MEF 70

SD-WAN Service Attributes and Services

July 2019

Disclaimer

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

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

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

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

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

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

Implementation or use of specific MEF standards, specifications, or recommendations will be voluntary. This document is provided “as is” with no warranties whatsoever, express of 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

List of Figures

List of Tables

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.

- Amdocs Management Limited
- Ceragon Networks
- Cisco
- Colt
- Fujitsu Network Communications
- Huawei Technologies
- Nokia Networks
- Silver Peak
- Verizon

2 Abstract

The SD-WAN Service Attributes and Services Standard defines the externally-visible behavior of SD-WAN Services. The Service description 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 Service Attributes – i.e., the enumeration and description of the information that is agreed 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 the Service description. Rigorous definition of Service Attributes also facilitates information modeling for API and protocol definitions.

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.

It is important to distinguish between the SD-WAN Service and the Underlay Connectivity Services over which the SD-WAN operates. An SD-WAN Service Provider provides the SD-WAN Service to the Subscriber. The SD-WAN Service Provider may provide one or more of the Underlay Connectivity Services, but some or all of them may be provided by the SD-WAN Subscriber or other Service Providers.

3 Terminology and Abbreviations

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

In addition, terms defined in MEF 61.1 [21] 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 [18] or MEF 61.1 [21].

Term	Definition	Reference
Application Flow	A subset of the IP packets that arrive at an Ingress SD-WAN UNI, identified by a set of Application Flow Criteria, and distinct from the subset for any other Application Flow at that SD-WAN UNI.	This document
Application Flow Criterion	A rule that is used to classify IP Packets at an SD-WAN UNI.	This document
Application Flow Group	An aggregation of Application Flows at an SD-WAN UNI that can be used to assign a common Policy to the Application Flows and/or share bandwidth commitments and limitations among Application Flows.	This document
Egress IP Packet	An IP Packet transmitted to the Subscriber Network by the Service Provider at a UNI.	This document *
Ingress IP Packet	An IP Packet received from the Subscriber Network by the Service Provider at a UNI.	This document *
Internet Breakout	The forwarding of Application Flows, based on Policy, to (and from) the Internet via one or more Internet Underlay Connectivity Services located at SD-WAN Edges in the SD-WAN Service.	This document
Local Internet Breakout	Internet Breakout in which Ingress IP Packets at an SD-WAN UNI are forwarded over an Internet Underlay Connectivity Service at the SD-WAN Edge where the UNI is located.	This document
Policy	A set of rules that can be assigned to an Application Flow, possibly through membership in an Application Flow Group, that determines the handling by the SD-WAN Service of IP Packets in the Application Flow.	This document
Policy Criterion	One of the rules that compose a Policy	This document
SD-WAN	Software Defined Wide Area Network (see SD-WAN Service)	This document
SD-WAN Edge	Network functions (physical or virtual) that are located between the Underlay Connectivity Service UNI and the SD-WAN UNI.	This document
SD-WAN Service	An application-aware, policy-driven connectivity service, offered by a Service Provider, that optimizes transport of IP Packets over multiple underlay networks. 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

Term	Definition	Reference
SD-WAN Subscriber	A Subscriber of an SD-WAN Service	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 that partitions Ingress IP Packets into Application Flows, applies a Policy to each IP Packet based on the associated Application Flow, and selects an appropriate path to transport the IP Packet over the SWVC.	This document
Service Provider	An organization that provides services to Subscribers. In this document, "Service Provider" means "SD-WAN Service Provider".	This document *
Service Provider Network	The aggregation of Underlay Connectivity Services, TVCs, SD-WAN Edges, controllers, and orchestrators used to deliver an SD-WAN Service to a Subscriber.	This document
SLA	Service Level Agreement	This document *
Subscriber	The end-user of a service. In this document, "Subscriber" should be read as meaning "SD-WAN Subscriber".	This document *
Subscriber Network	A network belonging to a given Subscriber that is connected to the Service Provider at one or more 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 path between SD-WAN Edges across an Underlay Connectivity Service that provides a well-defined set of transport characteristics (e.g., delay, security, bandwidth, etc.).	This document
TVC	Tunnel Virtual Connection	This document
UCS	Underlay Connectivity Service	This document
UCS UNI	Underlay Connectivity Service User Network Interface	This document
Underlay Connectivity Service	A Service providing connectivity between two or more of the Subscriber's locations, over which an SD-WAN Service is provided; for example, an IP Service or a Carrier Ethernet service.	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
UNI	Short for User Network Interface. In this document, UNI without a modifier (such as "UCS UNI") means SD-WAN UNI.	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 [1], RFC 8174 [16]) 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 Introduction

An SD-WAN Service provides a virtual overlay network that enables application-aware, policy- driven, and orchestrated connectivity between SD-WAN User Network Interfaces, and provides the logical construct of a L3 Virtual Private Routed Network for the Subscriber that conveys IP Packets between Subscriber sites.

An SD-WAN Service operates over one or more Underlay Connectivity Services. Since the SD-WAN service can use multiple disparate Underlay Connectivity Services, it can offer more differentiated service delivery capabilities than connectivity services based on a single transport facility.

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

SD-WAN benefits can be manifested in the ability to adjust aspects of the service in near real time to meet business needs. This is done by the Subscriber by specifying desired behaviors at the level of familiar business concepts, such as applications and locations and by the Service Provider by monitoring the performance of the service and modifying how packets in each Application Flow are forwarded based on the assignment of policy and the real-time telemetry from the underlying network components.

This document defines Service Attributes that describe the externally visible behavior and operation of an SD-WAN Service as experienced by the Subscriber and that form the basis of the agreement between the buyer of the service (the SD-WAN Subscriber) and the seller (the SD-WAN Service Provider). It describes the behavior from the viewpoint of the Subscriber Network and therefore all requirements are on the Service Provider.

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

5.1 Document Scope

This document provides definition and description of:

- SD-WAN Service Components
- SD-WAN Service functionality as viewed by the Subscriber
- Service Attributes for SD-WAN Virtual Connection (SWVC), SWVC End Point, and SD-WAN UNI
- Policies, the Policy Criteria that compose them, and required behavior for a base set of Policy Criteria
- Application Flows, the Application Flow Criteria that describe their characteristics, and a base set of required Application Flow Criteria
- The SD-WAN UNI and details of Subscriber connection to the SD-WAN Service

This document does not include any normative[1] information relating to:

- Orchestration of SD-WAN Services
- Management of SD-WAN Services
- LSO APIs
- Service Attributes or Policies related to Performance metric definitions or objectives for packet delay and packet loss service performance. There is a single performance objective identified in the document—Service Uptime.
- Service Attributes related to Underlay Connectivity Services and Tunnel Virtual Connections
- Service Attributes or Policies related to Application Flow priorities
- Service Attributes related to the logical topology of an SD-WAN Service
- IP Forwarding paradigms other than longest prefix match-based forwarding
- Details of Underlay Connectivity Service inclusion into an SD-WAN Service. The SD-WAN Service, as described in this document, assumes that appropriate Underlay Connectivity Services have been integrated into the SD-WAN infrastructure without details about the organization that owns a particular Underlay Connectivity Service and the business relationships associated with its inclusion.
- 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 other than at an SD-WAN UNI

5.2 Characteristics of an SD-WAN Service

A MEF SD-WAN Service has the following characteristics:

- The Subscriber connects to the 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[2].
- Ingress IP Packets at the UNI are segregated into Application Flows that can be based on the IP Packet data as well as the layer 2, 3, and 4 networking headers.
- The SD-WAN Service supports 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.
- SD-WAN Services offer encryption between SD-WAN Edges.
- Service quality objectives are based on the Policy applied to each Application Flow.
- Application Flows can be blocked/discarded 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 Group share a single bandwidth commitment and limit.

[1] In various sections of the document there may be informative text referring to some of these items.

[2] Layer 2 SD-WAN Services are out of scope for this document but could be covered in a future version of this standard or in another MEF standard.

- Managed SD-WAN Services typically provide a Subscriber web portal and/or API with a dashboard of network health and performance and application information.
- In a co-managed SD-WAN Service (management of the service is split between the Subscriber and the Service Provider), the portal and/or API can enable the Subscriber to modify aspects of the SD-WAN service such as defining Application Flows and creating/modifying Application Flow Policies.
- SD-WAN Services align with the concepts of MEF LSO principles including Service Orchestration.

5.3 Organization of the Standard

The remainder of the document is organized as follows:

- Definitions, key concepts, and document conventions are detailed in section 6.
- An overview of Application Flows and Policies is provided in section 7.
- Service Attributes for the SD-WAN Virtual Connection (SWVC) are described in section 8.
- Service Attributes for the SD-WAN Virtual Connection End Point are described in section 9.
- Service Attributes for the SD-WAN UNI are described in section 10.

6 Key Concepts and Definitions

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

6.1 Service Attributes

MEF Services, such as SD-WAN, are 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; this is 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 provider of the service mandates a particular value.
- The Subscriber selects from a set of options specified by the provider.
- The Subscriber requests a particular value, and the 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 and also the rules and policies associated with 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.

6.2 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)

Several additional components are (or may be) visible to the Subscriber but are not described by SD-WAN Service Attributes. These include:

- Subscriber Network
- Service Provider Network
- Underlay Connectivity Service (UCS)
- Tunnel Virtual Connection (TVC)

Figure 1 shows the SD-WAN Service components.

