Understanding SD-WAN Managed Services

Service Components, MEF LSO Reference Architecture and Use Cases

July 2017

Table of Contents

1. INTRODUCTION 3

2. EXECUTIVE SUMMARY 3

3. KEY BUSINESS DRIVERS AND MARKET OPPORTUNITIES 3

3.1 SD-WAN: Threat or Opportunity? 4
3.2 MEF Lifecycle Service Orchestration Reference Architecture 4

4. FUNDAMENTAL CHARACTERISTICS OF SD-WANS 5

4.1 Secure, IP-based Virtual Overlay Network 5
4.2 Transport-independence of Underlay Network 5
4.3 Service Assurance of each SD-WAN Tunnel 5
4.4 Application-Driven Packet Forwarding 5
4.5 High Availability through Multiple WANs 6
4.6 Policy-based Packet Forwarding 6
4.7 Service Automation via Centralized Management, Control and Orchestration 6
4.8 WAN Optimization 6

5. SD-WAN SERVICE COMPONENTS 7

5.1 SD-WAN Edge 7
5.2 SD-WAN Gateway 8
5.3 SD-WAN Controller 8
5.4 Service Orchestrator 9
5.5 Subscriber Web Portal 9

6. SD-WAN MANAGED SERVICE USE CASES IN THE LSO REFERENCE ARCHITECTURE 10

6.1 SD-WAN service tunneled over Internet and MPLS WANs 10
6.2 SD-WAN service tunneled over Multiple ISPs 10
6.3 SD-WAN Service with SD-WAN Edge vCPE supporting multiple VNFs 11
6.4 SD-WAN Service with SD-WAN Edge VNF running in the Cloud 11
6.5 SD-WAN Service interoperating with MPLS VPN 12

7. SUMMARY OF SD-WAN SERVICE COMPONENTS IN THE LSO RA 12

8. SUMMARY 13

9. ABOUT THE MEF 13

10. PARTICIPATING IN MEF'S SD-WAN WORK 13

11. TERMINOLOGY 14

12. REFERENCES 15

13. ACKNOWLEDGEMENTS 15

List of Figures

Figure 1: Top 5 Purchasing Drivers and Deployment Challenges 4
Figure 2: MEF LSO Reference Architecture 4
Figure 3: Do LSO RA implementations provide a competitive advantage? 4
Figure 4: SD-WAN service tunneled over Internet and MPLS WANs 10
Figure 5: SD-WAN service tunneled over for 4 different ISPs 10
Figure 6: SD-WAN Service with SD-WAN Edge vCPE supporting 11
Figure 7: SD-WAN Service with SD-WAN Edge VNF running in Cloud 11
Figure 8: SD-WAN sites interconnecting with MPLS VPN sites 12
Figure 9: Consolidated diagram of SD-WAN Managed Service Use Cases discussed 12

1. Introduction

As society continues to evolve into a pervasive, interconnection of people, devices and content, networks become an important part of this new world. While the Internet has proven to be the global fabric that interconnects all things, networks need to provide more value than simply raw bandwidth. As networks globally transform themselves into an on-demand and real-time set of programmable systems, many applications are moving to the cloud as an IT utility for a globalized and mobile workforce. While the advancements of Multi-Protocol Label Switching (MPLS) and Carrier Ethernet (CE) have proven to deliver a business grade private Wide Area Network (WAN) for enterprises worldwide, challenges persist. The time it takes to bring up new sites and interconnecting sites or public or private clouds has increasingly become an issue. Today it can take many months to enable a multi-national business to connect various sites globally to each other or to their public and private clouds. Additionally, services changes, even just bandwidth changes, can often take weeks because they involve manual workflow-based processes that are unacceptable for a society now accustomed to on-demand cloud-based applications and services. Software-Defined WANs (SD-WANs) have emerged as one such solution to address these issues.

While the networking industry is embracing SD-WANs as a panacea for an instant and on-demand solution, SD-WAN terminology, deployment scenarios, solution architectures, and open, standardized APIs have yet to be defined. There are many use cases for SD-WANs from providing a complete secure, multi-site VPN service to simply providing access to off-net sites via last mile Internet broadband. Unlike other network connectivity services, SD-WANs use application-driven networking where application traffic, e.g., Skype for Business or SAP traffic, is forwarded over different WANs based on QoS, Security and Business priority policies. Since SD-WANs provide centralized control and management automation plus a secured overlay network over multiple WANs, enterprises worldwide can reduce the cost of their WANs while having similar business grade WAN performance and security guarantees. However, SD-WANs must be operated by either the enterprise or by a service provider. Many enterprises prefer to have a Communications Service Provider (CSP) or Managed Service Provider (MSP) deliver an SD-WAN managed service rather than own and operate the SD-WAN themselves since network management and operations is not their core business. CSPs and MSPs are now aggressively introducing SD-WAN managed services to address the enterprise challenges and deliver agile, assured and orchestrated Third Network connectivity services leveraging SD-WAN technologies.

2. Executive Summary

This paper introduces terminology for different SD-WAN managed service components and illustrates how they fit into MEF's Lifecycle Service Orchestration (LSO) Reference Architecture (RA) to facilitate multi-vendor interoperability and operational agility. The paper provides example SD-WAN managed service use cases illustrating the MEF LSO reference architecture interfaces. The target audience for this paper encompasses a broad audience including Telecom service providers, Internet service providers (ISP), cable operators/MSOs, cloud service providers, managed service providers, and SD-WAN technology providers.

3. Key Business Drivers and Market Opportunities

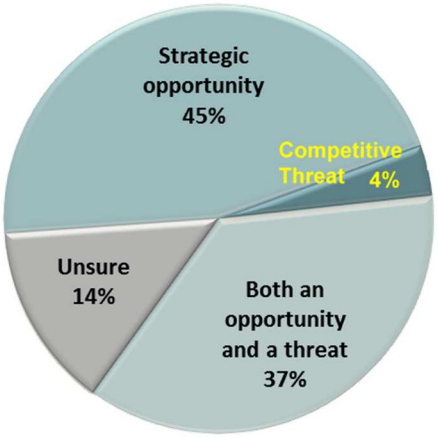
In 2016, MEF and Vertical Systems Group published a report (available exclusively to MEF members) of survey results from respondents representing 50 service providers and 37 technology providers with participants responsible for product management and planning, product marketing, network/systems architecture, and engineering. The survey focused on dynamic network connectivity services, such as SD-WAN services, that enable customers to directly control their network resources on demand. Figure 1 indicates the top 5 purchasing drivers and top 5 deployment challenges when trying to deliver dynamic connectivity services.

