



**MEF Standard**  
**MEF 70.1**

**SD-WAN Service Attributes and Service Framework**

**November 2021**

## Disclaimer

© MEF Forum 2021. All Rights Reserved.

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. This document is provided “as is” with no warranties whatsoever, express or implied, including without limitation, any warranties of merchantability, non-infringement, accuracy, completeness or fitness for any particular purpose. MEF and its members disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this document.

## Table of Contents

<b>1</b>	<b>List of Contributing Members .....</b>	<b>1</b>
<b>2</b>	<b>Abstract.....</b>	<b>2</b>
<b>3</b>	<b>Terminology and Abbreviations.....</b>	<b>3</b>
<b>4</b>	<b>Compliance Levels .....</b>	<b>7</b>
<b>5</b>	<b>Document Conventions.....</b>	<b>7</b>
5.1	Numerical Prefix Conventions .....	7
5.2	Notational Conventions .....	7
5.3	Diagram Conventions .....	8
<b>6</b>	<b>Introduction.....</b>	<b>9</b>
6.1	Document Scope.....	9
6.2	Characteristics of an SD-WAN Service .....	10
6.3	Organization of the Standard .....	11
<b>7</b>	<b>Key Concepts, Definitions, and Conventions .....</b>	<b>12</b>
7.1	Service Attributes .....	12
7.2	SD-WAN Service Components Overview .....	12
7.3	SD-WAN Subscriber and SD-WAN Service Provider.....	13
7.4	SD-WAN UNI .....	14
7.5	Subscriber Network and Service Provider Network.....	16
7.6	Underlay Connectivity Service, UCS UNI, and UCS End Point .....	16
7.7	Tunnel Virtual Connection (TVC) .....	18
7.8	SD-WAN Virtual Connection and SWVC End Point .....	20
7.9	Application Flow, Application Flows Specifications, and Policies .....	20
7.10	Zone .....	21
7.11	Virtual Topology .....	22
7.12	Internet Breakout .....	23
7.13	SD-WAN Edge.....	24
7.14	SD-WAN Services Framework .....	25
7.15	SD-WAN IP Packet Delivery .....	26
7.15.1	IP Packet Forwarding.....	27
7.15.2	IP Packet Transparency.....	27
7.16	Identifier String.....	28
<b>8</b>	<b>Application Flows and Policies .....</b>	<b>30</b>
8.1	Application Flows.....	30
8.2	Application Flow Specifications and Application Flow Criteria .....	31
8.3	Application Flow Specification Groups .....	32
8.4	Policies and Policy Criteria .....	32
<b>9</b>	<b>SD-WAN Virtual Connection (SWVC) Service Attributes.....</b>	<b>34</b>
9.1	SWVC Identifier Service Attribute .....	35
9.2	SWVC List of End Points Service Attribute .....	35
9.3	SWVC List of UCSs Service Attribute .....	35

9.4	SWVC Service Uptime Objective Service Attribute .....	35
9.5	SWVC Reserved Prefixes Service Attribute .....	36
9.6	SWVC List of Zones Service Attribute .....	37
9.7	SWVC List of Virtual Topologies Service Attribute .....	39
9.7.1	vtType=multipoint-to-multipoint.....	39
9.7.2	vtType=rooted-multipoint .....	40
9.8	SWVC Performance Time Intervals Service Attribute .....	41
9.9	SWVC List of Security Policies Service Attribute.....	41
9.10	SWVC List of Policies Service Attribute .....	41
9.10.1	Policy Criteria specification and interaction.....	44
9.10.2	Ingress Policy Criteria.....	45
9.10.3	Egress Policy Criteria .....	57
9.11	SWVC List of Application Flow Specification Groups Service Attribute.....	58
9.12	SWVC List of Application Flow Specifications Service Attribute .....	58
<b>10</b>	<b>SD-WAN Virtual Connection (SWVC) End Point Service Attributes .....</b>	<b>64</b>
10.1	SWVC End Point Identifier Service Attribute .....	64
10.2	SWVC End Point Associated UNI Service Attribute.....	64
10.3	SWVC End Point List of UCS End Points Service Attribute.....	64
10.4	SWVC End Point Policy Map Service Attribute .....	65
10.4.1	Ingress Policy Assignment.....	66
10.4.2	Egress Policy Assignment.....	68
10.4.3	Examples of Ingress Application Flows and Policy Assignment .....	69
<b>11</b>	<b>SD-WAN UNI Service Attributes .....</b>	<b>71</b>
11.1	SD-WAN UNI Identifier Service Attribute .....	71
11.2	SD-WAN UNI L2 Interface Service Attribute .....	72
11.3	SD-WAN UNI Maximum L2 Frame Size Service Attribute .....	73
11.4	SD-WAN UNI IPv4 Connection Addressing Service Attribute .....	73
11.5	SD-WAN UNI IPv6 Connection Addressing Service Attribute .....	75
11.6	SD-WAN UNI Routing Protocols Service Attribute.....	77
11.6.1	Static .....	78
11.6.2	BGP.....	79
11.6.3	OSPF.....	82
<b>12</b>	<b>UCS Service Attributes.....</b>	<b>84</b>
12.1	UCS Identifier Service Attribute .....	84
12.2	UCS Type Service Attribute.....	84
12.3	UCS Billing Method Service Attribute .....	85
<b>13</b>	<b>UCS UNI Service Attributes .....</b>	<b>86</b>
13.1	UCS UNI Identifier Service Attribute .....	86
<b>14</b>	<b>UCS End Point Service Attributes .....</b>	<b>87</b>
14.1	UCS End Point Identifier Service Attribute .....	87
14.2	UCS End Point Backup Service Attribute .....	87
14.3	UCS End Point Breakout Service Attribute .....	87

<b>15</b>	<b>Performance Metrics .....</b>	<b>89</b>
15.1	Qualified Packets .....	89
15.2	One-Way Packet Delay .....	89
15.3	One-Way Mean Packet Delay Performance Metric .....	90
15.4	One-Way Mean Packet Delay Variation Performance Metric .....	90
15.5	One-Way Packet Loss Ratio Performance Metric .....	90
<b>16</b>	<b>References .....</b>	<b>92</b>
<b>Appendix A</b>	<b>Processing Application Flows (Informative).....</b>	<b>95</b>
A.1	Process View .....	95
A.2	Ingress Packet Flow View .....	97
<b>Appendix B</b>	<b>SD-WAN Use Cases (Informative).....</b>	<b>98</b>
B.1	Hybrid WAN .....	98
B.2	Dual Internet WAN .....	99
<b>Appendix C</b>	<b>Major Changes from MEF 70 to MEF 70.1 (Informative).....</b>	<b>100</b>

## List of Figures

Figure 1 – Diagram Conventions .....	8
Figure 2 – Components of an SD-WAN Service .....	13
Figure 3 – Ingress and Egress .....	15
Figure 4 – Multiple SD-WAN UNIs .....	15
Figure 5 – TVCs .....	19
Figure 6 – Zones and Policy Assignment examples .....	22
Figure 7 – Different Virtual Topologies in an SWVC .....	23
Figure 8 – Local Internet Breakout .....	24
Figure 9 – Relationship of Service Components .....	26
Figure 10 – Application Flows .....	32
Figure 11 – Examples of two multipoint-to-multipoint Virtual Topologies .....	39
Figure 12 – Example of rooted-multipoint Virtual Topology .....	40
Figure 13 – Operation of BANDWIDTH Policy Criterion .....	54
Figure 14 – Precedence for Policy Assignment .....	67
Figure 15 – Assigning Ingress Policies .....	69
Figure 16 – BGP Configurations Examples .....	79
Figure 17 – Application Flows, Policies, and Forwarding .....	95
Figure 18 – Ingress Packet Flow .....	97
Figure 19 – Use Case: Hybrid WAN .....	98
Figure 20 – Use Case: Dual Internet WAN .....	99

## List of Tables

Table 1 – Terminology and Abbreviations .....	6
Table 2 – Numerical Prefix Conventions.....	7
Table 3 – Summary of SWVC Service Attributes .....	34
Table 4 – Policy Criteria – Support Required.....	42
Table 5 – Policy Criteria – Support Recommended .....	43
Table 6 – Performance Metrics .....	51
Table 7 – Application Flow Criteria – Support Required.....	60
Table 8 – Application Flow Criteria – Support Recommended .....	62
Table 9 – Summary of SWVC End Point Service Attributes .....	64
Table 10 – Summary of SD-WAN UNI Service Attributes .....	71
Table 11 – Summary of UCS Service Attributes.....	84
Table 12 – Summary of UCS UNI Service Attributes.....	86
Table 13 – Summary of UCS End Point Service Attributes .....	87

## 1 List of Contributing Members

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

- Albis-Elcon
- AT&T
- Bell Canada
- Ciena
- Cisco
- Fortinet
- Fujitsu
- Futurewei
- Nokia
- Oracle
- Orange
- Spirent
- Versa Networks

## 2 Abstract

The SD-WAN Service Attributes and Service Framework Standard defines the externally visible behavior of a MEF SD-WAN Service. A Service deployment is based on an agreement between an SD-WAN Subscriber (the buyer) and an SD-WAN Service Provider (the seller) that includes agreement on the values of a set of SD-WAN Service Attributes defined in this document.

This document includes:

SD-WAN Important Concepts – description of important components and concepts, i.e., the building blocks that are used to define and describe a MEF SD-WAN Service.

SD-WAN Service Attributes – the enumeration and description of the information that is agreed to between the SD-WAN Subscriber and the SD-WAN Service Provider. The values of these Service Attributes are determined by agreement between the Subscriber and Service Provider, subject to constraints imposed by this standard.

SD-WAN Service Framework – A framework for defining instances of an SD-WAN Service based on the definitions, service elements, and Service Attributes included in the document.

### 3 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. In these cases, the third column is used to provide the reference that is controlling, in other MEF or external documents.

In addition, terms defined in MEF 61.1 [29] are included in this document by reference and are not repeated in the table below. Terms marked with \* are adapted from terms in MEF 10.4 [26] or MEF 61.1 [29].

Term	Definition	Reference
Application Flow	A sequence of IP Packets that Ingress at an SD-WAN UNI or are directed towards an SD-WAN UNI from a UCS that: <ol style="list-style-type: none"> <li>1. Match the same Application Flow Specification, and</li> <li>2. Have source IP Addresses in the same Zone or are all in the <i>Zone Internet</i></li> </ol>	This document
Application Flow Criterion	A specific condition for matching an IP Packet such as a field/value pair or identification by an algorithm or heuristic.	This document
Application Flow Specification Group	A named set of Application Flow Specifications.	This document
Application Flow Specification	A named set of Application Flow Criteria.	This document
Egress Application Flow	An Application Flow consisting of IP Packets directed toward an SD-WAN UNI by the Service Provider.	This document
Egress IP Packet	An IP Packet transmitted to the Subscriber Network by the Service Provider at an SD-WAN UNI.	This document *
Egress Policy	A Policy that is assigned to Egress Application Flows.	This document
Egress Policy Criterion	A Policy Criterion that can be used in Egress Policies.	This document
Egress UNI	For a given IP Packet flowing over the SD-WAN Service, the SD-WAN UNI where the IP Packet is received by the Subscriber Network from the Service Provider Network.	This document
Ingress Application Flow	An Application Flow consisting of Ingress IP Packets at an SD-WAN UNI.	This document
Ingress IP Packet	An IP Packet received from the Subscriber Network by the Service Provider at an SD-WAN UNI.	This document *
Ingress Policy	A Policy that is assigned to Ingress Application Flows.	This document
Ingress Policy Criterion	A Policy Criterion that can be used in Ingress Policies.	This document
Ingress UNI	For a given IP Packet flowing over the SD-WAN Service, the SD-WAN UNI where the IP Packet is received by the Service Provider Network from the Subscriber Network.	This document

Term	Definition	Reference
Internet Access Service	Public Internet connectivity service purchased by a Subscriber from an Internet Service Provider.	MEF 69 [31]
Internet Breakout	The forwarding of IP Packets in Application Flows, based on Policy, to Internet destinations via Internet Access UCSs.	This document
Local Internet Breakout	Internet Breakout in which Ingress IP Packets are forwarded over Internet Access UCSs connected to the SD-WAN Edge where the Ingress SD-WAN UNI is located.	This document
Path	A single TVC or a sequence of TVCs that connect a pair of SD-WAN Edges over which IP Packets are forwarded between UNIs located at the SD-WAN Edges.	This document
Performance Metric	One of several performance-related properties of a Path that can be measured and for which Application Flow requirements can be specified through Policy assignment.	This document
Policy	A named list of Policy Criteria that can be assigned to an Application Flow and that determines how an SD-WAN Service handles IP Packets in the Application Flow.	This document
Policy Criterion	A criterion that describes a specific objective or constraint on IP Packet handling.	This document
Qualified Packet	An Ingress IP Packet that complies with specific criteria and for which Performance Metrics are defined.	This document
SD-WAN	Software Defined Wide Area Network (see SD-WAN Service)	This document
SD-WAN Edge	A set of network functions (physical or virtual) that are located between the SD-WAN UNI(s) and the Underlay Connectivity Service UNI(s).	This document
SD-WAN Service	An overlay connectivity service that optimizes transport of IP Packets over one or more Underlay Connectivity Services by recognizing applications (Application Flows) and determining forwarding behavior by applying Policies to them. MEF SD-WAN Services are specified using Service Attributes defined in this MEF Standard.	This document
SD-WAN Service Provider	A Service Provider for an SD-WAN Service	This document
SD-WAN Subscriber	A Subscriber of an SD-WAN Service	This document
SD-WAN UNI	SD-WAN User Network Interface	This document
SD-WAN User Network Interface	The demarcation point between the responsibility of the SD-WAN Service Provider and the SD-WAN Subscriber.	This document
SD-WAN Virtual Connection	An association of SD-WAN Virtual Connection End Points in an SD-WAN Service that provides the logical construct of a L3 Virtual Private Routed Network for a Subscriber.	This document
SD-WAN Virtual Connection End Point	A logical construct at an SD-WAN UNI where Policies are associated with Ingress and Egress Application Flows.	This document

Term	Definition	Reference
Security Policy	A set of parameters that are agreed between the Subscriber and Service Provider (as part of the SWVC List of Policies Service Attribute) and that specify which Security Functions are to be applied to an Application Flow.	MEF 88 [33]
Service Provider	An organization that provides services to Subscribers. In this document, "Service Provider" means "SD-WAN Service Provider".	This document *
Service Provider Network	As seen from the point-of-view of the Subscriber, the aggregation of Underlay Connectivity Services (which may be provided by different organizations), TVCs, SD-WAN Edges, controllers, and orchestrators used to deliver an SD-WAN Service to a Subscriber. In this document, "Service Provider Network" means "SD-WAN Service Provider Network".	This document
Subscriber	The end-user of a service. In this document, "Subscriber" should be read as meaning "SD-WAN Subscriber".	This document *
Subscriber Location	Any place where there is an SD-WAN UNI.	This document
Subscriber Network	A network belonging to a given Subscriber (or other organization authorized by the Subscriber) that is connected to the Service Provider Network at one or more SD-WAN UNIs.	This document *
SWVC	SD-WAN Virtual Connection	This document
SWVC End Point	SD-WAN Virtual Connection End Point	This document
Tunnel Virtual Connection	A point-to-point forwarding relationship between two SD-WAN Edges that associates: <ul style="list-style-type: none"> <li>two UCS End Points in a given single Underlay Connectivity Service that is not an Internet Access Service, or</li> <li>a UCS End Point in each of two Internet Access Underlay Connectivity Services</li> </ul> and has a well-defined set of packet delivery characteristics (e.g., delay, security, bandwidth, etc.)	This document
TVC	Tunnel Virtual Connection	This document
UCS / UCSs	Underlay Connectivity Service / Services	This document
UCS UNI	Underlay Connectivity Service User Network Interface	This document
Underlay Connectivity Service	A service providing connectivity between two or more Subscriber Locations, or between a Subscriber Location and the Internet, over which an SD-WAN Service is provided; for example, a private IP Service or a Carrier Ethernet service.	This document
Underlay Connectivity Service End Point	A construct at the Underlay Connectivity Service UNI to which a distinct subset of IP Packets passing over the Underlay Connectivity Service UNI is mapped.	This document
Underlay Connectivity Service Provider	An organization that provides an Underlay Connectivity Service to a Subscriber or SD-WAN Service Provider.	This document
Underlay Connectivity Service UNI	A UNI in an Underlay Connectivity Service	This document

Term	Definition	Reference
UNI	Short for User Network Interface. In this document, UNI without a modifier (such as “UCS UNI”) means SD-WAN UNI.	This document
Virtual Topology	A specific definition of the allowed forwarding behavior between a defined set of SWVC UNIs in an SWVC that can be applied to certain Application Flows by Policy.	This document
Zone	A subset of the IP hosts in the Subscriber Network identified by a set of IP Prefixes, or the Internet.	This document

**Table 1 – Terminology and Abbreviations**

## 4 Compliance Levels

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 (RFC 2119 [6], RFC 8174 [24]) 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.

## 5 Document Conventions

This section describes the numerical, notational and diagrammatic conventions used in the document.

### 5.1 Numerical Prefix Conventions

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

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

Table 2 – Numerical Prefix Conventions

### 5.2 Notational Conventions

There are several places in the document where mathematical, set, and other notational structures are specified. These items are specified using different types of brackets as follows:

- { xxx, yyy } – wide angle brackets are used to surround n-tuples
- [ xxx, yyy, zzz ] – square brackets are used to surround lists
- { a, b, c } – braces are used to surround sets

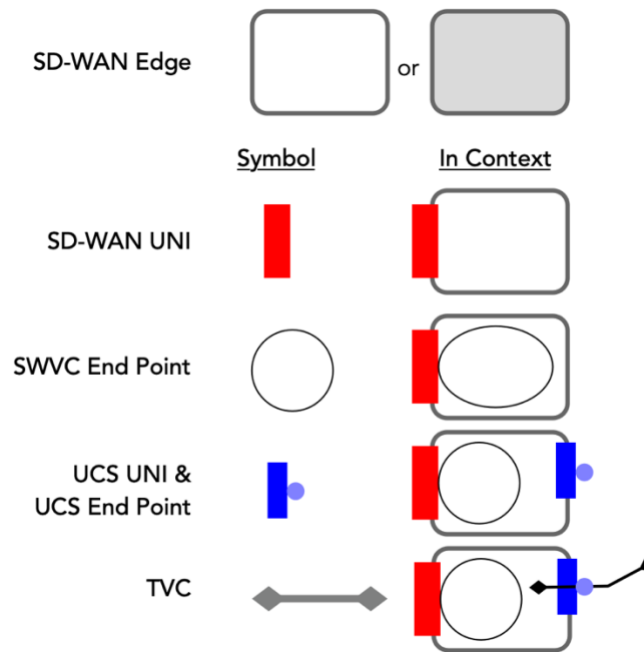
These brackets can be composed in many ways. For example:

[ < x1, y1 >, < x2, y2 >, < x3, y3 >] = a list of 2-tuples

< x1, [ < a1, b1, c1 >, < a2, b2, c2 >, < a3, b3, c3 >] > = a 2-tuple where the second element is a list of 3-tuples

### 5.3 Diagram Conventions

The diagrams in this document have a number of components that appear frequently. These components are represented in a standard way as described in the following diagram:



**Figure 1 – Diagram Conventions**

SD-WAN Edges are represented by rectangles with rounded corners. The edges are thicker gray lines, and they are white or light gray inside. SD-WAN User Network Interfaces (UNIs) are solid red rectangles. They are usually shown in conjunction with an SD-WAN Edge. SWVC End Points are represented as circles (sometimes as ovals in order to fit text) and are usually shown in conjunction with the SD-WAN Edge and SD-WAN UNI. The UCS UNI is shown as a solid blue rectangle and is usually shown on the opposite side of the SD-WAN edge from the SD-WAN UNI. The UCS End Point is a small circle attached to the UCS side of the UCS UNI. A TVC is represented as a line of any color with diamonds at both ends.

## 6 Introduction

An SD-WAN Service is a connectivity service that creates an overlay network over one or more Underlay Connectivity Services. An SD-WAN Service enables orchestrated connectivity that recognizes Application Flows at ingress to the Service and forwards them between SD-WAN UNIs based on Policies that are applied to them. An SD-WAN Service provides the logical construct of a Virtual Private Routed Network (see RFC 2764 [12]) for the Subscriber that transports IP Packets between Subscriber Locations. Additionally, an SD-WAN Service may provide connectivity between SD-WAN User Network Interfaces and the public Internet.

Since the SD-WAN Service can use multiple and possibly disparate Underlay Connectivity Services, it can offer more differentiated service delivery capabilities than natively using a single connectivity service.

It is important to distinguish between the SD-WAN Service and the Underlay Connectivity Services over which the SD-WAN Service operates. An SD-WAN Service Provider is responsible for providing the SD-WAN Service to the Subscriber. The SD-WAN Service Provider may be responsible for none, some, or all of the Underlay Connectivity Services. The Subscriber may also use Underlay Connectivity Services from any UCS Service Provider.

An SD-WAN service is aware of, and forwards traffic based on, Application Flows (see section 7.9). The Service agreement includes specification of Application Flows—IP Packets that match a set of criteria—and Policies that describe requirements and constraints on the forwarding of the Application Flows.

A benefit of an SD-WAN Service is the ability to adjust aspects of the service in near real time to meet business needs. These are expressed in SD-WAN Policies defined in this document. The Service Provider monitors the performance of the available forwarding options and modifies how packets in each Application Flow are forwarded to achieve the desired behavior.

This document defines Service Attributes that describe the externally visible behavior and operation of an SD-WAN Service as experienced by the Subscriber. It also defines Service Attributes for the Underlay Connectivity Services (and related components) whose values are necessary to define the behavior of SD-WAN Policies.

Several SD-WAN use cases are described in Appendix B.

### 6.1 Document Scope

MEF 70.1 includes definition and description of:<sup>1</sup>

- SD-WAN Service components
- SD-WAN Service functionality visible to the Subscriber
- Service Attributes for SD-WAN Virtual Connection (SWVC), SWVC End Point, and SD-WAN UNI

---

<sup>1</sup> A list of major differences between MEF 70 and MEF 70.1 is provided in Appendix C.

- Policies and the Policy Criteria that compose them, and required behavior for a set of Policy Criteria
- Application Flows, Application Flow Specifications, and the Application Flow Criteria that compose the Application Flow Specifications
- The SD-WAN UNI and details of Subscriber connection to the SD-WAN Service
- Service Attributes to describe key characteristics of an Underlay Connectivity Services (UCS), Underlay Connectivity Service UNIs, and Underlay Connectivity Service End Points from an SD-WAN Service perspective
- The assignment of Policies to Ingress and Egress Application Flows at an SWVC End Point.
- Support for multiple Virtual Topologies that can be assigned to Ingress Application Flows by Policy
- Support for partitioning the Subscriber's IP hosts into Zones
- Key characteristics of Tunnel Virtual Connections

This document does not include any normative<sup>2</sup> information relating to:

- Management and orchestration of SD-WAN Services
- LSO APIs
- Service Attributes related to Tunnel Virtual Connections
- IP Forwarding paradigms other than longest prefix match-based forwarding
- Details about creation of Tunnel Virtual Connections (TVCs). The SD-WAN Service assumes that the Service Provider provisions/creates the necessary TVCs with the appropriate characteristics to support the Policy requirements of the Subscriber.
- Interconnection of an SD-WAN Service to a cloud service that does not provide an SD-WAN UNI

## 6.2 Characteristics of an SD-WAN Service

A MEF SD-WAN Service has the following characteristics:

- 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 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.
- SWVC topologies are defined by Policies and IP forwarding constraints.
- An SD-WAN Service can offer encryption between SD-WAN Edges.
- 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. Members of an Application Flow Specification Group share a single bandwidth commitment and limit.

---

<sup>2</sup> In various sections of the document there may be informative text referring to some of these items.

- 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.

### **6.3 Organization of the Standard**

The remainder of the document is organized as follows:

- Definitions, key concepts, and document conventions are detailed in section 7.
- An overview of Application Flows and Policies is provided in section 8.
- Service Attributes for the SD-WAN Virtual Connection (SWVC) are described in section 9.
- Service Attributes for the SD-WAN Virtual Connection End Point are described in section 10.
- Service Attributes for the SD-WAN UNI are described in section 11.
- Service Attributes for Underlay Connectivity Service, UCS UNI, and UCS End Point are described in sections 12, 13, and 14 respectively.
- Performance Metrics used in the PERFORMANCE Policy Criterion are defined in section 15.

## 7 Key Concepts, Definitions, and Conventions

This section provides definitions, key concepts, and overviews of the components of a MEF SD-WAN Service.

### 7.1 Service Attributes

The behavior of MEF Services, such as SD-WAN, is specified using Service Attributes. A Service Attribute captures specific information that is agreed on between the Service Provider and the Subscriber of a MEF Service, and it describes some aspect of the service behavior. How such an agreement is reached, and the specific values agreed upon, might have an impact on the price of the service or on other business or commercial aspects of the relationship between the Subscriber and the Service Provider; these details are outside the scope of this document. Some examples of how agreement could be reached are given below, but this is not an exhaustive list.

- The Service Provider mandates a particular value.
- The Subscriber selects from a set of options specified by the Service Provider.
- The Subscriber requests a particular value, and the Service Provider accepts it.
- The Subscriber and the Service Provider negotiate to reach a mutually acceptable value.

Service Attributes describe the externally visible behavior of the service as experienced by the Subscriber, including the definitions of major SD-WAN capabilities such as Application Flow Specifications, Policies, Zones, Virtual Topologies, etc., that affect how traffic is handled within the SD-WAN Service. However, they do not constrain how the service is implemented by the Service Provider, nor how the Subscriber implements their network. The initial value for each Service Attribute is agreed upon by the Subscriber and the Service Provider in advance of the service deployment. The Subscriber and the Service Provider may subsequently agree on changes to the values of certain Service Attributes. This document does not constrain how such agreement is reached; for example, if the Service Provider allows the Subscriber to select an initial value from a pre-determined set of values, they might further allow them to change their selection at any time during the lifetime of the service.

### 7.2 SD-WAN Service Components Overview

MEF SD-WAN Services are specified by Service Attributes for three logical constructs:

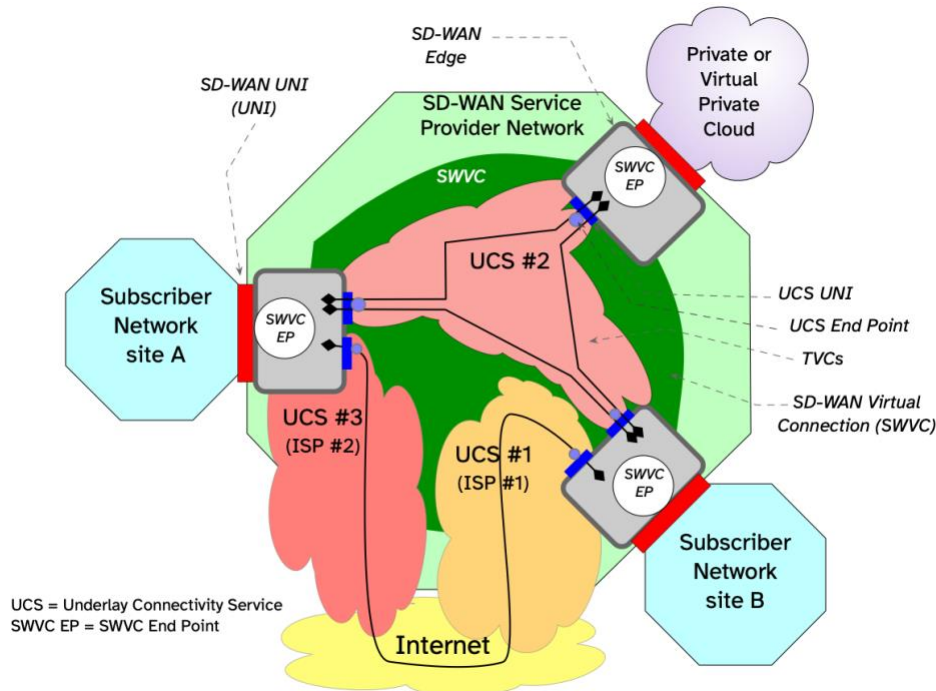
- SD-WAN Virtual Connection (SWVC)
- SD-WAN Virtual Connection End Point
- SD-WAN UNI (in this document, UNI refers to an SD-WAN UNI, unless otherwise specified)

Service Attributes are also specified for certain aspects of the Underlay Connectivity Services (UCS), UCS UNIs, and UCS End Points in order to provide a basis for SD-WAN features and Service Attributes described in this document.

Details of four additional components are discussed in this document but are not described by Service Attributes. These components may (or may not) be visible to the Subscriber. These components are described in the indicated sections:

- Subscriber Network (clearly this is visible to the Subscriber) (section 7.5)
- Service Provider Network (section 7.5)
- Tunnel Virtual Connection (TVC) (section 7.7)
- SD-WAN Edge (section 7.13)

Figure 2 shows the SD-WAN Service components described above.



**Figure 2 – Components of an SD-WAN Service**

Note that in Figure 2, one of the Subscriber sites is a connection to a Private or Virtual Private Cloud, which may not be located at the Subscriber's physical location. However, the SD-WAN Edge and its components (SD-WAN UNI, SWVC End Point, etc.) at this Subscriber Location operate no differently than at any of the other Subscriber Locations.

Each Underlay Connectivity Service terminates at a service demarcation point, i.e., a UCS UNI (since they are also services), which is shown in the diagram. Depending on the type of Underlay Connectivity Service, this could be an Ethernet UNI (as defined in MEF 10.4 [26]), an IP UNI (as defined in MEF 61.1 [29] including Internet Access as defined in MEF 69 [31]), an L1 UNI (as defined in MEF 63 [30]), or analogous service demarcation for other non-MEF services. Since the UCS UNI can provide access to multiple services (consider a UCS UNI with multiple Carrier Ethernet services), the UCS End Point is the logical construct that associates a specific UCS with the UCS UNI (see section 7.6). Note that Figure 2 shows a case where each UCS UNI provides access to a single UCS, and therefore has only a single UCS End Point.

### 7.3 SD-WAN Subscriber and SD-WAN Service Provider

This document deals, primarily, with two organizations—the SD-WAN Subscriber and the SD-WAN Service Provider. The SD-WAN Subscriber is the organization that uses services described

by the Service Attributes specified in this document. The SD-WAN Service Provider is the organization that provides those services.

