MEF 90

SD-WAN Certification Test Requirements

July 2020

Disclaimer

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

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

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

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

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

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

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

Table of Contents

List of Tables

1 List of Contributing Members

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

PCCW Global

Spirent

2 Abstract

The MEF SD-WAN Certification Test Requirements document specifies the testable requirements for the service attributes, functions and capabilities defined in the MEF SD-WAN Attributes and Service Standard (MEF 70 [3]).

The Certification Test Requirements are the basis for development and maintenance of the MEF Authorized Certification Test Partner (ACTP) SD-WAN Certification Test Plans.

As such, the document is an important aid to service providers and technology solution providers to prepare for successful completion of the conformance certification of their products with the MEF 70 standard.

The Test Requirements are also intended to enable standardization of the service level agreement between the SD-WAN service provider and SD-WAN subscriber, which is crucially important for accelerating the market adoption of SD-WAN services.

MEF 70 is the first industry standard definition of an SD-WAN service. It provides an important basis for service providers and technology solution providers to differentiate their service offerings from those of their competitors who may be loosely using the description “SD-WAN” to their customers in a new but rapidly emerging market.

The MEF 3.0 SD-WAN Test Requirements are defined according to the MEF 70 specification and the document determines the conformance of externally visible behavior of SD-WAN services.

3 Terminology and Abbreviations

Terminology and abbreviations used in this document are defined in MEF 70 [3] section 3 and are not repeated here.

Consistent with their use in MEF 70, Policy Criteria names such as ENCRYPTION and Application Flow Criteria names such as SDPORT are shown in all upper case.

4 Compliance Levels

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

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

This document does not contain explicit requirements. All requirements referenced in this document are from MEF 70 [3].

5 SD-WAN Testable Functions and Requirements

The MEF 3.0 SD-WAN Certification Test Requirements document enumerates functions of an SD-WAN that can be tested as part of a certification test and the requirements that describe these functions.

Not every requirement in the SD-WAN Standard is included in the Certification Test Requirements. There are several reasons for this.

First, not all requirements are appropriate to test (for example, determining if an implementation supports the correct format for an Identifier String provides little value in a certification test).

More importantly, not all functionality and requirements are testable. Many items such as SWVC Service Uptime represent an agreement between the Service Provider and Subscriber. However, verification that Service Uptime is computed correctly is based on the Performance Evaluation Interval, which is not defined in MEF 70. Similarly, functions that define the relationships between the SD-WAN Service abstractions (SWVC, SWVC End Point, UNI) such as the list of End Points associated with an SWVC or the identifier of the UNI at which an end point is located do not represent implemented functions that are readily measurable.

This section lists the requirements in MEF 70 which are identified as R###[N or T]. Each requirement is specified with either "T" which indicates that it is testable (and worth testing) or "N" which indicates that it is not testable (or not worth testing), for example, R1[N]. The text of the standard contains some informative text that describes behavior that is testable. Tests based on such text is labeled as INFx_y[T] in this document where x_y indicates the section in MEF 70.

6 Requirements Coverage

Each requirement in the specification is evaluated as being either Testable or Not Testable. Section 7 of this document has subsections for each major functional area of MEF 70 [3] and the requirements associated with each.

The following table lists all of the requirements and where each of them is discussed in section 7.

Requirement	Testable	Section	Notes
R1	N	7.2.1	
R2	N	7.2.1	
R3	Y	7.3.1	
R4	Y	7.3.2	
R5	Y	7.3.3	
R6	Y	7.3.4	
R7	N	7.4	
R8	N	7.4	
R9	N	7.4	
R10	N	7.5	
R11	N	7.5	
R12	N	7.5	
R13	Y	7.5	
R14	N	7.6	
R15	N	7.6	
R16	N	7.3.5	
R17	N	7.7.3	
R18	N	7.7.3	
R19	N	7.7.5	
R20	N	7.7.5	
R21	N	7.7.5	
R22	Y	7.7.2	
R23	Y	7.7.1	
R24	Y	7.7.1	
R25	Y	7.7.1	
R26	Y	7.7.1	
R27	Y	7.7.1	
R28	Y	7.7.1	
R29	Y	7.7.1	
R30	Y	7.7.1	
R31	Y	7.7.1	
R32	Y	7.7.1	
R33	Y	7.7.1	
R34	Y	7.7.1	
R35	Y	7.7.1	
R36	Y	7.7.1	