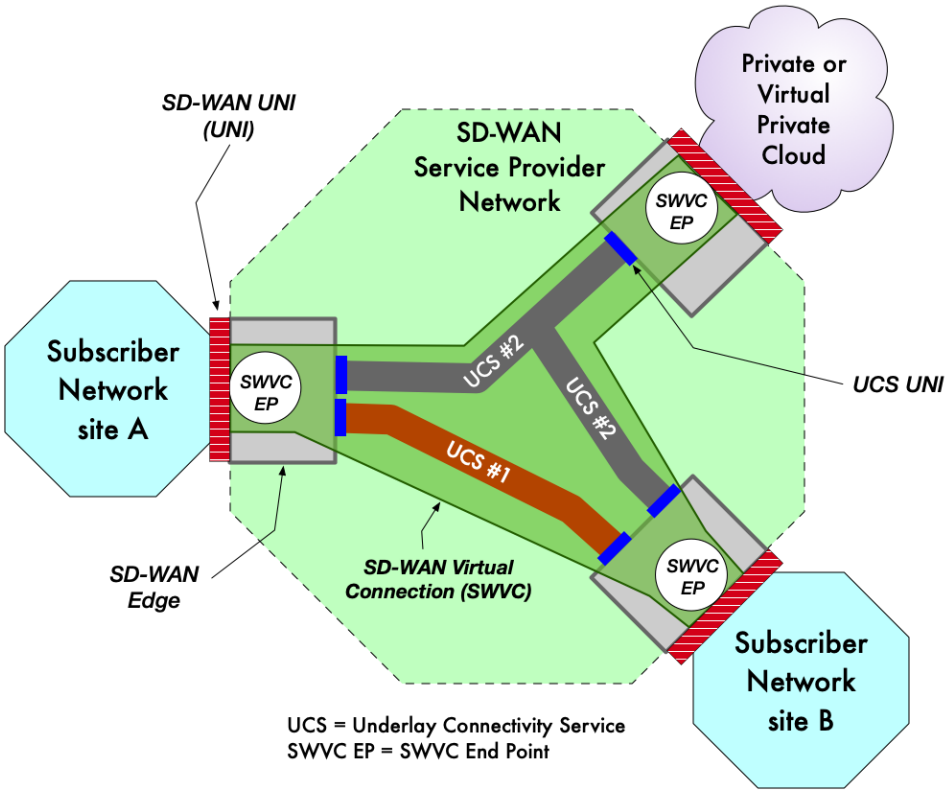

Figure 1 – Components of an SD-WAN Service

Note that in Figure 1 one of the Subscriber sites is connected to a Private or Virtual Private Cloud which may not be located at the Subscriber's physical location. This type of connection operates no differently in the SD-WAN Service than any of the other Subscriber Network locations—although for the cloud connection the SD-WAN Edge is usually a virtual network function (VNF), whereas for the other sites the SD-WAN Edge could be either a physical network function (PNF) or a VNF.

Two additional components, the Tunnel Virtual Connection (TVC) and the SD-WAN Edge, are also described since these components are used to describe the operation of the SD-WAN Service. These components are shown in Figure 2 (the SD-WAN Edge is also shown in Figure 1).

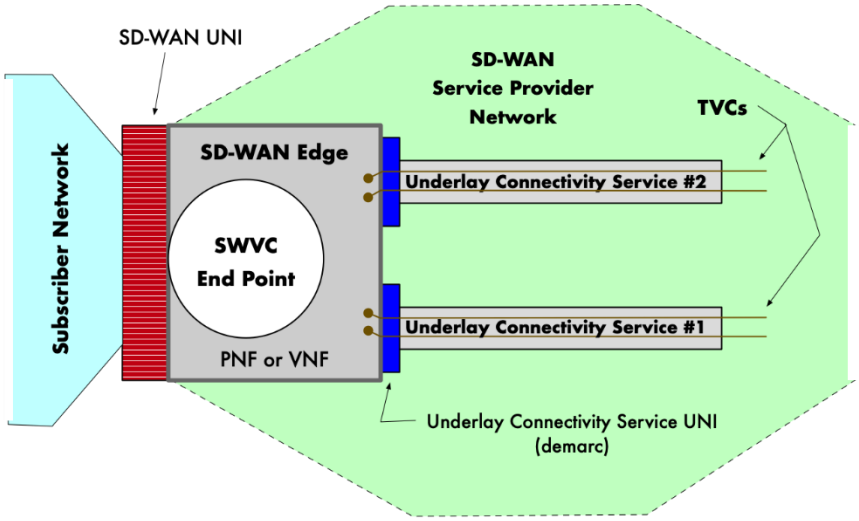

Figure 2 – SD-WAN Edge and TVCs

Figure 2 shows the SD-WAN Edge, a physical or virtual network function, which includes the SWVC End Point. The SD-WAN Edge has the UNI on one side (left) and the Underlay Connectivity Services on the other side (right).

Each Underlay Connectivity Service terminates at a service demarcation point, i.e., 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 [18]), an IP UNI (as defined in MEF 61.1 [21]), an L1 UNI (as defined in MEF 63 [22]), or analogous service demarcation for other non-MEF services.

Figure 2 also shows TVCs across the Underlay Connectivity Services. TVCs or Tunnel Virtual Connections are point-to-point paths across the Underlay Connectivity Services that define the logical forwarding topology of the SD-WAN Service. TVCs are described in section 6.7.

6.3 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 using the Service Attributes specified in this document and 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, a government department, etc. At its most basic, an SD-WAN Service provides connectivity for IP Packets between different parts of the Subscriber's network (different Subscriber or partner physical locations or private/virtual private clouds) or between the Subscriber's network and the public Internet using Internet Breakout (described in section 6.9).

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.

6.4 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 6.5). The basic unit of transport at the SD-WAN UNI is the 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 reference 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 SD-WAN 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:

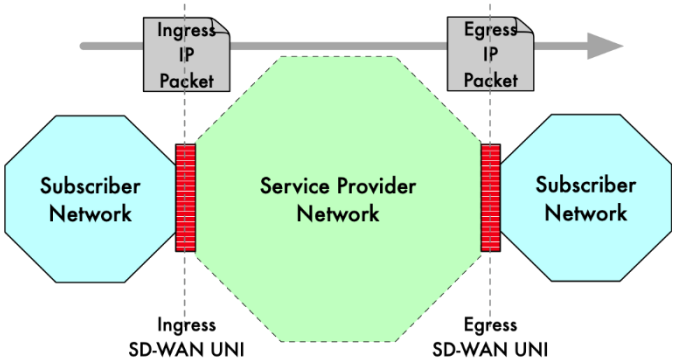

Figure 3 – Ingress and Egress

Terminology warning: Since SD-WAN is an overlay 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.

6.5 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 (such as a partner, cloud provider, etc.) that is connected to the Service Provider at two or more UNIs and accesses the SD-WAN Service.

The Service Provider Network represents the set of components and logical constructs used by the Service Provider in order to provide an SD-WAN Service. It includes SD-WAN Edges, Underlay Connectivity Services, Tunnel Virtual Connections, and a number of 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 6.6) 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.[3]

6.6 Underlay Connectivity Service

SD-WAN Services operate over Underlay Connectivity Services (UCS). Underlay Connectivity Services are network service offerings that provide connectivity between the Subscriber sites.

Underlay Connectivity Services can include a variety of services including (but not limited to) Ethernet Services (as defined in MEF 6.2 [18]), IP Services (as defined in MEF 61.1 [21]), L1 Connectivity Services (as defined in MEF 63 [22]), and public Internet Services. Access to these Underlay Connectivity Services can be via a variety of networking technologies, such as DSL, HFC, LTE, fiber, WiFi, Ethernet, and the transport can be based on Ethernet switching, IP Routing, MPLS, or other technologies.

Underlay Connectivity Services have several characteristics that are relevant to the Policies that determine the forwarding of Application Flows within the SD-WAN Service.[4]

[3] This case is not precluded in this document nor is it explicitly discussed. Details for supporting Underlay Connectivity Services that are provided by the Subscriber are not in scope for this document.

[4] Service Attributes for Underlay Connectivity Services are out of scope for this version of the specification. It is expected that a future version of the document will incorporate Service Attributes that define SD-WAN Edge connectivity to the Underlay Connectivity Services.

- An Underlay Connectivity Service is *Public* or *Private*. The primary distinction is whether the Underlay Connectivity Service is carried (in whole or in part) over public Internet Services.
- 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 100Mbps. 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.
- The Service Provider and Subscriber can agree that an Underlay Connectivity Service is designated as a *Backup* UCS at an SD-WAN Edge.
- Underlay Connectivity Services have bandwidth limitations.
- Underlay Connectivity Services have performance characteristics, e.g., 1% packet loss or 50ms packet latency and Performance Objectives usually specified in a Service Level Specification.

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 and an IPsec tunnel over the public Internet) 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 Public Internet). Underlay Connectivity Services arranged independently by the Subscriber can also be used by the SD-WAN Service. How the Subscriber communicates the details of such Underlay Connectivity Services to the SD-WAN Service Provider in this case, and the division of responsibility for such services between the Subscriber and the SD-WAN Service Provider are outside the scope of this document.

6.7 Tunnel Virtual Connection (TVC)

An SD-WAN Service Provider typically builds point-to-point paths called Tunnel Virtual Connections (TVCs) across the various Underlay Connectivity Services that compose an SD-WAN Service. Each TVC is built over a single Underlay Connectivity Service and has a well-defined set of characteristics, many of which are inherited from the Underlay Connectivity Service. One of the important functions of the SD-WAN Edge is to select a TVC over which to forward each ingress IP Packet.

TVCs are internal to the Service implementation and therefore do not have Service Attributes. However, TVCs play an important part of the packet forwarding function in the SD-WAN Edge, so a brief discussion is warranted.

Each TVC is built over an Underlay Connectivity Service and has characteristics that are mostly inherited from the Underlay Connectivity Service. Characteristics of a TVC include:

- A TVC is *Public* or *Private* based on the Underlay Connectivity Service that it is built on.
- A TVC has a charge model of *fixed-rate* or *usage-based* that reflects the Underlay Connectivity Service that it is built on.
- A TVC can be *encrypted* or *unencrypted.*

- A TVC has performance and bandwidth constraints and behaviors that derive from the Underlay Connectivity Service that it is built on.

