SD-WAN AND BEYOND: DELIVERING VIRTUAL NETWORK SERVICES

A Technical Paper prepared for SCTE/ISBE by

Ralph Santitoro
Head of SDN/NFV/SD-WAN Solutions
Fujitsu Network Communications
(805) 791-0711
ralph.santitoro@us.fujitsu.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

Introduction

Software-defined wide area networks (SD-WANs) have generated much enthusiasm in the industry because they solve real business challenges for both enterprise subscribers and communications service providers (CSPs). SD-WANs leverage software-defined networking (SDN), network functions virtualization (NFV) and lifecycle service orchestration (LSO) technologies making them the ideal foundation for deploying new, on-demand virtual network services. This paper describes the fundamental capabilities of SD-WAN services, their operational and deployment considerations, key benefits to enterprise subscribers and CSPs, and use cases for connecting places and things. The paper also discusses key architectural and deployment considerations required to extend an SD-WAN service via virtual network functions (VNFs) operating on virtual customer premises equipment (vCPE) and virtual private clouds (VPC) to deliver additional virtual network services.

The Journey to Virtual Network Services

SD-WANs are the confluence of several technologies that have developed over the years augmented with newer technologies providing virtualization and centralized management and control resulting in virtual network services. The evolution to SD-WAN as we know it today fundamentally consists of wide area network (WAN) connectivity using the Internet protocol (IP) to create virtual private networks (VPNs) secured typically through IPsec-encrypted tunnels. The IPsec tunnels operate over a physical underlay (transport) network. This enables SD-WANs to operate over multiple WANs types, e.g., dedicated Internet access and MPLS, referred to as hybrid WANs. SD-WANs also support WAN optimization which serves two purposes; increase the amount of usable bandwidth and correct for packet loss over WANs.

SD-WANs can be constructed using the aforementioned technologies. However, SD-WANs didn't become highly popular until automation was added via centralized management and control using SDN, NFV and end-to-end service orchestration. Refer to ***Figure 1***.

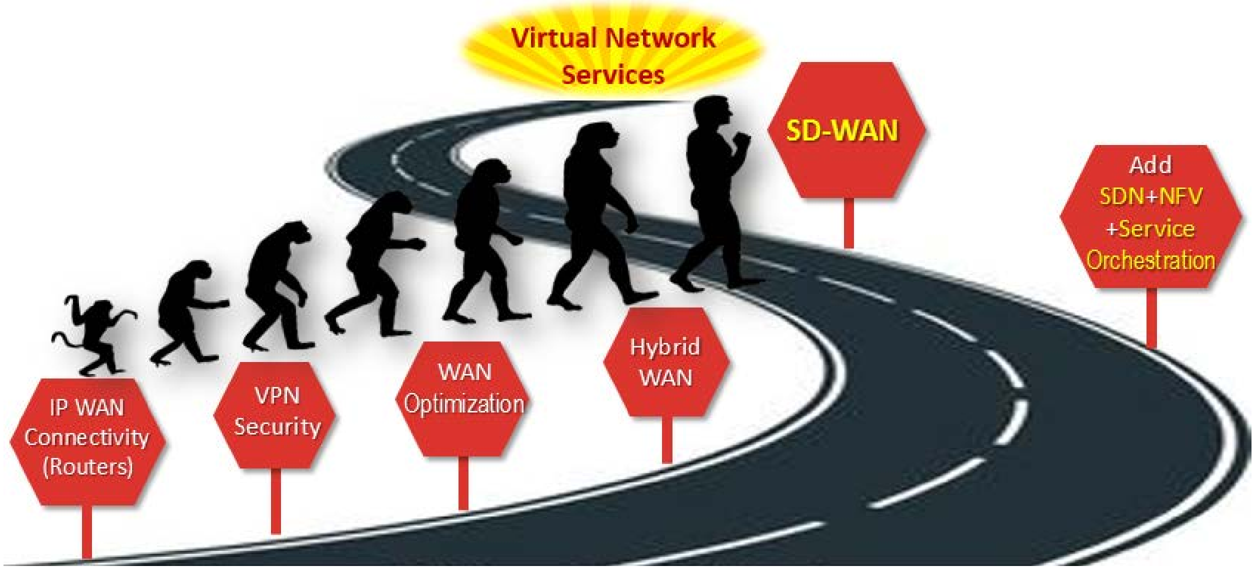

Figure 1 - The journey to SD-WAN and beyond

What is an SD-WAN and what does it do?