There is no restriction on the type of organization that can act as a Subscriber. For example, a Subscriber can be an enterprise, a mobile operator, an IT system integrator, or a government department. At its most basic, an SD-WAN Service provides connectivity for IP Packets between different parts of the Subscriber Network or between the Subscriber Network and the Public Internet using Internet Breakout (described in section 7.12).

The remainder of this document uses “Service Provider” to refer to the SD-WAN Service Provider and “Subscriber” to refer to the SD-WAN Subscriber.

## 7.4 SD-WAN UNI

An SD-WAN User Network Interface, or SD-WAN UNI, is the demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber. The SD-WAN UNI is on the boundary between the Subscriber Network and the Service Provider Network (see section 7.5). The basic unit of transport at the SD-WAN UNI is an IP Packet.

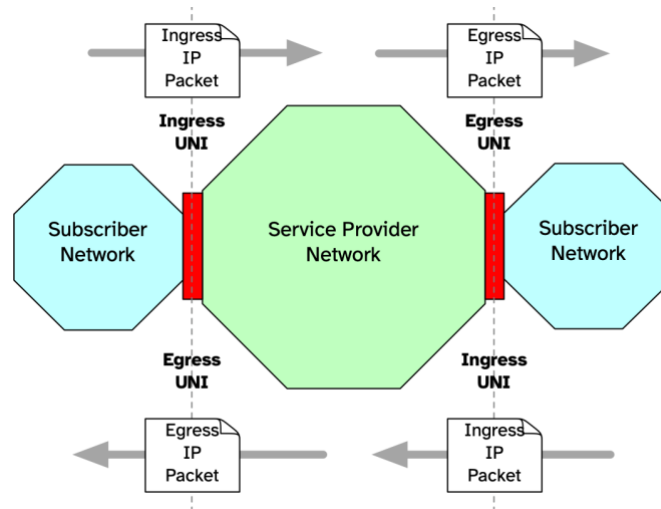
In the remainder of this document when the abbreviation “UNI” is used without a modifier, it refers to the SD-WAN UNI (references to the UCS UNI always include “UCS”).

Formally, the UNI is a demarcation point. The term UNI is often used to also refer to the network connection between the Subscriber Network and the Service Provider Network, but the actual location of the reference point is important because it defines where the Service Provider’s responsibility starts and also because service performance is defined from UNI to UNI.

**[R1]** An SD-WAN UNI **MUST** be dedicated to a single Subscriber.

**[R2]** An SD-WAN UNI **MUST** be dedicated to a single Service Provider.

An IP Packet that crosses the UNI from the Subscriber to the Service Provider is called an *Ingress* IP Packet, and the UNI is the *Ingress UNI* for that IP Packet. Similarly, an IP Packet that crosses the UNI from Service Provider to the Subscriber is called an *Egress* IP Packet, and the UNI is the *Egress UNI* for that IP Packet. These are shown in the following diagram:

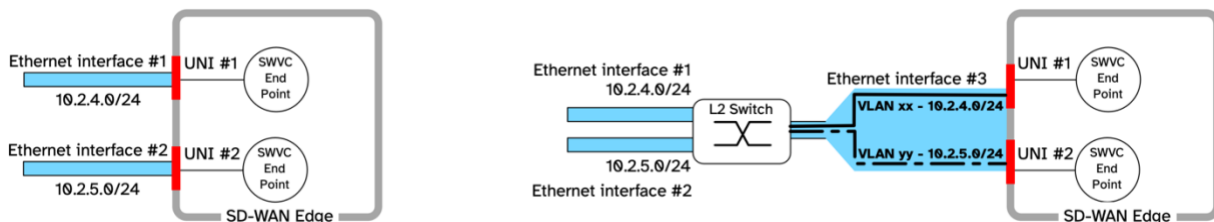


**Figure 3 – Ingress and Egress**

**Terminology note:** Since SD-WAN is an overlay network service, the terms *Ingress* and *Egress* can also be (and often are) applied to IP packets crossing the Underlay Connectivity Service UNIs. This can create ambiguity and confusion. In this document their use *only* refers to packets crossing the SD-WAN UNI as shown in Figure 3.

As with other MEF services, an SD-WAN Service (specifically, the SWVC) is an association of Service End Points (SWVC End Points in this case), and each SWVC End Point is associated with a UNI—the SWVC accepts an IP Packet at an Ingress UNI and delivers it to an Egress UNI (or to the Internet in the case of Internet Breakout).

An SD-WAN UNI connects to one or more IPv4 or IPv6 Subscriber subnets (see sections 11.4 and 11.5). Commonly, each Subscriber site has an SD-WAN Edge with a single UNI, but an SD-WAN Edge could support multiple UNIs. These UNIs can be separate physical Ethernet connections or a single Ethernet connection with multiple VLANs (see section 11.2) as shown in Figure 4 (or a combination of these approaches). The two examples in Figure 4 are equivalent from the SD-WAN Edge point of view.



**Figure 4 – Multiple SD-WAN UNIs**

There are several reasons for having multiple physical or logical Ethernet interfaces and their associated UNIs. One reason might just be convenience, for example, connecting the first floor

Ethernet and the second floor Ethernet to different ports on the SD-WAN Edge. Another might be for segregation of traffic, e.g., Ethernet interface #1 might connect to the Guest-WiFi Access Point and Ethernet interface #2 to the corporate router.<sup>3</sup>

One benefit of supporting multiple UNIs for the same SWVC at an SD-WAN Edge is that Policy assignment is done based on the Ingress UNI<sup>4</sup>. Therefore, an Application Flow that results from matching an Application Flow Specification and Zone at one Ingress UNI can be assigned a different Policy than an Application Flow that results from matching the same Application Flow Specification and Zone at another Ingress UNI.

## 7.5 Subscriber Network and Service Provider Network

The Subscriber Network is defined as the network belonging to the Subscriber (or another organization authorized by the Subscriber) that is connected to the Service Provider Network at two or more UNIs.

The Service Provider Network represents the set of components and logical constructs used by the Service Provider to provide an SD-WAN Service. It includes SD-WAN Edges, Underlay Connectivity Services, Tunnel Virtual Connections, and several control and management functions, services, and servers.

The name “Service Provider Network” indicates that the SD-WAN Service Provider integrates all of these components into the SD-WAN Service offering but does not make a statement about the owner or operator of any given component—all components may be owned and operated by the Service Provider, or some components (or even all) may be owned and operated by one or more other organizations.

The Service Provider Network can be completely opaque, that is, the Subscriber connects to the Service Provider Network at the UNIs, and the SD-WAN Service provides the desired connectivity, but the Subscriber has no insight into any of the underlying components. Alternatively, the Subscriber can agree with the Service Provider that some of the Subscriber’s existing (i.e., previously contracted) Underlay Connectivity Services (see section 7.6) are to be used with the SD-WAN Service. In that case, these Underlay Connectivity Services are known to the Subscriber; however, other underlying components of the SD-WAN Service may remain opaque.

## 7.6 Underlay Connectivity Service, UCS UNI, and UCS End Point

An SD-WAN Service is an overlay network service that operates over one or more Underlay Connectivity Services. Underlay Connectivity Services are network services that provide connectivity between Subscriber Locations or between a Subscriber Location and the Internet.

---

<sup>3</sup> It is also possible that the UNIs are associated with different SD-WAN Services (SWVCs), but this is not in scope for this document.

<sup>4</sup> Policy is actually assigned at the SWVC End Point, but since there is a one-to-one relationship between the UNI and the SWVC End Point it makes more sense to use UNI here since it the section on UNIs.

Underlay Connectivity Services can include a variety of services, including (but not limited to) Ethernet Services (as defined in MEF 6.3 [26]), IP Services (defined in MEF 61.1 [29]), Internet Access Services (defined in MEF 69 [31]), and L1 Connectivity Services (defined in MEF 63 [30]). Access to these Underlay Connectivity Services can be via a variety of networking technologies, such as DSL, HFC, LTE, fiber, Wi-Fi, Ethernet; and the transport can be based on Ethernet switching, IP routing, MPLS, or other technologies.

Underlay Connectivity Services have several characteristics that can be used by Policies that determine the forwarding of Application Flows within the SD-WAN Service.

- An Underlay Connectivity Service is referred to as *Private* or *Public*. A Public UCS is an Internet Access Service such as described in MEF 69 [31]. (See section 12.2.)
- Cost for usage of an Underlay Connectivity Service is *flat-rate* or *usage-based*. Flat rate means that a given amount of service bandwidth is billed at a fixed amount for the billing period, e.g., \$50/month for 100 Mb/s. Usage-based means that service is billed based on the amount of data that is transmitted or received, e.g., £10/GB. More complex charging structures are also possible. (See section 12.3.)
- The Service Provider and Subscriber can agree that an Underlay Connectivity Service is designated as a *Backup* UCS at an SD-WAN Edge (UCS UNI). See section 9.10.2.7 for more detail about the use of a UCS designated as *Backup*. (Also, see section 14.2.)
- As with all communications services, Underlay Connectivity Services have bandwidth limitations and performance characteristics that can affect services that run over them.

A UCS is a service with a UCS Subscriber and a UCS Service Provider, and it is likely that there are service parameters and attributes that are agreed on by those parties (examples might be UCS Bandwidth and IP Addressing), but that UCS service agreement is separate from the SD-WAN Service.

SD-WAN Services are frequently deployed over multiple, and often disparate, Underlay Connectivity Services. Multiple Underlay Connectivity Services with different performance and cost characteristics (e.g., an IP-VPN over MPLS Network versus an Internet Access Service) can be used to provide cost benefits, resiliency, and differentiated transport.

Underlay Connectivity Services can be provided by the SD-WAN Service Provider on its own network or over the networks of other network operators (including the Internet). Underlay Connectivity Services arranged independently by the Subscriber can also be used by the SD-WAN Service. Some details of the Underlay Connectivity Service are agreed to by the Subscriber and Service Provider as values of UCS, UCS UNI, and UCS End Point Service Attributes specified in this document. It is assumed that the Subscriber also communicates other details of the UCS to the SD-WAN Service Provider in this case. The division of responsibility for UCS services between the Subscriber and the SD-WAN Service Provider is outside the scope of this document.

The UCS has a demarcation point, a UCS UNI, that delineates the responsibility of the parties.

Many MEF Services, such as Carrier Ethernet Services, support *service multiplexing* at their corresponding UNIs, i.e., a single UNI providing access to multiple services and therefore multiple

service end points. For example, a Carrier Ethernet UNI could provide access to an EVP-LAN service connecting all U.S. facilities together, and an EVPL from one of those facilities (e.g., the headquarters) to a non-US facility. To accommodate this, the UCS UNI can likewise support service multiplexing, i.e., multiple UCS End Points at the UCS UNI, and each UCS End Point selects packets from one particular UCS at the UCS UNI and directs packets towards the one particular UCS at the UCS UNI. Also, the UCS attributes that can vary at each UCS UNI are associated with a UCS End Point. In the example above, the headquarters location would have two UCS End Points at the UCS UNI, and all the other facilities would have one. There is no requirement that an SD-WAN Service include all of the UCS End Points at a UCS UNI.

The UCS End Point is important in the SD-WAN Service context because the characteristics of the UCS, as seen by the SD-WAN Service, are not (necessarily) the same at all UCS UNIs in the UCS. For example, the amount of delivered bandwidth can be different at different UCS End Points.

As noted in section 7.4, the term “UNI” by itself always refers to the SD-WAN UNI. References to the UCS UNI are always “UCS UNI”.

## 7.7 Tunnel Virtual Connection (TVC)

A Tunnel Virtual Connection (TVC) is a point-to-point forwarding relationship between two SD-WAN Edges that associates either:

- two UCS End Points in a single Underlay Connectivity Service that is not an Internet Access Service, or
- a UCS End Point in each of two Internet Access Underlay Connectivity Services (such as defined in MEF 69 [31])

A Path between two SD-WAN UNIs is a single TVC between the SD-WAN Edges where the UNIs are located or a sequence of TVCs that link those SD-WAN Edges.

A TVC has performance and privacy/security characteristics, e.g., delay, bandwidth, encryption, etc.

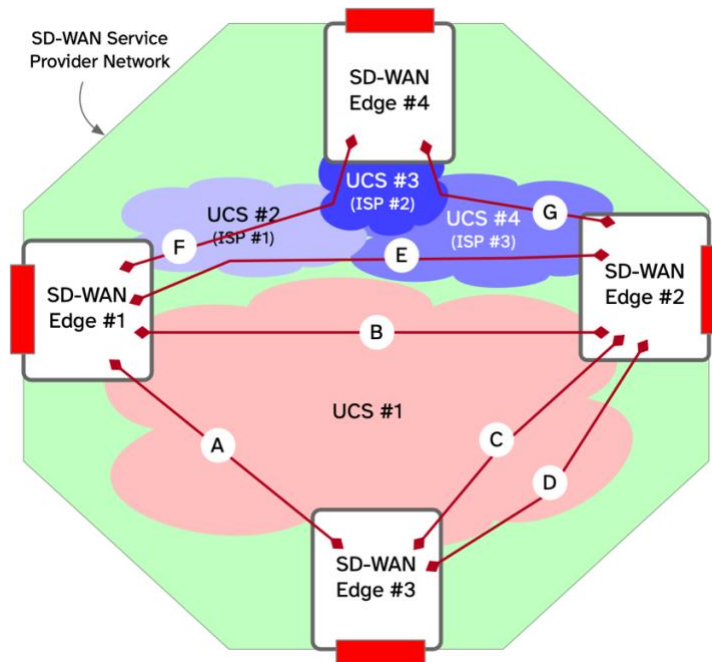
**[R3]** For an IP Packet in an Application Flow to be forwarded directly from one SD-WAN Edge to another SD-WAN Edge, there **MUST** be at least one TVC between the two SD-WAN Edges.

Although the name Tunnel Virtual Connection includes the word “tunnel”, this does not imply a particular implementation or instantiation, but rather that the forwarding relationship has a well-defined set of end points that source and sink packets.

As shown in Figure 5, two SD-WAN Edges can be connected by one TVC or multiple TVCs. Multiple TVCs can be provided between the same two SD-WAN Edges for several reasons, including:

- They traverse different UCSs and can provide resilience
- They traverse different UCSs and can provide additional bandwidth or load balancing
- They have different performance characteristics (e.g., different classes of service)

- They have different privacy/security characteristics



**Figure 5 – TVCs**

As shown in Figure 5 and based on [R3]:

- TVCs E, F, and G provide connectivity between (respectively):
  - SD-WAN Edges 1–2 (across UCS #2 and UCS #4),
  - SD-WAN Edges 1–4 (across UCS #2 and UCS #3), and
  - SD-WAN Edges 2–4 (across UCS #3 and UCS #4).
- TVCs A and C provide connectivity across UCS #1 between 1–3 and 2–3.
- TVC B provides connectivity from 1–2, which is also provided by TVC E. These two TVCs traverse different UCSs, which means they can provide different characteristics such as more bandwidth or more resiliency or different cost, etc.
- TVC D is between SD-WAN Edge 2 and SD-WAN Edge 3 parallel to C. Both are across the same UCS so there is no additional resiliency, but they could have different classes of service, or one of them might be encrypted, or they could be allocated to support different Application Flows.
- Note that the Path between the UNI at SD-WAN Edge 3 and UNI at SD-WAN Edge 4 requires the concatenation of multiple TVCs. This requires routing through another SD-WAN Edge, A–F, C–G, or D–G. The SD-WAN Service Provider is responsible for connectivity between SD-WAN Edges that are attached to different Underlay Connectivity Services. How this is done is beyond the scope of this document.

TVCs do not have Service Attributes that can be used by the Subscriber in Policy definitions, but they have several important characteristics:

- A TVC appears to each SD-WAN Edge as a single routing hop.
- If a TVC traverses an Internet Access UCS, then the TVC is Public; otherwise, it is Private.

- The SD-WAN Edge can implement encryption on a TVC basis, in which case all traffic forwarded across the TVC is encrypted.
- The performance of a TVC is one of the factors that affects whether the TVC is used for forwarding each Application Flow.

TVCs are the responsibility of the Service Provider and are not agreed to by the Subscriber. How they are instantiated, when they are instantiated, and whether they are ephemeral or long-lasting are all beyond the scope of this document. As noted above, there are no Service Attributes for TVCs, and this specification does not provide a mechanism for the Subscriber to refer to specific TVCs in Policy definitions. The Service Provider may or may not choose to expose information about TVCs to the Subscriber.

## 7.8 SD-WAN Virtual Connection and SWVC End Point

An SD-WAN Service comprises an SD-WAN Virtual Connection (SWVC), SD-WAN Virtual Connection (SWVC) End Points, and SD-WAN UNIs. Each UNI has an associated SWVC End Point, and the SWVC, itself, is an association of these SWVC End Points. The SWVC defines the logical connectivity of the SD-WAN Service as viewed by the Subscriber.

An SWVC End Point is a logical construct associated with each UNI (one SWVC End Point per UNI) that encapsulates the Service Attributes that assign Ingress Policies to Ingress Application Flows and Egress Policies to Egress Application Flows.

**[R4]** An SD-WAN UNI **MUST** be associated with, at most, one SWVC End Point.

[R4] allows a UNI without an SWVC End Point, but no SD-WAN traffic can be forwarded at this UNI. This may be a transitory state during SD-WAN Service creation or modification.

## 7.9 Application Flow, Application Flows Specifications, and Policies

A defining characteristic of an SD-WAN Service is the forwarding of IP Packets over an SWVC, where the SWVC may operate over multiple UCSs. UCSs may have different Service Attributes and characteristics. Policies are used to forward Application Flows over the most appropriate UCS(s).

An Application Flow can be described by a set of characteristics of the packet stream that can be identified based on inspection of individual IP Packets or sequences of IP Packets at a UNI. This set of characteristics has two parts, the Application Flow Specification, and the Zone. Application Flow Specifications are used to match specific fields or patterns in each IP Packet, and the Zone is assigned based on the source of the packet.

An Ingress Application Flow is a subset of the Ingress IP Packets at a UNI, and an Egress Application Flow is a subset of the IP Packets destined to egress at a UNI. The description is slightly different between ingress and egress because IP Packets in an Ingress Application Flow always arrive at the Ingress UNI, but IP Packets in an Egress Application Flow might be discarded by a Policy and therefore won't reach the Egress UNI.

Policies are assigned to each Application Flow at an SWVC End Point. An Ingress Policy describes the required forwarding behavior for Ingress Application Flows (e.g., should they be forwarded or discarded, should they be encrypted, should they be rate limited, and several more). An Egress Policy describes whether Egress Application Flows directed toward a UNI should be forwarded to that UNI or discarded due to security or other considerations.

Section 8 provides more detail about Application Flows and Policies.

## 7.10 Zone

The IP hosts (an IP host is an IP addressable network interface, either physical or virtual) in the Subscriber's network can be separated into groups that have different business and security requirements. Zones are used to define and describe these groups of IP hosts. At least one Zone is required in every SWVC. An SD-WAN Service can be used to forward traffic for some or all these Zones. Some examples of Zones are:

- Corporate Zone vs. Guest Zone
- Point-of-sale Zone vs. Corporate Zone
- Engineering Zone vs. Finance Zone vs. HR Zone
- Company Zone vs. Customer Zone vs. Vendor Zone vs. Guest Zone

An Application Flow is defined by the UNI, the Application Flow Specification that it matches, and its Zone (i.e., source IP host). Since Policies are assigned to Application Flows, IP Packets that match the same Application Flow Specification can have different treatment if they are in different Zones.

**Terminology Note:** This document uses the phrase “IP Packet in Zone ‘x’” to indicate that at the Ingress UNI, the IP Packet was received from an IP host that is in Zone ‘x’.

The SWVC List of Zones Service Attribute (section 9.6) specifies the Zones used by the SD-WAN Service.

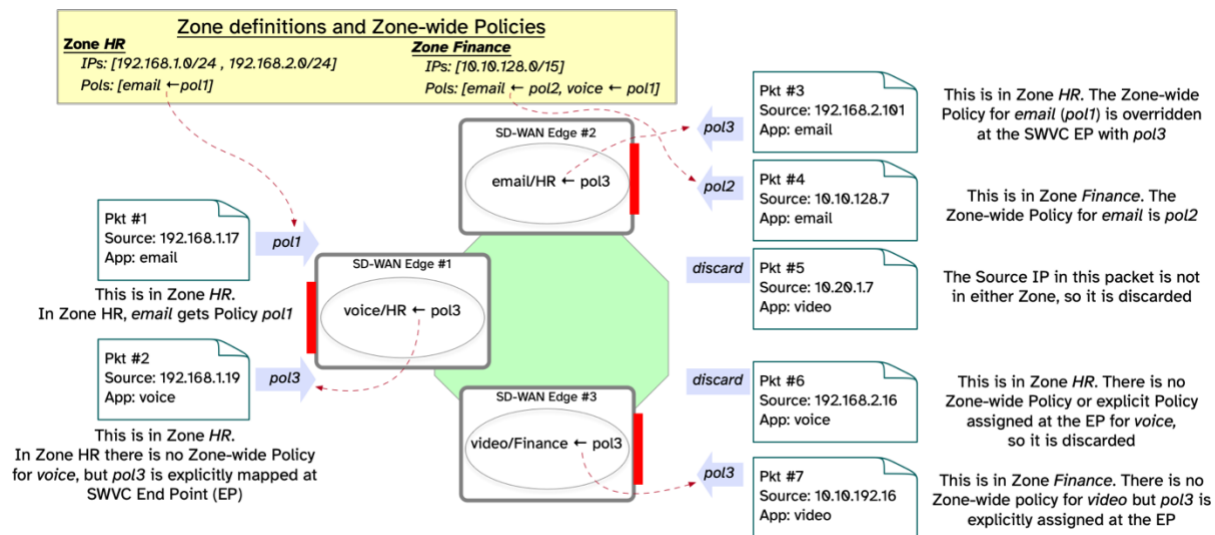
One of the goals of using Zones is commonality in handling Application Flows at different locations in the SD-WAN Service. For example, the same Policies can be assigned to Application Flows in “Guest-Wifi” Zone at every SWVC End Point in the SD-WAN Service that has a “Guest-Wifi” Zone. Hence, the SWVC List of Zones Service Attribute includes, for each Zone, a set of Zone-wide Application Flow-to-Policy mappings. Unless overridden by another Policy assigned at an SWVC End Point, these Policies are assigned at every SWVC End Point where the associated UNI has the Zone defined.

A Zone definition includes a list of IP prefixes that defines the IP subnets that compose the Zone. A host is assigned to a Zone if the IP address of the host is a member of one of the IP Prefixes for the Zone. If the source of an IP Packet or the destination of an IP Packet is not assigned to a Zone, the IP Packet is discarded (see [R24]).

In some scenarios, a Zone might be represented by the same set of IP Prefixes at every UNI, e.g., “Guest-Wifi” might be 192.168.1.0/24 everywhere. In other cases, a Zone might have different prefixes at different UNIs.

Zones can reduce the number of Application Flow Specifications while increasing the number of Application Flows at UNIs in the SWVC. A single Application Flow Specification, for example one called *email*, can be matched at an SD-WAN UNI against IP Packets in (arriving from) two Zones, e.g., *HR* and *Finance*, resulting in two Application Flows at the UNI,  $\langle email, HR \rangle$  and  $\langle email, Finance \rangle$ , and each one can have a different Policy assigned.

At the SWVC End Point, Zone-wide Policies are assigned to Application Flows (unless overridden). The following diagram shows many of the possible cases.

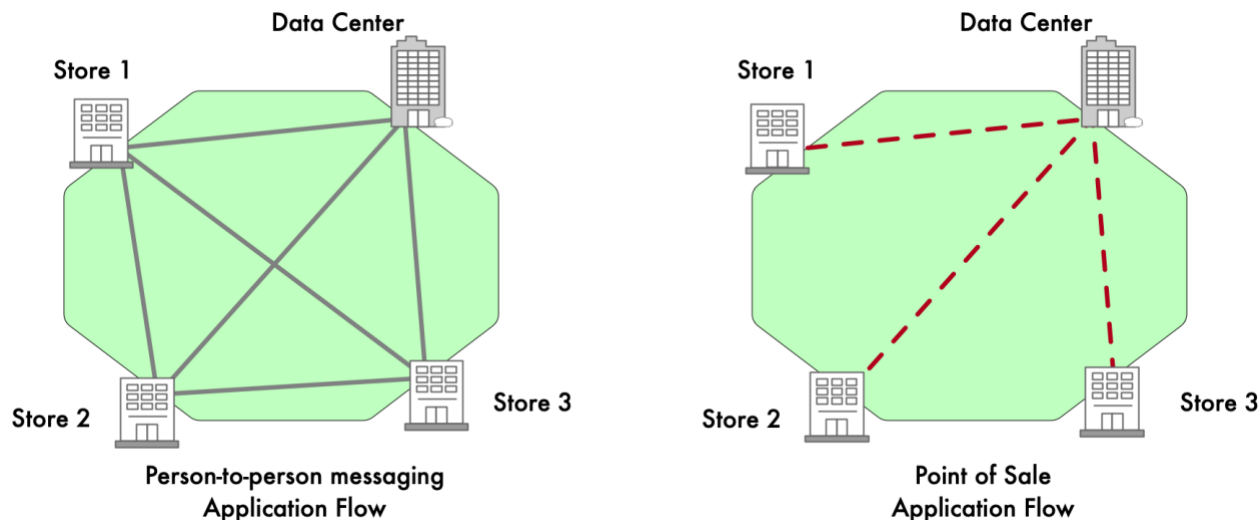


**Figure 6 – Zones and Policy Assignment examples**

Figure 6 depicts several examples of the options associated with Zones. There are two Zones, *HR* and *Finance*. *HR* has two IP subnets and one Zone-wide Policy (for *email*). *Finance* has one IP subnet and two Zone-wide Policies (one for *email* and one for *voice*). At each SWVC End Point Policy (inside the oval), *pol3* is explicitly mapped to one of the Application Flow/Zone combinations. Seven packets are presented at the three UNIs. The fat arrow outside of each packet indicates the Policy that is assigned to the packet at that SWVC End Point. Below or next to each packet is an explanation of why the Policy was assigned.

## 7.11 Virtual Topology

For many Application Flows, it might be desirable for IP Packets arriving at every UNI to be forwardable to every other UNI, but for other Application Flows, the desired forwarding behavior might be more limited. As an example, consider a retail subscriber with multiple stores. For a person-to-person messaging Application Flow across the company, a full mesh is useful, but the point-of-sale Application Flow in each store can only forward IP Packets to the POS controller, at the company data center.



**Figure 7 – Different Virtual Topologies in an SWVC**

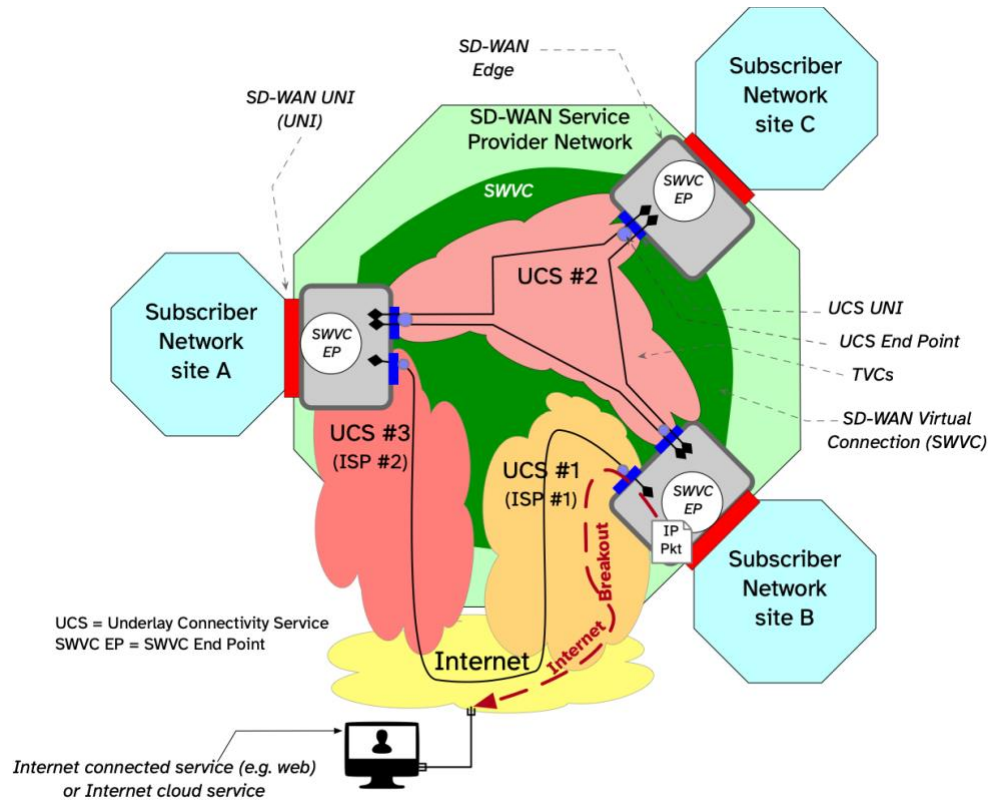
The Application Flows in this diagram experience two different forwarding behaviors in the same SD-WAN Service.

In this document, there can be multiple forwarding topologies in the SWVC. This is achieved by defining Virtual Topologies (see section 9.7), each of which includes a subset of the SWVC End Points (the full mesh of all the SWVC End Points is one of the possible Virtual Topologies). Each Application Flow is assigned to a Virtual Topology by Policy (see section 9.10.2.4).

### 7.12 Internet Breakout

When one or more of the Underlay Connectivity Services in an SD-WAN Service is an Internet Access Service, some Application Flows can be forwarded to Internet destinations rather than delivered to other SD-WAN UNIs. This forwarding behavior, called Internet Breakout, is assigned to an Application Flow by Policy (see section 9.10.2.6). The most common case is for IP Packets in the Application Flow to be forwarded to an Internet Access Service UCS that is connected to the SD-WAN Edge where the Ingress UNI for those IP Packets is located. This is called Local Internet Breakout.

An example of Local Internet Breakout is shown in Figure 8 (this is the same diagram as Figure 2 with the addition of an Internet-connected site outside of the SD-WAN Service). An ingress IP Packet at site B is forwarded across the UCS UNI for UCS #1 (an Internet Access UCS), but instead of being sent over one of the TVCs, it is forwarded to an Internet destination.



