This line has the fields.

MEF Specification

MEF x WD 0.18

MEF 3.0 SD-WAN Service Attributes and Service Definition

Technical Specification

August 1, 2018

Caution - this draft represents MEF work in progress and is subject to change.

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 document and have requested to be included in this list.

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

- ABC Networks
- XYZ Communications

2 Abstract

The SD-WAN Service Attributes and Service Definitions Technical Specification defines the externally-visible behavior of SD-WAN Services. The Service Definition is based on an agreement between a SD-WAN Subscriber (the customer) and an SD-WAN Service Provider that includes agreement on the values of a set of SD-WAN Service Attributes that are defined in this document.

This document combines functions that are frequently covered in separate MEF documents:

- Service Attribute definitions – i.e., the enumeration and description of the information that can be agreed on at the various interfaces 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 Definition. Rigorous definition of Service Attributes also facilitates information modeling for API and Protocol definitions. An example of a MEF Service Attributes definition Technical Specification is MEF 10.x (Subscriber Ethernet Service Attributes).
- Service Definition – the "product" that the Service Provider can sell to the Subscriber. An SD-WAN Service represents a particular type of connectivity capability with attributes that are constrained to values specified in this specification. Services can be subject to certification. An example of a MEF Service Definition Technical Specification is MEF 6.x (Subscriber Ethernet Service Definitions).

This is the first release of this specification. An attempt has been made to define a relatively complete set of Service Attributes for SD-WAN services. Nonetheless, it is likely that as this specification is revised new attributes will be defined and existing attributes will be refined, extended, or deleted.

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 [24] are included in this document by reference and are not repeated in the table below. Terms marked with * are adapted from terms in MEF4 [18], MEF 10.3 [19], MEF 23.2 [20], MEF 26.2 [21], or MEF 61 [24].

Term	Definition	Reference
Application	A subset of the IP packets that arrive at an SD-WAN UNI that are uniquely identified through adherence to a set of Application Criteria.	This document
Application Criterion	One of an agreed-on set of rules that are used to identify an Application at an SD-WAN UNI.	This document
Application Group	An aggregation of Applications at an SD-WAN UNI that can be used to assign a common Policy to the Applications and/or share bandwidth among the Applications.	This document
Class of Service Name	An administrative name assigned to a particular set of Performance Objectives that applies to traffic from Applications to which the Class of Service Name is applied.	This document *
CoS Name	Class of Service Name	This document *
Egress IP Packet	An IP Packet transmitted to the Subscriber at a UNI.	This document *
Ingress IP Packet	An IP Packet received from the Subscriber at a UNI.	This document *
Internet Protocol	A protocol for transmitting blocks of data from source to destination hosts within an interconnected system of packet-switched computer communication networks.	RFC 791 [2]
IP	Internet Protocol	RFC 791 [2]
IP Packet	Either an IPv4 Packet or an IPv6 Packet, from the start of the IP Version field to the end of the IP data field.	RFC 791 [2], RFC 2460 [9]
IP Prefix	A set of IP addresses, containing the contiguous range of IP addresses whose initial n bits all have the same value, for some value of n. Typically this is expressed by giving the first address in the range and the value of n (the “prefix length”).	This document *
IPv4	IP version 4	RFC 791 [2]
IPv6	IP version 6	RFC 2460 [9]
Performance Group	A set of SD-WAN End Point pairs that have the same values for Performance Objectives within a particular Class of Service	This document
Policy	A set of rules that can be applied to an Application that describe the desired handling by the SD-WAN of IP Packets that are described the Application definition.	This document
Policy Criterion	One of the rules that make up a Policy. Each Policy Criterion can specify a rule associated with Forward, Security, Business Requirements, Bandwidth resources, and Class of Service.	This document

Term	Definition	Reference
SD-WAN Service Provider	The organization that is the seller or provider for an SD-WAN Service	This document
SD-WAN Subscriber	The organization that is the purchaser or customer for an SD-WAN Service	This document
SD-WAN UNI	The reference point that represents the boundary between the responsibility of the Subscriber and the responsibility of the Service Provider.	This document
SD-WAN Subscriber Network	A network belonging to a given SD-WAN Subscriber, which is connected to an SD-WAN Service Provider at one or more SD-WAN UNIs.	This document
SD-WAN Virtual Connection	An association of SD-WAN Virtual Connection End Points that provides connectivity and transport of IP Packets between the associated End Points.	This document
SD-WAN Virtual Connection End Point	A logical construct at an SD-WAN UNI that partitions Ingress IP Packets into Applications, applies a Policy to each IP Packet based on the associated Application, and selects an appropriate path to transport the IP Packet over the SWVC.	This document
Service Attribute	Specific information agreed between the provider and the user of a service, as described in a MEF specification, that describes some aspect of the service behavior.	This document *
Service Level Agreement	The contract between the Subscriber and Service Provider specifying the service level commitments and related business agreements for a service.	This document *
Service Provider	SD-WAN Service Provider	This document
SLA	Service Level Agreement	This document *
SN	SD-WAN Subscriber Network	This document
SPN	Service Provider Network	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 Network Service that provides a well-defined set of transport characteristics (e.g., delay, security, bandwidth, etc.).	This document
TVC	Tunnel Virtual Connection	This document
Underlay Network	An Underlay Network is a physical network that provides all or part of the connectivity associated with an SD-WAN Service	This document
Underlay Network Service	A service offering providing transport across an Underlay Network. Examples are an IPSEC tunnel, IP-VPN, and Carrier Ethernet Service	This document
Underlay Network Service Provider	An organization that provides an Underlay Network Service to a Subscriber or SD-WAN Service Provider	This document
UNI	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 [17]) 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**.**

Editor Note 2: The following paragraph will be deleted if no conditional requirements are used in the document.

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

5 Numerical Prefix Conventions

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

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

Table 2 – Numerical Prefix Conventions

6 Introduction

6.1 SD-WAN Overview

An SD-WAN Service provides a virtual overlay network that delivers intelligent and orchestrated connectivity between SD-WAN Subscriber Networks (SNs) that are connected to the SD-WAN Service Provider at two or more SD-WAN User-Network Interfaces (SD-WAN UNIs).

An SD-WAN Service is a Software Defined transport service that emulates a Wide Area connection between locations, but since it sits on top of multiple disparate transport services, it can offer richer and more differentiated service delivery capabilities than traditional WAN Services.

Because SD-WAN is Software Defined, it can provide agility unavailable in traditional wide area services. This agility can be manifested both in the ability of the Subscriber to adjust aspects of the service in real time to meet business needs and the ability of the Service Provide to monitor the performance of the Service and modify the forwarding mechanisms based on real-time events in the network.

One of the most important aspects of SD-WAN is that, unlike other Services where most decisions are based on low-level header information in data packets (layer 1, 2, or 3 addressing), SD-WAN is "Application aware". The Service Definition includes specification of Applications that are recognized at the entry to the Service and a way to specify Policies that describe the appropriate handling of IP Packets associated with the various Applications.

This Technical Specification defines a set of Service Attributes that describe the externally visible behavior and operation of an SD-WAN Service and form the basis of the agreement between the purchaser 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. The Service Attributes are organized based on the components of the interface between the Subscriber and the Service Provider that they describe.

6.2 Characteristics of an SD-WAN Service

An SD-WAN Service is a connectivity service that transports IP Packets between Subscriber Networks. The SD-WAN Service is an overlay that uses paths built by the SD-WAN Service Provider across disparate[1] (underlay) network services to provide a resilient and cost-effective service. An SD-WAN Service consists of a single SD-WAN Virtual Connection (SWVC) and an SD-WAN UNI (UNI) at each Subscriber Site.

The Service has the following characteristics which are further described in this specification:

- The basic unit of transport is the IP Packet.
- The service topology is inherently a full mesh of endpoints, but policy and forwarding restrictions can result in a variety of hub and spoke topologies.

[1] Strictly speaking, the underlays don't have to be disparate, but much of the value of SD-WAN derives from having different types of underlays with different cost and performance characteristics.

- The Subscriber connects to the Service at an SD-WAN UNI.
- IP Packets presented to the Service at the SD-WAN UNI are segregated based on the Application with which they are associated.
- Service quality is differentiated Application based on Policy applied to each Application.
- Applications can be rate-limited and groups of applications can share bandwidth resources.
- Each Application can be assigned a Class of Service where the Class of Service specifies a set of Performance Metrics that are monitored and Performance Objectives for those Performance Metrics.

6.3 Organization of the Specification

The specification is organized as follows:

- Key concepts and definitions are detailed in Section **7**.
- Service Attributes for the SD-WAN Virtual Connection (SWVC) are described in section 9.
- Service Attributes for the SD-WAN Virtual Connection End Point are described in section 10.
- Service Attributes for the SD-WAN UNI are described in section 11.
- An Architectural Framework for SD-WAN Services is described in Appendix A.
- Several implementation issues and options are contained in Appendices B and C.

7 Key Concepts and Definitions

This section provides definitions and overviews of the major architectural components of a MEF 3.0 SD-WAN Service.

A MEF 3.0 SD-WAN Service is a connectivity service that provides Application-Aware, Policy-Based forwarding of IP Packets between Subscriber Networks[2]. An SD-WAN Service is based on the elements listed below (and further described below), and the values for the Service Attributes that represent the properties of these elements and that form the basis of a Service Level Agreement (SLA) between the SD-WAN Service Provider (called the "Service Provider" in this document) and the SD-WAN Subscriber (called the "Subscriber" in this document).

The elements of a MEF 3.0 SD-WAN Service are:

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

These elements all have properties (attributes) that affect the operation of the SD-WAN Service and are described in the Service Level Agreement between the SD-WAN Service Provider and the Subscriber. Some of these properties are inherent in a particular instance of the element (e.g., a link speed) and are immutable while some of them are configurable. Information models should exist for each of these elements.

In addition, there are several additional concepts and components that are important to the description and specification of an SD-WAN service but do not usually require agreement between the Subscriber and the Service Provider. These include:

- Subscriber Network
- SD-WAN Edge
- SD-WAN Service Provider
- Underlay Network
- Underlay Network Service
- Tunnel Virtual Connection (TVC)

These are all shown in the following diagram:

[2] One or more of the end points of an SD-WAN service can be at a connection to an external network which might provide further transport to a Subscriber location or might be a connection to a cloud-based service. In this case, the SD-WAN Edge is referred to in some MEF documents as an SD-WAN Gateway.

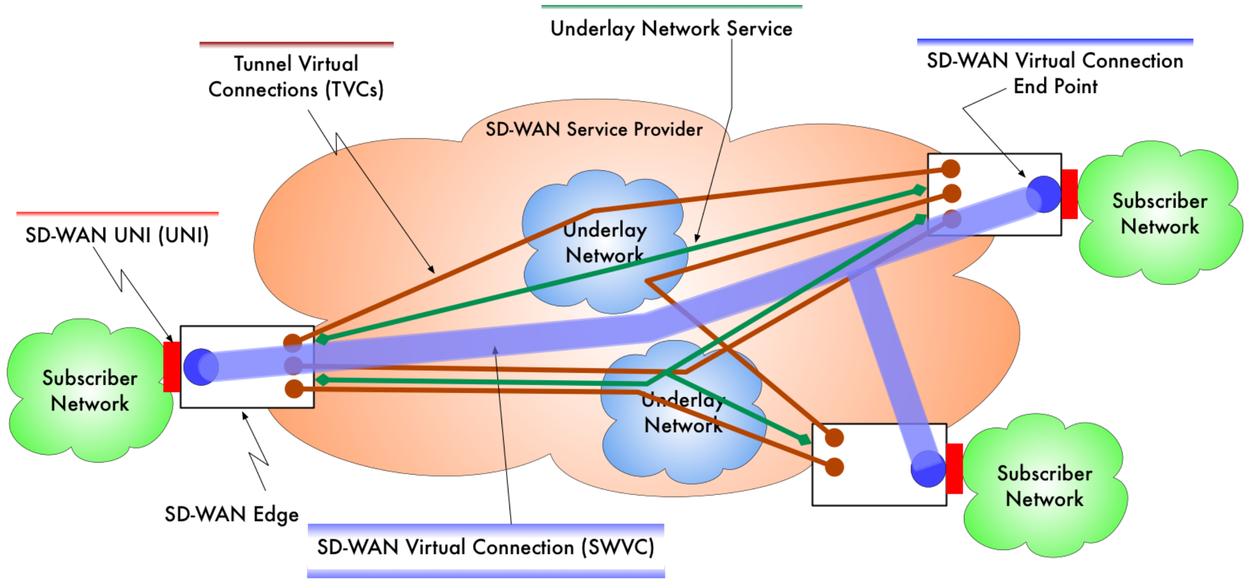

Figure 1 – Components of an SD-WAN Service

An informal description of the operation of the SD-WAN Service is as follows (note that each of these steps can have much more behind it than the simple description provided here):

- An IP Packet from the Subscriber Network crosses the SD-WAN UNI and arrives at the SD-WAN Edge.
- The SD-WAN End Point located in the SD-WAN Edge identifies the Application that the packet is associated with and also, optionally, the Application Group.
- The SD-WAN End Point applies the Policy Criteria assigned to the Application (which can be derived from a Group Policy as well as the individual Application Policy). This results in the packet being accepted or rejected (blacklisted Application). If accepted, a TVC is selected for the packet based on the Policy Criteria and the IP destination of the Packet.
- The packet arrives at the other end of the TVC where it is either forwarded to another TVC in the SD-WAN Edge (i.e., a routing hop) or presented to the SD-WAN End Point for delivery to the Subscriber Network via the local SD-WAN UNI.

Appendix A includes an informal, but more detailed, taxonomy of the various network components that are part of the SD-WAN ecosystem.

7.1 SD-WAN Subscriber and SD-WAN Service Provider

This document deals with two types of organizations, the SD-WAN Subscriber and the SD-WAN Service Provider. The SD-WAN Subscriber is the end-user of services described using the Service Attributes specified in this document and the SD-Service Provider is the organization that provides these services.

The SD-WAN Service is built on Underlay Networks and Underlay Network Services, which may be owned and operated by organizations other than SD-WAN Service Provider, and the business relationship with these other organizations may be initiated by the SD-WAN Service Provider or by the Subscriber. But, in the context of the SD-WAN Service itself, i.e., the interface at the SD-WAN UNI, the Subscriber and the SD-WAN Service Provider are the relevant actors.

In the interest of brevity, the reminder of this document uses “Service Provider” to refer to the SD-WAN Service Provider and “Subscriber” to refer to the SD-WAN Subscriber.

7.2 Subscriber Network and Service Provider Network

The “Subscriber Network” is defined as the network belonging to a given Subscriber that is connected to the Service Provider at one or more UNIs. There are no assumptions about the details of the Subscriber Network.

The “Service Provider Network” is not really a network in the typical sense of the word. It is more of a façade that encompasses a set of Underlay Networks, Underlay Network Services, and Tunnel Virtual Connections that are used to implement the SD-WAN Service. These components of the Service Provider Network might all be owned/managed by the SD-WAN Service Provider, or some of them might be purchased from other organizations.

The Service Provider Network may 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 may contract with the Service Provider to include some of the Subscriber’s existing WAN services in the SD-WAN Service and, in that case, some of the underlying components of the SD-WAN Service will be known to the Subscriber.

7.3 SD-WAN UNI (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 located between the Subscriber Network and the SD-WAN Edge.[3]

An IP Packet that crosses the SD-WAN UNI from the Subscriber to the Service Provider is called an Ingress IP Packet, and the SD-WAN UNI is the Ingress SD-WAN UNI for that IP Packet. Similarly, an IP Packet that crosses the SD-WAN UNI from Service Provider to the Subscriber is called an Egress IP Packet, and the SD-WAN UNI is the Egress SD-WAN UNI for that IP Packet.

In this document, the term “UNI” refers to the SD-WAN UNI.

