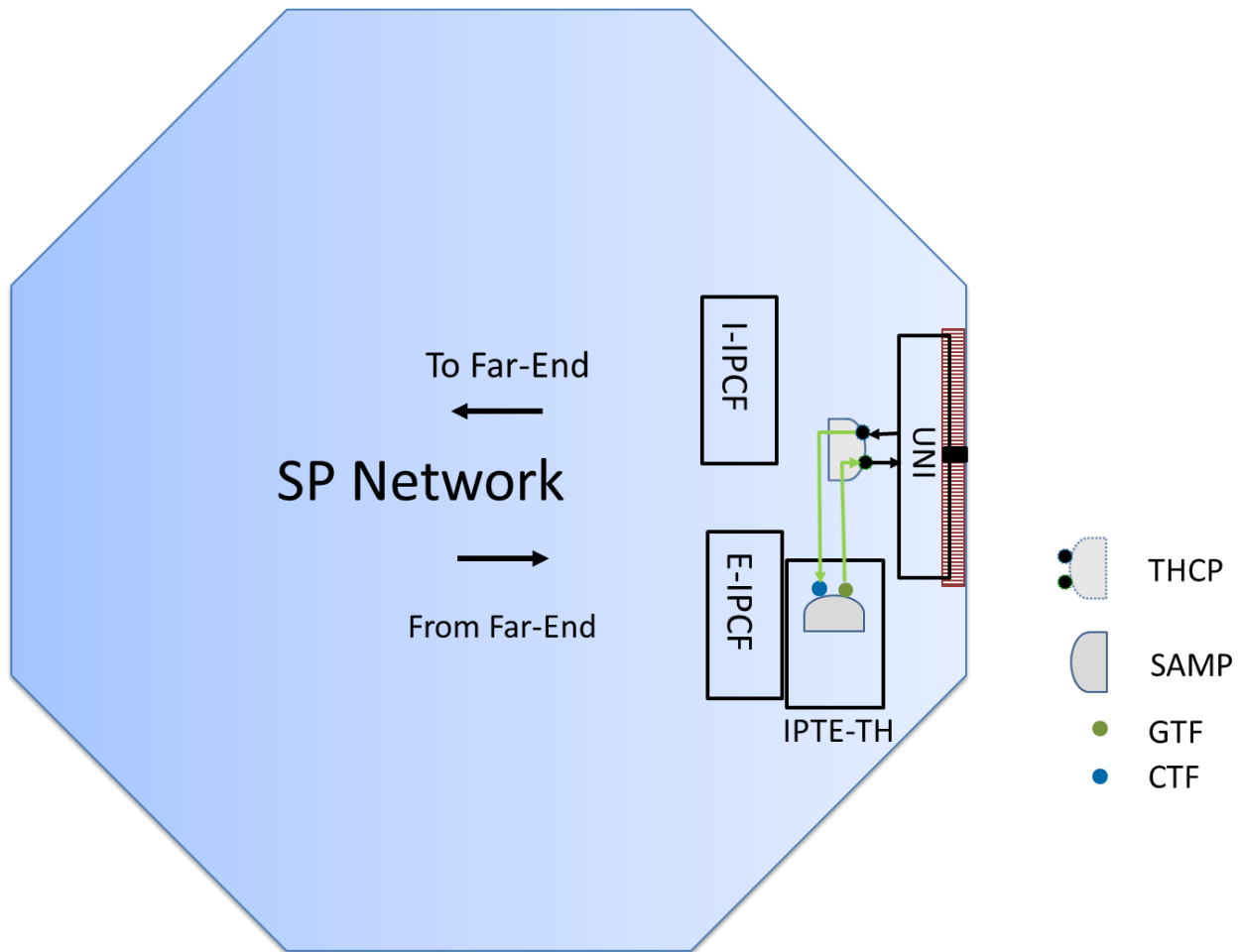


497
 498 **Figure 14 THCP Location to Verify IPVC and IPVC EP Service Attributes**

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

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

506



507

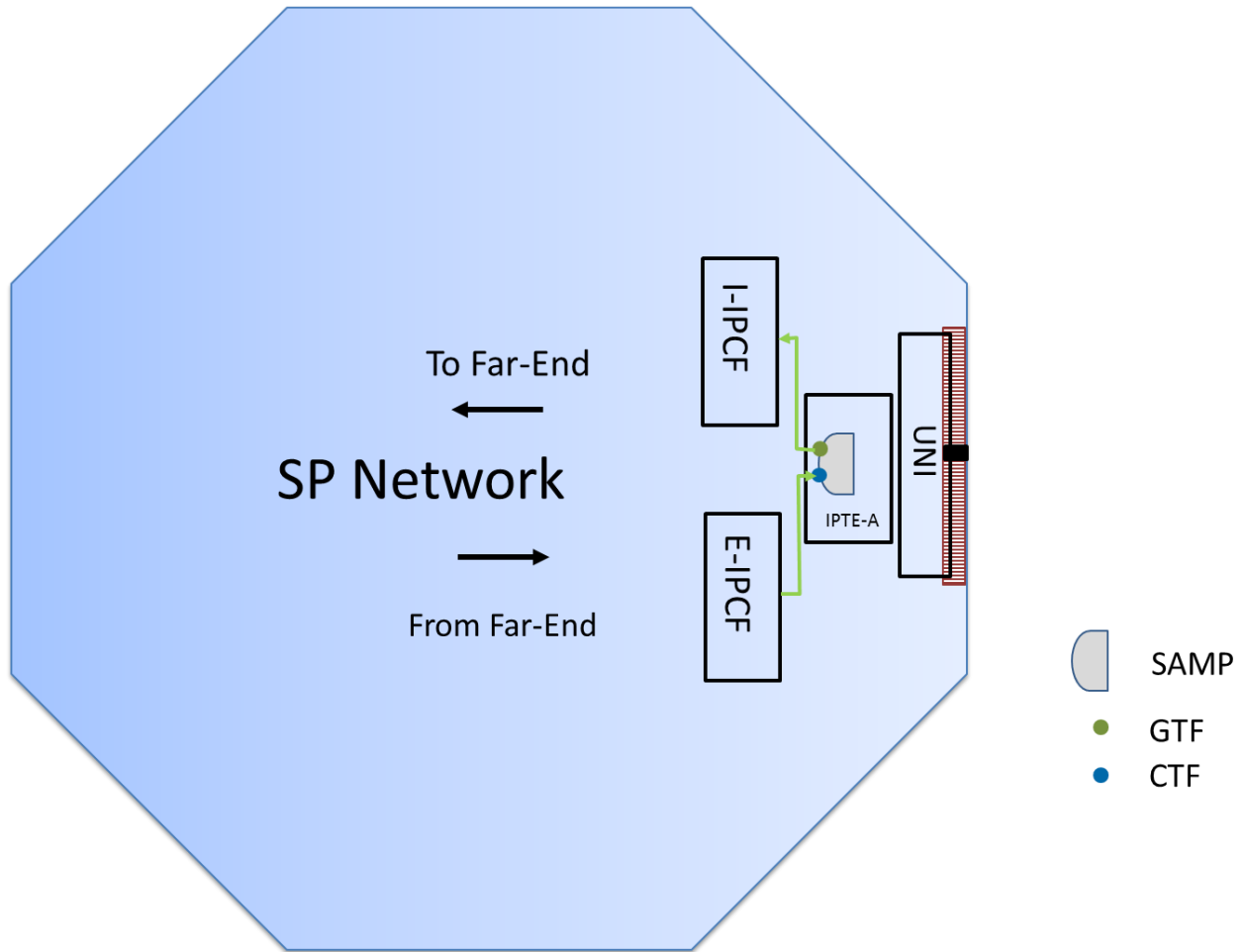
508 **Figure 15** THCP Location to Verify UNI and UNI Access Link Service Attributes