**Figure 8 – Local Internet Breakout**

If an Ingress Application Flow is assigned a Policy that indicates Internet Breakout is *Enabled*, then Ingress IP Packets in that Application Flow are forwarded using an Internet Access UCS that has UCS End Point Breakout Service Attribute *Enabled* (see section 14.3). If an appropriate Internet Access UCS is not available at the SD-WAN Edge containing the Ingress UNI for the Application Flow, the Service Provider may deliver the IP Packets over the SD-WAN Service (i.e., over one or more TVCs) to another SD-WAN Edge for “breakout” to the Internet.

If at least one Application Flow at a UNI has a Policy that indicates Internet Breakout is *Enabled*, then IP Packets received from Internet sources (rather than from another UNI) are allowed to egress at the UNI (subject to any Egress Policies applied). Otherwise, IP Packets received from Internet sources cannot be delivered to the UNI.

### 7.13 SD-WAN Edge

The SD-WAN Edge is a set of network functions (physical or virtual) located at the Service Provider side of the SD-WAN UNI, between the SD-WAN UNI(s) and the UCS UNI(s). It is part of the Service Provider Network, but it is commonly located at a Subscriber. It is situated between the SD-WAN UNIs, on its Subscriber side, and UCS UNIs of one or more Underlay Connectivity Services on its network side.

The SD-WAN Edge implements functionality that receives ingress IP Packets over the SD-WAN UNIs; determines how they should be handled according to routing information, applicable policies, other service attributes, and information about the UCSs; and if appropriate, forwards

them over one of the available UCS UNIs. Similarly, it receives packets over the UCS UNIs and determines how to handle them, including forwarding them over one of the SD-WAN UNIs to the Subscriber Network, if appropriate. The SD-WAN Edge thus implements all the functionality of the SD-WAN service that is not provided by a UCS. This includes Application Flow determination, Policy assignment, and routing/forwarding.

The SD-WAN Edge implements the functionality needed to connect to the Subscriber Network. It may also implement functionality that facilitates connection to the Underlay Connectivity Services, but these functions are out of scope for this specification.

## 7.14 SD-WAN Services Framework

An SD-WAN Service is a connectivity service, offered by a Service Provider, that optimizes transport of IP Packets over one or more Underlay Connectivity Services by recognizing Application Flows at ingress to the Service and forwarding them based on Policies that are applied to them.

A MEF SD-WAN Service consists of:

- Exactly one SWVC with a corresponding set of SWVC Service Attributes (see section 9).
- One<sup>5</sup> or more UNIs where the Subscriber accesses the SD-WAN Service, each with a corresponding set of UNI Service Attributes (see section 11).
- Exactly one SWVC End Point for the SWVC at each of those UNIs, where each SWVC End Point has a corresponding set of SWVC End Point Service Attributes (see section 10).
- One or more Underlay Connectivity Services (section 12) and corresponding UCS UNIs (section 13) and UCS End Points (section 14) and corresponding Service Attributes for each of them.

There is a one-to-one relationship between an SD-WAN Service and an SWVC. Note that the SWVC, the SWVC End Points, the UNIs, the Underlay Connectivity Services, and the UCS End Points (and their Service Attributes) are specific to a given SD-WAN Service instance.

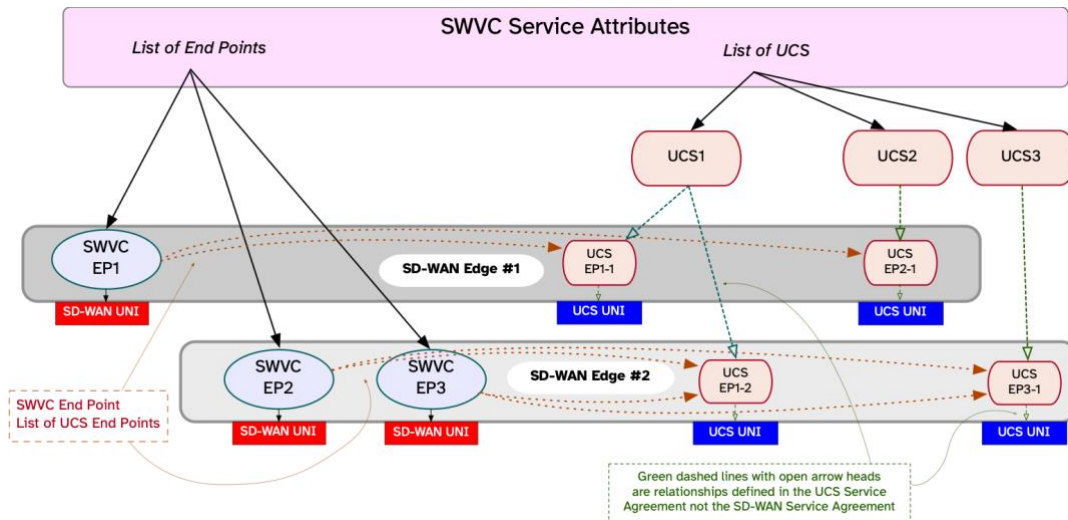
**[R5]** Each UCS and UCS End Point **MUST** be associated with at most one SWVC.

The reason that [R5] does not include the UCS UNI is that one UCS UNI could support multiple UCSs (each with a UCS End Point at the UCS UNI) and therefore a UCS UNI could support multiple SWVCs. Note, however, that supporting multiple SWVCs in an SD-WAN Edge is out of scope for this document.

The relationships between the various components of the SD-WAN Service and their Service Attributes are shown in the following diagram.

---

<sup>5</sup> An SD-WAN Service with only one UNI is unusual but there are scenarios where it might be appropriate.



**Figure 9 – Relationship of Service Components**

An SWVC is an association of SWVC End Points, and the SWVC includes a Service Attribute that identifies the SWVC End Points associated by the SWVC. Each SWVC End Point has a Service Attribute to identify the UNI at which it is located.

Each SWVC also has a list of Underlay Connectivity Services that are used to provide transport for the SWVC. Each UCS has a UCS End Point associated with the SD-WAN Edge that it services. Each UCS End Point associates its UCS with a UCS UNI.

In Figure 9, the SWVC has three SWVC End Points. EP1 is in SD-WAN Edge #1, and EP2 and EP3 are in SD-WAN Edge #2. There are three Underlay Connectivity Services. UCS1 has two UCS End Points, each associated with one of the SD-WAN Edges. UCS2 and UCS3 each has one UCS End Point—they are Internet Access Services. All SWVC End Points in an SD-WAN Edge have access to all UCS End Points in that SD-WAN Edge. Although not shown in the diagram, each UCS UNI could have multiple UCS End Points associated with it.

### 7.15 SD-WAN IP Packet Delivery

An SD-WAN Service delivers IP Packets between Subscriber Locations. In that sense, it shares many attributes with a MEF IP Service (as described in MEF 61.1, *IP Service Attributes* [29]). Therefore, many of the sections of this document are derived from MEF 61.1.<sup>6</sup>

Since IP Packet forwarding in SD-WAN Services is based on Application Flows and Policies, there are several Service Attributes defined to describe these capabilities, and several of the Service Attributes integrated from MEF 61.1 have been modified to focus on Application Flow-based forwarding rather than general IP/layer 3-based forwarding. An IP Service can be used as an Underlay Connectivity Service for an SD-WAN Service.

An SD-WAN Service (SWVC) provides the logical construct of an IP Virtual Private Routed Network for a Subscriber. This section describes the basic IP forwarding paradigm for an

<sup>6</sup> This is to ensure the greatest level of commonality between the two specifications as well as for expediency.

SD-WAN Service, and requirements that indicate which fields of an IP Packet can be modified while traversing the SD-WAN Service and under what conditions they can be modified.

#### 7.15.1 IP Packet Forwarding

The basic forwarding paradigm for an SD-WAN Service is a Virtual Private Routed Network (VPRN) as described in RFC 2764 [12]. As a VPRN, the SD-WAN Service relies on destination-based IP forwarding (based on standard IP longest prefix match), which can then have additional forwarding constraints as a result of Policies applied by the SD-WAN Service.

The Subscriber and the Service Provider may use static routing or a dynamic routing protocol at the UNI to exchange information about reachable IP Prefixes.

- [R6] The Service Provider **MUST NOT** deliver an ingress IP Packet to a UNI where the destination address is not reachable.

SD-WAN Services forward unicast, multicast, and broadcast IP Packets; however, this specification includes requirements for forwarding unicast IP Packets only. Requirements for forwarding of multicast and broadcast IP Packets are out of scope for this version of the standard.

The routing context of the SD-WAN Service may be independent of any routing contexts for the Underlay Connectivity Services used by the SD-WAN Service.

#### 7.15.2 IP Packet Transparency

In general, an SWVC conveys IP Packets without modifying the contents; however, there are some exceptions that are captured in the following requirements:

- [R7] If an Ingress IPv4 Packet is mapped to an SWVC and delivered as an Egress IPv4 Packet, and the packet has not been fragmented as described in RFC 791 [5], the Egress IPv4 Packet **MUST** be identical to the Ingress IPv4 Packet except that the following fields in the IPv4 header can be changed:
- The TTL field (RFC 791 [5])
  - The DS (RFC 3260 [15]) and ECN (RFC 3168 [14]) fields
  - The Loose Source and Record Route option, the Strict Source and Record Route option, and the Record Route option, if present in the packet (RFC 791 [5])
  - The Destination Address field, if the Loose Source and Record Route option or the Strict Source and Record Route option are present in the packet (RFC 791 [5])
  - The Header Checksum field (RFC 791 [5])
  - Any other field(s), subject to agreement between the Subscriber and the Service Provider
- [R8] If an Ingress IPv4 Packet is mapped to an SWVC and is fragmented by the Service Provider as described in RFC 791 [5] resulting in a number of corresponding IPv4 Packets that are delivered as Egress IPv4 Packets, the Egress IPv4 Packets **MUST** be such that reassembly as described in RFC 791

[5] results in an IP Packet that is identical to the Ingress IPv4 Packet except that the following fields in the IPv4 header can be changed:

- The TTL field (RFC 791 [5])
- The DS (RFC 3260 [15]) and ECN (RFC 3168 [14]) fields
- The Loose Source and Record Route option, the Strict Source and Record Route option, and the Record Route option, if present in the packet (RFC 791 [5])
- The Destination Address field, if the Loose Source and Record Route option or the Strict Source and Record Route option are present in the packet (RFC 791 [5])
- The Header Checksum field (RFC 791 [5])
- Any other field(s), subject to agreement between the Subscriber and the Service Provider

**[R9]** If an Ingress IPv6 Packet is mapped to an SWVC and delivered as an Egress IPv6 Packet, the Egress IPv6 Packet **MUST** be identical to the Ingress IPv6 Packet except that the following fields in the IPv6 header can be changed:

- The Hop Limit field (RFC 8200 [25])
- The DS (RFC 3260 [15]) and ECN (RFC 3168 [14]) fields
- The value of any options within a Hop-by-Hop Options header (if present) that have the third high-order bit in the option type field set (RFC 8200 [25])
- Any other field(s), subject to agreement between the Subscriber and the Service Provider

The use of the Loose Source and Record Route option, the Strict Source and Record Route option, and the Record Route option in IPv4 packets can cause problems due to the additional processing needed at each hop along the path. In addition, the Loose Source and Record Route option and the Strict Source and Record Route option open up a number of potential security risks as documented in RFC 6274, which outweigh any legitimate use.

**[O1]** A Service Provider **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.

## 7.16 Identifier String

Many of the Service Attribute values in this document are strings that are used for identification of an element. The document uses a single definition for the structure of these Identifier Strings.

The length of the Identifier String is not limited; however, since it is used in human interfaces, it is best to avoid very long Identifier Strings.<sup>7</sup>

---

<sup>7</sup> MEF 61.1 [29] limits these strings to 53 octets for MEF IP Services.

Since the Identifier String is used in human interfaces, the allowable character set is chosen to contain printable characters.<sup>8</sup>

- [R10]** An Identifier String **MUST** be a string consisting of one or more UTF-8 characters in the range of 32–126 (0x20 to 0x7e), inclusive.

---

<sup>8</sup> The definition only includes printable Latin characters. Inclusion of other printable characters is out of scope for this version of the document.

## 8 Application Flows and Policies

In an SD-WAN Service, IP Packets are classified into “Application Flows” at the Ingress and Egress UNIs and a “Policy” is assigned to each Application Flow to describe how the Service handles the Application Flow. There are several important logical constructs used in this standard to describe and define Application Flows and Policies:

- **Application Flow**
  - Application Flow Specification
  - Application Flow Criterion
  - Application Flow Specification Group
- **Policy**
  - Policy Criterion

There are several Service Attributes that relate to assigning Policies to Application Flows:

- SWVC List of Application Flow Specifications Service Attribute (section 9.12)
- SWVC List of Application Flow Specification Groups Service Attribute (9.11)
- SWVC List of Policies Service Attribute (9.10)
- SWVC List of Zones Service Attribute (section 9.6)
- SWVC End Point Policy Map Service Attribute (10.4)

The following subsections describe these constructs in detail and their relationship to each other.

### 8.1 Application Flows

An Application Flow is the subset of the IP Packets that ingress at a UNI or are destined for egress at a UNI that match a specific Application Flow Specification and are in a specific Zone.

The description is slightly different between ingress and egress because IP Packets in an Ingress Application Flow always arrive at the Ingress UNI, but IP Packets in an Egress Application Flow might be discarded by a Policy and therefore will not reach the Egress UNI. An Ingress IP Packet can be mapped to, at most, one Ingress Application Flow at a UNI and can belong to zero or one Egress Application Flow. The Ingress IP Packets that are mapped to a given Ingress Application Flow at a UNI will not necessarily belong to the same Egress Application Flow since different Ingress IP Packets can be destined to different UNIs.

Although the term “Application Flow” includes the word “Application” there is only a loose connection between the two. An Application Flow can map to (what is typically thought of as) an application, but it can also represent a subset or a superset. For example:

- An Application Flow can include IP Packets for several individual computer applications, such as “all packets that use the RTP protocol as defined in RFC 3550 [16]”, or
- IP Packets for a single application could be split among multiple Application Flows, such as a single video conferencing call resulting in a “Video” Application Flow and an “Audio” Application Flow, or an IP Phone resulting in an “Audio” Application Flow and a “Control/Signaling” Application Flow, or

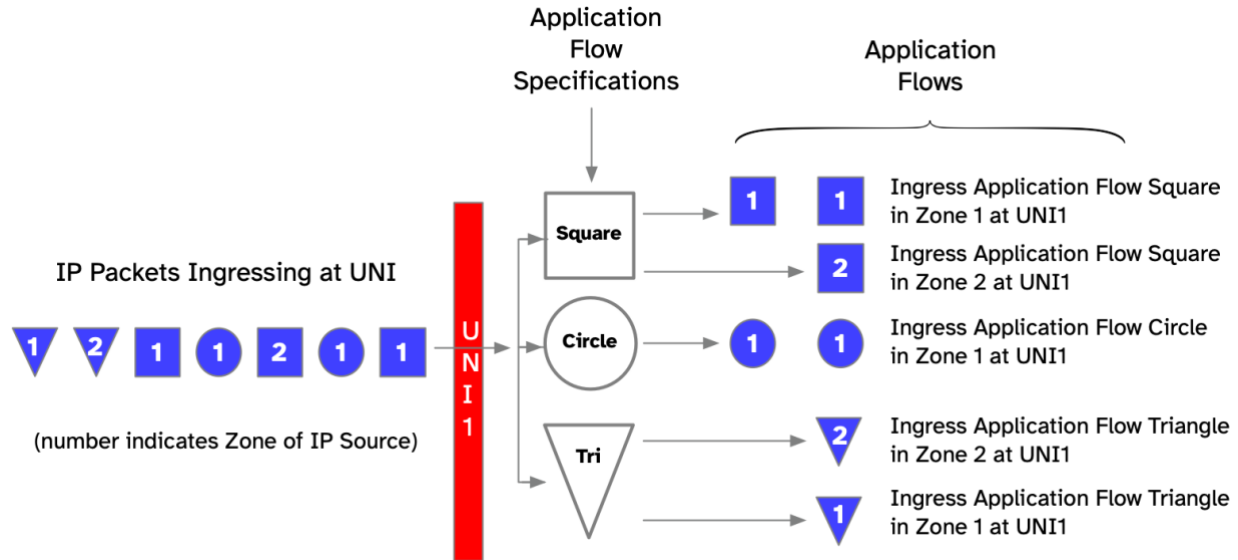
- An Application Flow can include all IP Packets from an IP address range, such as 10.10.10.x/24, which could, for example, represent all Point-of-Sale terminals at a location.

In this standard, Policies are assigned to Application Flows, not Applications. As part of the SD-WAN Service, the Subscriber and the Service Provider agree on the specifications for Application Flows that are identified at the SD-WAN UNIs. In the IP Phone example in the second bullet above, the SD-WAN Service's handling of the audio channel can be very different than its handling of the signaling channel, because a different Policy can be assigned to each. It is also possible to define a single Application Flow in such a way that it would include both of those components, in which case there would only be a single Policy assigned.

## 8.2 Application Flow Specifications and Application Flow Criteria

An "Application Flow Specification" describes a set of characteristics of the IP Packets that constitute an Application Flow. These characteristics, referred to as "Application Flow Criteria", can include matching specific packet fields (in any layer) against specific values, and can also include more complex algorithms and heuristics that inspect sequences of IP Packets. The SWVC List of Application Flow Specifications Service Attribute (section 9.12) describes the Application Flow Specifications that are available for the SWVC and the criteria (Application Flow Criteria) that compose them. Application Flow Specifications are used to categorize IP Packets that ingress at a UNI as well as IP Packets that are destined to an Egress UNI. The Service Provider is required to support some of Application Flow Criteria specified in this standard, and support is recommended for the rest. In many cases, the Service Provider provides a catalog of named, pre-defined matching criteria (accessible via the APPID Application Flow Criterion specified in section 9.12), and the Subscriber can select from the catalog. The Service Provider's catalog includes a description of the IP Packets that are matched by each of the items in the catalog.

It is often desirable to assign different Policies to IP Packets based on the Zone of the source IP host. For example, an *imap* IP Packet from Zone *engineering* may require different handling than the same IP Packet from Zone *corporate*. This concept is shown (for ingress) in the following diagram. Clearly, if the Subscriber has a single Zone, then, in effect, only the Application Flow Specification is relevant.



**Figure 10 – Application Flows<sup>9</sup>**

As shown in the diagram, a reference<sup>10</sup> to an Application Flow should include the UNI, the direction, the name of the Application Flow Specification that it matches, and its Zone—although some of these may be understood contextually.

### 8.3 Application Flow Specification Groups

Each Application Flow Specification can be a member of an “Application Flow Specification Group”. An Application Flow Specification Group provides a way to assign the same Policy to multiple Application Flow Specifications with a single assignment. See section 8.4 for more details. The SWVC List of Application Flow Specification Groups Service Attribute is described in section 9.11.

### 8.4 Policies and Policy Criteria

A Policy is a named set of Policy Criteria that can be assigned to an Application Flow and that determines how an SD-WAN Service handles IP Packets in the Application Flow. Each Policy Criterion describes a particular aspect of the handling of IP Packets to which the Policy is assigned. These aspects include requirements on UCS and TVC characteristics, forwarding requirements, security requirements, bandwidth commitments and limitations, performance goals, etc.

Policies are assigned to Application Flows at each SWVC End Point. Ingress Policies specify the desired behavior concerning forwarding of Ingress Application Flows and Egress Policies specify whether IP Packets in Egress Application Flows should be transmitted at the UNI or discarded based on security or other considerations.

<sup>9</sup> This diagram is not intended to imply any particular ordering of operations. An implementation could match Zone before Application Flow Specification, or after, or in parallel.

<sup>10</sup> There is no need in this document to formally name Application Flows, for example by assigning identifiers, but there is often a need to refer to them in explanatory text.

There are two Service Attributes that can assign a Policy to an Application Flow:

- SWVC List of Zones Service Attribute
- SWVC End Point Policy Map Service Attribute

A Zone definition in the SWVC List of Zones Service Attribute (see section 9.6) can include a Zone-wide Ingress Policy for Ingress IP Packets that match a specified Application Flow Specification or the Application Flow Specifications in an Application Flow Specification Group. This, in effect, becomes the default Ingress Policy at all SWVC End Points for Application Flows that match the Application Flow Specification(s) and that Zone.

The SWVC End Point Policy Map Service Attribute (section 10.4) allows an Ingress Policy and an Egress Policy to be assigned to a *⟨Zone, Application Flow Specification⟩* at the UNI for the SWVC End Point (i.e., an Application Flow) or to a *⟨Zone, Application Flow Specification Group⟩* at that UNI (one or more Application Flows).

This results in four ways that a Policy can be assigned to an Ingress Application Flow:

- Zone-wide Policy for an Application Flow Specification
- Zone-wide Policy for an Application Flow Specification Group
- SWVC End Point Policy Map for Application Flow Specification
- SWVC End Point Policy Map for Application Flow Specification Group

Since there are multiple mechanisms for assigning a Policy to a single Ingress Application Flow, there is a well-defined precedence as described in section 10.4.1.

For Egress Application Flows, the SWVC End Point Policy Map Service Attribute (see section 10.4) can associate an Egress Policy to an Application Flow. As with Ingress Application Flows, Egress Application Flows at an SWVC End Point (associated with the Egress UNI) are identified by matching an Application Flow Specification and a Zone, with the special case that IP Packets arriving directly from the Internet (i.e., not over a TVC) are assigned the reserved Zone name *Internet*. Section 10.4.2 provides additional detail assigning Policies to Egress Application Flows.

When a Policy is associated with an Application Flow Specification Group in a Zone at an SWVC End Point, the Policy is applied to each Application Flow that matches an Application Flow Specification that is a member of the Application Flow Specification Group. For example, using the Application Flow Specifications in Figure 10, *square*, *circle*, and *triangle* could all be members of an Application Flow Specification Group *shapes*. A Policy associated with the Application Flow Specification Group *shapes* in Zone 1 at UNI1 is assigned to the three resulting Application Flows *uni1/zone1/square*, *uni1/zone1/circle*, and *uni1/zone1/triangle*. Each of the Application Flows can, however, have an explicit Policy assignment that supersedes the Policy assigned to the Application Flow Specification Group (see section 10.4.1).

There is one exception to how Policies are applied using Application Flow Specification Groups, namely, the application of the BANDWIDTH Policy Criterion. When this Policy Criterion is in a Policy that is assigned to an Application Flow Specification Group, it operates differently, as described in section 9.10.2.9.

## 9 SD-WAN Virtual Connection (SWVC) Service Attributes

This section contains Service Attributes that apply to an SD-WAN Virtual Connection. There is one instance of these attributes for each SD-WAN Virtual Connection. The attributes are summarized in the following table, and each is described in more detail in the subsequent sections.

Attribute Name	Summary Description	Possible Values
SWVC Identifier	Identification of the SWVC for management purposes	Unique Identifier String for the SD-WAN Service.
SWVC List of End Points	The SWVC End Points that are associated by the SWVC	List of SWVC End Point Identifiers
SWVC List of UCSs	The Underlay Connectivity Services that are used by the SWVC	List of UCS Identifiers
SWVC Service Uptime Objective Service Attribute	The objective for Service Uptime for the SD-WAN Service during a Performance Evaluation Interval	<i>None</i> or a 3-tuple $\langle ts, T, \hat{U} \rangle$ where $ts$ is a date and time, $T$ is a duration, and $\hat{U}$ is a percentage between 0 and 100%
SWVC Reserved Prefixes	IP Prefixes reserved for use by the SP	<i>None</i> or list of IP Prefixes
SWVC List of Zones	A list of the Zones supported at one or more UNIs in the SD-WAN Service and Zone-wide Policies associated with the Zones	List of 3-tuples $\langle \text{name}, \text{list of IP Prefixes}, \text{list of policy mappings} \rangle$
SWVC List of Virtual Topologies	A list of named Virtual Topologies that can be assigned to Application Flows by Policy	List of 3-tuples $\langle \text{vtName}, \text{vtType}, \text{vtDescription} \rangle$
SWVC Performance Time Intervals	Time intervals used in the evaluation of the PERFORMANCE Policy Criterion and the Performance Metrics	3-tuple $\langle \text{evalinterval}, \text{arrivalinterval}, \text{irduration} \rangle$
SWVC List of Security Policies	A list of the Security Policies (defined in MEF 88) that are available for use in this SWVC	List of Security Policies (Identifier Strings)
SWVC List of Policies	A list of the Policies that can be applied to Application Flows carried by the SWVC	List of 2-tuples $\langle \text{Policy Name}, \text{List of Policy Criteria n-tuples} \rangle$
SWVC List of Application Flow Specification Groups	A list of the Application Flow Specification Groups. Each Application Flow Specification can, optionally, be a member of one of the Application Flow Specification Groups.	List of Application Flow Specification Group Names (Identifier Strings)
SWVC List of Application Flow Specifications	A list of the Application Flows Specifications that are recognized by the SD-WAN Service	List of 3-tuples $\langle \text{Application Flow Specification Name}, \text{List of Application Flow Specification Criteria}, \text{Application Flow Specification Group Name} \rangle$

**Table 3 – Summary of SWVC Service Attributes**

### 9.1 SWVC Identifier Service Attribute

The value of the SWVC Identifier Service Attribute is a string that is used by the Subscriber and the Service Provider to uniquely identify an SWVC.

- [R11] The value of the SWVC Identifier Service Attribute **MUST** be an Identifier String.
- [R12] The value of the SWVC Identifier Service Attribute **MUST** be unique across all SWVCs in the Service Provider Network.

### 9.2 SWVC List of End Points Service Attribute

The value of the SWVC List of End Points Service Attribute is a non-empty list of SWVC End Point Identifier Service Attribute values (section 10.1). The list contains one SWVC End Point Identifier value for each SWVC End Point connected by the SWVC.

- [R13] An SWVC End Point Identifier **MUST NOT** appear more than once in the value of the SWVC List of End Points Service Attribute.
- [R14] The SWVC End Points in the value of the SWVC List of End Points Service Attribute **MUST** all be associated with different UNIs.
- [R15] If an Egress IP Packet at an SWVC End Point results from an Ingress IP Packet at a different SWVC End Point, the two SWVC End Points **MUST** be associated by the same SWVC.

### 9.3 SWVC List of UCSs Service Attribute

The value of the SWVC List of UCSs Service Attribute is a non-empty list of UCS Identifier Service Attribute values (section 12.1). The list contains one UCS Identifier value for each Underlay Connectivity Service that is used by the SD-WAN Service (SWVC).

- [R16] A UCS Identifier **MUST NOT** appear more than once in the value of the SWVC List of UCSs Service Attribute.

Without at least one entry in the value of the SWVC List of UCSs Service Attribute, an SWVC cannot transport any IP Packets and is therefore not useful.

### 9.4 SWVC Service Uptime Objective Service Attribute

Service Uptime is the proportion of time, during a given time period  $T_k$ , that the SD-WAN Service is working from the perspective of the Subscriber, excluding any pre-agreed exceptions, e.g., maintenance intervals. The value of this Service Attribute is *None* or a 3-tuple  $\langle ts, T, \hat{U} \rangle$  where:

- $ts$  is a time that represents the date and time that evaluation of Service Uptime starts for the SWVC
- $T$  is a time duration, e.g., 1 month or 2 weeks, that is used in conjunction with  $ts$  to specify time intervals for determining when the Service Uptime Objective is met.

Note that the units for  $T$  are not constrained; in particular, “1 month” is an allowable value corresponding to a calendar month, e.g., from midnight on the 10<sup>th</sup> of one month up to but not including midnight the 10<sup>th</sup> of the following month.

- $\hat{U}$  is the objective for Service Uptime expressed as a percentage.

If the value of the Service Attribute is *None*, there is no Uptime Objective. If value of the Service Attribute is a 3-tuple, the time intervals are specified by the parameters  $ts$  and  $T$  in the value of this Service Attribute. One time period, denoted  $T_0$ , starts at time  $ts$  and has duration  $T$ . Each subsequent time period, denoted  $T_k$ , starts at time  $ts + kT$  where  $k$  is an integer, and has duration  $T$ ; in other words, each new time period starts as soon as the previous one ends. Service Uptime is evaluated for each time period  $T_k$ , so one can say that for a given  $T_k$ , the performance objective is either met or not met.

The definition of Service Uptime is expressed in [R17].

**[R17]** The Service Uptime for an SWVC during time period  $T_k$  **MUST** be defined as follows:

- Let  $O(T_k)$  be the total duration of outages during the time period  $T_k$ .
- Let  $M(T_k)$  be the total duration of maintenance periods during the time period  $T_k$ .
- Then define the Service Uptime  $U(T_k) = \frac{T - (M(T_k) + O(T_k))}{T - M(T_k)}$

An example of the value for this Service Attribute would be:

<”10-Jul-2018 00:00:00”, “1 month”, 99.8%>

**[R18]** If the SWVC Service Uptime Objective is not *None*, the SD-WAN Subscriber and Service Provider **MUST** agree on the definition of an outage, including determining when an outage starts and ends.

The definition of what constitutes an outage is often (but does not have to be) based on the raising and resolution of customer complaints (“trouble tickets”) rather than the actual performance of data traffic forwarded over the SD-WAN Service. The exact definition is outside the scope of this document.

**[R19]** The SWVC Service Uptime Objective for a given time interval,  $T_k$ , **MUST** be considered met if and only if  $U(T_k)$  is greater than or equal to the  $\hat{U}$  element in the value of this Service Attribute for time interval  $T_k$ .

The details of possible values of  $ts$  and  $T$  are beyond the scope of this document but, like all Service Attribute values, need to be agreed to by the Subscriber and Service Provider.

## 9.5 SWVC Reserved Prefixes Service Attribute

The SWVC Reserved Prefixes Service Attribute specifies a list of IP Prefixes that the Service Provider reserves for use for the SWVC within its own network or for distribution to the Subscriber via DHCP or SLAAC. The list can be empty or can contain IPv4 or IPv6 Prefixes or both. These

IP Prefixes need to be agreed upon so as to ensure they do not overlap with IP Prefixes assigned by the Subscriber inside the Subscriber Network.

Note that it is not necessary to reserve the Service Provider's IP address on the directly connected subnet for a UNI using this attribute; such addresses are implicitly reserved via the SD-WAN UNI IPv4 Connection Addresses Service Attribute (section 11.4) and the SD-WAN UNI IPv6 Connection Addresses Service Attribute (section 11.5).