Top 5 Purchasing Drivers	Top 5 Deployment Challenges
o Faster service provisioning	o Current OSS/BSS systems are inadequate
o Ability to scale the network on-demand	o Integration with legacy infrastructures
o Business agility to adjust to market dynamics	o Standards are insufficient or incomplete
o Ability to dynamically tailor to application needs	o Network operators not strategically committed
o Lower network connectivity service costs	o Funding constraints for deployment

Figure 1: Top 5 Purchasing Drivers and Deployment Challenges

3.1 SD-WAN: Threat or Opportunity?

Some CSPs and MSPs may view SD-WAN as a threat to their existing connectivity services such as MPLS VPNs. In January 2017, MEF and Vertical Systems published a report of 58% service provider and 42% technology provider respondents with job responsibilities including product management, product planning, product/technology development, network/systems architecture, engineering, and professional services. In the report only 4% of respondents viewed SD-WAN as a competitive threat while 45% viewed SD-WAN as a strategic opportunity. 37% viewed SD-WAN as both an opportunity and threat.



3.2 MEF Lifecycle Service Orchestration Reference Architecture

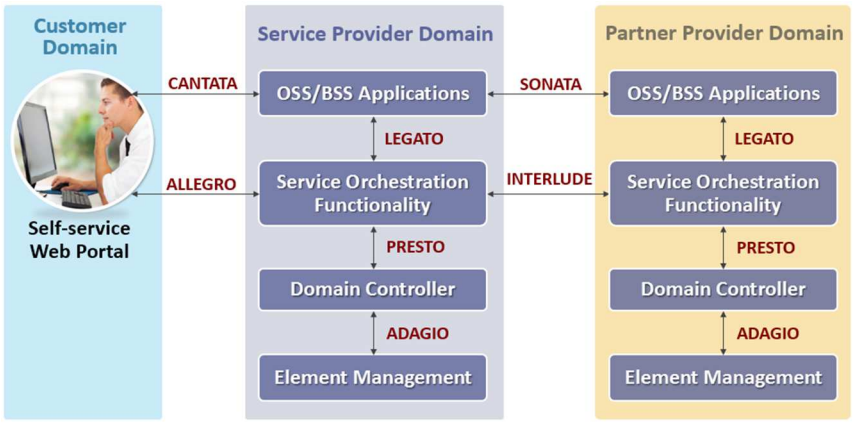


Figure 2: MEF LSO Reference Architecture

Many of the top purchasing drivers and deployment challenges from the survey relate to insufficient or inadequate automation and agility to deliver dynamic, on-demand services like SD-WAN. MEF has developed the Lifecycle Service Orchestration Reference Architecture, defined in MEF 55, enabling implementations to better address these challenges by providing a standard architecture and framework, which, in turn promotes interoperability. The MEF LSO RA defines APIs for essential functions such as service ordering, configuration, fulfillment, assurance and billing. These APIs are being developed for Northbound-Southbound interfaces from the lowest layer infrastructure to the highest layer business applications within a given service provider's network. The APIs are also being developed for Eastbound-Westbound interfaces providing inter-Provider communications.

As part of the MEF-Vertical Systems survey, respondents were asked if they think implementations using the MEF LSO Reference Architecture will have a competitive advantage. The results were overwhelmingly positive indicating that using the LSO RA to standardize the interfaces (APIs) between LSO functions as illustrated in Figure 2 will address the deployment challenges.

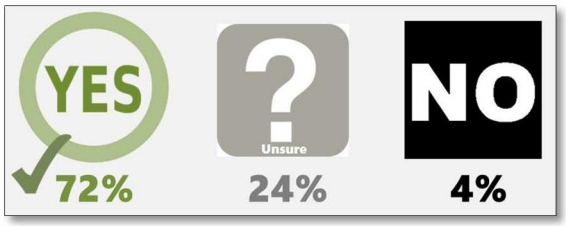


Figure 3: Do LSO RA implementations provide a competitive advantage?

4. Fundamental Characteristics of SD-WANs

No industry standard definition exists for an SD-WAN. SD-WAN implementations have incorporated WAN technologies and functions that have been developed over the years such as VPN, WAN Optimization, IPsec tunneling, hybrid WAN, deep packet inspection, policy management, service assurance and analytics while incorporating newer SDN, NFV, and Service Orchestration technologies. The latter three technologies provide the integration and service deployment automation that has made SD-WAN Managed Services so compelling. SD-WAN Managed Services are a specific use case for a MEF Third Network service using overlay networking technologies to deliver agile, assured and orchestrated application-driven connectivity services. Also, SD-WANs can operate over Internet access connections, enabling off-net sites to be quickly added to the SD-WAN without establishing interconnect agreements with off-net access providers.

MEF is working to standardize SD-WAN terminology, service components, reference architectures, LSO APIs, and an SD-WAN service definition. While SD-WAN service offerings will vary among service providers, Sections 4.1 to 4.7 discuss fundamental capabilities of SD-WAN managed services. Section 4.8 “WAN Optimization” is often delivered as a value added service to the base SD-WAN service offering. Other value added services could include advanced security services beyond an SD-WAN’s basic firewall and NAT capabilities.

4.1 Secure, IP-based Virtual Overlay Network

SD-WAN provide secure, IP-based virtual overlay networks that typically uses IPsec tunnels over Internet or MPLS underlay networks. SD-WANs support any topology, e.g., full/partial mesh and hub & spoke. Because IP-based SD-WANs are virtual overlay networks, no modifications need be made to any of the underlay networks. Also, IP-based SD-WAN implementations often use the public Internet as one of their WANs in which case they need to include some firewall and Network Address Translation (NAT) capabilities.

4.2 Transport-independence of Underlay Network

SD-WANs operate over any type of wireline or wireless access networks. Each WAN may use a different underlay service/technology, e.g., Dedicated Internet Access, Broadband Internet (Cable, DSL or PON), Internet over LTE, MPLS over T1s, or MPLS over fiber. This independence from the underlay network enables tremendous agility and simplicity in creating and deploying virtual network connectivity.

4.3 Service Assurance of each SD-WAN Tunnel

Service assurance is a critical part of any managed network service, including SD-WAN managed services. QoS performance, e.g., packet loss and packet latency, is measured over each SD-WAN tunnel in real-time. These measurements determine whether a particular WAN meets the performance requirements of an application resulting in application-based performance assurance. For example, a conferencing application may requires a packet loss less than 2% and a packet latency less than 50ms for an acceptable quality of experience. If any WAN meets this criteria, the application can be forwarded provided no pre-existing policy disallows transmission over a particular WAN, e.g., only use MPLS VPN and not Internet. Also, through techniques discussed in Section 4.8, the SD-WAN service can correct for packet loss in the underlay network resulting in higher QoS in the SD-WAN overlay tunnel.