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

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

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

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

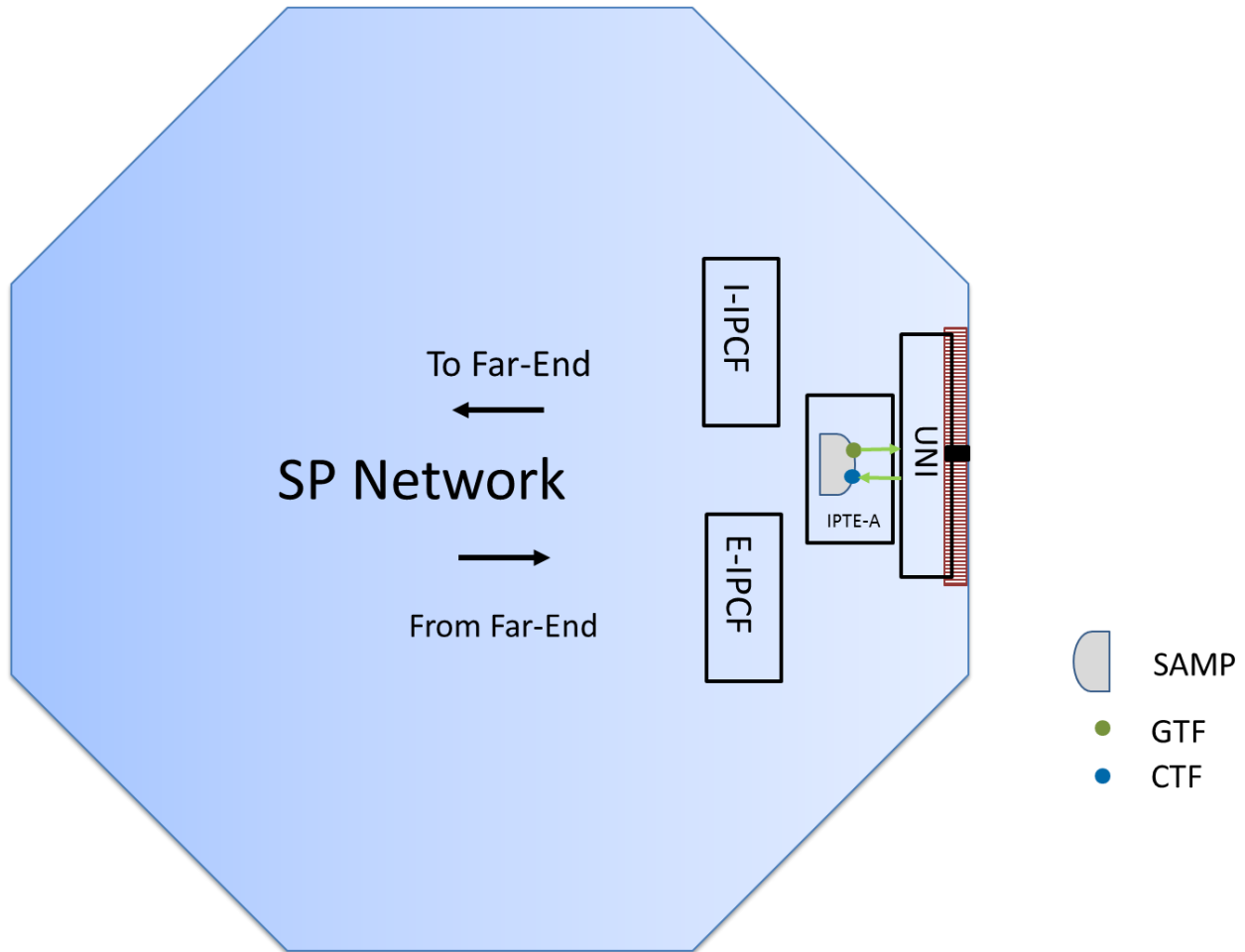


519

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

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

524



525

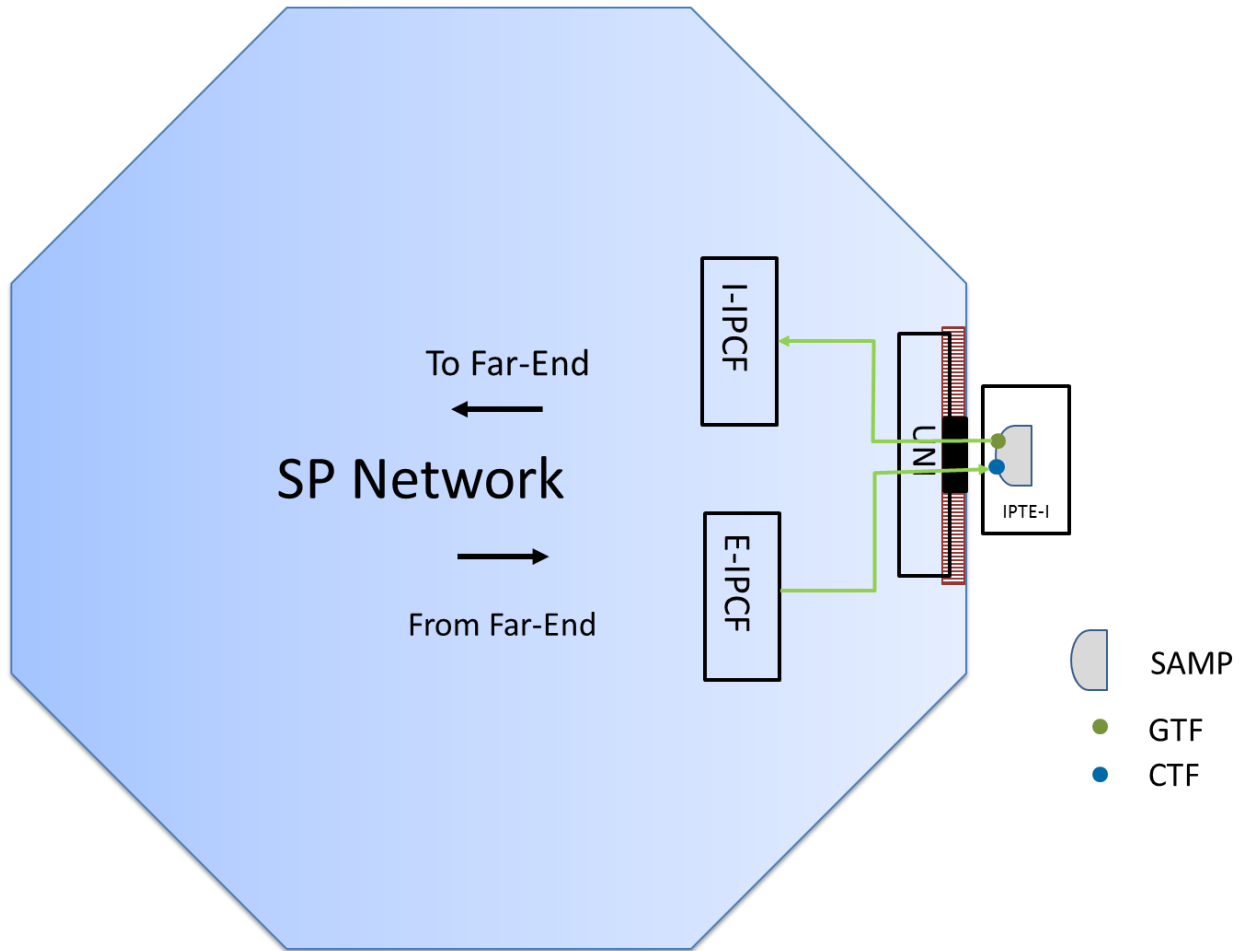
526 **Figure 17 SAMP Location in IPTE-A to Verify UNI and UNI Access Link Service Attributes**
 527

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

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

533 [R4] A SAMP implementation supporting an IPTE-A used to verify UNI and UNI
 534 Access Link Service Attributes **MUST** be implemented as shown in Figure
 535 17.

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



537

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

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

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

547

548 9 Service Attributes

549 IP Service Attributes are defined in MEF 61 [24]. This section defines how those Service At-
550 tributes are verified.

- 551
- 552 • For a specific service, each Service Attribute can either be 1) **Tested** using one of the test
553 methodologies defined in section 10 of this document, and the test result reported in the
554 SAT record, or 2) **Reported**, meaning that Service Attribute is not tested but the value of
555 the configured Service Attribute has to be reported in the SAT record or 3) **Not applica-**
556 **ble** in the context of SAT meaning that the Service Attribute is not tested nor its value re-
557 ported in the SAT record.
 - 558 • The first column of each table specifies the Service Attribute.
 - 559 • When a Service Attribute has to be **reported**, the second column, Report Status, of the
560 Service Attribute tables indicates if it is mandatory, optional, or NA to report the Service
561 Attribute.
 - 562 ○ There are two sub-columns under Report Status. The sub-column on the left is
563 for new IPVCs, UNIs, etc. as shown in Table 3. The sub-column on the right is
564 for new IPVC EPs being added to existing IPVCs as shown in Table 3.
 - 565 • When a Service Attribute has to be **tested**, the third column, Testing Status, of the Ser-
566 vice Attribute tables indicates if it is mandatory, optional, or NA to test the Service At-
567 tribute.
 - 568 ○ There are two sub-columns under Testing Status. The sub-column on the left is
569 for new IPVCs, UNIs, etc. as shown in Table 3. The sub-column on the right is
570 for new IPVC EPs being added to existing IPVCs as shown in Table 3.
 - 571 • The fourth column of the Service Attribute tables specifies which SAT methodology has
572 to be utilized to verify the Service Attribute.
 - 573 • The fifth column of the Service Attribute tables is used for comments and notes.

574 9.1 Configuration Testing

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

577 9.1.1 Subscriber UNI Service Attributes

578 Table 4 shows the Subscriber UNI Service Attributes.

579

580

581

582

583

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

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

584

Table 4 Per UNI Configuration Service Attributes

585
586
587

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

588
589
590
591

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

592

9.1.2 Subscriber UNI Access Link

593
594
595
596
597
598
599

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

600

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

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

601 **Table 5** Per UNI Access Link Configuration Service Attributes

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

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

610 **9.1.3 Subscriber IPVC Service Attributes**

611 Table 6 shows the Subscriber IPVC Service Attributes.

612

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

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

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

613

Table 6 Per IPVC Configuration Service Attributes

614

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

615

616

9.1.4 Subscriber IPVC End Point

617

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

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

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

619 **Table 7** Per IPVC EP Configuration Service Attributes

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

622 **9.2 Performance Testing**

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

630

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

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

631

Table 8 Performance Attributes

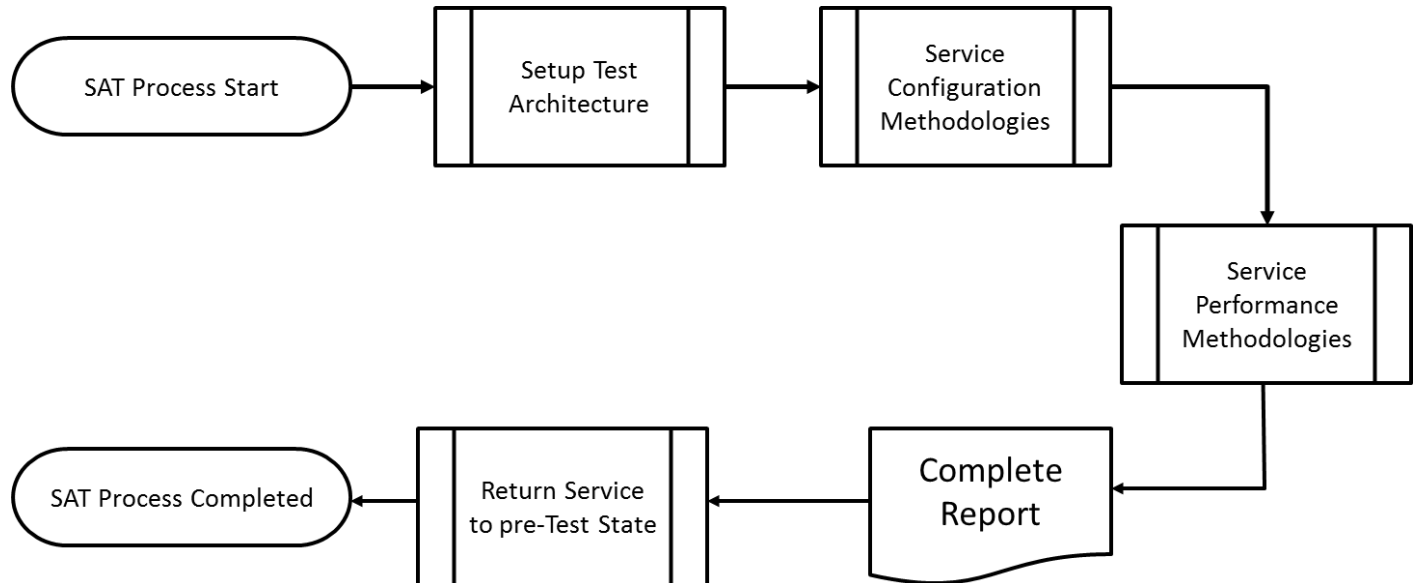
632 [R10] The Service Provider **MUST** test the performance attributes as shown in Table 8 for all new IPVCs and all new IPVC EPs being added to existing
 633 IPVCs.
 634

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

637 [R12] All Packet Loss Performance Attribute calculations **MUST** be based on Packet
 638 Loss measurements.
 639

640 **10 Service Activation Testing Methodologies**

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



648
 649 **Figure 19 Service Activation Test Process**

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

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

656 The second step in the SAT process is to perform Service Configuration methodologies. The
 657 methodologies define short measurements that are used to verify that the service has been con-
 658 figured as per the Service Description.