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

[3] Formally, the UNI is an abstract reference point. We also use the term UNI to refer to the network connection between the Subscriber Network to the Service Provider (i.e. SD-WAN Edge), and hence the “SD-WAN UNI Service Attributes” describe this connection. The actual location of the reference point is nonetheless important because it defines where Service Provider’s responsibility starts and also because service performance is defined from UNI to UNI. For a physical SD-WAN Edge the location of the reference point is of minor importance since the connection is usually a short wire or fiber, but for a virtual SD-WAN Edge the agreed upon location of the SSI reference point is more important.

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

7.4 SD-WAN Virtual Connection (SWVC)

The SD-WAN Virtual Connection represents the connectivity service provided by the Service Provider to the Subscriber between two or more UNIs. This connectivity is inherently "any-to-any", i.e., a mesh, but forwarding rules (expressed as Policy) can constrain the logical topology of the service.

More formally, an SD-WAN Virtual Connection (SWVC) is an association of two or more SD-WAN Virtual Connection (SWVC) End Points located at UNIs.

7.5 SWVC End Point

An SWVC End Point is a logical construct implemented in the SD-WAN Edge and associated with a UNI that partitions the IP Packets that pass over the UNI into separate flows, each associated with an Application, based on a set of Application-matching criteria defined in the SLA. The SWVC End Point is also the element that applies Policies to Applications and, by extension, applies them to each IP Packet. This includes (most importantly) steering each IP Packet to one of the TVCs that terminate in the SD-WAN Edge.

7.6 Underlay Network

An Underlay Network is a physical network that provides all or part of the connectivity associated with an SD-WAN Service. The Underlay Network is commonly operated by the SD-WAN Service Provider, but it can also be another organization that has been arranged by the Service Provider or the Subscriber.

The Underlay Network can be implemented on any physical network technology (or combinations of physical network technologies) such as DSL, HFC, LTE, fiber, WiFi, Ethernet, and the transport can be based on Ethernet switching, IP Routing, MPLS, Carrier Ethernet, or other technologies.

Support for multiple Underlay Networks is one of the defining attributes of SD-WAN. Multiple Underlay Networks with different performance and cost characteristics (e.g., an MPLS Network and the Public Internet) can be used to provide cost benefits, resiliency, and differentiated transport.

Underlay Networks have a few characteristics that can be inherited by the Services that ride on them:

- They can be *Public* or *Private*. Loosely defined, a Public Network is one where the user connection point is part of the addressing and forwarding/routing structure of the network (e.g., the Internet). A Private Network is one the addressing and forwarding at the connection point is isolated from the network itself.
- Their cost may be *flat-rate* or *usage-based*. An example of this distinction is $200/months vs. $10/TB.

- They have a set of performance and bandwidth characteristics that impose limits on the Services that they support.

7.7 Underlay Network Service

In most cases, SD-WAN Services do not make direct use of an Underlay Network, but rather, they use a Service built on top of the Underlay Network. We refer to this as an Underlay Network Service. For example, if the Underlay Network is the public Internet, the Underlay Network Service might be an IPSec tunnel. If the Underlay Network is a private MPLS network, the Underlay Network Service might be an IP-VPN. If the Underlay Network is a Carrier Ethernet Network, the Underlay Network Service might be an Ethernet Private LAN (EP-LAN) Service.

The Underlay Network Service can have a many-to-one relationship to the Underlay Service. For example, there can be multiple IPSec tunnels over the Internet or multiple IP-VPNs over an MPLS network.

The Underlay Network Service inherits some of the properties of the Underlay Network (e.g., if the Underlay Network is Public, then so is the Underlay Network Service). And the bandwidth and performance constraints of the Underlay Network can only be further constrained by the Underlay Network Service, they (obviously) can't be relaxed).

The Underlay Network Service can expose a different charging mechanism than the Underlay Network, and it can add value such as Encryption.

[R3] A MEF 3.0 SD-WAN Service **MUST** support at least 2 Underlay Network Services.

[D1] A MEF 3.0 SD-WAN Service **SHOULD** support at least 2 different types of Underlay Network Service.

7.8 Tunnel Virtual Connection (TVC)

An SD-WAN Service Provider configures point-to-point tunnels called Tunnel Virtual Connections (TVCs) across the various Underlay Network Services that compose the SD-WAN Service. Each TVC provides connectivity with a well-defined set of characteristics from one SD-WAN Edge to another SD-WAN Edge.

When an Ingress IP Packet arrives at a UNI, the SD-WAN End Point associates the IP Packet with an Application and then applies a Policy based on that Application. The selection of a TVC to transport the IP Packet is based on the Policy requirements and the IP Packet's destination (a routing decision).

The properties of the TVCs are important to the operation of the SD-WAN since these are used to match the Policy Criteria applied to an Application.

- TVCs are *Public* or *Private* based on the Underlay Network that they are built on.
- TVCs have a charge model of *fixed-rate* or *usage-based* that reflects the Underlay Network Service that they are built on.

- TVCs can be *encrypted* or *unencrypted*. Encryption may be provided by the Underlay Network Service or implemented at the TVC End Point in the SD-WAN Edge.
- TVCs can be designated as *Primary* or *Backup*.
- TVCs have performance and bandwidth constraints and behaviors that reflect the Underlay Network Service that they are built on.

7.9 MEF 3.0 SD-WAN Services Framework

A complete MEF 3.0 SD-WAN Service consists of:

- Exactly one SWVC, with a corresponding set of SWVC Service Attributes
- Two or more SD-WAN UNIs where the Subscriber Network accesses the service, each with a corresponding set of SD-WAN UNI Service Attributes
- Exactly one SWVC End Point for the SWVC associated with each of the UNIs, where each SWVC End Point has a corresponding set of SWVC End Point Service Attributes
- A set of Tunnel Virtual Connections (TVCs)

7.10 Service Attributes

MEF Services are specified using Service Attributes. A Service Attribute captures specific information that is agreed between the provider and the user of a MEF Service, and it describes some aspect of the service behavior. How such an agreement is reached, and the specific values agreed, 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 user of the service selects from a set of options specified by the provider.
- The user of the service requests a particular value, and the provider accepts it.
- The user and the provider of the service negotiate to reach a mutually acceptable value.

Service Attributes describe the externally visible behavior of the service; they do not constrain how the service is implemented by the Service Provider, or how the Subscriber implements their network.

Service Attributes describe the static attributes of a service that can be documented in an SLA; they do not describe dynamic state. So, for example, there can be a Service Attribute for the "Maximum Number of Widgets" but not for "Number of Widgets In Use". Similarly, for performance related attributes there can be a Service Attribute for "Maximum Allowed Delay" between two end points, but not one for "Current Delay".

There are two types of Service Attributes: Behavioral Service Attributes and Capability Service Attributes. Behavioral Service Attributes directly affect the behavior of the service as experienced by the Subscriber. As soon as the Service Provider has enacted a particular value, the Subscriber can test this to ensure the observed behavior matches that expected, for example by sending appropriate traffic over the service.

In contrast, Capability Service Attributes do not directly affect the behavior of the service; instead, they serve as hints to the Service Provider as to what changes to the service the Subscriber might request in future, and as hints to the Subscriber as to the likely response to such requests. Particular values of a Capability Service Attribute can constrain the acceptable values for other Service Attributes, but do not directly affect the behavior of the service and hence cannot be tested.

There are three elements associated with the interface between the SD-WAN Subscriber and the SD-WAN Service Provider. This specification defines the Service Attributes for these elements, as follows:

- SD-WAN Virtual Connection (SWVC) Service Attributes (section 9)
- SWVC End Point Service Attributes (section 10)
- SD-WAN Subscriber Interface Attributes (section 11)

7.11 SD-WAN Edge

The SD-WAN Edge is the "machine" (physical or virtual) that terminates the Service Provider side of the UNI connection between the Subscriber and the Service Provider on one side and terminates one or more "WAN" connections (TVCs) on the other side. The SD-WAN Edge is architecturally equivalent to a NID (Network Interface Device) in other types of services such as MEF Ethernet Services.

The SD-WAN Virtual Connection End Point can be thought of as residing in the SD-WAN Edge.

7.12 "Support" in Normative Language

When the term "support" is used in a normative context in this document and the normative language applies to the Service Provider, it means that the Service Provider must/should/may be capable of meeting the requirement upon agreement between the Subscriber and Service Provider.

7.13 Service Assurance

Service Assurance is provided through the definition of Classes of Service that can be associated with incoming IP Packets. Each Ingress IP Packet is associated with an Application and each Application is associated with a Policy that specifies a Class of Service.

The use of the Class of Service in SD-WAN is broader than in other MEF Services such as IP and Carrier Ethernet Services. Specifically, in other MEF Services CoS defines a static goal for Performance Objectives for the service that can be reported against. For example, for IP Services, if there is a Performance Objective that Packet Delay will be less than or equal to 20ms for 99.5% of all Packets over the measurement period (e.g., one month), then at the end of each month, the Service Provider reports on the actual performance that was measured and whether it met the objective or not.

Like the other Services, SD-WAN Services uses the Performance Objectives associated with a Class of Service for this purpose, but in addition, SD-WAN uses the Performance Objectives as part of the Packet Steering function at the SD-WAN Edge. The SD-WAN Service can continually monitor the performance of the various paths available in the SD-WAN Service and use the Performance Objectives associated with each Application to make a dynamic steering decision for IP Packets associated with each Application so that they traverse the path that provides the best available match against the Performance Objectives for conditions at that time.

Pairs of SWVC End Points are partitioned into Performance Groups (section 9.3) based primarily on the distance between them, and for each Class of Service, Performance Objectives are specified for Performance Metrics per Performance Group.

7.14 Identifier String

Many of the Service Attributes and 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 strings. The definition has two components: length and allowable character set.

The length of the identifier is limited so that systems (human interfaces, protocols, etc.) can be built to handle them deterministically.

[R4] An Identifier String **MUST** contain no more than 63 octets.

63 octets was chosen because it provided a reasonable maximum for a human-visible/usable string and allows for the fact that some protocols and data structures zero-terminate strings.

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

[R5] An Identifier String **MUST** be a non-null RFC 2579 [10] DisplayString but not contain the characters 0x00 through 0x1f.

7.15 Relationship to IP Service Attributes for Subscriber IP Services

An SD-WAN delivers IP Packets between Subscriber Networks. In that sense it shares many attributes with a general IP service. Therefore, many of the sections of this specification are derived[4] (copied) from the MEF 61, *IP Subscriber Service Attributes for Subscriber IP Services* [18].

Since SD-WAN is intended to provide simplified connectivity options, only a selected set of Service Attributes are integrated from MEF 61. Conversely, since SD-WAN Services are based on Applications and Policies, there are a number of Service Attributes defined to describe these capabilities and, in addition, several of the Service Attributes integrated from MEF 61 have been modified to focus on Application and Policy-based forwarding rather than general IP/layer 3-based forwarding.

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

Editor Note 3: I have tried to only include IP Service Attributes that I believed were critical in providing an IP Connectivity Service. It is possible (likely) that I erred in both directions – i.e., included some SAs that are not critical and omitted some that are.

8 Applications and Policies

Application awareness and the forwarding of IP Packets across different TVCs with different attributes based on Policies applied to Applications are two of the defining characteristics of SD-WAN.

As part of the Service Level Agreement (SLA), the Subscriber and the Service Provider agree on a list of Applications that will be detected at the SD-WAN Edge. For each of the agreed-on Applications, a Policy (list of Policy Criteria) is assigned which defines how IP Packets associated with the Application are handled.

We use the word "Application," but we can think of this more broadly. The SD-WAN Edge partitions the IP Packets that arrive at the UNI into well-defined groups or flows (the Applications) that we aggregate for the purpose of applying a Policy to each group.

So, an Application can be a packet flow that encompasses several individual computer applications, such as "all packets that use the RTP protocol" or, conversely, a single computer application could represent multiple SD-WAN Applications such as a single Skype conversation resulting in a "Skype Video" SD-WAN Application and a "Skype Audio" SD-WAN Application, as long as there is a means to identify these explicit flows in the packet stream.[5]

There are several parts to this process as shown in the following diagram.

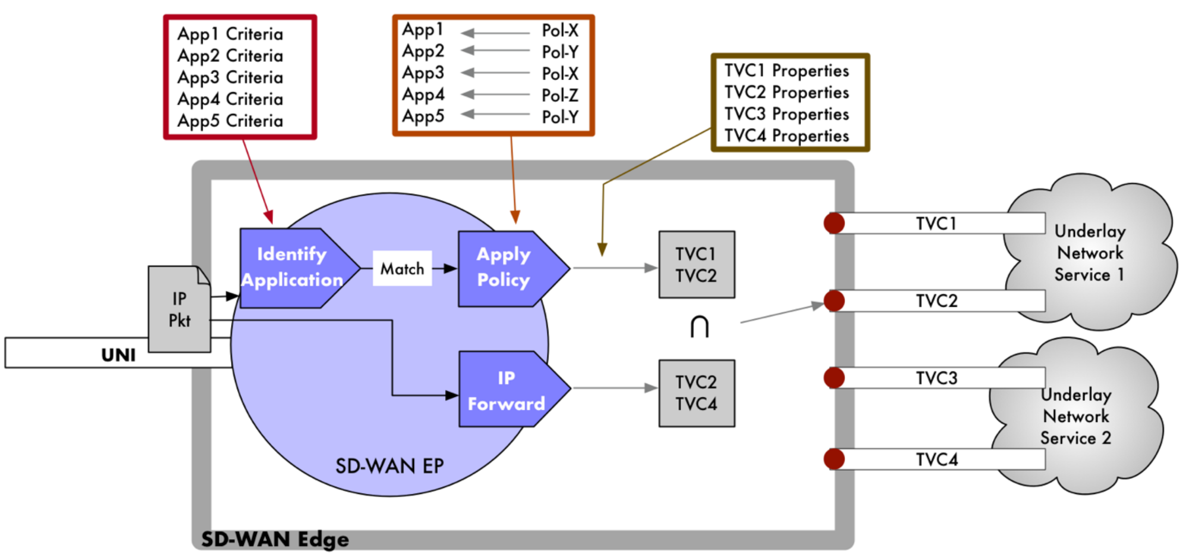

Figure 2 – Applications and Policies

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

When an IP Packet arrives at the SD-WAN End Point in the SD-WAN Edge, it is inspected to determine whether it matches one of the defined Applications. If it does, then a Policy is applied to the packet which, in conjunction with the known properties of the TVCs, results in a list of TVCs that can carry the IP Packet (in the diagram, TVC1 and TVC2). In addition, 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).

This is an idealized representation of the SD-WAN Edge. 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 exact details of the implementation are beyond the scope of this specification. The relevant point is that an IP Packet arrives, and it is either dropped or assigned to a TVC based on the Policy and IP Forwarding requirements of the IP Packet.

8.1 Organization of Applications and Policies Service Attributes

Operation of the SD-WAN Edge, as described above, depends on Service Attributes that are agreed on between the Subscriber and the Service Provider and documented in the Service Level Agreement. This section identifies the groups of Service Attributes associated with Applications and Policies. The details of these Service Attributes are described in the subsequent sections of this specification.

8.1.1 Applications

The SWVC List of Applications Service Attribute (section 9.10) describes the list of Applications that can be forwarded by the SD-WAN and the criteria used to identify them.

Although the Service Attribute allows detailed matching criteria for each Application, the expectation is that in many (most) cases, the SD-WAN Service Provider provides a catalog of "built-in" Applications that they support and the Subscriber can select Applications from the catalog. In this case, it is important that the Service Provider provide an explicit description of what is, and, if appropriate, what is not included in each of its standard Application definitions.

[R6] If the Service Provider provides a catalog of "built-in" Applications, the Service Provider **MUST** specify details of the match criteria for these Applications in the catalog or in the SLA.

Applications can be grouped into Application Groups. There are two purposes for grouping Applications. First, a Policy can be applied to the Group that is then "pushed down" onto each Application in the Group. For example, there might be three Applications in the Application Group "Streaming". A Policy can be applied to the Group "streaming" which is then inherited by the three Applications. Each Application can then override particular details of the Policy. The second purpose is to share bandwidth. Members of an Application Group can have their Bandwidth Profiles put into the same Bandwidth Envelope so that they can share bandwidth resources. This is described in section 9.11.2.