Also, by building point-to-point TVCs, a Service Provider creates a virtual topology that can be different from the physical topology of the Underlay Connectivity Service. For example, if one of the Underlay Connectivity Services is an EP-LAN service connecting all of the SD-WAN Edges, but the Service Provider only builds TVCs from the Headquarters site to each remote site (and not between the remote sites) then the SD-WAN Service is, effectively, a hub and spoke even though the Underlay Connectivity Service provides a full mesh.

6.8 SD-WAN Virtual Connection and SWVC End Point

An SD-WAN Service is formed of an SD-WAN Virtual Connection (SWVC) that links together SD-WAN Virtual Connection (SWVC) End Points located at UNIs. The SWVC defines the logical connectivity of the SD-WAN Service as viewed by the Subscriber.

An SWVC End Point is the logical function that associates Ingress IP Packets with Application Flows, and applies a Policy to each Ingress IP Packet in order to make an appropriate forwarding decision.

6.9 Internet Breakout

When one or more of the Underlay Connectivity Services in an SD-WAN Service is an Internet Service, some Application Flows can be forwarded directly to the Internet rather than delivered to another SD-WAN UNI. This capability is called Internet Breakout and it is assigned to an Application Flow by Policy (see section 8.5.4). The most common case is for the Application Flow to be forwarded to an Internet UCS that is connected to the SD-WAN Edge where the Ingress UNI (for the IP Packet) is located. This is called Local Internet Breakout.

An example of Local Internet Breakout is shown in Figure 4. An ingress IP Packet at site B is forwarded across the UCS UNI for UCS #1 (the Internet), but instead of being sent over one of the TVCs, it is forwarded directly to an Internet-connected destination.

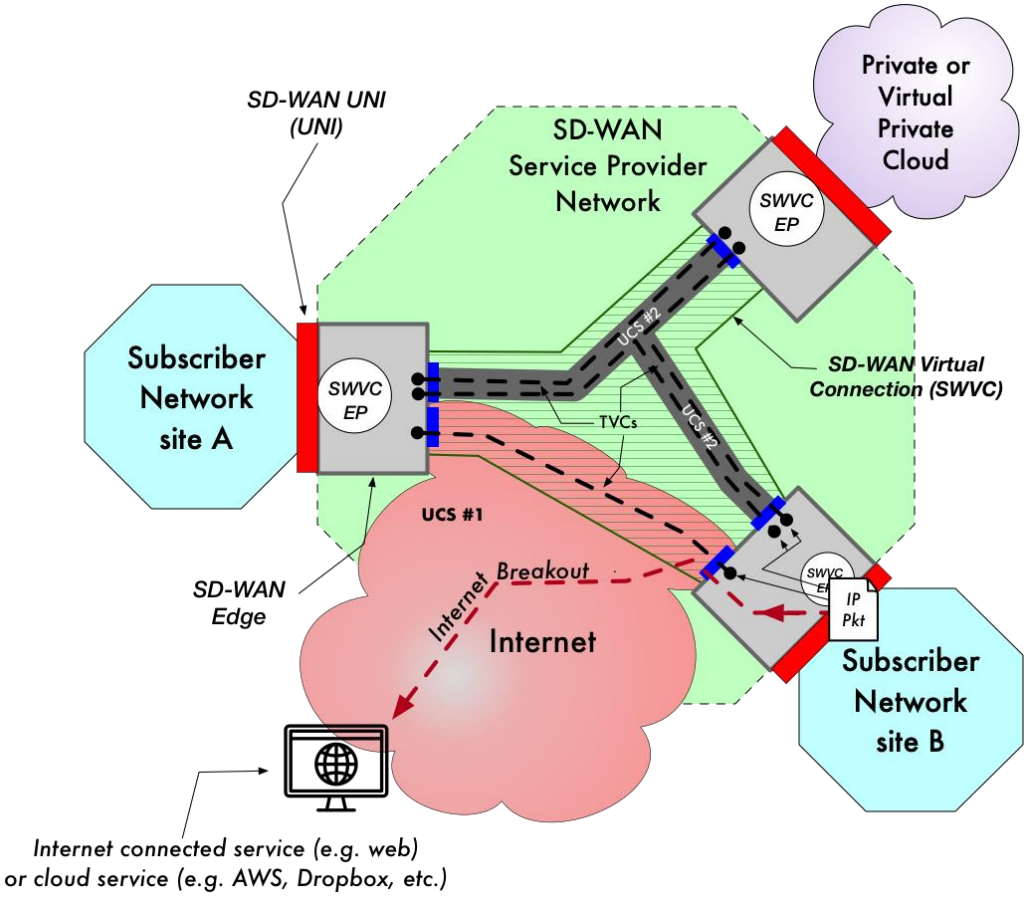

Figure 4 – Local Internet Breakout

If an Application Flow is assigned a Policy that indicates Internet Breakout and access to the Internet is not available at the SD-WAN Edge containing the Ingress UNI for the IP Packet, the Service Provider may deliver the packet over a TVC to another SD-WAN Edge for "breakout" to the Internet, but this is outside the scope of this document.

A UCS, such as an Internet UCS, is a service with a subscriber and a provider, and it is likely that there are service parameters that are agreed on by those parties, but that service agreement is separate from the SD-WAN Service agreement. Therefore, there is no need for the SD-WAN Subscriber and the SD-WAN Service Provider to agree on any SD-WAN Service Attribute values for the Internet Access Service (beyond the Application Flow recognition and Policy assignment). However, there are Internet Service parameters that need to be exchanged between the SD-WAN Subscriber and the SD-WAN Service Provider such as:

- Bandwidth
- Availability of NAT/PAT functionality
- IP Addressing

6.10 SD-WAN Edge

The SD-WAN Edge is the network function (physical or virtual) at the Service Provider side of the UNI reference point. It is part of the Service Provider Network, but it is commonly located at the Customer Premises when it is a physical network function. It is situated between the SD-WAN UNI, 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 UNI; 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 on over the SD-WAN UNI if appropriate. The SD-WAN Edge thus implements all of the data plane functionality of the SD-WAN service that is not provided by a UCS. This includes routing functionality and the functionality associated with implementing the SWVC End Point.

Note that the SD-WAN Edge may also implement functionality that facilitates connection to the Underlay Connectivity Services. These functions are out of scope for this specification.

6.11 SD-WAN Services Framework

An SD-WAN Service is an application-aware, policy-driven connectivity service, offered by a Service Provider, that optimizes transport of IP Packets over multiple underlay networks.

A complete MEF SD-WAN Service consists of:

- Exactly one SWVC with a corresponding set of SWVC Service Attributes (see section 8).
- Two or more UNIs where the Subscriber accesses the Service, each with a corresponding set of UNI Service Attributes (see section 10).
- 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 9).

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

6.12 SD-WAN IP Packet Delivery

An SD-WAN Service delivers IP Packets between Subscriber Network locations. In that sense it shares many attributes with a MEF IP Service (as described in MEF 61.1, *IP Service Attributes* [21]). Therefore, many of the sections of this document are derived from MEF 61.1.[5]

Since SD-WAN is intended to provide simplified connectivity options, only a selected set of Service Attributes are integrated from MEF 61.1. Conversely, since SD-WAN Services are based on Application Flows and Policies, there are a number of 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

[5] This is to ensure the greatest level of commonality between the two specifications as well as for expediency.

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 L3 (IP) Virtual Private Routed Network for a Subscriber. This section describes the basic IP forwarding paradigm for an 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.

6.12.1 IP Packet Forwarding

The basic forwarding paradigm for an SD-WAN Service is a Virtual Private Routed Network (VPRN) as described in RFC 2764 [9]. As a VPRN, the SD-WAN Service relies on destination-based IP forwarding (usually 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 such as:

- Source IP address
- Layer 4-based criteria such as TCP port number
- Layer 7 Application Flows

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. Details of this are out of scope for this version of the specification.

[R3] The Service Provider **MUST NOT** deliver an ingress IP Packet to a UNI where the destination address is not reachable, based on longest prefix matching.

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

6.12.2 IP Packet Transparency

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

[R4] If an Ingress IPv4 Data Packet is mapped to an SWVC and delivered as a Egress IPv4 Data Packet, and the packet has not been fragmented as described in RFC 791 [5], the Egress IPv4 Data Packet **MUST** be identical to the Ingress IPv4 Data Packet except that the following fields in the IPv4 header can be changed:

- The TTL field (RFC 791 [5])
- The DS (RFC 3260 [11]) and ECN (RFC 3168 [10]) 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

[R5] If an Ingress IPv4 Data 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 Data Packets **MUST** be such that reassembly as described in RFC 791 [5] results in an IP Packet that is identical to the Ingress IPv4 Data Packet except that the following fields in the IPv4 header can be changed:

- The TTL field (RFC 791 [5])
- The DS (RFC 3260 [11]) and ECN (RFC 3168 [10]) 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

[R6] If an Ingress IPv6 Data Packet is mapped to an SWVC and delivered as an Egress IPv6 Data Packet, the Egress IPv6 Data Packet **MUST** be identical to the Ingress IPv6 Data Packet except that the following fields in the IPv6 header can be changed:

- The Hop Limit field (RFC 8200 **[**17])
- The DS (RFC 3260 [11]) and ECN (RFC 3168 [10]) 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 [17])
- 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.

6.13 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, very long Identifier Strings should be avoided.[6]

The allowable character set is chosen to contain printable characters since the Identifier String is used in human interfaces.[7]

[R7] An Identifier String **MUST** be a string consisting of UTF-8 characters in the range of 32–126 (0x20 to 0x7e), inclusive.

