Draft Standard
MEF 90.2 Draft (R2)

SD-WAN Certification Phase 2 Cases and Requirements Cases and Requirements

January 2024

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

Disclaimer

This draft document represents MEF work in progress; it has not achieved full MEF standardization and is subject to change. Changes are likely before this becomes a fully endorsed MEF Standard. The reader is strongly encouraged to keep this in mind and review the Release Notes (if applicable) 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.

Disclaimer

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

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

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

a) Any express or implied license or right to or under any patent, copyright, trademark, or trade secret rights held or claimed by any MEF member which are or may be associated with the ideas, techniques, concepts, or expressions contained herein; nor
b) any warranty or representation that any MEF members will announce any product(s) and/or service(s) related to it, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor
c) any form of relationship between any MEF member and the recipient or user of this document.

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

Table of Contents

List of Figures

List of Tables

1 List of Contributing Members

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

Editor Note 1: *This list will be finalized before Letter Ballot. Any member that comments in at least one CfC is eligible to be included by opting in before the Letter Ballot is initiated. Note that the MEF member listed here (typically a company or organization) different from their representative.*

- ABC Networks
- XYZ Communications

2 Abstract

This document defines the test cases and requirements for SD-WAN certification. The certification includes a test methodology that is not limited to just the Service Attributes that are defined in MEF 70.1 [4] but also describes test cases for Routing and Access Control, UCS Impairment, SWVC Performance, and SWVC Stability and Reliability. Included in certification are both conformance with MEF 70.1 [4] and ratings on the test cases defined. This certification aims to inform enterprise customers which SD-WAN Service Providers and SD-WAN Edge Vendor solution Vendors are the most highly rated.

3 Release Notes

This document is currently out for Call for Comments Ballot number 3 and the contents of this document are subject to change based on comments received. All comments from Call for Comments Ballot 2 have been discussed and resolved.

4 Terminology and Abbreviations

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

In addition, terms defined in MEF 70.1 [4] are included in this document by reference and are not repeated in the table below.

Term	Definition	Reference
Conformant	Compatible with appropriate settings.	This document
Mean Opinion Score	The mean of opinion scores	ITU-T P.10/G.100 [3]
Non-Conformant	Not compatible with appropriate settings.	This document

Table 1 – Terminology

Abbreviation	Definition	Reference
CI/CD	Continuous Integration/Continuous Deployment	This document
CMS	Centralized Management System	This document
DIA	Direct Internet Access	This document
DNS	Domain Name Service	
FTP	File Transfer Protocol	
HA	High Availability	This document
HTTP	Hypertext Transfer Protocol	
HTTPS	Hypertext Transfer Protocol Secure	
IMAP	Internet Message Access Protocol	
IPsec	Internet Protocol Security	
LDAP	Lightweight Directory Access Protocol	
MOS	Mean Opinion Score	ITU-T P.10/G.100 [3]
NetBIOS	Network Basic Input Output System	
NTP	Network Time Protocol	
POP3	Post Office Protocol 3	
QoS	Quality of Service	This document
RADIUS	Remote Authentication Dial-In User Service	
RDP	Remote Desktop Protocol	
RTP	Real-time Transport Protocol	
RTCP	Real-time Transport Control Protocol	
RTSP	Real-Time Streaming Protocol	
SaaS	Software as a Service	This document
SCP	Secure Copy Protocol	
SFTP	Secure File Transfer Protocol	
SMB	Server Message Block Protocol	
SMTP	Simple Mail Transfer Protocol	

Abbreviation	Definition	Reference
SNMPV2	Simple Network Management Protocol version 2	
SSH	Secure Shell Protocol	
SSL	Secure Sockets Layer	
SYSLOG	System Logging Protocol	
TACACS+	Terminal Access Controller Access-Control System	
TFTP	Trivial File Transfer Protocol	
UDP	User Datagram Protocol	
VoIP	Voice over Internet Protocol	This document

Table 2 – Abbreviations

Editor Note 2: The terminology section will be updated in the next revision of this document.

5 Compliance Levels

The keywords "**MUST**," "**MUST NOT**," "**REQUIRED**," "**SHALL**," "**SHALL NOT**," "**SHOULD**," "**SHOULD NOT**," "**RECOMMENDED**," "**NOT RECOMMENDED**," "**MAY**," and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 (RFC 2119 [1], RFC 8174 [2]) when, and only when, they appear in all capitals, as shown here. All keywords must be in bold text.

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

Editor Note 3: The following paragraph will be deleted if no conditional requirements are used in the document.

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

6 Numerical Prefix Conventions

Editor Note 4: This section will be deleted unless numerical prefixes are used in the document.

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

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

Table 3 – Numerical Prefix Conventions

7 Introduction

MEF's first certification phase was based solely on the Service Attributes defined in MEF 70. The certification was found lacking in functionality. Phase 2 of SD-WAN certification changes what is tested significantly. Instead of verifying support for SD-WAN Service Attributes defined in MEF 70.1 [4], additional testing areas have been added. These areas of testing include the following:

- Routing and Access Control (section 9)
- SWVC Performance (section 8)
- WAN Impairment of the SD-WAN SWVC (section 9)
- SWVC Stability and Reliability (section 11)

This document defines specific test cases, test attributes, and test processes for each area noted above.

Test cases cover topics such as simple and complex policy operation, Mean Opinion Score (MOS) for video and voice applications, dynamic path selection based on performance criteria, IP packet processing of the SWVC, and management of the SWVC and associated SD-WAN Edge Vendor solutions.

Test attributes are described within test cases. Test attributes might be the length of IP Packets for throughput measurements, the number of connections per second for HTTP capacity, specific Service Attributes from MEF 70.1 [4], or impairments used to test MOS or packet loss.

Test processes are the steps used to perform the test measurements within a test case. The requirements associated with each test processes associated with each test case are described in this document.

Two terms are used within this document that must be understood. These terms are SD-WAN Edge Vendor and SD-WAN Service Provider. An SD-WAN Edge Vendor describes a solution vendor that provides the SD-WAN solution, including SD-WAN Edge and Manager. An SD-WAN Service Provider uses solutions from SD-WAN Edge Vendors to provide SD-WAN Service as described in MEF 70.1 [4].

The certification testing defined within this document is intended to provide a rating from D (lowest) to AAA (highest). Ratings are determined based on the results of the test cases defined in this document. For example, an SD-WAN Edge Vendor solution implementation that processes 64 Byte IP Packets at full line rate may be rated higher than an SD-WAN Edge Vendor solution implementation that limits the 64 Byte IP Packets to less than line rate. Ratings are based on weighting applied to each section of the test requirements in this document.

After the completion of certification testing, an overall rating is provided. This overall rating of an SD-WAN Edge Vendor solution implementation can be used to compare the ability of different SD-WAN Edge Vendors to meet the test requirements and, therefore, the requirements of SD-

WAN Service Providers and enterprise customers. In the same manner, SD-WAN Service Provider’s offerings can be compared to determine how two offerings best meet the end customer’s requirements.

In addition to the ratings, there is a MEF Certification PASS/FAIL result. This determines the conformance to MEF specifications in the area of certification. The conformance is based on the testing of MEF 70.1 requirements shown in section 12. The percentage of tests that must pass is still under discussion, and this text will be updated once this discussion concludes.

The testing defined within this document is intended to be repeatable to cover new software releases, service configurations, or updates to how an SD-WAN Edge Vendor solution is managed. The use of Continuous Integration/Continuous Deployment (CI/CD) strategies for MEF certification is being defined for the first time. Repeating the certification process allows ratings to increase or decrease based on the performance of an SD-WAN Edge Vendor solution or SD-WAN service during continued testing. If a new software release breaks a critical function, this can be identified during repeated certification testing, and the rating adjusted accordingly. In the same way, if a new software release provides fixes for shortfalls identified in previous certification testing, the rating can be increased accordingly. Unless otherwise specified for a specific subtest, the SD-WAN solution will be deployed using the default policy or recommended settings available to the public at the time of testing. All vendors will be provided with specific details about configuration requirements.

7.1 SD-WAN Overview

MEF 70.1 [4] describes the characteristics of SD-WAN Service as follows:

- The Subscriber connects to the SD-WAN Service at an SD-WAN UNI.
- The basic unit of transport at the SD-WAN UNI is an IP Packet.
- The SD-WAN Service provides a layer 3 IP-routed network.
- Ingress IP Packets at the SD-WAN UNI are classified, based on the IP Packet contents, into Application Flows.
- The SD-WAN Service can use policy-based autonomous traffic management.
- The SD-WAN Service utilizes one or more Underlay Connectivity Services.
- Policies and IP forwarding constraints define SWVC topologies.
- An SD-WAN Service can offer encryption between SD-WAN Edge Vendor solutions.
- Policies can specify performance goals for each Application Flow.
- Forwarding of an Application Flow can be blocked at an SWVC End Point by Policy.

- Each Application Flow can, by Policy, be subject to a bandwidth commitment and limit. Application Flow Specification Group members share a single bandwidth commitment and limit.

- An SD-WAN Service typically provides a Subscriber web portal and/or API that exposes network health, performance, and application information. The portal/API may also allow the Subscriber to modify aspects of the SD-WAN service, such as defining Application Flow Specifications and creating/modifying Policies.

- An SD-WAN Service aligns with the concepts of MEF LSO principles, including Service Orchestration.

Per MEF 70.1 [4], an SD-WAN service is made up of the following logical components that have Service Attributes defined for them:

- SD-WAN Virtual Connection (SWVC)

- SD-WAN Virtual Connection End Point (SWVC End Point)

- SD-WAN UNI (in this document, UNI refers to an SD-WAN UNI, unless otherwise specified)

In addition, MEF 70.1 [4] describes four additional components that do not have Service Attributes defined for them:

- Subscriber Network (clearly, this is visible to the Subscriber)

- Service Provider Network

- Tunnel Virtual Connection (TVC)

- SD-WAN Edge Vendor solution

Components included in SD-WAN certification include the Service Provider Network, the TVC, and the SD-WAN Edge Vendor solution.

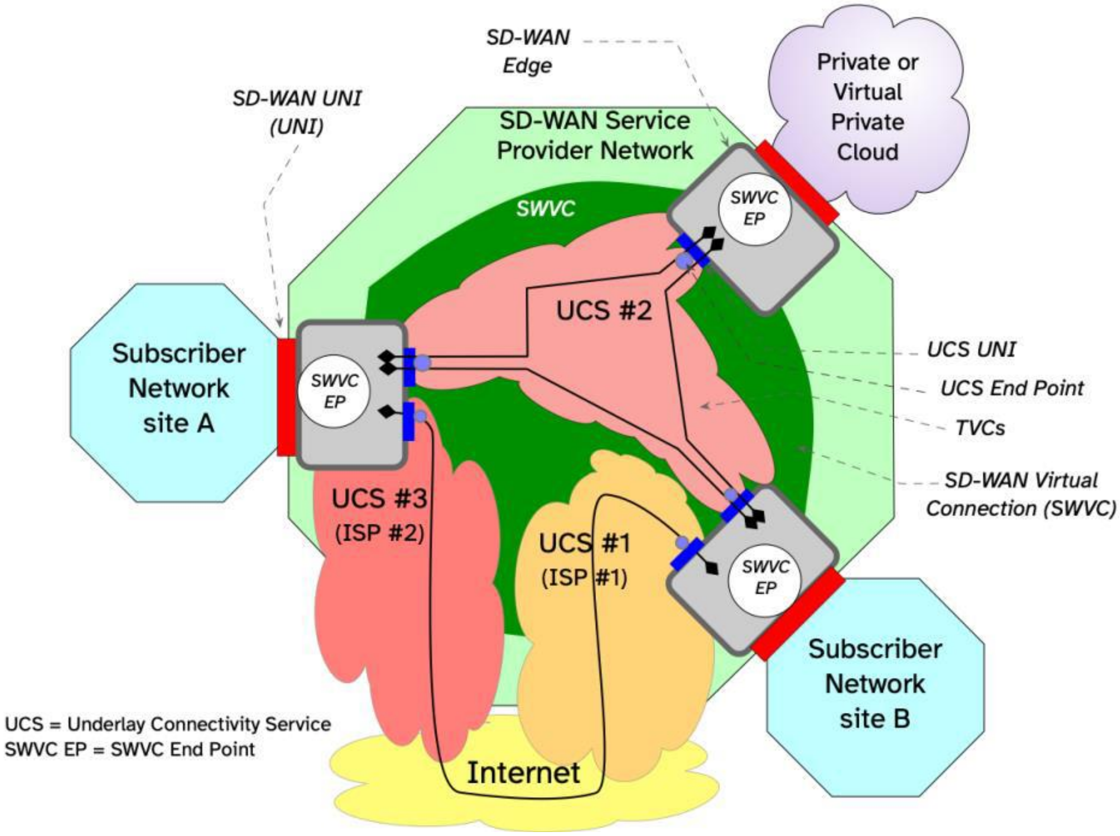
SD-WAN Edge
SD-WAN UNI (UNI)
SD-WAN Service Provider Network
Private or Virtual Private Cloud
SWVC
SWVC EP
UCS #2
Subscriber Network site A
SWVC EP
UCS UNI
UCS End Point
TVCs
SD-WAN Virtual Connection (SWVC)
UCS #3 (ISP #2)
UCS #1 (ISP #1)
SWVC EP
Subscriber Network site B
UCS = Underlay Connectivity Service
SWVC EP = SWVC End Point
Internet

Figure 1 – Example of SD-WAN Service as defined in MEF 70.1

Figure 1 provides a detailed view of an SD-WAN Service, including the SD-WAN UNIs, the SD-WAN Edge Vendor, the UCSs, UCS End Points, and UCS UNIs, an SP SD-WAN Service solution and SWVC End Points, the TVCs and the use of the Internet to connect the SD-WAN Edges. These are all detailed in MEF 70.1 [4].