8.1.2 Policies

A Policy is a list of Policy Criteria. For example, there might be a Policy called "Important" which has Policy Criteria (1) low delay, (2) high bandwidth, (3) any cost. (These are intended just to be illustrative.)

A Policy is assigned to each Application and each Application Group. The Policy assigned to an Application Group has no functional effect, it is just a way to apply a common set of Policy Criteria to the Group members (and also to allow them to share bandwidth). The Policy applied to an Application overrides any Policy Criteria that it has in common with the Group.

The Policy Criteria applied to an Application describe how the SD-WAN should handle IP Packets associated with the Application.

For example, the Policy assigned to a Group may only indicate a single Policy Criterion, e.g., *CoS Realtime*. So, a priori, each Application in the group starts with that Policy Criterion. Each Application can then apply other Policy Criterion specific to the Application which may include one that overrules the Group Policy.

The list of Policies that can be applied to Applications (and Application Groups) is an SD-WAN Virtual Connection Service Attribute and is used at all SD-WAN End Points in the SWVC. So, IP Packets for Applications associated with the Policy, "Important", will be forwarded based on the three criteria listed above at all SD-WAN End Points in the SWVC. However, each Policy defined for the SWVC can have criteria that are overridden at an SD-WAN End Point. For example, it is possible to define an override for "Important" at the London End Point that specifies (3) lowest cost.

For the SWVC List of Policies Service Attribute see section 9.11.

For the SWVC End Point List of Policy Overrides Service Attribute see section 10.3.

With the List of Applications and the List of Policies, the last step is mapping Policies to Applications. The SWVC Policy to Application Map Service Attribute (section 9.12) provides this connection.

9 SD-WAN Virtual Connection (SWVC) Service Attributes

This section contains Service Attributes that apply to a 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 a given SD-WAN Service.

SWVC List of SWVC End Points	The SWVC End Points that are associated by the service	List of SWVC End Point Identifiers
SWVC Performance Groups	A partition of the ordered End Point pairs into groups with similar performance characteristics	List of 2-tuples <Group Name, List of ordered End Point pairs>
SWVC Performance Monitoring Time	An indication of when Performance Monitoring starts for the SWVC and what the Performance Measurement Interval is	2-tuple <ts, T>
SWVC Class of Service Names	A list of the Class of Service Names that can be used on the SWVC and the Performance Objectives associated with each	List of 2-tuples <CoSN, PG>
SWVC MTU	Maximum size (in octets) of an IP Packet that can traverse the SWVC without fragmentation	Integer ≥ 1280
SWVC Path MTU Discovery	Indicates whether Path MTU Discovery is supported for the SWVC	*Enabled* or *Disabled*
SWVC Fragmentation	Indicates whether IPv4 Packets can be fragmented	*Enabled* or *Disabled*
SWVC Reserved Prefixes	IP Prefixes reserved for use by the SP	*None* or list of IP Prefixes
SWVC List of Applications	A list of the Applications that are recognized by the SD-WAN Service	List of 2-tuples <Application ID, List of Application Criteria n-tuples>
SWVC List of Policies	A list of the Policies that can be applied to Applications carried by the SWVC	List of 2-tuples <Policy Name, List of Policy Criteria n-tuples>
SWVC Policy to Application Map	A map associating Applications to Policy for the SWVC	List of 2-tuples <Application ID, Policy Name>

Table 3 – Summary of SWVC Service Attributes

9.1 SWVC Identifier Service Attribute

The value of the SWVC Identifier Service Attribute is a string that is used to identify an SWVC within the Service Provider's network.

[R7] The value of the SWVC Identifier **MUST** be an Identifier String.

[R8] The SWVC Identifier **MUST** be unique across all SWVC Identifier s in the Service Provider Network.

The value of the SWVC Identifier Service Attribute is intended for joint Subscriber/Service Provider management and control purposes. As an example, the Acme Service Provider might use "SWVC-0001898-MEGAMART" to represent the Service Provider's 1898th SD-WAN Service with the customer for the SWVC being MegaMart.

9.2 SWVC List of SWVC End Points Service Attribute

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

[R9] The value of the SWVC List of SWVC End Points Service Attribute **MUST** have at least two entries.

[R10] The entries in the SWVC List of SWVC End Points **MUST** be different.

[R11] An SWVC **MUST NOT** have more than one SWVC End Point at a given UNI.

[R12] If an Egress IP Packet at an SWVC End Point results from an Ingress IP Packet at a different SWVC End Point, the two SWVC End Points **MUST** be associated by the same SWVC.

9.3 SWVC Performance Groups Service Attribute

Most aspects of network performance relate directly to the geographic distance between endpoints. The delay for a "high" quality of service between Los Angeles and San Francisco is clearly different than for the same quality of service between Los Angeles and New York. There are other attributes such as link speed and number of hops that might be relevant in some cases, but these are usually second level effects.

The value of the SWVC Performance Groups Service Attribute is a list of 2-tuples, $\langle PGname, PGlist \rangle$ where:

- *PGname* is an Identifier String that is the name of the Performance Group.
- *PGlist* is a list of ordered End Point pairs

[R13] Each Performance Group name, *PGname,* in the value of the SWVC Performance Groups Service Attribute **MUST** be an Identifier String.

The performance between two End Points is assumed to be symmetric. This leads to the next requirement.[6]

[R14] If the ordered End Point pair (a, b) is in a Performance Group, the reverse pair (b, a) **MUST** be in the same Performance Group.

This service attribute groups pairs of SWVC End Points (sections 9.210) into sets that have similar performance characteristics. Each group contains two or more ordered pairs of SWVC End Points.

[6] For the other MEF services EVC, OVC, IPVC, the symmetry is described as desired (SHOULD) rather than required (MUST).

If a SWVC has *n* SWVC End Points, there are a total of $n \times (n - 1)$ ordered End Point pairs, and the Performance Groups form a partition of that set of End Point pairs.[7]

For example, if the End Points for an SWVC are: Dublin, Paris, Madrid, and Warsaw, these End Points can be organized into three Performance Groups as follows:

```
Short
(Dub, Par) (Par, Mad) (Par, Dub) (Mad, Par)

Medium
(Dub, Mad) (Mad Dub)

Long
(Dub, War) (Par, War) (Mad, War) (War, Dub) (War, Par) (War, Mad)
```

9.4 SWVC Performance Monitoring Time Service Attribute

Performance Monitoring of an SD-WAN Service is based on a sequence of monitoring intervals starting at a specified date and time. The value of the SWVC Performance Monitoring Time Service Attribute is a 2-tuple $\langle ts, T \rangle$ where:

- *ts* is a time that represents the date and time for the start of Performance Monitoring
- 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 Performance Objectives are 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.

The parameters *ts* and *T* together define a sequence of Performance Measurement intervals[8]:

$$T_k = [ts + kT, ts + (k + 1)T) \; k = 0, 1, 2, \ldots$$

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

<"10-Jul-2018 00:00:00", "1 month">

9.5 Service Performance

9.5.1 Class of Service and Class of Service Names

Each IP Packet forwarded on an SD-WAN Service has a Class of Service Name assigned to it. A Class of Service Name is an identifier that represents a particular set of Performance Objectives, which is assigned to each Application as a component of the Policy that is assigned to the Application.

[7] A Performance Group is like a Performance Tier in MEF 23.2 [20], but it adds specification of the End Point pairs included in each "tier". Also, instead of having a small number of fixed Performance Tiers (five in MEF 23.2), the SD-WAN Service Provider and Subscriber can agree on a set of "tiers" that makes sense for the Service End Points.

[8] The notation *[x…y)* indicates an interval that is closed at the bottom (i.e., includes the bottom value, *x*), and open at the top (i.e. includes all values up to but not including the top value, *y*).

In SD-WAN Services, the Class of Service has two purposes. The first is a static reporting function, i.e., did the Service, over the past measurement period, meet the Performance Objectives promised? This use is consistent with how other MEF Services use Class of Service.

The second purpose is to assist with path selection for each Application. The SD-WAN Service measures the ongoing performance of each of the paths in the Service and attempts to steer packets associated with each Application to the path that best meets the Application's Performance Objectives. This means that the IP Packets associated with a particular Application can be steered to a different path if the path that they are currently using no longer meets the Performance Objectives.[9]

A Service Provider can support any number of named Classes of Service such as, [Platinum, Gold, Silver*, Bronze], [Rock, Paper, Scissors*], or [Red, Blue*, Green]. The Service Provider designates one of the Class of Service Names as the default Class of Service (these are marked with an asterisk in the previous examples) and the default is used for any Application that does not have an explicit Class of Service Name assigned to it. Service Providers usually have standard Classes of Service that can be used for all Subscribers and can also define custom Classes of Service for individual customers/Applications.

The SWVC Class of Service Names Service Attribute (see section 9.5.4) specifies the Class of Service Names supported for the SD-WAN Service and the Performance Metrics and Objectives associated with each Class of Service Name.

9.5.2 Qualified Packets

Many of the Performance Metrics specified in the sections below apply to Qualified Packets. A Qualified Packet is any unicast IP Data Packet that satisfies the following criteria for a given period T_k, a given Cos Name C, and a given ordered pair of SWVC End Points $\langle i, j \rangle$ in a Performance Group, PG:

- The IP Data Packet ingresses at the UNI associated with SWVC End Point i.
- The IP Data Packet is associated with an Application whose Policy includes the Policy Criteria FORWARD=*Enabled* and COS=C.
- The IP Data Packet should be delivered to SWVC End Point j.
- The IP Data Packet is not discarded per requirements [O1], [R25], [R35],[R102] , or to comply with the requirements of RFC 791 [2] or RFC 2460 [9].
- The length of the IP Data Packet is less than or equal to the value of the SWVC MTU Service Attribute (section 9.6).
- The first bit of the Ingress IP Data Packet arrives at the UNI associated with SWVC End Point i within the time interval T_k.

[9] Clearly there needs to be some intelligence applied to this type of path switching and appropriate hysteresis in the decision process to minimize or avoid out-of-order and duplicated packet delivery. These techniques are a function of the implementation of the SD-WAN Edge and out of scope for this specification.

9.5.3 Performance Metrics and Performance Objectives Overview

Performance Objectives are specified as 3-tuples <*name, parameters, objective*>. SD-WAN Service allow specification of Performance Objectives for any of the following six Performance Metrics:

- One-way Packet Delay Percentile
- One-way Mean Packet Delay
- One-way Inter-Packet Delay Variation
- One-way Packet Delay Range
- One-way Packet Loss Ratio
- Service Uptime

The formal definition of each of these Performance Metrics is provided in section 13.

For each Performance Metric/Objective there is a set (possibly empty) of *parameters* specific to the Performance Metric and a value for the Performance Objective, *objective*. For example, the 3-tuple:

<“One Way Packet Delay Percentile”, <99.8%>, 20ms>

specifies an objective of 20ms for One-way Packet Delay Percentile, at 99.8% (the only parameter for this metric). In other words, “99.8% of all packets will be delivered in 20ms or less”.

Note that One-way Packet Delay Percentile and One-way Mean Packet Delay are different ways of characterizing delay for IP Packets in an SD-WAN Service. In most situations, it is only necessary to specify one of these metrics. Similarly, One-way Inter-Packet Delay Variation and One-way Packet Delay Range are different ways of characterizing delay variation for IP Packets in an SD-WAN Service, and in most situations, it is only necessary to specify one of these metrics.

9.5.4 SWVC Class of Service Names Service Attribute

Performance Objectives for each Class of Service Name must be specified for each Performance Group identified in the SWVC Performance Groups Service Attribute. (section 9.3). The organization is as shown in the following diagram:

$$CoSN_1 \begin{cases} PG_1 \begin{cases} PM_1 \\ PM_2 \\ PM_n \end{cases} \\ PG_2 \begin{cases} PM_1 \\ PM_2 \\ PM_n \end{cases} \end{cases}$$

$$CoSN_n \begin{cases} PG_1 \begin{cases} PM_1 \\ PM_2 \\ PM_q \end{cases} \\ PG_2 \begin{cases} PM_1 \\ PM_2 \\ PM_q \end{cases} \end{cases}$$

Figure 3 – Class of Service Performance Objective Structure

For each Class of Service, Performance Objectives can be specified for any set of Performance Metrics and the same Performance Metrics are specified for all Performance Groups for that Class of Service (although the Performance Objectives are usually different for each Performance Group).

The value of the SWVC Class of Service Names Service Attribute is a list of 3-tuples $\langle CoSN, PGList, dflag \rangle$ where:

- *CoSN* is a Class of Service Name as described in section 9.5.1
- *PGList* is a list of 2-tuples $\langle PGname, PMList \rangle$ where:
  - *PGname* is a Performance Group name as described in section 9.3
  - *PMList* is a list of Performance Objective 3-tuples as described in section 9.5.3
- *dflag* is a Boolean (*true, false*) that indicates whether this CoS Name is the default.

[R15] A Class of Service Name **MUST** be an Identifier String

[R16] Each Class of Service Name **MUST** appear exactly once in the value of the List of Class of Service Names Service Attribute.

[R17] Exactly one CoS Name **MUST** have *dflag=true*.

[R18] The *PGList* element in the value of the SWVC Class of Service Names Service Attribute **MUST** include an entry for each Performance Group listed in the SWVC Performance Groups Service Attribute.

[R19] Every Performance Group in *PGList* for a specific *CoSN* **MUST** have Performance Objectives for the same set of Performance Metrics (*PMList*) and Performance Metric Parameters.

The implication of [R19] is that all of the Performance Groups for a particular CoS Name have Performance Objectives for the same Performance Metrics with the same parameters. For example, if CoS *Red* has only a single metric, "One Way Frame Delay Percentile" with percentile *p*=99.8%, then this metric and parameter has to be included for each Performance Group, and no other Performance Metrics. The Performance Objective for each Performance Group will likely be different, e.g., Performance Group *Short* might have an objective of 10ms, *Medium*, 40ms, and *Long* 100ms. For the same service, CoS *Blue* can have objectives (for all Performance Groups) for "One Way Frame Delay Percentile" with *p*=99.5% and "One Way Packet Loss Ratio". The following diagram provides a way to view the definition of a particular Class of Service.

Class of Service ***Interactive***	PG ***Short***	PG ***Medium***	PG ***Long***
Packet Delay Percentile	15ms (99.5%)	50ms (99.5%)	150ms (99.5%)
Mean Packet Delay	-	-	-
Inter Packet Delay Variation	2ms (99%, 1 sec)	4ms (99%, 1 sec)	6ms (99%, 1 sec)
Packet Delay Range	-	-	-
Packet Loss Rate	-	-	-
Service Availability	99.98%	99.98%	99.98%

Figure 4 – Representation of a Class of Service

9.6 SWVC MTU Service Attribute

The SWVC Maximum Transmit Unit (MTU) Service Attribute is an integer ≥ 1280 that specifies the maximum length in octets of IP Data Packets that the Service Provider guarantees to be able to carry across the SWVC.

[R20] The value of the SWVC MTU Service Attribute **MUST** be less than or equal to the minimum of the values of the UNI IP MTU Service Attribute (see section 11.6) for all of the UNIs that the SWVC is attached to.

RFC 791 [2] specifies the minimum MTU for IPv4 Packets as 68 octets; however, it also requires that all devices can handle a packet of length 576 octets (possibly fragmented). RFC 2460 [9] specifies the minimum MTU for IPv6 Packets as 1280 octets, and this value is the required minimum value in all cases.

[R21] The SWVC MTU **MUST** be greater than or equal to 1280 octets.

IP Data Packets with a length greater than the SWVC MTU can be delivered as is, discarded by the Service Provider, or in the case of IPv4 packets, fragmented within the SD-WAN Edge or the Underlay Network Services (providing fragmentation is enabled, see section 9.8). Note that it might be that packets longer than the SWVC MTU can be delivered between certain pairs of SWVC EPs, but not between others. If the Service Provider delivers such packets where possible, the Subscriber can make use of this by using Path MTU Discovery (see section 9.7).