R37	Y	7.7.1	
R38	N	7.8	
R39	N	7.8	
R40	N	7.8	
R41	N	7.9.1	
R42	N	7.9.1	
R43	Y	7.9.3	
R44	Y	7.9.4	
R45	Y	7.9.6	Specific tests for R45 are not needed since this functionality will be verified as part of R43 and R46 testing.
R46	Y	7.9.2	
R47	N	7.9.1	
R48	Y	7.9.5	
R49	N	7.4	
R50	N	7.4	
R51	Y	7.10.1	
R52	Y	7.10.1	
R53	Y	7.10.1	
R54	Y	7.10.2	
R55	Y	7.10.3	
R56	Y	7.10.4	
R57	N	7.4	
R58	N	7.4	
R59	Y	7.12.2	
R60	Y	7.13.1	Specific tests for R60 are not needed since this functionality will be verified as part of the R59 testing.
R61	Y	7.14.1	
R62	Y	7.14.2	
R63	Y	7.14.3	Specific tests for R63 are not needed since this functionality will be verified as part of the R62 testing.
R64	N	7.14.4	
R65	N	7.14.4	
R66	Y	7.15.1	
R67	N	7.15.4	
R68	Y	7.15.2	
R69	Y	7.15.3	
R70	N	7.15.4	

Table 1 - MEF 70 Requirements Coverage

7 Test Requirements

7.1 Basic IP Router Functions

An SD-WAN Service as described in MEF 70 is an IP service and therefore the SD-WAN Edge must perform basic IP router functions. This set of tests will ensure that the SD-WAN Edge operates correctly as an IP Router on behalf of the Subscriber. Many of these tests are covered in the IP Forwarding section 7.3.

7.2 UNI Ownership and Association

7.2.1 R1[N] and R2[N]

The requirements describe that UNIs are associated with a single Service Provider and Single Subscriber.

7.3 IP Forwarding

7.3.1 R3[T]

R3 indicates that packets must not be delivered to a UNI if the destination is not reachable at that UNI.

7.3.1.1 Test R3.1

Set up 3 UNIs with IP address prefixes and inject a packet to one of the destinations and ensure that it is delivered only to the correct UNI.

7.3.1.2 Test R3.2

Set up 3 UNIs with IP address prefixes and inject a packet to an unknown destination and ensure that it is not delivered to any UNI.

7.3.1.3 Test R3.3

Set up 3 UNIs with two destination UNIs with overlapping IP addresses and one of the destination UNIs has a longer, more specific, prefix length than the other destination UNI. Inject a packet with a destination IP address in the overlapping range and ensure that it is delivered to the destination UNI with the more specific address based on the longest prefix matching.

7.3.2 R4[T]

R4 provides requirements for IPv4 transparency for non-fragmented packets.

7.3.2.1 Test R4.1

Send IPv4 packets below or at IP MTU of the UNI, the TVC and UCS with no Loose, Strict, or Record options and verify that only proper fields (according to R4) are changed.

7.3.2.2 Test R4.2

Send IPv4 packets below or at IP MTU of the UNI, the TVC and UCS with Loose and Record options and verify that only proper fields (according to R4) are changed if those options are supported by the device under test and the device under test is configured to forward IPv4 packets with those options.

7.3.2.3 Test R4.3

Send IPv4 packets below or at IP MTU of the UNI, the TVC and UCS with Loose and Record options and verify that packets are dropped if those options are not supported by the device under test or the device under test is configured to drop IPv4 packets with those options.

7.3.2.4 Test R4.4

Send IPv4 packets below or at IP MTU of the UNI, the TVC and UCS with Strict and Record options and verify that only proper fields (according to R4) are changed if those options are supported by the device under test and the device under test is configured to forward IPv4 packets with those options.

7.3.2.5 Test R4.5

Send IPv4 packets below or at IP MTU of the UNI, the TVC and UCS with Strict and Record options and verify that packets are dropped if options are not supported by the device under test or device under test is configured to drop IPv4 packets with those options.

7.3.2.6 Test R4.6

Send IPv4 packets below or at IP MTU of the UNI, the TVC and UCS with Record option and verify that only proper fields (according to R4) are changed if the Record option is supported by the device under test and the device under test is configured to forward IPv4 packets with the option.

7.3.2.7 Test R4.7

Send IPv4 packets below or at IP MTU of the UNI, the TVC and UCS with Record option and verify that packets are dropped if the Record option is not supported by the device under test or the device under test is configured to drop IPv4 packets with the option.

7.3.3 R5[T]

R5 provides requirements for IPv4 transparency for fragmented packets when IPv4 packet size including overhead exceeds the IP MTU of TVC or UCS UNI. Support for fragmentation and reassembly at TVC or UCS UNI is optional. Fragmentation and reassembly at the TVC and UCS UNI should be tested separately. Testing fragmentation and reassembly at both the TVC (IP MTU of UNI exceeds IP MTU of TVC) and UCS UNI (IP MTU of TVC exceeds the IP MTU of UNI) is out scope of this document and is not a test requirement. Testing fragmentation and reassembly by subscriber networks at the UNI when IPv4 packet size exceeds the IP MTU of the UNI is out scope of this document and is not a requirement.