659 The third step in the SAT process is to perform Service Performance methodologies. The per-
 660 formance testing methodology defines a longer term test period that is used to verify if the ser-
 661 vice meets the SAC.

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

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

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

668 SAT within a single Service Provider’s network does not require that there be interoperability.
 669 The Service Provider can easily determine if the IPTEs are compatible. Since the scope of SAT
 670 for IP services is currently a single Service Provider network, interoperability is not a major con-
 671 cern. If/when this scope expands to multiple providers’ networks interoperability becomes a ma-
 672 jor concern. If standardized protocols like TWAMP or STAMP are used to perform the meas-
 673 urements, interoperability is not an issue. If proprietary packet formats or measurement proto-
 674 cols are used, then interoperability becomes a challenge. To be interoperable, both IPTEs need
 675 to understand where time stamps, sequence numbers, etc. are located within an IP Packet so that
 676 they can perform measurements.

677 **10.1 Common Methodology Requirements**

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

680 **10.1.1 Test Packet Format and Length**

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

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

685 [R15] An implementation of an IPTe **MUST** be able to generate single length pack-
 686 ets.

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

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

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

693

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

694 **Table 9 IMIX Values**

695 The numerical values in Table 9 represent IP Packet lengths in bytes. Using the values in Table
696 9 a test pattern can be specified with different length packets sent. As an example aaagg speci-
697 fies a pattern of 64 64 64 1518 1518 byte packets. This pattern is repeated for the duration of the
698 test.

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

701 [CR1]< [D2] Packet lengths specified in IETF RFC 6985 section 4 **MUST** be support-
702 ed.

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

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

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

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

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

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

715 10.1.2 Common IP Test Equipment Requirements

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

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

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

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

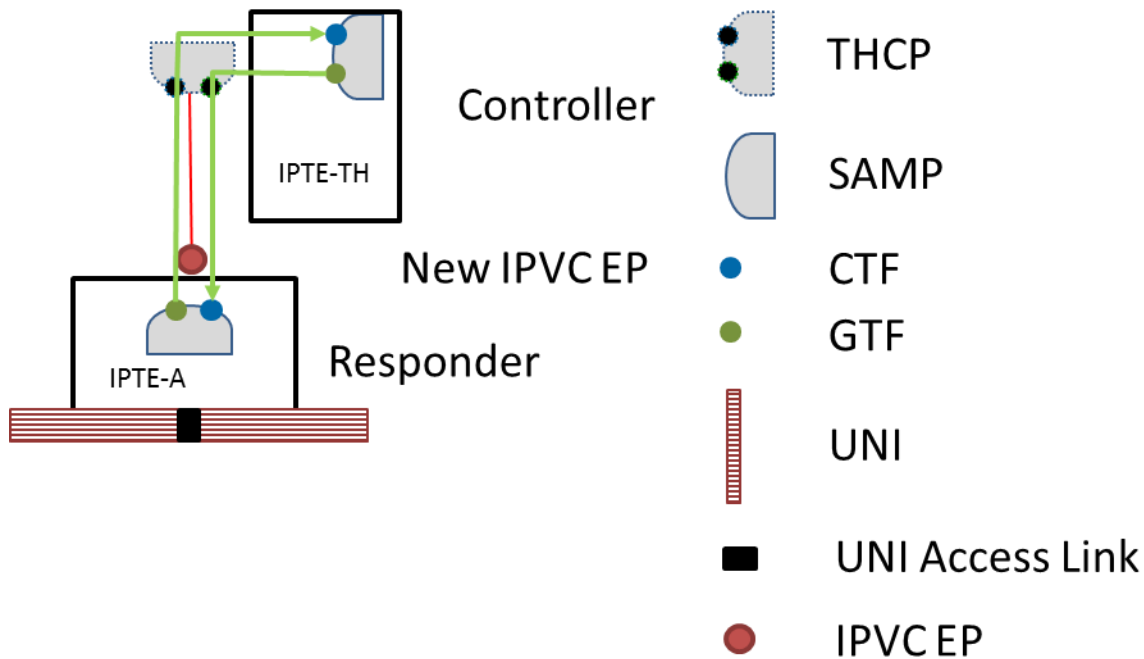
726 The delay performance metrics defined in MEF 61 [24] use a percentile of packets measured
727 over a period of time T. The method used by a particular IPTE implementation (timestamp loca-
728 tion, packet format, etc.) to perform delay measurements is outside the scope of this document.

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

734 [R19] SAT **MUST** be performed in both the forward and backward directions be-
 735 tween two IPTEs simultaneously.

736 **10.1.3 Test Measurements**

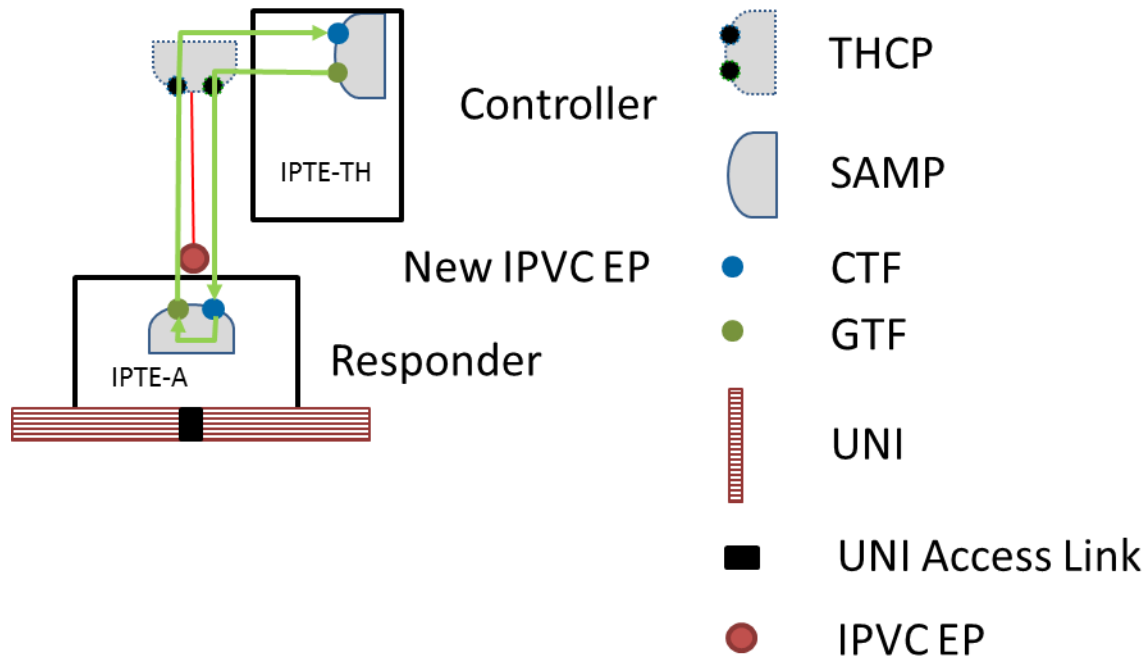
737 Test measurements are performed from the Controller end of the service to the Responder end of
 738 the service and from the Responder end of the service to the Controller end of the service. The
 739 Controller end initiates the Test measurement. The Responder end either processes the packet
 740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



743

744 **Figure 20 Responder Processing Packet**

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



753

754

Figure 21 Responder Looping Back Packet

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

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

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

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

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

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

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

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

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

784 10.2 Service Acceptance Criteria

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

788 A SAC is specified for each tested Service Attribute and direction of a test. SAC are for the
789 Forward and Backward directions of a service do not have to be the same for both directions al-
790 though they are normally. The value specified for a SAC is defined to ensure that the Service At-
791 tribute being measured meets Subscriber expectations. Due to the shorter duration measure-
792 ments used by SAT, a direct correlation between SLS values and SAC values does not need to be
793 done. Examples of SAC that can be used for Configuration or Performance tests are IR_{SAC} ,
794 PD/MPD_{SAC} , $IPDV/PDR_{SAC}$, and PLR_{SAC} . The use of these SAC are shown in the test methodol-
795 ogies in section 10.3 and 10.4.