## 9.6 SWVC List of Zones Service Attribute

As described in section 7.10, the IP hosts in the Subscriber Network can be partitioned into Zones. Application Flows are defined at a UNI based on an Application Flow Specification and a Zone, so different Policies can be assigned to IP Packets that match the same Application Flow Specification but are in different Zones.

The SWVC List of Zones Service Attribute provides the mechanism to identify the Zones supported by the SD-WAN Service and to enumerate a set of Zone-wide Policies for each Zone. A Zone-wide Policy associates a Policy with an Application Flow Specification (or Application Flow Specification Group). At each UNI that has an SWVC End Point, the Zone-wide Policy is assigned to the Application Flow that matches the Zone and Application Flow Specification unless overridden by using the SWVC End Point Policy Map Service Attribute (section 10.4). For example, a Zone-wide Policy can be used to send all web traffic (e.g., ports 80 and 443) from the Guest-Wifi Zone to an Internet Breakout.

The Zone definition includes a list of IP prefixes that defines the IP subnets that compose the Zone. A host is assigned to a Zone if the IP address of the host is a member of one of the IP Prefixes for the Zone. An Ingress IP Packet is assigned to a Zone based on its source IP address. An IP Packet directed toward a (Egress) UNI is assigned a Zone based on its source IP address unless it arrives from the Internet (i.e., did not ingress at an SD-WAN UNI), in which case it is assigned the reserved Zone *Internet*.

The value of this Service Attribute is a non-empty list of 3-tuples  $\langle zoneName, zonePrefixes, zoneIngressPolicies \rangle$  where:

- *zoneName* is an Identifier String that specifies the name of the Zone. It cannot have the values *Self*, *Internet*, or *All*.
- *zonePrefixes* is the keyword *default* or a non-empty list of IP Prefixes that identifies the hosts in the Zone
- *zoneIngressPolicies* is a list (possibly empty) of 2-tuples  $\langle zoneIngressAFS, zoneIPol \rangle$  where:
  - *zoneIngressAFS* is an Application Flow Specification Name from the value of the SWVC List of Application Flow Specifications Service Attribute (see section 9.12) or an Application Flow Specification Group Name from the value of the SWVC List of Application Flow Specification Groups Service Attribute (see section 9.11).
  - *zoneIPol* is the name of an Ingress Policy (see section 9.9)

Note that the value of this Service Attribute is a non-empty list, so definition of at least one Zone is required in each SWVC. In this case, the Zone can map all IP Packets or a subset of them.

- [R20] A Zone name, *zoneName*, **MUST** appear at most once in the value of the SWVC List of Zones Service Attribute.

The reserved Zone name *Internet* is used to assign Egress Policies to Application Flows coming from the Internet.

- [R21] An IP Prefix listed in *zonePrefixes* associated with a specific *zoneName* **MUST NOT** overlap with an IP Prefix listed in *zonePrefixes* associated with another *zoneName*.
- [R22] If *zonePrefixes* in any 3-tuple is *default*, all IP hosts in the Subscriber Network that are not assigned to any other Zone **MUST** be assigned to that Zone.
- [R23] The number of 3-tuples in the value of the SWVC List of Zones Service Attribute that have the keyword *default* in the *zonePrefixes* element **MUST NOT** be greater than 1.
- [R24] If the IP host associated with the source IP address of an Ingress IP Packet is not assigned to a Zone, the IP Packet **MUST** be discarded.

Note that IP Packets will not be discarded due to [R24] if a default zone is defined.

- [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.
- [R26] An IP Packet that arrives from the Internet **MUST** be assigned to the reserved Zone *Internet*.
- [R27] An Application Flow Specification Name or Application Flow Specification Group Name, *zoneIngressAFS*, **MUST** appear at most once in the Zone-wide Policy list, *zoneIngressPolicies*.
- [R28] A Zone name, *zoneName*, in the value of the SWVC List of Zones Service Attribute **MUST NOT** be one of the reserved names *Self*, *Internet*, or *All*. (See section 9.10.2.5.)

An example of the value of this Service Attribute might be:

```
[["Guest-Wifi", [192.168.1.0/24, 192.168.2.0/24], [{"webflows", "IBpolicy"}]],  
["Corp", [192.168.3.0/24], [{"webflows", "IBpolicy"}, {"vnc", "Block"}, {"else", "private"}]]]
```

In this example, two Zones are defined, *Guest-Wifi* and *Corp*. The *Guest-Wifi* Zone has one Zone-wide Policy mapping, *IBpolicy*, to forward all web traffic (*webflows*) directly to the Internet (via Internet Breakout). The *Corp* Zone has three global Policy mappings: all web traffic is forwarded to the Internet via *IBpolicy*; all screen-sharing traffic using the *vnc* protocol is blocked via the *Block* Policy; and everything *else* is sent over a UCS that is a private network, via *private* Policy.

## 9.7 SWVC List of Virtual Topologies Service Attribute

As described in section 7.11, an SD-WAN Service can present different forwarding topologies to different Application Flows. The SWVC List of Virtual Topologies Service Attribute provides the mechanism for defining these different forwarding topologies. The value of this Service Attribute is a list of 3-tuples of the form  $\langle vtName, vtType, vtEP \rangle$  where:

- *vtName* is an Identifier String that specifies the name of the Virtual Topology.
- *vtType* provides a description of the type of connectivity provided by the Virtual Topology. *vtType* can have one of the following values: *multipoint-to-multipoint*, *rooted-multipoint*.
- *vtEP* provides details of the SWVC End Points that are connected by the Virtual Topology. The form of *vtEP* is different for each value of *vtType*.

**[R29]** A Virtual Topology name, *vtName*, **MUST** appear exactly once in the value of the SWVC List of Topologies Service Attribute.

**[R30]** A Virtual Topology name, *vtName*, **MUST NOT** have the reserved name *Swvc*.

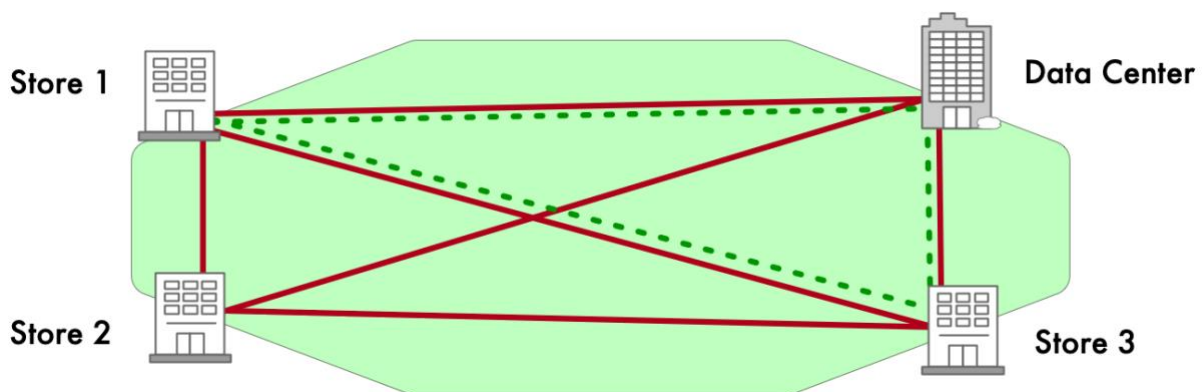
The reason for [R30] is that every SWVC has a pre-defined multipoint-to-multipoint Virtual Topology named *Swvc* that connects all SWVC End Points in the SWVC. Therefore, the value of this Service Attribute can be an empty list.

Specific details on each Virtual Topology type and its associated *vtEP* are described in sections 9.7.1 and 9.7.2. Section 9.10.2.4 includes requirements that define the specific forwarding constraints associated with each *vtType*.

### 9.7.1 *vtType=multipoint-to-multipoint*

The value *multipoint-to-multipoint* for *vtType* indicates that the Virtual Topology allows IP Packets in an Application Flow to be forwarded from any SWVC End Point specified in the *vtEP* element to any other SWVC End Point specified in the *vtEP* element.

**[R31]** If the value of *vtType* is *multipoint-to-multipoint* for a Virtual Topology in the SWVC List of Virtual Topologies Service Attribute, the value for *vtEP* **MUST** be a list of at least two SWVC End Point Identifiers (section 10.1).



**Figure 11 – Examples of two multipoint-to-multipoint Virtual Topologies**

Figure 11 shows an example of a multipoint-to-multipoint Virtual Topology in an SD-WAN network with four SD-WAN Edges. The red solid lines show a multipoint-to-multipoint Virtual Topology that contains all SWVC End Points, and the green dotted lines show another multipoint-to-multipoint Virtual Topology that contains End Points *Store 1*, *Store 3*, and *Data Center*.

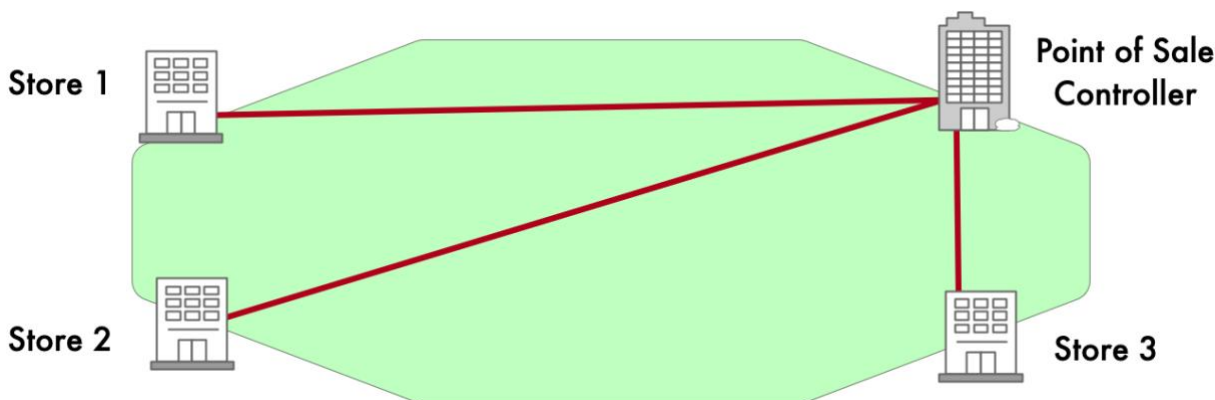
### 9.7.2 vtType=rooted-multipoint

In the case of *multipoint-to-multipoint*, all the SWVC End Points included in the topology have full connectivity to each other. A *rooted-multipoint* Virtual Topology, on the other hand, has restricted connectivity, i.e., traffic can be forwarded between some pairs of SWVC End Points, but not other pairs. This topology is often called a *tree* topology. Using this latter analogy, a rooted-multipoint Virtual Topology has some End Points referred to as *root* SWVC End Points and some SWVC End Points referred to as *leaf* SWVC End Points.

Root SWVC End Points have no forwarding restrictions, i.e., they can communicate with all other root SWVC End Points as well as all leaf SWVC End Points in the Virtual Topology. Leaf SWVC End Points, on the other hand, can only communicate with root SWVC End Points.

- [R32] If the value of *vtType* is *rooted-multipoint* for a Virtual Topology in the SWVC List of Virtual Topologies Service Attribute, the value of *vtEP* for the Virtual Topology **MUST** be a 2-tuple  $\langle \text{rootlist}, \text{leaflist} \rangle$ , where *rootlist* is a non-empty list of SWVC End Point Identifiers of root SWVC End Points and *leaflist* is a non-empty list of SWVC End Point Identifiers of leaf SWVC End Points (section 10.1).
- [R33] If the value of the *vtType* is *rooted-multipoint* for a Virtual Topology in the SWVC List of Virtual Topologies Service Attribute, an SWVC End Point Identifier **MUST** appear at most once in either the list of root SWVC End Points or the list of leaf SWVC End Points.

As noted in [R32], there must be at least one root SWVC End Point and one leaf SWVC End Point in the Virtual Topology. A tree with just two SWVC End Points is not very interesting (it is, in effect, just a multipoint-to-multipoint topology with two End Points), but additional SWVC End Points can be added.



**Figure 12 – Example of rooted-multipoint Virtual Topology**

Figure 12 shows an example of a *rooted-multipoint* Virtual Topology in an SD-WAN Service with four SD-WAN Edges. There is only a single root SWVC End Point, but there could be more than one. For example, there could be a backup POS controller at another location. The two controllers could communicate with each other since they would both be at root SWVC End Points, and all three stores (leaf SWVC End Points) could communicate with both controllers.

## 9.8 SWVC Performance Time Intervals Service Attribute

The SWVC Performance Time Intervals Service Attribute specifies a set of time intervals used in the determination of the performance of all Paths in the SWVC. The value of the Service Attribute is a 3-tuple  $\langle evalinterval, arrivalinterval, irduration \rangle$  where:

- *evalinterval* is the “look-back” interval in milliseconds for evaluation of the Performance Metrics specified in the PERFORMANCE Policy Criterion (section 9.10.2.8). The value is the interval over which the performance is evaluated, for example, 10,000 milliseconds.
- *arrivalinterval* is the difference in arrival times (specified in milliseconds) at the Ingress UNI between two packets used to compute the Mean One-Way Packet Delay Variation (as described in section 15.4).
- *irduration* is the time interval in milliseconds over which the Information Rate is determined in the evaluation of the BANDWIDTH Policy Criterion.

**[D1]** The *irduration* used for the BANDWIDTH Policy Criterion **SHOULD NOT** exceed 1000 milliseconds.

## 9.9 SWVC List of Security Policies Service Attribute

The value of the SWVC List of Security Policies Service Attribute is *None* or a non-empty list of Security Policies that are available for use with this SWVC. MEF 88 [33] section 6 defines the structure and content of each Security Policy in the SWVC List of Security Policies Service Attribute. The Security Policies are assigned to Ingress and Egress Application Flows via the AF-SECURITY-INGRESS Policy Criterion (section 9.10.2.10) and the AF-SECURITY-EGRESS Policy Criterion (section 9.10.3.2). One of the Security Policy parameters defined in MEF 88 [33] is the Security Policy Identifier.

## 9.10 SWVC List of Policies Service Attribute

Associated with each SWVC is a list of named Policies that can be assigned to each Application Flow using the SWVC End Point Policy Map (see section 10.4), or via Zone-wide Policies specified in the SWVC List of Zones (see section 9.6).

A Policy is composed of Policy Criteria. Each Policy Criterion is either an Ingress Policy Criterion—meaning that it is applicable to Ingress Application Flows—or an Egress Policy Criterion—meaning that it is applicable to Egress Application Flows—and each Policy can only contain one type (Ingress or Egress). If a Policy includes Ingress Policy Criteria, it is referred to as an Ingress Policy, and if a Policy includes Egress Policy Criteria, it is referred to as an Egress Policy.

The value of this Service Attribute is a non-empty list of 2-tuples of the form  $\langle polName, polCL \rangle$  where:

- *polName* is an Identifier String that specifies the name of the Policy. *polName* cannot be “Block” or “None”.
- *polCL* is a non-empty list of Policy Criteria 2-tuples, of the form  $\langle PCname, PCparam \rangle$  where:
  - *PCname* is an Identifier String containing a Policy Criterion name from Table 5, or a Service Provider-defined Policy Criterion name.
  - *PCparam* is a parameter value specific to the Policy Criterion specified in *PCname*.

**[R34]** A Policy name, *polName*, in the value of the SWVC List of Policies Service Attribute **MUST** appear, at most, once.

**[R35]** A Policy Criterion name, *PCname*, **MUST** appear, at most, once in each list of Policy Criteria, *polCL*, in the value of the SWVC List of Policies Service Attribute.

**[R36]** A Policy **MUST** contain either Ingress Policy Criteria or Egress Policy Criteria but not both.

**[R37]** The Policy Criteria supported by the Service Provider for composing SD-WAN Policies **MUST** include the Policy Criteria listed in Table 4.

PCname	Ingress / Egress	Description	Values
ENCRYPTION	Ingress	Indicates whether the Application Flow requires encryption	<i>Required-Always, Required-Public-Only, or Optional</i>
INTERNET-BREAKOUT	Ingress	Indicates whether the Application Flow should be forwarded to an Internet destination	<i>Enabled, Disabled</i>
PUBLIC-PRIVATE	Ingress	Indicates whether the Application Flow can traverse Internet Access Underlay Connectivity Services or not	<i>Private-only, Either</i>
BACKUP	Ingress	Indicates whether this Application Flow can use a UCS designated as “backup”	<i>Enabled, Disabled</i>

**Table 4 – Policy Criteria – Support Required**

**[D2]** The Policy Criteria supported by the Service Provider for composing SD-WAN Policies **SHOULD** include the Policy Criteria listed in Table 5.

PCName	Ingress / Egress	Description	Values
VIRTUAL-TOPOLOGY	Ingress	Indicates the Virtual Topology that the Application Flow should be forwarded over	Virtual Topology Name
ALLOWED-DESTINATION-ZONES	Ingress	Specifies which Zones the IP Packets in the Application Flow can be delivered to	A list of Zone Names
BILLING-METHOD	Ingress	Indicates whether the Application Flow can be sent over an Underlay Connectivity Service that has usage-based or flat-rate billing	<i>Flat-Rate-Only, Usage-Based-Only, Either</i>
PERFORMANCE	Ingress	Specifies a list of performance requirements for the Application Flow	See section 9.10.2.8
BANDWIDTH	Ingress	Specifies a bandwidth commitment and bandwidth limit on the Application Flow.	2-tuple containing the committed bandwidth and the bandwidth limit.
AF-SECURITY-INGRESS	Ingress	Specifies a list of Security functions to apply to the Application Flow at the Ingress UNI	<i>None</i> or an Application Flow Security Policy Identifier
BLOCK-SOURCE	Egress	Indicates specific ingress locations to disallow for egress	<i>List containing UNI and/or INTERNET</i>
AF-SECURITY-EGRESS	Egress	Specifies a list of Security functions to apply to the Application Flow at the Egress UNI	<i>None</i> or an Application Flow Security Policy Identifier

**Table 5 – Policy Criteria – Support Recommended**

Note that the Policy Criteria names used in Table 4 and Table 5 and the syntax used in the examples below are intended to describe the behavior of each Policy Criterion, and not to mandate an implementation or syntax. For example, no implementation needs to have a command or configuration parameter called BILLING-METHOD, but rather it can provide Policy functionality consistent with the BILLING-METHOD Policy Criterion described in this document.

The behavior of these Policy Criteria is described in subsequent sections.

**[R38]** If the Service Provider defines its own Policy Criteria, the description of each Policy Criterion agreed upon with the Subscriber **MUST** include the following items:

- A name for the Policy Criterion
- The possible values for the Policy Criterion
- The behavior associated with each value
- Whether it is an Ingress Policy Criterion or an Egress Policy Criterion
- The behavior of each value when used with INTERNET-BREAKOUT (for Ingress Policy Criteria)

- Any interactions that the Policy Criterion has with other Policy Criteria

**[R39]** If the Service Provider defines its own Policy Criterion as described in [R38], it **MUST NOT** reuse the *PCnames* in Table 4 and Table 5.

Example Ingress Policies (ipA and ipB) and Egress Policies (epA and epB) are shown below:

```
[  
  (ipA, [  
    (ENCRYPTION, Required-Always),  
    (INTERNET-BREAKOUT, Disabled),  
    (PUBLIC-PRIVATE, Either),  
    (BILLING-METHOD, Flat-rate-only),  
    (BACKUP, Disabled),  
    (VIRTUAL-TOPOLOGY, "Swvc" ),  
    (BANDWIDTH, (20Mbps, 50Mbps))  
  ]),  
  
  (ipB, [  
    (ENCRYPTION, Required-Public-Only),  
    (INTERNET-BREAKOUT, Disabled),  
    (PUBLIC-PRIVATE, Private-only),  
    (BILLING-METHOD, Flat-rate-only),  
    (BACKUP, Enabled),  
    (VIRTUAL-TOPOLOGY, "EngFacilities" ),  
    (BANDWIDTH, 50Mbps, None)  
  ]),  
  
  (epA, [(BLOCK-SOURCE, [INTERNET])]) ,  
  
  (epB, [(BLOCK-SOURCE, [UNI])])  
]
```

### 9.10.1 Policy Criteria specification and interaction

Each Service Provider supports a set of Policy Criteria that can include both criteria from the lists in Table 4 and Table 5 as well as other criteria defined by the Service Provider (see [R39] and [R38]). For a given SD-WAN Service, the Subscriber and the Service Provider agree (via this Service Attribute) on the criteria that will be used. This may be the entire set of Policy Criteria supported by the Service Provider or a subset.

**[R40]** Every Ingress Policy agreed on for a specific SD-WAN Service **MUST** include the same set of Policy Criteria.

**[R41]** For an Ingress IP Packet in a given Application Flow, if the Service Provider cannot forward the packet to the destination over an Underlay Connectivity Service (or a sequence of Underlay Connectivity Services) that meets the Policy for that Application Flow, the packet **MUST** be discarded.

[R40] requires that every Ingress Policy in an SD-WAN Service has the same set of Policy Criteria (although, clearly, the Policy Criteria can have different values). This ensures that all Policies are consistent, i.e., it avoids the “don’t know” situation. If, for example, the ALLOWED-DESTINATION-ZONES Policy Criterion were to be used in Policy A but not in Policy B, then

when forwarding an IP Packet in an Application Flow that has been assigned Policy B, there is no way to determine whether or not it can be delivered to the destination UNI.

It is possible that some Ingress Policy Criteria aren't relevant for a particular Policy, so most of the Ingress Policy Criteria include a way to indicate that they shouldn't be used in the determination of how IP Packets should be forwarded, such as a value of *Either* or *Any*.

[R41] indicates two necessary conditions that must be met for an IP Packet to be forwarded by the SD-WAN Service:

- A forwarding path exists, and
- The forwarding path meets the Policy assigned to the Application Flow

There is not a requirement like [R40] for Egress Policies. Since Egress Policies are used to inhibit the delivery of IP Packets to the Egress UNI, each one is tailored to the specific requirements for that purpose.

A few of the Policy Criteria descriptions in the following section refer to a TVC or UCS as being available or not available. Being "available" in this context means that it meets the two [R41] conditions. It is the Service Provider's responsibility to ensure that these conditions are met, but there can be transient and failure situations when they are not met.

Many of the Policy Criteria (but not all) are used to specify conditions that restrict the TVCs that are eligible to carry the Application Flow. Most of these Policy Criteria are binary, i.e., a TVC (in the Path used to forward the Application Flow) is eligible or not. The intersection of TVCs that satisfy these Policy Criteria provide an initial determination of the paths that can carry the Application Flow.

There are, however, some Policy Criteria that are not binary. For example, the PERFORMANCE Policy Criterion results in an ordered list of Paths based on a determination of how well they meet the stated performance goals for the Application Flow. The BANDWIDTH Policy Criterion is one of the few Policy Criteria that are more focused on individual IP Packets in the Application Flow rather than the Application Flow itself.

### 9.10.2 Ingress Policy Criteria

This section describes the parameters and behavior of the Ingress Policy Criteria specified in this document.

#### 9.10.2.1 ENCRYPTION Ingress Policy Criterion

The ENCRYPTION Policy Criterion provides a mechanism to specify whether an Application Flow is required to traverse encrypted TVCs. It can have the value *Required-Always*, *Required-Public-Only*, or *Optional*.

**[R42]** If Policy Criterion ENCRYPTION=*Required-Always* is applied to an Application Flow, the Path chosen for forwarding the Application Flow **MUST** include only TVCs that encrypt IP Packets in the Application Flow before forwarding over the Underlay Connectivity Service.

- [R43] If Policy Criterion ENCRYPTION=*Required-Public-Only* is applied to an Application Flow, any TVCs in the Path chosen for forwarding the Application Flow that traverse Public UCSs **MUST** encrypt IP Packets in the Application Flow before forwarding over the Public UCS.

[R42] and [R43] mean that encryption is applied by the SD-WAN Edge before packets are forwarded over the UCS UNI, and decryption is applied to packets received from the UCS at the destination SD-WAN Edge.<sup>11</sup>

- [R44] If Policy Criterion ENCRYPTION=*Optional* is applied to an Application Flow, then the Policy Criterion **MUST NOT** be considered in the forwarding decision for the Application Flow.

*Optional* indicates that the Subscriber doesn't need encryption for the Application Flow and it can be sent over either encrypted or unencrypted TVCs.

#### 9.10.2.2 PUBLIC-PRIVATE Ingress Policy Criterion

An SD-WAN Service can use *private* Underlay Connectivity Services such as MEF Carrier Ethernet Services and *public* Underlay Connectivity Services, i.e., Internet Access Services. The PUBLIC-PRIVATE Policy Criterion provides control over whether or not an Application Flow can traverse a public Underlay Connectivity Service, i.e., the Internet. It can have the value *Private-Only* or *Either*.

- [R45] If Policy Criterion PUBLIC-PRIVATE=*Private-Only* is applied to an Application Flow, the Path chosen for forwarding the Application Flow **MUST** include only TVCs that traverse a UCS whose UCS Type Service Attribute=*Private* (section 12.2).
- [R46] If Policy Criterion PUBLIC-PRIVATE=*Either* is applied to an Application Flow, then the Policy Criterion **MUST NOT** be considered in the forwarding decision for the Application Flow.

#### 9.10.2.3 BILLING-METHOD Ingress Policy Criterion

The cost for the use of a particular Underlay Connectivity Service can be flat rate (i.e., based on units of time such as \$500/month) or usage-based (i.e., based on how much data is sent across it such as \$10/TB). The BILLING-METHOD Policy Criterion provides control over the charge type of the network that can be used to forward an Application Flow. It can have the value *Flat-rate-Only*, *Usage-based-Only*, or *Either*.

- [R47] If Policy Criterion BILLING-METHOD=*Flat-rate-Only* is applied to an Application Flow, the Path chosen for forwarding the Application Flow **MUST** traverse UCSs whose UCS Billing Method Service Attribute=*Flat-rate* (section 12.3).

<sup>11</sup> Requirements related to the level and type of encryption are out of scope but may be addressed in a future version of the specification.

- [R48] If Policy Criterion BILLING-METHOD=*Usage-based-Only* is applied to an Application Flow, the Path chosen for forwarding the Application Flow **MUST** traverse UCSs whose UCS Billing Method Service Attribute=*Usage-based* (section 12.3).
- [R49] If Policy Criterion BILLING-METHOD=*Either* is applied to an Application Flow, then the Policy Criterion **MUST NOT** be considered in the forwarding decision for the Application Flow.

Refer to MEF 74 [32] for examples of a broader range of billing options that are currently beyond the scope of this document.

#### 9.10.2.4 VIRTUAL-TOPOLOGY Ingress Policy Criterion

The value of the VIRTUAL-TOPOLOGY Ingress Policy Criterion is either a Virtual Topology name from the *vtName* element in the value of the SWVC List of Virtual Topologies Service Attribute (section 9.7) or the value *Swvc*. The value specifies the Virtual Topology used to constrain forwarding of Ingress Application Flows to which it is applied.

Each Virtual Topology includes a list (or possibly two lists) of SWVC End Point Identifiers (see section 9.7), and the SWVC End Point is “in” the Virtual Topology if its Identifier is included in one of these lists.

- [R50] A Policy **MUST NOT** be assigned to an Application Flow for a UNI if the SWVC End Point at that UNI is not in the Virtual Topology specified in the VIRTUAL TOPOLOGY Policy Criterion in the Policy.

[R50] specifies the restriction on the SWVC End Point where a Virtual Topology is assigned to an Ingress Application Flow. Restrictions on the SWVC End Points at which the Application Flow can egress are specified independently for each of the Virtual Topology types.

- [R51] If Ingress Policies for an SWVC do not include the VIRTUAL-TOPOLOGY Policy Criterion, the behavior of every Policy **MUST** be as if *VIRTUAL-TOPOLOGY Swvc* were included in it.
- [R52] When a Policy containing the VIRTUAL-TOPOLOGY Policy Criterion is assigned to an Application Flow at an SWVC End Point and the value of *vtType* that is associated with the specified *vtName* is *multipoint-to-multipoint*, IP Packets in that Application Flow **MUST** egress only at SWVC End Points that are in the list of SWVC End Points for the Virtual Topology.

The *Swvc* Virtual Topology (see [R51]) is a multipoint-to-multipoint Virtual Topology that includes all SWVC End Points, and therefore an Ingress IP Packet assigned to the *Swvc* Virtual Topology can egress at any other SWVC End Point in the SWVC.

- [R53] When a Policy containing the VIRTUAL-TOPOLOGY Policy Criterion is assigned to an Application Flow at an SWVC End Point:

- if the value of *vtType* that is associated the specified *vtName* is rooted-multipoint, and
- if the SWVC End Point is in the list of leaf End Points in the Virtual Topology,

Then IP Packets in that Application Flow **MUST** egress only at SWVC End Points that are in the list of root End Points for the Virtual Topology.

**[R54]** When a Policy containing the VIRTUAL-TOPOLOGY Policy Criterion is assigned to an Application Flow at an SWVC End Point:

- if the value of *vtType* that is associated the specified *vtName* is *rooted-multipoint*, and
- if the SWVC End Point is in the list of root End Points in the Virtual Topology,

Then IP Packets in that Application Flow **MUST** egress only at SWVC End Points that are in the list of root SWVC End Points or the list of leaf SWVC End Points for the Virtual Topology.

[R53] and [R54] describe the forwarding restrictions associated with a rooted-multipoint Virtual Topology. [R53] specifies that an IP Packet that arrives from the Subscriber Network at a leaf SWVC End Point can only egress at a root SWVC End Point that is in the Virtual Topology, whereas [R54] indicates that if the ingress is at a root SWVC End Point, it can egress at any End Point in the Virtual Topology, root or leaf.

#### 9.10.2.5 ALLOWED-DESTINATION-ZONES Ingress Policy Criterion

The ALLOWED-DESTINATION-ZONES Ingress Policy Criterion indicates the Zones that an Ingress Packet can be delivered to, i.e., the Zones of destination IP hosts as determined by the destination IP addresses. The value is either *All* or a non-empty list where each entry is either the reserved name *Self* or a Zone name (see section 9.6).