7.3.3.1 Test R5.1

Send IPv4 packets that exceed the IP MTU of the TVC with no Loose, Strict, or Record options and verify that only proper fields (according to R4) are changed if the device under test supports IPv4 packet fragmentation and reassembly at the TVC.

7.3.3.2 Test R5.2

Send IPv4 packets that exceed the IP MTU of the UCS UNI with no Loose, Strict, or Record options and verify that only proper fields (according to R4) are changed if the device under test supports IPv4 packet fragmentation and reassembly at the TVC at the UCS UNI.

7.3.3.3 Test R5.3

Send IPv4 packets that exceed the IP MTU of the TVC with Loose and Record options and verify that only proper fields (according to R4) are changed if those options and packet fragmentation/reassembly at TVC are supported by the device under test and the device under test is configured to forward IPv4 packets with those options.

7.3.3.4 Test R5.4

Send IPv4 packets that exceed the IP MTU of the TVC with Loose and Record options and verify that packets are dropped if those options or packet fragmentation/reassembly at TVC are not supported by the device under test or the device under test is configured to drop IPv4 packets with those options.

7.3.3.5 Test R5.5

Send IPv4 that packets exceed the IP MTU of the UCS UNI with Loose and Record options and verify that only proper fields (according to R4) are changed if those options and packet fragmentation/reassembly at UCS UNI are supported by the device under test and the device under test is configured to forward IPv4 packets with those options.

7.3.3.6 Test R5.6

Send IPv4 packets that exceed the IP MTU of the UCS UNI with Loose and Record options and verify that packets are dropped if those options or packet fragmentation/reassembly at UCS UNI are not supported by the device under test or the device under test is configured to drop IPv4 packets with those options.

7.3.3.7 Test R5.7

Send IPv4 packets that exceed the IP MTU of the TVC with Strict and Record options and verify that only proper fields (according to R4) are changed if those options and packet fragmentation/reassembly at TVC are supported by the device under test and the device under test is configured to forward IPv4 packets with those options.

7.3.3.8 Test R5.8

Send IPv4 packets that exceed the IP MTU of the TVC with Strict and Record options and verify that packets are dropped if options or packet fragmentation/reassembly at TVC are not supported by the device under test or device under test is configured to drop IPv4 packets with those options.

7.3.3.9 Test R5.9

Send IPv4 packets that exceed the IP MTU of the UCS UNI with Strict and Record options and verify that only proper fields (according to R4) are changed if those options and packet fragmentation/reassembly at UCS UNI are supported by the device under test and the device under test is configured to forward IPv4 packets with those options.

7.3.3.10 Test R5.10

Send IPv4 packets that exceed the IP MTU of the UCS UNI with Strict and Record options and verify that packets are dropped if options or packet fragmentation/reassembly at UCS UNI are not supported by the device under test or device under test is configured to drop IPv4 packets with those options.

7.3.3.11 Test R5.11

Send IPv4 packets that exceed the IP MTU of the TVC with Record option and verify that only proper fields (according to R4) are changed if the Record option and packet fragmentation/reassembly at TVC are supported by the device under test and the device under test is configured to forward IPv4 packets with the option.

7.3.3.12 Test R5.12

Send IPv4 packets that exceed the IP MTU of the TVC with Record option and verify that packets are dropped if the Record option or packet fragmentation/reassembly at TVC are not supported by the device under test or the device under test is configured to drop IPv4 packets with the option.

7.3.3.13 Test R5.13

Send IPv4 packets that exceed the IP MTU of the UCS UNI with Record option and verify that only proper fields (according to R4) are changed if the Record option and packet fragmentation/reassembly at UCS UNI are supported by the device under test and the device under test is configured to forward IPv4 packets with the option.

7.3.3.14 Test R5.14

Send IPv4 packets that exceed the IP MTU of the UCS UNI with Record option and verify that packets are dropped if the Record option or packet fragmentation/reassembly at UCS UNI are not supported by the device under test or the device under test is configured to drop IPv4 packets with the option.

7.3.4 R6[T]

R6 provides requirements for IPv6 transparency. IPv6 support at SD-WAN UNI interface is considered as optional if IPv4 is enabled at the UNI interface. IPv6 support at TVC and UCS is also optional.

7.3.4.1 Test R6.1

Send IPv6 packet at MTU with no Hop-by-Hop Options header options and verify that only proper fields (according to R6) are changed.

7.3.4.2 Test R6.2

Send IPv6 packet at MTU with Hop-by-Hop Options header that have the third high-order bit in the option type field set and verify that only proper fields (according to R6) are changed.

7.3.5 R16[N]

R16 describes Service Provider reserved IP Prefixes.

7.4 Identifier Strings

- R7[N] Construction of an Identifier String
- R8[N] and R9[N] SWVC Identifier
- R49[N] and R50[N] SWVC End Point Identifier
- R57[N] and R58[N] UNI End Point Identifier

7.5 SWVC End Point Association

R10[N], R11[N], R12[N], R13[N] describe the association of End Points and SWVC.