7.2 Certification Testing Topology

The SD-WAN Test Architecture is shown in **Figure 2**. This figure covers the location of SD-WAN Edge Vendor solutions, UCSs interconnecting the SD-WAN Edge Vendor solutions, the SD-WAN UNIs, and the test tools used to generate and collect IP Packets.

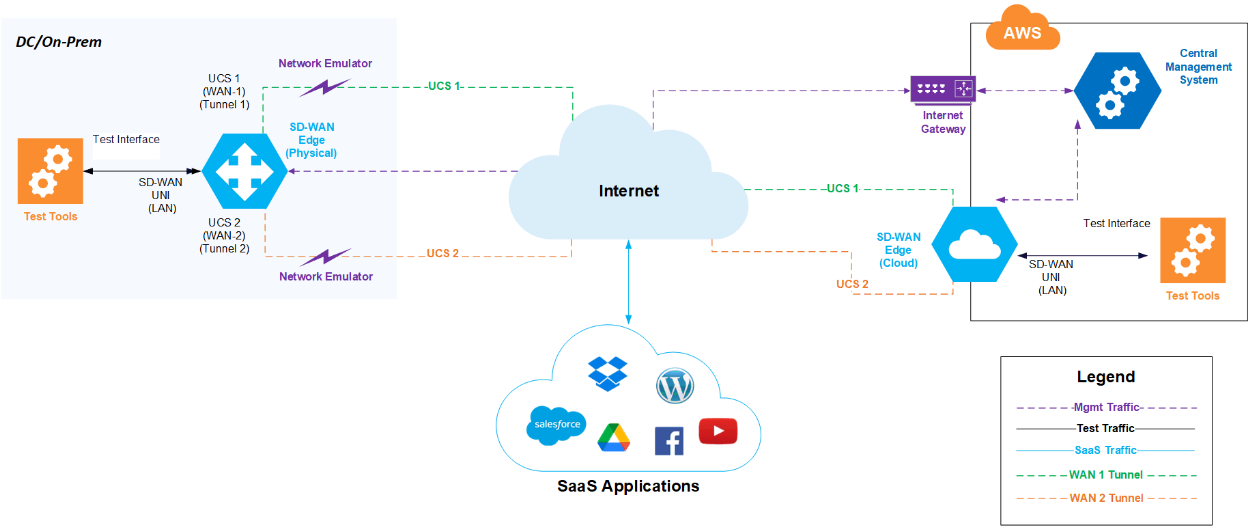

Figure 2 – SD-WAN Test Architecture for Virtual Edges

Figure 2 shows the testing for a cloud based SD-WAN solution. Methodologies that measure performance are not included in the testing for a cloud based SD-WAN solution.

The topology shown in **Figure 3** includes the HQ DC (On-Prem) location and an SD-WAN Edge Vendor solution in a public cloud. The UCSs have behavioral characteristics like those typically encountered over UCS links. The test harness baseline is recorded to ensure consistent behavior, then the vendor solution is deployed, and each test case is measured against the baseline.

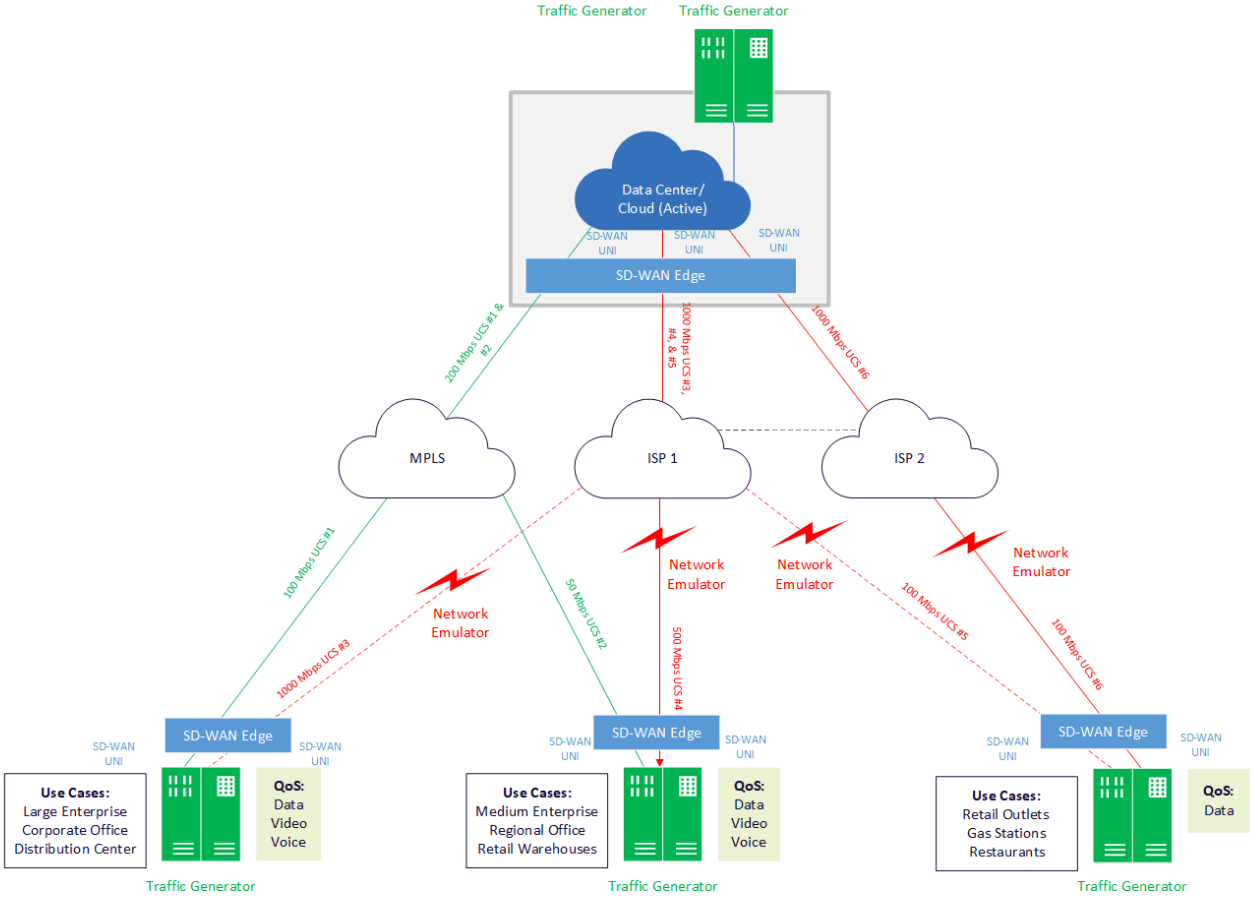

Figure 3 – Topology of Multiple Use Case Test Environment for SD-WAN

7.3 SD-WAN Edge Configuration for Testing

To enable a fair comparison between SD-WAN Edge configurations, each SD-WAN Edge Vendor will be asked to configure, as an example, their SD-WAN Edge to support the following:

- Allow Voice, Video, HTTP, SMTP, and FTP applications

Note: MEF 70.1 defines this as an Application Flow Specification and additional details on constraints placed on this can be found in that document.

- Prioritize Voice and Video traffic over HTTP, SMTP, and FTP

- Redirect traffic from one TVC (experiencing degradation or failure) to another TVC

7.4 What is Tested?

As indicated previously, what is tested goes beyond the requirements described in MEF 70.1 [6] to include the performance of SD-WAN Edges and SD-WAN Services. The below provides a view of areas that are tested:

- Routing and Access Control

- SWVC Performance
- UCS Impairment
- SWVC Stability and Reliability

Testing is performed based on a testing agreement. A testing agreement is completed between the tester (MEF/CR) and the Testee (SD-WAN Edge Vendor or SD-WAN Service Provider). It covers the scope of the testing. Implementations from a single vendor running one OS (e.g., VOS) on one type of processor (e.g., Intel) are all under one test agreement, regardless of the number of interfaces, speed of interfaces, etc., that a series of Vendor implementations support. Testing is accomplished via separate testing agreements if the vendor has more than one OS version and/or code base (e.g., Meraki^{TM} vs. Viptela^{TM} vs. iOS^{TM} or JunOS^{TM} vs. Linux^{TM}). If the vendor uses a different OS/code base when their SD-WAN Edge implementation is deployed on an ARM processor vs. an Intel Processor vs. custom silicon (e.g., a switch/router), there would be separate testing agreements.

If the SD-WAN Edge Vendor provides implementations of different sizes, the test configuration contains one of a small, medium, and large implementation.

For Service Providers, a testing agreement is required for each configuration offering they support. A Service Provider may have a single SD-WAN offering that uses a single SD-WAN Edge Vendor's solution. This requires a single testing agreement.

A single SD-WAN service offering from a Service Provider requires a single testing agreement.

A Service Provider may have multiple SD-WAN offerings, each that uses a different SD-WAN Edge Vendor. In this case, a test agreement is required for each offering.

When a Service Provider is being tested, the conditions are expected to be simulated in the test lab. This means there is an expectation of introducing the average One-way Packet Delay and Packet Loss seen within the Service Provider's network.

7.5 Policies Used for Testing

This document makes assumptions about the use of policies that define IP Packet forwarding. Policies can be default settings that pass IP Packets in a specific way, or they can be created to meet the requirements of a specific test case. In either case, it is expected that the SD-WAN Edge Vendor will provide the expertise required to create and assign any policies need to perform testing as described by a test case.

7.6 Testing, Ratings, and Certification

For each test case, a penalty may be assessed based on the SD-WAN Edge Vendor solution or SD-WAN Service Provider's ability to comply with the requirements of the test case. For Certification, conformance to requirements from MEF 70.1 [6] must be demonstrated through successful completion of the test case(s) used to verify conformance. The ratings and Certification is explained in detail in section 13.

8 SWVC Performance

The performance of the SWVC under test is measured by tests within this section of the document. All testing defined within this section is performed from the Headquarters to each Branch and from each Branch to the Headquarters.

8.1 Raw Packet Processing Performance

Test Objective: How much raw data can be transferred through the SD-WAN solution per second, and what are the associated latency and drop packet counts from each SD-WAN UNI at the Branches to the SD-WAN UNI at the Headquarters and from the Headquarters to each Branch.?

Test Process: This test uses User Datagram Protocol (UDP) packets of varying sizes generated by traffic generation appliances. A constant stream of the appropriate packet size—with variable source and destination IP addresses transmitting from a fixed source port to a fixed destination port—is transmitted through the underlay of the SWVC. Each packet contains dummy data and is targeted at a valid port on a valid IP address on the target subnet. Network monitoring tools verify the percentage load and frames per second figures across each SD-WAN UNI before each test begins. Multiple tests are run, and averages are taken where necessary.

This traffic does not attempt to simulate any form of real-world network condition. No TCP sessions are created during this test, and there is very little for the flow or policy engine to do. This test aims to determine the raw packet processing capability of the combination of each SD-WAN UNI and the SWVC. Frames are offered at the rate per second shown in **Table 4**, and the maximum number of Frames per second that pass without Packet Loss is recorded.

MEF 70.1 [6] requires that a Policy be assigned to an Application Flow at the ingress SD-WAN UNI. The test traffic needs to conform to a Policy created for this test so that the traffic can be forwarded to an egress SD-WAN UNI.

L2 Ethernet Frame Size (Bytes)	**L1 Ethernet Packet Overhead**			**L1 Ethernet Packet Size (Bytes)**	**L2 Ethernet Rate (Frames/Second)**
	Preamble (Bytes)	**Start Frame (Bytes)**	**Interpacket Gap (Bytes)**		
64	7	1	12	84	1,488,095
128	7	1	12	148	844,595
256	7	1	12	276	452,899
512	7	1	12	532	234, 962
1024	7	1	12	1044	119, 732
1280	7	1	12	1300	96,154
1400	7	1	12	1420	87,535

Table 4 – L2 Ethernet Frames per Second

Note: This testing is performed using encrypted TVCs. Performance is expected to be better using unencrypted TVCs.

8.1.1 64-Byte Packets

Maximum 1,488,095 frames per second per Gigabit of bandwidth. This test determines the ability of a device to process IP packets from the wire under the most challenging IP packet processing conditions.

[R1] The rate at which the SD-WAN Edge Vendor solution can process 64-byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

[R2] The rate at which the SP SD-WAN Service solution can process 64-byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

8.1.2 128-Byte Packets

Maximum 844,595 frames per second per Gigabit of bandwidth.

[R3] The rate at which the SD-WAN Edge Vendor solution can process 128-byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

[R4] The rate at which the SP SD-WAN Service solution can process 128128-byte Ethernet Frames per SD-WAN, UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

8.1.3 256-Byte Packets

Maximum 452,899 frames per second per Gigabit of bandwidth

[R5] The rate at which the SD-WAN Edge Vendor solution can process 256-byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

[R6] The rate at which the SP SD-WAN Service solution can process 256-byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

8.1.4 512-Byte Packets

Maximum 234,962 frames per second per Gigabit of bandwidth.

NoteL This test provides a reasonable indication of the ability of a device to process IP packets from the wire on an "average" network.