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

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

798 10.3 Service Configuration Tests

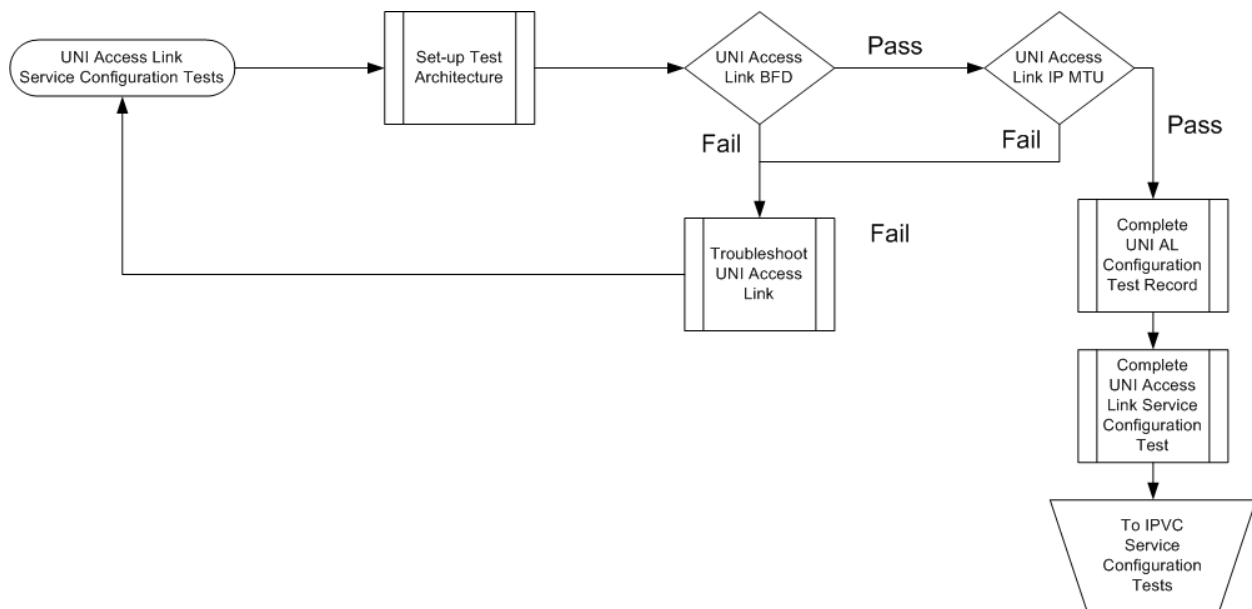
799 Service configuration tests are performed to verify that the IP Service has been correctly config-
800 ured and that tested Service Attributes are set per the service agreement between the Subscriber
801 and the Service Provider. Service configuration tests are normally of a short duration, long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

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

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

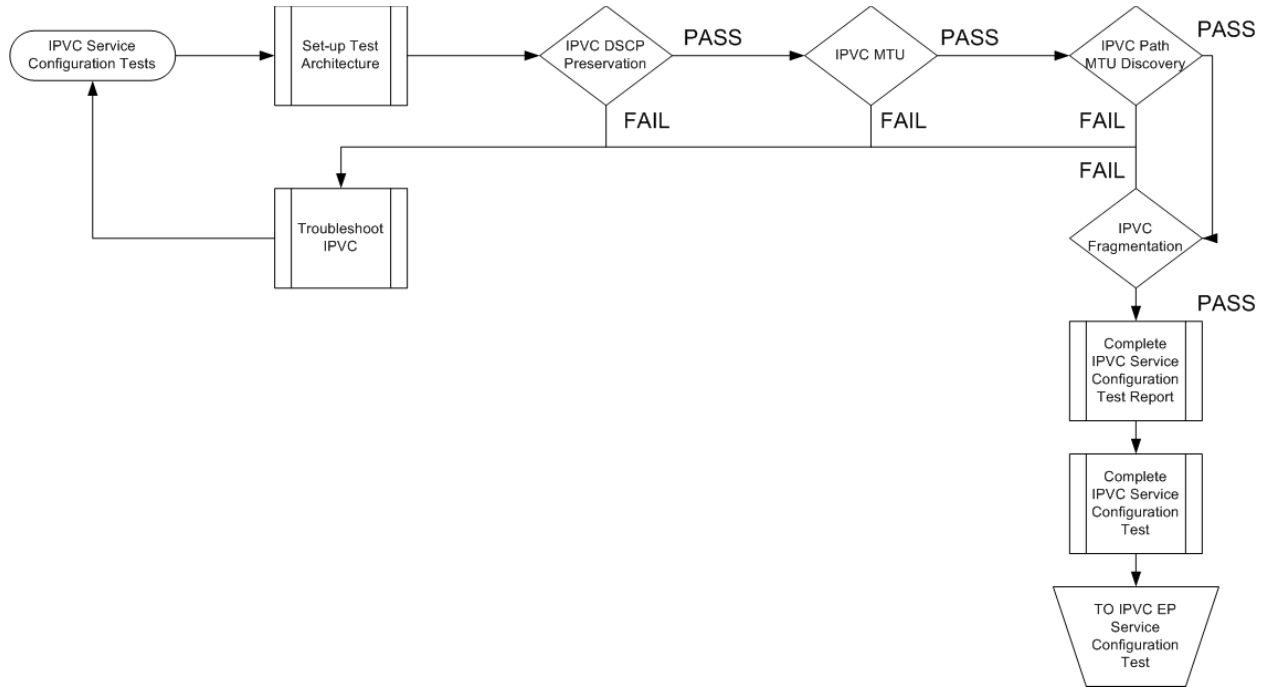
814 Service configuration tests are performed on a UNI at the time it is activated. Service configura-
 815 tion tests are performed on an UNI Access Link at the time that it is activated as described in
 816 section 7.2. The service configuration tests are performed on an IPVC and IPVC EP at the time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

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



823
 824
 825

Figure 22 UNI Access Link Service Configuration Tests

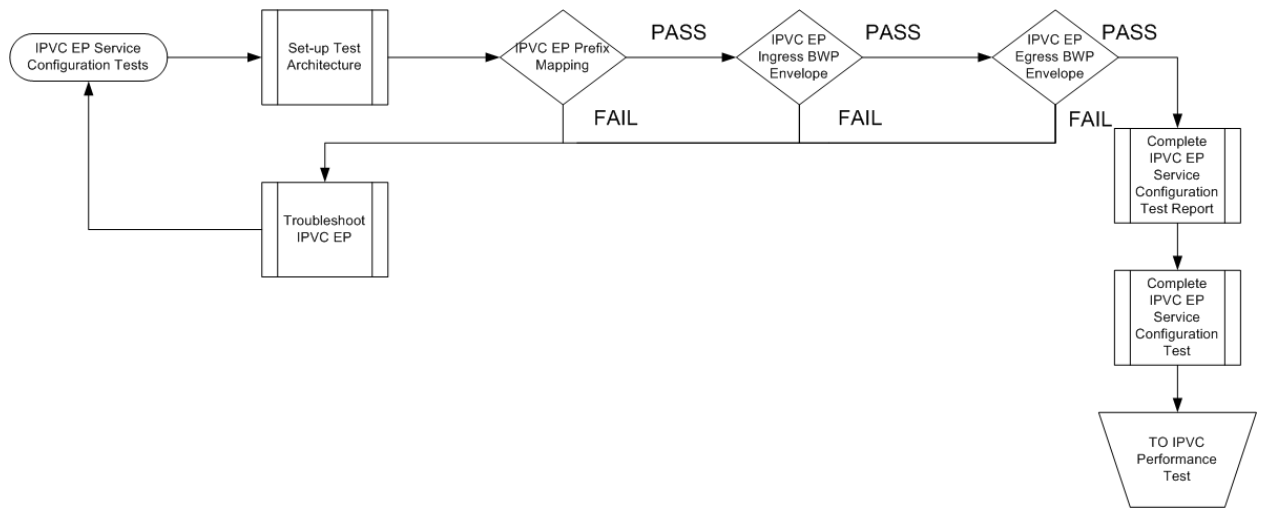


826

827

Figure 23 IPVC Service Configuration Tests

828



829

830

Figure 24 IPVC EP Service Configuration Tests

831 **10.3.1 UNI Access Link Service Configuration Test**

832 The UNI Access Link Service Configuration test methodologies are included in the following
 833 sections. UNI Access Link Service Configuration tests are performed when a UNI Access Link
 834 is initially configured after the UNI has been activated. Figure 9, Figure 10, Figure 11, Figure
 835 12, and Figure 13 show the configuration used to test the UNI Access Link.

836 **10.3.1.1 UNI Access Link BFD Service Provider Active**

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

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

842

Service Activation Test Methodology	
Test Name	UNI Access Link BFD
Test Type	Service Activation
Service Type	IP UNI Access Link
Test Status	Mandatory if UNI Access Link BFD Service Attribute is not <i>None</i> and the Active End Service Attribute is <i>SP</i> or <i>Both</i>
Test Objective	<p>Verify that if the UNI Access Link BFD attribute is not <i>None</i> that the following are configured correctly in the Service Provider's equipment:</p> <ul style="list-style-type: none"> • Connection Address Family • Transmission Interval • Detect Multiplier • Active End • Authentication Type
Test Procedure	<ul style="list-style-type: none"> • IPTE₁ located within SP network takes on the Active role of a BFD session as defined in IETF RFC 5880 [10] and sends BFD Control Packets encapsulated within IPv4 packets (when Connection Address Family = <i>IPv4</i> or <i>Both</i>) using attributes as defined in the service definition to the device (either Subscriber CE or Service Provider IPTE-I) at the Subscriber end of the UNI Access Link when Active End = <i>SP</i>. • IPTE₁ sends BFD Control Packets for period T_{BFD} or until the BFD session state is <i>Up</i> as defined in IETF RFC 5880 [10] . • IPTE₁ located within the SP network takes on the Active role of a BFD session as defined in IETF RFC 5880 [10] and sends BFD

	<p>Control Packets encapsulated within IPv6 packets (when Connection Address Family = <i>IPv6</i> or <i>Both</i>) using attributes as defined in the service definition to the device (either Subscriber CE or Service Provider IPTE-I) at the Subscriber end of the UNI Access Link when Active End = <i>SP</i>.</p> <ul style="list-style-type: none"> • IPTE₁ sends BFD Control Packets for period T_{BFD} or until the BFD session state is <i>Up</i> as defined in IETF RFC 5880 [10].
Variables	<p>Connection Address Family, Transmission Interval, Detect Multiplier, Active End, Authentication Type, BFD Session State, T_{BFD}</p>
Results	<p>Pass = BFD session is UP with transmission interval and detect multiplier as per the service definition.</p> <p>Fail = BFD session is not up when T_{BFD} expires or the transmission interval or detect multiplier is not as per the service definition.</p>
Remarks	<ol style="list-style-type: none"> 1. This test does not use PL or PLR as a unit. Instead it uses the BFD session state of UP and the correct transmission interval and detect multiplier as the indicators of the test. 2. This testing is only possible if there is a device connected to the UNI that is acting as a BFD peer. 3. Testing is done for IPv4, IPv6, or Both depending on the value of Connection Address Family