7.5.1 R13[T]

Set up two UNIs, UNI 1 and UNI 2, in SWVC 1 and another two UNIs, UNI 3 and UNI 4, in SWVC 2. UNI 1 and UNI 3 use the same IP addresses. UNI 2 and UNI 4 use the same IP addresses.

Send IP packets from UNI 1 to UNI 2 in SWVC 1 and ensure that the IP packets are only received by UNI 2 in SWVC1 and the IP packets are not delivered to UNI 4 in SWVC 2.

7.6 Service Uptime – SWVC Service Uptime Service Attribute

R14[N] and R15[N] defines how Service Uptime is computed and how the Objective is determined.

7.7 Policies – SWVC List of Policies Service Attribute

This section covers the requirements associated with Policy definition. Tests for R23 – R37 should be executed first in order to ensure that each Policy Criterion individually (without using other

Policy Criteria) selects the correct UCS. At least three of the six Policy Criteria specified in MEF 70 must be supported.

Note: For service provider live network testing, it is not required for all SD-WAN Edge/SWVC End Points to have a minimum of two UCSs, and to have both PUBLIC and PRIVATE UCSs. For example, it is acceptable that one of the sites only has one UCS of PUBLIC type. It is still required that at least one of the sites has both PUBLIC UCS and PRIVATE UCS (with one or more sites that are reachable by PUBLIC UCS, and one more sites that are reachable by PRIVATE UCS) if the service provider chooses to test with PUBLIC-PRIVATE policy criterion.

Also, policy attributes can be tested with Application Flows that originate at any site. For example, if site A does not have a private UCS, but site B and site C have both public UCS and private UCS, then instead of sending application flow from site A to site B, the policy attribute of PUBLIC-PRIVATE can be tested by sending an application flow from site B to site C.

7.7.1 R23[T] through R37[T]

These requirements describe the rules associated with each of the Policy Criteria defined in Table 3, Section 8.5 in MEF 70 [3]. Although it is not required that an implementation support all of the Policy Criteria, tests can be developed to determine whether the supported Policy Criteria behave correctly. For each of the Policy Criteria, verify that each of the allowed values selects an Underlay Connectivity Service (UCS) that is configured with the characteristic that matches the Policy Criterion value.

7.7.2 R22[T]

R22 indicates that an IP Packet can only be forwarded over the SD-WAN Service if the destination is reachable, and all of the Policy Criteria in the matched Policy are met, or one the criteria is INTERNET-BREAKOUT and it is enabled in the matched Policy. It must be discarded, if not.

7.7.2.1 Test R22.1

Define a policy that has two or more criteria enabled and none of the criteria is INTERNET-BREAKOUT. Assign the policy to an Application Flow. Set up multiple UCSs with IP reachability to the destination and only one of UCS matches all criteria. Verify that the only Underlay Connectivity Service that meets all criteria is selected for that Application Flow.

This is a sequence of tests that determine whether combinations of Policy Criteria are supported correctly.

7.7.2.2 Test R22.2

Define a policy that has two or more criteria enabled and none of the criteria is INTERNET-BREAKOUT. Assign the policy to an Application Flow. Set up one or more UCSs with IP reachability to the destination but none of the UCSs matches all criteria. Set up another UCS that matches all criteria but does not have IP reachability to the destination. Verify that the only Underlay Connectivity Service that meets all the criteria is selected for that Application Flow and packets are dropped as the destination is not reachable.

7.7.2.3 Test R22.3

Define a policy that has INTERNET-BREAKOUT and one other criterion enabled. Assign the policy to an Application Flow. Set up multiple UCSs with IP reachability to the destination and only one of UCS matches INTERNET-BREAKOUT criterion, and the same UCS also matches the other criterion. Verify that the only Underlay Connectivity Service that meets the INTERNET-BREAKOUT criterion is selected for that Application Flow.

7.7.2.4 Test R22.4

Define a policy that has INTERNET-BREAKOUT and one other criterion enabled. Assign the policy to an Application Flow. Set up multiple UCSs with IP reachability to the destination and only one of UCS matches INTERNET-BREAKOUT criterion, and the same UCS does not match the other criterion. Verify that the only Underlay Connectivity Service that meets the INTERNET-BREAKOUT criterion is selected for that Application Flow and the other criterion is ignored.

7.7.2.5 Test R22.5

Define a policy that has one or more criteria enabled and none of the criteria is ENCRYPTION. Assign the policy to an Application Flow. Set up multiple UCSs with IP reachability to the destination and none of UCS matches all criteria. Verify that none of the Underlay Connectivity Service is selected for that Application Flow and packets are dropped.

7.7.2.6 Test R22.6

Define a policy that one of the criteria is ENCRYPTION and it is enabled, and the other criteria is PUBLIC-PRIVATE and its value is set to *Private-Only*. Assign the policy to an Application Flow. Set up an environment so that encryption is only available over a Public network. The Application Flow should not be forwarded as encryption is not available over Private network.