[R7] The rate at which the SD-WAN Edge Vendor solution can process 512-byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

[R8] The rate at which the SP SD-WAN Service solution can process 512-byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

8.1.5 1024-Byte Packets

Maximum 119,732 frames per second per Gigabit of bandwidth.

Note: Some chipsets need help with uncommon IP packet sizes. This test determines whether or not the SD-WAN handles uncommon IP packet sizes appropriately.

[R9] The rate at which the SD-WAN Edge Vendor solution can process 1024-byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

[R10] The rate at which the SP SD-WAN Service solution can process 1024-byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

8.1.6 1280-Byte Packets

Maximum 96,154 frames per second per Gigabit of bandwidth.

[R11] The rate at which the SD-WAN Edge Vendor solution can process 1280 byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

[R12] The rate at which the SP SD-WAN Service solution can process 1280 byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

8.1.7 1400-Byte Packets

Maximum 87,535 frames per second per Gigabit of bandwidth.

Note: This test has been included to demonstrate how easy it is to achieve good results using large IP packets. Readers should use caution when considering test results that only quote performance figures using similar IP packet sizes. 1400 Byte frames are used versus 1518 Byte frames to avoid fragmentation during this test.

[R13] The rate at which the SD-WAN Edge Vendor solution can process 1400 byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

[R14] The rate at which the SP SD-WAN Service solution can process 1400 byte Ethernet Frames per SD-WAN UNI, as shown in **Table 4** per Gigabit of bandwidth, **MUST** be measured.

8.2 Latency and Packet Loss Test

Test Objective: The test measures the values of the Mean One-way Packet Delay and Packet Loss Ratio under various load conditions through the SD-WAN Edge to determine the contribution of the SD-WAN Edge to Packet Delay and Packet Loss.

Test Process: Test traffic is passed across the SWVC and through all UCSs simultaneously. Packet loss and average latency are recorded for each IP packet size (64, 128, 256, 512, 1024, 1280, and 1400 bytes) at a load level of 90% of the maximum throughput with zero Packet Loss, as previously determined in section 8.1. All measurements are performed from SD-WAN UNI to SD-WAN UNI.

[R15] For each of the Frame sizes (64, 128, 256, 512, 1024, 1280, and 1400 Bytes) offered at 90% of the maximum throughput with zero Frame Loss, the One-way Mean Packet Delay over the UCSs connecting the SD-WAN Edge Vendor solutions in the test configuration **MUST** be measured for each UCS on the SD-WAN Edge Vendor solution.

[R16] For each of the Frame sizes (64, 128, 256, 512, 1024, 1280, and 1400 Bytes) offered at 90% of the maximum throughput with zero Frame Loss, the One-way Mean Packet Delay over the UCSs connecting the SD-WAN Edge Vendor solutions in the test configuration **MUST** be measured for each UCS in the SWVC.

8.3 Maximum Capacity of TCP and HTTP

These tests aim to stress the policy or inspection engine and determine how it handles maximum number of TCP connections per second, maximum number of HTTP sessions per second, maximum number of application layer transactions per second, and maximum concurrent open connections. All IP packets contain valid payload and address data.

Note that in all tests, the following critical “breaking points”—where the final measurements are taken—are used:

Note: This testing is performed using Application Flow Specifications and Policies that allow all packets to be passed. This can also be configured as Failed Open rather than Failed Closed. Failed Open is when the solution passes all packets in a failed state. Failed Closed is defined as a solution that does not pass any packets in a failed state.

It is understood that SD-WAN Edge Vendors often provide different sized solutions. For the purposes of this document, these are classified as Small, Medium, and Large. These are defined below.

Small –

Medium –

Large –

Editor Note 5: Values for the number of interfaces and CPU size are required for these definitions. Input on these is requested.

8.3.1 Theoretical Maximum Concurrent TCP Connections

Test Objective: How many simultaneous sessions does the SD-WAN solution support? This test is designed to determine the maximum concurrent TCP connections of the SD-WAN Service with no data passing across the connections. This type of traffic would not typically be found on a standard SD-WAN Service, but it provides the means to determine the maximum possible concurrent connections figure.

Test Process: An increasing number of Layer 4 TCP sessions are opened through the SD-WAN Service. Each session is opened normally and then held open for the duration of the test as additional sessions are added up to the maximum possible. The load is increased until no more connections can be established, and this number is recorded.

[R17] The maximum number of concurrent TCP connections for the TVCs over a given UCS on the SD-WAN Edge Vendor solution **MUST** be measured as described in section 8.3.1.

[R18] The maximum number of concurrent TCP connections for the TVCs over a given UCS in an SP SD-WAN Service solution **MUST** be measured as described in section 8.3.1.

8.3.2 Maximum TCP Connections per Second

Test Objective: What is the maximum TCP connection rate of the SD-WAN solution with a one-byte TCP response size? This test is designed to determine the maximum TCP connection rate of the SD-WAN Service with one byte of data passing across the connections. This type of traffic would not typically be found on a typical network, but it provides the means to determine the maximum possible TCP connection rate.

Test Process: An increasing number of new sessions are established through the SD-WAN Service and ramped slowly to determine the exact point of failure. Each session is opened normally, one byte of data is passed to the host, and the session is closed immediately. Load increases until one or more of the breaking points defined earlier is reached.

[R19] The maximum number of TCP connections per second for the TVCs over a given UCS on the SD-WAN Edge Vendor solution **MUST** be measured as described in section 8.3.2.

[R20] The maximum number of TCP connections per second for the TVCs over a given UCS in an SP SD-WAN Service solution **MUST** be measured as described in section 8.3.2.

8.3.3 Maximum HTTP Connections per Second

Test Objective: What is the maximum HTTP connection rate of the SD-WAN solution with a one-byte HTTP response size? This test is designed to determine the maximum TCP connection rate of the SD-WAN Service based on a payload of one-byte HTTP response size. The response size defines the number of bytes in the body, excluding any bytes associated with the HTTP header. A one-byte response size is designed to provide theoretical maximum HTTP connections per second rate.

Test Process: The client and server use HTTP 1.0 without keep-alive; the client will open a TCP connection, send one HTTP request, and close the connection. This ensures that all TCP connections are closed immediately upon the request being satisfied; thus, any concurrent TCP connections will be caused purely due to the delay the SD-WAN Service introduces on the network. Load increases until one or more of the breaking points defined earlier is reached. The number of open HTTP connections per second is retrieved and recorded.

Note: HTTP 1.0 is used because it only generates one request, whereas HTTP 1.1 generates several requests.

[R21] The maximum number of HTTP connections per second for the TVCs over a given UCS on the SD-WAN Edge Vendor solution **MUST** be measured as described in section 8.3.3.

[R22] The maximum number of HTTP connections per second for the TVCs over a given UCS in an SP SD-WAN Service solution **MUST** be measured as described in section 8.3.3.

8.3.4 Maximum HTTP Transactions per Second

Test Objective: What is the maximum HTTP transaction rate of the SD-WAN solution with a one-byte HTTP response size using 10 HTTP GET requests? This test is designed to determine the maximum HTTP transaction rate of the SWVC with a one-byte HTTP response size. The object size defines the number of bytes in the body, excluding any bytes associated with the HTTP header. A one-byte response size is designed to provide maximum theoretical connections per second rate.

Test Process: The client and server are using HTTP 1.1 with persistence, and the client will open a TCP connection, send 10 HTTP requests, and close the connection. This ensures that TCP connections remain open until all 10 HTTP transactions are complete, thus eliminating the maximum connection per second rate as a bottleneck (one TCP connection = 10 HTTP transactions). Load increases until one or more of the breaking points defined earlier is reached. The number of open HTTP connections per second is retrieved and recorded.

[R23] The maximum number of HTTP transactions per second for the TVCs over a given UCS on the SD-WAN Edge Vendor solution **MUST** be measured as described in section 8.3.4.

[R24] The maximum number of HTTP transactions per second for the TVCs over a given UCS in an SP SD-WAN Service solution **MUST** be measured as described in section 8.3.4.

8.4 HTTP Capacity

This test stresses the detection engine to see how the device copes with HTTP network loads of varying average IP packet size and connections per second. By creating session-based traffic with varying session lengths, the device is forced to track valid TCP sessions, ensuring a higher workload than simple IP packet-based background traffic. The HTTP test traffic characteristics are shown in **Table 5**.

Each transaction consists of a single HTTP GET request with no transaction delays (i.e., the web server responds immediately to all requests). All IP packets contain valid payload (a mix of binary and ASCII objects) and address data. This test provides an excellent representation of a live network (albeit one biased towards HTTP traffic) at various network loads.

Connections per Second (per Gigabit)	**HTML Response Size (Bytes)**	**Total Response Size (Bytes)**
1,000	115,570	129,738
2,000	57,388	64,834
4,000	28,048	32,136
8,000	13,512	15,920
16,000	6,353	7,916
32,000	2,667	3,903

Table 5 – HTTP Test Traffic Characteristics

8.4.1 HTTP Connections per Second

Test Objective: How many HTTP connections can the SD-WAN solution process, and how does the size of what is being transferred impact performance?

Test Process: Maximum new connections per second per Gigabit traffic with corresponding HTML response. Connections per second are measured with 1000, 2000, 4000, 8000, 16,000, and 32,000 new connections being started per second.

Note: This test methodology requires that a policy that allows all IP Packets to pass over the test Application Flow Specification be used to perform the measurements,

[R25] The maximum number of HTTP connections per second for a SD-WAN UNI on the SD-WAN Edge Vendor solution **MUST** be measured as described in section 8.4.1.

[R26] The maximum number of HTTP connections per second for each SD-WAN UNI in an SP SD-WAN Service solution **MUST** be measured as described in section 8.4.1.

8.5 Application Average Response Time: HTTP

Test traffic is passed across the infrastructure switches and through all inline port pairs of the SWVC simultaneously (the latency of the basic infrastructure is known and is constant throughout the tests). The results are recorded at each HTML response size, as shown in Figure 4, at a load level of 95% of the maximum throughput with zero IP packet loss.

8.6 HTTPS Capacity

These tests aim to determine the performance curve and identify potential bottlenecks. The HTTPS detection engine is stressed to see how the device copes with network loads of varying average IP packet size and varying connections per second. By creating session-based traffic with varying session lengths, the device is forced to track valid TCP sessions, ensuring a higher workload for simple IP packet-based background traffic.

Each transaction consists of a single HTTP(S) GET request with no transaction delays (i.e., the web server responds immediately to all requests). All IP packets contain a valid payload (a mix of binary and ASCII objects) and address data.

Table 6 shows the two cipher suites that are used for testing. The suites are the two most popular across the Internet.

Protocol	Cipher Suite Description	(Value)	Frequency Ranking	Security Classification
TLS 1.3	TLS_AES_256_GCM_SHA384	(0x13,0x02)	1	Recommended
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	(0xC0, 0x30)	2	Secure

Table 6 – Cipher Suites

8.6.1 HTTPS Connections per Second

Test Objective: How many HTTPS connections can the SD-WAN solution process, and how do the cipher suite use and the size of what is being transferred impact performance. This test does cannot use an allow all policy. HTTPS packets are to be inspected.

Test Process: A maximum number of new connections per second per Gigabit traffic with corresponding HTTP response. Connections per second are measured with 1000, 2000, 4000, 8000, 16,000, and 32,000 new connections being started per second. Each Cipher suite is tested as shown in **Table 7** and **Table 8**.

TLS_AES_256_GCM_SHA384 (0x13, 0x02)		
Connections per Second (per Gigabit)	**HTML Response Size (bytes)**	**Total Response Size (bytes)**
1,000	113,340	127,666
2,000	54,917	62,455
4,000	25,700	29,710
8,000	11,170	13,483
16,000	3,870	5,358
32,000	150	1,227

Table 7 – Cipher Suite (0x13, 0x02)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30)		
Connections per Second (per Gigabit)	**HTML Response Size (bytes)**	**Total Response Size (bytes)**
1,000	115,000	129,360
2,000	56,257	62,945
4,000	26,970	31,047
8,000	12,394	14,808
16,000	5,047	6,738
32,000	1,365	2,605

Table 8 – Cipher Suite (0xC0, 0x30)

[R27] The maximum number of HTTPS connections per second for a SD-WAN UNI on the SD-WAN Edge Vendor solution **MUST** be measured as described in section 8.6.1

8.7 Application Average Application Response Time: HTTPS

Test Objective: This test measures the average application response time for HTTPS not the user response time.

Test Process: Test traffic is passed across the SWVC and through the SD-WAN Edge Vendor solution(s) simultaneously (the latency of the primary virtual infrastructure is known and is constant throughout the tests). The results are recorded at each response size (length of IP Packets) at a load level of 90% of the maximum throughput with zero packet loss, as previously determined in section 8.6.

[R28] The average response time of HTTPS connections for each UCS on the SD-WAN Edge Vendor solution **MUST** be measured as described in section 8.7.

[R29] The average response time of HTTPS connections for each UCS in an SP SD-WAN Service solution **MUST** be measured as described in section 8.7.

8.8 File download/copy time/speed

Test Objective: How quickly can files be downloaded, and how does the size of what is being downloaded impact performance?

