MEF White Paper

MEF 3.0 SD-WAN Services

November 2019

Disclaimer

© MEF Forum 2019. All Rights Reserved.

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

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

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

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

Table of Contents

List of Figures

List of Tables

1   Abstract

This White Paper is intended for SD-WAN Service Providers and their enterprise customers who want to understand what a standardized, managed SD-WAN service is and the benefits it brings to the industry. The rapid growth in adoption of SD-WAN services is creating a major business opportunity for established telecom service providers, smaller access connectivity providers, system integrators moving up the value chain as well as a wide range of technology vendors supplying SD-WAN technology, value-add VNFs, service orchestration solutions, and more.

The paper explains the abstract building blocks of SD-WAN services using standardized terminology developed in MEF (www.MEF.net) by service provider and SD-WAN vendor members in the context of the MEF 3.0 framework as part of the MEF 70 (SD-WAN Service Attributes and Services) Standard. This MEF standardization helps customers of SD-WAN services understand what they are buying and it helps break down the barriers to interoperable services. MEF standardization fosters an open marketplace and reduces the inevitable confusion in a very new, rapidly growing market which, without agreed terminology, can hold back growth and innovation. MEF's standardization also enables common open information and data models to be developed. These models are the cornerstone for open standard APIs to ultimately support automated service fulfillment and service assurance.

Primary use cases for managed SD-WAN services are introduced using MEF standardized constructs and the value of those use cases for SD-WAN service subscribers. The paper also addresses the requirements of managed SD-WAN services in different market verticals including Manufacturing and Logistics, Healthcare, Retail, Finance and Government, highlighting the huge potential for service providers tuning SD-WAN offerings to the needs of these verticals.

An overview of MEF's continuing work on many aspects of SD-WAN services is provided including: Certification of conformance to SD-WAN standards; addressing the emerging skill shortages in service providers and enterprises with a professional certification for SD-WAN; the application of LSO (Lifecycle Service Orchestration) to SD-WAN services to streamline automation and support multi-vendor SD-WAN service implementations; preparing SECaaS (Security as a Service) for the critically important standardized protection for application flows running over SD-WAN services as attack vulnerabilities multiply exponentially; and the disintermediation of business intent and service configuration using Intent-Based Networking principles which is necessary for highly agile SD-WAN service offerings that meet the constantly evolving enterprise application environment.

Finally, this White Paper highlights the importance of standardized Underlay Connectivity Services (e.g. the $60B+ Carrier Ethernet services market) as underlays for SD-WAN service overlays. It shows how returns on massive investments made by Communications Service Providers over the last couple of decades in connectivity infrastructure can be maximized to support and enhance SD-WAN services.

2   Introduction

The SD-WAN market is one of the fastest growing sectors in the communications industry, projected to generate tens of billions of dollars of revenue over the next five years. IDC estimates that the global SD-WAN infrastructure market (excluding managed services) will reach $US 5.3 billion by 2023 at 30.8% CAGR. The United States managed SD-WAN services market alone is projected to reach $US 4.5 billion by 2023 at 74% CAGR according to Vertical Systems Group. The main drivers of this market growth are enterprises seeking (1) better support for SaaS applications and multi-cloud and hybrid cloud usage and (2) easier management of WAN connectivity to improve application performance and user experience.
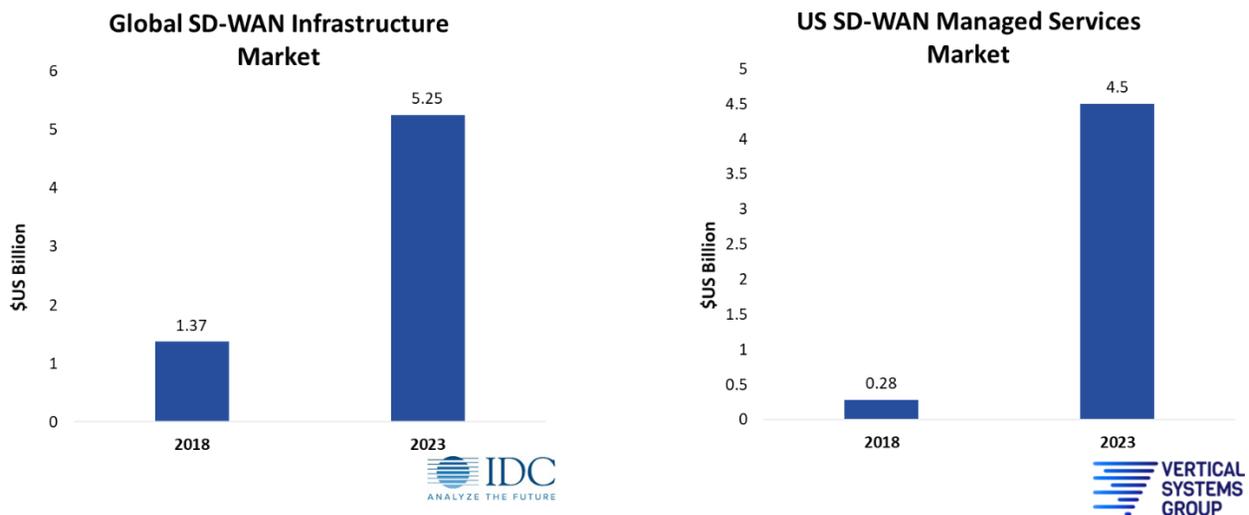
Figure 1 – Growth of SD-WAN market
(Sources: IDC www.idc.com; Vertical Systems www.verticalsystems.com)

However, today's SD-WAN market shares many similarities to the early days of today's US$ 80B+ Carrier Ethernet services and technology market before standardization and services, technology, and certification became available. This important and fast-growing SD-WAN services market is therefore attracting many new service providers and technology vendors that attach the term 'SD-WAN' to their product offering. Alongside high expectations about SD-WAN services that deliver performance/price advantages, greater flexibility, etc., there is a huge need for education and alignment on terminology. In fact, nearly 80% of service provider respondents in a joint survey that MEF conducted with Vertical Systems Group in 2018 identified the lack of an industry-standard service definition as a significant challenge for providers to offer or migrate to SD-WAN services.

This White Paper highlights the work that MEF is doing in order to address these and other issues that will enable the SD-WAN services market to grow even faster and meet its potential.

The paper introduces the industry's first SD-WAN service definition work by MEF as published in MEF 70 [1] and the wide range of MEF work that is underway and that builds on MEF 70 [1]. The paper also explains how MEF is addressing the needs for standardized terminology, architectural constructs and associated education.

⚠ This White Paper, as does MEF 70 [1], covers those SD-WAN services that are provided by service providers to enterprise customers with a contract and Service Level Agreement. These services might be fully managed by the service provider ('fully-managed SD-WAN services') or alternatively might be co-managed by the service provider and the enterprise subscriber ('partially-managed SD-WAN service'). These managed SD-WAN services do not include those 'do it yourself' SD-WAN solutions developed by enterprises.

3 MEF 3.0 SD-WAN Services

In July 2019, MEF published MEF 70 [1] - the industry's first global standard defining SD-WAN service attributes and services - to help accelerate SD-WAN market growth and facilitate creation of powerful new hybrid networking solutions that are optimized for digital transformation.

MEF-defined SD-WAN services are part of the MEF 3.0 Global Services Framework [2] that also includes MEF 3.0 Optical Transport services [3], MEF 3.0 Carrier Ethernet services [4], and MEF 3.0 IP services [5]. MEF defines MEF 3.0 services in a consistent way in order to, among other objectives, maximize the ability to use a single orchestration approach for all data connectivity services, as well as to reuse concepts in all the services standardization work. Examples of shared concepts in MEF 3.0 services are provided below, in the context of MEF 3.0 SD-WAN services. In general, MEF defines a service that can be offered as part of its product offerings by a service provider in such a way that it can be captured clearly and consistently described in Service Level Agreements. MEF defines such services regardless of the implementation used and instead focuses on abstractions of the service like service attributes. This leaves the service provider free to choose the most suitable technology vendors and design the most appropriate implementations while conforming to the SLA agreed with the enterprise customer.

Figure 2 – MEF 3.0 Framework

The MEF 70 [1] standard describes requirements for an application-aware, overlay WAN connectivity service that uses policies to determine how application flows are directed over multiple underlay networks irrespective of the underlay technologies or the service providers who deliver them.