SD-WANs are over-the-top (OTT) virtual overlay networks that operate over any underlay network. This means that with SD-WANs, any network topology can be created over wired or wireless access and core transport networks. This unique property enables SD-WANs to be created over underlay networks using different technologies such as Carrier Ethernet, broadband Internet [digital subscriber line (DSL), Cable, or passive optical network (PON)], WiFi or LTE access networks or IP or MPLS core networks. Also, because SD-WANs create virtual overlay networks, one can create any topology to interconnect sites and connect sites to their public and private clouds, software-as-a-service (SaaS) applications running in the cloud and their data centers.

To simplify operations, reduce costs and enhance agility and security, enterprises are accelerating the migration of applications running on servers on their premises, e.g., Microsoft Exchange Server, to the cloud using a SaaS applications, e.g., Microsoft Office 365. Because of this, SD-WANs will play an even larger role in interconnecting sites more often to the cloud rather than to other sites since information exchange will be done via cloud-centric applications. Refer to ***Figure 2***.

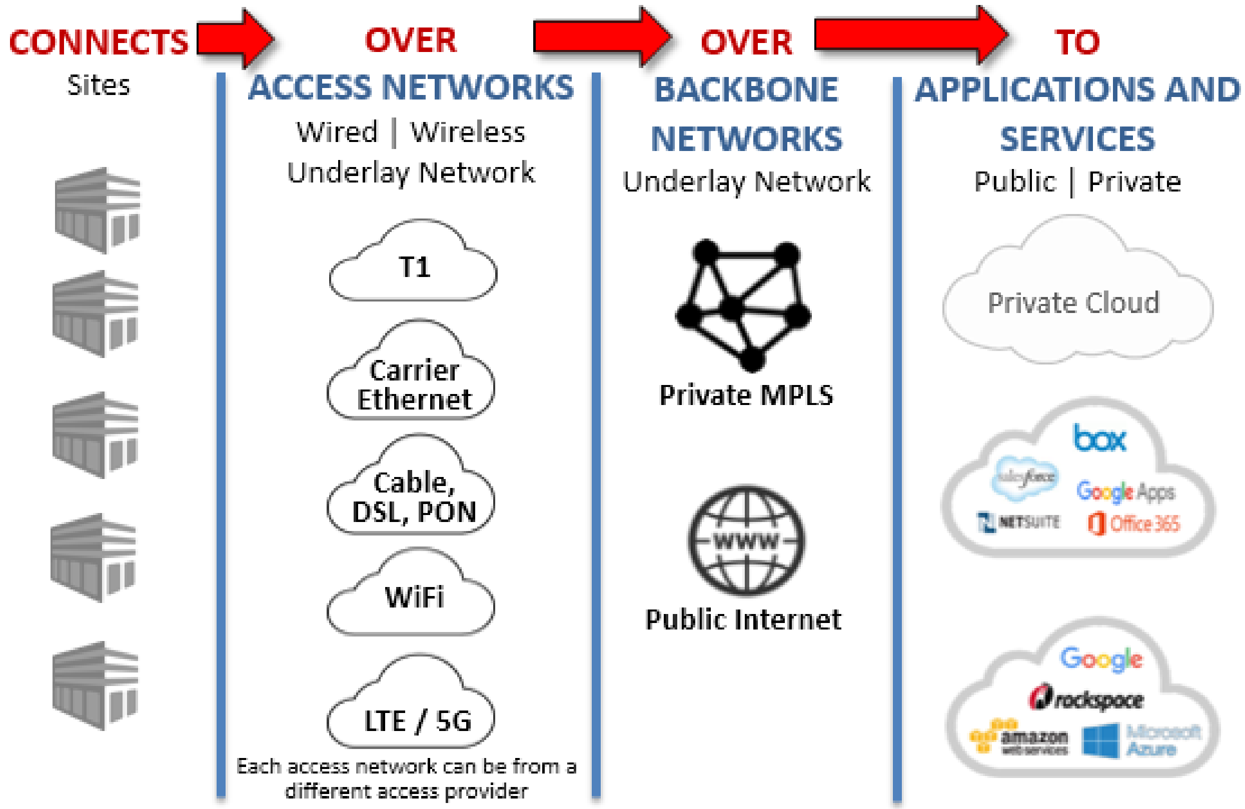

Figure 2 - SD-WAN interconnect sites and application

SD-WAN: Service provider threat or opportunity?

CSPs who currently offer MPLS connectivity services for enterprises, may find SD-WAN services a threat to their existing MPLS business. In some ways this is true given that MPLS service bandwidth typically cost 10-20 times more than broadband Internet. Unlike broadband Internet, MPLS does provide certain quality of service (QoS) performance assurances for some of the bandwidth through different classes of service. However SD-WAN's bandwidth optimization technologies can often compensate for QoS performance limitations of broadband Internet.