Test Process: Files from each of the following types are downloaded from the Internet to a local folder:

- MS Word files
- MS Excel files
- PDFs
- Zipped files/folders

This test is performed directly over the Internet without an SD-WAN Edge solution in the test path to establish a baseline. The SD-WAN Edge solution is then deployed, Internet Breakout is configured on the SD-WAN Edge solution, and measurements are performed simultaneously on the baseline and SD-WAN Edge solution over multiple days/weeks so that thousands of data points are collected. Outliers are discarded from these results. Thus, the results are relative to the baseline. The net increase in time to copy clean files of various sizes is determined, i.e., the time difference between copying files without an SD-WAN Edge and with an SD-WAN Edge.

8.8.1 Microsoft OneDrive

8.8.1.1 Net increase in time to copy clean file – 100KB

This test measures the net increase in time to copy a 100KB file.

[R30] The test **MUST** measure the net increase in time to copy a 100KB file for an SD-WAN Edge Vendor solution.

[R31] The test **MUST** measure the net increase in time to copy a 100KB file for an SP SD-WAN Service solution.

8.8.1.2 Net increase in time to copy clean file – 1MB

This test measures the net increase in time to copy a 1MB file.

[R32] The test **MUST** measure the net increase in time to copy a 1MB file for an SD-WAN Edge Vendor solution.

[R33] The test **MUST** measure the net increase in time to copy a 1MB file for an SP SD-WAN Service solution. .

8.8.1.3 Net increase in time to copy clean file – 10MB

This test measures the net increase in time to copy a 10MB file.

[R34] The test **MUST** measure the net increase in time to copy a 10MB file for an SD-WAN Edge Vendor solution.

[R35] The test **MUST** measure the net increase in time to copy a 10MB file for an SP SD-WAN Service solution.

8.8.1.4 Net increase in time to copy clean file – 100MB

This test measures the net increase in time to copy a 100MB file.

[R36] The test **MUST** measure the net increase in time to copy a 100MB file for an SD-WAN Edge Vendor solution.

[R37] The test **MUST** measure the net increase in time to copy a 100MB file for an SP SD-WAN Service solution.

8.8.2 Dropbox folder

8.8.2.1 Net increase in time to copy clean file – 100KB

This test measures the net increase in time to copy a 100KB file.

[R38] The test **MUST** measure the net increase in time to copy a 100KB file for an SD-WAN Edge Vendor solution.

[R39] The test **MUST** measure the net increase in time to copy a 100KB file for an SP SD-WAN Service solution.

8.8.2.2 Net increase in time to copy clean file – 1MB

This test measures the net increase in time to copy a 1MB file.

[R40] The test **MUST** measure the net increase in time to copy a 1MB file for an SD-WAN Edge Vendor solution.

[R41] The test **MUST** measure the net increase in time to copy a 1MB file for an SP SD-WAN Service solution.

8.8.2.3 Net increase in time to copy clean file – 10MB

This test measures the net increase in time to copy a 10MB file.

[R42] The test **MUST** measure the net increase in time to copy a 10MB file for an SD-WAN Edge Vendor solution.

[R43] The test **MUST** measure the net increase in time to copy a 10MB file for an SP SD-WAN Service solution.

8.8.2.4 Net increase in time to copy clean file – 100MB

This test measures the net increase in time to copy a 100MB file.

[R44] The test **MUST** measure the net increase in time to copy a 100MB file for an SD-WAN Edge Vendor solution.

[R45] The test **MUST** measure the net increase in time to copy a 100MB file for an SP SD-WAN Service solution.

8.8.3 Google Drive

8.8.3.1 Net increase in time to copy clean file – 100KB

This test measures the net increase in time to copy a 100KB file.

[R46] The test **MUST** measure the net increase in time to copy a 100KB file for an SD-WAN Edge Vendor solution.

[R47] The test **MUST** measure the net increase in time to copy a 100KB file for an SP SD-WAN Service solution.

8.8.3.2 Net increase in time to copy clean file – 1MB

This test measures the net increase in time to copy a 1MB file.

[R48] The test **MUST** measure the net increase in time to copy a 1MB file for an SD-WAN Edge Vendor solution.

[R49] The test **MUST** measure the net increase in time to copy a 1MB file for an SP SD-WAN Service solution.

8.8.3.3 Net increase in time to copy clean file – 10MB

This test measures the net increase in time to copy a 10MB file.

[R50] The test **MUST** measure the net increase in time to copy a 10MB file for an SD-WAN Edge Vendor solution.

[R51] The test **MUST** measure the net increase in time to copy a 10MB file for an SP SD-WAN Service solution.

8.8.3.4 Net increase in time to copy clean file – 100MB

This test measures the net increase in time to copy a 100MB file.

[R52] The test **MUST** measure the net increase in time to copy a 100MB file for an SD-WAN Edge Vendor solution.

[R53] The test **MUST** measure the net increase in time to copy a 100MB file for an SP SD-WAN Service solution.

8.8.4 HTTP web server

8.8.4.1 Net increase in time to copy clean file – 100KB

This test measures the net increase in time to copy a 100KB file.

[R54] The test **MUST** measure the net increase in time to copy a 100KB file for an SD-WAN Edge Vendor solution.

[R55] The test **MUST** measure the net increase in time to copy a 100KB file for an SP SD-WAN Service solution.

8.8.4.2 Net increase in time to copy clean file – 1MB

This test measures the net increase in time to copy a 1MB file.

[R56] The test **MUST** measure the net increase in time to copy a 1MB file for an SD-WAN Edge Vendor solution.

[R57] The test **MUST** measure the net increase in time to copy a 1MB file for an SP SD-WAN Service solution.

8.8.4.3 Net increase in time to copy clean file – 10MB

This test measures the net increase in time to copy a 10MB file.

[R58] The test **MUST** measure the net increase in time to copy a 10MB file for an SD-WAN Edge Vendor solution.

[R59] The test **MUST** measure the net increase in time to copy a 10MB file for an SP SD-WAN Service solution.

8.8.4.4 Net increase in time to copy clean file – 100MB

This test measures the net increase in time to copy a 100MB file.

[R60] The test **MUST** measure the net increase in time to copy a 100MB file for an SD-WAN Edge Vendor solution.

[R61] The test **MUST** measure the net increase in time to copy a 100MB file for an SP SD-WAN Service solution.

9 Routing and Access Control Testing

This section of certification testing covers the ability to verify that an SD-WAN Edge Vendor solution or a set of SD-WAN Edge Vendor solutions can establish and route traffic over various UCS technologies and Tunnel Virtual Connections (TVCs), and based on policy criteria, make decisions on forwarding traffic.

9.1 TVC Connectivity

An SWVC contains one or more UCSs (underlay) and TVCs. This test aims to ensure that TVCs can be established between SD-WAN Edges and that traffic can be forwarded between the SD-WAN Edges. Sometimes, the TVCs will be encrypted to support Encryption Policy requirements.

9.1.1 SD-WAN Edge to SD-WAN Edge Test

This test determines whether the SD-WAN Edges can establish TVCs and route traffic across multiple UCS End Points. Passing this test is an essential requirement for all SD-WAN Edges.

Test Objective: Does the SD-WAN solution correctly forward traffic toward the intended network segment?

Test Process: Create TVCs between the SD-WAN Edges in the test Testing Topology and ensure that traffic is forwarded across the appropriate UCS End Points and TVCs according to Application Flow Specifications and Policies as described in MEF 70.1. Test methodology may require that two TVCs are established, one encrypted and one unencrypted, The encrypted TVC is failed forcing all traffic that can be supported by the unencrypted TVC to flow over that TVC rather than being discarded.

[R62] An SD-WAN Edge Vendor solution **MUST** be able to establish TVCs and route traffic across multiple UCS endpoints, as described in section 9.1.1.

[R63] An SD-WAN Edge Vendor solution **MUST** be able to establish encrypted TVCs and route traffic over these TVCs based on an SD-WAN Policy that requires encryption.

[D1] An SD-WAN Edge Vendor solution **SHOULD** be able to establish unencrypted TVCs and route traffic.

[R64] An SP SD-WAN Service solution **MUST** be able to establish TVCs and route traffic across multiple UCS endpoints, as described in section 9.1.1.

9.1.1.1 Scoring Penalty

A 100% penalty is assessed if the SD-WAN Edge Vendor solution or an SP SD-WAN Service solution cannot establish and route traffic across multiple UCS End Points.

9.2 Data Center to Branch Office

As discussed in **Figure 3**, the test configuration simulates a Data Center and three Branch Offices. To fully test the Data Center, a second solution is located at the Data Center so that maximum throughput can be measured between the largest solutions. This test is used to verify how traffic is passed over private and public UCSs from the Data Center to the Branch Offices. If the SD-WAN Edge Vendor brings in a Large solution, they are expected to include two Large solutions so that they can be tested between them to measure the performance of the Large solution. The test between the two Large solutions does not include the rest if the test configuration, it simply provides a connection between the two Large solutions and the maximum throughput is tested between the two SD-WAN Edges. In addition Medium or Small solutions are placed at the Branch Offices.

9.2.1 Data Center to Branch Office Test

Test Objective: To verify that test traffic generated at the SD-WAN UNI connected to the Data Center is forwarded correctly based on Application Flow Specifications and Policies to the appropriate Branch Office.

Test Process: traffic is passed between the Data Center and each Branch office over TVCs with traffic up to 70% of the capacity of each UCS (private and public) as determined by testing in section 8.1. MOS for voice and video should remain consistent with the baseline.

[R65] An SD-WAN Edge Vendor solution **MUST** be able to address the traffic rate supported by TVCs as described in section 9.2.1.

9.2.1.1 Scoring Penalty

A 25% penalty is assessed if the SD-WAN Edge Vendor solution or the SP SD-WAN Service solution MOS is impacted by more than 40%.

9.3 Branch Office to Data Center

As discussed in **Figure 3**, the test configuration simulates a Data Center and three Branch Offices. This test is used to verify how traffic is passed over private and public UCSs from the Branch Offices to the Data Center

9.3.1 Branch to Data Center Office Test

Test Objective: To verify that test traffic generated at the SD-WAN UNI connected to the Branch Office is forwarded correctly based on Application Flow Specifications and Policies to the Data Center.

Test Process: traffic is passed between each Branch office and the Data Center over TVCs with traffic up to 70% of the capacity of each UCS (private and public) as determined by testing in section 8.1. MOS for voice and video should remain consistent with the baseline.

[R66] An SD-WAN Edge Vendor solution **MUST** be able to address the traffic rate supported by TVCs as described in section 9.2.1.

9.3.1.1 Scoring Penalty

A 25% penalty is assessed if the SD-WAN Edge Vendor solution or the SP SD-WAN Service solution MOS is impacted by more than 40%.

9.4 Simple Policy

This test verifies a Policy that allows all traffic to be passed. Some implementations may not require creating a policy to pass this test. If a policy is required, it must pass all packets received at each SD-WAN UNI.

9.4.1 Simple Policy Test

Test Objective: To what extent does the SD-WAN solution correctly enforce simple policies?

Test Process: One or more Application Flow Specifications with a baseline Policy that allows all traffic to be forwarded are created. This test verifies that all traffic is passed over the TVCs between SD-WAN Edges. From a test topology perspective, all traffic is passed from the SD-WAN Edge to the SD-WAN Edge implementation and may include multiple TVCs and load balancing. This ensures that the SD-WAN can pass traffic between all sites at a 70% capacity of the maximum found in section 8.1 over TVCs with a Packet Loss of < 1%.

[R67] An SD-WAN Edge Vendor solution **MUST** be able to pass all packets as described in section 9.4.1.

[R68] An SP SD-WAN Service solution **MUST** be able to pass all packets as described in section 9.4.1.

9.4.1.1 Scoring Penalty

A 100% penalty is assessed if the SD-WAN Edge Vendor solution or an SP SD-WAN Service solution cannot create policies where all traffic is passed.

9.5 Complex Policies

Multiple Egress and Ingress Policies can be required to allow or disallow certain protocols. The Complex Policy Tests verify that Policies can be configured for various Application Flow Specifications and protocols. Complex Policies are configured, and protocols or Application Flows are passed between SD-WAN Edges.

Test Objective: Does the SD-WAN solution correctly enforce complex policies with multiple zones (e.g., allow and deny specific and general traffic based on application, protocol, zone, etc.)?

9.5.1 Complex Policy Test

Test Objective: Determine if the SD-WAN solution correctly enforce Complex Policies with multiple Zones (e.g., allow and deny specific and general traffic based on Application Flow Specification, protocol, and zone).

Test Process: An example of the Application Flows and protocols that are tested are shown in **Table 9**. The exact list of protocols will be agreed to with the test house at the time of test plan development. These Application Flows and protocols are subject to degradation as Packet Delay and Inter-Packet Delay Variation increase. For this reason, the policy is configured only to use UCSs that meet the Performance Criteria for these protocols. This test is planned to be modified to include background traffic. Background traffic will be generated at 50% of the capacity of the SD-WAN Edge discovered in the benchmark value, as determined in section 8. The remaining traffic does not exceed 50% of the benchmark value. This test requires the use of Application Flow Specifications, Zones, and Policies.

Protocol or Application
VoIP
H.323
RTP
RTCP
RTSP
HTTP
HTTPS
SCP
SFTP
IMAP
SNMPv2
RADIUS
POP3
NetBIOS
TACACS+
SMB
NTP
Facebook
LinkedIn
LDAP
SYSLOG
Cisco Webex
Microsoft Teams
Zoom
Salesforce
Dropbox
Google Drive
Office 365

Table 9 – Example Tested Applications and Protocols

Table 9 shows examples of the Applications and Protocols that may be tested. Prior to testing, a list of the actual Applications and Protocols that will be tested are provided by the test house. The SD-WAN Edge Vendor is expected to assist with creating the appropriate Application Flow specifications and Policies to correctly pass the Applications and Protocols that are tested.