The reserved name *Self* is equivalent to the Zone that the IP Packet is in (i.e., the Zone of the source IP host). This allows a Policy to be reused for different Zones. Hence, ALLOWED-DESTINATION-ZONES *Self* means that the IP Packet can only be delivered to an Egress UNI if the destination address in the IP Packet is in the same Zone as the source address. Similarly, ALLOWED-DESTINATION-ZONES [*corp*, *Self*] means that the IP Packet can only be delivered to an Egress UNI if the destination address in the IP Packet is in the same Zone as the source address or is in Zone “corp”. Note that, in some cases, *Self* could actually be “corp” but this doesn’t have any impact on the Policy Criterion.

**[R55]** If the value of the ALLOWED-DESTINATION-ZONES Policy Criterion is a list of Zone names, each entry in the list **MUST** either be *Self* or be in the value of the SWVC List of Zones Service Attribute (section 9.6).

**[R56]** If the value of the ALLOWED-DESTINATION-ZONES Policy Criterion is a list of Zone names, each entry in the list **MUST** be unique.

Note that [R55] implies that the reserved Zone name *Internet* cannot be used as a value for this Policy Criterion. [R56] requires that each Zone name (including *Self*) can appear in the list exactly once.

**[R57]** A unicast IP Packet in an Application Flow **MUST NOT** be forwarded to an Egress UNI unless the value of the ALLOWED-DESTINATION-ZONES Policy Criterion is *All*, or the Destination Address in the IP Packet maps to either:

- one of the Zones listed in the ALLOWED-DESTINATION-ZONES Ingress Policy Criterion; or
- the Zone of the source IP host, if the ALLOWED-DESTINATION-ZONES Policy Criterion includes *Self*.

**[R58]** If Ingress Policies for the SWVC do not include the ALLOWED-DESTINATION-ZONES Policy Criterion, the behavior of every Policy **MUST** be as if *ALLOWED-DESTINATION-ZONES Self* were included in it.

[R58] indicates that if the Ingress Policies do not include the ALLOWED-DESTINATION-ZONES Policy Criterion (since either they all include it or none of them includes it), then each IP Packet (in all Application Flows) can only be forwarded to destinations that are in the same Zone as the IP Packet.

#### 9.10.2.6 *INTERNET-BREAKOUT Ingress Policy Criterion*

The INTERNET-BREAKOUT Policy Criterion indicates whether IP Packets in the Application Flow should be forwarded to an Internet destination and not to another UNI (see section 7.12). It can have the value *Enabled* or *Disabled*.

**[R59]** If the Policy Criterion INTERNET-BREAKOUT=*Enabled* is applied to an Application Flow, IP Packets in the Application Flow **MUST** be forwarded to Internet destinations over an Internet Access UCS at a UCS End Point with the UCS End Point Breakout Service Attribute = *Enabled* (section 14.3).

The Service Provider chooses an appropriate Internet Access UCS over which to forward IP Packets in the Application Flow. This may be an Internet Access UCS connected directly to the SD-WAN Edge where the Ingress UNI for the Application Flow is located, or it may be an Internet Access UCS located at another SD-WAN Edge (in which case the IP Packets are sent first over one or more TVCs to that SD-WAN Edge).

**[R60]** If the Policy Criterion INTERNET-BREAKOUT=*Disabled* is applied to an Application Flow, IP Packets in the Application Flow **MUST NOT** be forwarded to Internet destinations by the SD-WAN Service.

As a consequence of [R59] and [R60] either no IP Packets in the Application Flow are forwarded to other UNIs, or no IP Packets in the Application Flow are forwarded to Internet destinations.

**[R61]** If the Policy Criterion INTERNET-BREAKOUT=*Enabled* is applied to an Application Flow, all of the other Policy Criteria specified in Table 4 and Table

5, except BANDWIDTH, BILLING-METHOD, and AF-SECURITY-INGRESS, **MUST** be ignored for the Application Flow if it is forwarded to the Internet via Local Internet Breakout.

[R61] acknowledges that the other Policy Criteria (e.g., PUBLIC-PRIVATE and ENCRYPTION) are not relevant for Local Internet Breakout, except for those specified. Application Flows for packets destined for the Internet can have Bandwidth limitations. On the other hand, if the Internet Breakout occurs at an SD-WAN Edge other than the local one, the other Policy Criteria are used to describe its handling within the SD-WAN Service until the breakout location is reached.

**[R62]** If no Application Flows at a UNI are assigned a Policy that includes INTERNET-BREAKOUT=*Enabled*, then IP Packets from the Internet that are destined to the UNI **MUST** be discarded.

The purpose of [R62] is to protect the Subscriber Network from unsolicited Internet traffic. If none of the Application Flows at the UNI can “break out” to the Internet, then no traffic from the Internet should be forwarded back to the Subscriber at the UNI.

**[R63]** If Ingress Policies for the SWVC do not include the INTERNET-BREAKOUT Policy Criterion, the behavior of every Policy **MUST** be as if *INTERNET-BREAKOUT Disabled* were included in it.

#### 9.10.2.7 **BACKUP Ingress Policy Criterion**

A UCS can be designated as *Backup* at one or more of its UCS End Points (section 14.2). When there is at least one non-*Backup* UCS available at an SD-WAN Edge (availability of a UCS is defined by the explanatory text after [R41]), Application Flows are not forwarded toward the egress UNI over a UCS that is designated as *Backup*. However, since a *Backup* UCS may have lower bandwidth and/or higher cost, it may be desirable to restrict which Application Flows are permitted to use them. This control can be achieved using the BACKUP Policy Criterion. It can have the value *Enabled* or *Disabled*.

**[R64]** Application Flows **MUST NOT** be forwarded toward the destination UNI over a UCS End Point where the UCS End Point Backup Service Attribute=*Enabled*, if a Path to the destination egress UNI is available over a non-*Backup* UCS (i.e., where that Service Attribute value is *Disabled*).

**[R65]** If the Policy Criterion BACKUP=*Disabled* is assigned to an Application Flow, then IP Packets in the Application Flow **MUST** be discarded if only Paths to the destination egress UNI over *Backup* UCSs are available.

Note that Application Flows that have BACKUP=*Enabled* will likely be more resilient than those with BACKUP=*Disabled*.

### 9.10.2.8 PERFORMANCE Ingress Policy Criterion

One of the benefits of SD-WAN is that, assuming that there are multiple ways of reaching a destination, the SD-WAN Service can dynamically choose a Path that best meets the Policy applied to an Application Flow, and this includes Policy Criteria associated with performance.

An SD-WAN service can monitor the performance of the various Paths between SD-WAN Edges in real time and adjust the forwarding decisions based on the most recently measured performance. This document does not specify how or when an SD-WAN implementation measures performance or even that it does measure it.

The PERFORMANCE Policy Criterion allows the Subscriber to indicate the important Performance Metrics for each Ingress Application Flow. The value of the PERFORMANCE Policy Criterion is a 2-tuple *(primary, secondary)* where:

- *primary* is a 2-tuple *(metric, threshold)* or *None* that describes the most important Performance Metric for this Policy. *metric* is one of the Performance Metrics listed in Table 6 and *threshold* is a value for this Performance Metric described in the following paragraph or *None*.
- *secondary* is a list of zero or more 2-tuples *(metric, threshold)*. *metric* is one of the Performance Metrics listed in Table 6 and *threshold* is a value for this Performance Metric described in the following paragraph or *None*.

The *threshold* element in the previous definitions is a value for the Performance Metric that indicates the point at which the use of the Path for this Application Flow is questionable, i.e., if the value of this Performance Metric is worse than the *threshold*, use of the Path for this Application Flow should be avoided if possible—it should only be used as a last resort (see [R67]).

Performance Metric Name	Description
One-Way Mean Packet Delay	See section 15.3
One-Way Mean Packet Delay Variation	See section 15.4
One-Way Packet Loss Ratio	See section 15.5

**Table 6 – Performance Metrics**

The result of most Policy Criteria are binary decisions, i.e., a Path is acceptable or not, whereas the result of the PERFORMANCE Policy Criterion is described as an ordered list of acceptable Paths. The Performance Metrics specified in the value of the PERFORMANCE Policy Criterion are evaluated for each Path to the Egress UNI and the Paths are ordered by how well they meet the stated performance goals.

There is an expectation that if the Subscriber and the Service Provider agree to use a particular Performance Metric in the PERFORMANCE Ingress Policy Criterion, then the Service Provider measures that Performance Metric on a suitable basis.

- [R66] A Performance Metric parameter, *metric*, **MUST NOT** appear more than once in the value of the PERFORMANCE Policy Criterion, either in the *primary* element or the *secondary* element.
- [R67] A Path whose performance for any of the specified Performance Metrics (*primary* or *secondary*) is worse than the *threshold* value, if not *None*, **MUST** be placed in the list of Paths that result from the evaluation of this Policy Criterion after all Paths for which this is not the case.
- [R68] All Paths other than those described by [R67] **MUST** be ordered based on the Performance Metric specified in *primary*, from best to worst, except when the value of *primary* is *None*.

Note that [R67] and [R68] together indicate that a *threshold* is not needed for the *primary* Performance Metric if there are no *secondary* Performance Metrics specified, since the list will be ordered by the value of the *primary* and the worst performing Paths will always be at the end of the list.

- [D3] Forwarding of an IP Packet in an Application Flow to which the PERFORMANCE Policy Criterion is applied **SHOULD** favor Paths that appear earlier in the list of Paths that result from evaluation of the PERFORMANCE Policy Criterion.

Since the list is ordered based on the most important Performance Metric (except for those Paths demoted due to [R67]), [D3] indicates that it is desirable to use a Path that is earlier in the list. However, although the first Path in the list has the best *primary* performance, it might not be the best choice. For example, another item in the list might have acceptable *primary* performance but better overall performance taking into account other Performance Metrics. There could also be queueing issues, bandwidth issues, etc., that make the top item on the list less desirable.

In the following examples, the PERFORMANCE Policy Criterion is:

PERFORMANCE <(<"One-way Packet Delay", 20ms>, <"One-way Packet Loss Ratio", .03%>)>

There are three Paths to the destination, A, B, and C. In each case the values for the two Performance Metrics are shown and the Paths are listed in the order that would result from evaluation of this Policy Criterion

Case 1:

A = <10ms, .01%>

B = <12ms, .01%>

C = <12ms, .02%>

All values are less than the thresholds and the list is ordered based on the primary Performance Metric. In theory, B and C could be in the other order since they have the same value for the primary Performance Metric, but it is reasonable to assume that an implementation might order

these Paths based on the secondary Performance Metric in this case.

Case 2:

B =  $\langle 12\text{ms}, .01\% \rangle$

C =  $\langle 12\text{ms}, .02\% \rangle$

A =  $\langle 10\text{ms}, .04\% \rangle$

In this case, Path A with the best One-way Packet Delay has a One-way Packet Loss Ratio that jumped up above the threshold, so as indicated in [R67] that Path is placed at the end of the list.

Case 3:

C =  $\langle 12\text{ms}, .02\% \rangle$

A =  $\langle 10\text{ms}, .035\% \rangle$

B =  $\langle 21\text{ms}, .01\% \rangle$

In this case, the One-way Packet Delay for Path B jumped up to 21ms which is above the threshold for that Performance Metric. Although the One-way Packet Loss Ratio for Path A improved over Case 2, it is still above the threshold. So, both Path A and Path B were moved to the end of the list and Path C is now the favored Path.

#### 9.10.2.9 BANDWIDTH Ingress Policy Criterion

The BANDWIDTH Policy Criterion provides a method to express the intended bandwidth requirements for an Application Flow, and the probability of packet discard in the face of varying bandwidth contention for Underlay Connectivity Service resources.

The effect of applying the BANDWIDTH Policy Criterion to an Application Flow is to declare IP Packets in the Application Flow either conformant or non-conformant. IP Packets in the Application Flow can be discarded or delayed (traffic shaping) in order to meet the Policy applied to the Application Flow.

For the purpose of determining conformance, the information rate of the Application Flow is computed over time intervals of length *irduration*, which is an element in the value of the SWVC Performance Time Intervals Service Attribute (section 9.8).

The value of the BANDWIDTH Policy Criterion is a 2-tuple  $\langle \text{commit}, \text{limit} \rangle$  where:

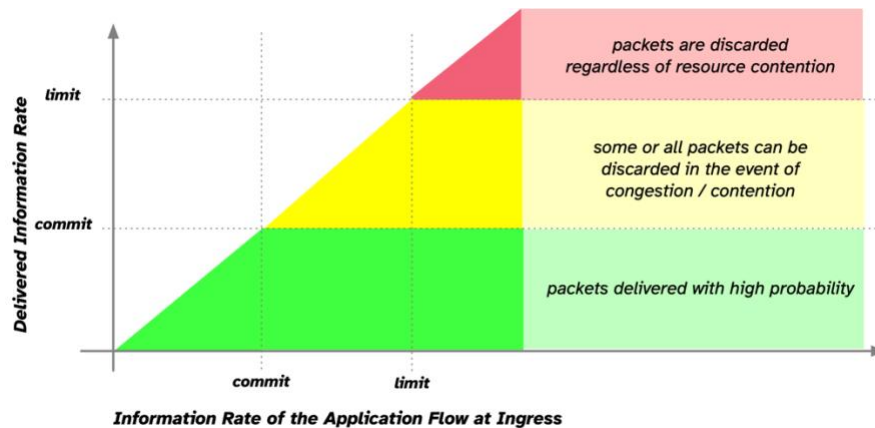
- *commit* – is the threshold information rate (bits per second) at or below which the SD-WAN Service Provider commits to deliver packets in the Application Flow with high probability under all traffic conditions, i.e., regardless of the information rate for other Application Flows at this UNI, or at other UNIs in the same SD-WAN Edge.
- *limit* – is the threshold information rate (bits per second) above which the Service Provider does not deliver IP Packet in the Application Flow under any traffic conditions, i.e., the SD-WAN Service Provider discards IP Packets in the Application Flow regardless of the bandwidth used for other Application Flows at this UNI, or at other UNIs in the same SD-WAN Edge. The value for *limit* can be *None*.

**[R69]** In the value of the BANDWIDTH Policy Criterion, *limit* **MUST** be greater than or equal to *commit* or *None*.

Specifying a value greater than 0 for *commit* indicates that delivering at least this rate is necessary to achieve the desired or intended level of performance for the Application Flow, whereas *commit* = 0 indicates that the Application Flow can operate with however much (or little) bandwidth is available.

The intent of specifying a value for *limit* is to indicate an upper bound on the bandwidth used by the Application Flow so that it does not crowd out other Application Flows. Specifying *limit* = *None*, means that there is no maximum imposed on the Application Flow up to the limits imposed by the SD-WAN UNI speed (which needs to be agreed on between the Subscriber and Service Provider) and Underlay Connectivity Service bandwidth constraints.

The intended behavior is shown in the following diagram.



**Figure 13 – Operation of BANDWIDTH Policy Criterion**

For an information rate from zero up to the *commit* bandwidth (the green area), the expectation is that IP Packets in the Application Flow are delivered with high probability. In the event of network congestion in the forwarding Path, such packets in the Application Flow have a low probability of discard. They could be discarded due to other Policy Criteria or by Security Policies, but not by this Policy Criterion.

For an information rate between *commit* and *limit* (the yellow area), IP Packets in the Application Flow are delivered with high probability unless there is contention with IP Packets in other Application Flows for the available UCS bandwidth. In this case, the Service Provider might discard IP Packets in this Application Flow, to reduce its impact on UCS utilization (but not such that it is reduced below *commit*).

For an information rate at *limit* and above (the red area), the Service Provider discards IP Packets in the Application Flow regardless of resource contention.

Note that if *commit*=0 the yellow area would extend down to the horizontal axis (i.e., covering the green area), and if *limit*=*None* the yellow area would extend upwards to the limit imposed by the UNI.

In order to achieve this behavior, there is an expectation that the Subscriber and the Service Provider have agreed on sufficient Underlay Connectivity Service capacity so that the *commit*

values for all Application Flows can be met. This agreement should take into account other traffic that shares the capacity of the UCS such as traffic from other UNIs and traffic routed through the SD-WAN Edge. How the average information rates are determined and the behavior of the rate limiting function are described below.

The effect of metering a stream of IP Packets – that is, comparing the actual sequence of IP Packets that pass the metering point to the description in terms of the BANDWIDTH Policy Criterion parameters – is to declare IP Packets in the Application Flow either conformant or non-conformant. This information can be used to take further action, for example policing or shaping. The combined effect is such that each packet has one of three outcomes:

- The IP Packet is discarded
- The IP Packet is forwarded immediately
- The IP Packet is forwarded after a short delay

This document does not specify the implementation of the bandwidth measurement/limiting by the Service Provider.

- [R70] Bandwidth metering **MUST** occur after it is determined that the IP Packet will be forwarded based on Policy and IP Forwarding considerations.

The following requirements define the behavior imposed by the BANDWIDTH Policy Criterion using the parameters *commit*, and *limit*.

- [R71] The information rate for IP Packets in an Application Flow that are declared conformant over any time interval equal to *irduration* **MUST** be at least the lower of *commit* and the information rate for IP Packets in that Application Flow that pass the metering point over that time interval.
- [R72] IP Packets in an Application Flow **MUST** be declared non-conformant in order to ensure that the information rate for such packets over any time interval equal to *irduration* that are declared conformant is, at most, *limit*.
- [O2] If the information rate for IP Packets in an Application Flow that pass the metering point over any time interval equal to *irduration* is greater than *commit*, then IP Packets in the Application Flow **MAY** be declared non-conformant in order to ensure that the information rate over that time interval for IP Packets across all Application Flows at a UNI does not exceed the available capacity of the Underlay Connectivity Services at that UNI.
- [O3] If, given the traffic received for various Application Flows with various Policies applied, the traffic that needs to be forwarded over a given Underlay Connectivity Service over any time interval equal to *irduration* exceeds the available capacity of that Underlay Connectivity Service, IP Packets in the affected Application Flows **MAY** be declared non-conformant in Application Flows where the information rate for IP Packets in the Application Flow that pass the metering point over that time interval is greater than *commit*.

The requirements above ([R71], [R72], [O2], and [O3]) describe how packets are declared conformant to the BANDWIDTH Policy (i.e., delivered with a high probability of success) or non-conformant (subject to discard as noted in [R74]).

[R71] indicates that at least the commit rate must be declared conformant if that much traffic is presented, i.e., if the average rate is less than or equal to *commit*, all of the traffic is declared conformant. On the other hand, [R72] indicates that the Service Provider discards packets to ensure that the average rate is less than limit.

[O2] and [O3] deal with the case where the average rate is between *commit* and *limit*. They indicate that the Service Provider may drop packets if the average rate is in this range if that is necessary to not exceed the total amount of UCS bandwidth or to avoid congestion on any particular UCS.

Note that the above requirements specify constraints over any time interval of duration *irduration*—i.e., they require a ‘sliding window’. Constraining bandwidth using a fixed, recurring, window can have the effect of declaring bursts of traffic “green” that are twice as large as intended, as described in MEF 23.2 [28] Appendix H.2.

When the total amount of traffic received at an SD-WAN UNI exceeds the available capacity of the associated Underlay Connectivity Services, some packets may need to be discarded, even though each individual Application Flow is operating below the maximum specified in the BANDWIDTH Policy Criterion. It is at the Service Provider’s discretion which packets to discard, so long as each Application Flow still gets its commit rate. For example, they might discard an equal number of packets from each Application Flow, or they might drop as many packets as possible from a single Application Flow.

Similarly, even when the total amount of traffic is less than the total available capacity on the Underlay Connectivity Services, the combination of traffic across different Application Flows with different policies might mean that the traffic that needs to be forwarded over a given Underlay Connectivity Service exceeds its capacity. Again, in that case, it is at the Service Providers discretion which packets to discard.

**[R73]** An Application Flow **MUST** be declared conformant unless it is declared non-conformant by a condition specified in [R72], [O2], or [O3].

**[R74]** IP Packets in an Application Flow that are declared non-conformant **MUST** be discarded.

In cases where the BANDWIDTH Policy Criterion is applied using an Application Flow Specification Group, the BANDWIDTH Policy Criterion operates differently than other Policy Criteria. For all other Policy Criteria, the Policy Criteria are applied to the Application Flows that match the Application Flow Specifications in the Application Flow Specification Group (that don’t have their own explicit Policy assignment). For the BANDWIDTH Policy Criterion, all of these Application Flows are aggregated into a single “flow” (for the purpose of applying this Policy Criterion) and the specified bandwidth commitment and limit apply to the aggregate. In other words, all of those Application Flows share the bandwidth parameters specified in the Policy and are treated as a single flow for the purpose of determining the bandwidth.

For example, Application Flow Specification Group *fruit* includes Application Flow Specifications *apple*, *banana*, and *pear* and is associated with a Policy *p100* for Zone *market* at an SWVC End Point. Policy *p100* includes BANDWIDTH {100Mbps, 200Mbps}. The combined set of IP Packets associated with all three Application Flows (i.e., the Application Flows that match *apple*, *banana*, and *pear* in Zone *market*) has a bandwidth commitment of 100Mbps and a bandwidth limit of 200Mbps. If, at the same SWVC End Point, Application Flow *apple* in *market* is assigned Policy *p100*, then *apple* (in *market*) has a 100Mbps commitment and a 200Mbps limit and the aggregate of *banana* and *pear* (in *market*) is subject to the group policy (100Mbps/200Mbps).

#### 9.10.2.10 AF-SECURITY-INGRESS Ingress Policy Criterion

The AF-SECURITY-INGRESS Ingress Policy Criterion is used to select Application Flow security functions at the Ingress UNI as described in MEF 88 [33]. The value of this Policy Criterion is *None* or an Application Flow Security Policy Identifier from the value of the SWVC List of Security Policies Service Attribute (see section 9.9).

#### 9.10.3 Egress Policy Criteria

This section describes the parameters and behavior of the BLOCK-SOURCE and AF-SECURITY-EGRESS Egress Policy Criteria.

##### 9.10.3.1 BLOCK-SOURCE Egress Policy Criterion

The BLOCK-SOURCE Policy Criterion specifies a set of conditions that determine whether an Egress IP Packet should be delivered to the Egress UNI or discarded. The conditions reflect certain aspects of the source of the IP Packet. The value of the BLOCK-SOURCE Policy Criterion is a non-empty list of sources. Two sources are currently defined, UNI and INTERNET, so there are three possible restrictions:

- [UNI] – discard IP packets in the Application Flow if they originated at any other UNI in the SWVC.
- [INTERNET] – discard IP packets in the Application Flow if they originated on the Internet
- [UNI, INTERNET] – discard IP packets in the Application Flow regardless of their origin (i.e., this Application Flow cannot egress at this UNI).

**[R75]** If the origin of an IP Packet destined for an Egress UNI matches any source specified in the the BLOCK-SOURCE Policy Criterion, the IP Packet **MUST** be discarded (not forwarded across the Egress UNI).

##### 9.10.3.2 AF-SECURITY-EGRESS Egress Policy Criterion

The AF-SECURITY-EGRESS Egress Policy Criterion is used to select Application Flow security functions at the SWVC End Point associated with an Egress UNI, as described in MEF 88 [33]. The value of this Policy Criterion is *None* or an Application Flow Security Policy Identifier from the value of the SWVC List of Security Policies Service Attribute (see section 9.9).

## 9.11 SWVC List of Application Flow Specification Groups Service Attribute

The value of the SWVC List of Application Flow Specification Groups Service Attribute is a list (possibly empty) of Application Flow Specification Group names.

An Application Flow Specification (see sections 8 and 9.12) can be a member of an Application Flow Specification Group. Application Flow Specification Groups provide a mechanism for associating a Policy with multiple Application Flows. If a Policy is associated with an Application Flow Specification Group and Zone, then that Policy is associated with all Application Flows that match Application Flow Specifications (in that Zone) that are members of the Application Flow Specification Group. An Application Flow Specification that is a member of the Application Flow Specification Group could, nonetheless, have an explicit Policy assigned at the SWVC End Point (in the same Zone) in which case that assignment would supersede the Application Flow Specification Group assignment for that Application Flow Specification. Application Flow Specification Groups also provide a mechanism for Application Flows that match Application Flow Specifications that are members to share bandwidth commitments and limits (see section 9.10.2.9).

For example, Application Flow Specifications *banana*, *pear*, and *grape* can all be members of the Application Flow Specification Group *fruit*. Group membership is indicated in the definition of each Application Flow Specification (see section 9.12).

- [R76] Each Application Flow Specification Group name in the value of the SWVC List of Application Flow Specification Groups Service Attribute **MUST** be an Identifier String.
- [R77] Each Application Flow Specification Group name in the value of the SWVC List of Application Flow Specification Groups Service Attribute **MUST** appear, at most, once.
- [R78] An Application Flow Specification Group name in the value of the SWVC List of Application Flow Specification Groups Service Attribute **MUST NOT** have the value *None*.

## 9.12 SWVC List of Application Flow Specifications Service Attribute

The SWVC List of Application Flow Specifications Service Attribute specifies the Application Flows that can be recognized by the SD-WAN service and information about how to identify IP Packets in each Application Flow. The value of the Service Attribute is a non-empty ordered list of 3-tuples  $\langle AFName, AFCritList, AFGGroup \rangle$  where:

- *AFName* is an Identifier String that is used to refer to the Application Flow Specification (and resulting Application Flows).
- *AFCritList* is a non-empty list of Application Flow Criteria 2-tuples of the form  $\langle AFCritName, AFCritValue \rangle$  where:
  - *AFCritName* is an Identifier String containing an Application Flow Criterion Name from Table 7 or Table 8.

- *AFCritValue* contains the parameter values specific to the Application Flow Criterion specified in *AFCritName*. If there are no parameter values, *AFCritValue* is *None*.
  - *AFGroup* is an Application Flow Specification Group name contained in the value of the SWVC List of Application Flow Specification Groups Service Attribute (section 9.11) or *None* if the Application Flow is not a member of an Application Flow Specification Group.
- [R79] Each Application Flow Specification name, *AFName*, in the value of the SWVC List of Application Flow Specifications Service Attribute **MUST** appear, at most, once.
- [R80] Each Application Flow Specification name, *AFName*, in the value of the SWVC List of Application Flow Specifications Service Attribute **MUST NOT** be the same as an Application Flow Specification Group Name in the value of the SWVC List of Application Flow Specification Groups Service Attribute.
- [R81] An *AFCritName* **MUST NOT** appear more than once in the *AFCritList* for each item in the value of the SWVC List of Application Flow Specifications Service Attribute.
- [R82] If the *AFCritList* element in an entry of the SWVC List of Application Flow Specifications Service Attribute contains more than one Application Flow Criterion, an Ingress IP Packet **MUST** match all Application Flow Criteria in order to be associated with the Application Flow.
- [R83] Each Ingress IP Packet **MUST** be assigned to an Application Flow based on the first Application Flow Specification in the value of the SWVC List of Application Flow Specifications Service Attribute whose Application Flow Criteria it matches, if any.
- [R84] Any Ingress IP Packet that cannot be associated with an Application Flow based on the value of the List of Application Flow Specifications Service Attribute **MUST** be discarded.

As shown in the example later in this section, the criteria for one Application Flow Specification can be a subset of the criteria for another Application Flow Specification, so the order that the Application Flow Specifications are matched, and hence the order of the Application Flow Specification definitions in the value of this Service Attribute is important and is one aspect of the agreed value of this Service Attribute.

[R82] indicates that the Application Flow Specification is defined by the conjunction of a set of Application Flow Criteria. This doesn't allow for alternatives within an Application Flow. This constraint is partially mitigated by the fact that most of the Application Flow Criteria are ranges or lists of values. Also, an Application Flow Specification Group can provide alternatives. For example, one Application Flow Specification can have criteria X and Y, and a second Application Flow Specification can have criteria X and W. If the two Application Flow Specifications are put into an Application Flow Specification Group, a common Policy can be applied to the Application

Flow Specification Group and the matching Application Flows can share bandwidth resources, so it appears (almost) like a single Application Flow Specification defined as (X AND Y) OR (X AND W).

**[R85]** The Application Flow Criteria supported by the Service Provider **MUST** include the Application Flow Criteria listed in Table 7.

<i>AFCritName</i>	<i>Layer</i>	<i>Match</i>	<i>Values for AFCritValue</i>	<i>Reference</i>
SAV4	3	IPv4 Source Address	List of IPv4 prefixes	RFC 791 [5]
DAV4	3	IPv4 Destination Address	List of IPv4 prefixes	RFC 791 [5]
PROTV4	3	IPv4 Protocol List	List of integers in the range 0 to 255 or a list of keywords from [1] or a mix of integers and keywords	IANA Protocol Numbers Registry [1]
SAV6	3	IPv6 Source Address	List of IPv6 prefixes	RFC 8200 [25]
DAV6	3	IPv6 Destination Address	List of IPv6 prefixes	RFC 8200 [25]
NEXTHEADV6	3	IPv6 Next Header List	List of integers in the range 0 to 255 or a list of keywords from [1] or a mix of integers and keywords	IANA Protocol Numbers Registry [1]
DSCP	3	Differentiated Services Code Point	List of integers in the range 0 to 63	RFC 2474 [11]
SPORT	4	Transport Source Port <sup>12</sup>	List of integers in the range 0 to 65535 or a list of service names from [2] or a mix of integers and service names	IANA Service Name and Port Number Registry [2]
DPORT	4	Transport Destination Port	List of integers in the range 0 to 65535 or a list of service names from [2] or a mix of integers and service names	IANA Service Name and Port Number Registry [2]
APPID	3-7	Custom match including heuristic/algorithmic matching	List of arguments starting with the Application Identifier.	This provides the ability to reference a library of custom application flow specifications.
ANY	1-7	Match any IP Packet	<i>None</i>	

**Table 7 – Application Flow Criteria – Support Required**

The Application Flow Criteria listed in Table 7 represent the basic “IP 5-tuple” (and APPID and ANY). Note that the IPv4 criteria are optional if all the UNIs that have an SWVC End Point for this SWVC only support IPv6 addressing, and the IPv6 criteria are optional only if those UNIs only support IPv4 addressing (see sections 11.4 and 11.5).

<sup>12</sup> This (and the other Application Flow Criteria referring to ports) was changed from “TCP/UDP Source Port” to “Transport Source Port” in MEF 70.1. This change allows the field to cover additional transport protocols (specified in PROTV4 or NEXTHEADV6) such as SCTP [21] and DCCP [19].

The APPID Application Flow Criterion provides a method for referring to named packet matching definitions (both simple and complex) defined by the Service Provider. These can include standard matches available to all the Service Provider's Subscribers from a catalog and/or custom matches developed by the Service Provider by agreement with a particular Subscriber.