This poses an interesting dilemma for CSPs who want to offer or currently offer SD-WAN services. The high demand from SD-WAN services from enterprise subscribers is forcing the issue and CSPs are adapting. MEF Forum sponsored an industry survey on this topic and found that almost half of survey respondents (45%) considered SD-WAN services as a strategic opportunity while only 4% considered them to be a threat. Finally, 37% considered SD-WAN services to be both a threat and opportunity. Refer to ***Figure 3***.

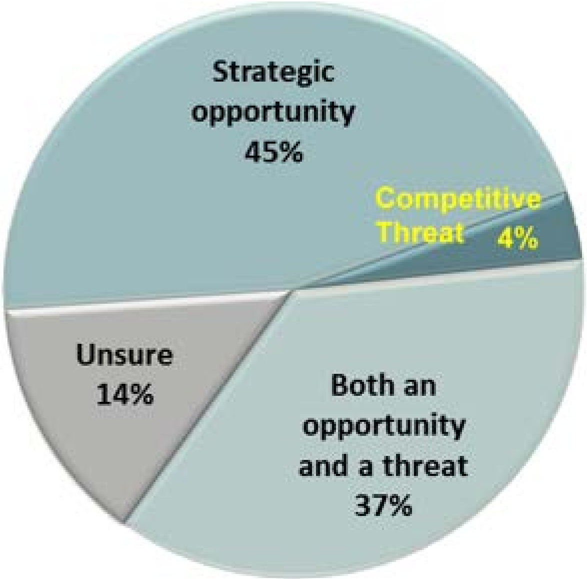

Figure 3 - SD-WAN results from MEF survey

CSPs will obtain incremental revenue from SD-WAN services while MPLS service revenue growth will be reduced or remain flat as SD-WAN enables Internet (both broadband and dedicated) to be used to grow bandwidth in addition to the current MPLS bandwidth in use. More importantly, CSPs must view SD-WAN services differently since they provide much more than connectivity. This will become clearer as SD-WAN service capabilities are discussed in the next section.

Fundamental capabilities of SD-WAN services

All SD-WAN services provide some fundamental capabilities. As with any new technology that has become popular and garnered the public's attention, SD-WAN too has had some overzealous marketers associate their products with it. This has been compounded by the lack of any standard service definition for SD-WAN or even the components used to construct an SD-WAN service. MEF Forum has embarked upon addressing this and has created working groups to define the service components, fundamental capabilities, reference architectures and implementations, and market education for SD-WAN services. MEF has also created the technical specification "MEF 55 Lifecycle Service Orchestration (LSO): Reference Architecture and Framework". This will be used for the management and orchestration for MEF-defined SD-WAN services.