[R69] An SD-WAN Edge Vendor solution **MUST** be able to pass protocols and applications as described in section 9.5.1

[R70] An SP SD-WAN Service solution **MUST** be able to pass protocols and applications as described in section 9.5.1

9.5.1.1 Scoring Penalty

A 50% penalty is assessed if the SD-WAN Edge Vendor solution or an SP SD-WAN Service solution cannot support Complex Policies for the Applications and Protocols to be tested.

10 UCS Impairment of SD-WAN SWVC

UCS impairments such as One-way Packet Loss Ratio (PLR), excessive One-way Mean Packet Delay (PD), or One-way Mean Inter-Packet Delay Variation (IPDV), Packet reordering, UCS saturation and congestion, and the use of Quality of Service (QoS) can impact the user experience and impact the overall effectiveness of SD-WAN. The tests described in this section cover various types of impairments of UCSs and verify how the SD-WAN Edge Vendor solution or an SP SD-WAN Service solution reacts to these impairments. Impairments are introduced on all Public UCSs, and the testing is performed from the Headquarters to all Branches simultaneously.

10.1 Quality of Experience

The time it takes for an SD-WAN Edge Vendor to detect a degradation or failure on a TVC and to redirect the packets to another TVC that is not impacted by the degradation or failure is measured in two values within this section (remediation is not enabled). The first is the Detection Time, measured from when a degradation or failure is introduced into the test configuration until an SD-WAN Edge detects the failure or degradation and reports it. This time is expected to be 3 seconds or less. The second is the Redirect Time, measured from when a degradation or failure is introduced into the test configuration until the packets have been redirected to a new TVC and the application is active. This time is expected to be 1 second or less. The Detect Time + the Redirect Time = the Total Time. The SD-WAN Edge is configured so that the Detect Time and Redirect Time thresholds can be met. The quality of experience throughout section 10.1 is measured using the Mean Opinion Score (MOS). For all tests shown below, there is background traffic running in addition to the Voice and Video traffic. This traffic is as shown below:

a. HTTP = ~20% of UCS Link BW (for each branch)

b. FTP = ~15% of UCS Link BW (for each branch)

c. SMTP = ~12% of UCS Link BW (for each branch)

d. Video = ~18% of UCS Link BW (for each branch)

e. Voice = ~10% of UCS Link BW (for each branch)

Note: MOS tests may result in lower priority classes experiencing Packet Loss or increased Packet Delay.

MOS is an estimated perceptual quality score that considers the effects of codec, the impact of IP impairments (such as packet loss) on the group of pictures, structure, and video content, and the effectiveness of loss concealment methods.

10.2 Impairments

The following sections describe the impairments that are introduced during the testing defined in sections 10.3 through 10.7. Some of the tests use a single impairment while others use a combination of impairments to perform measurements.

10.2.1 Packet Loss (Video & Voice)

Packet loss for both Voice and Video plays a significant role in affecting MOS. Minimal or zero packet loss signals a reliable and effective solution for real-time communication.

10.2.2 Duplicate Packets (Video & Voice)

Incorrect duplication techniques cause packets to be duplicated unnecessarily, which impacts bandwidth utilization rather than providing redundancy/reliability. Minimal or zero duplicate packets indicates effective processing of received packets.

10.2.3 Out-of-Order Packets (Video & Voice)

Incorrect duplication techniques cause packets to be duplicated unnecessarily, which impacts bandwidth utilization rather than providing redundancy/reliability. Minimal or zero duplicate packets indicates effective processing of received packets.

10.2.4 One-Way Packet Delay

The RTP one-way delay is used to assess the perceived quality of the link for Voice applications. High value indicates a possible lag in real-time applications.

10.2.5 Inter-Packet Delay Variation

Variation in packet delay indicates the frequency of the received packets. High value indicates serious issues for real-time applications.

10.3 Impact of Dynamic Path Selection

The goal of this test is to determine how long it takes for traffic to move to an available link when preconfigured impairments are applied. SWVCs employ various techniques to condition UCSs to ensure the reliability of data transmission.

The SD-WAN Edge Vendor or an SP SD-WAN Service solution should support path decisions on a per-flow basis according to available links and according to the conditions that exist on those links.

This test should be performed on all three sizes (Small, Medium, Large) of SD-WAN Edge Vendor solutions.

10.3.1 Impact of Packet Loss (Video & Voice)

Test Objective: This test determines the impact of Packet Loss on the SD-WAN Edge to carry Voice and Video traffic accompanied by other protocols and applications such as HTTP, FTP and SMTP.

Test Process: This test will simulate reordering of IP Packets in a Poisson and Gaussian distribution received over the UCSs in the SD-WAN test configuration. Voice and video traffic accompanied by background traffic (explained in 9.1) are passed over the test configuration, Packet Loss is introduced, and MOS is measured for Voice and Video, while other metrics mentioned in Quality of experience (section 9.1) are measured as well.

[R71] The Test **MUST** determine if an SD-WAN Edge Vendor solution is able to successfully forward IP packets during a period of Packet Loss based on Application Flow Specifications or Policies, as described in section 10.1.

[R72] The Test **MUST** determine if an SD-WAN Service Provider solution is able to successfully forward IP packets during a period of Packet Loss based on Application Flow Specifications or Policies, as described in section 10.1.

10.3.1.1 Scoring Penalty

A scoring penalty of no more than 20% is based on the MOS deviation from the benchmarks determined during testing in section 8. See **Table 15** for details

10.3.2 Impact of Packet Delay Variation

Test Objective: This test determines the impact of Inter-Packet Delay Variation on the SD-WAN Edge to carry Voice and Video traffic accompanied by other protocols and applications such as HTTP, FTP and SMTP.

Test Process: This test will simulate reordering of IP Packets in a Poisson and Gaussian distribution received over the UCSs in the SD-WAN test configuration. Voice and video traffic accompanied by background traffic (explained in 9.1) are passed over the test configuration, Packet Delay Variation is introduced, and MOS is measured for Voice and Video, while other metrics mentioned in Quality of experience (section 9.1) are measured as well.

[R73] The Test **MUST** determine if an SD-WAN Edge Vendor solution is able to successfully forward IP packets during a period of Packet delay variation based on Application Flow Specifications or Policies, as described in section 10.1.

[R74] The Test **MUST** determine if an SD-WAN Service Provider solution is able to successfully forward IP packets during a period of Packet delay variation based on Application Flow Specifications or Policies, as described in section 10.1.

10.3.2.1 Scoring Penalty

A scoring penalty of no more than 20% is based on the MOS deviation from the benchmarks determined during testing in section 8. See **Table 15** for details

10.4 Impact of Path Conditioning

SWVCs employ various techniques to condition UCSs to ensure the reliability of data transmission. Due to duplication some SD-WAN Edge Vendor solutions employ IP packet duplication, forward error correction, bonding, or load balancing to resolve the impact of duplication.

The SD-WAN Edge Vendor or an SP SD-WAN Service solution should identify the best path and guarantee priority policies (application, protocol, or other configured guidance) over known good links with other traffic transmitted as best effort.

This test should be performed on all three sizes (Small, Medium, Large) of SD-WAN Edge Vendor solutions.

10.4.1 Impact of IP Packet Reordering

Test Objective: This test determines the impact of IP Packet reordering on voice and video MOS.

Test Process: This test will simulate reordering of IP Packets in a Poisson and Gaussian distribution received over the UCSs in the SD-WAN test configuration. Voice and video traffic accompanied by background traffic (explained in 9.1) are passed over the test configuration, Packet Reordering is introduced, and MOS is measured for Voice and Video, while other metrics mentioned in Quality of experience (section 9.1) are measured as well.

Note: SD-WAN Edge Vendor and SP SD-WAN Service solutions should re-assemble the IP packets to preserve the whole frame sequence.

[R75] The Test **MUST** determine if an SD-WAN Edge Vendor solution is able to successfully forward IP packets during a period of IP packet reordering based on Application Flow Specifications or Policies, as described in section 10.1.

[R76] The Test **MUST** determine if an SD-WAN Service Provider solution is able to successfully forward IP packets during a period of IP packet reordering based on Application Flow Specifications or Policies, as described in section 10.1.

10.4.1.1 Scoring Penalty

A scoring penalty of no more than 20% is based on the MOS deviation from the benchmarks determined during testing in section 8. See **Table 15** for details

10.4.2 Impact of IP Packet Duplication

Test Objective: This test determines the impact of IP Packet duplication on voice and video MOS.

Test Process: This test will simulate reordering of IP Packets in a Poisson and Gaussian distribution received over the UCSs in the SD-WAN test configuration. Voice and video traffic accompanied by background traffic (explained in 9.1) are passed over the test configuration, Packet Duplication is introduced, and MOS is measured for Voice and Video, while other metrics mentioned in Quality of experience (section 9.1) are measured as well.

Note: SD-WAN Edge Vendor and SP SD-WAN Service solutions should take the next-in-sequence IP packet and drop the duplicates to preserve the whole frame sequence.

[R77] The Test **MUST** determine if an SD-WAN Edge Vendor solution is able to successfully forward IP packets during a period of IP packet duplication based on Application Flow Specifications or Policies, as described in section 10.4.2.

[R78] The Test **MUST** determine if an SD-WAN Service Provider solution is able to successfully forward IP packets during a period of IP packet duplication based on Application Flow Specifications or Policies, as described in section 10.4.2.

10.4.2.1 Scoring Penalty

A scoring penalty of no more than 20% is based on the MOS deviation from the benchmarks determined during testing in section 8. See **Table 15** for details

10.5 Impact of Link Saturation and Congestion

This test aims to ensure reliable bandwidth use in the SD-WAN or SWVC. This test should be performed on all three sizes (Small, Medium, Large) of SD-WAN Edge Vendor solutions.

10.5.1 Impact of Accumulate and Burst

Test Objective: This test measures the impact of both queueing and transmission delay on IP Packets traversing the UCSs between SD-WAN Edges.

Test Process: IP Packets are burst across the UCSs once a configured condition is met. This test will simulate the accumulation of IP Packets until the buffer queue has (N) IP Packets or until IP Packets have been accumulated for a specified time (T) with a minimum inter-burst gap. MOS is measured for Voice and Video, while other metrics mentioned in Quality of experience (section 9.1) are measured as well. MOS is measured for Voice and Video, while other metrics mentioned in Quality of experience (section 9.1) are measured as well.

Note: Both queueing and transmission delays are included in this test, and appropriate Application Flow Specifications and Policies are included in the configuration of the SD-WAN Edges.

This test should be performed on all three sizes (Small, Medium, Large) of SD-WAN Edge Vendor solutions.

[R79] The test **MUST** measure an SD-WAN Edge Vendor solution's ability to manage IP Packet forwarding during a period of IP packet accumulation and burst based on application or policy as described in section 10.5.1.

[R80] The test **MUST** measure an SD-WAN Service Providers solution's ability to manage IP Packet forwarding during a period of IP packet accumulation and burst based on application or policy as described in section 10.5.1.

10.5.1.1 Scoring Penalty

A scoring penalty of no more than 20% is based on the MOS deviation from the benchmarks determined during testing in section 8. See **Table 15** for details

10.5.2 Impact of Branch Congestion Network Behavior

Test Objective: This test verifies the ability of policers within the SD-WAN Edge to limit the data rate of a network stream to ensure that it does not exceed the specified limits.

Test Process: The saturation of the public UCSs is emulated. Testing verifies that traffic policing follows the MEF bandwidth profiles for Ethernet services described in MEF 41 [4] and MEF 41.0.1 [5]. To replicate congestion in the Branch, impairments will be applied to the links at the Branch in the direction from Branch to Data Center (to the emulated aggregation point, ISP 1, and ISP 2) shown in **Figure 3**. MOS is measured for Voice and Video, while other metrics mentioned in Quality of experience (section 9.1) are measured as well.

Note: This test is only performed at locations with Internet and MPLS connectivity, i.e., Branches 1 and 2. Congestion is applied across all ISP links, including Branch 3. The traffic is reduced ensure there is still room forward traffic without issues

[R81] The test **MUST** verify that the SD-WAN Edge Vendor solution is able to manage IP packet forwarding during a period of Branch congestion based on Application Flow Specification or Policy as described in section 10.5.2.

[R82] The test **MUST** verify that the SP SD-WAN Service solution **MUST** be able to manage IP packet forwarding during a period of Branch congestion based on Application Flow Specification or Policy as described in section 10.5.2.

10.5.2.1 Scoring Penalty

A scoring penalty of no more than 20% is based on the MOS deviation from the benchmarks determined during testing in section 8. See **Table 15** for details

10.5.3 Impact of Data Center Congestion Network Behavior

Test Objective: This test verifies the ability of policers within the SD-WAN Edge to limit the data rate of a network stream to ensure that it does not exceed the specified limits.

Test Process: To measure this, the saturation of the public UCSs is emulated. Testing verifies that traffic policing follows the MEF bandwidth profiles for Ethernet services described in MEF 41 [4] and MEF 41.0.1 [5]. To replicate congestion in the Data Center, congestion impairments will be applied to the UCSs (from the emulated aggregation point, ISP 1, and ISP 2 to the Data Center SD-WAN site) shown in **Figure 3**. MOS is measured for Voice and Video, while other metrics mentioned in Quality of experience (section 9.1) are measured as well.