MEF 70 [1] defines:

- **Service attributes** that describe the externally visible behavior of an SD-WAN service as experienced by the subscriber.
- **Rules** associated with how traffic is handled.
- **Key technical concepts and definitions** like an SD-WAN UNI, the SD-WAN Edge, Tunnel Virtual Connections, SD-WAN Virtual Connection End Points, and Underlay Connectivity Services.

SD-WAN standardization offers numerous benefits that help accelerate SD-WAN market growth while improving overall customer experience with hybrid networking solutions.

Key benefits include:

- Enabling a wide range of ecosystem stakeholders to use the same terminology when buying, selling, assessing, deploying, and delivering SD-WAN services.
- Making it easier to interface policy with intelligent underlay connectivity services to provide a better end-to-end application experience with guaranteed service resiliency.
- Facilitating inclusion of SD-WAN services in standardized LSO architectures, thereby advancing efforts to orchestrate MEF 3.0 SD-WAN services across automated networks.
- Paving the way for creation and implementation of certified MEF 3.0 SD-WAN services, which will give users confidence that a service meets a fundamental set of requirements.
- Providing the foundation for the development of SD-WAN APIs to support multiple interfaces in the MEF LSO architecture
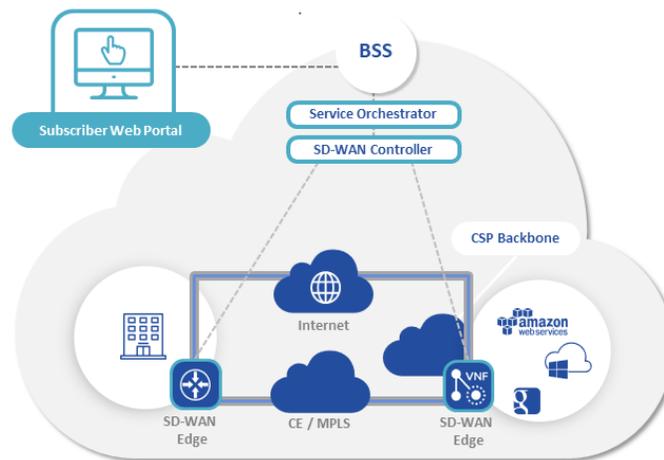
Figure 3 – SD-WAN Service with portal and edges

We now describe four different aspects of the SD-WAN service as defined in MEF 70 [1]:

- The two **parties** to the SD-WAN service - the SD-WAN Subscriber and the SD-WAN Service Provider
- The **components** used by the SD-WAN Service Provider to describe and build the SD-WAN service
- The **attributes** of the SD-WAN service experienced by the user of the service and their use in the Service Level Agreement
- The **overlay nature** of the SD-WAN service

3.1 SD-WAN Subscriber and SD-WAN Service Provider

MEF identifies two primary stakeholder organizations in the context of MEF 3.0 SD-WAN services — the SD-WAN Subscriber and the SD-WAN Service Provider. The SD-WAN Subscriber is the organization that buys and uses an SD-WAN service and the SD-WAN Service Provider is the organization that sells and provides that service.

There is no restriction on the type of organization that can act as a Subscriber; for example, a Subscriber can be an enterprise, a mobile operator, an IT system integrator, a government department, etc. At its most basic, an SD-WAN Service provides connectivity for IP Packets between different parts of the Subscriber's network (different Subscriber or partner physical locations or private/virtual private clouds) or between the Subscriber's network and the public Internet using Internet Breakout.

The remainder of this White Paper uses "Service Provider" to refer to the SD-WAN Service Provider and "Subscriber" to refer to the SD-WAN Subscriber.

MEF 3.0 services, in general, are provided by service providers to customers with a contract and Service Level Agreement. In the case of MEF 3.0 SD-WAN services, they might be fully managed by the service provider ('fully managed SD-WAN services') or alternatively might be co-managed by the service provider and the subscriber ('partially managed SD-WAN service').

3.2   SD-WAN Service Components

When the Subscriber and Service Provider negotiate the terms of the contract and SLA, they need to refer to the building blocks or components of the service - preferably using the standardized terminology defined by MEF in MEF 70 [1]. The following provides a high-level overview of those components and their purpose when using them to build an SD-WAN service.
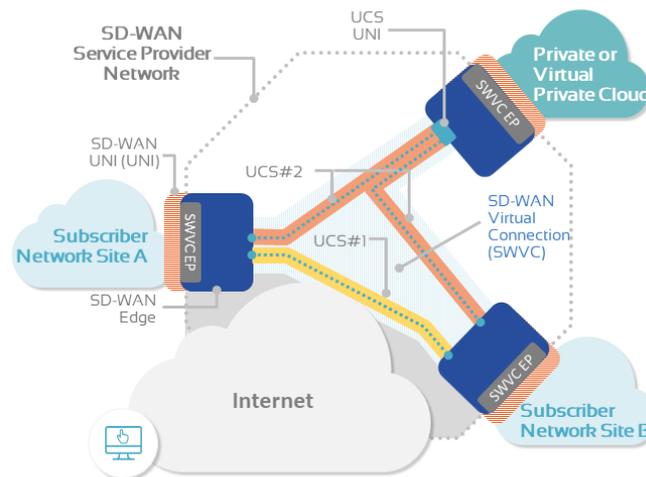
Figure 4 – SD-WAN Service components

3.2.1   SD-WAN UNI

As for any service, it's important to define the **demarcation point** between the responsibility of the service provider and that of the subscriber. In MEF terminology, this abstract demarcation point, or reference point, is called the SD-WAN User Network Interface or *SD-WAN UNI* (UNI pronounced *you'nee*) for short. The subscriber can only connect to the SD-WAN service at the SD-WAN UNI. When we say 'connect', we mean that the subscriber's IP packets can only enter and exit the SD-WAN service via an SD-WAN UNI.

Establishing the location and the type of the SD-WAN UNI is important because it delineates the boundary of responsibilities between the service provider and the subscriber for the SD-WAN service.

3.2.2   SD-WAN Virtual Connection (SWVC) and End Points

MEF 70 [1] introduces the concept of an SD-WAN Virtual Connection (SWVC) which is analogous to Carrier Ethernet service EVCs and OVCs. However, in the case of SD-WAN services, the SWVCs are defined in terms of **policies and IP forwarding constraints**. An SD-WAN Service is formed of an SD-WAN Virtual Connection (SWVC) that links together SD-WAN Virtual Connection (SWVC) End Points located at UNIs. In other words, the SWVC defines the logical connectivity of the SD-WAN Service as viewed by the Subscriber. An SWVC End Point is the logical function that associates Ingress IP Packets with Application Flows, and applies a Policy to each Ingress IP Packet in order to make an appropriate forwarding decision.

3.2.3   SD-WAN Underlay Connectivity Service (UCS)

MEF 70 [1] introduces the term *Underlay Connectivity Service (UCS)* which is the service providing **connectivity between one or more of the subscriber locations** to which the SD-WAN service is delivered. MEF 70 [1] requires at least one UCS per subscriber location. This would seem at first sight trivial. How can IP packets be delivered to a subscriber location as part of the SD-WAN service if that site doesn't have network connectivity? The reason for this stipulation is to make it the responsibility of the SD-WAN service provider to agree with the Subscriber the number and type of UCSs over which the SD-WAN service will be provided. In other words, in order to provide proper service assurance, the SD-WAN Service Provider must understand what underlay connectivity is being used for all parts of its SD-WAN service even if that SD-WAN service is an overlay service and the SD-WAN service provider does not own or control the UCS. What is acceptable in the world of Over the Top (OTT) where applications don't 'care' what they run over does not meet the requirements of a MEF 3.0 SD-WAN service and its application flows.

The UCS can support one of a variety of services including (but not limited to) Ethernet Services (as defined in MEF 6.2 [6] and MEF 51.1 [7]), IP Services (as defined in MEF 61.1 [5]), L1 Connectivity Services (as defined in MEF 63 [3]), and public Internet Access services. Access to these Underlay Connectivity Services can be via a variety of networking technologies, such as DSL, HFC, LTE, fiber, Wi-Fi, Ethernet, 5G and satellite. As can be seen, an SD-WAN service can operate over any type of forwarding plane from optical up to and including IP.

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

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

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

Underlay Connectivity Services can be provided by the SD-WAN Service Provider on its own network or over the networks of other network operators (including the Public Internet). Underlay Connectivity Services arranged independently by the Subscriber can also be used by the SD-WAN Service.