[R22] Ingress IP Data Packets with a length less than or equal to the value of the SWVC MTU Service Attribute **MUST NOT** be discarded or fragmented due to their length.

[O1] Ingress IP Data Packets with a length greater than the value of the SWVC MTU Service Attribute **MAY** be discarded or (for IPv4) fragmented.

Note that fragmentation can impact performance, and hence this can be disabled via the SWVC Fragmentation Service Attribute (section 9.8).

9.7 SWVC Path MTU Discovery Service Attribute

The SWVC Path MTU Discovery Service Attribute indicates whether the Service Provider supports the use of ICMP-based Path MTU Discovery, as specified in RFC 1191 [3] and RFC 1981 [4]. It takes one of two values, *Enabled* or *Disabled*.

[R23] When the SWVC Path MTU Discovery Service Attribute is *Enabled*, IP routers within the Service Provider Network **MUST** generate the relevant ICMP error messages when an IP Packet is received that is discarded due to its length (per requirements [O1] and [R25]).

Note that [O1] allows packets longer than the SWVC MTU to be discarded or fragmented if they are not delivered; however, [R25] only allows them to be discarded if fragmentation is disabled.

[R24] When the SWVC Path MTU Discovery Service Attribute is *Enabled*, ICMP error messages destined towards a Subscriber Network **MUST NOT** be filtered or discarded.

When SWVC Path MTU Discovery is *Enabled*, hosts within the Subscriber Network can rely on using the mechanisms of RFC 1191 [3] and RFC 1981 [4] to discover the MTU that can be used for transmission of IP Packets to each remote host. Regardless of the value of the SWVC Path MTU Discovery Service Attribute, hosts can use the mechanism of RFC 4821 [14] for path MTU discovery. Depending on the host implementation, hosts might be capable of using a different MTU for each remote host they transmit to or might select the minimum value of all the hosts they transmit to.

9.8 SWVC Fragmentation Service Attribute

The SWVC Fragmentation Service Attribute specifies whether IPv4 Packets that are longer than the IPVC MTU can be fragmented (as described in RFC 791 [1][2]) as they traverse the SWVC. It takes one of two values, *Enabled* or *Disabled*.

[R25] When the SWVC Fragmentation Service Attribute is *Disabled*, Ingress IPv4 Data Packets with a length greater than the value of the SWVC MTU Service Attribute **MUST NOT** be fragmented.

Note that when the value is *Enabled*, IP Data Packets that are longer than the SWVC MTU might be delivered, fragmented or discarded, per [O1]. When the value is *Disabled*, such packets are delivered or discarded.

9.9 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, but which are nevertheless 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 so as to ensure they do not overlap with IP Prefixes used by the Subscriber inside the Subscriber Network.

[R26] The Subscriber **MUST NOT** use IP addresses that are within the IP Prefixes listed in the SWVC Reserved Prefixes Service Attribute for devices in the Subscriber Network.

One possible use for the SWVC Reserved Prefixes Service Attribute is if the Service Provider exposes the IP addresses for loopback interfaces on their PE devices to the Subscriber; this can help the Subscriber diagnose network problems using tools like ping and traceroute.

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 11.4 and 11.5.

9.10 SWVC List of Applications Service Attribute

The SWVC List of Applications Service Attribute specifies the Applications that can be recognized by the SD-WAN service and information about how to identify IP Packets associated with each Application. The value of the Service Attribute is a 3-tuple $\langle appID, appCL, appGroup\rangle$ where:

- *appID* is an Identifier String that is used to refer the Application description. The *appID* is not the actual Application Name, although it could be. For example, if the Application is "Skype", the *appID* could be "Voice", or it could be "Skype", or it could be "Mike", etc.
- *appCL* is a non-empty list of Application Criteria 2-tuples of the form $\langle ACName, ACValue\rangle$ where:
    - *ACName* is an Identifier String containing an Application Criterion Name from Table 4 or Table 5 or other Service Provider Application Criterion Name.
    - *ACValue* is a non-empty list of parameter values specific to the Application Criterion specified in *ACName*.
- *appGroup* is an optional Application Group Identifier that, if specified, is an Identifier String that identifies an Application Group that this application belongs to.

[R27] Each Application ID, *appID*, in the value of the SWVC List of Applications Service Attribute **MUST** be an Identifier String.

[R28] Each Application ID, *appID*, in the value of the SWVC List of Applications Service Attribute **MUST** appear, at most, once.

[R29] Every IP Packet received at the UNI **MUST** be associated with, at most, one Application.

[R30] If the Application Criteria for two or more Applications result in the situation where some IP Packets could be associated with more than one Application, the Service Provider **MUST** specify the order that the Application Criteria are applied.

As shown in the example later in this section, the criteria for one Application can be a subset of the criteria for another Application, so the order that the Applications are matched is important. It is the Service Provider's responsibility to ensure that the Subscriber knows exactly how the choice of Applications is made in this case. In general, the expectation is that the most restrictive Criteria will be applied first and the most general Criteria will be applied last.

[D2] If an IP Packet can be associated with more than one Application, the Service Provider **SHOULD** associate it with the most restrictive (most qualified) Application.

[R31] Then Application Criterion *ALL* **MUST** appear in, at most, one Application in the value of the SWVC List of Applications Service Attribute.

[R32] If an Application in the value of the SWVC List of Applications Service Attribute includes the Application Criterion *ALL*, it **MUST** be the last Application matched.

The Application Criterion *ALL* is used to provide a means to match all IP Packets that have not been matched by the explicitly listed Applications, i.e., a "catch-all". Therefore, only one application can use that Application Criterion and it must be the last one to be matched.

The *appGroup* element in the 4-tuple allows multiple Applications to be combined into an Application Group for the purpose of applying a common Policy and/or to share bandwidth. For example, Applications "Skype", "GoToMeeting" and "Webex" can all be members of the *appGroup* "Streaming Apps".

[R33] Each Application Group Identifier, *appGroup*, if specified **MUST** be an Identifier String.

[R34] Each Application Group Identifer, *appGroup*, **MUST** be unique among all Application Identifiers and Application Group Identifiers.

How the SD-WAN Edge applies the Application Criteria (*appCL*) to an Ingress IP Packet is implementation dependent and beyond the scope of this document.

[R35] Any Ingress IP Packet that cannot be associated with an Application from the value of the List of Applications Service Attribute **MUST NOT** forwarded on the SWVC.

[R36] If the *appCL* associated with an Application contains more than one entry, an Ingress IP Packet **MUST** match all entries in order to be associated with the Application.

The implications of [R36] is that the Application is defined by the conjunction of a set of Application Criteria. This doesn't allow for alternatives with an Application. However, the Application Group concept can provide alternatives. For example, one Application can have criteria X and Y and a second Application can have criteria X and W. If the two applications 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 defined as (X and Y) or (X and W).

[R37] The Service Provider **MUST** support the Application Criteria listed in Table 4.

Editor Note 4: Note that these two tables are intended (at this time) to be illustrative rather than definitive or exhaustive. We can add and remove items and organize them between the two tables as appropriate.

ACName	Description	Value
ALL	All IP Packets not matched by other Applications	No value
PROTNUM	IP Protocol Number	Integer from 0-255
PROTNAME	IP Protocol Name	Name from "Keyword" field of IANA document (ref). E.g., "TCP" or "UDP"
IPSA	IP Source Address	Standard IPv4 or IPv6 address
IPDA	IP Destination Address	Standard IPv4 or IPv6 address
IPSADA	IP Source or Destination Address	Standard IPv4 or IPv6 address
IPDARANGE	IP Destination Address Range	2 Standard IPv4 or IPv6 addresses representing the beginning and end of a range
SPORTNUM	TCP/UDP Source Port Number	Integer from 1 to 65535
DPORTNUM	TCP/UDP Destination Port Number	Integer from 1 to 65535
SDPORTNUM	Either TCP/UDP Source or Destination Port Number	Integer from 1 to 65535
SPORTNAME	TCP/UDP Source Port Name	Name from "Service" field of IANA document (ref)
DPORTNAME	TCP/UDP Destination Port Name	Name from "Service" field of IANA document (ref)
SDPORTNAME	Either TCP/UDP Source or Destination Port Name	Name from "Service" field of IANA document (ref)

Table 4 – Required Application Criteria

[D3] The Service Provider **SHOULD** support the Application Criteria listed in Table 5.

ACName	Description	Value
CATALOG	One of a list of known applications recognized by the Service Provider	An Identifier String
SPORTNUMLIST	A list of TCP/UDP Source Port Numbers	List of 1 or more integers from 0-255
DPORTNUM-LIST	A list of TCP/UDP Destination Port Numbers	List of 1 or more integers from 0-255
SDPORTNUM-LIST	A list of TCP/UDP Port Numbers in either the Source or Destination	List of 1 or more integers from 0-255
DOMAINLIST	Traffic to or frame a specific Domain	A list of domain names (not a full URL)

Table 5 – Optional Application Criteria

[O2] The Service Provider **MAY** support Application Criteria not listed in Table 4 or Table 5.

[R38] If the Service Provider defines its own Application Criteria, the ACNames used by the Service Provider **MUST NOT** be the same as any of the ACNames in Table 4 or Table 5.

Following is an example value for this Service Attribute:

```
”all Yahoo”
        (DOMAIN, “yahoo.com”)
”web-Yahoo”
        (DOMAIN, “yahoo.com”
        (SDPORTNUMLIST, <80,443,8080>)
”VOIP”
        (SDPORTNAME,”RTP”)
”Skype”
        (CATALOG, “Skype-for-Business”)
```

In this example, some IP packets can match both “all-Yahoo” and “web-Yahoo”. Based on [D2], the Service Provider would ensure that IP Packets are matched against “web-Yahoo” first unless it is otherwise agreed between the Service Provider and Subscriber.

9.11 SWVC List of Policies Service Attribute

Associated with each SWVC is a list of named Policies. Each Policy consists of a Policy Name and list of Policy Criteria for how to “process” traffic to which the policy is applied. Policies applied to an Application are normally enforced at all SWVC End Points in the SD-WAN Service, however some Policy Criteria can be overridden at the End Points. The Policy Criteria that can be overridden are identified “Override” column in the tables below. The SWVC List of Policy Overrides Service Attribute (section 10.3) is used to specify these overrides.

There are four types of Policy Criteria:

- Security/Forwarding Policies
- Business Policies
- Class of Service Policies
- Bandwidth Policies

These Policy Criteria types are useful for discussion and documentation purposes and are included for these purposes (i.e., they are informational, not normative).

Each Policy in the value of this Service Attribute is a 2-tuple of the form $\langle polID, polCL \rangle$ where:

- *polID* is an Identifier String that specifies the name of the Policy.
- *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 6, or Table 7 or other Service Provider-defined Policy Criterion Name.
    - *PCparam* is a non-empty list of parameter values specific to the Policy Criterion specified in *PCName*.

[R39] The value of the SWVC List of Policies Service Attribute **MUST** contain at least one entry.

[R40] Each Policy Criteria Name, *PCName*, in the value of the SWVC List of Policies Service Attribute **MUST** be an Identifier String.

[R41] Each Policy Criteria Name, *PCName*, in the value of the SWVC List of Policies Service Attribute **MUST** appear, at most, once.

Every Policy Criterion, except FORWARD, has a default value, therefore every Policy (an aggregation of Policy Criteria defined by this Service Attribute) can be thought of as having every Policy Criterion, where some are explicit, and others are implicit (i.e., defaulted).

Each Application inherits Policy Criteria from the Policy applied to the Application Group that is a member of, if any, and can override some or all of these Policy Criteria with a Policy applied to the Application directly.[10]

Section 9.11.1 describes Security/Forwarding, Business, and CoS Policy Criteria and section 9.11.1.1 describes Bandwidth Policy Criteria.

9.11.1 Security/Forwarding, Business, and CoS Policy Criteria

The Security/Forwarding, Business, and CoS Policy Criteria are listed in Table 6 and described in the subsequent sections.

[10] Since the default values are the same for the Group and the Application it doesn't matter if we include the implicit (default) criteria in this inheritance or not.

[R42] The Service Provider **MUST** support the Policy Criteria list in Table 6.

PCname	Description	Over-ride?
FORWARD	Should the application be accepted for forwarding over the SWVC?	Yes
ENCRYPTION	Does the application require transport to be encrypted?	No
UNDERLAY	Must the application traverse a private network only?	No
CHARGE-TYPE	Can this application be sent over usage-based or flat-rate transport?	No
BACKUP-USAGE	Can this application use a backup link or only a primary link? This provides a mechanism to shed bandwidth if the backup infrastructure doesn't support total bandwidth.	No
COS	The Class of Service (i.e., Performance Objectives) to use for IP Packets associated with the Application.	Yes

Table 6 – Security/Forwarding, Business and CoS Policy Criteria

[O3] The Service Provider **MAY** support Policy Criteria not listed in Table 6.

[R43] 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 6 or Table 7.

9.11.1.1 FORWARD Policy Criterion

IP Packets that arrive at the UNI can be forwarded over the SD-WAN service or discarded. Usually, they are forwarded, but it can be desirable to block/blacklist certain applications, either for the SD-WAN overall or at one or more UNIs. The FORWARD Policy Criterion provides this control explicitly. The allowed values are *Enabled* and *Disabled*. This is the only Policy Criterion that does not have a default value. Every Policy must have at least one Policy Criterion, and this one is the most basic, so it is always required.

[R44] If Policy Criterion FORWARD=*Enabled* is applied to an Application, then the Service Provider **MUST** attempt to forward IP Packets associated with the Application over the SD-WAN Service.

[R45] If Policy Criterion FORWARD=*Disabled* is applied to an Application, then the Service Provide **MUST NOT** forward any IP Packets associated with the Application over the SD-WAN Service.

[R46] Every Policy **MUST** explicitly include the FORWARD Policy Criterion.

[R47] If the Policy Criterion FORWARD=*Disabled* is applied to an Application the Service Provider **MUST** ignore all other Policy Criteria for that Application.

9.11.1.2 ENCRYPTION Policy Criterion

IP Packets forwarded over the SD-WAN service can be encrypted. The ENCRYPTION Policy Criterion provides control over whether they are sent over an encrypted path. It can have values *Required*, *Preferred*, *None*. The default value is *Required*.

[R48] If Policy Criterion ENCRYPTION=*Required* is applied to an Application, then IP Packets associated with the application **MUST** be sent over the SD-WAN Service via an encrypted path, if one is available.

[R49] If the Policy Criterion ENCRYPTION=*Required* is applied to an Application, and an encrypted path through the SD-WAN Service is not available, the Service Provider **MUST** discard IP Packets associated with the Application unless an alternative disposition has been agreed to between the Subscriber and the Service Provider.

[R50] If Policy Criterion ENCRYPTION=*None* is applied to an Application, then IP Packets associated with the application **MUST** be sent over the SD-WAN Service via a path that does not perform encryption, if one is available.

[R51] If Policy Criterion ENCRYPTION=*None* is applied to an Application and an unencrypted path through the SD-WAN Service is not available, the Service Provider **MUST** discard IP Packets associated with the Application unless an alternative disposition has been agreed to between the Subscriber and the Service Provider.

[R52] If Policy Criterion ENCRYPTION=*Preferred* is applied to an Application, IP Packets associated with the application **MUST** be sent over the SD-WAN Service via an encrypted path if one is available, and via an unencrypted path if an encrypted path is not available.

[R53] If no ENCRYPTION Policy Criterion is applied to a specific Application, then IP Packets associated with that Application **MUST** be treated as if ENCRYPTION=*Required* were applied.

Editor Note 5: I can envision addition Criteria associated with ENCRYPTION such as Protocol requirements or key length, etc. Contribution Needed.

9.11.1.3 UNDERLAY Policy Criterion

The Underlay Networks on which the SD-WAN Service is built can include private networks such as MPLS Networks, Carrier Ethernet Services, private IP Networks, etc., but they can also include public networks such as the Internet. The UNDERLAY Policy Criterion provides control over whether or not IP packets associated with and Application can traverse public networks. It can have values *Private-Only*, *Private-Preferred*, *Public, and Internet* and the default value is *Public*.