Per the MEF work, the following describes the fundamental capabilities for an SD-WAN service. These capabilities are described in more detail in the MEF's paper "*Understanding SD-WAN Managed Services: Service Components, MEF LSO Reference Architecture and Use Cases*"

SD-WAN services provide encrypted IP tunnels (SD-WAN tunnels) over the underlay transport networks. Since SD-WAN services can be created over the Internet in addition to private networks, e.g., MPLS or Carrier Ethernet, encryption and some firewall functionality is critical to have a viable service. SD-WAN services operate over any wired or wireless underlay transport network. SD-WAN tunnels are built over these underlay networks and do not require any modifications to them.

SD-WAN services take QoS performance measurements (PMs) over each WAN to identify the packet loss, delay (latency) and delay variation (often referred to as jitter). These QoS PMs are used to make application forwarding decisions over SD-WAN tunnels which operate over the different WAN underlay networks.

Unlike other connectivity services, SD-WAN services forward packets based on application type thus making the service much more desirable for enterprise subscribers. SD-WAN services can identify the specific application, e.g., Skype for Business, or grouping by application type, e.g., real-time applications, and decide over which WAN the application should traverse. Other WAN services, such as Carrier Ethernet, MPLS or Internet, focus on forwarding packets at the network layer with no knowledge of the application to which those packets are associated. SD-WAN services forward the packets by application using QoS, security or business priority policies. This capability provides great value to enterprise subscribers because they are more interested in application performance than packet performance. Because policy management is centralized, it is less error prone than having to push policies down to each device individually via a device command line interface (CLI) or scripts.

SD-WAN services use WAN load balancing, diverse WAN and access network providers, and wireline plus wireless WANs to achieve a high availability service. One or more of these techniques may be used in an SD-WAN service deployment.

Unlike other WAN services, SD-WAN services achieve high levels of automation through centralized management, control and orchestration taking advantage of SDN and LSO technologies. This results in new enterprise sites to be turned up literally in minutes. Site configuration information, such as LAN and WAN IP addresses, number of WANs, and WAN types, is collected as part of the site planning and provisioning process. This information can then be prepopulated into a site ‘profile’ which is then used to configure the SD-WAN device. When the device is cabled to an Internet WAN and powered up, it can remotely retrieve its configuration from the site profile in a manner similar to how cable modems remotely retrieve their configuration once they are powered up. This automated configuration is referred to as zero touch provisioning (ZTP).

Finally, WAN optimization is an important part of an SD-WAN service and uses techniques to increase WAN bandwidth utilization for a given amount of WAN bandwidth. WAN optimization can include capabilities to minimize WAN bandwidth using data compression, TCP optimization, data caching, and data de-duplication techniques. These techniques reduce the amount of information that must be transmitted and thus free up WAN bandwidth for other applications. WAN optimization can also reduce packet loss introduced in the underlay network by using forward error correction (FEC). FEC sends additional information enabling the receiving SD-WAN device to reconstruct packets negating the need for the sender to completely retransmit the packet saving WAN bandwidth.

SD-WAN service components

To add clarity to the industry, MEF Forum has defined five service components used in an SD-WAN service as illustrated in ***Figure 4***. Some service components are used internally by the service provider while others are located on the customer premises and used by the enterprise subscriber.