843 **Table 10** UNI Access Link BFD Test Methodology

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

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

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

849 **10.3.1.2 UNI Access Link BFD Subscriber Active**

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

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

855

Service Activation Test Methodology

Test Name	UNI Access Link BFD
Test Type	Service Activation
Service Type	IP UNI Access Link
Test Status	Mandatory if UNI Access Link BFD Service Attribute is not <i>None</i> and Active End Service Attribute is <i>Subscriber</i>
Test Objective	<p>Verify that if the UNI Access Link BFD attribute is not <i>None</i> that the following are configured correctly in the Service Provider's equipment:</p> <ul style="list-style-type: none"> • Connection Address Family • Transmission Interval • Detect Multiplier • Active End • Authentication Type
Test Procedure	<ul style="list-style-type: none"> • IPTE₁ located within the Service Provider network takes on the Passive role of a BFD session as defined in IETF RFC 5880 [10] and waits for BFD Control Packets from device (either Subscriber CE or Service Provider IPTE-I) at the Subscriber end of the UNI Access Link encapsulated in IPv4 (when Connection Address Family = IPv4 or Both) packets using attributes as defined in the service definition from the device at the Subscriber end of the UNI Access Link when Active End = Subscriber. • IPTE₁ waits for BFD Control Packets for period T_{BFD}, for a pre-determined time, or until the BFD session state is <i>Up</i> as defined in IETF RFC 5880 [10]. • IPTE₁ located within the Service Provider network takes on the Passive role of a BFD session as defined in IETF RFC 5880 [10] and waits for BFD Control Packets from device (either Subscriber CE or Service Provider IPTE-I) at the Subscriber end of the UNI Access Link encapsulated in IPv6 (when Connection Address Family = IPv6 or Both) packets using attributes as defined in the service definition from the device at the Subscriber end of the UNI Access Link when Active End = Subscriber. • IPTE₁ waits for BFD Control Packets for period T_{BFD}, for a pre-determined time, or until the BFD session state is <i>Up</i> as defined in IETF RFC 5880 [10].

Variables	Connection Address Family, Transmission Interval, Detect Multiplier, Active End, Authentication Type, BFD Session State, T_{BFD}
Results	<p>Pass = BFD session is up with transmission interval and detect multiplier as per the service definition.</p> <p>Fail = BFD session is not up when T_{BFD} expires or the transmission interval or detect multiplier is not as per the service definition.</p>
Remarks	<ol style="list-style-type: none"> 1. This test does not use PL or PLR as a unit. Instead it uses the BFD session state of UP and the correct transmission interval and detect multiplier as the indicators of the test. 2. This testing is only possible if a device is connected to the UNI and is acting as a BFD peer. 3. Testing is done for IPv4, IPv6, or Both depending on the value of Connection Address Family

856 **Table 11** UNI Access Link BFD Test Methodology

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

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

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

862 **10.3.1.3 UNI Access Link IP MTU**

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

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

871

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

Test Status	Optional for new UNI AL
Test Objective	Verify that the UNI Access Link IP MTU attribute is configured correctly.
Test Procedure	<ul style="list-style-type: none"> • IPTE₁ offers IP Data Service packets with the DA of IPTE₂ as per the Service Definition with a length equal to the UNI AL IP MTU at EI₁ with a rate up to IR_{SC} and for a time T_{SC} as specified by the Service Provider. • IPTE₂ verifies that the packets offered at EI₁ are received as defined in the Service Definition at EI₂. Packet Loss is acceptable up to PLR_{SAC}, where PLR_{SAC} is the SAC for Packet Loss Ratio. • Simultaneously, IPTE₂ offers IP Data Service packets with the DA of IPTE₁ as per the Service Definition with a length equal to the UNI AL IP MTU at EI₂ with a rate up to IR_{SC} and for a time T_{SC} as specified by the Service Provider. • IPTE₁ verifies that the packets offered at EI₂ are received as defined in the Service Definition at EI₁. Packet Loss is acceptable up to PLR_{SAC}, where PLR_{SAC} is the SAC for Packet Loss Ratio.
Variables	DA, IPVC MTU, IR _{SC} , T _{SC} , PL, and PLR _{SAC}
Results	Pass, Fail
Remarks	<ol style="list-style-type: none"> 1. Testing is only possible if an IPVC is configured on the UNI. 2. A range of IP Data Service packet lengths starting as small as 68B and increasing to the maximum length desired can be used instead of a single length 3. This testing is only possible if there is an IPTE at the Subscriber end of the UNI. This could be an IPTE-A in the CE or an IPTE-I connected to the UNI.

872 **Table 12** UNI Access Link IP MTU Test Methodology

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

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

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

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

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

879 **10.3.2 IPVC Configuration Tests**

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

885 **10.3.2.1 IPVC DSCP Preservation**

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

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

889

Service Activation Test Methodology	
Test Name	IPVC DSCP Preservation
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory when <i>Enabled</i>
Test Objective	Verify that the IPVC DSCP Preservation attribute is configured correctly.
Test Procedure	<ul style="list-style-type: none"> • IPTE₁ offers IP Data Service packets with the DA of IPTE₂ as per the Service Definition at EI₁ with a rate equal to IR_{SC} for a time T_{SC} and with a DSCP value in the below list. • IPTE₂ verifies that the packets received at EI₂ have the same DSCP as was offered at EI₁. An IP Data Service packet received with an incorrect DSCP value is considered lost. Packet Loss is acceptable up to PLR_{SAC}, where PLR_{SAC} is the SAC for Packet Loss Ratio. Note: The method used to communicate the DSCP value between IPTE₁ and IPTE₂ is beyond the scope of this document. • Simultaneously, IPTE₂ offers IP Data Service packets with the DA of IPTE₁ as per the Service Definition at EI₂ with a rate equal to IR_{SC} for a time T_{SC} and with the same DSCP value as bullet 1. • IPTE₁ verifies that the packets received at EI₁ have the same DSCP as was offered at EI₂. An IP Data Service packet received

	<p>with an incorrect DSCP is considered lost. Packet Loss is acceptable up to PLR_{SAC}, where PLR_{SAC} is the SAC for Packet Loss Ratio. Note: The method used to communicate the DSCP value between $IPTE_1$ and $IPTE_2$ is beyond the scope of this document.</p> <ul style="list-style-type: none"> The above is repeated for each DSCP value that is included in the list for the IPVC that is agreed to by the Service Provider and Subscriber.
Variables	List of DSCP values, IR_{SC} , T_{SC} , PLR_{SAC}
Results	Pass or fail
Remarks	<ol style="list-style-type: none"> The DSCP value in packets is set per the Service Definition and is maintained in received packets for the test to pass. At minimum a sample of the 64 DSCP values is tested. The SP and Subscriber can determine how large a sample is sufficient to test. Figure 14, Figure 16, and Figure 18 show the SAMP location needed at each end of this Test Methodology to ensure that any DSCP manipulation points are included in the test. PLR_{SAC} for this test is recommended to be set at 0%.

890

Table 13 IPVC DSCP Preservation Test Methodology

891

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

892

893

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

894

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

895

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

896

10.3.2.2 IPVC MTU

897

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

898

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

899

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

Service Type	IPVC
Test Status	Mandatory for new IPVC, Mandatory for new IPVC EP on new UNI, Optional for new IPVC EP on UNI with existing IPVCs
Test Objective	Verify that the IPVC MTU attribute is configured correctly.
Test Procedure	<ul style="list-style-type: none"> • IPTE₁ offers IP Data Service packets with the DA of IPTE₂ as per the Service Definition with a length equal to the IPVC MTU at EI₁ with a rate equal to IR_{SC} and for a time T_{SC} as specified by the Service Provider. • IPTE₂ verifies that the packets offered at EI₁ are received as defined in the Service Definition at EI₂. Packet Loss is acceptable up to PLR_{SAC}, where PLR_{SAC} is the SAC for Packet Loss Ratio. • Simultaneously, IPTE₂ offers IP Data Service packets with the DA of IPTE₁ as per the Service Definition with a length equal to the IPVC MTU at EI₂ with a rate equal to IR_{SC} and for a time T_{SC} as specified by the Service Provider. • IPTE₁ verifies that the packets offered at EI₂ are received as defined in the Service Definition at EI₁. Packet Loss is acceptable up to PLR_{SAC}, where PLR_{SAC} is the SAC for Packet Loss Ratio.
Variables	IPVC MTU, IR _{SC} , T _{SC} , and PLR _{SAC}
Results	Pass, Fail
Remarks	<ol style="list-style-type: none"> 1. A range of IP Data Service packet lengths starting as small as 68B and increasing to the maximum length desired can be used instead of a single length

Table 14 IPVC MTU Test Methodology

900

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

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

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

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

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

908 **10.3.2.3 IPVC Path MTU Discovery**

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

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

913

Service Activation Test Methodology	
Test Name	IPVC Path MTU Discovery
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory for new IPVC when <i>Enabled</i>
Test Objective	Verify that the IPVC Path MTU Discovery attribute is configured correctly.
Test Procedure	<ul style="list-style-type: none"> • IPTE₁ offers IP Data Service packets with the DA of IPTE₂ in excess by 10% of the largest UNI AL IP MTU for UNIs in the IPVC with the DF bit set at rate IR_{SC} for period T_{SC}. • IPTE₁ collects ICMP Datagram Too Big messages for IPv4 or Packet Too Big messages for IPv6 received from the Service Provider network. If any messages are received test passes. If no messages are received the test fails. • Simultaneously, IPTE₂ offers IP Data Service packets with the DA of IPTE₁ in excess by 10% of the largest UNI AL IP MTU for UNIs in the IPVC with the DF bit set at rate IR_{SC} for period T_{SC}. • IPTE₂ collects ICMP Datagram Too Big messages for IPv4 or Packet Too Big messages for IPv6 received from the Service Provider network. If any messages are received test passes. If no messages are received the test fails.
Variables	IR _{SC} , T _{SC} , DA, ICMP messages
Results	Pass = Appropriate ICMP message received from SP network during time T _{SC} Fail = No ICMP message received from SP network during time T _{SC} for

	any IP Data Service packet size
Remarks	

914 **Table 15** IPVC Path MTU Discovery Test Methodology

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

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

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

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

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

922 **10.3.2.4 IPVC Fragmentation**

923 The correct configuration of the IPVC Fragmentation attribute is verified with this method-
924 ology.

925 [R57] The IPVC Fragmentation attribute **MUST** be verified as described in Table
926 16.