3.2.4   Tunnel Virtual Connection (TVC)

In MEF 70 [1], Tunnel Virtual Connection (TVC) is a point-to-point forwarding relationship between two SD-WAN Edges that has a specified set of performance and privacy/security characteristics. A TVC traverses an Underlay Connectivity Service. At an SD-WAN Edge, Application Flows can be directly forwarded to another SD-WAN Edge if there is at least one TVC to that SD-WAN Edge.

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

Important characteristics of TVCs include:
- If any UCS traversed by a TVC is a Public network, then the TVC is *Public*, otherwise it is *Private.*
- The SD-WAN Edge can implement encryption on a TVC basis in which case all traffic forwarded across the TVC is encrypted.
- The quality of service provided by the UCS Service Provider results in a measurable set of Performance Metrics that can be used to select a TVC for forwarding Application Flows that have defined performance goals.

3.2.5   SD-WAN Edge

The SD-WAN Edge is the **collection of network functions** (physical or virtual) that are located between the Underlay Connectivity Service UNI and the SD-WAN UNI. The SD-WAN Edge is not equivalent to the SD-WAN UNI nor to the SWVC End Point. One of the important functions of the SD-WAN Edge is to select a TVC over which to forward each ingress IP Packet at the SWVC End Point.

3.2.6   SD-WAN Application Flows and Policies

A MEF 3.0 SD-WAN service is oriented around private routing for IP Packets that match specified sets of criteria – Application Flows – and the rules and constraints applied to the forwarding of those Application Flows - SD-WAN service policies.

Application flows are a very central aspect of the expectations of the Subscriber from the SD-WAN service with service quality objectives based on the policy applied to each Application Flow.

The Application Flow is the basic building block of how the SD-WAN Edge function operates. The SD-WAN Edge comprises three main components.

- Application Classification that matches the packets at the SD-WAN UNI to a specific Application Flow definition.
- Policy that captures the SD-WAN policies which are associated with the Application Flow and therefore impact on the forwarding decision, depending on the current state of each TVC, and are used to select which TVCs are suitable
- TVC Forwarding Decision that makes the IP forwarding decision about which TVCs (of the ones selected by Policy) can reach the IP destination for each IP Packet.
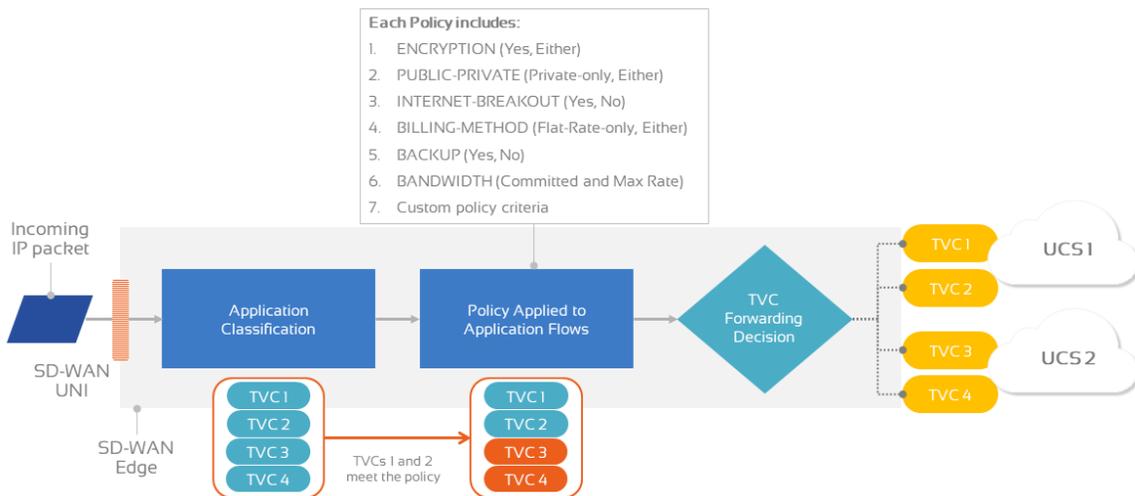
Figure 5 – Policies and SD-WAN

Another important aspect of a MEF 70 [1] SD-WAN service is that is required to support policy-based autonomous traffic management. In other words, the SD-WAN service has to be able to translate the policy requirements of the Subscriber into traffic management in the SD-WAN service that is not dependent on manual configuration but can be accomplished autonomously.

3.3   SD-WAN Service Attributes

MEF 3.0 SD-WAN services are specified using service attributes as defined in MEF 70 [1] and describe what the Subscriber quantitatively will receive from the SD-WAN service. This is analogous to the subscriber Carrier Ethernet service attributes defined by MEF in the standard MEF 10.4 [8].

A service attribute captures specific information that is agreed on between the Service Provider and the Subscriber of a MEF SD-WAN Service, and it describes some aspect of the service behavior. How such an agreement is reached, and the specific values agreed upon, might have an impact on the price of the service or on other business or commercial aspects of the relationship between

the Subscriber and the Service Provider. Examples of how agreement can be reached between the SD-WAN service provider and the Subscriber include:

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

Service Attributes describe the externally visible behavior of the service as experienced by the Subscriber and also the rules and policies associated with how traffic is handled within the SD-WAN Service. However, they do not constrain how the service is implemented by the Service Provider, nor how the Subscriber implements their network. This latter point is very important because it means that the language used between the Subscriber and SD-WAN service provider is the 'what' is expected from the SD-WAN service while leaving all the aspects of 'how' to the Service Provider.

The initial value for each Service Attribute is agreed upon by the Subscriber and the Service Provider in advance of the service deployment. The Subscriber and the Service Provider may subsequently agree on changes to the values of certain Service Attributes. Similarly, the Service Provider could allow the Subscriber to select an initial value from a pre-determined set of values, and the Service Provider might further allow the Subscriber to change the attribute values selection at any time during the lifetime of the service.

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

3.4 SD-WAN Overlay and Underlay

MEF defines an SD-WAN service as a service that provides a Subscriber with a virtual overlay network that enables application-aware, policy-driven, and orchestrated connectivity between SD-WAN User Network Interfaces (UNIs). It also provides the logical construct of a L3 Virtual Private Routed Network for the Subscriber that conveys IP Packets between Subscriber sites. MEF 3.0 SD-WAN services can take advantage of multiple Underlay Connectivity Services (UCS) to deliver differentiated service capabilities rather than connectivity services based on a single transport facility. Importantly, MEF has defined Optical Transport, Carrier Ethernet and IP services in a suite of standards, and these service definitions are an important basis for Underlay Connectivity Services. In other words, MEF 3.0 SD-WAN services are defined as overlay services, and MEF 3.0 Optical Transport, Carrier Ethernet and IP services can be used as Underlay Connectivity Services to support the SD-WAN overlay service.

4 SD-WAN Use Cases

Now that we introduced the concepts of Subscriber and Service Provider, the various service components used to build and deliver the service, the attributes describing what the subscriber should

receive in terms of service and the overlay nature of MEF-defined SD-WAN services, we now look at the generic uses of SD-WAN services by SD-WAN Subscribers.

4.1 Multiple Underlay Connectivity Services

One of the major attractions of SD-WAN services is the ability to minimize application downtime experienced by the enterprise user without sacrificing application performance and without having to buy additional expensive dedicated managed service connectivity to each enterprise location. The key to making these trade-offs is to understand the various combinations of two or more Underlay Connectivity Services that can be made at each enterprise location. In this section, we look at the following combinations of two Underlay Connectivity Services for SD-WAN services.