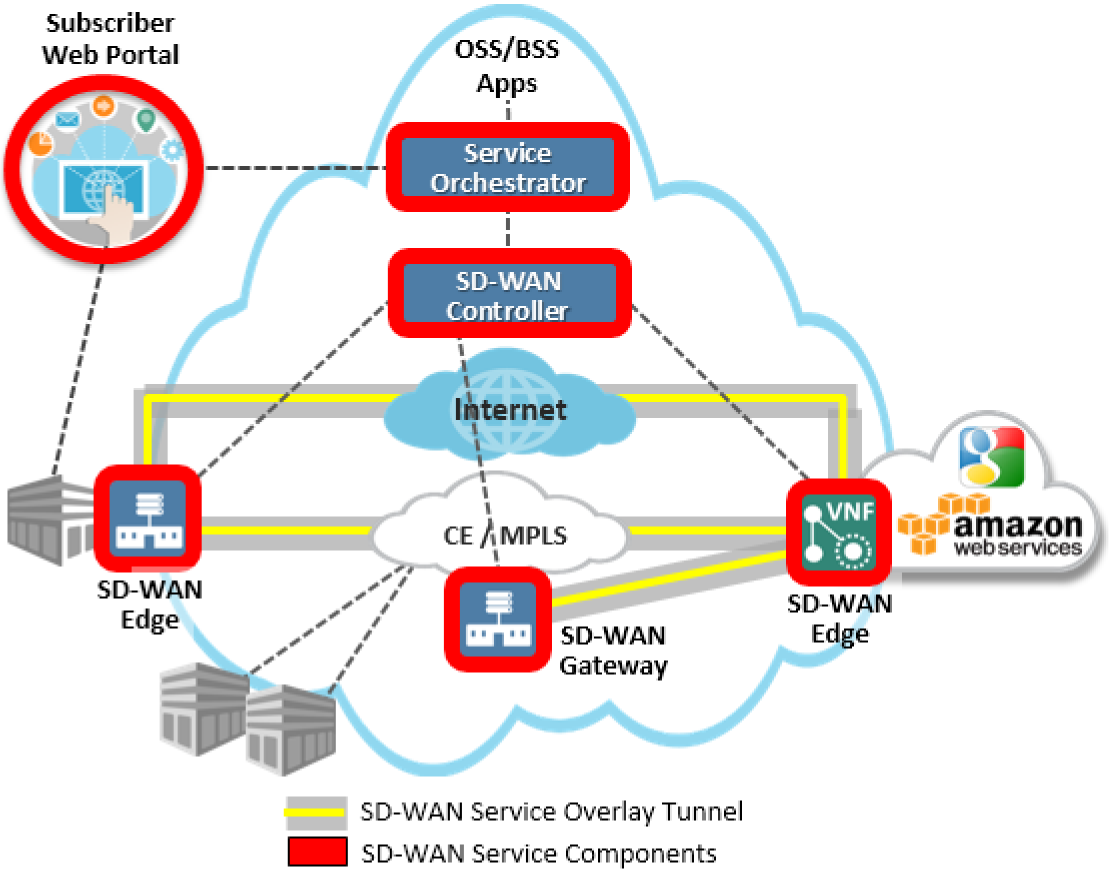

Figure 4 - SD-WAN service components defined by MEF

The SD-WAN Edge is a physical or virtual appliance which is placed on the customer premises, data center or cloud. The SD-WAN Edge may consist of a CPE, a VNF running on a vCPE, or a VNF running in a virtual private cloud, e.g., running on a compute instance in Amazon Web Services (AWS). The SD-WAN Edge initiates and terminates the SD-WAN tunnels over WANs plus measures WAN QoS performance. It also enforces application-based QoS, security and business priority policies that are used to steers packets over different SD-WAN tunnels. The SD-WAN Gateway is a special case of an SD-WAN Edge which enables sites interconnected via SD-WAN tunnels to connect to sites without SD-WAN Edges that are interconnected via other private networks such as MPLS or Carrier Ethernet.

The SD-WAN Controller is responsible for the centralized management each SD-WAN Edge and SD-WAN Gateway under its control. This may entail pushing down configuration and policies received from the Service Orchestrator or receiving alerts and alarms which are subsequently sent to the Service Orchestrator. The Service Orchestrator is responsible for lifecycle service management of the SD-WAN service and may interface with one or more SD-WAN Controllers depending upon the size of the network or geographic placement requirements. Note that some implementations combine Service Orchestrator and SD-WAN Controller. However, these two functions have been separated to facilitate placement into the MEF LSO RA. Finally, the Service Orchestrator is often used to centrally manage other services in addition to SD-WAN services.