7.7.2.7 Test R22.7

Define a policy that one of the criteria is ENCRYPTION and it is enabled, and the other criteria is PUBLIC-PRIVATE and its value is set to "*Public-Only"*. Assign the policy to an Application Flow. Set up an environment so that encryption is only available over a Public network. The Application Flow should be forwarded to the UCS that goes over the Public network.

Note: For service provider live network testing, it is acceptable to use statistics or packet capture on the device under test to verify if packets are properly encrypted or decrypted.

7.7.2.8 Test R22.8

Define a policy that has BACKUP and one other criterion enabled. Assign the policy to an Application Flow. Set up multiple UCSs with IP reachability to the destination. All UCSs meet the other criterion and only one of UCS is designated as Backup. Verify that the Underlay Connectivity Service that is designated as the Backup is not selected for that Application Flow.

7.7.2.9 Test R22.9

Define a policy that has BACKUP and one other criterion enabled. Assign the policy to an Application Flow. Set up multiple UCSs with IP reachability to the destination. All UCSs meet the other criterion and only one of UCS is designated as Backup. Change the network topology so that only the UCS that is designated as Backup has IP reachability to the destination. Verify that the Underlay Connectivity Service that is designated as the Backup is selected for that Application Flow.

7.7.2.10 Test R22.10

Define a policy that has two or more criteria and BACKUP is not one of the criteria. Assign the policy to an Application Flow. Set up multiple UCSs with IP reachability to the destination. All UCSs meet all other criteria and only one of UCS is designated as BACKUP. Change the network topology so that only the UCS that is designated as Backup has IP reachability to the destination. Verify that the Underlay Connectivity Service that is designated as the Backup is not selected for that Application Flow.

7.7.2.11 Test R22.11

Define a policy that has two or more criteria and only one of the criteria is set to *Either*. Assign the policy to an Application Flow. Set up a UCS that meets all criteria with IP reachability to the destination. Verify the Underlay Connectivity Service that is selected for that Application Flow.

7.7.2.12 Test R22.12

Define a policy that has two or more criteria and only one of the criteria is set to *Either*. Assign the policy to an Application Flow. Set up a UCS that meets all other criteria with IP reachability to the destination except the criterion with the *Either* value. Verify the Underlay Connectivity Service that is selected for that Application Flow.

*7.7.2.13 Test R22.13-**

Run tests with other combinations of support Policy Criteria and verify that the behavior is as expected.

7.7.3 R17[N] and R18[N]

These describe the construction of a Policy.

7.7.4 D1[N]

Table 3 in MEF 70 [3] defines a set of policies that may be supported. If supported the tests are covered in [R23] - [R37].

7.7.5 R19[N], R20[N], and R21[N]

These describe requirements for constructing Policy Criteria definitions.

7.7.6 R35[T], R36[T], and R37[T]

Set up three Application Flows with the same IP destination. For each Application Flow, assign a policy that includes the BANDWDITH criterion with a committed traffic rate and a maximum traffic rate. Set up one UCS that matches policies for all the Application Flows with IP reachability to the destination. Set up the UCS so that the bandwidth of the UCS exceeds the sum of the committed bandwidth of all Application Flows but is lower than the sum of maximum bandwidth of all Application Flows.

7.7.6.1 Test R35

For each Application Flow, send traffic below the committed rate simultaneously over the same Underlay Connectivity Service. Traffic for all three application flows MUST be forwarded without any packet drop.

7.7.6.2 Test R36.1

For all three Application Flows, send traffic above the committed rate but below the maximum rate simultaneously over the same Underlay Connectivity Service. Set up the UCS so that the bandwidth of the UCS exceeds the sum of the traffic rates of all Application Flows. The minimum throughput for each Application Flow should exceed or equal its committed rate. For each Application Flow, traffic above the committed rate but below the maximum rate MAY be marked or dropped.

7.7.6.3 Test R36.2

For all three Application Flows, send traffic above the committed rate but below the maximum rate simultaneously over the same Underlay Connectivity Service. Set up the UCS so that the bandwidth of the UCS is lower than the sum of the traffic rates of all Application Flows. The minimum throughput for each Application Flow should exceed or equal its committed rate. For each Application Flow, traffic above the committed rate but below the maximum rate MAY be marked or dropped. Packet drop is expected.

7.7.6.4 Test R37

For each Application Flow, send traffic above the maximum rate simultaneously over the same Underlay Connectivity Service. The minimum throughput for each application flow should exceed or equal its committed rate. For each Application Flow, traffic above the maximum rate MUST be dropped.

7.8 Application Flow Groups – SWVC List of Application Flow Groups SA

R38[N] and R39[N] and R40[N] describe the definition/creation of Application Flow Groups. These are not directly testable but are necessary for testing Application Flows and Policies.