- Dual Managed WAN Service (e.g. Private IP VPN service + Private IP VPN service)
- Hybrid WAN (e.g. Private IP VPN service + Internet Access service)
- Dual Internet (i.e. Internet Access service + Internet Access service)

4.1.1 Dual Managed WAN

In many instances, enterprises have mission critical applications running over their managed UCS (e.g., Private IP VPN service) for a given site and have purchased an additional managed UCS (e.g., Private IP VPN service) for that branch to provide redundancy in order to have an immediate connection should the first UCS fail. However, that second UCS stands idle in standby mode until brought into use when the active UCS fails for any reason. SD-WAN services offered by service providers can utilize both these UCSs in active-active mode while maintaining the same resilience offered by the original active-standby configuration. The diagram shows a case where the enterprise originally had two Private IP VPN services—one of which was in idle mode 99% of the time until SD-WAN was introduced—and the enterprise's connectivity capacity was doubled reducing the redundancy only by half.
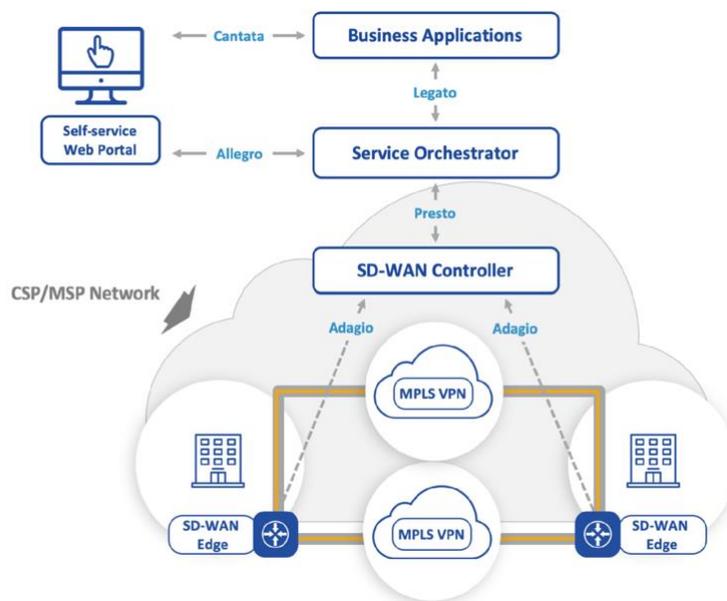

Figure 6 – SD-WAN Dual Managed WAN use case

4.1.2   Hybrid WAN

Similar to the Dual Managed WAN use case, the Hybrid WAN use case employs two Underlay Connectivity Services but in this scenario, one is a managed connectivity service (e.g., Private IP VPN service) and the second is an unmanaged Internet service (e.g. Dedicated Internet Access (DIA)). Here, the Subscriber may have previously been using the Private IP VPN service for all the applications being run to the branch office and needs to cost-effectively expand bandwidth availability. The Subscriber is able to enhance the Subscriber's Private IP VPN service with an Internet Access service. This service can be used to offload non-critical traffic either during high usage periods or as a matter of policy – e.g., for email or Slack. SD-WAN allows for multiple UCSs to be in concurrent usage addressing different business needs. There is also degree of resilience in the event that one of the connections goes down, important applications can continue to run on the still active connectivity service.
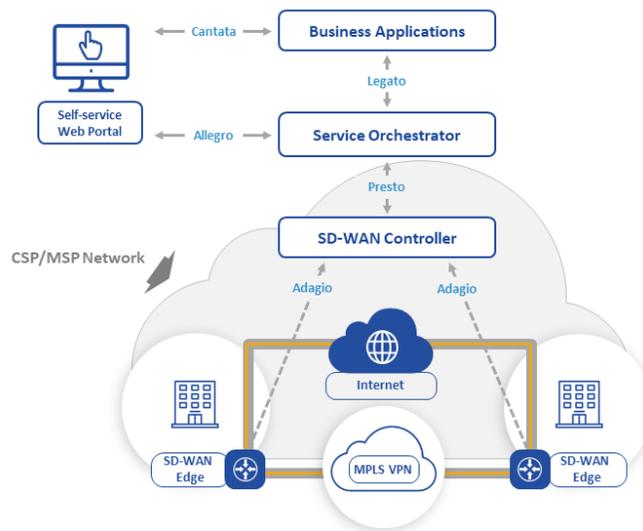

Figure 7 – SD-WAN Hybrid WAN use case

4.1.3   Dual Internet WAN

In this third variation on the Dual WAN use case category, the SD-WAN Subscriber may not have the ability to have a managed WAN service (e.g., Private IP VPN service) delivered to a given enterprise location whereas there may be a range of Internet Access service offerings there. In order to maximize redundancy, the SD-WAN Subscriber uses the SD-WAN service over a combination of two or more Internet Access services from different service providers with intelligent routing of application flows between the Internet Access services to maximize performance.
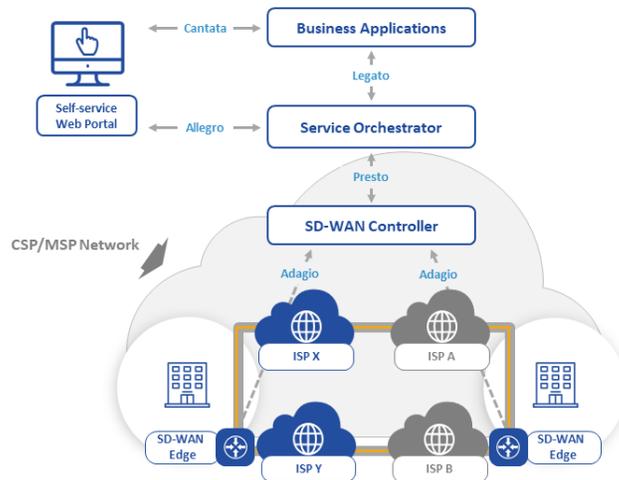

Figure 8 – SD-WAN Dual Internet use case

4.2   Local Internet Breakout

Branch offices of enterprises are increasingly using cloud services and applications. Rather than sending the traffic from these cloud applications through to the enterprise headquarters and from there to the public cloud, it makes more sense to have a local breakout at the branch office to the Internet and to go directly to the public cloud from there. For example, a South African enterprise using a cloud-based office application suite might previously have run the application's traffic via the enterprise link up to London HQ and from there to the local cloud application provider's cloud. However, today it makes more sense to provide the branch office in South Africa with a local Internet breakout and have the traffic go directly to the local application services location in South Africa thereby gaining performance and reducing waste of the valuable bandwidth between the branch office and the UK HQ. Note that the Internet breakout uses the same Internet Underlay Connectivity Service as the SD-WAN service itself, but Internet traffic is delivered directly to and from the Internet while other traffic traverses a TVC across the Internet UCS to reach other SD-WAN Edges.
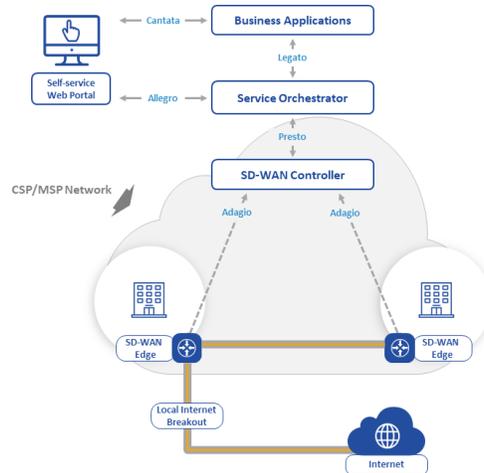
Figure 9 – Local Internet Breakout use case

This is an important use case of SD-WAN services. Although the Internet connection is not part of the SD-WAN service per se, the processing at the SD-WAN Edge of application flows to determine what goes to a TVC and what goes over the Internet breakout connection is part of the SD-WAN service.

4.3   Wireless Connectivity

Rapid onboarding of additional SD-WAN Subscriber endpoints (e.g. for IoT) is an important aspect of the SD-WAN service. In the scenario of the only connectivity at a given endpoint being wireless (e.g. LTE), the ability to turn up a site with appropriate policies to provide both performance and security assurance can be well-served by SD-WAN services. Note that the wireless connectivity could be used as part of any type of Underlay Connectivity Service, e.g. it could be part of an Internet Access service or a Private IP VPN service.
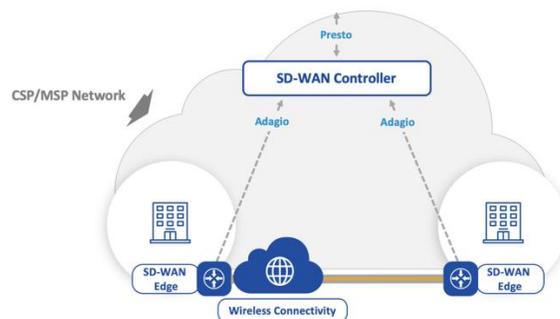
Figure 10 – Wireless Connectivity use case

4.4   SD-WAN Edge Deployment Use Cases

In contrast to the Multiple Underlay Connectivity Services, Local Internet Breakout and Wireless Connectivity use cases focus on the implementation of the underlay connectivity in the SD-WAN service, the following use cases relate to the implementation of the SD-WAN service edge. They

draw attention to the relevance of using virtualized network functions (VNFs) when deploying SD-WAN services to different edge points.