APPID can include simple protocol matches that can be accomplished with the other Policy Criteria, such as DPORT, (e.g., APPID match-dest-port 443) or *SSH* or *SNMP* or *RTP*, but they can also support more complex packet inspection, enabling identification of specific applications such as *Microsoft365*<sup>13</sup>, *Webex*<sup>14</sup>, or *Facebook*<sup>15</sup>.

- [R86]** If the Service Provider defines a named packet matching definition (either standard or custom) for use with the APPID Application Flow Criterion, the description provided to the Subscriber **MUST** include the following information:
- The Application Identifier
  - Additional Arguments Required (beyond the Identifier)
  - Details of the applications and application traffic matched by the APPID.

Complex matches, for example, using deep packet inspection, often require inspection of several initial packets and may include heuristics to define the characteristics of an Application Flow. These details are included in the description of the matching logic required by [R86].

For example:

- An APPID with name SIP: There are no additional arguments required, and the match is performed by inspecting the TCP or UDP source and destination port in each IP Packet for value 5060 or value 5061.
- An APPID named SIPUSER: This includes an additional argument "user-id". The operation of this match is the same as SIP with the addition that if the port match is successful, the SIP *To* and *From* fields are matched against the "user-id".

The Application Flow Criterion ANY matches all IP Packets. This criterion allows an Application Flow Specification to be defined that includes all "unmatched" IP Packets. A Policy can then be assigned to resulting Application Flows (per Zone) at the SWVC End Point. In general, if this Application Flow Criterion is used, it should be in the last Application Flow Specification in the list, since no IP Packets are matched against subsequent Application Flow Specifications. An example is provided later in this section.

- [R87]** If an entry in the value of the SWVC List of Application Flow Specifications Service Attribute includes the Application Flow Criterion ANY, that entry **MUST NOT** contain any other Application Flow Criteria.

Support for the Application Flow Criteria listed in Table 8 is optional. They provided additional capabilities or additional expressivity in Application Flow Specifications.

<sup>13</sup> Microsoft365 is a registered trademark of Microsoft Corporation

<sup>14</sup> Webex is a registered trademark of Cisco Systems Incorporated

<sup>15</sup> Facebook is a registered trademark of Facebook Incorporated

**[D4]** The Application Flow Criteria supported by the Service Provider **SHOULD** include the Application Flow Criteria listed in Table 8.

AFCritName	Layer	Match	Values for AFCritValue	Reference	Note
ETHERTYPE	2	EtherType	List of Integers in the range 0x0600 to 0xffff, e.g. 0x0800 for IPv4	802.3 [4]	Since SD-WAN is a layer 3 service, not all implementations have access to the L2 header during Application Flow matching, hence this Application Flow Criterion is optional.
SDAV4	3	IPv4 Source or Destination Address	List of IPv4 prefixes	RFC 791 [5]	This Application Flow Criterion allows an Application Flow to match a list of values for <i>either</i> the source or destination address. Support for this Application Flow Criterion is optional since it can be accomplished with two Application Flows based on the required criteria.
SDAV6	3	IPv6 Source or Destination Address	List of IPv6 prefixes	RFC 8200 [25]	Same as previous
SDPORT	4	Transport Source or Destination Port List	List of integers in the range 0 to 65535 or a list of service names from [2] or a mix of integers and service names	IANA Service Name and Port Number Registry [2]	This Application Flow Criterion allows an Application Flow to match a list of values for <i>either</i> the source or destination port. Support for this Application Flow Criterion is optional since it can be accomplished with two Application Flows based on the required criteria.

**Table 8 – Application Flow Criteria – Support Recommended**

It is important to note that Table 7 and Table 8 are not intended to describe the implementation or “syntax” of how Application Flows are described in any product or service, but rather the capabilities that are available. For example, no implementation is required to have a command or configuration parameter called DPORT, but rather that the implementation can “match packets with destination port =x”.

Here is an example value for this Service Attribute with four Application Flow Specifications:

```
[ {peach,      [{SAV4, [192.168.7.0/24] }, {DPORT, [80,443,8080] }], round }
  {VOIP, [{APPID, ["RTP"] }], None }
  {banana,     [{DPORT, [80]}], long }
```

[  
  <Else,            [{ANY, None}], None >  
]

In this example, Application Flow Specification *peach* matches IP Packets from any 192.168.7.x address destined to port 80 or 443 or 8080 (and this Application Flow Specification is in the Application Flow Specification Group *round*). Application Flow Specification *VOIP* selects IP Packets that are matched by the APPID “RTP”. Application Flow Specification *banana* matches any IP Packet to port 80 that is not matched by *peach*, and this Application Flow Specification is in Application Flow Specification Group *long*. At the end of the list is the Application Flow Specification *Else*, which includes matches IP Packets not matched by the other three.

In this example, it is important that *banana* is after *peach* because there are some IP Packets that would match both definitions, but the desired behavior is that they are assigned to *peach*. If *banana* were first, then IP Packets with a source address in 192.168.7.x and destination port 80 would match to Application Flow Specification *banana* rather than Application Flow Specification *peach*.

It is also important to note that many Application Flow Specifications are not symmetric. For example, *banana* above, matches traffic destined *to* port 80, but response traffic will be *from* port 80. It can be made symmetric by using SDPORT, if that is available, or by adding another Application Flow Specification, e.g., *rbanana*, which has SPORT 80. At each SD-WAN Edge a Policy can be assigned to one or both (with appropriate Zone qualification).

## 10 SD-WAN Virtual Connection (SWVC) End Point Service Attributes

The SWVC End Point is the construct that represents the attachment of an SWVC to a UNI. The SWVC End Point provides a container for attributes of the SWVC that can differ at each UNI.

This section describes Service Attributes at each SWVC End Point which are summarized in the following table, and each is described in more detail in the subsequent sections.

Attribute Name	Summary Description	Possible Values
SWVC End Point Identifier	Identification of the SWVC End Point for management purposes	Unique Identifier String for a given SWVC End Point.
SWVC End Point Associated UNI	Identifies the UNI that the SWVC End Point is associated with	An SD-WAN UNI Identifier
SWVC End Point List of UCS End Points	A list of the UCS End Points accessible by the SWVC End Point	List of UCS End Point Identifiers
SWVC End Point Policy Map	Maps Policies to Application Flows	A list of 4-tuples <zone, app, ipol, epol>

**Table 9 – Summary of SWVC End Point Service Attributes**

### 10.1 SWVC End Point Identifier Service Attribute

The value of the SWVC End Point Identifier Service Attribute is a string that is used to allow the Subscriber and Service Provider to uniquely identify the association of the SWVC with a UNI.

**[R88]** The value of the SWVC End Point Identifier Service Attribute **MUST** be an Identifier String.

**[R89]** The value of the SWVC End Point Identifier Service Attribute **MUST** be unique across all SWVC End Points in the Service Provider Network.

### 10.2 SWVC End Point Associated UNI Service Attribute

The value of the SWVC End Point Associated UNI Service Attribute is an SD-WAN UNI Identifier Service Attribute value per section 11.1, which serves to specify the UNI that the SWVC End Point is associating with the SWVC. The SWVC End Point is said to be at this UNI.

### 10.3 SWVC End Point List of UCS End Points Service Attribute

Each SWVC End Point has a list of one or more UCS End Points to which it can forward Ingress IP Packets (from the UNI) and from which it can forward Egress IP Packets (towards the UNI). The value of the SWVC End Point List of UCS End Points Service Attribute is a non-empty list of UCS End Point Identifiers (section 14.1).

- [R90]** For any two SWVC End Points in an SWVC, one of the following **MUST** be true:
- the values of their respective SWVC End Point List of UCS End Points are identical
  - the intersection of their respective SWVC End Point List of UCS End Points is null

[R90] indicates that for every pair of SWVC End Points, either their List of UCS End Points are the same (have the same UCS End Points) which indicates that both are in the same SD-WAN Edge, or they have no UCS End Points in common which indicates that they are in different SD-WAN Edges. This means that every UNI in an SD-WAN Edge can use every UCS End Point in that SD-WAN Edge even if it only requires forwarding to a subset of them. Any desired restrictions on forwarding can be achieved by Policies.

#### 10.4 SWVC End Point Policy Map Service Attribute

The SWVC End Point Policy Map specifies the Policies that are assigned to Application Flows at the SWVC End Point. The value of the SWVC End Point Policy Map is a (possibly empty)<sup>16</sup> list of 4-tuples  $\langle zone, app, ipol, epol \rangle$  where:

- *zone* is a Zone name
- *app* is an Application Flow Specification or Application Flow Specification Group name
- *ipol* is *None* or the name of an Ingress Policy
- *epol* is *None* or the name of an Egress Policy

The 4-tuple argument can be thought of as having two components. The pair  $\langle zone, app \rangle$  defines the Application Flow (or Application Flows if *app* is an Application Flow Specification Group) at the UNI where this SWVC End Point is located, and the pair  $\langle ipol, epol \rangle$  specify the Policy assignment to the Application Flow(s).

- [R91]** The *zone* element in each entry in the value of the SWVC End Point Policy Map **MUST** be one of the Zones listed in the SWVC List of Zones Service Attribute (section 9.6) or *Internet*.
- [R92]** The *app* element in each entry in the value of the SWVC End Point Policy Map **MUST** be either:
- an Application Flow Specification Group name from the value of the SWVC List of Application Flow Specification Groups Service Attribute (see section 9.11), or,
  - an Application Flow Specification name from the value of the SWVC List of Application Flow Specifications Service Attribute (see section 9.12)

<sup>16</sup> An empty list only makes sense if all allowed Application Flows are covered by Zone-wide Policies and no Egress Policies are used.

- [R93] For a specific value of the *zone* element and a specified value of *app* in the value of the SWVC End Point Policy Map, the combination  $\langle zone, app \rangle$  **MUST** appear in, at most, one entry in the list.
- [R94] The *ipol* element in each entry in the value of the SWVC End Point Policy Map **MUST** be either *None* or the name of an Ingress Policy from the value of the SWVC List of Policies Service Attribute (see section 9.10).
- [R95] If the *zone* element of an entry in the value of the SWVC End Point Policy Map is *Internet*, then the *ipol* element in that entry **MUST** be *None*.
- [R96] The *epol* element in each entry in the value of the SWVC End Point Policy Map **MUST** be either *None* or the name of an Egress Policy from the value of the SWVC List of Policies Service Attribute (see section 9.10).

#### 10.4.1 Ingress Policy Assignment

An Ingress Policy can be assigned to an Application Flow either via the SWVC End Point Policy Map Service Attribute or via a Zone-wide Policy assignment specified in the SWVC List of Zones Service Attribute.

The SWVC List of Zones Service Attribute can assign a Zone-wide Ingress Policy to one or more Application Flows by associating a Policy with an Application Flow Specification (meaning the Policy is assigned to a single Application Flow at each UNI) or an Application Flow Specification Group (meaning the Policy is assigned to one or more Application Flows at each UNI). The Zone is implicit in both cases.

The first two elements  $\langle zone, app \rangle$  of the value of the SWVC End Point Policy Map Service Attribute specify one or more Application Flows. The *app* element can be an Application Flow Specification, (thus specifying a single Application Flow at this UNI), or it can be an Application Flow Specification Group (thus specifying one or more Application Flows at this UNI). The *ipol* element identifies the Ingress Policy that is assigned to the specified Application Flows.

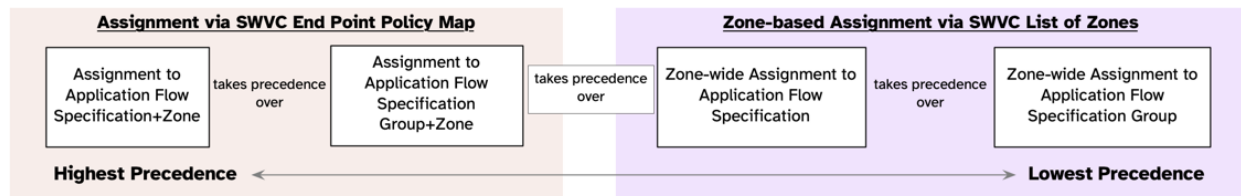
This results in four ways that an Ingress Policy could be assigned to an Application Flow identified by a given UNI, Application Flow Specification, and Zone:

- By using the SWVC List of Zones Service Attribute to associate a Policy with the Zone and the Application Flow Specification.
- By using the SWVC List of Zones Service Attribute to associate a Policy with the Zone and with an Application Flow Specification Group of which the Application Flow Specification is a member.
- By using the SWVC End Point Policy Map Service Attribute for the SWVC End Point at the UNI to associate a Policy with the Zone and the Application Flow Specification.
- By using the SWVC End Point Policy Map Service Attribute for the SWVC End Point at the UNI with the Zone and with an Application Flow Specification Group of which the Application Flow Specification is a member.

There is a well-defined precedence among the four. [R97], [R98], and [R99] define this precedence.

- [R97]** Assignment of an Ingress Policy to an Application Flow via the SWVC End Point Policy Map Service Attribute **MUST** take precedence over assignment via the SWVC List of Zones Service Attribute.
- [R98]** Assignment of an Ingress Policy to an Application Flow via an entry in the SWVC End Point Policy Map Service Attribute that specifies the corresponding Application Flow Specification **MUST** take precedence over assignment via an entry that specifies an Application Flow Specification Group of which the corresponding Application Flow Specification is a member.
- [R99]** Assignment of an Ingress Policy to an Application Flow via an entry in the SWVC List of Zones Service Attribute that specifies the corresponding Application Flow Specification **MUST** take precedence over assignment via an entry that specifies an Application Flow Specification Group of which the corresponding Application Flow Specification is a member.

Note that [R97] means that a Policy assigned via the SWVC List of Zones Service Attribute might be overridden by a Policy assigned via the SWVC End Point Policy Map Service Attribute at some UNIs but not others. Requirements [R97] through [R99] describe a precedence for Policy assignment that is depicted in Figure 14.



**Figure 14 – Precedence for Policy Assignment**

- [R100]** If an Application Flow is not assigned an Ingress Policy via any of the four methods discussed in [R97] through [R99] at a UNI, Ingress IP Packets mapped to the Application Flow **MUST** be discarded.
- [R101]** If an Application Flow is assigned the reserved Ingress Policy name *Block* at a UNI, Ingress IP Packets mapped to the Application Flow **MUST** be discarded.

If an Ingress Policy is associated with an Application Flow Specification Group (in a Zone), then that Ingress Policy is assigned to all of the Application Flows that match that Zone and any of the Application Flow Specifications in the Application Flow Specification Group (assuming no higher precedence assignment). [R101] provides a mechanism to selectively disallow forwarding of one or more those Application Flows by assigning the Ingress Policy *Block* (see section 9.10) to one or more Application Flow Specifications in the Zone (since [R100] cannot be invoked). Note that [R41] includes additional conditions for forwarding an Application Flow.

Not forwarding an Application Flow (either due to not having an Ingress Policy assigned or by explicit assignment of the reserved Policy, *Block*), only refers to Application Flows that ingress at the UNI.

#### 10.4.2 Egress Policy Assignment

An Egress Policy can be assigned to an Application Flow via the SWVC End Point Policy Map Service Attribute at the Egress SWVC End Point.

The first two elements  $\langle zone, app \rangle$  of the value of the SWVC End Point Policy Map Service Attribute specify one or more Application Flows. The *app* element can be an Application Flow Specification, (thus specifying a single Application Flow at this UNI), or it can be an Application Flow Specification Group (thus specifying one or more Application Flows at this UNI). The *epol* element identifies the Egress Policy that is assigned to the specified Application Flows. Egress Policies can be assigned to IP Packets from the Internet by specifying the reserved Zone name, *Internet*.

An Application Flow at an Egress UNI is, in the general case, an aggregation of IP Packets from multiple Ingress Application Flows. Consider the following example:

- at SWVC End Point 1 there is an Ingress Application Flow that matches Application Flow Specification *email* in Zone *corp*. Some of this Application Flow is forwarded to SWVC End Point 2 and some to SWVC End Point 3.
- at SWVC End Point 2 there is an Ingress Application Flow that matches Application Flow *email* in Zone *corp*. Some of this Application Flow is forwarded to SWVC End Point 1 and some to SWVC End Point 3.
- At SWVC End Point 3 the Egress Application Flow that matches Application Flow Specification *email* in Zone *corp* is the aggregate of the portion forwarded from SWVC End Point 1 and the portion forwarded from SWVC End Point 2.

Egress Application Flows are delivered to an Egress UNI unless blocked by an Egress Policy (including a security function as described in MEF 88 [33] via the AF-SECURITY-EGRESS Policy Criterion (Section 9.10.3.2)).

**[R102]** If an Egress Policy is not assigned to an Application Flow at an Egress UNI, then Egress IP Packets that are in the Application Flow **MUST** be forwarded to the Egress UNI.

[R102] can occur if no Policies are mapped to the Application Flow at the SWVC End Point, or if the *epol* element is *None*.

If it is necessary to block an Application Flow at an Egress UNI, this can be achieved by specifying an Egress Policy (*epol* element) that includes a BLOCK-SOURCE Policy Criterion for UNI and INTERNET.

**[R103]** Assignment of an Egress Policy to an Application Flow via an entry in the SWVC End Point Policy Map Service Attribute that specifies the corresponding Application Flow Specification **MUST** take precedence over

assignment via an entry that specifies an Application Flow Specification Group of which the corresponding Application Flow Specification is a member.

### 10.4.3 Examples of Ingress Application Flows and Policy Assignment

Figure 15 depicts the precedence for assigning an Ingress Policy to an Application Flow. The SD-WAN Service has three Subscriber sites (A, B, and C) with a single Zone, *hr*, defined. The SWVC has four Application Flow Specifications: *apple*, *banana*, *celery*, *basil* (via the SWVC List of Application Flow Specifications Service Attribute in section 9.12). *Apple* and *banana* are in Application Flow Specification Group *fruit*. Application Flow Specifications *celery* and *basil* are not in any Application Flow Specification Group. Zone *hr* has a single Zone-wide Policy assignment (*basil* ← *sprinkle*).

The SWVC also has three Ingress Policies: *bake*, *cook*, and *sprinkle* (via the SWVC List of Policies Service Attribute in section 9.9). All SWVCs have a reserved Policy named *Block*.

Note: In the diagram and subsequent explanatory text, *xxxx<sub>yy</sub>* should be interpreted as the Application Flow that matches Application Flow Specification *xxxx* and is in Zone *yy*.

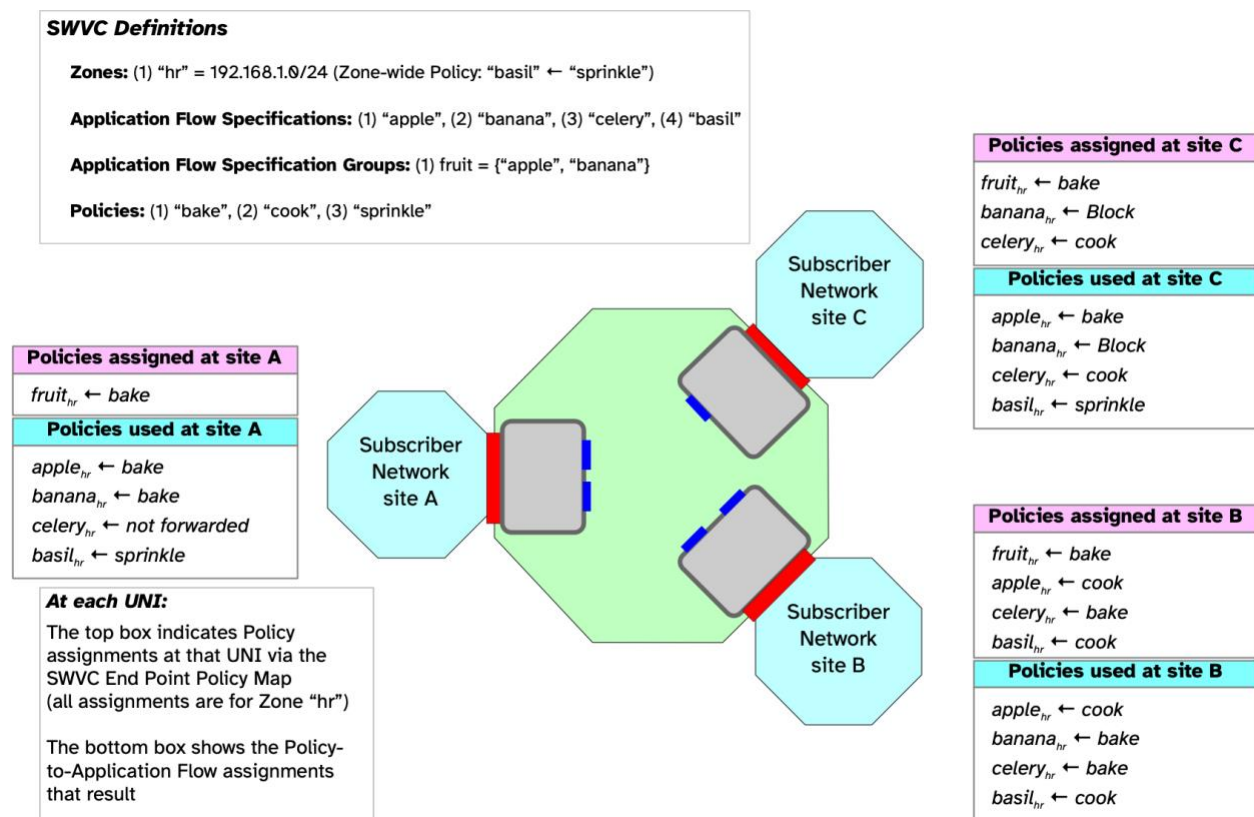


Figure 15 – Assigning Ingress Policies

At site A:

- Policy *bake* is associated with (via the SWVC End Point Policy Map) Application Flow Specification Group *fruit* in Zone *hr*. This means that *apple<sub>hr</sub>* and *banana<sub>hr</sub>* are forwarded based on Policy *bake*.

- Application flow *basil<sub>hr</sub>* is forwarded based on the Zone-wide Policy *sprinkle*.
- Application flow *celery<sub>hr</sub>* does not have a Zone-wide Policy nor is it assigned a Policy via the SWVC End Point Policy Map, so it is not forwarded.

At site B:

- Policy *bake* is associated with Application Flow Specification Group *fruit* in *hr*. So, *banana<sub>hr</sub>* is forwarded based on Policy *bake*, but Policy *cook* is assigned to Application Flow *apple<sub>hr</sub>*, overriding the Application Flow Specification Group association.
- Application Flow *celery<sub>hr</sub>* is forwarded based on the Policy *bake* (via the SWVC End Point Policy Map).
- Application Flow *basil<sub>hr</sub>* is forwarded based on the Policy *cook* (via the SWVC End Point Policy Map overriding the Zone-wide Policy).

At site C:

- Policy *bake* is associated with Application Flow Specification Group *fruit* in *hr*. So, *apple<sub>hr</sub>* is forwarded based on Policy *bake*, but Policy *Block* is assigned to Application Flow *banana<sub>hr</sub>*, so it is not forwarded.
- Application Flow *celery<sub>hr</sub>* is forwarded based on the Policy *cook* (via the SWVC End Point Policy Map).
- Application Flow *basil<sub>hr</sub>* is forwarded based on the Zone-wide Policy *sprinkle*.

## 11 SD-WAN UNI Service Attributes

The UNI is a reference point that represents the demarcation between the responsibility of the Subscriber and the responsibility of the Service Provider. As a result, at any given UNI there is only a single Subscriber and a single Service Provider (see [R1] and [R2]).

This section includes the Service Attributes at each UNI which are summarized in the following table and described in more detail in the subsequent sections. Since an SD-WAN Service delivers IP packets between multiple Subscriber Locations, much of this section is adapted from the UNI Services Attributes and UNI Access Link Service Attributes section of the IP Service Attributes MEF Standard, MEF 61.1 [29] in order to achieve the greatest amount of commonality between MEF IP Services and MEF SD-WAN Services.

Attribute Name	Summary Description	Possible Values
SD-WAN UNI Identifier	Identification of the UNI for management purposes	Unique Identifier String for the UNI
SD-WAN UNI L2 Interface	Describes the underlying L2 interface for the UNI	<i>Untagged or CVLAN x</i>
SD-WAN UNI Maximum L2 Frame Size	Specifies the maximum length L2 frame that is accepted by the Service Provider	An integer number of bytes $\geq 1522$
SD-WAN UNI IPv4 Connection Addressing	IPv4 Connection Address mechanism	<i>None, Static, or DHCP</i>
SD-WAN UNI IPv6 Connection Addressing	IPv6 Connection Address mechanism	<i>None, DHCP, SLAAC, Static or LL-only</i>
SD-WAN UNI Routing Protocols	List of Routing Protocols used across the UNI	See section 11.6

**Table 10 – Summary of SD-WAN UNI Service Attributes**

### 11.1 SD-WAN UNI Identifier Service Attribute

The value of the SD-WAN UNI Identifier Service Attribute is a string that is used to allow the Subscriber and Service Provider to uniquely identify the UNI.

**[R104]** The value of the SD-WAN UNI Identifier Service Attribute **MUST** be an Identifier String.

**[R105]** The value of the SD-WAN UNI Identifier Service Attribute **MUST** be unique across all SD-WAN UNIs in the Service Provider Network.

As an example, the Subscriber and Service Provider might agree to use “NY-1” as a value of the SD-WAN UNI Identifier Service Attribute.

## 11.2 SD-WAN UNI L2 Interface Service Attribute

The SD-WAN UNI L2 Interface Service Attribute describes the underlying network layer that carries IP Packets across the UNI. The fundamental role of the UNI is to be able to convey IP Packets (layer 3) between the Subscriber and the SP.

The SD-WAN UNI layer 2 is an Ethernet MAC. The value of this Service Attribute describes the set of Ethernet MAC frames that are mapped to the UNI at layer 2. The possible values are *Untagged* and *CVLAN x* where *x* is a VLAN ID in the range 1 to 4094.

- [R106] The format for an L2 frame that crosses the UNI **MUST** be that of the Ethernet MAC Frame that is specified in Clause 3 of IEEE Std 802.3-2018 [4] except for section 3.2.7 of that document.

Note that [R106] means that Ethernet MAC frames will be discarded by the SD-WAN Edge if they are not properly constructed. For example, a Service Frame with an incorrect Frame Check Sequence will be discarded. Section 3.2.7 in IEEE Std. 802.3-2018 [4] describes the maximum length of the client data field and limits it to 1982 bytes (2000-byte frame), however this specification does not impose this limit. The Subscriber and the Service Provider can agree to any value subject to the constraints described in the SD-WAN UNI Maximum L2 Frame Size Service Attribute (section 11.3).

The following Ethernet MAC Frame formats are defined:

- When the field following the Source Address field is a TPID (Tag Protocol ID defined in IEEE Std 802.1Q-2018 [3]) with the value 0x8100 and the corresponding VLAN ID is not 0x0000, the Ethernet MAC Frame is said to be a *C-Tagged frame* and the value of the VLAN ID field is referred to as the C-VID.
- When the two bytes following the Source Address do not contain the values 0x8100 or 0x88a8, the Ethernet MAC Frame is said to be an *Untagged frame*.

C-Tagged and Untagged frames are eligible to be mapped to the UNI, subject to the constraints imposed by the value of this Service Attribute. Handling of other frame types is beyond the scope of this document.

- [R107] If the value of the SD-WAN UNI L2 Interface Service Attribute is *Untagged*, then all Untagged Ethernet MAC Frames on the underlying physical or virtual Ethernet link **MUST** be delivered to the UNI.
- [R108] If the value of the SD-WAN UNI L2 Interface Service Attribute is *Untagged*, then C-tagged Ethernet MAC Frames on the underlying physical or virtual Ethernet link **MUST NOT** be delivered to the UNI.
- [R109] If the value of the SD-WAN UNI L2 Interface Service Attribute is *CVLAN x*, then all C-tagged Ethernet MAC Frames with a C-VID of *x* on the underlying physical or virtual Ethernet link **MUST** be delivered to the UNI.
- [R110] If the value of the SD-WAN UNI L2 Interface Service Attribute is *CVLAN x*, then Untagged and C-tagged Ethernet MAC Frames with a C-VID other than *x*

on the underlying physical or virtual Ethernet link **MUST NOT** be delivered to the UNI.

The details and parameters of the layer 1 interface, including the speed of the interface, must be agreed to between the Subscriber and the Service Provider but are beyond the scope of this specification.

The implication of supporting a single VLAN at a UNI (i.e., CVLAN x) is that the layer 1 channel that is conveying the Ethernet MAC frames can potentially access multiple UNIs. Each C-VID value can be mapped to a different UNI for the same SD-WAN Service, or a different SD-WAN Service, or, in theory, a different type of service. Details of this capability are out of scope for this document but may be included in a future version.

### 11.3 SD-WAN UNI Maximum L2 Frame Size Service Attribute

The SD-WAN UNI L2 Maximum Frame Size Service Attributes specifies the maximum Ethernet MAC frame size that will be accepted by the Service Provider at the UNI.

[R111] The value for the SD-WAN UNI L2 Maximum Frame Size **MUST** be an integer number of bytes  $\geq 1522$ .

[D5] Any L2 Frame that crosses the Ingress UNI whose length exceeds the value of the SD-WAN UNI L2 Maximum Frame Size **SHOULD** be discarded.

### 11.4 SD-WAN UNI IPv4 Connection Addressing Service Attribute

The SD-WAN UNI IPv4 Connection Addressing Service Attribute specifies how IPv4 addresses are allocated to the devices on the Subscriber side of the UNI. The Service Attribute has one of three possible values: *None*, *DHCP*, or *Static*. In the case of DHCP and Static there are some additional parameters.

If the IPv4 Connection Addressing is *None*, no IPv4 addresses are used and IPv4 is disabled on the link. Note that in this case IPv6 connection addresses are needed.

[R112] If the value of the SD-WAN UNI IPv4 Connection Addressing Service Attribute is *None*, IPv4 Packets **MUST NOT** be forwarded to or from the UNI.

[R113] The SD-WAN UNI IPv4 Connection Addressing Service Attribute and the SD-WAN UNI IPv6 Connection Addressing Service Attribute (section 11.5) **MUST NOT** both have the value *None*.

If the value of the SD-WAN UNI IPv4 Connection Addressing Service Attribute is *DHCP*, then DHCP is used by devices in the Subscriber Network to request IPv4 addresses in a given subnet from the Service Provider as described in RFC 2131 [7] and RFC 2132 [8]. The Service Provider hosts the DHCP server and the Subscriber devices act as the DHCP clients.