7.9 Application Flows – SWVC List of Application Flows Service Attribute

This section describes the composition of Application Flows from Application Flow Criterion and additional rules associated with how ingress IP Packets are associated with Application Flows.

The tests should be executed in the following order:

- Tests for R46
- Tests for R43
- Tests for R44
- Tests for R48

7.9.1 R41[N], R42[N], and R47[N]

These requirements define how Application Flows are specified.

7.9.2 R46[T]

R46 identifies the list of Application Flow criteria that must be supported.

7.9.2.1 Test R46.1 – R46.n

For each Application Flow Criterion, define an Application Flow with the criterion and generate a sequence of packets that match and do not match the criterion. Ensure that the delivered packets match the Application Flow Criterion (Application Flow Criteria that support a list should be tested for a single value and multiple values.)

7.9.3 R43[T]

R43 requires that an IP Packet must match all of the criteria in the Application Flow definition.

Notes:

- MEF SD-WAN service can be IPv4, or IPv6, or dual stack. IPv4 related Application Flow criteria are considered as mandatory if IPv4 service is offered in IPv4 at the UNIs. IPv6 Application Flow criteria are considered as mandatory if IPv6 service is offered at the UNIs.
- IPv4 related Application Flow criteria are considered as optional if IPv4 is not enabled at any of the UNIs. IPv6 Application Flow criteria are considered as optional if IPv6 is not enabled at any of the UNIs.
- Support for Ethertype Application Flow criterion is considered as optional.
- For PROTV4 IPv4 Protocol List Application Flow criterion, support for TCP, UDP and ICMP protocols is mandatory. Support for other protocols is considered as optional.
- For NEXTHEADv6 IPv6 Next Header Protocol List Application Flow criterion, support for TCP, UDP and ICMPv6 protocols is considered as mandatory. Support for other protocols is considered as optional.
- For PROTV4 IPv4 Protocol List Application Flow criterion, it is considered as mandatory to test an Application Flow definition that can match IPv4 packets with two different protocols (TCP and UDP) at the same time. Matching more than two different protocols with the PROTV4 IPv4 Protocol List Application Flow criterion is considered as optional.

- For NEXTHEADv6 IPv6 Next Header Protocol List Application Flow criterion, it is considered as mandatory to test an Application Flow definition that can match IPv6 packets with two different protocols (TCP and UDP) at the same time. Matching more than two different protocols with the NEXTHEADv6 IPv6 Next Header Protocol List Application Flow criterion is considered as optional.
- Support for SDPORT (TCP/UDP Source or Destination Port List) Application Flow criterion is considered as optional.
- For DPORT TCP/UDP Destination Port List Application Flow criterion, it is considered as mandatory to support well-known and widely used ports such as SMTP(25), HTTP(80), HTTPS(443), FTP(20, 21), IMAP(143), SSH(22), TELNET(23), DNS(53), NTP(123), and POP3(110).
- TCP Application Flows are stateful and TCP sessions are initiated by clients with an ephemeral source port and a well-known destination port. UDP Application Flows are connectionless. For SPORT TCP/UDP Source Port List Application Flow criterion, it is considered as optional to match ephemeral source ports. It is considered acceptable to have clients to initiate TCP or UDP connections to a server before "SPORT TCP/UDP Source Port List" Application Flow criterion is used to match the Application Flows from server to clients.
- It is considered acceptable to use DPI/Layer 7 application template as an alternative to match Application Flows with TCP/UDP source port or destination port.

7.9.3.1 Test R43.1

Define an Application Flow with any two criteria (except ANY) defined in MEF 70 [3], a trivial policy and generate a sequence of packets that match both criteria, one of the criteria, and none of the criteria. Ensure that only packets that match both Application Flow Criteria are delivered to the destination.

7.9.3.2 Test R43.2

Define an Application Flow with any three criteria (except ANY) defined in MEF 70, a trivial policy and generate a sequence of packets that match all three criteria, one or two of the criteria, and none of the criteria. Ensure that only packets that match all three Application Flow Criteria are delivered to the destination.

7.9.3.3 Test R43.3

Define an Application Flow with DPORT and DAV4, a trivial policy and generate a sequence of packets that match both DPORT and DAV4, match DPORT but not DAV4, match DPORT but not DAV4, and do not match DPORT nor DAV4. Ensure that the delivered packets match all Application Flow Criteria, that is, match both DPORT and DAV4.

7.9.3.4 Test R43.4

Define an Application Flow with DPORT, DAV4, and SPORT, a trivial policy and generate a sequence of packets that match all criteria, match some of the criteria, and do not match any of the criteria. Ensure that the delivered packets match all Application Flow Criteria, that is, match DPORT, DAV4, and SPORT.