4.4.1 SD-WAN Edge VNF on uCPE: Multiple Virtual Network Services
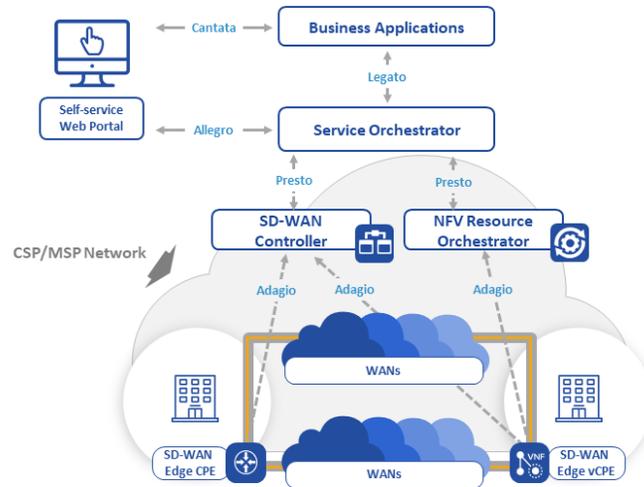
Figure 11 – Edge VNF on uCPE use case

Increasingly the SD-WAN Edge is implemented as one or more VNFs hosted on a uCPE. The advantages of such implementations are:

- No truck roll to deploy a vendor-specific device to the customer premises which enables greater scalability of endpoints for the SD-WAN service as well as geographic coverage.

- Consolidation of multiple VNFs (Virtual Network Function) that could run on the SD-WAN vCPE/uCPE and the flexibility of service function chaining of the VNFs in order to add additional services to that of the SD-WAN service.

4.4.2   SD-WAN Edge VNF Running in the Cloud
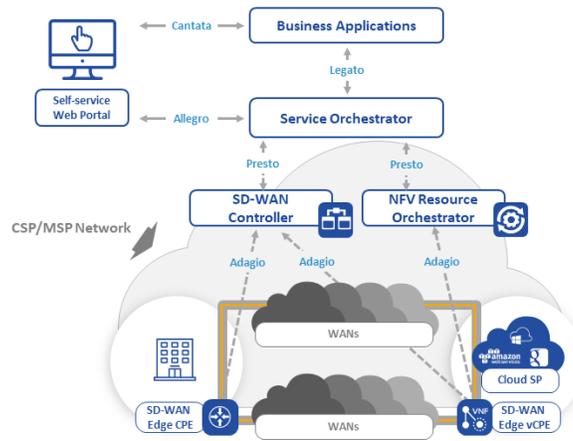
Figure 12 – Virtualized SD-WAN Edge in the cloud

With enterprises increasingly using cloud-based applications, SD-WAN services are being used to provide secure connectivity to those applications with the appropriate connectivity performance. However, service providers typically will not want, or be able, to deploy dedicated vendor devices into all the cloud providers that their SD-WAN Subscribers work with. The ability to be able to deploy virtualized SD-WAN edges in the cloud provider becomes of paramount importance.

4.5   Off-Net Extension

Many enterprises already have widespread connectivity for their branch offices using Private IP VPN services. Rather than onboard additional sites using Private IP VPN services or re-architecting all the connectivity to be SD-WAN service based, some enterprises prefer to extend the footprint of their connectivity by introducing SD-WAN service endpoints incrementally with a gateway to the IP VPNs running over MPLS for existing sites.
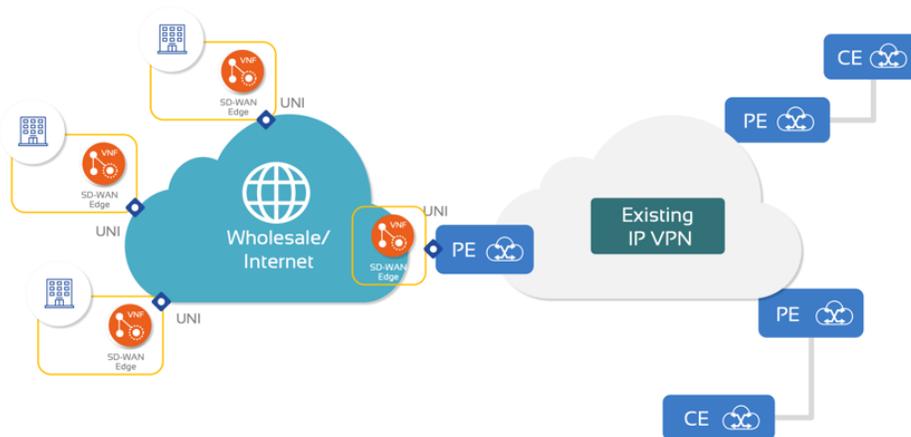
Figure 13 – Off-Net Extension

A more advanced example of this use case is where an MPLS backbone is used by a service provider in each of several countries in one region. These backbones are controlled by a single service provider and can be treated as a single Private IP VPN service underlay. Access to the Private IP VPN service underlay can be made available by regional gateways, legacy MPLS endpoints in the region or Internet connectivity from any other region of the world, with SD-WAN service being provided as an overlay service by a single provider to all these various types of endpoint.

This use case can be thought of as 'brownfield' scenario.

4.6 Multi-Cloud

ONUG's SD-WAN 2.0 Working Group [9] is focused on addressing specific challenges in integrating SD-WAN connectivity into enterprise hybrid multi-cloud environments. As part of its work, the working group defined use case requirements for typical deployment scenarios, including multiple cloud provider connections, application performance assurance, scaling, security policy enforcement, hybrid environment security integration, and multi-domain connectivity orchestration.
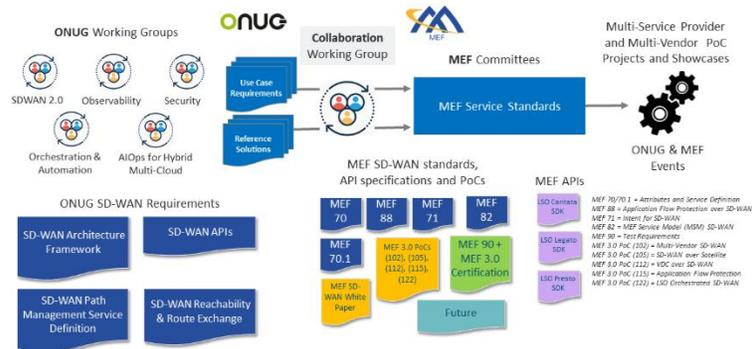
Figure 14 – Enterprise Use Cases

MEF and ONUG are now collaborating to influence MEF's ongoing SD-WAN projects so that the appropriate service specifications and certifications can be further matured. ONUG and MEF will collaborate on the joint definition of common service models and APIs for automating SD-WAN services, with initial areas of focus including:

- ONUG SD-WAN 1.0 service models and API specifications
- ONUG SD-WAN 2.0 multi-cloud integration use cases
- Application security for SD-WANs
- Intent-based networking and service automation for SD-WANs

5   Business Outcomes for SD-WAN Vertical Markets

In this section, we consider the use of SD-WAN services in different market verticals which illustrate the various business outcomes for using SD-WAN services.

Managed SD-WAN services are still in the main considered only in the context of generic use cases. However, the market is starting to see differentiated SD-WAN services being offered to cater more specifically to the unique needs of various market sectors. As a result of proven market traction and service maturity, SD-WAN Service Providers are building solid use cases and industry vertical specific managed service offerings. There are also patterns emerging for the reasons why specific verticals might want to adopt SD-WAN technology which are presented in the table below.

MEF 70-compliant SD-WAN services are a very valuable offering to support the following industry-specific drivers and trends. Also, in order to scale SD-WAN services to meet requirements of vertical markets, it is essential to have the suite of supporting APIs enabled by MEF 70 for the full management of these SD-WAN services.