4.4 Application-Driven Packet Forwarding

SD-WANs perform application-level classification (up to OSI Layer 7) at the customer premises. This enables subscribers to specify the applications which are forwarded over SD-WAN tunnels over different WANs. The WAN or SD-WAN tunnel selection is determined by an application’s QoS, security or business policy requirements.

4.5 High Availability through Multiple WANs

SD-WANs support packet forwarding over one or more WANs at each site. This is often referred to as hybrid WAN when a site has two or more WAN connections and each WAN uses a different WAN technology, e.g., Internet and MPLS VPN. When using multiple WANs, SD-WAN tunnels are created over each WAN. Each WAN underlay network can use a different wireline or wireless access provider providing SD-WAN tunnel diversity. SD-WAN tunnels can operate over different underlay network technologies. For example, SD-WAN tunnels can be created over Internet connections from different ISPs, Internet and MPLS VPNs, or MPLS VPN and LTE (Internet) enabling service provider, network path, or physical path diversity.

4.6 Policy-based Packet Forwarding

SD-WANs use policies to make application forwarding (or blocking) decisions for SD-WANs tunnels over each WAN. Policies can be based on each application or application grouping, e.g., real-time media or conferencing application. Policy enforcement considers an application's QoS performance requirements or an organization's security or business priority policy requirements. For example, a QoS policy may be set so Skype for Business packets are forwarded over any WAN as long as its QoS performance requirements, e.g., packet latency and loss, are met so users get an acceptable quality of experience (QoE). A security policy may be set so Skype for Business packets are sent over the MPLS VPN and not the Internet. A business priority policy may be set so payment card transactions be sent ahead of any Skype for Business packets. This may result in an occasional degradation of a user's QoE for a Skype for Business call occurring during the payment card transaction. However, in this case, the organization deems their payment card transactions to have higher importance than Skype for Business calls.

4.7 Service Automation via Centralized Management, Control and Orchestration

Service automation is achieved via centralized management, control and orchestration of SD-WAN tunnels with automatic configuration of SD-WAN customer premises equipment. The latter is referred to as "zero touch provisioning" (ZTP) where all configuration information is pre-populated into the centralized management system. When the SD-WAN customer premises equipement (CPE) is powered up and connected to the Internet, it retrieve its configuration and policies without needing to send a service provider installer to the customer premises. ZTP enables subscribers to self-install the CPE by simply plugging in LAN, WAN and power cables. Management, control and orchestration functions are accessible via web portals or APIs. Depending upon the role assigned to a user, e.g., subscriber, service provider or network administrator, on-demand service modifications and service monitoring can be done via a web portal.

4.8 WAN Optimization

WAN Optimization is the compilation of many different functions that increase WAN bandwidth and QoS performance. WAN Optimization can include data deduplication, data compression, data caching, forward error correction and protocol spoofing. Since WAN optimization is not required at all SD-WAN sites, it is often delivered as a value-added service. Data deduplication, data compression, data caching and protocol spoofing reduce the amount of WAN bandwidth required by minimizing the amount of data transmitted over the WAN. Forward error correction (FEC) compensates for WAN packet loss by sending duplicate packets over multiple WANs and then reassembles the packets in the correct sequence at the receiving end. FEC enables SD-WANs overlay tunnels to provide essentially zero packet loss using lower cost, higher packet loss Internet broadband underlay networks. This approach is used to augment or replace higher cost private lines or VPN services.

5. SD-WAN Service Components

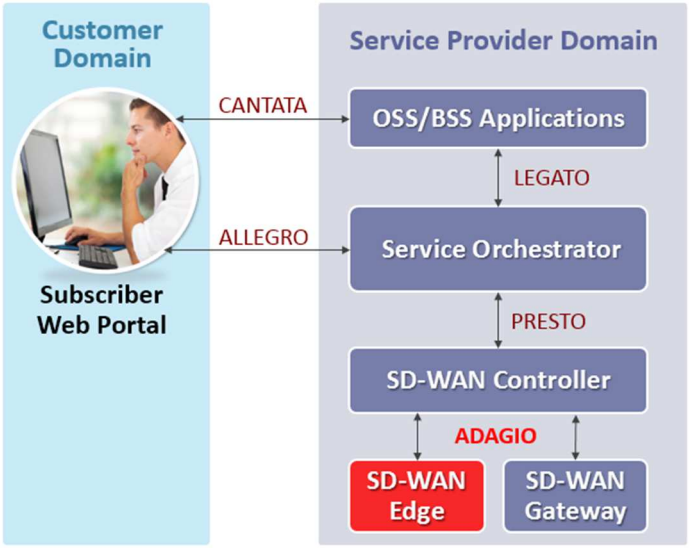
This section describes the fundamental functionality of service components that may be used in an SD-WAN managed service. Subsequent MEF publications will articulate more details as they are further defined. This section will illustrate where each of these service components fit into MEF's LSO Reference Architecture.

- SD-WAN Edge
- SD-WAN Controller
- Service Orchestrator
- SD-WAN Gateway
- Subscriber Web Portal

Using the generalized MEF LSO Reference Architecture from Figure 2, we can overlay each of the SD-WAN Service Components to understand their placement in the architecture and the associated LSO RA interfaces with which they must interact. Refer to Figure 9 for the placement of the different SD-WAN service components in a comprehensive network diagram. To simplify the discussion, this paper will focus on a single provider domain and thus not cover the LSO RA Sonata and Interlude interfaces which are used for the communication of inter-provider service functions.

5.1 SD-WAN Edge

The SD-WAN Edge is where the SD-WAN tunnel is initiated or terminated and provides the SD-WAN service demarcation similar to how an Ethernet NID provides the service demarcation for a Carrier Ethernet service. The SD-WAN Edge creates and terminates secured (encrypted) tunnels over different types of wired or wireless underlay networks, such as T1s/E1s, broadband Internet (DSL, Cable, and PON), WiFi and LTE wireless access networks, and IP (Internet) and MPLS core networks.