[R54] If the Policy Criterion UNDERLAY=*Private-Only* is applied to an Application, then IP Packets associated with the Application **MUST** be sent over the SD-WAN via a path that traverses only private networks, if one is available.

[R55] If the Policy Criterion UNDERLAY=*Private-Only* is applied to an Application and a path through the SD-WAN Service that traverses only private networks is not available, the Service Provider **MUST** discard IP Packets associated with the Application unless an alternative disposition has been agreed to between the Service Provider and the Subscriber.

[O4] If the Policy Criterion UNDERLAY=*Public* is applied to an Application or no UNDERLAY Policy Criterion is associated with the Application, then IP Packets associated the Application **MAY** traverse a path that includes both Private and Public networks such as the Internet.

[R56] If the Policy Criterion UNDERLAY=*Private-Preferred* is applied to an Application, then IP Packets associated with the Application **MUST** be sent over the SD-WAN via a path that traverses only private networks if such a path exists, and sent via alternative paths if a path through private networks is not available.

The Policy Criterion UNDERLAY=*Internet* has the same meaning as UNDERLAY=*Public* but has the additional capability that IP Packets associated with the Application can be sent via a local Internet breakout if such a connection is available and provides a delivery mechanism that meets the other Policies associated with the Application.

9.11.1.4 CHARGE-TYPE Policy Criterion

The cost for the use of a particular Underlay Network 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 CHARGE-TYPE Policy Criterion provides control over the charge type of the network that can be used to forward an Application. It can have values *Flat-Only*, *Prefer-Flat*, *Usage-Based* and the default is *Flat-Only*.

[R57] If Policy Criterion CHARGE-TYPE=*Flat-Only* is applied to an Application, then IP Packets associated with the Application **MUST** be sent over the SD-WAN Service via paths with flat-rate (i.e., time-based) charges.

[R58] If Policy Criterion CHARGE-TYPE=*Usage-Only* is applied to an Application, then IP Packets associated with the Application **MUST** be sent over the SD-WAN Service via paths with usage-based charges.

[R59] If Policy Criterion CHARGE-TYPE=*Prefer-Flat* is applied to an Application, then IP Packets associated with the Application **MUST** be sent over the SD-WAN Service via paths with flat-rate (i.e. time-based) charges if available and via Underlay Networks with usage-based charges otherwise.

9.11.1.5 BACKUP-USAGE Policy Criterion

Some TVC can be designated as Primary and some as Backup. The BACKUP-USAGE Policy Criterion provides control over whether IP Packets associated with an Application are sent over TVCs designated as Primary or Primary and Backup. This can be useful if, for example, Backup TVCs don't support as much bandwidth as the Primary TVCs. In this case, some applications can be designated to only use Primary TVCs so that their bandwidth is shed if the Primary fails. This criterion can have values *Primary-and-Backup* and *Primary-Only* and the default is *Primary-and-Backu*p.

[R60] If Policy Criterion BACKUP-USAGE=*Primary-and-Backup* is applied to an Application, then IP-Packets associated with the Application **MUST** be sent over the SD-WAN via paths that are designated as *Primary* if such a path is available and over paths designated *Backup*, if available, if no *Primary* paths are available.

[R61] If Policy Criterion BACKUP-USAGE=*Primary-Only* is applied to an Application, then IP-Packets associated with the Application **MUST NOT** be sent over the SD-WAN via paths that are designated as *Backup*.

[R62] If no BACKUP-USAGE Policy Criterion is applied to a specific Application, then IP Packets associated with that Application **MUST** be treated as if BACKUP-USAGE=*Primary-and-Backup* were applied.

Note that Applications that have the BACKUP-USAGE=*Primary-and-Backup* will likely be more resilient than those with *Primary-Only*. Therefore, the Class of Service associated with the former would likely have a higher Performance Objective for Service Availability than the later if this Performance Metric is used.

9.11.1.6 COS Policy Criterion

Each Application is associated with a Class of Service that describes Performance Objectives for Performance Metrics that are important to successful transfer of data for the Application. For example, real time applications such as audio or video streaming have problems if the Packet Delay Variation and Frame Loss are high and often have some limits on allowable Packet Delay whereas file transfers are less sensitive to these Performance Metrics. This means that real time applications may require more expensive transport. This Policy Criterion can have the value of any of the Class of Service Names enumerated in the SWVC Class of Service Names Service Attribute (see section 9.5.4). The default value for this Policy Criterion is the Class of Service Name that is designated as the default (see [R17]).

[R63] The Service Provider **MUST** steer IP Packets associated with an Application to paths across the SD-WAN that have performance characteristics that most closely align with the Performance Objectives specified for the Class of Service associated with the Application by the COS Policy Criterion.

The words "most closely align" are critical in [R63]. Contractually, the determination of whether the Service meets the Performance Objectives is made on the basis of a monitoring period (e.g., a month). “Were 99.8% of all VoIP Packets delivered with a delay ≤ 20ms in January?” In order to meet this Objective, VoIP Packets have to be sent over paths that will yield the desired result. But such a path might not always be available, for example, during a failure period. In this case the Service Provider is expected to forward Packets over the best possible path even if it currently doesn’t meet the Performance Objectives for the Application. This is why Objectives such as Delay are defined as percentiles.

[R64] If no COS Policy Criterion is applied to a specific Application, the Class of Service Name for the Application **MUST** be the CoS Name that is designated as the default in the SWVC Class of Service Names Service Attribute.

9.11.2 Bandwidth Policy Criteria

Bandwidth Profiles are used to parameterize the bandwidth limits that can be placed on Bandwidth Profile Flows. In SD-WAN, a Bandwidth Profile Flow is an Application. Bandwidth Profile Flows are organized into Envelopes and all of the Bandwidth Profile Flows in an Envelope (if there are more than one) can share some of the bandwidth resources assigned to the Envelope according to some rules. Section 12 provides a detailed description and explanation of Bandwidth Profiles, Bandwidth Profile Flows, and Bandwidth Profile Envelopes.

The Bandwidth Profile for an Application can reside either in an Application Envelope that contains a single Bandwidth Profile Flow, the Application, or in a Group Envelope that contains Bandwidth Profile Flows for Group members that have opted into the Group Envelope so that they can share bandwidth resources.

The assignment of a Bandwidth Profile Flow to an Envelope is based on Policy Criteria specified below and described in the following flowchart:

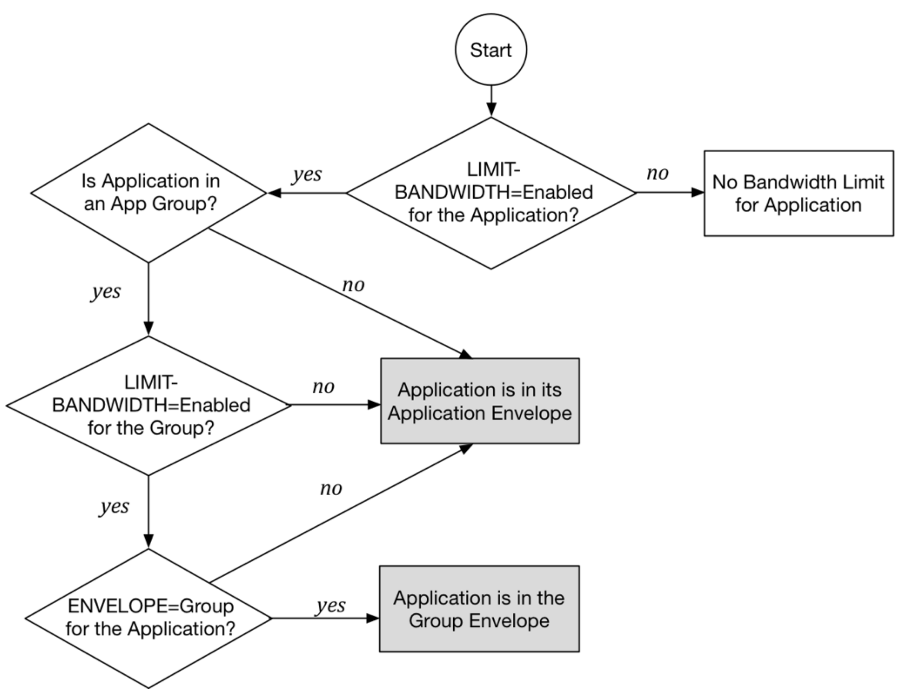

Figure 5 – Assigning Bandwidth Profiles to Envelopes

The Bandwidth Profile Flow associated with an Application (that has LIMIT-BANDWIDTH enabled) is in an Application Envelope if any of the following are true:

- The Application is not a member of an Application Group
- The Application Group that the Application is a member of does not have a LIMIT-BANDWIDTH=*Enabled* Policy Criterion
- The Application does not have ENVELOPE=*Group* Policy Criterion

If the Application Group has LIMIT-BANDWIDTH=*Enabled* and and the Application has ENVELOPE=*Group*, then the Bandwidth Profile Flow associated with the Application is in the Group Envelope.

The Policy Criteria associated with Bandwidth Profiles are listed in Table 7 and described in the subsequent sections. Note that the use and behavior of these Policy Criteria is different for Applications and Application Groups.

[R65] The Service Provider **MUST** support the Bandwidth Policy Criteria identified in Table 7.

PCname	Description	Override
LIMIT-BANDWIDTH	Should this application be bandwidth limited?	Yes
BANDWIDTH-PROFILE	Characterization of the bandwidth limits for this application.	Yes
ENVELOPE	Which envelope should the application use	Yes

Table 7 – Bandwidth Policy Criteria

9.11.2.1 LIMIT-BANDWIDTH Policy Criterion

When applied to an Application, the LIMIT-BANDWIDTH Policy Criterion is used to indicate whether there are bandwidth limits (and hence a Bandwidth Profile and Envelope) on this Application. When applied to an Application Group, it is passed on to all group members (as are all Policy Criteria), and also indicates whether or not the group has an Envelope to share bandwidth resources between group members. The criterion can have values *Enabled* and *Disabled*, and the default value is *Disabled*.

[R66] If no LIMIT-BANDWIDTH Policy Criterion is applied to a specific Application, then IP Packets associated with that Application **MUST** be treated as if LIMIT-BANDWIDTH=*Disabled* were applied.

[R67] If the Policy Criterion LIMIT-BANDWIDTH=*Disabled* is applied to an Application, all of the other Bandwidth Profile Policy Criteria **MUST** be ignored for that Application.

9.11.2.2 BANDWIDTH-PROFILE Policy Criterion

The Bandwidth Profile is the quantitative description of the allowed bandwidth for an Application. The value of the BANDWIDTH-PROFILE Policy Criterion is either a <*5-tuple*> as described in section 12.3 or *None*. *None* is the default value.

[R68] If the Policy Criterion LIMIT-BANDWIDTH=*Enabled* is assigned to an Application, the Policy Criterion BANDWIDTH-PROFILE=<*5-tuple*> **MUST** be assigned to the Application.

[R69] If no BANDWIDTH-PROFILE Policy Criterion is applied to an Application, then IP Packets associated with that Application **MUST** be treated as if BANDWIDTH-PROFILE=*None* were applied.

[R70] The BANDWIDTH-PROFILE Policy Criterion **MUST NOT** be applied to an Application Group.

The Bandwidth Profile includes a Flow identifier which is unique for each Application, so it isn't possible to apply the same Bandwidth Profile to all of the group members.

9.11.2.3 ENVELOPE Policy Criterion

The ENVELOPE Policy Criterion is used to indicate whether the Bandwidth Profile specified for an Application should reside in a Group Envelope or an Application Envelope, and the Envelope parameters. The criterion can have values *Group, None,* or a 2-tuple <$MAXIR_E$, T_E> representing the Envelope parameters (see section 12.2). The default value is *None*.

[R71] If the Policy Criterion LIMIT-BANDWIDTH=*Enabled* is assigned to an Application, the Policy Criterion ENVELOPE=*Group* or ENVELOPE=<*2-tuple*> **MUST** be assigned to the application.

If an Application is being bandwidth limited, then [R68] ensures that there is a Bandwidth Profile for the Application and [R71] ensures that the Bandwidth Profile is put into an Envelope (either a Group Envelope or an Application Envelope).

[R72] If the Policy Criterion LIMIT-BANDWIDTH=*Enabled* is assigned to an Application Group, the Policy Criterion ENVELOPE=<*2-tuple*> **MUST** be assigned to the Group.

Enabling LIMIT-BANDWIDTH for an Application Group, in effect, creates the Group Envelope and therefore specification of the Envelope parameters is required.

9.12 Policy Examples

9.12.1 Default Policy

As noted in section 9.11 every Policy Criterion except FORWARD has a default value. This means that there is, in effect, a default Policy represented by a list of Policy Criteria that only contains FORWARD=Enabled:

```
"this is the default policy",
        (FORWARD, Enabled) ; explicit
        (ENCRYPTION, Required)
        (UNDERLAY, Public)
        (CHARGE-TYPE, Flat-only)
        (BACKUP, Primary-and-Backup)
        (COS, default CoS Name)
        (LIMIT-BANDWIDTH, Disabled)
        (BANDWIDTH-PROFILE, None)
        (ENVELOPE, None)
```

9.12.2 Application Bandwidth Profiles

If an Application, app1, (not part of a group) needs to be bandwidth limited then the following Policy Criteria would be specified:

```
"application bandwidth limit",
        (FORWARD, Enabled)
        (LIMIT-BANDWIDTH, Enabled)
        (BANDWIDTH-PROFILE, <50Mbps, 50Mbps, 1, "Optimize Delay")
        (ENVELOPE, <100Mbps, 250ms>)
```

9.12.3 Group Bandwidth Profiles

If a Group, grp1, has 3 Applications, app1, app2, app3:

```
"policy to apply to grp1",
        (FORWARD, Enabled)
        (LIMIT-BANDWIDTH, Enabled)
        (ENVELOPE, <100Mbps, 250ms>)
```

If app1 and app2 are sharing bandwidth in the Group Envelope:

```
"policy to apply to app1",
        (FORWARD, Enabled)
        (LIMIT-BANDWIDTH, Enabled)
        (BANDWIDTH-PROFILE,<50Mbps, 100Mbps, 2, "Optimize Delay")
        (ENVELOPE, Group)

"policy to apply to app2",
        (FORWARD, Enabled)
        (LIMIT-BANDWIDTH, Enabled)
        (BANDWIDTH-PROFILE, <75Mbps, 100Mbps, 1 "Optimize Delay")
        (ENVELOPE, Group)
```

If app3 wants to be in its own Application Envelope:

```
"policy to apply to app3",
        (FORWARD, Enabled)
        (LIMIT-BANDWIDTH, Enabled)
        (BANDWIDTH-PROFILE, <150Mbps, 150Mbps, 1 "Optimize Delay")
        (ENVELOPE, <150Mbps, 200ms>)
```

9.13 SWVC Policy to Application Map Service Attribute

This Service Attribute provides the mapping of Policies to Ingress IP Packets that are associated with specified Applications or Groups (of Application). The value of this Service Attribute is a non-empty list of 2-tuples of the form $\langle app, pol \rangle$ where:

- *app* is an Application ID, or an Application Group ID contained in the SWVC List of Applications Service Attribute (section 9.10)
- *pol* is a Policy Name from the SWVC List of Policies Service Attribute (section 9.11).

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

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

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

Attribute Name	Summary Description	Possible Values
SWVC End Point Identifier	Identification of the SWVC End Point for management purposes	Unique Identifier String for a given SWVC End Point.
SWVC End Point UNI	Identifies the UNI that the End Point is associated with	A SD-WAN UNI Identifier
SWVC End Point List of Policy Overrides	List of Policy Criteria that have overrides at this End Point	List of Policy Criteria n-tuples>

Table 8 – Summary of SWVC End Point Service Attributes

10.1 SWVC End Point Identifier Service Attribute

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

[R73] The value of the SWVC End Point Identifier **MUST** be an Identifier String.

[R74] The value of the SWVC End Point Identifier Service Attribute **MUST** be unique among all the Service Provider SWVC End Points.

10.2 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 11.1, which serves to specify the UNI where the SWVC End Point is located. The SWVC End Point is said to be at this UNI.