[R83] The test **MUST** verify that the SD-WAN Edge Vendor solution is able to manage IP packet forwarding during a period of “last mile” impairments based on Application Flow Specification or Policy as described in section 10.5.3.

[R84] The test **MUST** verify that the SP SD-WAN Service solution **is** able to manage IP packet forwarding during a period of “last mile” impairments based on Application Flow Specification or Policy as described in section 10.5.3.

10.5.3.1 Scoring Penalty

A scoring penalty of no more than 20% is based on the MOS deviation from the benchmarks determined during testing in section 8. See **Table 15** for details

10.6 Impact of Quality of Service

QoS is essential for business-critical applications such as voice and video. If given priority, these applications must be prioritized if a link has bad performance indicators. This test measures QoS using voice traffic and video streams. The test will include MOS for video and call measurements for VoIP. This test should be performed on all three sizes (Small, Medium, Large) of SD-WAN Edge Vendor solutions.

10.6.1 Impact of All Impairments

Test Objective: This test determines the impact of all impairments on IP Packets traversing the UCSs between SD-WAN Edges in the test configuration. The SD-WAN Service should manage traffic according to configured QoS policies.

Test Process: Impairments are introduced on all UCSs included in the test configuration. MOS is measured for Voice and Video, while other metrics mentioned in Quality of experience (section 9.1) are measured as well. The impairments included in this test are:

- Packet Loss (0-10%)
- Packet Delay Variation (0-300 milliseconds)
- Packet Reordering (0-10%)
- Packet Duplication (0-10%)
- Accumulate and burst packets (0-50 milliseconds)
- Data Center egress congestion (0-50%)
- Branch Office ingress congestion (0-50%)
- All Impairments (all of the above)

Note: All UCSs (except MPLS links) in the test configuration are impaired during this test.

[R85] The test **MUST** verify that the SD-WAN Edge Vendor solution **is** able to manage IP packet forwarding during all impairments based on Application Flow Specification or Policy as described in section 10.6.1.

[R86] The test **MUST** verify that the SP SD-WAN Service solution **is** able to manage IP packet forwarding during all impairments based on Application Flow Specification or Policy as described in section 10.6.1.

10.6.1.1 Scoring Penalty

A scoring penalty of no more than 20% is based on the MOS deviation from the benchmarks determined during testing in section 8. See **Table 15** for details.

10.7 Application-Aware Traffic Steering

This test will assess how the product directs various Application Flow Specifications for applications besides video and voice. The behavior will be observed and recorded to establish whether voice/video and data are sent over the same link once impairments are applied and which application takes precedence based on Application Flow Specifications and Policies.

These complex outbound and inbound Policies consist of many rules, objects, and applications that verify whether the SD-WAN can accurately determine the correct application (regardless of port/protocol used) and then take the appropriate action.

- VoIP
- Business video (Webex, Microsoft Skype Professional, etc.)
- Popular social networking websites (web applications)
- Other basic legacy applications (e.g., FTP, Telnet)

A product's ability to perform the following functions will be tested for each application.

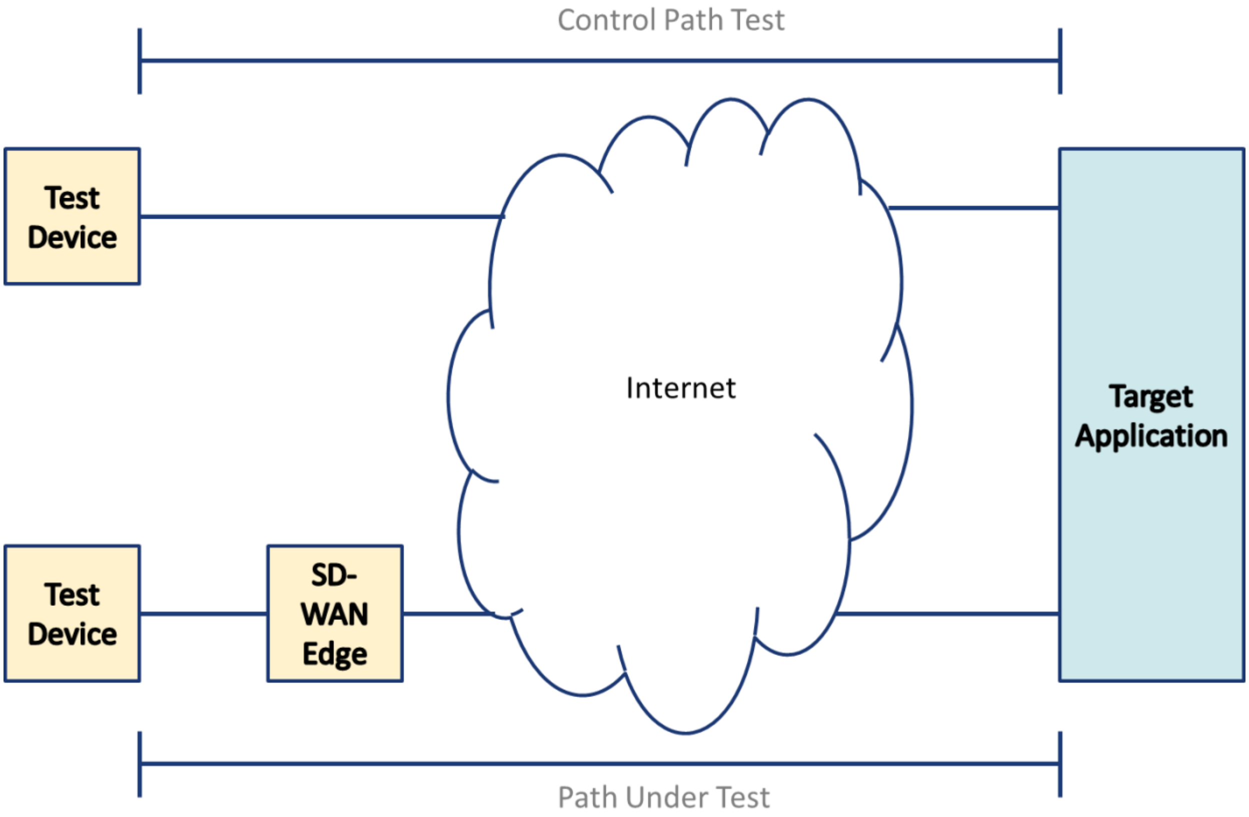

Figure 4 – Baseline Control Path vs. Path Under Test

Figure 4 shows that when tests of Policies are run to applications on the internet (Path Under Test), there is also a Control test (baseline) that is underway for the same application at the same time. The results of the tests on the Path Under Test are then compared to the results of the Control Path. The baseline is done without an SD-WAN edge delta between the measurements indicates the contribution of the SD-WAN Edge(s) to the test device results. Outlier test results are removed from the results. The path under test includes an SD-WAN Edge delta between the test device and the target application. The delta in performance between the Baseline and path under test is measured. Outliers [if any] are ignored.

10.7.1.1 Steer (DIA)

Test Objective: This test verifies that the SD-WAN Edge can identify an application accurately, map it to an Application Flow Specification, and direct it over the correct Public UCS according to a configured Policy.

Test Process: Application Flow Specifications and Policies are created that steer certain test traffic to the Public UCS. The test traffic is then sent from the Data Center to each Branch, and it is verified that this test traffic uses the Public UCS.

[R87] The test **MUST** verify that the SD-WAN Edge Vendor solution is able to steer IP packets based on Application Flow Specification and Policy, as described in section 10.7.1.1.

[R88] The test **MUST** verify that the SP SD-WAN Service solution is able to steer IP packets based on Application Flow Specification and Policy, as described in section 10.7.1.1.

10.7.1.2 Drop Low-Priority Application During Congestion Event

Test Objective: This test verifies that when a UCS bandwidth exhaustion occurs, high-priority Application Flows take precedence over low-priority Application Flows based on Policy Criteria.

Test Process: UCSs between the Branch and the Data Center are congested at 90%. IP Packets for different Application Flows are introduced at the SD-WAN UNI, and MOS is measured on the high-priority Application Flows to ensure they do not suffer degradation.

[R89] The test **MUST** verify that the SD-WAN Edge Vendor solution **is** able to manage IP packet forwarding based on Application Flow Specification or Policy as described in section 10.7.1.2.

[R90] The test **MUST** verify that the SP SD-WAN Service solution **is** able to manage IP packet forwarding based on Application Flow Specification or Policy as described in section 10.7.1.2.

10.7.1.2.1 Scoring Penalty

A 40% penalty is assessed if the SD-WAN Edge Vendor solution or an SP SD-WAN Service solution cannot complete one of the tests in section 10.7.1.1 or 10.7.1.2 (steer traffic or drop low-priority Application Flows). A penalty of 50% is assessed if the SD-WAN Vendor solution or SP SD-WAN solution cannot complete both of the tests in sections 10.7.1.1 and 10.7.1.2 (steer traffic and drop low-priority Application Flows).

Editor Note 6: The ability of SD-WAN Edge Vendor solutions to block specific actions within an application is under discussion. If this is not supportable by the majority of vendors, it will be dropped.

11 SWVC Stability and Reliability

This document section addresses the stability and reliability of the SD-WAN Edge Vendor solution or an SP SD-WAN Service solution. These are measured by verifying the behavior of the state engine in the SD-WAN Edge Vendor solution(s) under a load. The other SD-WAN Edge included in the testing is of equal or greater capacity.

11.1 The behavior of the State Engine Under Load

These tests aim to determine whether the SD-WAN Edge Vendor solution can preserve the state across many concurrent connections over a four hour period. At various points throughout the test (including after the maximum has been reached), it is confirmed that the SD-WAN Edge Vendor solution can still verify and block traffic that violates the currently applied Policy while confirming that legitimate traffic is not blocked. The SD-WAN Edge Vendor solution must be able to apply Policy decisions effectively based on inspected traffic at all load levels.

11.1.1 Passing Legitimate Traffic – Normal Load

Test Objective: This test verifies that the SD-WAN Edge Vendor solution continues to pass legitimate traffic as the number of concurrent open sessions reaches 75% of the maximum determined previously in performance testing.

Test Process: Sessions are opened until 75% of the maximum is reached. Test Traffic is then introduced to see if IP Packets can be passed between the Data Center and the Branches. This requires the appropriate Application Flow Specifications and Policies to be created.

[R91] The test **MUST** verify that the SD-WAN Edge Vendor solution passes traffic, as described in section 11.1.1.

11.1.2 State Preservation – Maximum Sessions Exceeded

Test Objective: This test aims to determine whether the SD-WAN Edge Vendor solution maintains the state of pre-existing sessions as the number of open sessions exceeds the maximum determined previously by 110% in performance testing.

Test Process: It is verified that either the oldest/random sessions expire before a new session is created or the new session is blocked. If a session is expired, the far-end must be notified that the session has expired. This prevents the far-end from reassembling the new session data passed through.

Editor Note 7: A question has been raised on if the session is stateful, and the near-end is expecting an ACK from the far-end if it can be detected under these conditions. Comments on this are requested.

[R92] The ability of the SD-WAN Edge Vendor solution to preserve the state as described in section 11.1.2 **MUST** be confirmed.

11.1.3 Drop Non-Conformant Traffic – Maximum Sessions Exceeded

Test Objective: This test verifies that the SD-WAN Edge solution continues to drop all traffic not associated with existing sessions as the number of open sessions exceeds the maximum determined previously in performance testing.

Test Process: Sessions are opened until 110% of the maximum is reached. Test Traffic is then introduced to see if IP Packets can be passed between the Data Center and the Branches. This requires the apprpriate Application Flow Specifications and Policies to be created.

[R93] The test **MUST** verify that the SD-WAN Edge Vendor solution to drop traffic, as described in section 11.1.3.

11.1.4 Scoring Penalty

A 100% penalty is assessed if the SD-WAN Edge Vendor solution cannot pass legitimate traffic under normal load, preserve state, or drop legitimate traffic as specified above. This penalty is assessed for each of the three functions the solution cannot perform.

12 Testing of MEF 70.1 Requirements

This section aims to identify which requirements from MEF 70.1 are tested using the test methodologies defined in sections 9, 8, 9, and 11

MEF 70.1 Requirement	Testable (T) or Not Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this document	Comments
R1	N			
R2	N			
R3	T	M	9.1.1	[R3] IP reachability **MUST** exist between two SD-WAN Edges for IP Packets to be forwarded.
R4	N			
R5	N			
R6	T	M	7.1.1	[R6] The SD-WAN solution **MUST NOT** deliver an ingress IP Packet to a UNI where the destination address is not reachable.
R7	T	D		Need Methodology
R8	T	D		Need Methodology
R9	T	D		Need Methodology IPv6 requirement
O1	T	D		Need Methodology [O1] An SD-WAN solution MAY discard Ingress IPv4 Packets that contain the Loose Source and Record Route option, the Strict Source and Record Route option, or the Record Route option.
R10	N			
R11	N			
R12	N			
R13	N			
R14	N			
R15	N			
R16	N			
R17	N			
R18	N			
R19	N			

MEF 70.1 Requirement	Testable (T) or Not Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this document	Comments
R20	N			
R21	T	D		Need Methodology [R21] An IP Prefix **MUST** be assigned to only one Zone.
R22	T	D		Need Methodology [R22] The ability to send all IP hosts not assigned to any other Zone **MUST** be sent to the default Zone if a default Zone exists.
R23	T	D		Need Methodology [R23] There **MUST** only be one default Zone.
R24	T	D		Need Methodology [R24] If the IP host with the same source IP Address of an Ingress IP Packet is not assigned to a Zone, the IP Packet **MUST** be discarded.
R25	T	D		Need Methodology [R25] An IP Packet that arrives from a UNI **MUST** be associated with the Zone of the IP host associated with the Source IP Address of the IP Packet.