The Subscriber Web Portal enables authorized and authenticated enterprise users to modify an SD-WAN service. Such changes may include modifying SD-WAN bandwidth, adding security policies, and adding or removing SD-WAN tunnels (service connectivity) between sites.

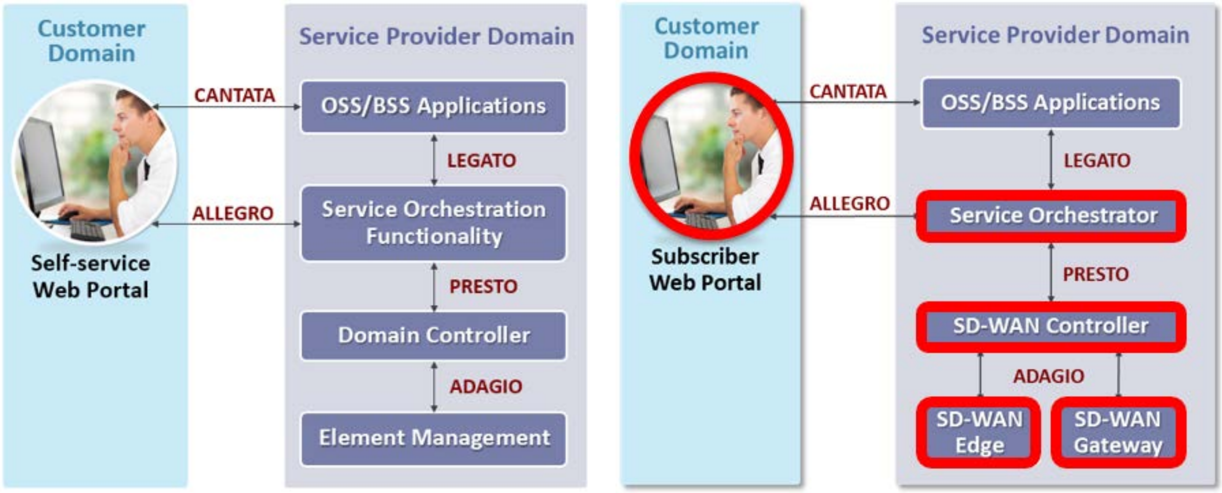

Figure 5 - SD-WAN service components mapped into MEF 55 LSO RA

The diagram on the left in ***Figure 5*** is the MEF 55 LSO reference architecture (RA) which defines different management interface reference points. The diagram on the right of ***Figure 5*** illustrates where the aforementioned SD-WAN service components, highlighted in red, are mapped in the MEF LSO RA. MEF members will use this RA to construct reference implementations and developed application programming interfaces (APIs) and data models to facilitate implementations.

SD-WAN use cases

1. SD-WAN Use Case: Hybrid WAN

This use case illustrates how two enterprise sites are interconnected via an MPLS VPN service and how they use the Internet to access public web sites, SaaS applications, cloud service providers, etc. The Internet service provider (ISP) may be different for each site as illustrated by ISP A and ISP B. Since Internet bandwidth often costs 10-20 times less than MPLS VPN bandwidth, the enterprise would like to use both MPLS VPN and a secured Internet to interconnect the sites since their MPLS VPN bandwidth is insufficient. This would enable them to increase inter-site bandwidth without purchasing additional MPLS VPN bandwidth. Refer to the present mode of operation (PMO) in ***Figure 6***.