927

Service Activation Test Methodology	
Test Name	IPVC Fragmentation
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory when <i>Disabled</i>
Test Objective	Verify that the IPVC Fragmentation Service Attribute is configured correctly.
Test Procedure	<ul style="list-style-type: none"> • IPTE₁ offers at EI₁ IP Data Service packets with the DA of IPTE₂ of a length 15% greater than the IPVC MTU with a rate equal to IR_{SC} for a time of T_{SC}. • IPTE₂ verifies at EI₂ that no fragmented IP Data Service packets are be received. • Simultaneously IPTE₂ offers at EI₂ IP Data Service packets with

	<p>the DA of IPTE₁ of a length 15% greater than the IPVC MTU with a rate equal to IR_{SC} for a time of T_{SC}.</p> <ul style="list-style-type: none"> • IPTE₁ verifies at EI₁ that no fragmented IP Data Service packets are be received.
Variables	IR _{SC} , T _{SC} , PLR _{SAC} , DA
Results	<p>Pass = IP Data Service packets received with no fragmented packets received</p> <p>Fail = Any fragmented IP Data Service packets received during T_{SC}</p>
Remarks	<ol style="list-style-type: none"> 1. The Pass condition of no fragmented packets received includes no IP Data Service packets received. MEF 61 [24] allows packets greater than the MTU to be passed, fragmented, or discarded. If no packets are received they might have been discarded which means that the behavior is correct.

928 **Table 16** IPVC Fragmentation Test Methodology

- 929 [R58] The methodology **MUST** report the CoS Name of test packets used in this
930 methodology.
- 931 [R59] The methodology **MUST** report the length of test packets used for the test.
- 932 [R60] The methodology **MUST** report the IR_{SC} and T_{SC} used for the test.
- 933 [R61] The methodology **MUST** report the number of fragmented packets received.
- 934 [R62] The methodology **MUST** report pass or fail for the test.

935 **10.3.3 IPVC EP Configuration Tests**

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

941 **10.3.3.1 IPVC EP Prefix Mapping**

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

- 944 [R63] The IPVC EP Prefix Mapping Service Attribute **MUST** be verified as de-
945 scribed in Table 17.

946

Service Activation Test Methodology	
Test Name	IPVC EP Prefix Mapping
Test Type	Service Activation
Service Type	IPVC EP
Test Status	Mandatory when IPVC EP Prefix Mapping list in non-empty
Test Objective	Verify that the IPVC EP Prefix Mapping Service Attribute is configured correctly.
Test Procedure	<ul style="list-style-type: none"> • IPTE₁ offers IP Data Service packets with the DA for IPTE₂ at EI₁ at rate IR_{SC} for time T_{SC} using a SA for IPTE₁ that is not on the IPVC EP Prefix Mapping list. • IPTE₂ counts IP Data Service packets received at EI₂ from IPTE₁ for time T_{SC} and calculates PLR. • IPTE₁ then offers IP Data Service packets with the DA for IPTE₂ at EI₁ at rate IR_{SC} for time T_{SC} using a SA for IPTE₁ that is on the IPVC EP Prefix Mapping list. • IPTE₂ counts IP Data Service packets received at EI₂ from IPTE₁ for time T_{SC} and calculates PLR. • IPTE₂ then offers IP Data Service packets at EI₂ at rate IR_{SC} for time T_{SC} using a DA for IPTE₁ that is on the IPVC EP Prefix Mapping list. • IPTE₁ counts IP Data Service packets received at EI₁ from IPTE₂ for time T_{SC} and calculates PLR. • IPTE₂ then offers IP Data Service packets at EI₂ at rate IR_{SC} for time T_{SC} using a DA for IPTE₁ that is not on the IPVC EP Prefix Mapping list. • IPTE₁ counts IP Data Service packets received at EI₁ from IPTE₂ for time T_{SC} and calculates PLR.
Variables	IR _{SC} , T _{SC} , PLR _{SAC} , SA, DA
Results	Pass = From IPTE ₁ to IPTE ₂ with SA not in list PLR = 100% From IPTE ₁ to IPTE ₂ with SA in list $PLR \geq PLR_{SAC}$

	<p>From IPTE₂ to IPTE₁ with DA in list PLR $\geq PLR_{SAC}$</p> <p>From IPTE₂ to IPTE₁ with DA not in list PLR = 100%</p> <p>Fail = From IPTE₁ to IPTE₂ with SA not in list PLR < 100%</p> <p>From IPTE₁ to IPTE₂ with SA in list PLR $\geq PLR_{SAC}$</p> <p>From IPTE₂ to IPTE₁ with DA in list PLR $\geq PLR_{SAC}$</p> <p>From IPTE₂ to IPTE₁ with DA not in list PLR < 100%</p>
Remarks	

947 **Table 17** IPVC EP Profile Mapping Test Methodology

- 948 [R64] The methodology **MUST** report the CoS Name of test packets used in this
- 949 methodology.
- 950 [R65] The methodology **MUST** report the length of test packets used for the test.
- 951 [R66] The methodology **MUST** report the IR_{SC} and T_{SC} used for the test.
- 952 [R67] The methodology **MUST** report the SA and/or DA used for each step.
- 953 [R68] The methodology **MUST** report the number of packets received and the PL.
- 954 [R69] The methodology **MUST** report pass or fail for the test.

955 **10.3.3.2 IPVC EP Ingress BWP Envelope**

956 There are three tests that are performed to verify the IPVC EP Ingress BWP Envelope. The ag-
 957 gregate bandwidth of all flows within the envelope is tested, the bandwidth of each flow within
 958 the envelope is tested, the bandwidth of each flow simultaneously is tested. The test methodolo-
 959 gy for each of these is shown in the following sections.

960 **10.3.3.2.1 IPVC EP Ingress BWP Envelope Aggregate Methodology**

961 The correct configuration of the aggregate of all flows within the IPVC EP Ingress BWP Enve-
 962 lope attribute is verified with this test methodology.

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

965

Service Activation Test Methodology	
Test Name	IPVC EP Ingress BWP Envelope aggregate
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory if IPVC EP Ingress BWP Envelope not <i>None</i>
Test Objective	Verify that the IPVC EP Ingress BWP Envelope aggregate attribute is configured correctly.
Test Procedure	<ul style="list-style-type: none"> • IPTE₁ offers IP Data Service packets with the DA of IPTE₂ and a rate equal to $MaxIR_E$ for a time T_{SC} at EI₁ in accordance with the service description. • IPTE₂ counts the number of IP Data Service packets received at EI₂ determining the PL and measuring the PLR. Packet loss is acceptable up to PLR_{SAC}.
Variables	$DA, MaxIR_E, T_{SC}, PL, PLR_{SAC}$
Results	Pass = Packet loss is within PLR_{SAC} Fail = Packet loss is not within PLR_{SAC}
Remarks	<ol style="list-style-type: none"> 1. Ingress BWP Envelope test includes total aggregate information rate of traffic across all BWP Flows in the Envelope.

966

Table 18 IPVC Ingress BWP Envelope Aggregate Test Methodology

967

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

968

969

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

970

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

971

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

972

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

973

10.3.3.2.2 IPVC EP Ingress BWP Envelope per Flow

974

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

975

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

978

Service Activation Test Methodology	
Test Name	IPVC EP Ingress BWP Envelope per Flow
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory if IPVC EP Ingress BWP Envelope not <i>None</i>
Test Objective	Verify that the IPVC EP Ingress BWP Envelope attribute is configured correctly for each flow within the Envelope.
Test Procedure	<ul style="list-style-type: none"> • IPTE₁ offers IP Data Service packets with the DA of IPTE₂, a CoS marking equal to the IPVC EP Ingress Class of Service Map for the flow, a rate equal to $MaxIR_i$ for a time T_{SC} at EI₁ in accordance with the service description. • IPTE₂ counts the number of IP Data Service packets received at EI₂ determining the PL and measuring the PLR. Packet loss is acceptable up to PLR_{SAC}. • This is repeated for flows 1..n in the envelope.
Variables	DA, CoS Map, $MaxIR_i$, T_{SC} , PL, PLR_{SAC}
Results	Pass = Packet loss is within PLR_{SAC} Fail = Packet loss is not within PLR_{SAC}
Remarks	<ol style="list-style-type: none"> 1. A failure of any flow in the envelope represents a failure of all flows in the envelope.

979 **Table 19** IPVC Ingress BWP Envelope per Flow Test Methodology

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

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

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

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

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

986 10.3.3.2.3 IPVC EP Ingress BWP Envelope All Flows Simultaneously

987 The correct configuration of all flows simultaneously within the IPVC EP Ingress BWP Enve-
 988 lope is verified using this test methodology.

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

991

Service Activation Test Methodology	
Test Name	IPVC EP Ingress BWP Envelope all Flows simultaneously
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory if IPVC EP Ingress BWP Envelope not <i>None</i>
Test Objective	Verify that the IPVC EP Ingress BWP Envelope attribute is configured correctly for all flows within the Envelope.
Test Procedure	<ul style="list-style-type: none"> • IPTE₁ offers IP Data Service packets with the DA of IPTE₂, a CoS marking equal to the IPVC EP Ingress Class of Service Map for each flow within the envelope simultaneously, a rate equal to <i>MaxIR_i</i> for each flow, for a time <i>T_{SC}</i> at EI₁ in accordance with the service description. • IPTE₂ counts the number of IP Data Service packets received at EI₂ for each flow within the envelope determining the PL and calculating the <i>PLR</i>. Packet loss is acceptable up to <i>PLR_{SAC}</i>.
Variables	DA, CoS Map, <i>MaxIR_i</i> , <i>T_{SC}</i> , PL, <i>PLR_{SAC}</i>
Results	Pass = Packet loss is within <i>PLR_{SAC}</i> Fail = Packet loss is not within <i>PLR_{SAC}</i>
Remarks	<ol style="list-style-type: none"> 1. A failure of any flow in the envelope represents a failure of all flows in the envelope.