MEF 70.1 Requirement	**Testable (T) or Not Testable (N)**	**Mandatory (M), Deferred (D), or Optional (O)**	**Test Methodology from this document**	**Comments**
R26	T	D		Need methodology [R26] An IP Packet that arrives from the Internet **MUST** be assigned to the Zone identified for IP Packets destined for the Internet.
R27	N			
R28	N			
R29	N			
R30	N			
R31	T	M	7.1.1	[R31] Rules supporting Multi-point to Multi-point connections **MUST** identify at least two interfaces on the SD-WAN solution per connection.
R32	T	M	7.1.1	[R32] Rules supporting Rooted Multi-point connections **MUST** identify the roots and leaves.
R33	T	M	7.1.1	[R33] an interface **MUST** appear once, either as a root or a leaf but not both.
D1	N			
R34	T	D		Config methodology [R34a] The SD-WAN solution **MUST** have a method of specifying the behavior of ingress and egress IP Packets. [R34] If names are used in the method, the name **MUST** appear at most only once.

MEF 70.1 Requirement	**Testable (T) or Not Testable (N)**	**Mandatory (M), Deferred (D), or Optional (O)**	**Test Methodology from this document**	**Comments**
R35	N			
R36	T	D		Configuration Methodology [R36] The method **MUST** define either Ingress or Egress behavior but not both.
R37	T	D		Configuration Methodology [R37] The method **MUST** support defining the criteria descriptions shown in Table 4.
D2	T	D		Configuration Methodology [D2] The method **SHOULD** support defining the criteria descriptions shown in Table 5.
R38	T	O	9.5.1	SP ONLY. 7.5.1 will be updated for SP Beta
R39	N			
R40	T	D		Configuration Methodology [R40] The method **MUST** use the same criteria for each set of rules used for a given SD-WAN Service. Note different criteria values are permitted.

MEF 70.1 Requirement	**Testable (T) or Not Testable (N)**	**Mandatory (M), Deferred (D), or Optional (O)**	**Test Methodology from this document**	**Comments**
R41	T	D		Configuration Methodology [R41] If the SD-WAN solution cannot forward an IP Packet over the underlay, it **MUST** be discarded.
R42	T	D		Need Methodology and test configuration change [R42] If the SD-WAN solution rules require that a given private flow be encrypted, the SD-WAN solution **MUST** encrypt the IP Packets before forwarding them over the underlay.
R43	T	D		Need Methodology and test configuration change [R43] If the SD-WAN solution rules require that a given public flow be encrypted, the SD-WAN solution **MUST** encrypt the IP Packets before forwarding them over the underlay.

MEF 70.1 Requirement	**Testable (T) or Not Testable (N)**	**Mandatory (M), Deferred (D), or Optional (O)**	**Test Methodology from this document**	**Comments**
R44	T	D		Need Methodology and test configuration change [R44] If the SD-WAN solution rules specify that encryption is optional, then whether an underlay is encrypted or not **MUST NOT** be taken into account when forwarding decisions are being made.
R45	T	M		Will be added for Beta [R45] If the SD-WAN solution rules for a flow include private underlay only, then the SD-WAN solution **MUST** only forward IP Packets belonging to a flow over private underlay.
R46	T	M		Will be added for Beta [R46] If the SD-WAN solution rules for a flow include public or private underlay, then the SD-WAN solution **MUST** forward IP Packets belonging to a flow over public or private underlay.

MEF 70.1 Requirement	**Testable (T) or Not Testable (N)**	**Mandatory (M), Deferred (D), or Optional (O)**	**Test Methodology from this document**	**Comments**
R47	T	D		Configuration Methodology [R47] If the SD-WAN solution rules for a flow include underlays that are flat rate billed (policy name), then the SD-WAN solution **MUST** forward IP Packets belonging to a flow over flat rate billed underlay.
R48	T	D		Configuration Methodology [R48] If the SD-WAN solution rules for a flow include underlays that are usage based billed (policy name), then the SD-WAN solution **MUST** forward IP Packets belonging to a flow over usage rate billed underlay.
R49	T	D		Configuration Methodology [R49] If the SD-WAN solution rules for a flow include either (policy name) usage based or flat rate billing underlays, then the SD-WAN solution **MUST** not take into account the billing method when making forwarding decisions.

MEF 70.1 Requirement	**Testable (T) or Not Testable (N)**	**Mandatory (M), Deferred (D), or Optional (O)**	**Test Methodology from this document**	**Comments**
R50	T	D		Configuration Methodology [R50] If a flow is not included in a virtual topology the SD-WAN solution **MUST NOT** allow rules to be created for the flow.
R51	N			
R52	N			
R53	N			
R54	N			
R55	N			
R56	N			
R57	T	M	7.1.1	[R57] The SD-WAN solution **MUST** forward an ingress unicast IP Packet to an egress UNI that is included in the zone(s) specified in the SD-WAN solution rules.
R58	T	D		Need methodology [R58] If the SD-WAN solution rules do not specify the zones that ingress unicast IP Packets can be forward to, the IP Packets **MUST** be treated as if the criteria value is self in the rule.

MEF 70.1 Requirement	Testable (T) or Not Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this document	Comments
R59	T	M	8.8.4	[R59] If the rules for a flow specify that they IP Packets belonging to the flow are forwarded to the Internet, the IP Packets **MUST** be forwarded over a UNI that has access to the Internet.
R60	T	M	8.8.4	[R60] If the rules for a flow specify that IP Packets belonging to the flow are not to be forwarded to the Internet, the IP Packets **MUST NOT** be forwarded over a UNI that has direct access to the Internet.
R61	N			
R62	T	M	8.8.4	[R62] If none of the criteria of a rule for a flow include that IP Packets are forwarded over the Internet, then any IP Packets from the Internet and destined to the LAN UNI **MUST** be discarded.
R63	T	M	8.8.4	[R63] If the SD-WAN solution rules do not specify the behavior for IP Packets destined or from the Internet, the IP Packets **MUST** be treated as if the criteria value is disabled in the rule.

MEF 70.1 Requirement	Testable (T) or Not Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this document	Comments
R64	T	M	7.1.1	[R64] If the SD-WAN solution allows WAN UNIs to be enabled as backup only, IP Packets belonging to any flow **MUST NOT** be forwarded over that WAN UNI if other WAN UNIs exist and are operational to the destination.
R65	T	M	7.1.1	[R65] If the SD-WAN solution has rules that specify that IP Packets belonging to a flow are not forwarded to WAN UNIs marked as backup, then IP Packets belonging to that flow **MUST** be discarded if no WAN UNI exists that is not marked as backup.
R66	N			
R67	N			
R68	N			
D3	N			
R69	N			

MEF 70.1 Requirement	**Testable (T) or Not Testable (N)**	**Mandatory (M), Deferred (D), or Optional (O)**	**Test Methodology from this document**	**Comments**
R70	T	D		Need Methodology [70all] The SD-WAN solution **MUST** provide a method to specify a minimum bandwidth for a flow. The SD-WAN solution **MUST** declare ingress IP Packets as either conformant or non-conformant. The SD-WAN solution **MUST** discard non-conformant IP Packets when congestion on a WAN UNI occurs.
R71	T	D		Covered in R70all
R72	T	D		Covered in R70all
O2	T	D		Covered in R70all
O3	T	D		Covered in R70all
R73	T	D		Covered in R70all
R74	T	D		Covered in R70all
R75	T	M	9.1.1 (add block)	[R75] If the origin of an IP Packet destined for an Egress LAN UNI matches any source specified by the SD-WAN solution rules as blocked, the IP Packet **MUST** be discarded (not forwarded across the Egress UNI).
R76	N			
R77	N			
R78	N			
R79	N			
R80	N			

MEF 70.1 Requirement	**Testable (T) or Not Testable (N)**	**Mandatory (M), Deferred (D), or Optional (O)**	**Test Methodology from this document**	**Comments**
R81	N			
R82	T	D		Configuration Methodology [R82] If the SD-WAN solution rules specify more than one criterion, the rules for a flow **MUST** contain all the criteria.
R83	T	M	9.1.1	[R83] Each Ingress IP Packet **MUST** be mapped to a flow and forwarded based in SD-WAN solution rules.
R84	T	M	9.1.1	[R84] If an Ingress IP Packet cannot be associated to a flow, it **MUST** be discarded.
R85	T	M	9.5.1	[R85] The SD-WAN solution rules for flows **MUST** use the criteria specified in MEF 70.1 Table 7.
R86	T	M	7.4.1 (simple), 7.5.1 (complex)	[R86] The SD-WAN solution rules for flows **MUST** allow for the definition of simple and complex flows.
R87	T	M	7.4.1	[R87] If the SD-WAN solution rules for flows is set to pass any IP Packets, other criteria **MUST NOT** be specified.
D4	T	O	9.5.1	[D4] The SD-WAN solution rules for flows **SHOULD** use the criteria specified in MEF 70.1 Table 8.
R88	N			
R89	N			

MEF 70.1 Requirement	Testable (T) or Not Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this document	Comments
R90	N			
R91	N			
R92	N			
R93	N			
R94	N			
R95	N			
R96	N			
R97	N			
R98	N			
R99	N			
R100	T	M	9.1.1	[R100] If a SD-WAN solution flow is not assigned an Ingress set of rules by one of the four methods defined in R97-R99, IP Packets mapped to that flow **MUST** be discarded.
R101	T	M	9.1.1	[R101] If an SD-WAN solution flow is configured to block IP Packets, Ingress IP Packets mapped to that flow **MUST** be blocked,
R102	T	M	9.1.1	[R102] If a SD-WAN solution flow is not assigned an Egress set of rules, IP Packets mapped to that flow **MUST** be forwarded to the Egress LAN UNI.
R103	N			
R104	N			
R105	N			
R106	N			
R107	N			
R108	N			
R109	N			
R110	N			
R111	N			
D5	N			

MEF 70.1 Requirement	Testable (T) or Not Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this document	Comments
R112	T	M	9.1.1	[R112] If the SD-WAN solution rules specify that the LAN UNI do not allow IPv4 IP Packets then IPv4 Packets **MUST NOT** be forwarded to or from the LAN UNI.
R113	T	D		Need methodology (IPv6 or Both) [R113] The SD-WAN solution rules **MUST** allow either IPv4, IPv6, or both.
R114	T	D		Need solution [R114] When the SD-WAN solution rules for the LAN UNI specify that DHCP is used, the SD-WAN solution **MUST** use DHCP to convey to the Subscriber, in addition to the IPv4 address, the subnet mask and the default router address. No applicable CyberRatings test methodology. DHCP test case for SD-WAN UNI needed. Test per MEF 90

MEF 70.1 Requirement	Testable (T) or Not Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this document	Comments
R115	T	D		Need Methodology [R115] If the SD-WAN solution rules define that the UNI IPv4 Connection Addressing is DHCP, addresses that are dynamically assigned by DHCP **MUST** be taken from within an IP Prefix listed in the rules. No applicable CyberRatings test methodology. DHCP test case for SD-WAN UNI needed. Test per MEF 90
R116	N			
R117	N			
R118	T			Need Methodology [R118] If the SD-WAN solution rules for the LAN UNI do not allow IPv6 IP Packets, IPv6 Packets **MUST NOT** be forwarded to or from the LAN UNI.

MEF 70.1 Requirement	**Testable (T) or Not Testable (N)**	**Mandatory (M), Deferred (D), or Optional (O)**	**Test Methodology from this document**	**Comments**
R119	T	M		Need Methodology [R119] When the SD-WAN solution rules for the LAN UNI specify that DHCP is used, the SD-WAN solution **MUST** use DHCP to convey to the Subscriber, in addition to the IPv6 address, the subnet mask and the default router address. No applicable CyberRatings test methodology. DHCP test case for SD-WAN UNI needed. Test per MEF 90
R120	N			
R121	N			
R122	N			
R123	N			
R124	N			
R125	N			
R126	N			
R127	N			
R128	T	D		Configuration Methodology [R128] When the routing protocol for the LAN UNI is BGP, BGP as specified in RFC 4271 [18] **MUST** be used across the UNI to exchange routing information. Need BGP test cases

MEF 70.1 Requirement	**Testable (T) or Not Testable (N)**	**Mandatory (M), Deferred (D), or Optional (O)**	**Test Methodology from this document**	**Comments**
R129	T	D		Configuration Methodology [R129] When the LAN UNI routing protocol is BGP, the SD-WAN solution **MUST** support 4-octet AS Numbers as described in RFC 6793 [23]. Need BGP test cases
R130	N			
R131	N			
R132	T	D		Configuration Methodology [132] When routing protocol is BGP, if the Authentication parameter is MD5, authentication using MD5 **MUST** be supported by the SD-WAN solution as described in RFC 4271 [18] using the specified password. Need BGP test cases
R133	N			

MEF 70.1 Requirement	Testable (T) or Not Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this document	Comments
R134	T	D		Configuration Methodology [R134] Each entry in the BGP Community List and BGP Extended Community List parameters **MUST** have an associated semantic that describes how the SD-WAN solution will handle routes advertised with that value. Need BGP test cases
R135	T	D		Configuration Methodology [R135] When the BGP Damping parameter is not None, the SD-WAN solution **MUST** apply route flap damping as described in RFC 2439 [10]. Need BGP test cases
R136	N			
R137	T	D		Configuration Methodology [R137] When the BGP Damping parameter is None, the SD-WAN solution **MUST NOT** apply route flap damping. Need BGP test cases

MEF 70.1 Requirement	Testable (T) or Not Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this document	Comments
R138	T	D		Configuration Methodology [R138] When the BGP AS Override parameter is Enabled, the SD-WAN solution MUST overwrite all instances of the Subscriber's AS Number in the AS Path with their own AS Number, in routes advertised to the Subscriber. Need BGP test cases
R139	T	D		Configuration Methodology [R139] When the LAN UNI routing protocol is OSPF, then OSPF as specified in RFC 2328 [9] (for IPv4) and/or RFC 5340 [22] (for IPv6) **MUST** be used across the LAN UNI to exchange routing information. Need OSPF test cases
R140	N			
R141	N			
R142	N			
R143	N			
R144	N			
R145	N			
R146	N			
R147	N			
R148	N			

MEF 70.1 Requirement	Testable (T) or Not Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this document	Comments
R149	T	O	8.2	[R149] If the SD-WAN solution rules include a criterion specifying certain performance which includes a reference to One-Way Mean Packet Delay, it **MUST** be defined as follows for each Path p between UNIs x and y: Let Δ= {δ1, δ2, δ3, … δn} represent the One-Way Packet Delays of the n Qualified Packets sent from UNI x to UNI y across Path p during a time interval whose duration is the value of the evalinterval element of the SWVC Performance Time Intervals Service Attribute. Then the One-Way Mean Packet Delay for p over that interval is the arithmetic mean of the values δ1 … δn. If n=0 during the time interval, the One-Way Mean Packet Delay for that time interval is zero.