10.3 SWVC End Point List of Policy Overrides Service Attribute

Policies are specified for each Application through the use of the SWVC Policy to Application Map Service Attribute (section 9.12). Those policies are normally applied at each SWVC End Point in the SD-WAN Service. There are circumstances, however, where the Subscriber requires different behavior at some End Points. Certain Policy Criteria can be overridden at an End Point using the SWVC End Point List of Policy Overrides Service Attribute. The Policy Criteria that can be overridden are identified in Table 6 and Table 7 with "Yes" in the Override column.

The value of the SWVC End Point List of Policy Overrides Service Attribute is a 2-tuple $\langle appID, polCL \rangle$ where:

- *appID* is an Application Identifier included in the SWVC List of Applications Service Attribute (section 9.10)
- *polCL* a list Policy Criteria n-tuples as described in section 9.11.

For example, it is possible that the Subscriber wants an Application "VoIP" to be forwarded at all End Points except Berlin. The Policy mapped to Application VoIP will include the criterion <*Forward, Enabled*>. However, at the Berlin End Point there can be an override:

<"VoIP", <*Forward, Disabled*>>

Another common use of the Policy override might be related to the use of Bandwidth Profiles. An application might not have a bandwidth limit except at one or two End Points, or it might have a different bandwidth limit at some End Points.

11 SD-WAN UNI (UNI) Service Attributes

The SD-WAN UNI is the demarcation between the responsibility of the Subscriber and the responsibility of the Service Provide. The UNI logically resides along the physical network connection between the Subscriber Network and the Service Provider Network. We refer to this network connection as the UNI Access Link.

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 provides IP connectivity between Subscriber networks, 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 [24] in order to achieve the greatest amount of commonality between MEF IP Services and MEF SD-WAN Services. Since this specification assumes that the UNI is composed of a single access link, it does not split the attributes across two elements as the IP Service Specification does (i.e., UNI and UNI Access Links).

Attribute Name	Summary Description	Possible Values
SD-WAN UNI Identifier	Identification of the UNI for management purposes	Unique Identifier String
SD-WAN UNI Edge Type	Indicates whether the SD-WAN Edge a Physical Device or a VNF	*Physical* or *Virtual*
SD-WAN UNI L2 Technology	Describes the underlying L2 technology for the UNI	See section 11.2
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*
SD-WAN UNI IPv4 Maximum Transmission Unit Service Attribute	Maximum size, in octets, of an IP Packet that can traverse the UNI Access Link	Integer ≥ 1280

Table 9 – Summary of SD-WAN UNI Service Attributes

11.1 SD-WAN UNI Identifier Service Attribute

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

[R75] The value for the SD-WAN UNI Identifier Service Attribute **MUST** be an Identifier String.

[R76] The value of the SD-WAN UNI Identifier Service Attribute **MUST** be unique among all UNIs in the Service Provider's network.

As an example, the Subscriber and Service Provider might agree to use "CompanyA-NY-1" as a value of the SD-WAN UNI Identifier Service Attribute and this could signify UNI #1 at the NY office of Company A.

Note that [R75] does allow two Service Providers to use the same identifier for different UNIs (one UNI per Service Provider). Of course, using globally unique identifiers for UNIs meets [R75].

11.2 SD-WAN UNI Edge Type Service Attribute

The SD-WAN Edge can be implemented as a Physical Device at the Subscriber premises or as a Virtual Network Function implemented somewhere in the network. The value of the SD-WAN Edge Type Service Attribute can be *Physical* or *Virtual*.

11.3 SD-WAN UNI L2 Technology Service Attribute

The SD-WAN UNI L2 technology Service Attribute describes the underlying network layers that carry IP Packets across the UNI. The fundamental property of the UNI is to be able to convey IP Packets between the Subscriber and the SP. This Service Attribute is relevant when the value of the SD-WAN UNI Edge Type Service Attribute is *Physical*.

The details of the immediately-lower network layer always need to be agreed and hence specified in this Service Attribute. The number of other layers that need to be specified depends on the scenario; for example, if the Service Provider supplies a physical connection to the Subscriber, then the details of the physical layer (L1) and the datalink layer (L2) need to be specified. Conversely, if the Service Provider and the Subscriber connect using an IP-Sec tunnel over the public Internet, then the details of the IP-Sec tunnel need to be agreed, but the details of how the Service Provider connects to the Internet and how the Subscriber connects to the Internet do not need to be agreed or specified as part of this attribute.

In general, sufficient parameters need to be specified to describe the responsibility of the Service Provider as viewed by the Subscriber. Anything which is entirely within the Service Provider's domain and is not visible to the Subscriber does not need to be specified. For example, if the Service Provider provides a physical Ethernet link, then the attributes of the link need to be specified, but what is connected to the Service Provider's end of the link does not. The Service Provider could connect their PE directly to the physical Ethernet connection, or they might carry the IP Packets over an intervening Carrier Ethernet access network before they reach the PE. As this is opaque to the Subscriber, it does not need to be specified.

The following L2 technologies can be used for the UNI:

11.3.1 Point-to-Point Ethernet Link

This is the simplest and most common case. The Service Provider provides a single physical point-to-point Ethernet connection to the Subscriber, over which IP Packets are carried. No VLANs are used.

In this case, the L2 Technology is Ethernet, and no additional L2 parameters are needed. However, some additional L2 parameters can be agreed if desired, for example Ethernet OAM protocols could be agreed to be used.

The only lower layer in this case is the physical layer, and here the type of Ethernet PHY needs to be specified, along with any other physical layer attributes such as auto-negotiation and the type of optical fiber.

11.3.2 Ethernet Link Aggregation Group

The UNI can be provided over an Ethernet Link Aggregation Group (LAG) based IEEE Std 802.1AX [1]. This solution can provide increased bandwidth, or increased link resiliency, or both compared to a single Ethernet link. Implementation of the LAG can include the Dynamic Resilient Network Interconnect (DRNI) specified in the 802.1AX. As with the single Ethernet link the Subscriber and the Service Provider can agree on various L2 parameters such as Ethernet OAM protocols, physical layer attributes for the Ethernet links that compose the LAG, as well as some aspects of the Link Aggregation Group.

11.3.3 802.11 Wireless LAN

Access to the SD-WAN Edge (and the SWVC End Point) can be provided over an 802.11 Wireless LAN (i.e., WiFi). The general expectation is that the Subscriber Network side of the UNI terminates in a single Subscriber device (bridge or router, usually) which provides access to the rest of the Subscriber Network. An 802.11 Wireless LAN can be used for this purpose, but it can also provide direct access for multiple Wireless Subscriber devices to access the SD-WAN UNI without going through a Subscriber-side gateway.

11.4 SD-WAN UNI IPv4 Connection Addressing Service Attribute

The SD-WAN UNI IPv4 Connection Addressing Service Attribute specifies how IPv4 addresses are allocated to the devices connected to the UNI Access Link. 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 by the devices connected to the UNI Access Link and IPv4 is disabled on the link. Note that in this case IPv6 connection addresses are needed.

[R77] The SD-WAN UNI IPv4 Connection Addressing Service Attribute and the SD-WAN UNI Interface IPv6 Connection Addressing Service Attribute (section 11.5) **MUST NOT** both have the value *None*.

If the IPv4 Connection Addressing is *DHCP*, then DHCP is used by the Subscriber devices to request IPv4 addresses in a given subnet from the Service Provider as described in RFC 2131 [6] and RFC 2132 [7]. The Service Provider device acts as the DHCP server and the Subscriber devices act as the DHCP clients.

[R78] 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 router address.

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

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

- 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)
  - Subscriber IPv4 Address (IPv4 address or *Not Specified*)
  - Reserved Prefixes List (List of IPv4 Prefixes, possibly empty)
- 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)
- Reserved Prefixes List (List of IPv4 Prefixes, possibly empty)

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.

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.

For the primary subnet, if IPv4 Connection Addressing is *Static*, the Subscriber's IPv4 address can also be specified.

A list (possibly empty) of reserved IP Prefixes can be specified (section 9.9); these specify IP addresses that are not available for the Subscriber to assign statically. If DHCP is used, the IPv4 address range from which addresses are dynamically assigned is taken from this pool of reserved addresses.

When IPv4 Connection Addressing is *Static*, the Service Provider's addresses are assumed to also be the router/gateway addresses, via which the Subscriber can route traffic over the UNI Access Link.

[R79] If 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.

[R80] If the SD-WAN UNI IPv4 Connection Addressing is *Static*, and the Primary Subnet Subscriber IPv4 Address is an IPv4 address, it **MUST** be an IPv4 address within the Connection Primary IPv4 Prefix, that is different to the Primary Subnet Service Provider IPv4 Addresses.

[R81] If the SD-WAN UNI IPv4 Connection Addressing is *DHCP*, the Primary Subnet Subscriber IPv4 Address **MUST** be *Not Specified*.

[R82] IP Prefixes contained in the Primary Subnet Reserved Prefixes List **MUST** contain a subset of IPv4 addresses that are within the Connection Primary IPv4 Prefix.

[R83] If the SD-WAN UNI IPv4 Connection Addressing is *DHCP*, addresses that are dynamically assigned by DHCP within the Connection Primary IPv4 Prefix **MUST** be taken from within one of the IP Prefixes in the Primary Subnet Reserved Prefixes List.

[R84] IP Prefixes contained in the Reserved Prefixes List in an entry in the Secondary Subnet List **MUST** contain a subset of IPv4 addresses that are within the Connection Secondary IPv4 Prefix for that entry in the Secondary Subnet List.

[R85] If the SD-WAN UNI IPv4 Connection Addressing is *DHCP*, addresses that are dynamically assigned by DHCP within the Connection Secondary IPv4 Prefix for an entry in the Secondary Subnet List **MUST** be taken from within one of the IP Prefixes in the Reserved Prefixes List for that entry in the Secondary Subnet List.

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 reserved for dynamic assignment.

[R86] If the SD-WAN UNI IPv4 Connection Addressing is *DHCP* or *Static*, the Subscriber **MUST NOT** statically assign any of the following for use on the UNI Access Link by Subscriber devices:

- 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 IPv4 address within the Connection Primary IPv4 Prefix other than the Primary Subnet Subscriber IPv4 Address, unless it is *Not Specified*.
- 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 an IP Prefix in the Primary Subnet Reserved Prefixes List or within the Reserved Prefixes List for an entry in the Secondary Subnet List.

11.5 SD-WAN UNI IPv6 Connection Addressing Service Attribute

The SD-WAN UNI IPv6 Connection Addressing specifies how IPv6 addresses are allocated to the devices connected to the UNI. It is one of the five values *None*, *DHCP*, *SLAAC*, *Static* or *LL-only*, plus in the case of *DHCP*, *SLAAC* or *Static*, some additional parameters. If the IPv6 Connection

Addressing is *None*, no IPv6 addresses are used by the devices connected to the UNI and IPv6 is disabled on the link. Note that in this case IPv4 connection addresses are needed (see [R77]).

If the IPv6 Connection Addressing is not *None*, then IPv6 link local addresses are used on the UNI. If the value is *LL-only*, these are the only IPv6 addresses used on the UNI.

If the 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 [13]. The Service Provider device acts as the DHCP server and the Subscriber devices act as the DHCP clients.

[R87] When the IPv6 Connection Addressing 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 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 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 [15]. The Router Advertisements that convey the IP Prefix can also be used to determine the subnet mask 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 mask length between 0 and 127, in bits)
    - Service Provider IPv6 Addresses (Non-empty list of IPv6 addresses)
    - Reserved Prefixes List (List of IPv6 Prefixes, possibly empty)
- For *Static*, Subscriber IPv6 Address (IPv6 address or *Not Specified*)

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.

If Static addressing is used, the Subscriber's IPv6 address can also be specified.

A list (possibly empty) of reserved IP Prefixes can be specified (section 9.9); these specify IP addresses that are not available for the Subscriber to assign statically. If DHCP is used, the IPv6 address range from which addresses are dynamically assigned is taken from this pool of reserved addresses.

When Static addressing is used, the SP's addresses are assumed to also be the router/gateway addresses, via which the Subscriber can route traffic over this UNI.

[R88] If the SD-WAN UNI IPv6 Connection Addressing is *Static*, *DHCP* or *SLAAC*, for each subnet, there **MUST** be only one Service Provider IPv6 Address specified.

[R89] If 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.

[R90] If the SD-WAN UNI IPv6 Connection Addressing is *Static*, and the Subscriber IPv6 Address is an IPv6 address, it **MUST** be an IPv6 address within the Connection IPv6 Prefix for the first entry in the Subnet List, that is different to the Service Provider IPv6 Addresses for that entry.

[R91] If the SD-WAN UNI IPv6 Connection Addressing is *DHCP* or *SLAAC*, the Subscriber IPv6 Address **MUST** be *Not Specified*.

[R92] For a given entry in the Subnet List, IP Prefixes contained in the Reserved Prefixes List **MUST** contain a subset of IPv6 addresses that are within the Connection IPv6 Prefix for that entry.

[R93] If 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 the Reserved Prefixes List for one of the entries in the Subnet List.

[R94] If the SD-WAN UNI IPv6 Connection Addressing is *SLAAC*, the IP Prefix advertised by the Service Provider as described in RFC 4862 [15] 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 addresses reserved for dynamic assignment.

[R95] If 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 IPv6 address within the Connection IPv6 Prefix for the first entry in the Subnet List other than the Subscriber IPv6 Address, unless it is *Not Specified*.
- 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 an IP Prefix in the Reserved Prefixes in an entry in the Subnet List.

11.6 SD-WAN UNI IP Maximum Transmission Unit (MTU) Service Attribute

The SD-WAN UNI IP Maximum Transmit Unit (MTU) Service Attribute is an integer ≥ 1280 that specifies the maximum length in octets of IP Packets that can be conveyed across the UNI. It is used to determine the maximum value of the SWVC MTU (see section 9.6) for the SWVC associated with the UNI, and also affects IP Control Protocol Packets at the UNI.

RFC 791 [2] specifies the minimum MTU for IPv4 Packets as 68 octets; however, it also requires that all devices can handle a packet of length 576 octets (possibly fragmented). RFC 2460 [9] specifies the minimum MTU for IPv6 Packets as 1280 octets. For SD-WAN, this value is the required minimum value in all cases.

[R96] The SD-WAN UNI IP MTU **MUST** be greater than or equal to 1280 octets.

If a Service Provider transmits IP Control Protocol Packets across a UNI, they cannot exceed the SD-WAN UNI IP MTU. Similarly, Ingress IP Control Protocol Packets with a length greater than the SD-WAN UNI IP MTU can be discarded by the Service Provider, even if the corresponding protocol is normally peered. Note that the corresponding requirements for IP Data Packets can be found in section 9.6.

[R97] Egress IP Control Protocol Packets **MUST** have a length less than or equal to the value of the SD-WAN UNI IP MTU Service Attribute.

[R98] Ingress IP Control Protocol Packets with a length less than or equal to the value of the SD-WAN UNI IP MTU Service Attribute **MUST NOT** be discarded due to their length.

[O5] Ingress IP Control Protocol Packets with a length strictly greater than the value of the SD-WAN UNI IP MTU Service Attribute **MAY** be discarded.

12 Bandwidth Profiles

Bandwidth Policies are applied to limit data rate of IP Packets associated with an Application. Bandwidth Policies are based on Bandwidth Profiles, Bandwidth Profile Flows, and Bandwidth Profile Envelopes.

12.1 Bandwidth Profiles and Bandwidth Profile Flows

A Bandwidth Profile is a specification of the temporal properties of a sequence of IP Packets at a UNI. The sequence of IP Packets to which a Bandwidth Profile is applied is called a Bandwidth

Profile Flow (BWP Flow) and in the case of SD-WAN the Bandwidth Profile Flow is the sequence of IP Packets associated with an Application.