- [R114]** When the IPv4 Connection Addressing is *DHCP*, the Service Provider **MUST** use DHCP to convey to the Subscriber, in addition to the IPv4 address, the subnet mask and the default router address.

If the value of the SD-WAN UNI IPv4 Connection Addressing is *Static*, then IPv4 addresses in a given IPv4 subnet are statically assigned to the Service Provider and the Subscriber.

For *DHCP* and *Static*, a number of further parameters have to be agreed including:

- Primary Subnet:
  - IPv4 Prefix (IPv4 address prefix and mask length between 0 and 31, in bits)
  - Service Provider IPv4 Addresses (Non-empty list of IPv4 addresses)
- Optional Secondary Subnet List; each entry containing:
  - IPv4 Prefix (IPv4 address prefix and mask length between 0 and 31, in bits)
  - Service Provider IPv4 Addresses (Non-empty list of IPv4 addresses)

The parameters consist of a primary subnet and zero or more secondary subnets. In each case, the IP Prefix is specified, along with the Service Provider's IPv4 addresses. In the case of the primary subnet, this IP Prefix is referred to as the Connection Primary IPv4 Prefix, and for a secondary subnet, the Connection Secondary IPv4 Prefix.

For *DHCP* the address of the Subscriber's default router is provided in the DHCP response. For *Static* addressing, the Service Provider's addresses are assumed to be the default router addresses.

Note that the IPv4 Prefix and Service Provider addresses need to be agreed even when DHCP is used, so that the Subscriber can ensure they do not conflict with any other addressing used within the Subscriber Network.

If DHCP is used, the IPv4 address range from which Subscriber addresses are dynamically assigned is taken from the prefixes listed in the value of the SWVC Reserved Prefixes Service Attribute that are subnets of the Connection Primary IPv4 Prefix or a Connection Secondary IPv4 Prefix.

- [R115]** If the value of SD-WAN UNI IPv4 Connection Addressing is *DHCP*, addresses that are dynamically assigned by DHCP within the Connection Primary IPv4 Prefix or a Connection Secondary IPv4 Prefix **MUST** be taken from within an IP Prefix listed in the SWVC Reserved Prefixes Service Attribute (section 9.5) that is a subnet of the Connection Primary IPv4 Prefix or Connection Secondary IPv4 Prefix.

For example, if the SWVC List of Reserved Prefixes includes:

- 192.168.1.0/26
- 192.168.2.0/26

and the Connection Primary IPv4 Prefix is 192.168.1.0/24, DHCP can dynamically assign addresses 192.168.1.1 through 63 and the Subscriber can assign addresses 192.168.1.64 through 254 (note that [R117] prohibits the Subscriber from assigning the highest address in the prefix).

- [R116] If the value of the SD-WAN UNI IPv4 Connection Addressing is *Static* or *DHCP*, for the Primary Subnet and for each Secondary Subnet, the Service Provider IPv4 Addresses **MUST** be within the specified IPv4 Prefix.

The Subscriber can statically assign any IPv4 address within the subnets identified by the Connection IPv4 Prefixes, other than the Service Provider address itself, the lowest and highest possible addresses, which are generally reserved, and any addresses within IP Prefixes listed in the value of the SWVC Reserved Prefixes Service Attribute (see section 9.5).

- [R117] If the value of the SD-WAN UNI IPv4 Connection Addressing is *DHCP* or *Static*, the Subscriber **MUST NOT** statically assign any of the following for use by Subscriber devices connected to the UNI:
- Any IPv4 address that is neither within the Connection Primary IPv4 Prefix nor within the Connection Secondary IPv4 Prefix for an entry in the Secondary Subnet List.
  - Any of the Primary Subnet Service Provider IPv4 Addresses.
  - Any of the Service Provider IPv4 Addresses specified in an entry in the Secondary Subnet List.
  - The lowest and highest IPv4 addresses in the Connection Primary IPv4 Prefix, if the prefix length is less than or equal to 30.
  - The lowest and highest IPv4 addresses in the Connection Secondary IPv4 Prefix for an entry in the Secondary Subnet List, if the prefix length is less than or equal to 30.
  - Any IPv4 address within IP Prefixes listed in the value of the SWVC Reserved Prefixes Service Attribute (see section 9.5).

## 11.5 SD-WAN UNI IPv6 Connection Addressing Service Attribute

The SD-WAN UNI IPv6 Connection Addressing specifies how IPv6 addresses are allocated to the devices connected to the UNI. It is one of the five values *None*, *DHCP*, *SLAAC*, *Static* or *LL-only*, plus in the case of *DHCP*, *SLAAC* or *Static*, some additional parameters. If the IPv6 Connection Addressing is *None*, no IPv6 addresses are used by the devices connected to the UNI and IPv6 is disabled on the link. Note that in this case IPv4 connection addresses are needed (see [R113]).

- [R118] If the value of the SD-WAN UNI IPv6 Connection Addressing Service Attribute is *None*, IPv6 Packets **MUST NOT** be forwarded to or from the UNI.

If the value of the SD-WAN UNI IPv6 Connection Addressing Service Attribute is one of *DHCP*, *Static*, *SLAAC*, or *LL-only*, then IPv6 Link-Local addresses are present on the UNI. If the value is *LL-only*, then only IPv6 Link-Local addressing is used on the UNI.

If the value of the SD-WAN UNI IPv6 Connection Addressing is *DHCP*, then DHCPv6 is used by the Subscriber devices to request IPv6 addresses in a given subnet from the Service Provider as described in RFC 3315 [16]. The Service Provider hosts the DHCP server, and the Subscriber devices act as the DHCP clients.

- [R119] When the value of the SD-WAN UNI IPv6 Connection Addressing Service Attribute is *DHCP*, the Service Provider **MUST** use DHCP to convey to the

Subscriber, in addition to the IPv6 address, the subnet mask and the default router address.

If the value of the SD-WAN UNI IPv6 Connection Addressing is *Static*, then IPv6 addresses in a given IPv6 subnet are statically assigned to the Service Provider and the Subscriber.

If the value of the SD-WAN UNI IPv6 Connection Addressing is *SLAAC*, then Stateless Address Autoconfiguration (SLAAC) is used by the Subscriber devices to create unique IPv6 global addresses within an IP Prefix advertised by the Service Provider as described in RFC 4862 [20]. The Router Advertisements that convey the IP Prefix are also used to convey the prefix length and router address.

For *DHCP*, *SLAAC* and *Static*, several further parameters have to be agreed:

- Subnet List of one or more subnets, each comprising:
  - IPv6 Prefix
    - IPv6 address prefix and prefix length between 0 and 128 for *DHCP* and *Static*, or
    - IPv6 address prefix and prefix length of 64 for *SLAAC*
  - Service Provider IPv6 Addresses (Non-empty list of IPv6 addresses)

The parameters consist of a list of one or more subnets. For each subnet, the IPv6 prefix and the Service Provider's IPv6 address are specified. The IPv6 Prefix is referred to as a Connection IPv6 Prefix. Note that an IP Prefix and Service Provider addresses need to be agreed even when DHCP or SLAAC is used, so that the Subscriber can ensure they do not conflict with any other addressing used within the Subscriber Network.

A list (possibly empty) of reserved IP Prefixes can be specified (section 9.5); these specify IP addresses that are not available for the Subscriber to assign statically.

If DHCP is used, the IPv6 address range, from which Subscriber addresses are dynamically assigned, is taken from the prefixes listed in the value of the SWVC Reserved Prefixes Service Attribute that are subnets of any Connection IPv6 Prefix.

**[R120]** If the value of the SD-WAN UNI IPv6 Connection Addressing is *Static*, *DHCP* or *SLAAC*, for each entry in the Subnet List, the Service Provider IPv6 Addresses **MUST** be within the Connection IPv6 Prefix for that entry.

**[R121]** If the value of the SD-WAN UNI IPv6 Connection Addressing is *DHCP*, addresses that are dynamically assigned by DHCP within one of the Connection IPv6 Prefixes **MUST** be taken from within an IP Prefix in the value of the SWVC Reserved Prefixes (section 9.5) that is a subnet of that Connection IPv6 Prefix.

**[R122]** If the value of the SD-WAN UNI IPv6 Connection Addressing is *SLAAC*, the IP Prefix advertised by the Service Provider as described in RFC 4862 [20] using Router Advertisements **MUST** be the Connection IPv6 Prefix for the first entry in the Subnet List.

The Subscriber can statically assign any IPv6 address within the subnets identified by the Connection IPv6 Prefix in each entry, other than the Service Provider address itself, the lowest and highest possible addresses, which are generally reserved, and any address within IP Prefixes listed in the value of the SWVC Reserved Prefixes Service Attribute (see section 9.5).

- [R123] If the value of the SD-WAN UNI IPv6 Connection Addressing is *DHCP*, *SLAAC* or *Static*, the Subscriber **MUST NOT** statically assign any of the following for use on the UNI by Subscriber devices:
- Any IPv6 address that is not within the Connection IPv6 Prefix for an entry in the Subnet List.
  - Any IPv6 address within the Connection IPv6 Prefix for the first entry in the Subnet List, if the SD-WAN UNI IPv6 Connection Addressing is *SLAAC*.
  - Any of the Service Provider IPv6 Addresses specified in an entry in the Subnet List.
  - The lowest and highest IPv6 addresses in the Connection IPv6 Prefix for an entry in the Subnet List if the prefix length is less than or equal to 126.
  - Any IPv6 address within IP Prefixes listed in the value of the SWVC Reserved Prefixes Service Attribute (see section 9.5).

## 11.6 SD-WAN UNI Routing Protocols Service Attribute

The SD-WAN UNI Routing Protocols Service Attribute specifies the routing protocols and associated parameters that are used to exchange IP routes across the UNI. The value is a list of protocols (possibly empty), where each entry consists of the protocol name (one of *Static*, *BGP*, or *OSPF*), the type of routes that will be exchanged (one of *IPv4*, *IPv6* or *Both*), and a set of additional parameters as specified in the subsections below.

- [R124] The value of the SD-WAN UNI Routing Protocols Service Attribute **MUST NOT** contain more than one entry for the same protocol name, except when there are exactly two entries with a given protocol name, one with route type IPv4 and one with route type IPv6.

Note that regardless of the routing protocol in use, the Service Provider is responsible for forwarding IP Packets with a destination IP Address within the IP Prefixes identified by the SD-WAN UNI IPv4 Connection Addressing Service Attribute (see section 11.4) and the SD-WAN UNI IPv6 Connection Addressing Service Attribute (see section 11.5) toward the corresponding UNI.

When all of the end hosts in the Subscriber Network that are reachable at a given UNI are directly adjacent (at Layer 3) to that UNI (i.e. there is no router on the Subscriber's side of the UNI), and therefore only use IP addresses within the IP Prefixes identified by the SD-WAN UNI IPv4 Connection Addressing Service Attribute (see section 11.4) and the SD-WAN UNI IPv6 Connection Addressing Service Attribute (see section 11.5), there is no need to specify any additional routing information (static routing or dynamic routing protocols). In that case, the Subscriber can use a "default gateway", i.e., a default route towards the Service Provider's address

specified in the SD-WAN UNI IPv4 Connection Addressing Service Attribute (see section 11.4) or the SD-WAN UNI IPv6 Connection Addressing Service Attribute (see section 11.5). As above, the Service Provider directs traffic towards the UNI that is destined for an IP address within the IP Prefix identified by the connection addressing attributes, and in this case the value of the SD-WAN UNI Routing Protocols Service Attribute can be an empty list.

Each of the routing protocols specified below has a parameter for setting the administrative distance. This is a numeric metric used to control which routes are selected, when there are multiple routes for the same IP Prefix. A lower number indicates a more preferable route.

Setting the administrative distance can be useful when the same IP Prefix in the Subscriber Network is reachable via two or more UNIs, to allow the Subscriber to select which UNI the Service Provider should use to reach IP Addresses within the IP Prefix. Note that once a given UNI is selected, it remains the Service Provider's responsibility to direct IP Packets from the Ingress UNI to that Egress UNI over the UCSs in accordance with the Policy that is applied to those IP Packets. Setting the administrative distance only impacts which Egress UNI is used to reach the destination.

- [R125] IP Prefixes identified by the SD-WAN UNI IPv4 Connection Addressing Service Attribute (see section 11.4) and the SD-WAN UNI IPv6 Connection Addressing Service Attribute (see section 11.5) **MUST** be assigned an administrative distance of 0.
- [R126] For a given UNI, routes towards other UNIs **MUST** be assigned an administrative distance of 200.
- [R127] When selecting the best route for packet delivery as described in section 7.15, the Service Provider **MUST** select a route with the lowest administrative distance.

Note that the administrative distance values used in this document and specified in the value of the SD-WAN UNI Routing Protocols Service Attribute are only related to each other, to specify the relative preference of routes. They might or might not correspond with administrative distance values actually used in the Service Provider's devices to implement the behavior.

If two routes for an IP Prefix have the same administrative distance, then the Service Provider is free to choose which Egress UNI to use to deliver an IP Packet destined for that IP Prefix.

For BGP and OSPF, setting a different administrative distance for different IP Prefixes is not supported in this version of the standard.

### 11.6.1 Static

When an entry in the SD-WAN UNI Routing Protocols list is for *Static*, the IP Prefixes reachable in the Subscriber Network directly attached to this UNI are specified as additional parameters in the entry. These are known as Static IP Routes. For each Static IP Route, the following information is specified in addition to the IP Prefix:

- A next hop IP address in the Subscriber Network

- Administrative Distance, an integer greater than 0 and less than 256.

The Service Provider directs traffic destined for an address within any of the Static IP Routes towards the UNI, using the next hop address. The Subscriber routes traffic towards the UNI (e.g., by using a default or aggregate route).

The same IP Prefix can be specified more than once in the list of Static IP Routes, if it has different forwarding information.

If a static prefix is specified with a next hop address that is not reachable over this UNI, the Static IP Route is considered inactive and hence is not used by the Service Provider for directing traffic. In particular, the Static IP Route is not used if the specified next hop can only be reached via a different UNI.

Note: if a Static IP Route is specified that matches the IP Prefix for the connection addresses for the UNI (see sections 11.4 and 11.5) the connected route is always preferred as it has administrative distance fixed to 0.

### 11.6.2 BGP

When an entry in the SD-WAN UNI Routing Protocols is for *BGP*, BGP as specified in RFC 4271 [18] is used across the UNI to exchange routing information. The Subscriber uses BGP to advertise IP Prefixes used within the Subscriber Network that are reachable over the UNI to the Service Provider, which consequently directs traffic destined for any IP address within those IP Prefixes towards the UNI corresponding to the next hop associated with the IP Prefix. The Service Provider uses BGP to advertise IP Prefixes that are reachable via other UNIs in the SWVC so that the Subscriber can direct traffic towards those IP Prefixes over the corresponding UNIs. The capabilities described in this section cover several common configurations including the five shown in Figure 16.

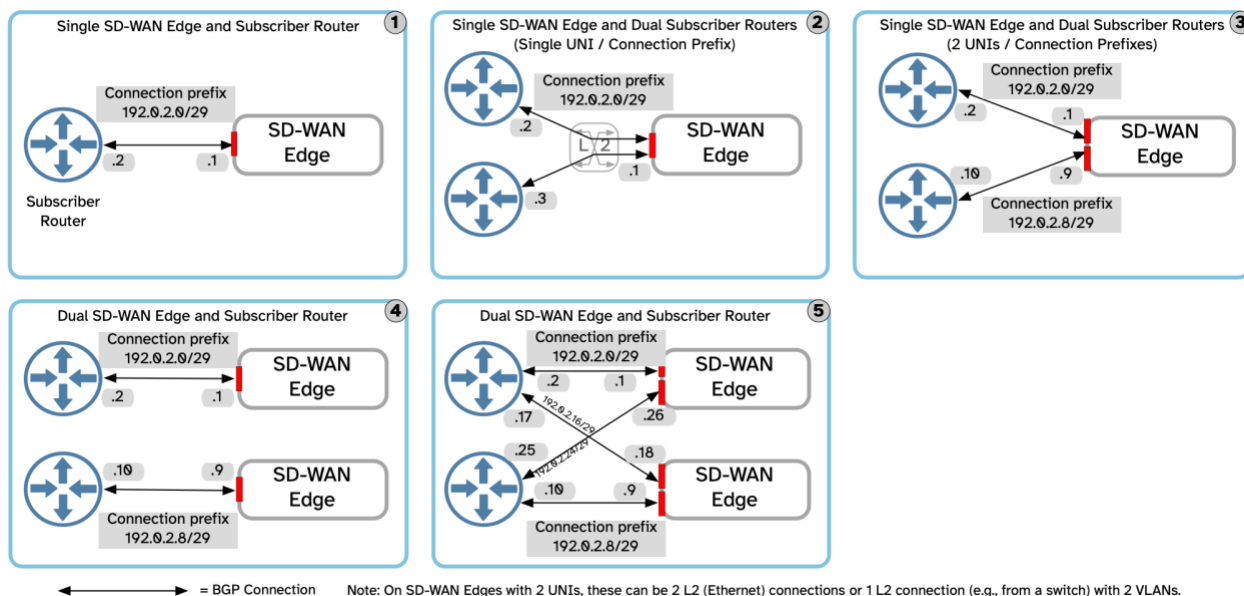


Figure 16 – BGP Configurations Examples

The Subscriber and the SD-WAN Edges use BGP to advertise and learn IP Prefixes that are reachable via UNIs in the SWVC, so that the Subscriber can direct traffic destined for those IP Prefixes towards the Service Provider, over the UNI corresponding to the next hop associated with the IP Prefix.

- [R128]** When an entry in the SD-WAN UNI Routing Protocols is specified for *BGP*, BGP as specified in RFC 4271 [18] **MUST** be used across the UNI to exchange routing information.

The additional parameters that need to be agreed on when BGP is used:

- The AS Number of the Subscriber
- The AS Number of the Service Provider
- Connection Address Family (*IPv4* or *IPv6*)
- A list of one or more Subscriber IP Addresses at the UNI that are:
  - In the address family identified by the Connection Address Family parameter
  - Within the Connection Primary IPv4 Prefix (see section 11.4) or a Connection IPv6 Prefix (see section 11.5) for the UNI, and
  - Not included in any of the Service Provider's reserved addresses (which includes DHCP-assigned addresses)
- Authentication (None or MD5 plus a password)
- BGP Community List (may be empty) (see below)
- BGP Extended Community List (may be empty) (see below)
- Hold Time (time in seconds)
- Damping (None or a set of damping parameters)
- AS Override (Enabled or Disabled)
- Administrative Distance (integer greater than 0 and less than 256)

The Subscriber's and Service Provider's AS Numbers are used to establish BGP peerings.

One or more BGP sessions can be established between the Subscriber and the SD-WAN Edge. These sessions can be established using either IPv4 or IPv6, as specified by the Connection Address Family parameter. For each session a Subscriber IP Address within one of the connection prefixes (see sections 11.4 and 11.5) is agreed on. For IPv4 sessions, the session is established between this Subscriber address and the first Service Provider address in the primary subnet specified in the SD-WAN UNI IPv4 Connection Addressing Service Attribute (section 11.4). For IPv6 sessions, the session is established between the specified Subscriber address and the first Service Provider address in the first subnet specified in the SD-WAN UNI IPv6 Connection Addressing Service Attribute (section 11.5). These peering sessions are single hop eBGP connections. Note in this case that the same values for the parameters above apply to each of these BGP peering sessions.

- [R129]** When an entry in the value of the SD-WAN UNI Routing Protocols Service Attribute is BGP, the Service Provider **MUST** support 4-octet AS Numbers as described in RFC 6793 [23].

- [R130]** When an entry in the value of the SD-WAN UNI Routing Protocols Service Attribute is BGP, and the Connection Address Family parameter is IPv4, then

the SD-WAN UNI IPV4 Connection Addressing Service Attribute (section 11.4) **MUST** be *Static*.

- [R131] When an entry in the value of the SD-WAN UNI Routing Protocols Service Attribute is BGP, and the Connection Address Family parameter is IPv6, then the SD-WAN UNI IPV6 Connection Addressing Service Attribute (Section 11.5) **MUST** be *Static*.
- [R132] When an entry in the value of the SD-WAN UNI Routing Protocols Service Attribute is BGP, if the Authentication parameter is MD5, authentication using MD5 **MUST** be used as described in RFC 4271 [18] using the specified password.

The Service Provider can configure BGP to wait passively for the Subscriber's devices to connect to it; this is helpful if it is not known whether the Subscriber devices are available yet. To ensure this works, the Subscriber has to use active mode.

- [R133] The Subscriber **MUST NOT** use passive TCP establishment for BGP sessions with the Service Provider.

The Service Provider, however, can use passive TCP establishment for BGP sessions with the Subscriber.

BGP Communities and Extended Communities allow additional metadata to be attached to route advertisements. Except in the case of the few standardized well-known values, this additional metadata has no intrinsic meaning. However, it is common for Service Providers to define a set of Communities or Extended Communities with associated semantics, that the Subscriber can attach to their route advertisements in order to affect how they are handled by the Service Provider.

- [R134] Each entry in the BGP Community List and BGP Extended Community List parameters **MUST** have an associated semantic that describes how the Service Provider will handle routes advertised with that value.

The Hold Time parameter indicates the agreed Hold Time used for the BGP sessions. The possible values are 0 or an integer in the range 3–65535, as defined in RFC 4271 [18].

The Service Provider can apply route flap damping to advertisements from the Subscriber, but in this case the parameters have to be agreed.

- [R135] When the Damping parameter is not None, the Service Provider **MUST** apply route flap damping as described in RFC 2439 [10].
- [R136] When the Damping parameter is not None, a single set of parameters as described in section 4.2 of RFC 2439 [10] **MUST** be agreed.
- [R137] When the Damping parameter is None, the Service Provider **MUST NOT** apply route flap damping.

In cases where the Subscriber uses the same AS number in different parts of the Subscriber Network, it is necessary to tweak the normal handling of AS Paths in routes advertised to the Subscriber at each UNI, to prevent the routes being discarded due to BGP's loop prevention mechanisms. Two mechanisms are commonly used for this:

- The Subscriber can configure their BGP routers to disable the loop prevention mechanism in the case where their own AS Number appears in the AS Path (this is commonly known as "Allow-AS-in"). In this case, the Service Provider does not need to be aware that this is being done and hence no parameters need to be agreed.
- The Service Provider can overwrite instances of the Subscriber's AS Number in the AS Path with their own AS Number, when advertising routes to the Subscriber (this is commonly known as "AS Override"). This needs to be explicitly agreed between the Service Provider and the Subscriber.

**[R138]** When the AS Override parameter is Enabled, the Service Provider **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.

The Administrative Distance is applied by the Service Provider to all IP Prefixes advertised by the Subscriber over the UNI using BGP.

### 11.6.3 OSPF

When an entry in the UNI Routing Protocols is for *OSPF*, then OSPF as specified in RFC 2328 [9] (for IPv4) and/or RFC 5340 [22] (for IPv6) is used across the UNI to exchange routing information. The Subscriber uses OSPF to advertise to the Service Provider IP Prefixes used within the Subscriber Network that are reachable via the UNI. The Service Provider consequently directs traffic destined for any IP address within those IP Prefixes towards the UNI over which the IP Prefixes were advertised. The Service Provider uses OSPF to advertise IP Prefixes that are reachable via other UNIs in the SWVC, so that the Subscriber can direct traffic towards those IP Prefixes over the corresponding UNIs.

**[R139]** When an entry in the UNI Routing Protocols is specified for *OSPF*, then OSPF as specified in RFC 2328 [9] (for IPv4) and/or RFC 5340 [22] (for IPv6) **MUST** be used across the UNI to exchange routing information.

The additional parameters that need to be agreed when OSPF is used are:

- Area ID (0 – 4294967295, normally expressed as an IPv4 address)
- Area type (*Normal*, *Stub* or *NSSA*)
- Authentication Type (for IPv4: None, Password, or Message Digest)
- Hello Interval (0 – 65535, in seconds)
- Dead Interval (0 – 4294967295, in seconds)
- Retransmit Interval (integer greater than 0, in seconds)
- Administrative Distance (integer in the range 1–255)

The Area ID is a 32-bit number (typically written as an IPv4 address) that specifies the OSPF Area.

If the Area ID is 0 (0.0.0.0), the area is the OSPF Backbone area. This can be used at the UNI, for example, if the Subscriber wishes for the Service Provider to implement a “super backbone” configuration, which allows the remote networks to appear to be in the same OSPF Backbone Area (Area ID 0), preserving the Subscriber’s route types. If a “super-backbone” is not used, the Subscriber’s routes from the remote locations will be learned as external, which can affect the routing within the Subscriber Network.

The Area Type indicates the type of OSPF Area. An Area Type of Normal means the area is not a stub or NSSA (see RFC 3101 [13]).

The Authentication Type indicates the type of authentication used for IPv4 OSPFv2 adjacencies. Authentication for IPv6/OSPFv3 is beyond the scope of this document. The Hello Interval, Dead Interval, and Retransmit Interval specify the various timers that are used to create OSPF adjacencies.

The Administrative Distance is an integer greater than 0 and is applied by the Service Provider to all IP Prefixes advertised by the Subscriber over the UNI using OSPF.

Note: parameters, behavior and requirements relating to the use of OSPF Sham links, and further parameters relating to authentication are not addressed in this version of the standard.

## 12 UCS Service Attributes

This section contains Service Attributes that apply to each of the Underlay Connectivity Services that compose the SD-WAN Service (SWVC). There is one instance of these attributes for each Underlay Connectivity Service underlying the SWVC.

Underlay Connectivity Services are network services independent of the SD-WAN Service and can have a large number of “characteristics” or “attributes” that define their configuration and behavior. This specification assumes that all those attributes are agreed on between the UCS Subscriber and the UCS Service Provider and, if necessary, communicated to the SD-WAN Service Provider (e.g., if the UCS Subscriber is not the SD-WAN Service Provider). The UCS and UCS End Point Service Attributes defined in this document are in addition to those attributes and include only those attributes necessary to define UCS external interfaces and behavior to the extent necessary to implement SD-WAN Policies. Attributes that are internal to the UCS itself, such as those defining the associations between the UCS and UCS End Points or between the UCS End Point and UCS UNI are part of the UCS Service Agreement described earlier in this paragraph and are not included as Service Attributes for the SD-WAN Service.

The UCS Service Attributes are summarized in the following table, and each is described in more detail in the subsequent sections.

Attribute Name	Summary Description	Possible Values
UCS Identifier	Identification of the Underlay Connectivity Service for management purposes.	Unique Identifier String for the SD-WAN Service
UCS Type	Indicates whether the UCS is a Public UCS (i.e., Internet Access Service) or a Private UCS.	<i>Public</i> or <i>Private</i>
UCS Billing Method	Indicates how the UCS is billed	<i>Flat-rate</i> or <i>Usage-based</i>

**Table 11 – Summary of UCS Service Attributes**

### 12.1 UCS Identifier Service Attribute

The value of the UCS Identifier Service Attribute is a string that is used to allow the Subscriber and Service Provider to uniquely identify an Underlay Connectivity Service.

**[R140]** The value of the UCS Identifier Service Attribute **MUST** be an Identifier String.

**[R141]** The value of the UCS Identifier Service Attribute **MUST** be unique across all UCS Identifiers in the Service Provider Network.

### 12.2 UCS Type Service Attribute

The value of the UCS Type Service Attribute indicates whether the UCS is a Public UCS (i.e., an Internet Access Service) or a Private UCS. The possible values are *Public* and *Private*.

- [R142] If the Underlay Connectivity Service is an IP Service with characteristics consistent with the following MEF 61.1 [29] Service Attributes: IPVC Topology Service Attribute = *Cloud Access* and IPVC Cloud Service Attribute with Cloud Type parameter = *Internet Access*; then the value of the UCS Type Service Attribute **MUST** be *Public*.
- [R143] If the Underlay Connectivity Service is not an Internet Access Service as described in [R142], then the value of the UCS Type Service Attribute **MUST** be *Private*.

### 12.3 UCS Billing Method Service Attribute

The UCS Billing Method Service Attribute indicates how access to the Underlay Connectivity Service is billed. The allowed values are *Flat-rate*, *Usage-based*, and *Other*.

## 13 UCS UNI Service Attributes

Access to an Underlay Connectivity Service is provided at the SD-WAN Edge via the UCS UNI. MEF uses the term UNI consistently across all service standards to represent the demarcation point between the responsibility of the Subscriber and the responsibility of the Service Provider. Although not all Underlay Connectivity Services are MEF Services, the concept of this demarcation point is relevant to all carrier-based services. So, if the Underlay Connectivity Service is a MEF service the UCS UNI refers to the MEF-defined UNI for that service and if the Underlay Connectivity Service is not a MEF-defined service the UCS UNI refers, nonetheless, to the relevant demarcation point.

The UCS UNI Service Attributes are summarized in the following table, and each is described in more detail in the subsequent sections.

Attribute Name	Summary Description	Possible Values
UCS UNI Identifier	Identification of the Underlay Connectivity Service UNI for management purposes.	Identifier String

**Table 12 – Summary of UCS UNI Service Attributes**

### 13.1 UCS UNI Identifier Service Attribute

The value of the UCS UNI Identifier Service Attribute is a string that is used to allow the Subscriber and Service Provider to uniquely identify an Underlay Connectivity Service UNI.

- [R144] The value of the UCS UNI Identifier Service Attribute **MUST** be an Identifier String.
- [R145] The value of the UCS UNI Identifier Service Attribute **MUST** be unique across all UCS UNI Identifiers in the Service Provider Network.

## 14 UCS End Point Service Attributes

A UCS is connected to a UCS UNI by a UCS End Point. As discussed in section 7.6, some service architectures support multiple UCSs at the same UCS UNI. The UCS End Point captures Service Attributes at the UCS UNI whose value can differ between UCSs.

The UCS End Point Service Attributes are summarized in the following table and described in the subsequent sections.

Attribute Name	Summary Description	Possible Values
UCS End Point Identifier	Identification of the Underlay Connectivity Service End Point.	Identifier String
UCS End Point Backup	Indicates whether the UCS should be treated as a Primary underlay or a Backup underlay at this UCS End Point.	<i>Enabled or Disabled</i>
UCS End Point Breakout	Indicates whether the SD-WAN Service can “break out” to the underlying UCS Service from this End Point.	<i>Enabled or Disabled</i>

**Table 13 – Summary of UCS End Point Service Attributes**

### 14.1 UCS End Point Identifier Service Attribute

The value of the UCS End Point Identifier Service Attribute is a string that is used to allow the Subscriber and Service Provider to uniquely identify an Underlay Connectivity Service End Point.