Vertical	Drivers and Trends
Manufacturing and Logistics (Industry 4.0) *The difference between Industry 4.0 and Industry 3.0 is the data connectivity between physical devices that creates a coordinated, intelligent, flexible and distributed production system. That data connectivity should be optimized and secured in real-time for the needs of that distributed production system. SD-WAN service can provide that data connectivity to support Industry 4.0 even in mission-critical applications.*	**Rapid matching of production facilities to requirements for new products** • Supply chain accuracy • Stock and supplier management for just-in-time engineering • Rapid time-to-market for products • Plant re-tooling **Including remote facilities in production capabilities both robustly and securely** • Integration of acquired sites in a rapid expansion • Strengthened security for SCADA systems and IoT endpoints • Autonomous network telemetry • 5G network slicing • Multi-access Edge Computing **Pre-empting and mitigating production failures** • Predictive maintenance in production processes • Digital twin technology

Vertical	Drivers and Trends
Healthcare *Transformation of clinical labs, medical practices, hospitals, and care centers has resulted in the term 'Digital Healthcare'* *SD-WAN will underpin adoption of healthcare IoT, population health, AI, data analytics, clinical workflow, and tele-health solutions*	**Extending geographical footprint of medical expertise and care** • Immersive healthcare experiences using virtual reality (VR), augmented reality (AR) and mixed reality (MR) • Mobile clinics and MRIs • New therapies are also developing, underpinned by technology innovation: examples include virtual & augmented (AR/VR) reality and digital engagement therapy. • 5G Ambulance **Improving security of health data** • Better security in medical device IoT (MDIoT) - IoMT devices are becoming prolific in healthcare, and these simple devices are difficult to secure and breaches very challenging to repair • Better healthcare cybersecurity far beyond patient data protection but defense against potential state-sponsored cyber-terrorism **Improving patient experience** • Digital twin technology
Finance *While banks and other financial institutions have been closing the familiar high street branches in large numbers of the last decade, a new set of customer needs are evolving that require more than browser/smart phone interfaces can provide. SD-WAN services offer both the performance and security assurance that are essential for the reputation of financial services offering advanced digital services.*	**Rapid set up, adjustment and re-distribution of physical branch facilities to meet changing localized market needs** • Pop-up stores & intelligent kiosks • Automation - customer movements and experiences can be monitored with big data assessments for test and strengthening of branch performance. • Meeting multi-generational customer demands with a modern customer-centric environment • Leveraging customer data - branch systems and tools must connect up all the touch points with clients **Improving security of financial data** • Consistent branch security policy compliance **Improving customer experience** • AR/VR • Robotics and wearable technologies • Interactive Teller Machine (ITM) technology and self-service kiosks - 'drive-through' customer experience e.g., customers can use an ATM to scan an ID document and get approval for a cash withdrawal while they are waiting for a card replacement, without having to interact with a human

Vertical	Drivers and Trends
Government *With its ever-growing obligations to provide broad and secure services to each and every citizen wherever they are in the country while reducing or at best maintaining current budgets, governments are increasingly dependent on digital capabilities. SD-WAN offers both opportunities and risks for governments to innovate citizen services while protecting exponentially growing attack surfaces vulnerable to cyber-criminals. Recent ransomware attacks on municipalities and police forces demonstrate that many LAN-based systems are still vulnerable, and connectivity solutions are only part of the equation.*	**Rapid set up, adjustment and re-distribution of physical branch facilities to meet changing localized citizen needs and range of verticals** • Government agency networks act like commercial enterprises • Agencies have a lot of branch offices, and they want to be able to turn them up quickly if needed (for example, FEMA). • Larger offices are sometimes using SD-WAN with multiple connections, including back-up connectivity over wireless (and especially want this capability as 5G emerges) • Need to handle multiple verticals under the nation or state government umbrella • Thousands of remote offices and branches with low bandwidth • Differentiation from local government/municipalities • Ability to handle home schooling in remote areas (e.g. via satellite) • Emergency 'cell on wheels' **Maximizing taxpayer ROI** • Key drivers: performance and cost savings (connectivity, management, staff). Shift from 2x Private IP VPN service to 1x Private IP VPN service + dedicated Internet. • Managed services reduce dependence on internal IT agencies • Greater use of cloud and Internet and less VPNs • Use of smaller localized service providers rather than the larger telcos that have large footprints **Reconfiguration of security architecture** • Safely bypassing security gateways that reduce performance • Ability to use policies dynamically to handle wide range of data security classification levels **Simplifying procurement** • Standardized and certified SD-WAN • Standardized terminology across multiple government agencies

Table 1 – Requirements of SD-WAN services per market vertical

6 Upcoming MEF Developments for SD-WAN Services

The publication of MEF 70 [1] has created the basis for a wide range of new work in MEF to support the rapidly evolving needs of the SD-WAN services market. The following provides a brief overview of those activities and the opportunities for industry players to participate in that MEF work.

MEF SD-WAN Certification

MEF is extending its program of certifying the compliance with MEF standards to include certification of SD-WAN services and SD-WAN technology solutions. The MEF 3.0 SD-WAN certification program provides an important baseline for technology vendors, service providers and enterprises to identify those companies that meet the baseline requirements for standardized SD-WAN services, reduce market confusion and accelerate the growth of the SD-WAN services market.

MEF Professional Certification

MEF is also extending its professional certification program to address the rapidly growing shortfall in skilled staff both in the service provider industry as well as in their customer enterprises which is significantly hindering the adoption of SD-WAN services. This skills shortfall has been identified as a major market inhibitor by service providers in joint research conducted by MEF with analyst groups in 2019.

Enhanced SD-WAN Service Definition

MEF already has begun work on the next phase of SD-WAN standardization – MEF 70.1 – that will be of high interest to many enterprises and service providers. This work includes defining:

- Service attributes for application flow performance and business importance.
- SD-WAN service topology and connectivity.
- Underlay connectivity service parameters.

Security Application Flows over SD-WAN

Security vulnerabilities of any service grow in direct proportion to the 'attack surface' of the service. In the case of SD-WAN, the ability to support tens or hundreds of thousands of endpoints with a single SD-WAN service means the opportunities for attackers can grow exponentially. This is both a major challenge for the SD-WAN Subscribers and SD-WAN Service Providers, and a major opportunity for Managed Security Service Providers (MSSPs)

MEF's Application Security for SD-WAN project is focused on defining policy criteria and actions to protect applications (application flows) over an SD-WAN service. Work includes defining

threats, security functions, and security policy terminology and attributes, and then describing what actions a security policy should take in response to certain threats.
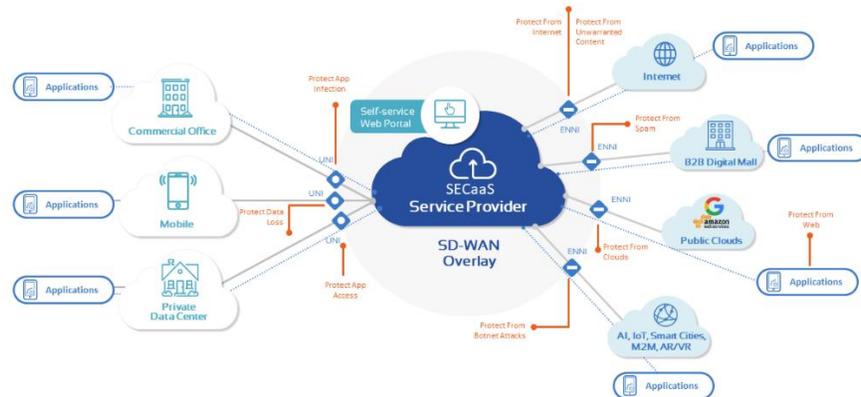

Figure 15 – Protection of application flows over SD-WAN services

The threats being addressed can come from within the SD-WAN subscriber's network or externally from the Internet when connecting to public clouds and other Internet hosts. One key area the project is currently addressing is defining Zones whereby the enterprise subscriber defines a grouping of subnets, using business function naming, where unique security policies are applied. Examples of Zones include a Point-of-Sales (POS) Terminal Zone where POS terminals are segregated from the rest of the network to protect payment card transactions connecting to a data center from being scanned and information stolen. Another Zone could be a Guest Wi-Fi Zone where visitors are allowed access to the Internet but are segregated from the corporate network. For each Zone, security policies would be applied for various defense postures.