R150	T	O	10.1	[R150] If the SD-WAN solution rules include a criterion specifying certain performance which includes a reference to One-Way Mean Packet Delay Variation, it **MUST** be defined as follows for each Path p between UNIs x and y: Let Δ= {δ1, δ2, δ3, … δn} represent the One-Way Packet Delays of the n Qualified Packets sent from UNI x to UNI y across Path p during a time interval whose duration is the value of the evalinterval element of the SWVC Performance Time Intervals Service Attribute. Let Δ′=the set of all pairs of elements {δr, δs} in Δ such that s>r and the difference in the arrival time at the Ingress UNI of packets s and r equals the of value the arrivalinterval element in the SWVC Performance Time Intervals Service Attribute. If Δ′ is null, then the One-Way Mean Packet Delay Variation for the time interval is zero. Otherwise, let vrs be the absolute value of the

MEF 70.1 Requirement	Testable (T) or Not Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this document	Comments
				difference in One-Way Packet Delay for each pair, {δr, δs} in Δ′, i.e., $vrs=\lvert\delta r-\delta s\rvert$. Then the One-Way Mean Packet Delay Variation for p over that interval is the arithmetic mean of the values vrs for each element in Δ′.

MEF 70.1 Requirement	Testable (T) or Not Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this document	Comments
R151	T	O	8.2	[R151] If the SD-WAN solution rules include a criterion specifying certain performance which includes a reference to One-Way Packet Loss Ratio, it **MUST** be defined as follows for each Path p between UNIs x and y: Let s represent the total number of Qualified Packets sent from UNI x to UNI y across Path p during a time interval whose duration is the value of the evalinterval element of the SWVC Performance Time Intervals Service Attribute. Let r represent the total number of unique (not duplicate) Qualified Packets received from UNI x at UNI y on p that were sent during the same period. Then the One-Way Packet Loss Ratio over that interval for p is defined as follows: If s=0 then the One-Way Packet Loss Ratio is 0. If s>0 then the One-Way Packet Loss Ratio is (s-r)/s

Table 10 – MEF 70.1 Requirements

13 Rating Methodology

The method used to determine the rating for an SD-WAN Edge Vendor solution or an SP SD-WAN Service solution under test use objective methods to provide a rating. Ratings use a 0-to-800-point scale. The point values for each rating are shown in **Table 11**.

Rating	Minimum Points	Maximum Points
AAA	775	800
AA	720	774
A	660	719
BBB	590	659
BB	540	589
B	480	539
CCC	420	479
CC	360	419
C	300	359
D	0	299

Table 11 – Rating Point Values

Each session of testing begins with the allocation of 800 points. for each major section of the testing (Routing and Access Control, SWVC Performance Score, UCS Impairment of SD-WAN SWVC, and SWVC Stability and Reliability). In each area, points are deducted from the 800 points when a test does not perform as specified. A percentage of points is allocated to specific sections of the document. This is shown in **Table 12**. The total points from each section are added up and the sum is divided by 5 to determine the Total Rating and appears on the badge.

Section Number	Total Points	Penalty	Total Points Remaining	Comments
9.1.1		100%		
9.2		25%		
9.4		100%		
9.5		50%		A penalty is assessed for each protocol not supported
	800			
8.1		20%		See the initial MOS penalty
8.2		No penalty		Benchmarking
8.3		No penalty		Benchmarking
8.4		No penalty		Benchmarking
8.5		No penalty		Benchmarking
8.6		No penalty		Benchmarking
8.7		No penalty		Benchmarking
8.8		No penalty		Benchmarking
	NA benchmarking only			
10.1		No penalty		Record values
10.2.1		No penalty		Record values
10.2.2		No penalty		Record values
10.2.3		No penalty		Record values
10.2.4		No penalty		Record values
10.2.5		No penalty		Record values
10.3.1		20%		See MOS penalty (**Table 15**)
10.3.2		20%		See MOS penalty (**Table 15**)
10.4.2		20%		See MOS penalty (**Table 15**)
10.5.1		20%		See MOS penalty (**Table 15**)
10.5.2		20%		See MOS penalty (**Table 15**)
10.5.3		20%		See MOS penalty (**Table 15**)
10.6.1		20%		See MOS penalty (**Table 15**)

Section Number	Total Points	Penalty	Total Points Remaining	Comments
10.7.1.1 10.7.1.2		40% for 1 test not supported 50% for both tests were not supported		Test performed with 60% capacity traffic present
	800			
11.1.1		100%		
11.1.2		100%		
11.1.3		100%		
	800			
Total Rating				

Table 12 – Point Penalty Allocation per Section

As seen in **Table 12**, some testing areas are considered “table stakes” for an SD-WAN Edge Vendor solution or an SP SD-WAN Service solution, and test results that indicate that the expected capabilities are not provided result in a significant penalty.

Other testing areas are considered “nice to have” functions, and a lower penalty is deducted if the test results in these areas are lower than expected.

Editor Note 8: As a part of the Beta testing, the severity of penalties will be reviewed to ensure that they are fair and provide a realistic view of the performance of a solution.

Some testing areas are used as benchmarks for the performance of the SD-WAN Edge Vendor solution, or an SP SD-WAN Service solution compared to other tests that introduce impairments or high loads to determine their impact on the performance. For the benchmarking testing done in section 8.1 a penalty for a measured MOS less than the maximum is assessed. Other tests performed in section 8 are purely benchmarking tests. No points are deducted for these areas.

For MOS assessed for Video, the penalties are defined in Table 13.

MOS	Penalty	Comments
4.53	No penalty	Very Satisfied
4.5	No penalty	Very Satisfied
4.4	No penalty	Very Satisfied
4.3	No penalty	Satisfied
4.2	No penalty	Satisfied
4.1	No penalty	Satisfied
4.0	.5%	Some Users Satisfied
3.9	1.0%	Some Users Satisfied
3.8	1.5%	Some Users Satisfied
3.7	2.0%	Some Users Satisfied
3.63	3.0%	Some Users Satisfied
3.5	4.0%	Many Users Dissatisfied
3.4	5.0%	Many Users Dissatisfied
3.3	6.0%	Many Users Dissatisfied
3.2	7.0%	Many Users Dissatisfied
3.1	8.0%	Many Users Dissatisfied
3.0	9.0%	Nearly All Users Dissatisfied
2.9	10.0%	Nearly All Users Dissatisfied
2.8	11.0%	Nearly All Users Dissatisfied
2.7	12.0%	Nearly All Users Dissatisfied
2.6	13.0%	Nearly All Users Dissatisfied
2.5	14.0%	Not Recommended
2.4	15.0%	Not Recommended
2.3	16.0%	Not Recommended
2.2	17.0%	Not Recommended
2.1	18.0%	Not Recommended
2.0	19.0%	Not Recommended
1.9	20.0%	Not Recommended
1.8	20.0%	Not Recommended
1.7	20.0%	Not Recommended
1.6	20.0%	Not Recommended
1.5	20.0%	Not Recommended
1.4	20.0%	Not Recommended
1.3	20.0%	Not Recommended
1.2	20.0%	Not Recommended
1.1	20.0%	Not Recommended
1.0	20.0%	Not Recommended

Table 13 – Video Initial MOS Penalty

The penalties in Table 13 reflect industry standards for MOS measurements for Video applications. Penalties are not assessed for MOS considered Satisfied or Very Satisfied. Penalties are assessed for MOS considered Some Users Satisfied, Many Users Dissatisfied, Nearly All Users Dissatisfied, and Not Recommended.

The penalties for initial MOS are shown in Table 14.

MOS	Penalty	Comments
4.41	No penalty	Very Satisfied
4.3	No penalty	Very Satisfied
4.2	No penalty	Satisfied
4.1	No penalty	Satisfied
4.0	.5%	Some Users Satisfied
3.9	1.0%	Some Users Satisfied
3.8	1.5%	Some Users Satisfied
3.7	2.0%	Some Users Satisfied
3.63	3.0%	Some Users Satisfied
3.5	4.0%	Many Users Dissatisfied
3.4	5.0%	Many Users Dissatisfied
3.3	6.0%	Many Users Dissatisfied
3.2	7.0%	Many Users Dissatisfied
3.1	8.0%	Many Users Dissatisfied
3.0	9.0%	Nearly All Users Dissatisfied
2.9	10.0%	Nearly All Users Dissatisfied
2.8	11.0%	Nearly All Users Dissatisfied
2.7	12.0%	Nearly All Users Dissatisfied
2.6	13.0%	Nearly All Users Dissatisfied
2.5	14.0%	Not Recommended
2.4	15.0%	Not Recommended
2.3	16.0%	Not Recommended
2.2	17.0%	Not Recommended
2.1	18.0%	Not Recommended
2.0	19.0%	Not Recommended
1.9	20.0%	Not Recommended
1.8	20.0%	Not Recommended
1.7	20.0%	Not Recommended
1.6	20.0%	Not Recommended
1.5	20.0%	Not Recommended
1.4	20.0%	Not Recommended
1.3	20.0%	Not Recommended
1.2	20.0%	Not Recommended
1.1	20.0%	Not Recommended
1.0	20.0%	Not Recommended

Table 14 – Voice Initial MOS Penalty

The penalties in Table 14 reflect industry standards for MOS measurements for Voice applications. Penalties are not assessed for MOS considered Satisfied or Very Satisfied. Penalties are assessed for MOS considered Some Users Satisfied, Many Users Dissatisfied, Nearly All Users Dissatisfied, and Not Recommended.

Table 15 reflects the penalties assessed for degraded MOS results for tests performed.

Δ from Benchmark MOS	**Penalty**	**Comments**
Any Δ from Benchmark MOS that still falls within the acceptable range	0%	
0.1	1%	
0.2	2%	
0.3	3%	
0.4	4%	
0.5	5%	
0.6	6%	
0.7	7%	
0.8	8%	
0.9	9%	
1.0	10%	
1.1	11%	
1.2	12%	
1.3	13%	
1.4	14%	
1.5	15%	
1.6	16%	
1.7	17%	
1.8	18%	
1.9	19%	
2.0	20%	

Table 15 – Δ from Benchmark MOS Penalty

Table 15 reflects the penalty for the delta from the benchmark MOS measurement. When voice or video is tested, a MOS is recorded, and the delta from the benchmark is calculated. The appropriate penalty, up to 20%, is enforced.

Note: A lower MOS that falls within the acceptable range does not incur any penalty.

13.1 MEF Certification Criteria

Pass/Fail criteria have been defined within this section to allow for a MEF Certification. Scores are calculated as described below.

It is proposed that a minimum of 90% of the requirements from MEF 70.1 [6] shown in section 12 as testable mandatory for an SD-WAN Edge Vendor solution or an SD-WAN SP service to be eligible for MEF Certification.

14 References

[1] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, by Scott Bradner, March 1997

[2] IETF RFC 8174, *Ambiguity of Uppercase vs. Lowercase in RFC 2119 Key Words*, by B Leiba, May 2017, Copyright © 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

[3] ITU-T P.10/G.100, *SERIES P: TELEPHONE TRANSMISSION QUALITY, TELEPHONE INSTALLATIONS, LOCAL LINE NETWORKS, SERIES P: TELEPHONE TRANSMISSION QUALITY, TELEPHONE INSTALLATIONS, LOCAL LINE NETWORKS*, 11/27

[4] MEF 41, *Generic Token Bucket Algorithm*, October 2013

[5] MEF 41.0.1, *Amendment to MEF 41: Clarification of Generic Token Bucket Algorithm (GTBA) Behavior*, July 2020

[6] MEF 70.1, SD-WAN Service Attributes and Service Framework, November 2021

Appendix A Acknowledgments (Informative)

The following contributors participated in developing this document and have requested to be included in this list.