[6] MEF 61.1 [21] limits these strings to 53 octets for MEF IP Services.

[7] The definition only includes printable Latin characters. Inclusion of other printable characters can be considered in a future version of the document.

7 Application Flows and Policies

Forwarding of IP Packets across different Underlay Connectivity Services with different attributes based on Policies applied to Application Flows is one of the defining characteristics of SD-WAN Services.

As part of the SD-WAN Service, the Subscriber and the Service Provider agree on the Application Flows that are identified at the SD-WAN Edges. For each of the agreed-on Application Flows, a Policy (list of Policy Criteria) is assigned, which defines how IP Packets in the Application Flow are handled.

An Application Flow can be described by a broad set of characteristics of the packet stream that can be identified at the UNI[8], including standard layer 2 and layer 3 fields such as addresses, ports, and protocols. In addition, many SD-WAN implementations can perform deep packet inspection (DPI) up through layer 7. Therefore:

- 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 [13]” or, conversely,
- 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 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.

Forwarding of an Application Flow is based both on the Policy assigned to the flow and IP forwarding requirements, which together determine the best TVC for forwarding each IP Packet in the Application Flow. Appendix A includes an example of how the implementation of this process could be structured.

7.1 Application Flows

The SWVC List of Application Flows Service Attribute (section 8.7) describes the list of Application Flows that can be forwarded by the SD-WAN and the criteria used to identify them.

The Service Attribute allows detailed matching criteria for each Application Flow to be specified. A small set of required criteria are provided in this document (in section 8.7), and the Service Provider and Subscriber can agree on additional criteria based on the capabilities of the deployed equipment and their business requirements. In many cases, the Service Provider provides a catalog of “built-in” or “pre-defined” Application Flows specified using these criteria, and the Subscriber can select from the catalog. In this case, the Service Provider's catalog needs to include an explicit description of what is, and, if appropriate, what is not included in each of its standard Application Flow definitions, as this, combined with the set selected by the Subscriber, constitutes the value of the Service Attribute.

Each Application Flow can be a member of an Application Flow Group (The SWVC List of Application Flow Groups Service Attribute is described in section 8.6). There are two purposes for grouping Application Flows. First, a Policy can be applied to the Group at an SWVC End Point that then applies to all members of the Application Flow Group. For example, there might be three Application Flows, *apple*, *banana*, and

[8] The techniques and technologies used to identify the flows are outside the scope of this specification.

pear in the Application Group *fruits*. A Policy can be assigned to the group *fruits*, which becomes the Policy for the three Application Flows. Each Application Flow in the group can nonetheless have an explicit Policy assignment that supersedes the group Policy.

The second purpose of an Application Flow Group is to allow a single bandwidth commitment and limit to be applied to a group of Application Flows. Application Flows that are members of an Application Flow Group to which a Policy has been assigned are treated as single aggregated flow of IP Packets that are subject to the bandwidth commitment and limit specified in the Application Flow Group's Policy (see section 8.5.7).

7.2 Policies

A Policy is a list of Policy Criteria (listed in section 8.5). Policies are assigned to Application Flows and Application Flow Groups at each SWVC End Point (see section 9.3). A Policy provides details on how Ingress[9] IP Packets associated with each Application Flow (or the members of an Application Flow Group) should be handled by the SD-WAN Service, providing rules concerning forwarding, security, rate limits, and others.

As noted in section 7.1, when a Policy is assigned to an Application Flow Group at an SWVC End Point, it applies to all Application Flows in the group unless superseded by an explicit Policy assignment to the Application Flow (but note that treatment of the BANDWIDTH Policy Criterion as described in section 8.5.7 operates a bit differently).

For example, if there is an Application Flow Group called *fruits* containing Application Flows *banana*, *apple*, and *pear*, and a Policy *jam* is assigned to this Application Flow Group at an SWVC End Point, then the three listed flows will be forwarded over the SD-WAN using Policy *jam*. However, if at the SWVC End Point the Policy *jelly* is assigned to Application Flow *apple*, then *banana* and *pear* will be forwarded using Policy *jam*, and *apple* will be forwarded using Policy *jelly*. This behavior is formally defined in [R54].

7.3 Examples of Policies and Application Flows

In Figure 5 the SD-WAN Service has three Subscriber sites (A, B, and C). The SWVC has three Applications Flows, *apple*, *banana*, and *vegetable* (via the SWVC List of Application Flows Service Attribute in section 8.7). *Apple* and *banana* are in Application Flow Group *fruit*. Application Flow *vegetable* is not in any Application Flow Group.

The SWVC also has two Policies, *fast* and *faster* (via the SWVC List of Policies Service Attribute in section 8.5). All SWVCs have a reserved Policy named *block*.

[9] Policies only apply to Ingress IP Packets. Packets that arrive at the SD-WAN Edge from other sites are forwarded to the UNI regardless of Policies that are associated with their Application Flow.

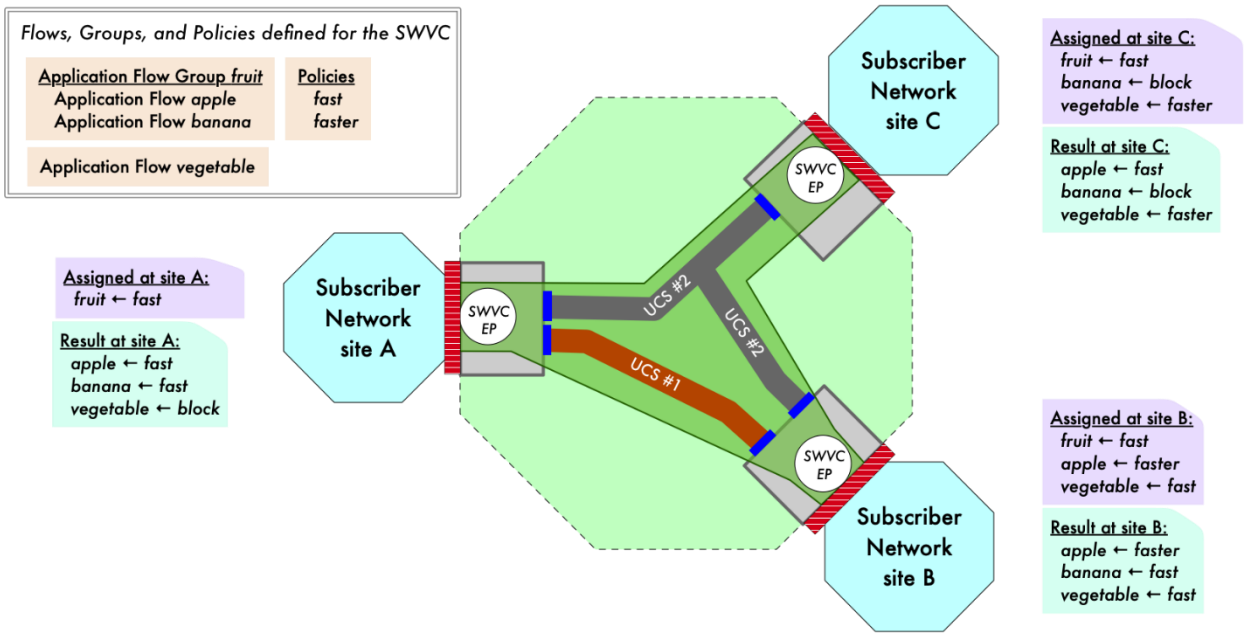

Figure 5 – Examples of Application Flows and Policies

At site A, using the SWVC End Point Policy Map Service Attribute (see section 9.3), the Policy *fast* is assigned to Application Flow Group *fruit*. This means that all members of that Group (i.e., *apple* and *banana*) are forwarded based on Policy *fast*. Since no Policy is mapped to Application Flow *vegetable* at site A, Ingress IP Packets in this Application Flow are not forwarded (they are blocked/blacklisted).

At site B, Policy *fast* is assigned to Application Flow Group *fruit*. But, here, Policy *faster* is assigned to Application Flow *apple*. So, at site B, *apple* is forward based on Policy *faster* and *banana* is forwarded based on Policy *fast*, as is Application Flow *vegetable*.

At site C, Policy *fast* is assigned to Application Flow Group *fruit*. But here, the reserved Policy *block* is assigned to *banana*. So, at site C, *apple* is forwarded based on Policy *fast*, but *banana* is not forwarded. Application Flow *vegetable* is forwarded based on Policy *faster*.

8 SD-WAN Virtual Connection (SWVC) Service Attributes

This section contains Service Attributes that apply to an SD-WAN Virtual Connection as a whole. 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 End Point List	The SWVC End Points that are connected by the SWVC	List of SWVC End Point Identifiers
SWVC Service Uptime Objective Service Attribute	The objective for Service Uptime for the SD-WAN Service during a Performance Evaluation Interval	3-tuple <ts, T, Û> where ts is a date and time, T is a duration, and Û is a percentage between 0 and 100%
SWVC Reserved Prefixes	IP Prefixes reserved for use by the SP	*None* or list of IP Prefixes
SWVC List of Policies	A list of the Policies that can be applied to Application Flows carried by the SWVC	List of 2-tuples <Policy Name, List of Policy Criteria n-tuples>
SWVC List of Application Flow Groups	A list of the Application Flow Groups that Application Flows can be members of.	List of 2-tuples <Application Flow Group Name, Application Flow Group Policy>
SWVC List of Application Flows	A list of the Application Flows that are recognized by the SD-WAN Service	List of 3-tuples <Application Flow Name, List of Application Flow Criteria, Application Flow Group Name>

Table 2 – Summary of SWVC Service Attributes

8.1 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.

[R8] The value of the SWVC Identifier Service Attribute **MUST** be an Identifier String.