**[R146]** The value of the UCS End Point Identifier Service Attribute **MUST** be an Identifier String.

**[R147]** The value of the UCS End Point Identifier Service Attribute **MUST** be unique across all UCS End Point Identifiers for SWVCs (SD-WAN Services) in the Service Provider network.

### 14.2 UCS End Point Backup Service Attribute

This Service Attribute allows the Service Provider and Subscriber to agree on whether the UCS (at this UCS End Point) performs the role of a Backup UCS for some Application Flows. The value of the UCS End Point Backup Service Attribute can be *Enabled* or *Disabled* indicating whether the UCS can be used for any Application Flow (*Disabled*) or only those flows whose Policy at this SD-WAN Edge indicates that they can use a Backup UCS. See section 9.10.2.7 for details about how the BACKUP Policy is used.

### 14.3 UCS End Point Breakout Service Attribute

Application Flows can be assigned Policies that allow them to be forwarded to IP destinations that are reachable via the UCS rather than via the Subscriber Network at an SD-WAN UNI. This

operation is referred to as “breakout”. This Service Attribute allows the Subscriber and Service Provider to agree on the UCS End Points that allow breakout. Breakout can occur at all UCS End Points in the UCS or at specific UCS End Points. If breakout is disallowed at a UCS End Point, Application Flows can be forwarded over the SWVC (i.e., over TVCs in the SWVC) to another SD-WAN Edge connected to the UCS that allows breakout at the UCS End Point.

Although, in the general case, any UCS can support breakout, in this standard only Underlay Connectivity Services that are Internet Access Services (the value of the UCS Type Service Attribute is *Public*) support breakout (see Internet Breakout in section 7.12). Since all Internet Access UCSs are, in effect, connected, disallowing breakout at one UCS End Point implies that the Application Flows can be forwarded to another SD-WAN Edge with an Internet Access UCS with an End Point that allows breakout.

The value of the UCS End Point Breakout Service Attribute can be *Enabled* or *Disabled* and indicates whether breakout is allowed at the UCS End Point.

**[R148]** If the value of the UCS End Point Breakout Service Attribute is *Disabled*, IP Packets that are in Application Flows that are eligible (by Policy) for breakout **MUST NOT** break out at the UCS End Point.

Defining this Service Attribute as a generic “breakout” Service Attribute rather than specifically an Internet Breakout Service Attribute, provides flexibility for the Service Provider to define additional breakout-related Policy Criteria and capabilities.

## 15 Performance Metrics

The PERFORMANCE Policy Criterion (see section 9.10.2.8) provides the means for Policies to specify real-time performance requirements for Application Flows. The SD-WAN Service attempts to forward IP Packets over Paths that meet or exceed the performance goals specified in the PERFORMANCE Policy Criterion, consistent with the requirements and restrictions posed by other Policy Criteria. The Performance Criterion supports three different Performance Metrics: One-way Packet Delay, One-way Packet Delay Variation, and One-way Packet Loss Ratio.

Section 15.1 defines Qualified Packets that are the packets for which the Performance metrics apply. Section 15.2 defines One-Way Packet Delay, on which two of the three metrics are based. The subsequent three subsections define the three Performance Metrics used in this document.

### 15.1 Qualified Packets

The Performance Metrics defined in the sections below apply to Qualified Packets. A Qualified Packet between two UNIs, referred to as  $x$  and  $y$ , across a Path, referred to as  $p$ , is any unicast IP Packet that satisfies the following conditions:

- The IP Packet ingresses at UNI  $x$
- The destination of the IP Packet is at UNI  $y$
- The IP Packet is not discarded per requirements [R24], [R41], [R62], [R65], [R74], [R75], [R84], [R100], [R101], [D5], [O1]
- The Path  $p$  is chosen to carry the IP Packet
- The IP Packet is not fragmented
- The IP Packet does not incur significant intentional delay as a result of applying a security policy agreed to between the Service Provider and the Subscriber.

The final bullet in the list above is focused on delays as a result of security functions (such as those described in MEF 88 [33]) that require extended analysis (e.g., quarantining or malware detection and removal). Small increases in delay due to processing are expected to be factored into the agreed-on performance goals for the Service.

### 15.2 One-Way Packet Delay

The One-way Packet Delay for a Qualified Packet that is sent from UNI  $x$  to UNI  $y$  across Path  $p$  is defined as the time elapsed from the reception of the first bit of the packet at the Ingress UNI until the transmission of the last bit of the first corresponding Packet at the Egress UNI. If the packet is erroneously duplicated as it traverses the network, the delay is based on the first copy that is delivered.

Note that this definition of One-way Packet Delay for a packet includes the delays encountered as a result of transmission across the Ingress and Egress UNIs as well as that introduced by the network that connects them.

### 15.3 One-Way Mean Packet Delay Performance Metric

**[R149]** If a PERFORMANCE Policy Criterion includes a reference to One-Way Mean Packet Delay in the *primary* or *secondary* element, it **MUST** be defined as follows for each Path  $p$  between UNIs  $x$  and  $y$ :

Let  $\Delta = \{\delta_1, \delta_2, \delta_3, \dots, \delta_n\}$  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  $\delta_1 \dots \delta_n$ . If  $n=0$  during the time interval, the One-Way Mean Packet Delay for that time interval is zero.

### 15.4 One-Way Mean Packet Delay Variation Performance Metric

**[R150]** If the PERFORMANCE Policy Criterion includes a reference to One-Way Mean Packet Delay Variation in the *primary* or *secondary* element, it **MUST** be defined as follows for each Path  $p$  between UNIs  $x$  and  $y$ :

Let  $\Delta = \{\delta_1, \delta_2, \delta_3, \dots, \delta_n\}$  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  $\Delta'$  be the set of all pairs of elements  $\{\delta_r, \delta_s\}$  in  $\Delta$  such that  $s > r$  and the difference in the arrival time at the Ingress UNI of packets  $s$  and  $r$  equals the value of the *arrivalinterval* element in the SWVC Performance Time Intervals Service Attribute. If  $\Delta'$  is *null*, then the One-Way Mean Packet Delay Variation for the time interval is zero. Otherwise, let  $v_{rs}$  be the absolute value of the difference in One-Way Packet Delay for each pair,  $\{\delta_r, \delta_s\}$  in  $\Delta'$ , i.e.,  $v_{rs} = |\delta_r - \delta_s|$ . Then the One-Way Mean Packet Delay Variation for  $p$  over that interval is the arithmetic mean of the values  $v_{rs}$  for each element in  $\Delta'$ .

### 15.5 One-Way Packet Loss Ratio Performance Metric

**[R151]** If the *primary* or *secondary* element of the PERFORMANCE Policy Criterion 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  $(s-r)/s$

The One-Way Packet Loss Ratio is usually represented as a percentage.

## 16 References

- [1] IANA, *Protocol Numbers*,  
<https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>
- [2] IANA, *Service Name and Transport Protocol Port Number Registry*,  
<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>
- [3] IEEE Std 802.1Q-2018, *IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks*, May 2018
- [4] IEEE Std 802.3-2018, *IEEE Standard for Ethernet*, August 2018
- [5] IETF RFC 791, *Internet Protocol*, September 1981
- [6] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, March 1997
- [7] IETF RFC 2131, *Dynamic Host Configuration Protocol*, March 1997
- [8] IETF RFC 2132, *DHCP Options and BOOTP Vendor Extensions*, March 1997
- [9] IETF RFC 2328, *OSPF Version 2*, by John Moy, April 1998. Copyright © The Internet Society (1998). All Rights Reserved.
- [10] IETF RFC 2439, *BGP Route Flap Damping*, by Curtis Villamizar and Ravi Chandra and Dr. Ramesh Govindan, November 1998. Copyright © The Internet Society (1998). All Rights Reserved.
- [11] IETF RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, Fred Baker and David L. Black and Kathleen Nichols and Steven L. Blake, December 1998. Copyright © The Internet Society (1998). All Rights Reserved.
- [12] IETF RFC 2764, *A Framework for IP Based Virtual Private Networks*, by Andrew G. Malis and Dr. Arthur Y. Lin and Dr. Juha Heinanen and Bryan Gleeson and Dr. Grenville Armitage, February 2000. Copyright © The Internet Society (2000). All Rights Reserved.
- [13] IETF RFC 3101, *The OSPF Not-So-Stubby Area (NSSA) Option*, by Dr. Patrick W. Murphy, January 2003. Copyright © The Internet Society (2003). All Rights Reserved.
- [14] IETF RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP*, by Sally Floyd and Dr. K. K. Ramakrishnan and David L. Black, September 2001. Copyright © The Internet Society (2001). All Rights Reserved.
- [15] IETF RFC 3260, *New Terminology and Clarifications for Diffserv*, by Daniel B. Grossman, April 2002. Copyright © The Internet Society (2002). All Rights Reserved.

- [16] IETF RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, by Charles E. Perkins and Bernie Volz and Ted Lemon and Michael Carney and Jim Bound, July 2003. Copyright © The Internet Society (2003). All Rights Reserved.
- [17] IETF RFC 3550, *RTP: A Transport Protocol for Real Time Applications*, by Henning Schulzrinne and Stephen L. Casner and Ron Frederick and Van Jacobson, July 2003. Copyright © The Internet Society (2003). All Rights Reserved.
- [18] IETF RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*, by Yakov Rekhter and Susan Hares and Tony Li, January 2006. Copyright © The Internet Society (2006). All Rights Reserved.
- [19] IETF RFC 4342, *Profile for Datagram Congestion Control Protocol (DCCP)*, by Jitendra Padhye and Sally Floyd and Eddie Kohler, March 2006. Copyright © The Internet Society (2006). All Rights Reserved.
- [20] IETF RFC 4862, *IPv6 Stateless Address Autoconfiguration*, by Dr. Thomas Narten and Tatsuya Jinmei and Dr. Susan Thomson, September 2007. Copyright © The Internet Society (2007). All Rights Reserved.
- [21] IETF RFC 4960, *Stream Control Transmission Protocol*, by Randall R. Stewart, September 2007. Copyright © The Internet Society (2007). All Rights Reserved.
- [22] IETF RFC 5340, *OSPF for IPv6*, by Dennis Ferguson and Acee Lindem and John Moy, July 2008. Copyright © The Internet Society (2007). All Rights Reserved.
- [23] IETF RFC 6793, *BGP Support for Four-Octet Autonomous System (AS) Number Space*, by Quaizar Vohra and Enke Chen, December 2012. Copyright © The Internet Society (2012). All Rights Reserved.
- [24] IETF RFC 8174, *Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words*, by Barry Leiba, May 2017. Copyright © The Internet Society (2017). All Rights Reserved.
- [25] IETF RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*, by Dr. Steve E. Deering and Bob Hinden, July 2017. Copyright © The Internet Society (2017). All Rights Reserved.
- [26] MEF 6.3, *Subscriber Ethernet Services Definitions*, November 2019
- [27] MEF 10.4, *Ethernet Service Attributes*, Phase 4, December 2018
- [28] MEF 23.2, *Carrier Ethernet Class of Service – Phase 3*, August 2016
- [29] MEF 61.1, *IP Service Attributes*, January 2019
- [30] MEF 63, *Subscriber Layer 1 Service Attributes*, August 2018
- [31] MEF 69, *Subscriber IP Service Definitions*, November 2019

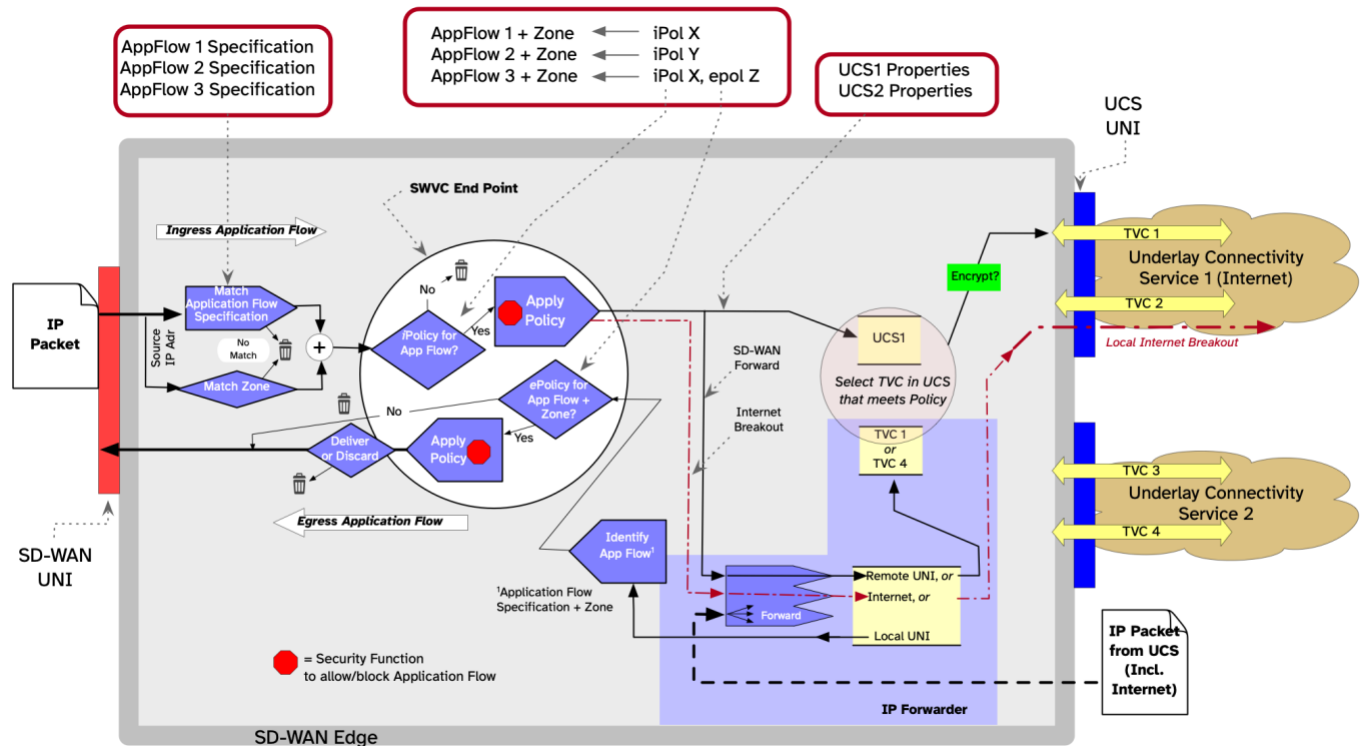
- [32] MEF 74, *Commercial Affecting Attributes Technical Standard*, December 2018
- [33] MEF 88, *Application Flow Security for SD-WAN Services*, November 2021
- [34] MEF White Paper, *Understanding SD-WAN Managed Services*, July 2017

## Appendix A Processing Application Flows (Informative)

This appendix describes the external behavior expected at the SD-WAN Edge in two ways. The first section describes a hypothetical processing architecture. It does not imply that any implementation be architected or implemented based on this model. The second part describes the behavior from a IP Packet and Service Attribute point of view.

### A.1 Process View

There are several steps in determining how to forward IP Packets as shown in Figure 17.<sup>17</sup>



**Figure 17 – Application Flows, Policies, and Forwarding**

Each Ingress IP Packet is inspected to associate it with an Application Flow. This requires identifying which Application Flow Specification it matches. The source IP Address of the IP Packet is used to select the Zone. If the packet does not match any of the defined Application Flow Specifications or if the source address doesn't match a Zone, it is discarded. The Policy assigned to the Application Flow is then applied to the IP Packet (if no Policy is assigned, the IP Packet is discarded). Based on the Policy and the properties of the Underlay Connectivity Services and TVCs, a list of TVCs that can carry the IP Packet (in the diagram, TVC1 in UCS1) is determined.

The IP Forwarder determines where to forward this IP Packet. There are four possibilities:

- There is no route to the destination and the IP Packet is discarded

<sup>17</sup> This example assumes that the Service Provider has created all of the necessary TVCs to meet the Policy and connectivity requirements of the SD-WAN Service, and that the necessary IP routing information has been agreed to and configured.

- The destination is at a remote UNI, i.e., the IP Packet must be forwarded across the SD-WAN Service. This results in a list of TVCs.
- The destination is on the Internet, i.e., the IP Packet must be forwarded to an Internet UCS if Policy allows Internet Breakout. The Internet Breakout can be local if an Internet UCS is available at the SD-WAN Edge or the IP Packet can be forwarded over the SD-WAN Service (i.e., a TVC) to another SD-WAN Edge for Internet Breakout.
- The destination is a UNI at this SD-WAN Edge and the IP Packet is forwarded to a local UNI if the Application Flow Policy allows.

If the destination is at a remote UNI, the forwarding process results in a list of TVCs that can reach the destination (in the diagram, TVC1 and TVC4). The intersection of this list and the TVCs that meet the Policy determines the TVC (or TVCs) that can carry the IP Packet (in this case, TVC1). Of course, it is possible for the intersection to include more than one TVC, in which case the Service Provider can choose any of them—the choice could be based on load balancing, performance optimization, or other criteria.

Packets arriving from the Underlay Connectivity Services go through a similar process. The IP Forwarder determines the destination (which can be the same as in the list above). If the IP Packet is destined for a remote UNI or the Internet (i.e., this is just an intermediate hop) then it is forwarded as appropriate. If the IP Packet is destined for a local UNI, the Application Flow Policy can be applied to the IP Packet to determine if it can be delivered to the UNI.

- If no Egress Policy is associated with the Application Flow, the IP Packet is forwarded to the UNI (note that this is the opposite of what happens for Ingress)
- If an Egress Policy is associated with the Application Flow, the IP Packet is forwarded or blocked based on that Policy.

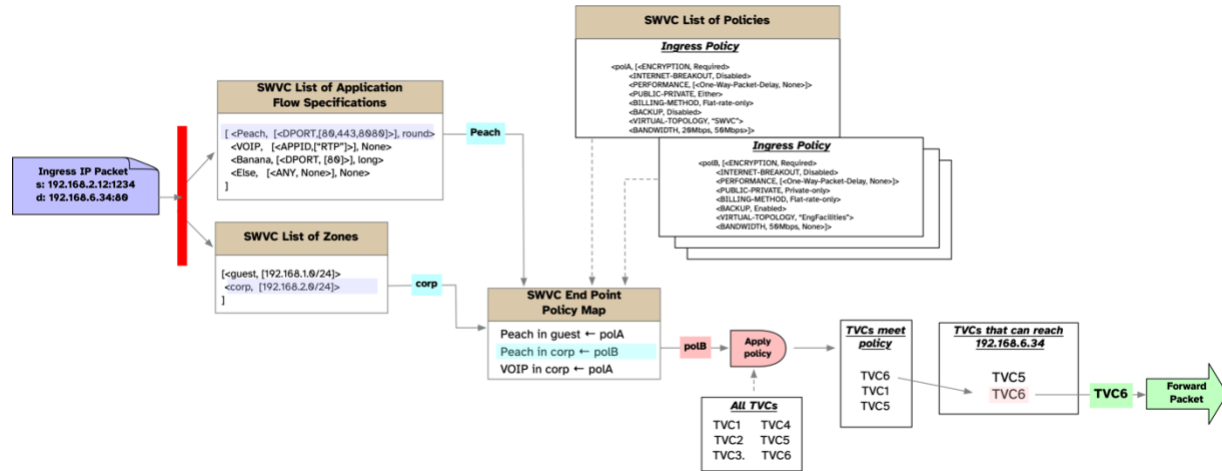
An Egress Policy is determined based on the Application Flow to which the IP Packet was assigned at the Ingress UNI. Since Application Flow Specifications and Zone definitions are SWVC-wide, these can, in most cases be determined at the Egress SWVC End Point. One exception is packets arriving from the Internet. As noted in section 10.4.2, these packets are assigned to the reserved Zone named *Internet*.

Figure 17 is a conceptual representation of the SD-WAN Edge functionality which is attempting to describe the externally visible behavior. In a given implementation the various processes could run in parallel, or they could be sequential or a mix. The description is implicitly assuming forwarding based on standard IP routing, but other IP forwarding approaches are possible, such as Policy-Based Routing, in which case this part of the process might be included in the “Apply Policy” process. The details of the implementation are beyond the scope of this document. The relevant point is that an IP Packet arrives, and one of four actions can be taken:

- It is forwarded over a TVC to another SD-WAN Edge
- It is forwarded to a local UNI
- It is forwarded to the Internet using Internet Breakout
- It is discarded

## A.2 Ingress Packet Flow View

The following diagram depicts the sequence of Service Attribute definitions that operate on an Ingress IP Packet.



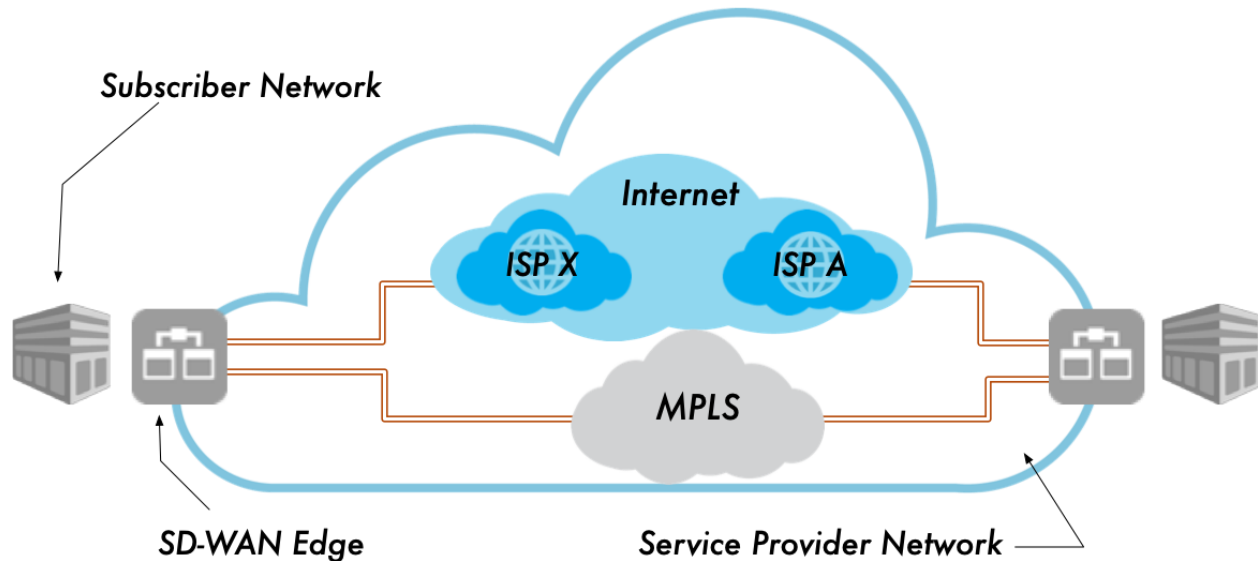
**Figure 18 – Ingress Packet Flow**

An Ingress IP Packet is assigned to an Application Flow based on the Application Flow Specification and the Zone. These two attributes of the IP Packet result in the selection of a Policy. In this case the IP Packet is associated with Application Flow *Peach* in Zone *corp*. This combination selects Policy *polB*. Policy *polB* can be met by TVCs 6, 1, and 5, ordered by the performance requirements specified by the PERFORMANCE Policy Criterion. TVCs 5 and 6 can reach the destination and therefore TVC6 is used because it has better performance.

## Appendix B SD-WAN Use Cases (Informative)

This section provides several SD-WAN use cases to assist in putting the normative sections of this document into context. These diagrams and text have been derived from the MEF white paper, *Understanding SD-WAN Managed Services* [34].

### B.1 Hybrid WAN

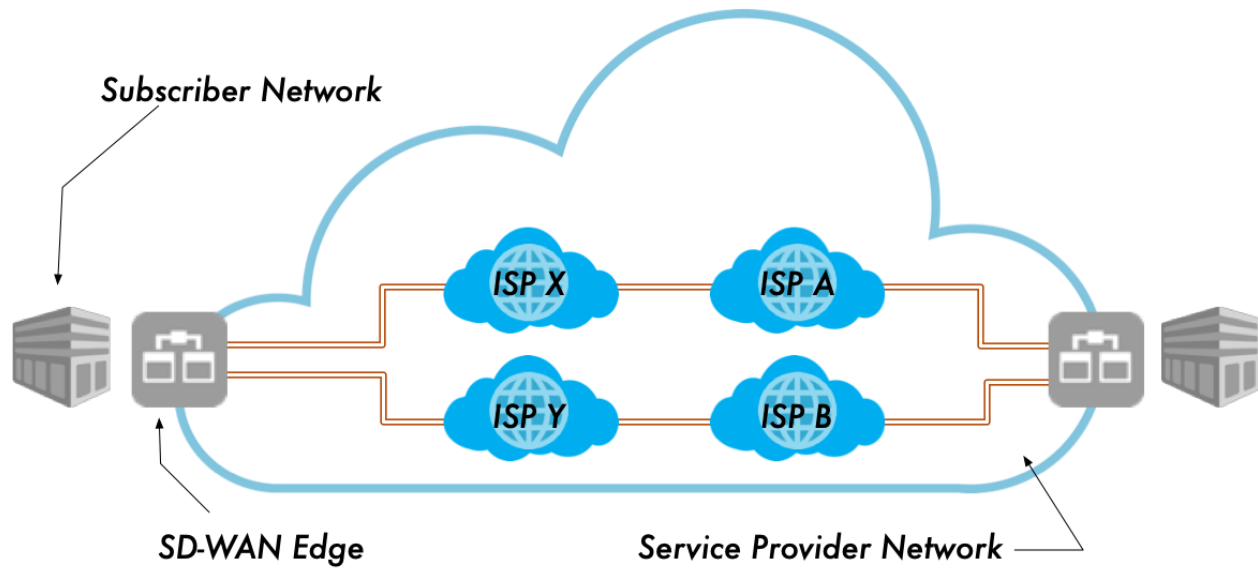


**Figure 19 – Use Case: Hybrid WAN**

Figure 19 illustrates a use case for an SD-WAN Service operating over three Underlay Connectivity Services, an Internet UCS (actually this is two UCS since each Internet Access Service is a different UCS) and an IP VPN UCS (e.g., implemented over MPLS) between the two sites. This hybrid UCS use case enables the Subscriber to use the multiple UCSs to achieve higher resiliency.

This is, perhaps, one of the most popular use cases because many enterprise Subscribers have both Internet and IP VPN UCSs to interconnect their sites, so the SD-WAN managed service enables them to take advantage of the benefits that SD-WAN provides over multiple UCSs.

## B.2 Dual Internet WAN



**Figure 20 – Use Case: Dual Internet WAN**

Figure 20 illustrates a use case for an SD-WAN service operating over multiple Internet Service Providers (ISPs) to achieve resiliency using multiple Internet Underlay Connectivity Services plus different ISPs. The ISPs' Internet connections could be DSL, Cable Internet, a dedicated Internet Access (DIA) service, or a combination of these.

Because the ISPs may not be the SD-WAN Service Provider, this use case could be applied to a larger SD-WAN managed service deployment where both sites are off-net and can only be reached via the Internet WAN.

## Appendix C Major Changes from MEF 70 to MEF 70.1 (Informative)

The following list represents the major changes in this standard, MEF 70.1, from the previous version, MEF 70:

- The document title was changed from “SD-WAN Service Attributes and Services” to “SD-WAN Service Attributes and Service Framework”.
- Added section 5.1 with Numerical Prefix Conventions and 5.2 with Notational Conventions. Move Diagram Conventions from section 7 to section 5.3.
- Inclusion of Service Attributes for Underlay Connectivity Services, UCS UNIs, and UCS End Points
- An updated definition of Application Flow that includes packet flows that both ingress a UNI and are directed toward the UNI
- Definition of Application Flow Specification as distinct from Application Flow
- Rename Application Flow Group to Application Flow Specification Group
- An updated and enhanced description of Application Flow Criteria
- The table of Application Flow Criteria and the table of Policy Criteria were split into two tables, those that Service Providers are required to support and those that Service Providers should support.
- The values for most Application Flow Criteria are now lists of items rather than individual items.
- The DSCP Field was added to the list of Application Flow Criteria that require support.
- An updated definition of Tunnel Virtual Connection (TVC) providing a more detailed and implementation-independent description
- New PERFORMANCE Ingress Policy Criterion to specify performance goals for an Application Flow
- New SWVC List of Security Policies Service Attribute
- New AF-SECURITY-INGRESS Ingress Policy Criterion and AF-SECURITY-EGRESS Egress Policy Criterion to invoke security functions listed in MEF 88 for an Application Flow.
- Support for Egress Policies and Egress Policy Criteria
- New BLOCK-SOURCE Egress Policy Criterion

- Updated and clarified description of the BANDWIDTH Ingress Policy Criterion
- New SD-WAN UNI Routing Service Attribute to allow the Subscriber to specify/advertise reachable subnets at the UNI
- New Service Attributes and Policy Criteria to support multiple Virtual Topologies that can be assigned by Policy
- Support for partitioning the Subscribers IP Hosts into Zones and assigning Zone-wide Ingress Policies
- Removed support for Priority-tagged frames from the SD-WAN UNI L2 Interface Service Attribute.
- Uniqueness requirements were tightened for the SWVC, SWVC End Point, and SD-WAN UNI Identifiers (Service Attributes).
- Updated the SWVC Service Uptime Objective Service Attribute with a requirement that provides a definition of “outage”.
- Several Policy Criteria with Boolean values were normalized to use *Enabled* and *Disabled* as values (as opposed to Yes/No, True/False, etc.).
- The parameters for the ENCRYPTION Policy Criterion have been changed from *Required* and *Either* to *Required-Always*, *Required-Public-Only*, *Either*. Modified the argument to several Application Flow Criteria to be a list (several of them were already lists, now all of them are).
- Clarified definitions and descriptions in several sections and concepts without changing the normative intention of the text. These include Internet Breakout and INTERNET-BREAKOUT Policy Criterion, BANDWIDTH Policy Criterion, definitions of the Performance Metrics.
- The *PCParam* element in SWVC List of Policies Service Attribute was changed from a list of parameters to a single parameter. If multiple parameters are needed, the Policy Criterion can define the argument as a list (or a n-tuple, if appropriate).