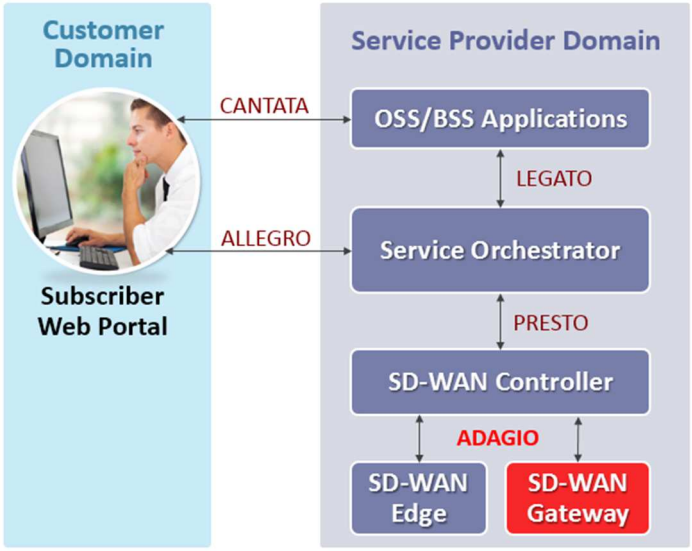


The SD-WAN Edge also performs application-based QoS and security policy enforcement, application forwarding over one or more WAN connections, and QoS performance measurements over each WAN to determine WAN path selection. The SD-WAN Edge may also perform WAN optimization functions such as packet buffering/reordering, data deduplication, data compression, and forward error correction. Since SD-WAN Edges often connect to public Internet WANs, they would include, at a minimum, some NAT and firewall capabilities.

The SD-WAN Edge functionality may be provided by a physical CPE device resident on the customer premises and managed by the CSP or MSP. SD-WAN Edge functionality may also be implemented as a software-based virtual network function (VNF) which may run on a virtual CPE (vCPE) at the customer premises or any other type of generalized compute platform, e.g., server in a data center, which may also be managed by the CSP or MSP or by a cloud service provider. Note that vCPE, uCPE and 'white box' server are often used interchangeably in the industry. This remainder of this paper will use the vCPE term.

The MSP or CSP operates and maintains the SD-WAN Edge as part of an SD-WAN managed service. In the MEF LSO RA, an SD-WAN Edge communicates with the SD-WAN Controller via the Adagio interface.

5.2 SD-WAN Gateway



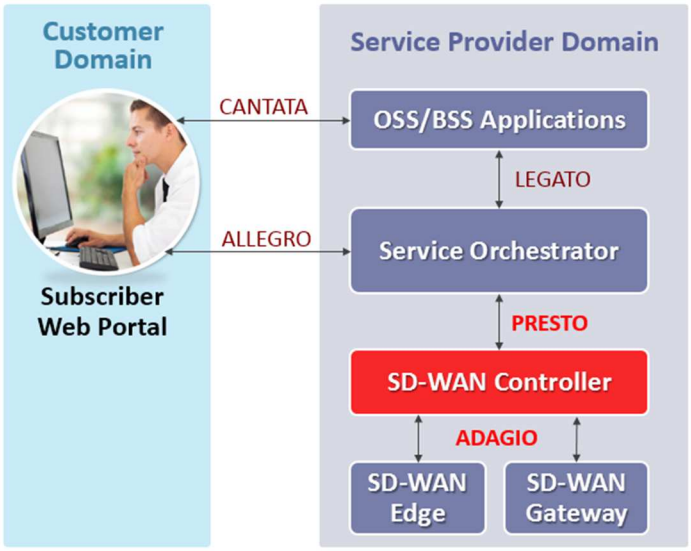
The SD-WAN Gateway is a special case of an SD-WAN Edge that also enables sites interconnected via the SD-WAN to connect to other sites interconnected via alternative VPN technologies, e.g., CE or MPLS VPNs. There are two ways to deliver an SD-WAN service to sites connected via another VPN service. One way requires an SD-WAN Edge to be placed at each subscriber site connected to the VPN service so SD-WAN tunnels can be created over the VPN.

Another way is to use an SD-WAN Gateway. In this scenario, an SD-WAN Gateway initiates and terminates the SD-WAN tunnels like an SD-WAN Edge and initiates and terminates VPN connections to and from sites interconnected by the VPN. This approach enables sites interconnected via SD-WAN and other VPN technology domains to intercommunicate. This approach does not require SD-WAN Edges to be placed at each VPN site to achieve interconnectivity. However, SD-WAN service capabilities such as application-based traffic forwarding over multiple WANs or QoS and Security policy management will not be available at the MPLS VPN sites because they do not have SD-WAN Edges which perform these functions.

The MSP or CSP operates and maintains the SD-WAN Gateways as part of an SD-WAN managed service. In the MEF LSO RA, the SD-WAN Gateway communicates with its SD-WAN Controller via the Adagio interface.

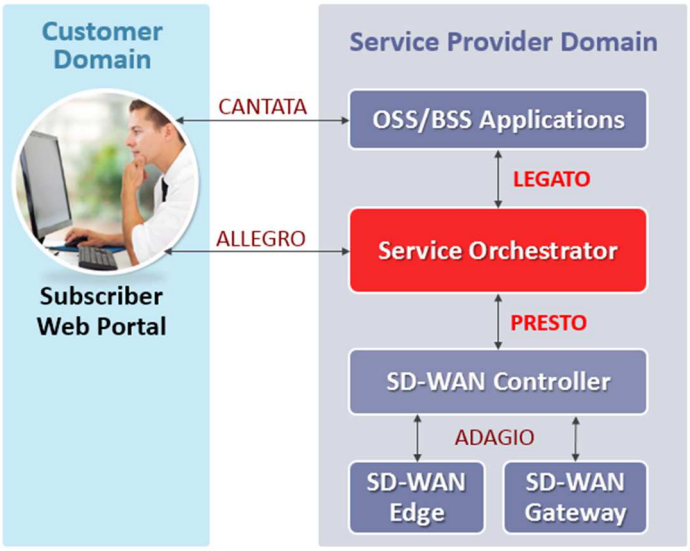
5.3 SD-WAN Controller

The SD-WAN Controller provides physical or virtual device management for all SD-WAN Edges and SD-WAN Gateways associated with the controller. This includes, but is not limited to, configuration and activation, IP address management, and pushing down policies onto SD-WAN Edges and SD-WAN Gateways. The SD-WAN controller maintains connections to all SD-WAN Edges and SD-WAN Gateways to identify the operational state of SD-WAN tunnels across different WANs and retrieve QoS performance metrics for each SD-WAN tunnel. These metrics are used by the Service Orchestrator.



The MSP or CSP operates and maintains the SD-WAN Controller as part an SD-WAN managed service. In the MEF LSO RA, the SD-WAN Controller communicates northbound with its Service Orchestrator via the Presto interface and southbound, via the Adagio interface, to SD-WAN Edges and SD-WAN Gateways it controls. Note that some SD-WAN implementations may combine the SD-WAN Controller and Service Orchestrator.