[R9] The value of the SWVC Identifier Service Attribute **MUST** be unique across all SWVC Identifiers for SWVCs (SD-WAN Services) purchased by the Subscriber from the Service Provider.

[R9] requires that all SWVCs purchased by the Subscriber from a particular Service Provider have different SWVC Identifiers. For example, if the Subscriber has SWVC with identifier *CorpIntranet* with Service Provider X, it cannot have another SWVC with that identifier with Service Provider X. The Subscriber can have an SWVC with a different Service Provider with identifier *CorpIntranet* (although that would likely

be a poor choice). Conversely, the Service Provider can agree to use the identifier *CorpIntranet* for three different SWVCs sold to three different Subscribers.

8.2 SWVC End Point List Service Attribute

The value of the SWVC End Point List Service Attribute is a list of SWVC End Point Identifier Service Attribute values (section 9.1). The list contains one SWVC End Point Identifier value for each SWVC End Point connected by the SWVC.

[R10] The value of the SWVC End Point List Service Attribute **MUST** have at least two entries.

[R11] An SWVC End Point Identifier **MUST NOT** appear in the value SWVC End Point List Service Attribute more than once.

[R12] An SWVC **MUST NOT** have more than one SWVC End Point at a given UNI.

[R13] 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.

8.3 SWVC Service Uptime Objective Service Attribute

Service Uptime is the proportion of time, during a given time period T_k, that the service is working from the perspective of the Subscriber, excluding any pre-agreed exceptions, for example, maintenance intervals. The value of this Service Attribute is a 3-tuple $\langle ts, T, \widehat{U} \rangle$ 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 for T, corresponding to a calendar month, e.g., from midnight on the 10th of one month up to but not including midnight the 10th of the following month.
- $\widehat{U}$ is the objective for Service Uptime expressed as a percentage.

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 [R14].

[R14] 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%>

[R15] The SWVC Service Uptime Objective for a given time interval, T_k, **MUST** be considered met 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.

8.4 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 their own network or for distribution to the Subscriber via DHCP or SLAAC. Addresses in these prefixes may be exposed to the Subscriber, for example for diagnostics purposes. 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.

[R16] The Service Provider **MUST** identify IP Prefixes that are reserved in the SWVC and cannot be assigned by the Subscriber.

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 automatically reserved. See sections 10.4 and 10.5.

8.5 SWVC List of Policies Service Attribute

Associated with each SWVC is a list of named Policies that can be applied to Application Flows and Application Flow Groups at SWVC End Points (see section 9.3).

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"*.
- *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 3, or a Service Provider-defined Policy Criterion name.
  - *PCparam* is a non-empty list of parameter values specific to the Policy Criterion specified in *PCName*.

[R17] A Policy name, *polName*, in the value of the SWVC List of Policies Service Attribute **MUST** appear, at most, once.

[R18] 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.

[D1] The Policy Criteria listed in Table 3 **SHOULD** be supported for SWVCs.

PCname	Description	Values
ENCRYPTION	Indicates whether or not the Application Flow requires encryption.	*Yes, Either*
PUBLIC-PRIVATE	Indicates whether the Application Flow can traverse Public or Private Underlay Connectivity Services (or both).	*Private-only, Either*
INTERNET-BREAKOUT	Indicates whether the Application Flow should be forwarded to an Internet destination.	*Yes, No*
BILLING-METHOD	Indicates whether the Application Flow can be sent over an Underlay Connectivity Service that has usage-based or flat-rate billing.	*Flat-Rate-Only, Either*
BACKUP	Indicates whether this Application Flow can use a TVC designated as "backup".	*Yes, No*
BANDWIDTH	Specifies a rate limit on the Application Flow.	*<commit, max>*

Table 3 – Policy Criteria

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

[R19] If the Service Provider defines its own Policy Criteria, the *PCName*s chosen by the Service Provider **MUST NOT** be the same as any of the *PCName*s in Table 3.

[R20] 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:

- The *PCName*
- The possible values for the Policy Criterion
- The behavior associated with each value
- The behavior of each value when used with INTERNET-BREAKOUT
- Any interactions that the Policy Criterion has with other Policy Criteria

An example of a value for this Service Attribute is shown below:

```
[
<polA, [<ENCRYPTION, Yes>
       <INTERNET-BREAKOUT, No>
       <PUBLIC-PRIVATE, Either>
       <BILLING-METHOD, Flat-rate-only>
```

```
        <BACKUP, No>
        <BANDWIDTH, 20Mbps, 50Mbps>]>

<polB, [<ENCRYPTION, Yes>

        <INTERNET-BREAKOUT, No>
        <PUBLIC-PRIVATE, Private-only>
        <BILLING-METHOD, Flat-rate-only>

        <BACKUP, Yes>
        <BANDWIDTH, 50Mbps, none>]>
]
```

8.5.1 Policy Criteria specification and interaction

Each Service Provider supports a set of Policy Criteria that can include both criteria from the list in Table 3 as well as other criteria defined by the Service Provider (see [R19] and [R20]). 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.

[R21] Every Policy agreed to between the Subscriber and the Service Provider for a given SD-WAN Service **MUST** include values for the same set of Policy Criteria.

[R22] For an Ingress IP Packet mapped to a given Application Flow, if the Service Provider cannot forward the packet to the egress UNI 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.

[R21] requires that every Policy in an SD-WAN Service has the same set of Policy Criteria. This ensures that all Policies are deterministic, i.e., it avoids the "don't know" situation. If, for example, the ENCRYPTION Policy Criterion were to be used in Policy A but not in Policy B, then when an IP Packet arrives for an Application Flow that has been assigned Policy B, there is no way to determine whether or not it has to be encrypted. There are no "default" values.

[R22] indicates that two conditions must be met for an IP Packet to be forwarded by the SD-WAN Service:

- A forwarding path exists — i.e., a UCS or sequence of UCS is available to carry the IP Packet to its destination UNI, and
- The forwarding path meets the Policy assigned to the Application Flow

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 these two 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.

It is possible that some Policy Criteria aren't relevant for a particular Policy. In that case the Policy Criterion has a value that indicates that it should not be used to determine how the associated Application Flow is forwarded (this value is usually *Either* or *Any*).

8.5.2 ENCRYPTION Policy Criterion

IP Packets forwarded over the SWVC can be encrypted. The ENCRYPTION Policy Criterion provides a mechanism to specify whether or not encryption is required. It can have the value *Yes* or *Either*.

[R23] If Policy Criterion ENCRYPTION=*Yes* is applied to an Application Flow, then the Application Flow **MUST** be encrypted before it is forwarded over the Underlay Connectivity Service.

[R23] means that encryption is applied by the SD-WAN Edge before packets are forwarded over the UCS UNI, and decryption is applied to packets received at the destination SD-WAN Edge. This is typically implemented by instantiating an encrypted TVC.[10]

[R24] If the Policy Criterion ENCRYPTION=*Either* is applied to an Application Flow, then this Policy Criterion **MUST NOT** be considered in the forwarding decision for the Application Flow.

8.5.3 PUBLIC-PRIVATE Policy Criterion

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

[R25] If the Policy Criterion PUBLIC-PRIVATE=*Private-Only* is applied to an Application Flow, then the Application Flow **MUST** be forwarded over Underlay Connectivity Services that do not traverse the public Internet.

[R26] If the Policy Criterion PUBLIC-PRIVATE=*Either* is applied to an Application Flow, then this Policy Criterion **MUST NOT** be considered in the forwarding decision for the Application Flow.

8.5.4 INTERNET-BREAKOUT Policy Criterion

The INTERNET-BREAKOUT Policy Criterion indicates whether the Application Flow should be forwarded directly to the Internet using Internet Breakout (see section 6.9). It can have the value *Yes* or *No*.

[R27] If the Policy Criterion INTERNET-BREAKOUT=*Yes* is applied to an Application Flow, the Application Flow **MUST** be forwarded to the Internet over an Internet UCS.

[10] Requirements related to the level and type of encryption are out of scope but may be addressed in a future version of the specification.

The Service Provider chooses an appropriate Internet UCS over which to forward the Application Flow. It is expected that, in most cases, this is a UCS that is directly connected at the SD-WAN Edge where the IP Packet crosses the Ingress UNI, i.e., Local Internet Breakout.

[R28] If the Policy Criterion INTERNET-BREAKOUT=*No* is applied to an Application Flow, the Application Flow, if it is not blocked or discarded for other reasons, **MUST** be forwarded into the SWVC and delivered to another SD-WAN End Point in the SWVC.

[R29] If the Policy Criterion INTERNET-BREAKOUT=*Yes* is applied to an Application Flow, all of the other Policy Criteria specified in Table 3, except BANDWIDTH, **MUST** be ignored for the Application Flow if it is forwarded to the Internet via Local Internet Breakout.

[R29] acknowledges that the other Policy Criteria (e.g., PUBLIC-PRIVATE and ENCRYPTION) are not relevant for Local Internet Breakout, except for BANDWIDTH. 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.

8.5.5 BILLING-METHOD 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* or *Either*.

[R30] If Policy Criterion BILLING-METHOD=*Flat-Rate-Only* is applied to an Application Flow, then the Application Flow **MUST** be forwarded over an Underlay Connectivity Service with flat-rate (i.e., time-based) charging.

[R31] If Policy Criterion BILLING-METHOD=*Either* is applied to an Application Flow, then this Policy Criterion **MUST NOT** be considered in the forwarding decision for the Application Flow.

This Policy Criterion does not include a *Usage-Only* option. Since flat-rate services are paid for whether they are used or not, it seems unlikely that a Subscriber would want to avoid using a flat-rate service if one were available and met the constraints imposed by the other Policy Criteria.