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

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

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

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

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

998 [R87] The methodology **MUST** report pass or fail for the test.
999

1000 **10.3.3.3 IPVC EP Egress BWP Envelope**

1001 There are three tests that are performed to verify the IPVC EP Egress BWP Envelope. The ag-
1002 gregate bandwidth of all flows within the envelope is tested, the bandwidth of each flow within
1003 the envelope is tested, the bandwidth of each flow simultaneously is tested. The test methodolo-
1004 gy for each of these is shown in the following sections.

1005 **10.3.3.3.1 IPVC EP Egress BWP Envelope Aggregate Methodology**

1006 The correct configuration of the aggregate of all flows within the IPVC EP Egress BWP Enve-
1007 lope attribute is verified with this test methodology.

1008 [R88] The aggregate of all flows within the IPVC EP Egress BWP Envelope attrib-
1009 ute **MUST** be verified as described in Table 21.

1010

Service Activation Test Methodology	
Test Name	IPVC EP Egress BWP Envelope aggregate
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory if IPVC EP Egress BWP Envelope not <i>None</i>
Test Objective	Verify that the IPVC EP Egress BWP Envelope aggregate attribute is configured correctly.
Test Procedure	<ul style="list-style-type: none"> • IPTE₂ offers IP Data Service packets with the DA of IPTE₁ and a rate equal to $MaxIR_E$ for a time T_{SC} at EI₂ in accordance with the service description. • IPTE₁ counts the number of IP Data Service packets received at EI₁ determining the PL and measuring the PLR_{SAC}. Packet loss is acceptable up to PLR_{SAC}.
Variables	$DA, MaxIR_E, T_{SC}, PL, PLR_{SAC}$
Results	Pass = Packet loss is within PLR_{SAC}

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

1011 **Table 21** IPVC Egress BWP Envelope Aggregate Test Methodology

1012 [R89] The methodology **MUST** report the CoS Name of test packets used in this
1013 methodology.

1014 [R90] The methodology **MUST** report the length of test packets used for the test.

1015 [R91] The methodology **MUST** report the $MAXIR_E$ and T_{SC} used for the test.

1016 [R92] The methodology **MUST** report the PL.

1017 [R93] The methodology **MUST** report pass or fail for the test.

1018 10.3.3.3.2 IPVC EP Egress BWP Envelope per Flow

1019 The correct configuration of each flow within the IPVC EP Egress BWP Envelope is verified
1020 using this test methodology.

1021 [R94] Each flow within the IPVC EP Egress BWP Envelope **MUST** be verified as
1022 described in Table 22.

1023

Service Activation Test Methodology	
Test Name	IPVC EP Egress BWP Envelope per Flow
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory if IPVC EP Egress BWP Envelope not <i>None</i>
Test Objective	Verify that the IPVC EP Egress BWP Envelope attribute is configured correctly for each flow within the Envelope.
Test Procedure	<ul style="list-style-type: none"> • IPTE₂ offers IP Data Service packets with the DA of IPTE₁, a CoS marking equal to the IPVC EP Ingress Class of Service Map for the flow, a rate equal to $MaxIR_i$ for a time equal to T_{SC} at EI₂ in accordance with the service description. • IPTE₁ counts the number of IP Data Service packets received at EI₁ determining the PL and measuring the PLR_{SAC}. Packet loss is acceptable up to PLR_{SAC}.

	<ul style="list-style-type: none"> This is repeated for flows 1..n in the envelope.
Variables	DA, CoS Map, $MaxIR_E$, T_{SC} , PL, PLR_{SAC}
Results	Pass = Packet loss is within PLR_{SAC} Fail = Packet loss is not within PLR_{SAC}
Remarks	<ol style="list-style-type: none"> A failure of any flow in the envelope represents a failure of all flows in the envelope.

Table 22 IPVC Egress BWP Envelope per Flow Test Methodology

- 1024
- 1025 [R95] The methodology **MUST** report the CoS Name of test packets used in this
- 1026 methodology.
- 1027 [R96] The methodology **MUST** report the length of test packets used for the test.
- 1028 [R97] The methodology **MUST** report the $MAXIR_i$ and T_{SC} used for the test.
- 1029 [R98] The methodology **MUST** report the PL.
- 1030 [R99] The methodology **MUST** report pass or fail for the test.

1031 10.3.3.3.3 IPVC EP Egress BWP Envelope All Flows Simultaneously

1032 The correct configuration of all flows simultaneously within the IPVC EP Egress BWP Envelope

1033 is verified using this test methodology.

- 1034 [R100] All flows within the IPVC EP Egress BWP Envelope **MUST** be verified sim-
- 1035 ultaneously as described in Table 23

Service Activation Test Methodology	
Test Name	IPVC EP Egress BWP Envelope all Flows simultaneously
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory if IPVC EP Egress BWP Envelope not <i>None</i>
Test Objective	Verify that the IPVC EP Egress BWP Envelope attribute is configured correctly for all flows within the Envelope.
Test Procedure	<ul style="list-style-type: none"> IPTE₂ offers IP Data Service packets with the DA of IPTE₁, a CoS marking equal to the IPVC EP Egress Class of Service Map

	<p>for each flow within the envelope simultaneously, a rate equal to $MaxIR_i$ for each flow, for a time T_{SC} at EI₂ in accordance with the service description.</p> <ul style="list-style-type: none"> • IPTE₁ counts the number of IP Data Service packets received at EI₁ for each flow within the envelope determining the PL and calculating the <i>PLR</i>. Packet loss is acceptable up to PLR_{SAC}.
Variables	DA, CoS Map, $MaxIR_i$, T_{SC} , PL, PLR_{SAC}
Results	<p>Pass = Packet loss is within PLR_{SAC}</p> <p>Fail = Packet loss is not within PLR_{SAC}</p>
Remarks	<p>1. A failure of any flow in the envelope represents a failure of all flows in the envelope.</p>

1037 **Table 23** IPVC Egress BWP Envelope for all Flows within the Envelope Test Methodology

- 1038 [R101] The methodology **MUST** report the CoS Name of test packets used in this
- 1039 methodology.
- 1040 [R102] The methodology **MUST** report the length of test packets used for the test.
- 1041 [R103] The methodology **MUST** report the $MAXIR_i$ and T_{SC} used for the test.
- 1042 [R104] The methodology **MUST** report the PL.
- 1043 [R105] The methodology **MUST** report pass or fail for the test.

1044 **10.4 Service Performance Tests**

1045 Service performance tests are used to ensure that the service meets performance expectations of

1046 the Subscriber. Service performance tests measure percentile of PD, MPD, IPDV, PDR, and

1047 PLR. To perform these measurements an IPTE generates and/or receives test packets.

1048 Timestamps within the packets are used to perform delay measurements and the count of packets

1049 is used to determine IP Packet loss. There are several mechanisms that can be used to measure

1050 delay and loss. Examples are TWAMP Light, STAMP, and TWAMP. Other methods are also

1051 acceptable. To calculate one-way Packet Delay Percentile or Mean Packet Delay, either Time of

1052 Day synchronization between the two IPTEs is supported (in which case one-way measurements

1053 can be used), or two-way measurements are taken and divided in half to approximate the one-

1054 way packet delay. If two-way measurements are divided in half, this is indicated in the report.

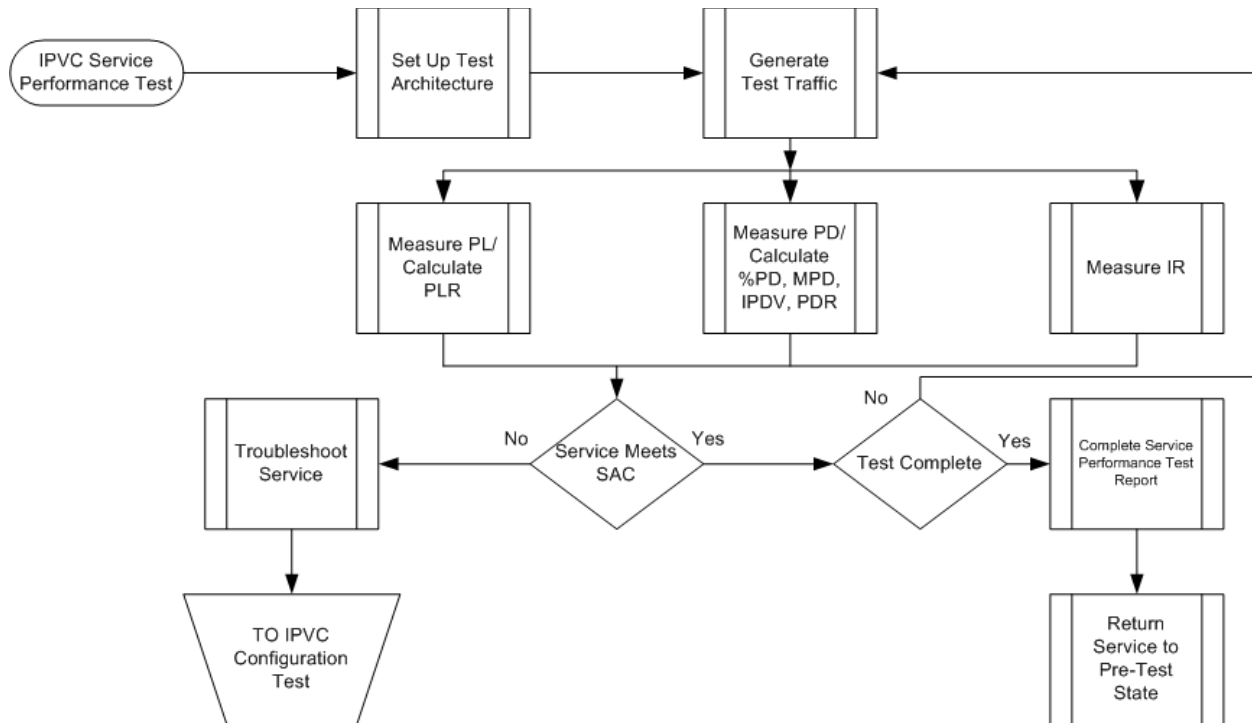


Figure 25 Service Performance Flow

1055
1056
1057 **10.4.1 Service Performance Test Duration**

1058 As discussed previously, the duration of the service performance test is significantly longer than
1059 the service configuration tests. To approximate the expected performance of the service, a long-
1060 ger test is required. There are three recommended test durations, 15 minutes, 2 hours, or 24 hours.