5.4 Service Orchestrator

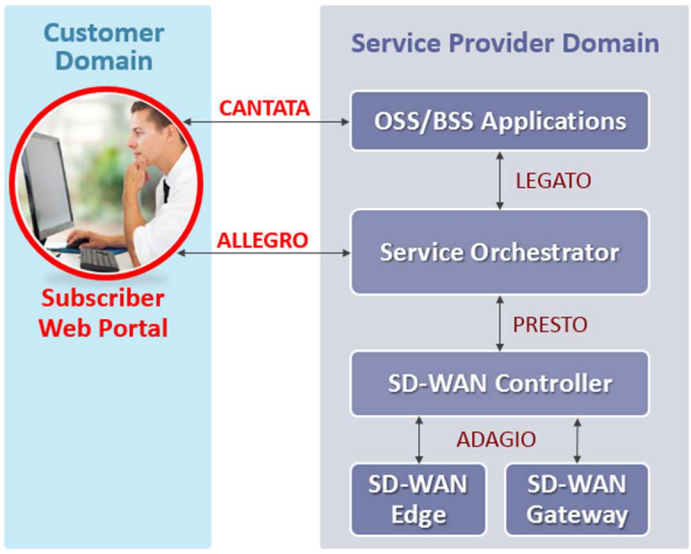


The Service Orchestrator provides the service management of the SD-WAN service lifecycle including service fulfillment, performance, control, assurance, usage, analytics, security and policy. For example, the Service Orchestrator is responsible for configuring the end-to-end SD-WAN managed service between SD-WAN Edges and SD-WAN Gateways over one or more underlay WANs, e.g., Internet and MPLS, setting up application-based forwarding over WANs based on security, QoS or business or intent-based policies.

The MSP or CSP operates and maintains the Service Orchestrator with an SD-WAN managed service. In the MEF LSO RA, the Service Orchestrator communicates northbound with the Service Provider's OSS/BSS applications via the Legato interface for functions such as service activation and southbound to the SD-WAN Controller via the Presto interface. The Service Orchestrator also can obtain service modification requests from a Subscriber Portal via the Allegro interface. Note that some SD-WAN implementations may combine the SD-WAN Controller and Service Orchestrator.

5.5 Subscriber Web Portal

The MSP or CSP typically integrates the Subscriber Web Portal for the SD-WAN managed service into their existing customer portal used for other managed services. In the MEF LSO RA, the Subscriber Web Portal communicates with the Service Provider's OSS/BSS applications via the Cantata interface for functions such as initial subscriber account setup, ensuring a service payment method is available and active, authorize a user to activate a new service, and the initial SD-WAN service activation.



After the SD-WAN service is activated, the Subscriber Web Portal communicates with the Service Orchestrator via the Allegro interface for SD-WAN service modifications such as setting up different QoS, security or business policies based on a user's role, e.g., 'view-only' capability or ability to modify the SD-WAN service. The Service Orchestrator also obtains service modification requests from the Subscriber Portal via the Allegro interface.

6. SD-WAN Managed Service Use Cases in the LSO Reference Architecture

6.1 SD-WAN service tunneled over Internet and MPLS WANs

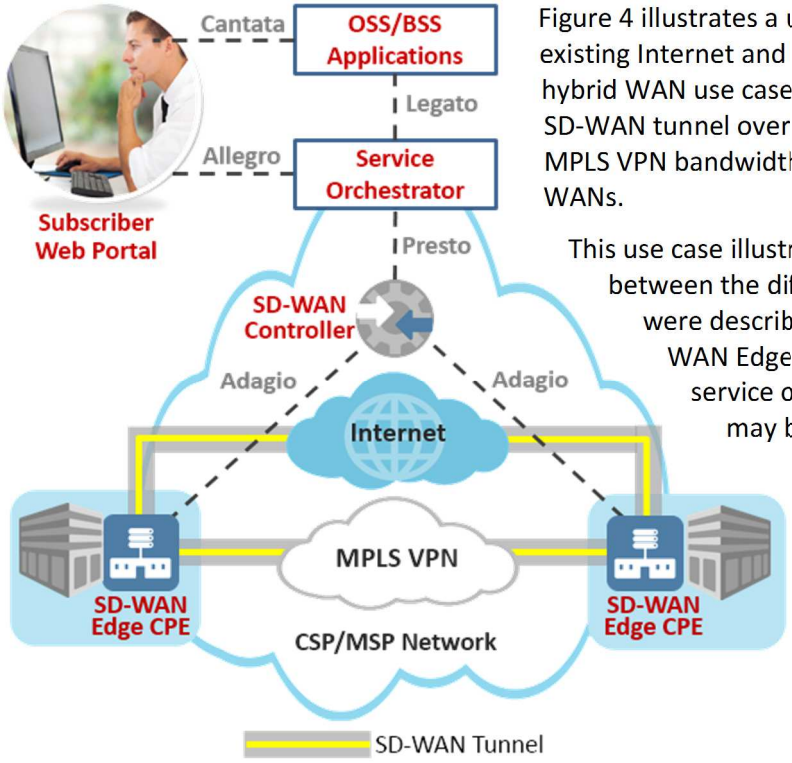


Figure 4: SD-WAN service tunneled over Internet and MPLS WANs

Figure 4 illustrates a use case for an SD-WAN managed across existing Internet and MPLS VPN WANs between two sites. This hybrid WAN use case enables the subscriber to use an encrypted SD-WAN tunnel over the Internet to augment their site-to-site MPLS VPN bandwidth and achieve higher resiliency using two WANs.

This use case illustrates the different LSO RA interfaces between the different SD-WAN service components that were described in Section 5. Both sites are using an SD-WAN Edge CPE. The CSP or MSP delivers the SD-WAN service over existing Internet and MPLS VPNs which may be provided by a different CSP or MSP.