Also, this Policy Criterion provides a simplified model for how Underlay Connectivity Service charge models can be used. There are other possible models such as a threshold-based model where one type would be used up to a particular level of bandwidth and the other would be used beyond that. Alternative models and situations are beyond the scope of this document. Refer to MEF 74 [23] for examples of a broader range of billing options.

8.5.6 BACKUP Policy Criterion

As noted in section 6.6, a UCS can be designated as *Backup*. When there is at least one non-*Backup* UCS available at an SD-WAN Edge (availability of a UCS is described by [R22] and the explanatory text around it), Ingress IP Packets are not forwarded toward the egress UNI over a UCS that is designated as *Backup*. However, since *Backup* UCSs 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 *Yes* or *No*.

[R32] Application Flows **MUST NOT** be forwarded toward the destination egress UNI over a UCS that is designated as *Backup* if a non-*Backup* UCS to the destination egress UNI is available.

[R33] If the Policy Criterion BACKUP=*No* is assigned to an Application Flow, then the Application Flow **MUST** be discarded if only *Backup* UCSs to the destination egress UNI are available.

Note that Application Flows that have BACKUP=*yes* will likely be more resilient than those with BACKUP=*no*.

8.5.7 BANDWIDTH Policy Criterion

The BANDWIDTH Policy Criterion specifies a rate (bandwidth) commitment and a rate limit on an Application Flow or Application Flow Group.

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

- *commit* is the average information rate in bits per second that is committed to the Application Flow or *none*
- *max* is a limit on the average information rate in bits per second that can be used by the Application Flow or *none*

In both cases, the average information rate is calculated over a time interval determined by the Service Provider and referred to in the following requirements as the "averaging interval".

Specifying *commit=none* is equivalent to *commit*=0, i.e., there is no bandwidth committed to the Application Flow. Specifying *max=none* is equivalent to *max*=∞, i.e., there is no maximum imposed on the Application Flow (up to the limits imposed by the UNI speed and Underlay Connectivity Service capacity).

[R34] In the value of the BANDWIDTH Policy Criterion, the *max* element **MUST** be greater than or equal to the *commit* element.

There is an expectation that the Subscriber and the Service Provider have agreed on sufficient Underlay Connectivity Service capacity so that the bandwidth committed to all Application Flows can be met. How the average information rates are determined and the behavior of the rate limiting function are described below.

The BANDWIDTH Policy Criterion when applied to an Application Flow Group operates differently than other Policy Criteria. For all other Policy Criteria applied to an Application Flow Group, the Policy Criteria are simply applied to the members of the group (that don't have their own explicit Policy assignment). For the BANDWIDTH Policy Criterion, the specified bandwidth limits apply to all members of the group (that don't have their own explicit Policy assignment) in the aggregate. In other words, all of those group members share the bandwidth limits specified in the Policy and are treated as a single flow for the purpose of determining the bandwidth. The remainder of this section uses the term Application Flow to refer to both a single Application Flow and an aggregated Application Flow Group "flow".

The effect of metering a stream of IP Packets – that is, comparing the actual sequence of IP Packets to the description in terms of the BANDWIDTH Policy Criterion parameters – is to declare each packet 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 constrain the implementation of the bandwidth limiting by the Service Provider, nor does it constrain where the bandwidth limiting is implemented, i.e., the metering point.

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

[R35] The average information rate for IP Packets in an Application Flow that are declared conformant **MUST** be at least the lower of the average information rate for IP Packets that pass the metering point in Application Flow over a time interval equal to the averaging interval and *commit*.

[O2] IP Packets in an Application Flow **MAY** be declared non-conformant in order to ensure that the average information rate for such packets over any time interval equal to the averaging interval that are declared conformant is, at most, *max*.

[O3] IP Packets in an Application Flow **MAY** be declared non-conformant in order to ensure that the average information rate for IP Packets across all Application Flows at a UNI does not exceed the available capacity of the Underlay Connectivity Services at that UNI.

[O4] 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 in order to meet all of the Policies exceeds the capacity of that Underlay Connectivity Service, IP Packets in the affected Application Flows **MAY** be declared non-conformant.

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 Providers discretion which packets to discard, so long as each Application Flow still gets its committed 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.

[R36] An IP Packet in an Application Flow **MUST** be declared conformant unless it is declared non-conformant by a condition specified in [O2], [O3], or [O4].

[R37] IP Packets that are declared non-conformant **MUST** be discarded.

8.6 SWVC List of Application Flow Groups Service Attribute

An Application Flow (see sections 7 and 8.7) can be a member of an Application Flow Group. Application Flow Groups provide the mechanism for associating a Policy with multiple Application Flows at an SWVC End Point. If a Policy is associated with an Application Flow Group at an SWVC End Point, then that Policy is associated with all Application Flows that are members of the group. (Each Application Flow can replace the Group Policy association with its own Policy association at an SWVC Endpoint.) Application Flow Groups also provide a mechanism for the members to share bandwidth commitments and limits (see section 8.5.7).

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

For example, Application Flows “Banana”, “Pear” and “Grape” can all be members of the Application Flow Group “FruitService”. Group membership is indicated in the definition of each Application Flow (see section 8.7).

[R38] Each Application Flow Group name in the value of the SWVC List of Application Flow Groups Service Attribute **MUST** be an Identifier String.

[R39] Each Application Flow Group name in the value of the SWVC List of Application Flow Groups Service Attribute **MUST** appear, at most, once.

[R40] An Application Flow Group name in the value of the SWVC List of Application Flow Groups Service Attribute **MUST NOT** have the value *none*.

8.7 SWVC List of Application Flows Service Attribute

The SWVC List of Application Flows 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 $\langle appName, appCL, appGroup \rangle$ where:

- *appName* is an Identifier String that is used to refer to the Application Flow.

- *appCL* is a non-empty list of Application Flow Criteria 2-tuples of the form $\langle ACName, ACValue \rangle$ where:
  - *ACName* is an Identifier String containing an Application Flow Criterion Name from Table 4 or other Service Provider Application Flow Criterion Name.
  - *ACValue* contains the parameter values specific to the Application Flow Criterion specified in *ACName*. If there are no parameter values, *ACValue* is *none*.
- *appGroup* is an Application Flow Group name contained in the value of the SWVC List of Application Flow Groups Service Attribute or *none* if the Application Flow is not a member of an Application Flow Group.

[R41] Each Application Flow name, *appName*, in the value of the SWVC List of Application Flows Service Attribute **MUST** appear, at most, once.

[R42] Each Application Flow name, *appName*, in the value of the SWVC List of Application Flows Service Attribute **MUST NOT** be the same as an Application Flow Group Name in the value of the SWVC List of Application Flow Groups Service Attribute.

[R43] If the *appCL* element in an entry of the SWVC List of Application Flows 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.

[R44] Each Ingress IP Packet **MUST** be assigned to the first Application Flow in the value of the SWVC List of Application Flows Service Attribute whose Application Flow Criteria it matches, if any.

[R45] Any Ingress IP Packet that cannot be associated with an Application Flow from the value of the List of Application Flows Service Attribute **MUST** be discarded.

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

[R43] indicates that the Application Flow is defined by the conjunction of a set of Application Flow Criteria. This doesn't allow for alternatives within an Application Flow. This is partially mitigated by the fact that many of the Criteria are ranges or lists of values. Also, the Application Flow Group can provide alternatives. For example, one Application Flow can have criteria X and Y, and a second Application Flow can have criteria X and W. If the two Application Flows are put into an Application Group, a common Policy can be applied to the Group and the two Applications can share bandwidth resources, so it appears (almost) like a single Application Flow defined as (X and Y) or (X and W).

[R46] Application Flow Criteria that can be used to describe Application Flows **MUST** include the Criteria listed in Table 4, except for APPID.

ACName	Layer	Match	Values for *ACValue*	Reference
ETHERTYPE	2	Ethertype	Integer in the range 0x0600 to 0xffff, e.g. 0x0800 for IPv4	802.3 [4]
CVLANS	2	C-VLAN ID List	Integer in the range 0 to 4094	802.1Q[3]
SAV4	3	IPv4 Source Address	IPv4 prefix	RFC 791 [5]
DAV4	3	IPv4 Destination Address	IPv4 prefix	RFC 791 [5]
SDAV4	3	IPv4 Source or Destination Address	IPv4 prefix	RFC 791 [5]
PROTV4	3	IPv4 Protocol List	List of integers in the range 0 to 255	IANA Protocol Numbers Registry [1]
SAV6	3	IPv6 Source Address	IPv6 prefix	RFC 8200 [17]
DAV6	3	IPv6 Destination Address	IPv6 prefix	RFC 8200 [17]
SDAV6	3	IPv6 Source or Destination Address	IPv6 prefix	RFC 8200 [17]
NEXT-HEADV6	3	IPv6 Next Header List	List of integers in the range 0 to 255	IANA Protocol Numbers Registry [1]
SPORT	4	TCP/UDP Source Port List	List of integers in the range 0 to 65535	IANA Service Name and Port Number Registry [2]
DPORT	4	TCP/UDP Destination Port List	List of integers in the range 0 to 65535	IANA Service Name and Port Number Registry [2]

SDPORT	4	TCP/UDP Source or Destination Port List	List of integers in the range 0 to 65535	IANA Service Name and Port Number Registry [2]
APPID	4 - 7	Application Identifier	List of arguments starting with the Application Identifier.	Custom Match
ANY	1 – 7	Match Any IP Packet	No arguments	

Table 4 – Required Application Flow Criteria

Table 4 includes all of the basic layer 2 through layer 4 fields that all implementations are expected to be able to match against Ingress IP Packets. The exception is the *APPID* Criterion. The *APPID* Policy Criterion provides the ability for the Service Provider to define and name both simple and complex matches. These can include *standard* matches available to all of the Service Provider's Subscribers from a catalog and/or *custom* matches developed by the Service Provider by agreement with a particular Subscriber.