**Orchestrated SD-WAN and Lifecycle Service Orchestration (LSO)**
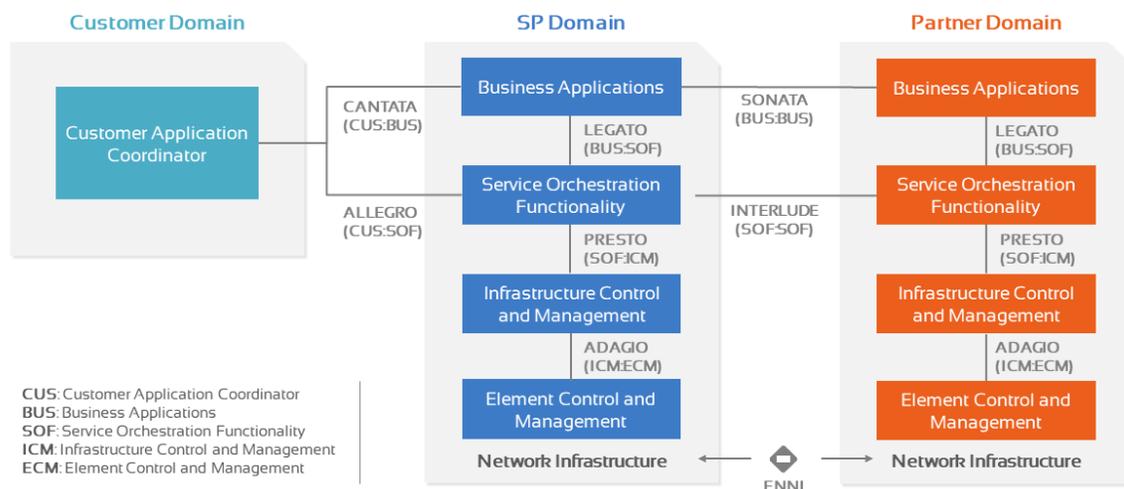
Figure 16 – LSO Reference Architecture

SD-WAN services increasingly rely on a range of stakeholders in the ecosystem including technology vendors (e.g., SD-WAN solutions, value-add services using NFV, uCPEs, service orches-

tration, service and security assurance, policy management etc.) and service providers (e.g., established telcos and MSPs currently offering managed business services, rural telcos, ISPs, system integrators becoming MSPs etc.) The ability to interconnect with each other and to rapidly onboard new players into existing service offerings is essential. This is best achieved by standardizing the interface points between different parts of the ecosystem and leveraging the capabilities of NFV, SDN and LSO effectively.
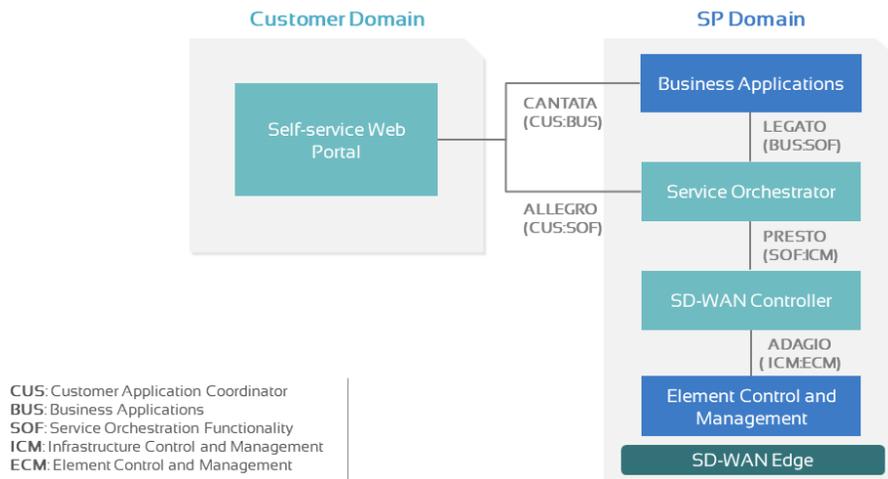
Figure 17 – SD-WAN Service Orchestration Architecture

Therefore, within a broader MEF Services Model (MSM) project related to orchestration of MEF 3.0 services, MEF is modeling MEF 70 SD-WAN service in UML to ensure consistency of LSO APIs across many reference points within the LSO framework. The initial focus of the SD-WAN work centers on LSO Legato, which supports interactions between business applications and service orchestration functionality, as well as at LSO Presto which supports Underlay Connectivity Service provisioning and SOAM. MEF's SD-WAN modelling work also has applicability for the LSO Cantata and LSO Allegro interfaces associated with product- and service-related management interactions between a customer and a service provider for single-view portals and e-Commerce offerings.
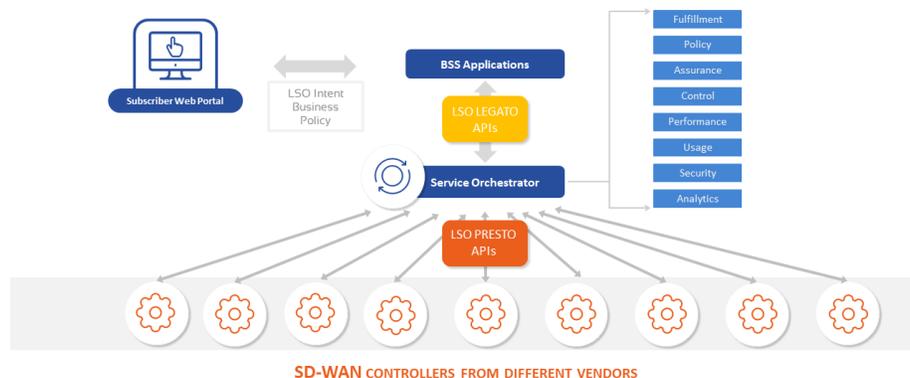
Figure 18 – Using LSO Presto APIs for Multi SD-WAN vendor implementations

SOAM and SAT for SD-WAN

The work of MEF in defining Service OAM and Service Activation Testing (SAT) for Carrier Ethernet and IP services can be used to enhance SD-WAN service performance assurance by using SOAM information from Underlay Connectivity Services. This is being explored in MEF work building on standards like MEF 30.1 [10], MEF 35.1 [11], MEF 48 [12], MEF 66 [13], and MEF 83 [14].

Using Intent for SD-WAN

MEF's IBN (Intent-Based Networking) work aims to enable an SD-WAN service subscriber to set intent-related performance and security objectives and have that be translated into granular technical policies at the network level. Toward this goal, MEF is building Domain Specific Languages (DSLs) – using restricted natural languages – that will simplify APIs that sit between end-users and service providers.
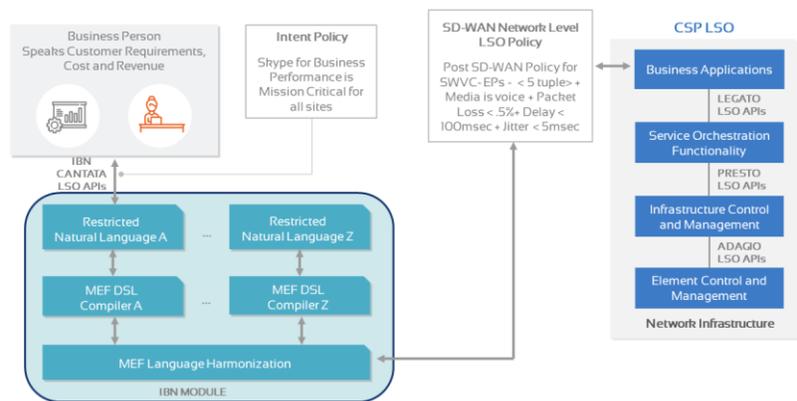
Figure 19 - Using Intent-Based Networking for SD-WAN services

7 Summary

The broad range of work in MEF on standardizing SD-WAN services has already led to the industry's first standard defining SD-WAN services and attributes as well as the industry leading MEF 3.0 certification program for SD-WAN service providers and vendors. The industry has its first standardized service terminology for SD-WAN in MEF 70 [1], and this is already helping to reduce confusion around SD-WAN while simplifying interactions between providers and their service subscribers as they choose optimal SD-WAN solutions for their offerings.

SD-WAN use cases are quickly evolving to take advantage of the capabilities of SD-WAN services, and industry verticals are beginning to hone their requirements to optimize SD-WAN services for their specific needs.

LSO orchestration of SD-WANs is an important next step to enable multivendor solutions to be offered by SD-WAN service providers, and MEF's work on information and data models based on MEF 70 [1] will significantly enhance the capabilities of the resulting APIs needed for such orchestration.

The work of MEF on SD-WAN has just begun with the introduction of standardization of security for application flows running over SD-WANs, the use of Intent to streamline the enterprise configuration of its business needs into the use of SD-WAN services and the use of SOAM and SAT defined for Underlay Connectivity Services to maximize the capabilities of SD-WAN as an overlay service.

The MEF invites all those that consider themselves to be a part of the SD-WAN ecosystem to participate in the standardization work of the MEF, to engage in the certification programs for service providers, technology vendors and individual subject matter experts, and to position themselves as market leaders.