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

6.2 SD-WAN service tunneled over Multiple ISPs

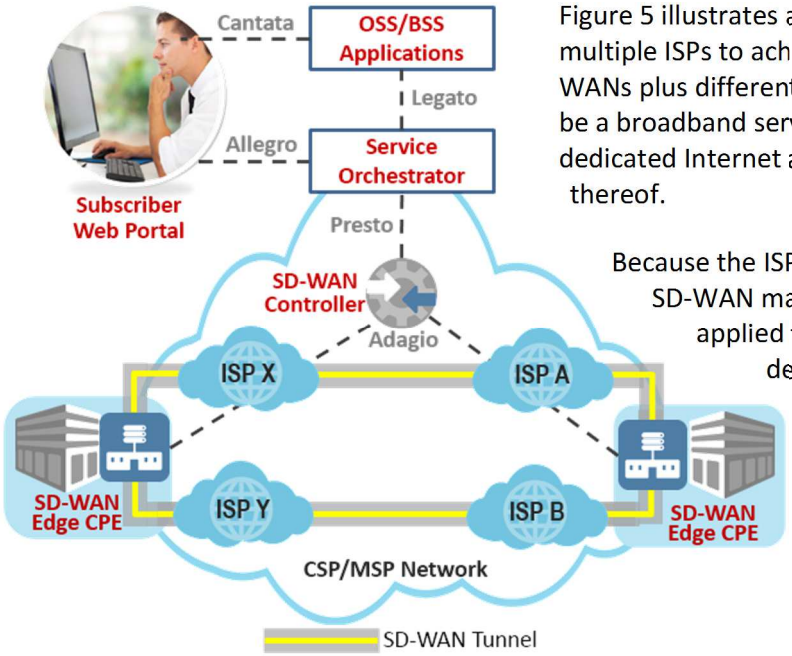


Figure 5: SD-WAN service tunneled over for 4 different ISPs

Figure 5 illustrates a use case for an SD-WAN service across multiple ISPs to achieve the WAN resiliency using multiple WANs plus different ISPs. The ISP's Internet connection could be a broadband service using DSL or Cable Internet or a dedicated Internet access (DIA) service or a combination thereof.

Because the ISPs may not be the CSP or MSP delivering the SD-WAN managed service, this use case could be applied to a larger SD-WAN managed service deployment where both sites in Figure 5 are off-net and can only be reached via an Internet WAN. Furthermore, by having multiple ISPs and multiple Internet WANs for each site, the CSP or MSP offering the SD-WAN managed service could offer a better SLA due to the added WAN resiliency.

6.3 SD-WAN Service with SD-WAN Edge vCPE supporting multiple VNFs

Figure 6 illustrates a use case for an SD-WAN service across multiple WANs using an SD-WAN Edge CPE (left site) and an SD-WAN Edge vCPE (right site). By using the SD-WAN Edge VNF on the SD-WAN Edge vCPE, the CSP or MSP can provide additional revenue-generating virtual network services on the vCPE by adding more VNFs provided the vCPE has sufficient compute resources to support them.

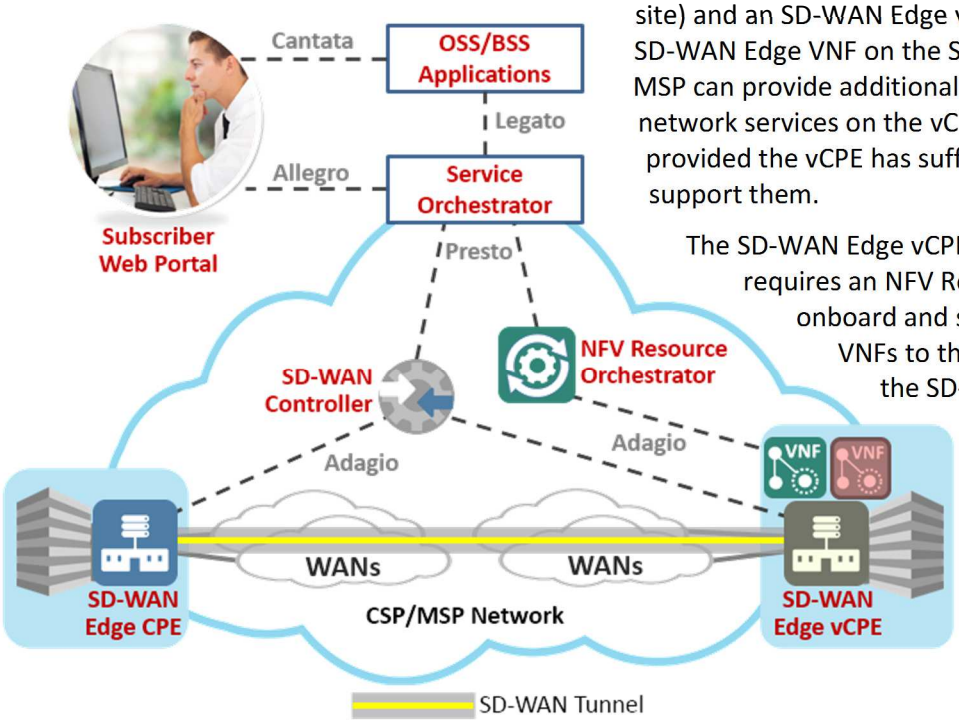


Figure 6: SD-WAN Service with SD-WAN Edge vCPE supporting SD-WAN Edge VNF and additional Virtual Network Services

The SD-WAN Edge vCPE acting as NFV Infrastructure requires an NFV Resource Orchestrator to onboard and service chain the additional VNFs to the SD-WAN Edge VNF. Both the SD-WAN Controller and NFV Resource Orchestrator are managed by a Service Orchestrator providing the LSO Service Orchestration Functions (SOF) which orchestrates both the SD-WAN service plus additional virtual network services delivered by the VNFs on the vCPE.

6.4 SD-WAN Service with SD-WAN Edge VNF running in the Cloud

Figure 7 illustrates a use case for an SD-WAN service across multiple WANs with an SD-WAN Edge CPE (left site) and an SD-WAN Edge VNF running in a cloud environment. In this use case, the SD-WAN service tunnel begins on the SD-WAN Edge CPE at the left site and terminates on the physical compute server or virtual machine (VM) where the application is running, e.g., in a cloud service provider environment.