The effect of applying a Bandwidth Profile to a Bandwidth Profile Flow is that each IP Packet in the "flow" can experience one of three outcomes:

1. The IP Packet can be discarded
2. The IP Packet can be forwarded on the SWVC immediately
3. The IP Packet can be delayed for a short time and then forwarded on the SWVC

How the Service Provider implements the bandwidth limit is beyond the scope of this specifications, but the common approaches are through the use of a token bucket policer (as described in RFC 2698 [11] and MEF 41 [22]) or a shaper. If a policer is used, then outcomes #1 and #2 are possible, a packet either meets the rate criteria and is forwarded or it doesn't, and it is dropped. This approach prioritizes delay and delay variation over throughput. Alternatively, if a shaper is used, all three outcomes are possible. If the flow exceeds the rate limit and the shaper cannot buffer additional packets, the packet is discarded. Otherwise the packet is buffered and transmitted when the channel is available which could be immediately or after a "short" delay. This approach prioritizes throughput over delay and delay variation. See, also, sections 12.4 and 12.5 for more details about the behavior of Bandwidth Profiles and handling of Packet Bursts.

12.2 Bandwidth Profile Envelopes

Bandwidth Profile Flows are assigned to Bandwidth Profile Envelopes (BWP Envelopes). Assigning multiple Bandwidth Profile Flows to the same Bandwidth Profile Envelope allows those flows to share bandwidth resources. Each Bandwidth Profile Envelope has two parameters[11]:

- The Envelope Maximum Information Rate (denoted $MaxIR_E$) in bits per second. This is the limit on the total aggregate information rate of traffic across all Bandwidth Profile Flows in the Envelope.
- The Envelope IR Time (denoted T_E) in milliseconds. This is the time period over which average Information Rates are calculated and thus it limits the size of a burst.

12.3 Bandwidth Profile Parameters

A Bandwidth Profile provides the means to describe the bandwidth limit on the IP Packet flow associated with an Application. It is a 5-tuple $\langle FlowID, CIR, MaxIR,\ Weight, Burst\rangle$ where:

- *FlowID* is a unique integer between 1 and *n*, where *n* is the number of BWP Flows in the BWP Envelope.
- *CIR* is the Committed Information Rate in bits per second
- *MaxIR* is the Maximum Information Rate in bits per second

[11] In MEF 61 [24] the Envelope includes a third parameter, the list of Bandwidth Profile Flows. We don't include this since it is directly based on the Applications and/or Application Group.

- *Weight* is an integer greater than 0 that represents the weight of this Bandwidth Profile Flow relative to other Bandwidth Profile Flows in the same Envelope.
- *Burst* is the burst behavior which can be either *Optimize-Delay* or *Optimize-Throughput*

In a given BWP Envelope, the CIR, MaxIR, Weight and Burst Behavior for the Bandwidth Profile Flow with Flow Identifier *i* are denoted CIR_i, $MaxIR_i$, $Weight_i$ and $Burst_i$ respectively. Note that the Flow Identifier of a BWP Flow is used only as an identifier and does not imply any particular ordering or prioritization between the flows.

[R99] For a BWP Flow *i* contained in a BWP Envelope, $MaxIR_i$ **MUST** be greater than or equal to CIR_i.

[R100] The sum of the Committed Information Rates (*CIR*s) for all of the BWP Flows in an Envelope **MUST** be less than or equal to the total information rate for the Envelope ($MaxIR_E$).

A description of how the Bandwidth Profile is used to limit bandwidth in a stream of IP Packets and a further discussion of Packet Bursts are provided in the following two sections (12.4 and 12.5) respectively.

12.4 Bandwidth Profile Behavior

The desired behavior described by a Bandwidth Profile is specified in terms of average information rates. The average information rate of a stream of IP Packets over a given time is defined to be the sum of the lengths of the IP Packets in the stream (in octets), multiplied by 8, and divided by the time in seconds. In other words, if N is the number of IP Packets in a stream of IP Packets that passes a reference point (e.g. a UNI) during a time interval of duration *t*, and L_p is the length of the p^{th} such IP Packet, the average information rate is:

$$IR = 8\frac{\sum_{p=1}^{N} L_p}{t}$$

Recall that an IP Packet is defined to be from the start of the IP Version field to the end of the IP data field, inclusive, and the length is therefore calculated accordingly.

Defining the average information rate in this way means that bursts of IP Packets are possible; for instance, a burst of IP Packets might pass the reference point at a rate much higher than the average information rate, but for a time much shorter than *t*, provided that IP packets pass the reference point at a rate lower than the average information rate for the remainder of *t*. The maximum size of such a burst is constrained by the time interval *t*.

Informally, the behavior of a Bandwidth Profile meter is as follows:

- For each BWP Flow *i* in a BWP Envelope, allocate up to CIR_i to that flow, if necessary (i.e. if at least that much traffic for the BWP Flow is arriving at the reference point).
- Determine how much available bandwidth remains, by subtracting the amounts allocated in step one from the $MaxIR_E$ for the Envelope.

- Allocate this remainder across all the BWP Flows, such that:
    - No more is allocated to a given BWP Flow than the amount of traffic arriving for that flow at the reference point.
    - No more is allocated to a given BWP Flow than the *MaxIR* for that flow.
    - Taking into account the amount allocated in the first step above, the ratio of bandwidth allocated to contended flows is equal to the ratio of their Weights.

This behavior ensures that traffic is divided fairly between the BWP Flows according to their relative weights.

The behavior is captured in the following requirements.

[R101] The average information rate for IP Packets in BWP Flow i over any time interval of duration T_E that are declared conformant by the Bandwidth Profile meter **MUST** be at least the lower of the average information rate for IP Packets in BWP Flow i over that time interval that are received by the Bandwidth Profile meter, and CIR_i.

[O6] IP Packets in BWP Flow i **MAY** be declared non-conformant in order to ensure that the average information rate for such packets over any time interval of duration T_E that are declared conformant by the Bandwidth Profile meter is at most $MaxIR_i$.

[O7] IP Packets in BWP Flows contained in a given BWP Envelope **MAY** be declared non-conformant in order to ensure that the average information rate for all such packets over any time interval of duration T_E that are declared conformant by the Bandwidth Profile meter is at most $MaxIR_E$.

[R102] If IP Packets in BWP Flows contained in a given BWP Envelope are declared non-conformant per [O7], this **MUST** be done in such a way that [R99] is met for each such BWP Flow, and the ratio of the average information rates over any time interval of duration T_E for packets that are declared conformant across all BWP Flows in the Envelope is equal to the ratio of the weights for those BWP Flows, except when the average information rate for IP Packets in a BWP Flow over that time interval that are received by the Bandwidth Profile meter is less than the ratio of weights would otherwise indicate.

Note that the above requirements specify constraints over any time interval of duration T_E – i.e., they suggest a ‘sliding window’. Constraining bandwidth using a fixed, recurring, window can have the effect of allowing double the amount of traffic as intended, as described in MEF 23.2 [20] Appendix H.2.

[R103] An IP Packet in a BWP Flow **MUST** be declared conformant unless it meets one of the conditions in requirements [O6], [O7], or [R100].

[R104] IP Packets that are declared non-conformant by a Bandwidth Profile meter **MUST** be discarded.

Note that IP Packets discarded as a result of the above requirements are not considered Qualified IP Packets, and hence do not contribute to any Packet Loss Ratio objective that might be specified in the SLA. Conversely, IP Packets that are declared conformant by the Bandwidth Profile meter do constitute Qualified IP Packets (provided they meet the other criteria specified in section 9.5.2), and hence cannot be discarded without risk of failing to meet a Packet Loss Ratio objective.

[D4] When IP Packets are discarded as a result of applying a Bandwidth Profile, the SP **SHOULD** use techniques such as Weighted Random Early Detect (WRED) to determine which IP Packets to discard.

12.5 Packet Bursts

When a burst of packets is received – that is, a number of IP Packets in quick succession such that the IR over a short time exceeds the average IR over T_E – it can be beneficial to delay some of the packets such that the burst is "smoothed out". This is typically implemented by queuing packets (up to some maximum) and servicing the queue at the desired rate – in other words, by shaping.

The benefits of this "smoothing" behavior are twofold: firstly, it means that the aggregate of all traffic flows across the SPs network is more predictable, and hence the network can be implemented with smaller buffers; and secondly, the overall throughput for a given flow can be improved. The latter comes about because of the particular interaction between the behavior of TCP and round-trip time – see, for example, Appendix G of MEF 23.2 [20] for analysis of this.

The disadvantage of "smoothing" bursty traffic is that packet delay and inter-packet delay variation are adversely affected. If packets are queued for transmission, then the average end-to-end delay will of course increase. Additionally, as different packets can be queued for different lengths of time, the delay variation is also increased.

To accommodate this, the final parameter for each BWP Flow in a BWP Envelope is the Burst Behavior. If the BWP Flow comprises traffic that is sensitive to delay and delay variation, such as voice or video traffic, then the Burst Behavior can be set to *Optimize-Delay*. Conversely, if for example, the BWP Flow comprises predominantly TCP traffic or is more sensitive to loss, the Burst Behavior can be set to *Optimize-Throughput*.

There are no specific requirements specifically relating to the Burst Behavior parameter; it is included as a guide for the SP as to how to implement the Bandwidth Profile behavior so as to meet the Subscriber's needs and provide them with a good quality of experience; for example, whether to apply shaping, policing or a combination of these to the BWP Flow.

[O8] The SP **MAY** delay certain IP Packets in a given BWP Flow before applying the Bandwidth profile meter, in order to increase the number of IP Packets in the BWP Flow that are declared conformant.

Note that such a delay is included in the One-way Packet Delay (section **Error! Reference source not found.**) and can impact any delay-related Performance Metrics that are monitored for the SWVC.

Whether packets are delayed or not, they cannot be re-ordered.

[R105] The application of a Bandwidth Profile **MUST NOT** change the order of IP Packets within a given BWP Flow.

13 Performance Metrics

This section provides the formal description of each of the six Performance Metrics that can be included in a Class of Service definition for a MEF 3.0 SD-WAN Service:

- One-way Packet Delay Percentile
- One-way Mean Packet Delay
- One-way Inter-Packet Delay Variation
- One-way Packet Delay Range
- One-way Packet Loss Ratio
- Service Uptime

Four of these Performance Metrics are based on the definition of One-way Packet Delay which is described first (section 13.1). The definitions then follow starting in section 13.2.

13.1 One-way Packet Delay

The one-way packet delay for an IP Data Packet that flows between two UNIs, UNI_i and UNI_j is defined as the time elapsed from the reception of the first bit of the packet at UNI_i until the transmission of the last bit of the first corresponding egress packet at UNI_j. If the packet is erroneously duplicated as it traverses the network, the delay is based on the first copy that is delivered.

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

One-way packet delay is used in the definition of several Performance Metrics as defined below.

13.2 One-way Packet Delay Percentile Performance Metric

The One-way Packet Delay Performance Metric is the maximum, over all the ordered End Point pairs in a given Performance Group, *PG*, of the p_{th} percentile of one-way packet delay for Qualified Packets for a given ordered End Point pair, a given CoS Name, and a given time period T_k. This Performance Metric has one additional parameter, *p*, the Packet Delay percentile.

[R106] If One-way Packet Delay Percentile is specified for a Class of Service, *C*, with Packet Delay Percentile, *p*, then during time period T_k it **MUST** be defined as follows for each Performance Group:

- Let $\delta(T_k, C, PG, \langle i, j\rangle, p)$ represent the p^{th} percentile of one-way packet delay for all Qualified Packets for the time period T_k, CoS Name C, and ordered pair of End Points $\langle i, j\rangle$ in PG that ingress at End Point i and are delivered to End Point j. If there are no such packets, then let $\delta(T_k, C, PG, \langle i, j\rangle, p) = 0$.
- Then the One-way Packet Delay Percentile Performance Metric $d(T_k, C\ PG, p)$ is the maximum of the values for $\delta(T_k, C, PG, \langle i, j\rangle, p)$ for all ordered pairs of End Points $\langle i, j\rangle$ in PG.

[R107] If the Performance Objective 3-tuple:

<"One-way Packet Delay Percentile", *p*, *obj*>

is specified for a Class of Service C and a Performance Group PG, then the Performance Objective **MUST** be considered met for time period T_k if $d(T_k, C\ PG, p) \leq obj$.

13.3 One-way Mean Packet Delay Performance

The One-way Mean Packet Delay Performance Metric is the maximum, over all of the ordered End Point pairs in a given Performance Group, PG, of the arithmetic mean of one-way packet delay for Qualified Packets for a given ordered End Point pair, a given CoS Name, and a given time period T_k. This Performance Metric has no additional parameters.

[R108] If One-way Mean Packet Delay is specified for a Class of Service, C, then during time period T_k it **MUST** be defined as follows for each Performance Group:

- Let $\mu(T_k, C, PG, \langle i, j\rangle)$ represent the mean of one-way packet delay for all Qualified Packets for the time period T_k, CoS Name C, and ordered pair of End Points $\langle i, j\rangle$ in PG that ingress at End Point i and are delivered to End Point j. If there are no such packets the let $\mu(T_k, C, PG, \langle i, j\rangle) = 0$.
- Then the One-way Mean Packet Delay Performance Metric $u(T_k, C\ PG)$ is the maximum of the values for $\mu(T_k, C, PG, \langle i, j\rangle)$ for all ordered pairs of End Points $\langle i, j\rangle$ in PG.

[R109] If the Performance Objective 3-tuple: <"One-way Mean Packet Delay", , *obj*> is specified for a Class of Service C and a Performance Group PG, then the Performance Objective **MUST** be considered met for time period T_k if $u(T_k, C\ PG) \leq obj$.

13.4 One-way Inter-Packet Delay Variation Performance Metric

The One-way Inter-Packet Delay Variation Performance Metric is the maximum, over all of the ordered End Point pairs in a given Performance Group, PG, of the v^{th} percentile of differences between the one-way packet delays of Qualified Packets that arrive at times specified by a given interval τ, for a given ordered End Point pair, a given CoS Name, and a given time period T_k. This

Performance Metric has two additional parameters, v, the Inter-Packet Delay Variation percentile, and τ, the difference in time of arrival of packets.

[R110] If One-way Inter-Packet Delay Variation is specified for a Class of Service, C, then during time period T_k it **MUST** be defined as follows for each Performance Group:

- Let $a(P, Q, T_k, C, PG, \langle i, j \rangle)$ be the absolute difference between the one-way packet delay of packet P and the one-way packet delay of packet Q where P and Q are Qualified Packets for the time period T_k, CoS Name C, and ordered pair of End Points $\langle i, j \rangle$ in PG, P and Q ingressing at End Point i, in that order, and egressing at End Point j.
- Let $\omega(T_k, C, PG, \langle i, j \rangle, \tau, v)$ represent the v^{th} percentile of the values of $a(P, Q, T_k, C, PG\ \langle i, j \rangle)$ for all packets P and Q where the difference between the time packet P arrives at End Point i and the time packet Q arrives at End Point i is equal to τ. If there are no such packets, let $\omega(T_k, C, PG, \langle i, j \rangle, \tau, v) = 0$.
- Then the One-way Inter-Packet Delay Variation Performance Metric $w(T_k, C, PG, \tau, v)$ is the maximum of all of the values of $\omega(T_k, C, PG, \langle i, j \rangle, \tau, v)$ for all ordered pairs of End Points $\langle i, j \rangle$ in PG.

The definition of IPDV can be thought of as being determined by selecting pairs of packets, P and Q, whose arrival time differs by τ and then calculating the absolute difference in their one-way packet delays. Note that if P takes longer than Q, the difference in one-way packet delay will be negative, whereas if P takes less time than Q, the difference will be positive. However, since the absolute value of the difference is used in the calculation, these cases are treated identically.

[R111] If the Performance Objective 3-tuple:

<"One-way Inter-Packet Delay Variation", <τ, v>, *obj*>

is specified for a Class of Service C and a Performance Group PG, then the Performance Objective **MUST** be considered met for time period T_k if $w(T_k, C\ PG, \tau, v) \leq obj$.