7.9.3.5 Test R43.5

Define an Application Flow with DPORT and DAV6, a trivial policy and generate a sequence of packets that match both DPORT and DAV6, match DPORT but not DAV6, match DPORT but not DAV6, and do not match DPORT nor DAV6. Ensure that delivered packets match all Application Flow Criteria, that is, match both DPORT and DAV6.

7.9.3.6 Test R43.6

Define an Application Flow with DPORT, DAV6, and SPORT, a trivial policy and generate a sequence of packets that match all criteria, match some of the criteria and do not match any of the criteria. Ensure that delivered packets match all Application Flow Criteria, that is, match DPORT, DAV6 and SPORT.

7.9.3.7 Test R43.7

Define an Application Flow with SDPORT and SDAV4, a trivial policy and generate a sequence of packets that match both DPORT and DAV4, match both DPORT and SAV4, match both SPORT and DAV4, match both SPORT and SAV4, match DPORT but not DAV4, match DPORT but not SAV4, match SPORT but not DAV4, match SPORT but not SAV4, and do not match DPORT, nor SPORT, nor DAV4, nor SAV4. Ensure that delivered packets match all Application Flow Criteria, that is, match either DPORT or SPORT, and either DAV4 or SAV4.

7.9.3.8 Test R43.8

Define an Application Flow with SDPORT and SDAV6, a trivial policy and generate a sequence of packets that match both DPORT and DAV6, match both DPORT and SAV6, match both SPORT and DAV6, match both SPORT and SAV6, match DPORT but not DAV6, match DPORT but not SAV6, match SPORT but not DAV6, match SPORT but not SAV6, and do not match DPORT, nor SPORT, nor DAV6, nor SAV6. Ensure that delivered packets match all Application Flow Criteria, that is, match either DPORT or SPORT, and either DAV6 or SAV6.

7.9.3.9 Test R43.9

Define an Application Flow with all criteria (except for ANY) defined in MEF70, a trivial policy and generate a sequence of packets that match all criteria, some of the criteria, and none of the criteria. Ensure that delivered packets match all Application Flow Criteria.

7.9.4 R44[T]

R44 describes that the list of Application Flow definitions is “ordered”, and an IP Packet is associated with the Application Flow that it matches first in the list. This disambiguates the behavior in the case where an IP Packet could match multiple Application Flows.

7.9.4.1 Test R44.1

Create two Application Flows where one of them is a subset of the other (e.g., DPORT 80 and DPORT 80/SAV4 a.b.c.d). Apply a different Policy to each Application Flow that allows distinguishing the flows. Examples are PUBLIC-PRIVATE or using BANDWIDTH (e.g., 20/20

and 40/40 with offered flow of each greater than the specified max). Specify the Application Flows in both orders and ensure that the behavior is as expected.

7.9.5 R48[T]

R48 is a requirement on how the Application Flow ANY is used.

7.9.5.1 Test R48.1

Rerun one test from R46.* with the inclusion of ANY as a second Application Flow definition. Run a discrimination test as described in test R44.1 to verify that the two flows (specific and ANY) are recognized and get the appropriate Policy.

Define an Application Flow with two or more criteria with ANY being one of the criteria, a trivial policy and generate a sequence of packets that match all of the non-ANY criteria, some of the non-ANY criteria, and none of the non-ANY criteria. Ensure all packets are delivered.

7.9.6 R45[T]

R45 indicates that an IP Packet that cannot be associated with an Application Flow must be discarded.

No test needed since this will be shown in the R46 and R43 tests

7.10 Assigning Policies to Application Flows – SWVC End Point Policy Map Service Attribute

7.10.1 R51[T], R52[T], R53[T]

R51, R52, and R53 indicate how Policies can be assigned to both Application Flows and Application Flow Groups and an SWVC End Point.

7.10.2 R54[T]

R54 indicates that a Policy assigned to an Application Flow supersedes (for that Application Flow) a Policy assigned to the Application Flow Group to which the Application Flow belongs.

Set up an Application Flow that is a member of an Application Flow Group. Assign a policy to the Application Flow. Assign another policy to the Application Flow Group. Set up one UCS with IP reachability to the destination that matches the policy for the Application Flow. Set up another UCS with IP reachability to the destination that matches the policy for the Application Flow Group. Verify that the Underlay Connectivity Service matches the policy for the Application Flow is selected.

7.10.3 R55[T]

R55 indicates that an Application Flow that is not assigned a Policy at an SWVC End Point is discarded at that End Point (i.e., not forwarded over the SD-WAN).

Define an Application Flow. Do not assign any Policy to it. Verify that all packets matching the Application Flow are dropped at the UNI and not forwarded over the SD-WAN.

7.10.4 R56[T]

R56 indicates that if the reserved Policy named "block" is mapped to an Application Flow, the Application Flow must be discarded.