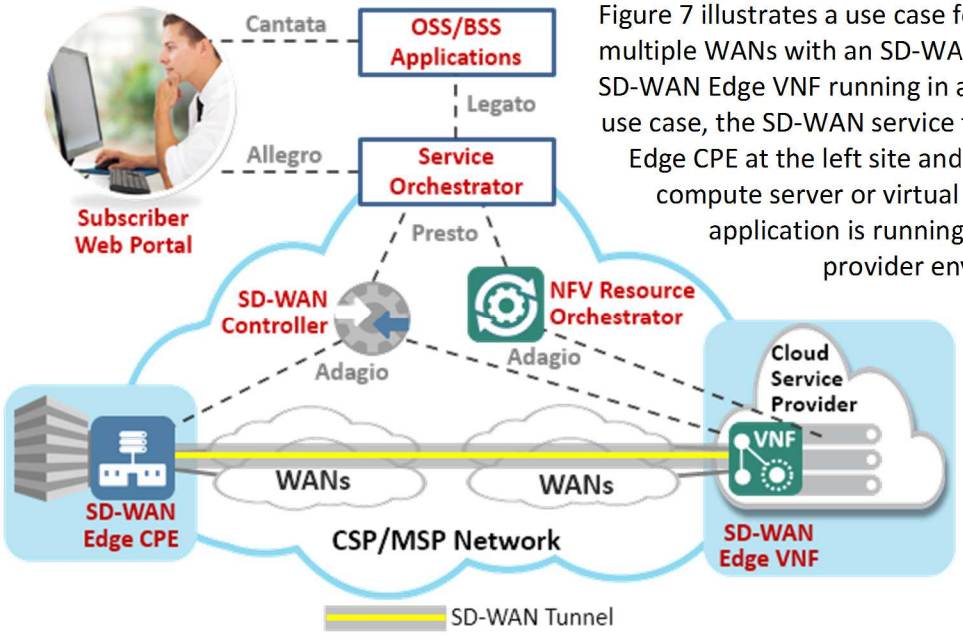


Figure 7: SD-WAN Service with SD-WAN Edge VNF running in Cloud

The benefit of terminating the SD-WAN tunnel on the server or VM is that the SD-WAN tunnel provides secure connectivity between the site on the left and the cloud applications inside the cloud service provider's data center.

6.5 SD-WAN Service interoperating with MPLS VPN

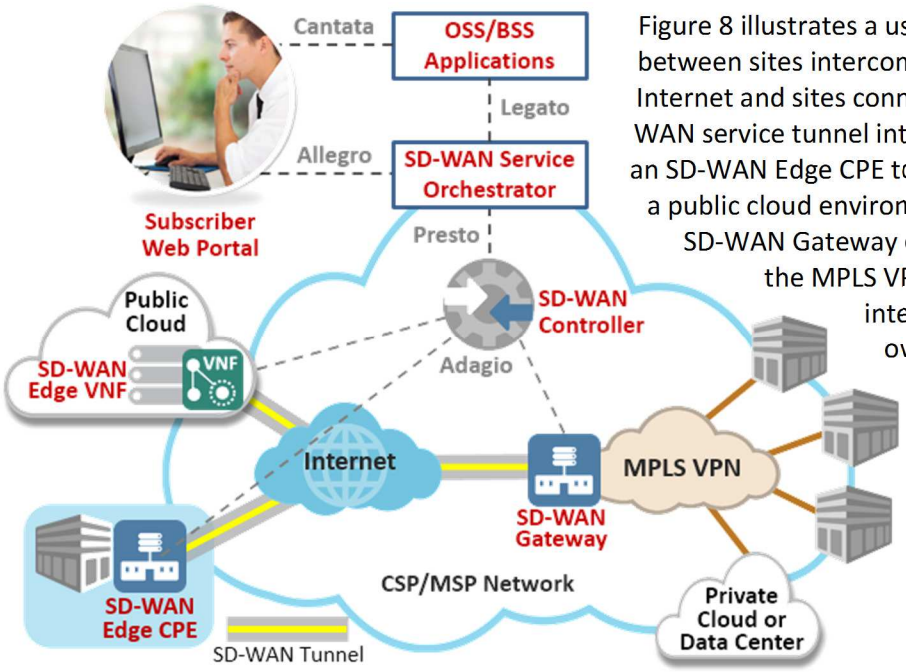


Figure 8: SD-WAN sites interconnecting with MPLS VPN sites

Figure 8 illustrates a use case for an SD-WAN Gateway between sites interconnected via an SD-WAN over the Internet and sites connected via a MPLS VPN. The SD-WAN service tunnel interconnects the bottom left site via an SD-WAN Edge CPE to an SD-WAN Edge VNF running in a public cloud environment to an SD-WAN Gateway. An SD-WAN Gateway enables sites interconnected via the MPLS VPN to communicate with sites interconnected via SD-WAN tunnels over the Internet.

This use case provides a simpler, less costly, faster way to interconnect existing MPLS VPN sites with new, typically off-net, sites using a local Internet connection when it may not be cost effective or take too long to build out the MPLS VPN to reach these new sites.

7. Summary of SD-WAN Service Components in the LSO RA

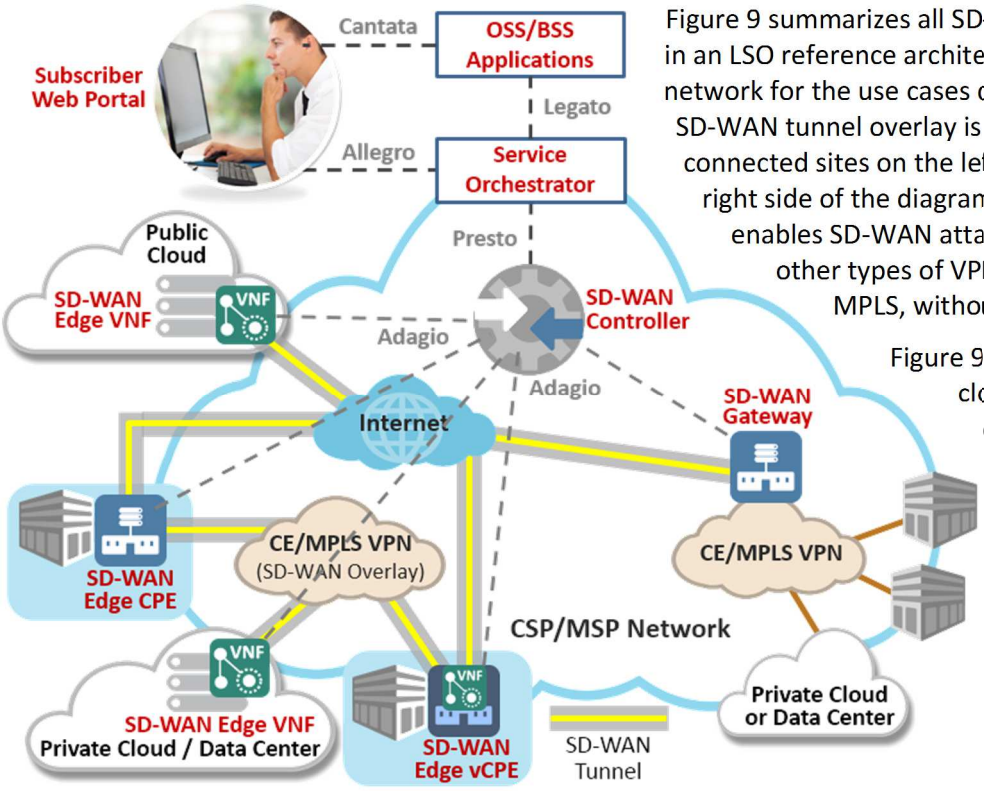


Figure 9: Consolidated diagram of SD-WAN Managed Service Use Cases discussed

Figure 9 summarizes all SD-WAN service components in an LSO reference architecture for a single operator network for the use cases discussed in this paper. An SD-WAN tunnel overlay is used for Internet and MPLS-connected sites on the left of the diagram. On the right side of the diagram, an SD-WAN Gateway enables SD-WAN attached sites to connect to other types of VPN-attached sites, e.g., CE or MPLS, without using an SD-WAN overlay.