13.5 One-way Packet Delay Range Performance Metric

The One-way Packet Delay Range Performance Metric is the maximum, over all of the ordered End Point pairs in a given Performance Group, PG, of the r^{th} percentile of the one-way packet delay and the minimum one-way packet delay for Qualified Packets for a given ordered End Point pair, a given CoS Name, and a given time period T_k. This Performance Metric has one additional parameter, r, the Packet Delay Range percentile.

[R112] If One-way Packet Delay Range is specified for a Class of Service, C, then during time period T_k it **MUST** be defined as follows for each Performance Group:

- Let $\gamma(T_k, C, PG, \langle i, j \rangle, r)$ represent the rth percentile of one-way packet delay for all Qualified Packets for the time period T_k, CoS Name C, and ordered pair of End Points $\langle i, j \rangle$ in *PG* that ingress at End Point *i* and are delivered to End Point *j*. If there are no such packets the let $\gamma(T_k, C, PG, \langle i, j \rangle, r) = 0$.

- Let $m(T_k, C, PG, \langle i, j \rangle)$ represent the minimum one-way packet delay for all Qualified Packets for the time period T_k, CoS Name *C*, and ordered pair of End Points $\langle i, j \rangle$ in *PG* that ingress at End Point *i* and are delivered to End Point *j*. If there are no such packets the let $m(T_k, C, PG, \langle i, j \rangle) = 0$.
- Then the One-way Packet Delay Range Performance Metric $g(T_k, C, PG, r)$ is the maximum of the values of:

$$\gamma(T_k, C, PG, \langle i, j \rangle, r) - m(T_k, C, PG, \langle i, j \rangle)$$

for all ordered pairs of End Points $\langle i, j \rangle$ in *PG*.

[R113] If the Performance Objective 3-tuple:
<"One-way Packet Delay Range", *r*, *obj*>
is specified for a Class of Service *C* and a Performance Group *PG*, then the Performance Objective **MUST** be considered met for time period T_k if $g(T_k, C\ PG, r) \leq obj$.

13.6 One-way Packet Loss Ratio Performance Metric

The One-way Packet Loss Ratio Performance Metric is the maximum, over all of the ordered End Point pairs in a given Performance Group, *PG*, of the ratio of lost packets to transmitted packets for Qualified Packets for a given ordered End Point pair, a given CoS Name, and a given time period T_k. This Performance Metric has no additional parameters.

[R114] If One-way Packet Loss Ratio is specified for a Class of Service, *C*, then during time period T_k it **MUST** be defined as follows for each Performance Group:

- Let $I(T_k, C, PG, \langle i, j \rangle)$ be the number of Qualified Packets for the time period T_k, CoS Name *C*, and ordered pair of End Points $\langle i, j \rangle$ in *PG* that are received at End Point *i*.
- Let $J(T_k, C, PG, \langle i, j \rangle)$ be the number of unique (not duplicated) Qualified Packets for the time period T_k, CoS Name *C*, and ordered pair of End Points $\langle i, j \rangle$ in *PG* that are transmitted at End Point *j*.
- Define $f(T_k, C, PG, \langle i, j \rangle) = \frac{I(T_k, C\ PG\ \langle i, j \rangle) - J(T_k, C\ PG\ \langle i, j \rangle)}{I(T_k, C\ PG\ \langle i, j \rangle)}$ if $I(T_k, C, PG, \langle i, j \rangle) > 0$ and 0 otherwise.
- Then the One-way Packet Loss Ratio Performance Metric $F(T_k, C, PG)$ is the maximum of all of the values of $f(T_k, C, PG, \langle i, j \rangle)$ for all ordered pairs of End Points $\langle i, j \rangle$ in *PG*.

The Packet Loss Ratio is usually expressed as a percentage.

Note that per the definition above, packets that are eventually delivered are not considered lost, no matter how long the packet delay is.

[R115] If the Performance Objective 3-tuple: <“One-way Packet Loss Ratio”, , *obj*> is specified for a Class of Service C and a Performance Group PG, then the Performance Objective **MUST** be considered met for time period T_k if $F(T_k, C\ PG) \leq obj$

Note also that RFC 7680 [16] defines a metric for one-way loss of packets across Internet paths that is similar to the definition of Packet Loss Ratio in this specification. It builds on notions introduced and discussed in the IP Performance Metrics (IPPM) Framework document, RFC 2330 [8].

13.7 Service Uptime Performance Metric

The Service Uptime Performance Metric 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. This Performance Metric has no additional parameters.

[R116] If Service Uptime is specified for a Class of Service, C, then during time period T_k it **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 $U(T_k) = \frac{T-\left(M(T_k)+O(T_k)\right)}{T-M(T_k)}$

Note that the value T used in the definition of the Service Uptime is the second element of the SWVC Performance Monitoring Time Service Attribute (see section 9.4).

Service Uptime is usually expressed as a percentage.

[R117] If Service Update is specified for a Class of Service, C, the Subscriber and the Service Provider **MUST** agree on the definition of an outage, including when an outage starts and ends.

[R118] If the Performance Objective 3-tuple: <“Service Uptime”, , *obj*> is specified for a Class of Service C, then the Performance Objective **MUST** be considered met for time period T_k if $U(T_k) \geq obj$

14 Central Administration

Central Administration is one of the defining features of SD-WAN.

The Subscriber is able to manage the behavior and performance of a geographically dispersed network, even with localized needs and policies, without having to interact with individual network elements.

Central administration provides more agility (all changes and configurations, regardless of scope, need to be commanded in only one place or via one interface) at a lower cost (staff can concentrate on determining the best policy and network usage, not logging on to individual network elements to implement changes in brittle, command line configuration).

[R119] The Service Provider **MUST** provide the Subscriber with one central point of administration for the entire SD-WAN.

[D5] The Service Provider **SHOULD** provide the Subscriber with an API that supports all central management functions.

[O9] The Service Provider **MAY** provide the subscriber with a web portal for administration; this is a popular option for many subscribers who do not have particularly large networks or specialized requirements.

The details of administration will not be a subject of this version of this specification, but see Appendix B for relevant MEF work in this area.

15 References

[1] IEEE Std 802.1AX – 2014, *IEEE Standard for Local and metropolitan area networks – Link Aggregation*, December 2014

[2] Internet Engineering Task Force RFC 791, *Internet Protocol*, September 1981

[3] Internet Engineering Task Force RFC 1191, *Path MTU Discovery*, November 1990

[4] Internet Engineering Task Force RFC 1981, *Path MTU Discovery for IP version 6*, August 1996

[5] Internet Engineering Task Force RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, March 1997

[6] Internet Engineering Task Force RFC 2131, *Dynamic Host Configuration Protocol*, March 1997

[7] Internet Engineering Task Force RFC 2132, *DHCP Options and BOOTP Vendor Extensions*, March 1997

[8] Internet Engineering Task Force RFC 2330, *Framework for IP Performance Metrics*, May 1998

[9] Internet Engineering Task Force RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*, December 1998

[10] Internet Engineering Task Force RFC 2579, *Textual Conventions for SMIv2*, April 1999

[11] Internet Engineering Task Force RFC 2698, *A Two Rate Three Color Marker*, September 1999

[12] Internet Engineering Task Force RFC 3260, *New Terminology and Clarifications for Diffserv*, April 2002

[13] Internet Engineering Task Force RFC 3315, *Dynamic Host Configuration Protocol for* IPv6 (DHCPv6), July 2003

[14] Internet Engineering Task Force RFC 4821, *Packetization Layer Path MTU Discovery*, March 2007

[15] Internet Engineering Task Force RFC 4862, *IPv6 Stateless Address Autoconfiguration*, September 2007

[16] Internet Engineering Task Force RFC 7680, *A One-Way Loss Metric for IP Performance Metrics (IPPM)*, January 2016

[17] Internet Engineering Task Force RFC 8174, *Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words*, May 2017

[18] MEF 4, *Metro Ethernet Network Architecture Framework – Part 1: Generic Framework*, May 2004

[19] MEF 10.3, *Ethernet Service Attributes, Phase 3*, August 2016

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

[21] MEF 26.2, *External Network Network Interfaces (ENNI) and Operator Service Attributes*, August 2016

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

[23] MEF 51, *OVC Services Definitions*, August 2015

[24] MEF 61, *IP Service Attributes for Subscriber IP Services*, April 2018

[25] MEF 62, *Managed Access E-Line Service Implementation Agreement,* May 2018

Appendix A SD-WAN Architectural Framework (Informative)

SD-WAN Service are sold to Subscribers by SD-WAN Service Providers. In many cases the Subscriber doesn't have visibility to anything other than the SD-WAN UNI (UNI), but in other cases the SD-WAN Subscriber's visibility extends further into the network.

Regardless, SD-WAN Services are built on a framework that contains a number of components and organizations. This section provides an overview of that framework and assigns names to the various components that can be used in discussions, negotiations, and agreements associated with SD-WAN.

The framework is shown in the following diagram. The following sections include pointers to the relevant sections in this specification for components that are described elsewhere and an informal description for components that are not described elsewhere in the document. This diagram represents one Subscriber site and is, in effect, mirrored at each other site.

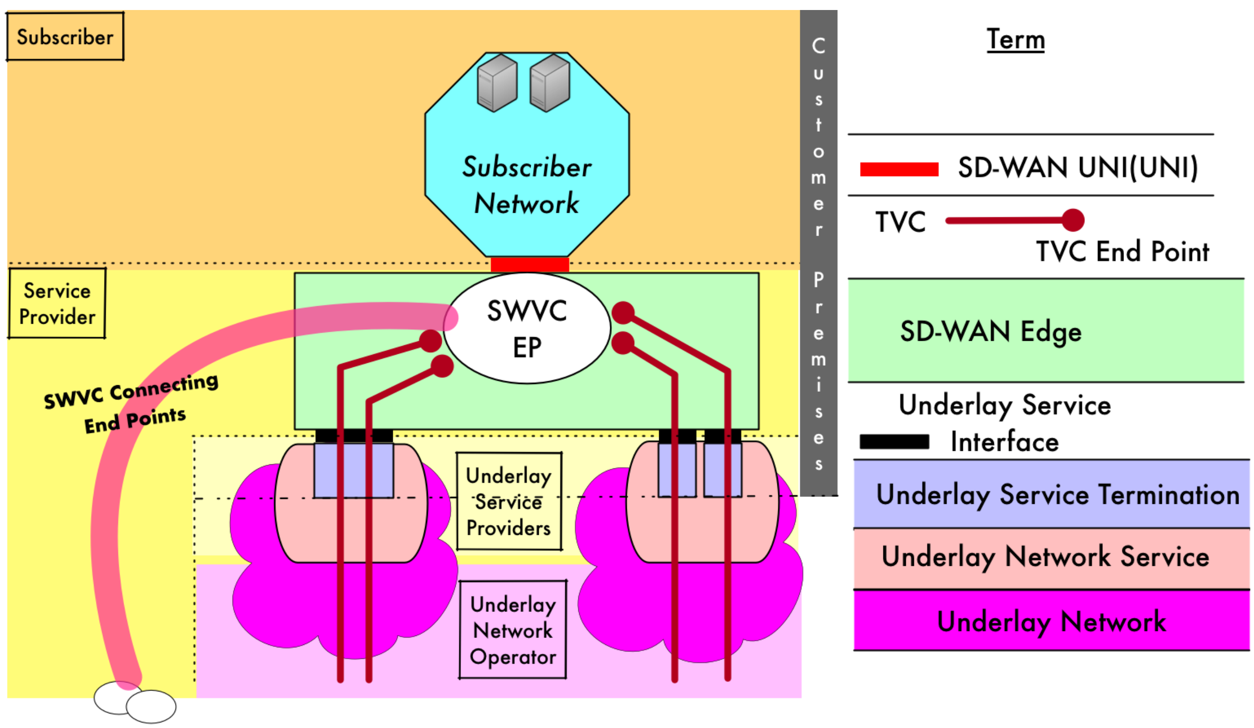

Figure 6 – SD-WAN Architectural Components

A.1 Underlay Network

See section 7.6.

A.2 Underlay Network Service

See section 7.7.

A.3 Underlay Service Termination

The access connection terminates at the Customer Premises in an Underlay Service Termination (purple rectangle) device which can be a PON ONT, DSL Modem, T1 CSU, LTE Modem, Cable Modem, router, NID, etc. The device that is appropriate to the Underlay Service and access connection. The user side of the Underlay Service Termination, the Underlay Service Interface is always an Ethernet. For example, if the Underlay Network Service is a Carrier Ethernet Service, the Underlay Service Termination is a “NID” and the Underlay Service Interface is the Carrier Ethernet Service UNI. The Interface provides the demarcation of responsibility between the Underlay Service Provider and the organization that procured the Underlay Service (SD-WAN Service Provider or Subscriber). These interfaces connect into the SD-WAN Edge.

A.4 Tunnel Virtual Connection (TVC)

See section 7.8.

A.5 SD-WAN Edge

See sections 7.11, 7.510.

A.6 SD-WAN UNI (UNI)

See sections 7.3 and 11.

A.7 Subscriber Network (SN)

See sections7.1 and 7.2.

A.8 SD-WAN Virtual Connection

See sections 7.4, 7.5, 9, and 10.

Appendix B SD-WAN and LSO (Informative)

As noted in section 14, central administration is a defining characteristic of SD-WAN, and all administration should be available via programmatic interfaces.

The SD-WAN market and its needs are evolving, and the list of required functions will remain dynamic for some time, but suggested candidates for required functionality currently include:

- Creating a new SWVC
- Modifying an existing SWVC
- Setting/modifying/deactivating/removing Policies
- Setting/modifying/deactivating/removing Application definitions

- Obtaining operational information - i.e., the state of connections, how packets are being routed (especially important if there are cost implications of different routing, some of which may be necessary to maintain performance)

The MEF's Multi-Vendor SD-WAN project is actively engaged in determining how SD-WAN central administration can be assisted by use of the MEF's Lifecycle Service Orchestration reference points.

A proposed mapping of SD-WAN components onto the LSO Reference architecture is shown in Figure 7. Because this specification describes an SD-WAN Service as agreed between a Subscriber and their Service Provider, the functionality described herein would most likely be across the Cantata and Allegro reference points. Future versions of this specification will describe those in usable detail.

Future versions of this specification may also describe other relationships – for example, between a Service Provider and its partners, or give more detail on Underlay provided by the Subscriber. As a result, the other LSO reference points may become relevant to SD-WAN Services in the future.

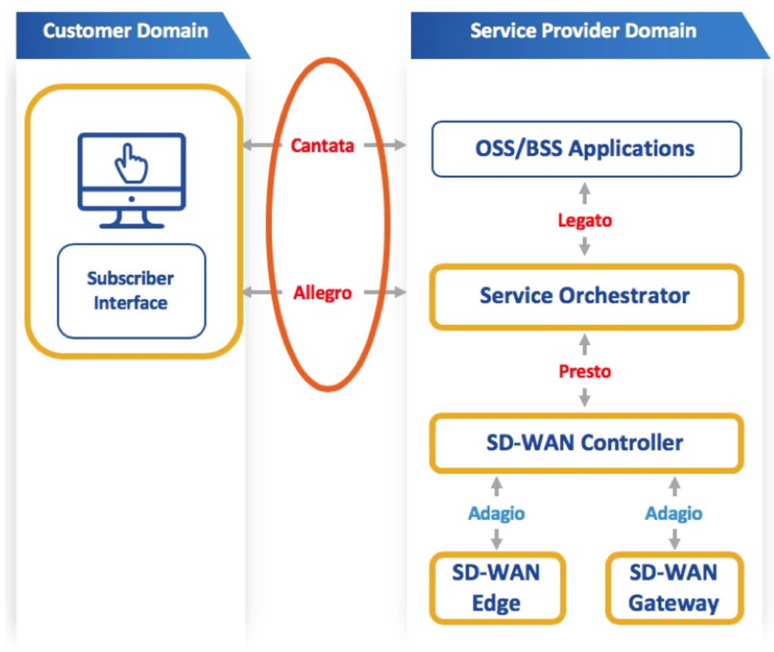

Figure 7 – SD-WAN Architectural Components in LSO Reference Architecture

Appendix C SD-WAN Use Cases (Informative)

Editor Note 6: Contributions Needed!