APPID matches could be simple protocol matches (that could be accomplished with the other Criteria such as DPORT) such as "SSH" or "SNMP" or "RTP", but they can also support deeper inspection of packets such as "SNMP GET NEXT" or "HTTP POST" or "TWAMP [15] STOP-SESSION".

[R47] If the Service Provider defines an APPID (either a standard or a custom match), the description provided to the Subscriber **MUST** include the following information:

- The Application Identifier
- Addition Arguments Required (beyond the Identifier)
- Description of the operational logic of the match including the fields that are inspected, the values that they are matched against, and any additional logic associated with the match (e.g., dependencies).

Complex matches, for example, using deep packet inspection, often require inspection of several initial packets and may include heuristics to define the characteristics of the Application Flow. These details are included in the description of the matching logic required by [R47].

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 for value 5060 or 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 to be defined that includes all "unmatched" IP Packets and assign a Policy to that Application Flow. In general, if this Application Flow Criterion is used, it should be in the last Application Flow definition in the list, since no IP Packets are matched against subsequent Application Flow definitions.

[R48] If an entry in the value of the SWVC List of Application Flows Service Attribute includes the Application Flow Criterion ANY, that entry **MUST NOT** contain any other Application Flow Criteria.

Following is an example value for this Service Attribute with four Application Flows:

```
[
<Peach,  [<SAV4, 192.168.7.0/24>,<DPORT, [80,443,8080]>], round>
<VOIP,   [<APPID,"RTP">], none>
<Banana, [<DPORT, [80]>], long>
<Else,   [<ANY>], none>
]
```

In this example, Application Flow *Peach* includes packets from any 192.168.7.x address destined to port 80 or 443 or 8080 (and this flow is in the group *round*). Application Flow *VOIP* includes packets that are matched by the built in "RTP" flow match. Application Flow *Banana* is any packet to port 80 that is not matched by *Peach*, and this flow is in group *long*. At the end of the list is the Application Flow *Else*, which includes all IP Packets not matched by the other three.

In this example, it is important that *Banana* is after *Peach* because it matches a subset of *Peach*. If *Banana* were first, then port 80 packets would never be assigned to Application Flow *Peach*.

9 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 UNI	Identifies the UNI that the End Point is associated with	An SD-WAN UNI Identifier
SWVC End Point Policy Map	Maps Policies to Application Flows and Application Flow Groups	A list of 2-tuples <app,pol>

Table 5 – Summary of SWVC End Point Service Attributes

9.1 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.

[R49] The value of the SWVC End Point Identifier Service Attribute **MUST** be an Identifier String.

[R50] The value of the SWVC End Point Identifier Service Attribute **MUST** be unique among all SWVC End Point Identifiers in SWVCs purchased by the Subscriber from the Service Provider.

9.2 SWVC End Point UNI Service Attribute

The value of the SWVC End Point UNI Service Attribute is an SD-WAN UNI Identifier Service Attribute value per section 10.1, which serves to specify the UNI where the SWVC End Point is located. The SWVC End Point is said to be at this UNI.

9.3 SWVC End Point Policy Map

The SWVC End Point Policy Map specifies the Policies that are assigned to Application Flows and Application Flow Groups at the SWVC End Point. The value of the SWVC End Point Policy Map is a list of 2-tuples $\langle app, pol \rangle$ where:

- *app* is an Application Flow or Application Flow Group name
- *pol* is a Policy name

[R51] The *app* element in each entry in the value of the SWVC End Point Policy Map **MUST** be either:

- an Application Flow Group name from the value of the SWVC List of Application Flow Groups Service Attribute (see section 8.6), or,
- an Application Flow name from the value of the SWVC List of Application Flows Service Attribute (see section 8.7)

[R52] A specific value for the *app* element in the value of the SWVC End Point Policy Map **MUST** appear in, at most, one entry in the list.

[R53] The *pol* element in each entry in the value of the SWVC End Point Policy Map **MUST** be a Policy Name from the value of the SWVC List of Policies Service Attribute (see section 8.5)

In order for an Application Flow to be forwarded at an SWVC End Point, it must have an assigned Policy. This can happen in two ways:

- The Application Flow can be a member of an Application Flow Group that has an assigned Policy at the SWVC End Point, or,
- The Application Flow, itself, can have an assigned Policy at the SWVC End Point.

[R54] If an Application Flow and the Application Flow Group in which the Application Flow is a member are both assigned a Policy at an SWVC End Point, the Policy assigned to the Application Flow **MUST** be used for the Application Flow.

[R54] notes that a Policy associated, explicitly, with an Application Flow overrides any Policy association for the Application Flow Group to which that Application Flow is a member.

[R55] If an Application Flow is not assigned a Policy at an SWVC End Point in the SWVC End Point Policy Map and is not a member of an Application Flow Group that is assigned a Policy at that SWVC End Point, Ingress IP Packets mapped to the Application Flow **MUST** be discarded at that SWVC End Point.

[R56] If an Application Flow is assigned the reserved Policy name *block* at an SWVC End Point in the SWVC End Point Policy Map, either explicitly or through membership in an Application Flow Group, Ingress IP Packets mapped to the Application Flow **MUST** be discarded at the SWVC End Point.

In order to block (blacklist) an Application Flow that is a member of an Application Flow Group that has an assigned Policy, the Application Flow is assigned the reserved Policy *block* (see section 8.5).

Note that blocking/blacklisting an Application Flow (either by not having a Policy assigned or by explicit assignment of the reserved Policy, *block*, only refers to Ingress IP Packets. Egress IP Packets (i.e., IP Packets that were forwarded from other UNIs) are delivered to the UNI for these Application Flows.

10 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.

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 Network locations, much of this section is adapted from the UNI Services Attributes and UNI Access Link Service Attributes section of the MEF Service Attributes for Subscriber IP Services Technical Specification, MEF 61.1 [21] 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	*UT/PT or CVLAN x*
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 ≥ 1522
SD-WAN UNI IPv4 Connection Addressing Service Attribute	IPv4 Connection Address mechanism	*None, Static, or DHCP*
SD-WAN UNI IPv6 Connection Addressing Service Attribute	IPv6 Connection Address mechanism	*None, DHCP, SLAAC, Static* or *LL-only*

Table 6 – Summary of SD-WAN UNI Service Attributes

10.1 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.

[R57] The value of the SD-WAN UNI Identifier Service Attribute **MUST** be an Identifier String.

[R58] The value of the SD-WAN UNI Identifier Service Attribute **MUST** be unique among all UNIs in SWVCs (SD-WAN Services) purchased by the Subscriber from the Service Provider.

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.

Note that [R57] does allow the same identifier to be used in two of the Subscriber's SD-WAN Services if they are with different Service Providers.

10.2 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 and subsequently mapped to SWVC End Point associated with the UNI. The possible values are *UT/PT*, and *CVLAN x*.

[R59] 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 [R59] 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 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 10.3).

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*.
- When the field following the Source Address field is a TPID with the value 0x8100 and the corresponding VLAN ID is 0x0000, the Ethernet MAC Frame is said to be a *Priority Tagged frame*.
- When the field following the Source Address field is a TPID with the value 0x88a8, the Ethernet MAC Frame is said to be an *S-Tagged frame*.
- 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, Priority-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 S-tagged frames is beyond the scope of this document.

If the value of the SD-WAN UNI L2 Interface Service Attribute is *UT/PT*, then only Untagged and Priority-tagged frames that are received over the underlying physical or virtual layer 1 Ethernet link are mapped to the UNI.

If the value of the SD-WAN UNI L2 Interface Service Attribute is *CVLAN x*, then only C-Tagged frames that contain a C-VLAN Tag with a VLAN ID of *x* that are received over the underlying physical or virtual layer 1 Ethernet link are are mapped to the UNI. .

The Ethernet MAC frames are delivered over a layer 1 interface that supports an Ethernet MAC. This can be a physical interface such as any of the supported copper, optical, or wireless PHYs. It can also be a virtual interface such as a vNIC in a server. The details and parameters of the layer 1 interface must be agreed 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-VLAN 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.

10.3 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.

[R60] The value for the SD-WAN UNI L2 Maximum Frame Size **MUST** be an integer number of bytes ≥ 1522.

[D2] 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.

10.4 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.

[R61] The SD-WAN UNI IPv4 Connection Addressing Service Attribute and the SD-WAN UNI IPv6 Connection Addressing Service Attribute (section 10.5) **MUST NOT** both have the value *None*.

If the value of the SD-WAN UNI IPv4 Connection Addressing 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.

[R62] 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. In this context, *Static* refers to manual configuration of the IPv4 Connection Addressing on the Subscriber devices.

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)
- 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.

Any address within the IPv4 Connection Addressing subnet(s) can be used by the Subscriber for configuring Subscriber equipment, excluding the Service Provider IPv4 addresses and any addresses within prefixes listed in the value of the SWVC Reserved Prefixes Service Attribute (see section 8.4).

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 Primary Subnet IPv4 Prefix or a Secondary subnet IPv4 prefix.

[R63] If the 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 8.4) 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 Primary Subnet 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 [R65] prohibits the Subscriber from assigning the highest address in the prefix).

[R64] 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 8.4).

[R65] 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 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 8.4).

10.5 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 [R61]).

If the value of the SD-WAN UNI IPv6 Connection Addressing Service Attribute is one of *DHCP, Static, SLAAC, 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 [12]. The Service Provider hosts the DHCP server and the Subscriber devices act as the DHCP clients.

[R66] 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 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 [14]. The Router Advertisements that convey the IP Prefix is also be used to convey the prefix length and router address.

For *DHCP*, *SLAAC* and *Static*, a number of 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 SP's IPv6 address are specified. The IPv6 Prefix is referred to as the 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 8.4); 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.