1061 **[D5]** The Service Provider **SHOULD** support at least one of these test durations.

1062 The duration of the performance test is agreed to between the Service Provider and the Subscrib-
1063 er.

1064 **[R106]** The Service Performance test duration **MUST** be agreed to by the Service
1065 Provider and Subscriber from one of the three test durations above.

1066 **10.4.2 Service Performance Service Loss and Delay**

1067 When an IPVC is being activated, the performance of each CoS Name applicable to the IPVC is
1068 tested one CoS Name at a time between each set of IPVC EPs in the IPVC. The test methodolo-
1069 gy in Table 24 is used to perform loss and delay measurements between each set of IPVC EPs.

1070 **[R107]** The loss and delay performance of each set of IPVC EPs in a new IPVC
1071 **MUST** be verified as specified in Table 24.

1072

Service Activation Test Methodology

Test Name	Service Performance Loss and Delay
Test Type	Service Activation
Service Type	IPVC
Test Status	Mandatory for new IPVC, Mandatory for new IPVC EP
Test Objective	Verify that the IPVC performance meets the SAC.
Test Procedure	<ul style="list-style-type: none"> • Packet length can be any single length or multiple lengths as specified in the IMIX pattern shown in section 10.1.1. • IPTE₁ offers packets with the DA of IPTE₂ at a constant rate equal to $MaxIR_i$ for the Bandwidth Profile Flow that the CoS Name and IPVC is mapped to for time T_{SP}. • IPTE₂ counts the packets received and transmitted. It measures the received IR_{MEAS}, PL_{MEAS}, and PD_{MEAS}. IPTE₂ calculates the MPD_{MEAS}, $IPDV_{MEAS}$ and/or PDR_{MEAS} from PD_{MEAS} and PLR_{MEAS} from PL_{MEAS}. • Simultaneously, IPTE₂ offers packets with the DA of IPTE₁ at a constant rate equal to $MaxIR_i$ for the Bandwidth Profile Flow that the CoS Name and IPVC is mapped to for time T_{SP}. • IPTE₁ counts the packets received and transmitted. It measures the received IR_{MEAS}, PL_{MEAS}, and PD_{MEAS}. IPTE₁ calculates the MPD_{MEAS}, $IPDV_{MEAS}$ and/or PDR_{MEAS} from PD_{MEAS} and PLR_{MEAS} from PL_{MEAS}. • IR_{SAC}, PD_{SAC} and/or MPD_{SAC}, $IPDV_{SAC}$ and/or PDR_{SAC}, and PLR_{SAC} are the limits specified by SAC. • This process is repeated for each Bandwidth Profile Flow contained in the IPVC and for packets that are not mapped to a particular Bandwidth Profile Flow. • If the IR_{MEAS}, PLR_{MEAS}, PD_{MEAS} and/or MPD_{MEAS}, and $IPDV_{MEAS}$ and/or PDR_{MEAS} are within the limits of SAC for each flow and for packets not mapped to a particular Bandwidth Profile Flow at IPTE₁ and IPTE₂ the result is Pass.
Variables	Packet lengths, T_{SP} , IR_{SAC} , PD_{SAC} , MPD_{SAC} , $IPDV_{SAC}$, PDR_{SAC} , PLR_{SAC}
Results	Pass = All Bandwidth Profile Flows and packets not mapped to a particular Bandwidth Profile Flow have to meet IR_{SAC} , PD_{SAC} and/or MPD_{SAC} ,

	<p>$IPDV_{SAC}$ and/or PDR_{SAC}, and PLR_{SAC} for this test to pass.</p> <p>Fail = Any Bandwidth Profile Flow or packets not mapped to a particular Bandwidth Profile Flow fail to meet IR_{SAC}, PD_{SAC} and/or MPD_{SAC}, $IPDV_{SAC}$ and/or PDR_{SAC}, and PLR_{SAC} this test fails.</p>
Remarks	<p>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.</p>

1073 **Table 24** Service Performance Loss and Delay Test Methodology

- 1074 [R108] The methodology **MUST** report the CoS Name of test packets used in this
1075 methodology.
- 1076 [R109] The methodology **MUST** report the length of test packets used for the test.
- 1077 [R110] The methodology **MUST** report the $MAXIR_i$ and T_{SP} used for the test.
- 1078 [R111] The methodology **MUST** report the IR, PL, %PD, MPD, IPDV, PDR.
- 1079 [R112] The methodology **MUST** report pass or fail for the test.
1080

1081 **11 Results**

1082 After all tests have been completed a SAT record is created. The SAT record contains the attrib-
1083 ute and test result information described in section 9 and 10. The results from the different tests
1084 on a particular service are mapped into one SAT record for that service. The SAT record can be
1085 shared with the Subscriber and can be stored within Service Provider management systems. The
1086 format of the SAT record is not mandated by this document.

1087 **11.1 Monitoring Test**

1088 While a particular test is in progress, the ability to query the IPTE(s) for the status of the test is
1089 needed. This does not include interim measurement results but does include the test status.

1090 [R113] An IPTE-TH, IPTE-A, or IPTE-I **MUST** allow a user or system to monitor
1091 the status of a test.

1092 An IPTE can support autonomous reporting of test status or can support retrieving the status of
1093 the test through queries by the Service Provider's support systems.

1094 **11.1.1 Test Report**

1095 The test report format is not defined within this document. The expectation is that the test report
1096 contains all the attributes specified in section 9 and 10. The Test Report can be provided to the
1097 Subscriber by the Service Provider or can be maintained by the Service Provider for future refer-
1098 ence. An example of the contents of a Test Report is shown in Appendix A.

1099 Editor's Note: Upon the completion of this document, additional work will be performed that
1100 will define the IP Services SAT Test Report format and Interface Profile Specification.
1101

1102 12 References

- 1103 [1] BBF TR-143, *Enabling Network Throughput Performance Tests and Statistical Moni-*
1104 *toring*, May 2008
- 1105 [2] IEEE Std 1003.1-2017, *Draft Standard for Information Technology – Portable Operat-*
1106 *ing System Interface (POSIX)*, 2017
- 1107 [3] IETF RFC 791, *Internet Protocol DARPA Internet Program Protocol Specification*,
1108 September 1981
- 1109 [4] IETF RFC 792, *Internet Control Message Protocol, DARPA Internet Program Protocol*
1110 *Specification*, September 1981
- 1111 [5] IETF RFC 2131, *Dynamic Host Configuration Protocol*, March 1997
- 1112 [6] IETF RFC 2474, *Definition of Differentiated Service Field (DS)*, December 1998
- 1113 [7] IETF RFC 2544, *Benchmarking Methodology for Network Interconnect Devices*, March
1114 1999
- 1115 [8] IETF RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*, February 2006
- 1116 [9] IETF RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and*
1117 *IPv6*, March 2010
- 1118 [10] IETF RFC 5880, *Bidirectional Forwarding Detection (BFD)*, June 2010
- 1119 [11] IETF RFC 6349, *Framework for TCP Throughput Testing*, August 2011
- 1120 [12] IETF RFC 6985, *IMIX Genome: Specification of Variable Packet Sizes for Additional*
1121 *Testing*, July 2013
- 1122 [13] IETF RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*, July 2017
- 1123 [14] International Standards Organisation ISO/IEC 7498-1, *Information Technology – Open*
1124 *Systems Interconnection – Basic Reference Model: The Basic Model*, November 1994
- 1125 [15] ITU-T Recommendation Y.1540, *Internet protocol data communication service – IP IP*
1126 *Packet transfer and availability performance*, July 2016
- 1127 [16] ITU-T Recommendation Y.1541, *Network performance objectives for IP-based ser-*
1128 *vices*, December 2011
- 1129 [17] ITU-T Recommendation Y.1541 Amendment 1, *New Appendix XII – Considerations*
1130 *for low speed access networks*, December 2013
- 1131 [18] ITU-T Recommendation Y.1542, *Framework for achieving end-to-end IP performance*
1132 *objectives*, June 2010

- 1133 [19] ITU-T Recommendation Y.1544, *Multicast IP performance parameters*, July 2008
- 1134 [20] ITU-T Recommendation Y.1560, *Parameters for TCP connection performance in the*
1135 *presence of middleboxes*, September 2003
- 1136 [21] ITU-T Recommendation Y.1564, *Ethernet service activation test methodology*, Febru-
1137 *ary* 2016
- 1138 [22] MEF 10.3, *Ethernet Services Attributes Phase 3*, October 2013
- 1139 [23] MEF 48/48.1, *Carrier Ethernet Service Activation Testing Phases 1 and 2*,
- 1140 [24] MEF 61, *IP Service Attributes for Subscriber IP Services*, January 2018
- 1141 [25] MEF z.a, *Service OAM for IP Services*, April 2018
1142

1143 **Appendix A Test Report Content Example**

1144 An example of the contents of a Test Report is shown in Table 25. This is shown as an example
 1145 only. Normative text in sections 9 and 10 are used to specify exactly what Service Attributes are
 1146 reported.

1147 *Editor Note 3: Should we keep this appendix in the document?*

1148

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



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



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



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

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

Attributes	Report Attribute	Comments
Packet Loss Ratio	IR	
	IR _{SAC}	
	PLR _{SAC}	

1149

1150

1151

Table 25 Test Report Contents

1152 **Appendix B Information Rate Comparison**

1153 This appendix provides a comparison of the Information Rate (IR) between Layer 1 (L1), Layer
1154 2 (L2), and Layer 3 (L3). For the purposes of this document L2 is assumed to be Ethernet and
1155 L3 is assumed to be IP.

1156 *Editor Note 4: This appendix will be provided in the next release of this document.*