8   About MEF

An industry association of 200+ member companies, MEF has introduced the MEF 3.0 transformational global services framework for defining, delivering, and certifying assured services orchestrated across a global ecosystem of automated networks. MEF 3.0 services are designed to provide an on-demand, cloud-centric experience with user- and application-directed control over network resources and service capabilities. MEF 3.0 services are delivered over automated, virtualized, and interconnected networks powered by LSO, SDN, and NFV. MEF produces service specifications, LSO frameworks, open LSO APIs, software-driven reference implementations, and certification programs. MEF 3.0 work will enable automated delivery of standardized Carrier Ethernet, Optical Transport, IP, SD-WAN, Security-as-a-Service, and other Layer 4-7 services across multiple provider networks. For more information, visit https://www.mef.net and follow us on LinkedIn and Twitter @MEF_Forum.

9   Terminology

Term	Definition	Reference
API	Application Programming Interface	N/A
Application Flow	A subset of the IP packets that arrive at an Ingress SD-WAN UNI, identified by a set of Application Flow Criteria, and distinct from the subset for any other Application Flow at that SD-WAN UNI.	MEF 70
Application Flow Criterion	A rule that is used to classify IP Packets at an SD-WAN UNI.	MEF 70
AR	Augmented Reality	N/A
ATM	Automated Teller Machine	N/A
BSS	Business Support System	N/A
BUS	Business Applications	N/A
CAGR	Compound Annual Growth Rate	N/A
CE	Customer Edge	N/A
CES	Carrier Ethernet Services	N/A
CSP	Communications Service Provider	N/A
CUS	Customer Application Coordinator	N/A
DIA	Dedicated Internet Access	N/A

DSL	Digital Subscriber Line	N/A
ECM	Ethernet Control and Management	N/A
ENNI	External Network-to-Network Interface	N/A
EP-LAN	Ethernet Private Local Area Network	N/A
EVC	Ethernet Virtual Connection	N/A
FEMA	Federal Emergency Management Agency	N/A
HFC	Hybrid Fiber-Coaxial	N/A
IBN	Intent-Based Networking	N/A
ICM	Infrastructure Control and Management	N/A
ID	Identification	N/A
Internet Breakout	The forwarding of Application Flows, based on Policy, to (and from) the Internet via one or more Internet Underlay Connectivity Services located at SD-WAN Edges in the SD-WAN Service.	MEF 70
IoT	Internet of Things	N/A
IP-SEC	IP Security Protocol	N/A
IP-VPN	IP-based Virtual Private Network	N/A
ISP	Internet Service Provider	N/A
IT	Information Technology	N/A
LAN	Local Area Network	N/A
LIB	Local Internet Breakout	N/A
Local Internet Breakout	Internet Breakout in which Ingress IP Packets at an SD-WAN UNI are forwarded over an Internet Underlay Connectivity Service at the SD-WAN Edge where the UNI is located.	MEF 70
LSO	Lifecycle Service Orchestration	N/A
LTE	Long-Term Evolution	N/A
MDIoT	Medical Device IoT	N/A
MPLS	Multiprotocol Label Switching	N/A
MR	Mixed Reality	N/A
MRIs	Magnetic Resonance Imaging systems	N/A
MSM	MEF Services Model	N/A
MSP	Managed Service Provider	N/A
MSSP	Managed Security Service Provider	N/A
NFV	Network Functions Virtualization	N/A
ONUG	Open Networking User Group	N/A
OTS	Optical Transport Services	N/A
OTT	Over the Top	N/A
OVC	Operator Virtual Connection	N/A
PE	Provider Edge	N/A
Policy	A set of rules that can be assigned to an Application Flow, possibly through membership in an Application Flow Group, that determines the handling by	MEF 70

	the SD-WAN Service of IP Packets in the Application Flow.	
POS	Point of Sale	N/A
ROI	Return on Investment	N/A
SaaS	Software as a Service	N/A
SCADA	Supervisory control and data acquisition	N/A
SDN	Software Defined Networking	N/A
SDO	Standards Development Organization	N/A
SD-WAN	Software Defined Wide Area Network (see SD-WAN Service)	MEF 70
SD-WAN Service Provider	A Service Provider for an SD-WAN Service	MEF 70
SD-WAN Edge	Network functions (physical or virtual) that are located between the Underlay Connectivity Service UNI and the SD-WAN UNI.	MEF 70
SD-WAN Service	An application-aware, policy-driven connectivity service, offered by a Service Provider, that optimizes transport of IP Packets over multiple underlay networks. MEF SD-WAN Services are specified using Service Attributes defined in this MEF Standard.	MEF 70
SD-WAN Subscriber	A Subscriber of an SD-WAN Service	MEF 70
SD-WAN User Network Interface	The demarcation point between the responsibility of the SD-WAN Service Provider and the SD-WAN Subscriber.	MEF 70
SD-WAN Virtual Connection	An association of SD-WAN Virtual Connection End Points in an SD-WAN Service that provides the logical construct of a L3 Virtual Private Routed Network for a Subscriber.	MEF 70
SD-WAN Virtual Connection End Point	A logical construct at an SD-WAN UNI that partitions Ingress IP Packets into Application Flows, applies a Policy to each IP Packet based on the associated Application Flow, and selects an appropriate path to transport the IP Packet over the SWVC.	MEF 70
Service Provider	An organization that provides services to Subscribers. In this document, "Service Provider" means "SD-WAN Service Provider".	MEF 70
Service Provider Network	The aggregation of Underlay Connectivity Services, TVCs, SD-WAN Edges, controllers, and orchestrators used to deliver an SD-WAN Service to a Subscriber.	MEF 70
SLA	Service Level Agreement	N/A
SOAM	Service OAM (Operations, Administration, and Maintenance)	N/A
SOF	Service Orchestration Functionality	N/A

SP	Service Provider	N/A
Subscriber	The end-user of a service. In this document, "Subscriber" should be read as meaning "SD-WAN Subscriber".	MEF 70
SWVC	SD-WAN Virtual Connection	N/A
TVC	Tunnel Virtual Connection	N/A
uCPE	Universal Customer Premise Equipment	N/A
UCS	Underlay Connectivity Service	N/A
UML	Unified Modeling Language	N/A
UNI	User Network Interface	N/A
VNF	Virtual Network Function	N/A
VPN	Virtual Private Network	N/A
VPRN	Virtual Private Routed Network	N/A
VR	Virtual Reality	N/A

10 References

[1]   MEF 70 (MEF SD-WAN Service Attributes and Services Standard, July 2019)

[2]   MEF 3.0 Global Services Framework (MEF website)

[3]   MEF 63 (MEF Subscriber Layer 1 Service Attributes Standard, August 2018)

[4]   MEF Carrier Ethernet Services (MEF website)

[5]   MEF 61.1 (MEF IP Service Attributes Standard, May 2019)

[6]   MEF 6.2 (EVC Ethernet Services Definitions Phase 3, August 2014)

[7]   MEF 51.1 (Operator Ethernet Service Definitions, December 2018)

[8]   MEF 10.4 (Subscriber Ethernet Service Attributes, December 2018)

[9]   SD-WAN 2.0 Working Group (ONUG)

[10]   MEF 30.1 (Service OAM Fault Management Implementation Agreement, April 2013)

[11]   MEF 35.1 (Service OAM Performance Monitoring Implementation Agreement, May 2015)

[12]   MEF 48 (Carrier Ethernet Service Activation Testing (SAT), October 2014)

[13]   MEF 66 (SOAM for IP Services Draft Standard (R3), August 2019)

[14]   MEF 83 (Network Resource Model – OAM, September 2019)

11 Acknowledgements

- Daniel Bar-Lev (MEF) Editor
- Joel Stradling (Clavem Research)
- Zeev Draer (ADVA)
- Alastair Johnson (Cisco)
- Nico Walters (CMC Networks)
- Wanderlei Mathias de Paulo (Embratel)
- Johan Witters (Nokia)
- Mark Gibson (Amdocs)
- David Ball (Cisco)
- Jack Pugaczewski (CenturyLink)
- Philippe Lochon (Orange)
- Felonimo Bacquiano (Radius)
- Mario Bianchetti (Telecom Italia)
- Matt Duniam (New South Wales Government, Australia)
- Rami Yaron (Infovista)
- Matt Ringhofer (Infovista)
- Larry Samberg (MEF)
- Stan Hubbard (MEF)