Figure 9 also illustrates sites, public cloud and private cloud/data centers using SD-WAN Edge CPE, vCPE and VNFs, respectively, to create SD-WAN tunnels over the Internet and CE or MPLS VPN. SD-WAN Edge VNFs illustrate how SD-WAN tunnels can be extended to the applications or VMs running inside the cloud or data center.

8. Summary

The networking industry is embracing SD-WANs. However, SD-WAN terminology, deployment scenarios, solution architectures, and open APIs have yet to be standardized. A common SD-WAN vernacular would enable buyers, sellers and users to more effectively communicate requirements and intent while open, standard APIs facilitate and accelerate SD-WAN implementations and service deployments. SD-WAN benefits for service providers and subscribers are many. CSPs and MSPs are working towards introducing SD-WAN managed services to address enterprises' desire to outsource their managed network services.

MEF views SD-WAN managed services as a specific use case delivering on its Third Network vision of agile, assured and orchestrated connectivity services. MEF has created SD-WAN service projects to educate the market and build reference implementations using open, standard LSO APIs. This paper introduces some of this work. More will be introduced including Proof of Concept showcases demonstrating different SD-WAN reference implementations using LSO APIs plus additional market education through webinars, white papers and workshops at industry events.

9. About the MEF

An industry association of 210+ member companies, MEF is enabling service providers to create a global ecosystem of networks that deliver agile, assured, and orchestrated services for the digital economy and hyper-connected world. These services provide an on-demand, cloud-centric experience with user and application-directed control over network resources and service capabilities. They are delivered over automated, virtualized, and interconnected networks powered by LSO, SDN, and NFV. MEF produces globally adopted service specifications, LSO frameworks, open LSO APIs, reference implementations, and certification programs. MEF currently is developing open LSO APIs for orchestrating standardized wavelength, Carrier Ethernet, IP, SD-WAN, and Layer 4-7 services across multiple provider networks. For more information, visit www.MEF.net.

10. Participating in MEF's SD-WAN Work

MEF has two SD-WAN projects. The OpenCS SD-WAN project focuses on defining SD-WAN reference implementations (RI) and proof of concepts (POCs) using the MEF LSO Reference Architecture APIs to facilitate and accelerate SD-WAN service deployments. The project develops user stories which in turn are used to define and implement the different MEF LSO APIs based on which functionality is being proven out for a given RI or POC. The SD-WAN Market Education project is developing market educational material in the form of SD-WAN managed service tutorials, use cases, and promoting MEF SD-WAN-related products produced by the CTO group and other MEF committees and projects. We welcome MEF member participation in these projects.

11. Terminology

The terminology in the table below is used in this paper.

Term	Definition
CSP	Communications Services Provider. Encompasses a broad range of service providers including telecom service providers, MSOs, network service providers, and wireless service providers
Overlay Network	A virtual network abstracted from the transport (underlay) network
MSP	Managed Services Provider. A service provider that delivers managed network services. May also be a CSP.
SD-WAN Controller	An SD-WAN function responsible for managing and controlling the SD-WAN Edges and SD-WAN Gateways
SD-WAN Edge CPE	The physical equipment implementation of an SD-WAN Edge
SD-WAN Edge	The entity that provides all SD-WAN network functions (NFs) required where the SD-WAN overlay network (tunnel) is initiated and terminated. The NFs could be implemented as a physical CPE, a VNF running on a vCPE/uCPE, or a VNF running on a server in a data center. When referring to a particular implementation of this NF, you simply add an additional word indicating its implementation, e.g., SD-WAN Edge CPE, SD-WAN Edge VNF, etc.
SD-WAN Gateway	An network function (physical or virtual) that provides interoperability between SD-WAN connections to other types of VPNs such as MPLS VPNs.
SD-WAN Edge VNF	The virtual network function (VNF) implementation of the SD-WAN Edge that can run on a vCPE/uCPE or server
Traffic Steering	A technique to migrate application flows from one WAN link to another while preserving session persistency
Underlay Network	The transport network over which the SD-WAN service operates. This could be an access network or core network.
vCPE	Virtual CPE. A device located at the customer premises on which VNFs run using the Decentralized VNF deployment model defined in MEF's Carrier Ethernet and NFV paper. Note that vCPE, uCPE and 'white box' server are often used interchangeably in the industry.
WAN Optimization	Methods for improving performance over a WAN which can include data compression, TCP re-transmission optimizations (optimized for low bandwidth & high latency networks), application proxies, data de-duplication, forward error correction, etc.

12. References

The table below includes references to material discussed in this paper and other related material. Note that some reference are available only the MEF members and require MEF Wiki login credentials.

Reference	Source / Publication Date
An Industry Initiative for Third Generation Network and Services	MEF Forum / November 2016
Viewpoint 2016: Dynamic Network Connectivity Services - A Research Study Focused On Dynamic Third Network Services Powered By CE 2.0, LSO, SDN & NFV	Vertical Systems Group and MEF Forum *(Available exclusively to MEF members)* / February 2016
Emerging Third Network Services Enabled By LSO, SDN, NFV & CE 2.0	Vertical Systems Group and MEF Forum *(Available exclusively to MEF members)* / January 2017
MEF 55: Lifecycle Service Orchestration Reference Architecture and Framework	MEF Forum / March 2016
MEF OpenCS SD-WAN Project	MEF CTO Office *(Access to project on MEF wiki available exclusively to MEF members)*
MEF SD-WAN Market Education Project	MEF Global Marketing Committee *(Access to project on MEF wiki available exclusively to MEF members)*
MEF Third Network Vision	MEF Forum / November 2014
Carrier Ethernet and NFV	MEF Forum / July 2016

13. Acknowledgements

Editor and Principal Author:

- Ralph Santitoro, Fujitsu Network Communications

Contributors:

- Dudu Bercovich, Ceragon
- Lia d'Arlach, Fujitsu Network Communications
- Pascal Menezes, MEF
- Evgeniy Zhukov, NEC/Netcracker
- Anthony Peres, Nokia
- Yoav Cohen, RAD
- Joseph Ruffles, Riverbed
- Nav Chander, Silver Peak
- Tim Van Herck, VeloCloud