[R67] 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.

[R68] If the value of the SD-WAN UNI IPv6 Connection Addressing is *DHCP*, addresses that are dynamically assigned by DHCP **MUST** be taken from within one of the IP Prefixes in value of the SWVC Reserved Prefixes (section 8.4) that is a subnet of one of the Connection IPv6 Prefixes.

[R69] 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 [14] 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 8.4).

[R70] 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 8.4).

11 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 2764, *A Framework for IP Based Virtual Private Networks*, February 2000

[10] IETF RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP*, September 2001

[11] IETF RFC 3260, *New Terminology and Clarifications for Diffserv*, April 2002

[12] IETF RFC 3315, *Dynamic Host Configuration Protocol for IPv6* (DHCPv6), July 2003

[13] IETF RFC 3550, *RTP: A Transport Protocol for Real Time Applications*, July 2003

[14] IETF RFC 4862, *IPv6 Stateless Address Autoconfiguration*, September 2007

[15] IETF RFC 5357, *A Two-Way Active Measurement Protocol (TWAMP)*, October 2008

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

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

[18] MEF 6.2, *EVC Ethernet Services Definitions Phase 3*, August 2014

[19] MEF 10.4, Ethernet Service Attributes, Phase 4, December 2018

[20] MEF 23.2, *Carrier Ethernet Class of Service Implementation Agreement – Phase 3*, August 2016

[21] MEF 61.1, *IP Service Attributes*, January 2019

[22] MEF 63, *Subscriber Layer 1 Service Attributes*, August 2018

[23] MEF 74, *Commercial Affecting Attributes Technical Standard*, December 2018

[24] MEF, *Understanding SD-WAN Managed Services*, July 2017

Appendix A Processing Application Flows (Informative)

There are several steps in determining how to forward ingress IP Packets as shown in Figure 6.[11]

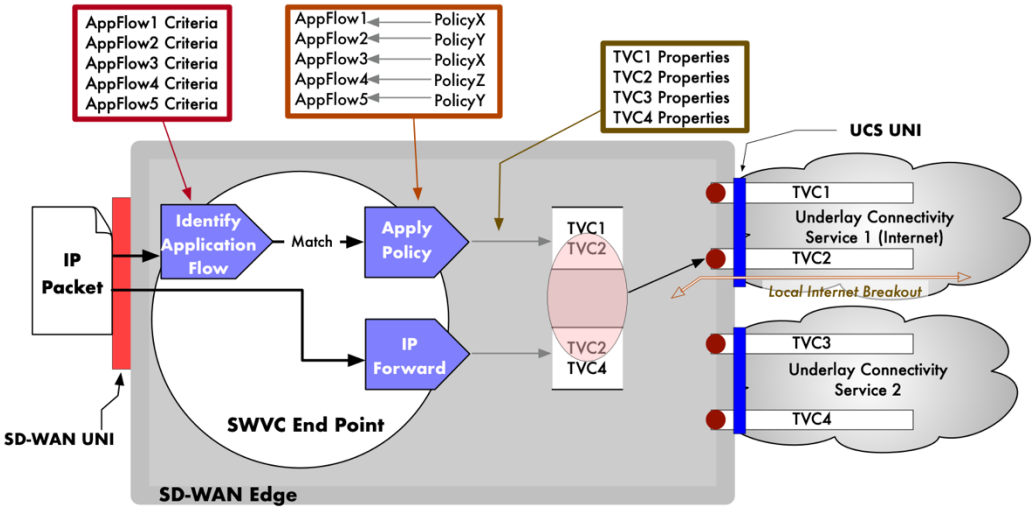

Figure 6 – Application Flows and Policies

After an IP Packet enters the SD-WAN Edge at the Ingress UNI, it is inspected to identify with which Application Flow it is associated (if the packet does not match any of the defined Application Flows, it is discarded). Then, a Policy is applied to the packet which, in conjunction with the properties of the TVCs, results in a list of TVCs that can carry the IP Packet (in the diagram, TVC1 and TVC2). If no Policy has been assigned to the Application Flow at this End Point, it is discarded. The IP Forwarder determines which TVCs can reach the destination (in the diagram, TVC2 and TVC4). The intersection of these results yields the TVC (or TVCs) that can carry the IP Packet (in this case, TVC2). 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.

If the Ingress IP Packet is part of an Application Flow whose Policy indicates that Internet Breakout is required, the packet will likely follow the Local Internet Breakout path shown in the diagram since UCS #1 is an Internet service.

This is a conceptual representation of the SD-WAN Edge functionality. The Policy process and IP Forwarder are shown in parallel. In a given implementation they could run in parallel (as shown) or they could be sequential in either order. 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

[11] 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.

beyond the scope of this document. The relevant point is that an IP Packet arrives, and it is either discarded or assigned to a TVC based on the Policy and IP Forwarding requirements of the IP Packet.

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* [24].

B.1 Hybrid WAN

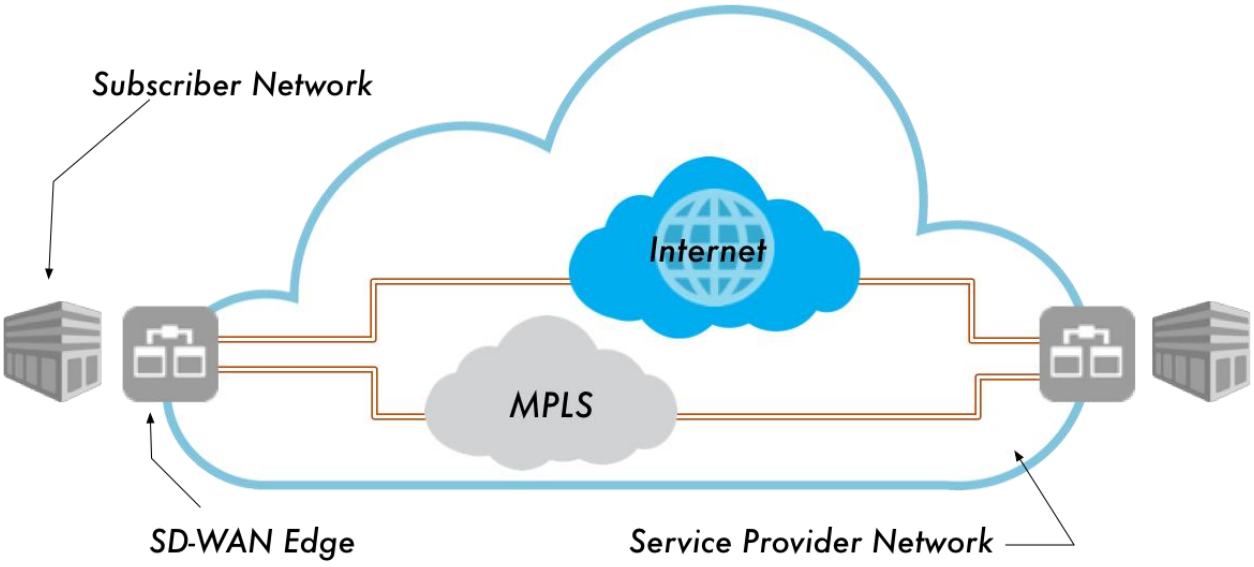

Figure 7 – Use Case: Hybrid WAN

Figure 7 illustrates a use case for an SD-WAN Service operating over two Underlay Connectivity Services, an Internet 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 two 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

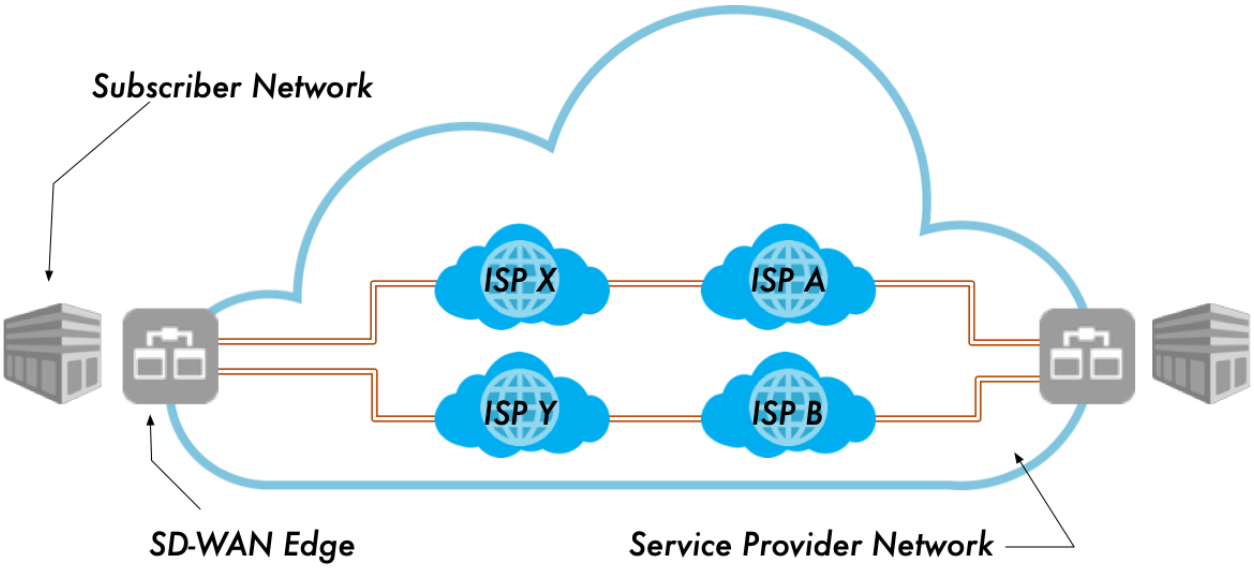

Figure 8 – Use Case: Dual Internet WAN

Figure 8 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 (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.