Define a Policy with the reserved Policy name "block" and has one or more criteria enabled. Assign the Policy to an Application Flow. Set up one or more UCSs with IP reachability to the destination that matches all criteria in the Policy. Verify that all packets matching the Application Flow are dropped at the UNI.

7.11 UNI L2 Interface Service Attribute

This Service Attribute describes the L2 frames that are accepted at the SD-WAN UNI and handed off to one or more UNIs.

Test order should be:

- Tests for INF10_2
- Test for R59
- Tests for D2

7.12 INF10_2

Section 10.2 requires each SD-WAN UNI to accept Ethernet frames with a specific C-VLAN ID value or untagged and priority tagged (UT/PT) frames.

Note: Support for priority tagged frames (with VLAN ID 0) at SD-WAN UNI interface is optional.

7.12.1.1 Test INF10_2.1

Configure system to deliver UT/PT frames to the SD-WAN Service and generate a sequence UT, PT, and C-VLAN tagged frames and ensure that only the UT and PT frames are accepted by the Service.

7.12.1.2 Test INF10_2.2

Configure system to deliver CVLAN "x" to the SD-WAN Service and generate a sequence of UT, PT, and C-VLAN tagged frames with multiple C-VLAN values and ensure that only frames with CVLAN x are accepted by the Service.

7.12.2 R59[T]

R59 indicates that only well-formed Ethernet MAC frames can be accepted at the UNI.

7.12.2.1 Test R59.1

Generate a sequence of Ethernet frames from 64 bytes to 1522 bytes with correct FCS and ensure that all are accepted and forwarded correctly.

7.12.2.2 Test R59.2

Generate a few frames with incorrect FCS and ensure that they are discarded.

7.12.2.3 Test R59.3

Generate a few frames smaller than 64 bytes and ensure that they are discarded.

7.12.2.4 Test R59.4

Generate a 64-byte frame with a C-tag and forward it to a UNI that is UT/PT. Ensure that the resulting frame is padded to 64 bytes before transmission.

7.13 UNI L2 Maximum Frame Size Service Attribute

7.13.1 R60[T]

R60 requires that the SD-WAN must support Ethernet frames up to, at least, 1522 bytes.

Configure the device under test with L2 Maximum Frame Size set to 1522 bytes and then send frames at 1522 bytes with correct FCS and ensure that all frames are accepted and forwarded correctly.

7.13.2 D2[T]

Requirement D2 indicates that a frame that exceeds the L2 Maximum Frame Size should be discarded. This is an optional test requirement as the test will always pass regardless of the result.

7.13.2.1 Test D2.1

Configure the device under test with L2 Maximum Frame Size set to 1522 bytes (usually default) and then send frames larger than 1522 bytes and record the results (discard or forward).

7.14 IPv4 Connection Addressing

7.14.1 R61[T]

R61 indicates that only one of the IPv4 and IPv6 Connection Addressing Service Attributes can have the value None. In other words, an implementation must include either IPv4 or IPv6 support at the UNI or both.

This is just a documentation requirement. The other tests will verify.

7.14.2 R62[T]

R62 describes how DHCP must be supported.

7.14.2.1 Test R62.1

A DHCP request is be sent to the Service Provider and the response will be inspected to ensure that it includes an IPv4 address from a prefix that meets the requirements of R63 (i.e., that it is from one of the primary or secondary prefixes allocated to the UNI and that it is from one of the prefixes in the SWVC Reserved Prefixes) and that the response includes an IP subnet mask, and IP default router address.

7.14.3 R63[T]

R62 describes how DHCP must be supported. An explicit test of R63 is not needed since it is included in Test R62.1.

7.14.4 R64[N] and R65[N]

R64 and R65 describe how Static and DHCP addressing must be supported and are not testable.

7.15 IPv6 Connection Addressing

T[Rxx] If IPv6 is supported, one or more of the following capabilities must be supported: DHCP, SLAAC, Static, or LL-only.

This is a documentation requirement. The other tests will verify.

7.15.1 R66[T]

R66 describes how DHCP must be supported.

7.15.1.1 Test R66.1

A DHCP request will be sent to the Service Provider and the response will be inspected to ensure that it includes an IPv6 address from a prefix that meets the requirements of R68 (i.e., that it is from one of the IPv6 prefixes allocated to the UNI and that it is from one of the prefixes in the SWVC Reserved Prefixes) and that the response includes an IP subnet mask.

7.15.2 R68[T]

An explicit test of R68 is not needed since it is included in Test 66.1.

7.15.3 R69[T]

R69 describes how SLAAC must be supported.

7.15.3.1 Test R69.1

The UNI is monitored for prefix advertisements and a received advertisement is verified against the first IP Prefix assigned to the UNI.

7.15.4 R67[N] and R70[N]

R67 and R70 describe additional requirements for DHCP, Static Address, and SLAAC support and are not testable.

8 References

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

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

[3] MEF 70, *SD-WAN Service Attributes and Services*, July 2019