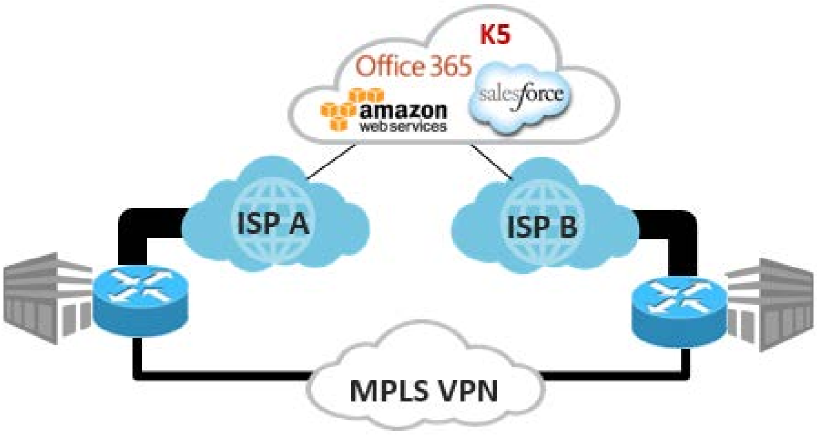

Figure 6 - PMO: Only MPLS VPN used for inter-site connectivity

In the future mode of operation (FMO), the enterprise subscriber uses the SD-WAN service to create SD-WAN tunnels across the Internet and MPLS VPN in effect sharing bandwidth across the different WANs. The SD-WAN tunnels across the Internet are encrypted so the enterprise information is secured. Each site can still connect to the public web sites via local Internet breakouts at each site. Furthermore, since an SD-WAN service provides application-based traffic forwarding, the enterprise can decide which WAN they want the application to traverse as indicated by the two red arrows in ***Figure 7***.

The WAN selection for a given application is determined by QoS, security or business priority policies. For example, an enterprise may set a QoS policy to send Skype for Business over any WAN as long as the packet loss is less than 2% and the packet latency is less than 40ms. A retailer may set a business priority policy to send all payment card transactions ahead of any other traffic since these are most important for their business. A financial institution may set a security policy whereby all inter-bank transactions are only sent over the SD-WAN tunnel over the MPLS VPN.

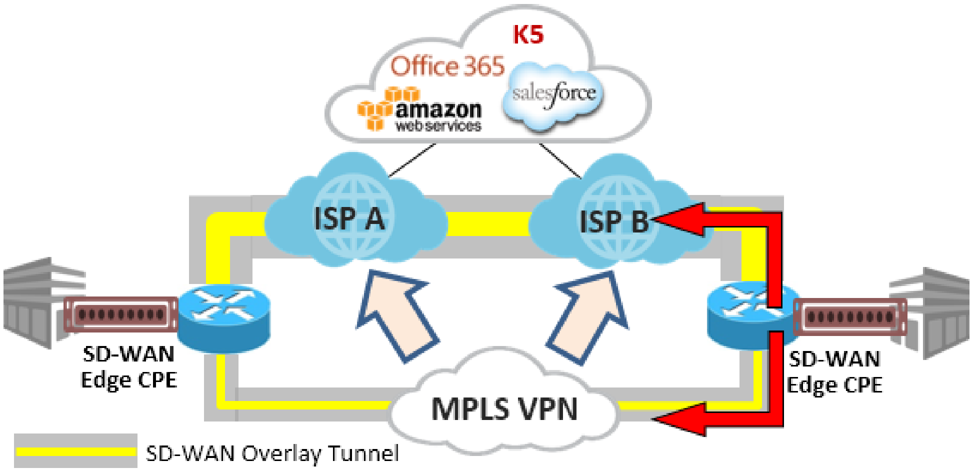

Figure 7 - FMO: MPLS VPN and Internet used for inter-site connectivity

2. SD-WAN Use Case: Secure Connectivity to Virtual Private Cloud

Enterprises are increasingly migrating applications running on site or in their data center to subscribing to a SaaS equivalent, e.g., migrating Microsoft Exchange Server to Office 365 SaaS. Furthermore, enterprises are increasingly renting virtual compute resources like infrastructure-as-a-service (IaaS) rather than purchasing physical servers and operating them on premise. As these applications and workloads migrate to the cloud, enterprises need to provide secure and increasingly higher bandwidth WAN connections to their VPC and SD-WAN services are an efficient and flexible way to support this. ***Figure 8*** illustrates an SD-WAN service interconnecting two sites over both MPLS and Internet WANs as discussed in the hybrid WAN use case in ***Figure 7***. In this case, however, an SD-WAN Edge VNF is instantiated in the cloud compute instance (IaaS) thus extending the SD-WAN to the VPC.

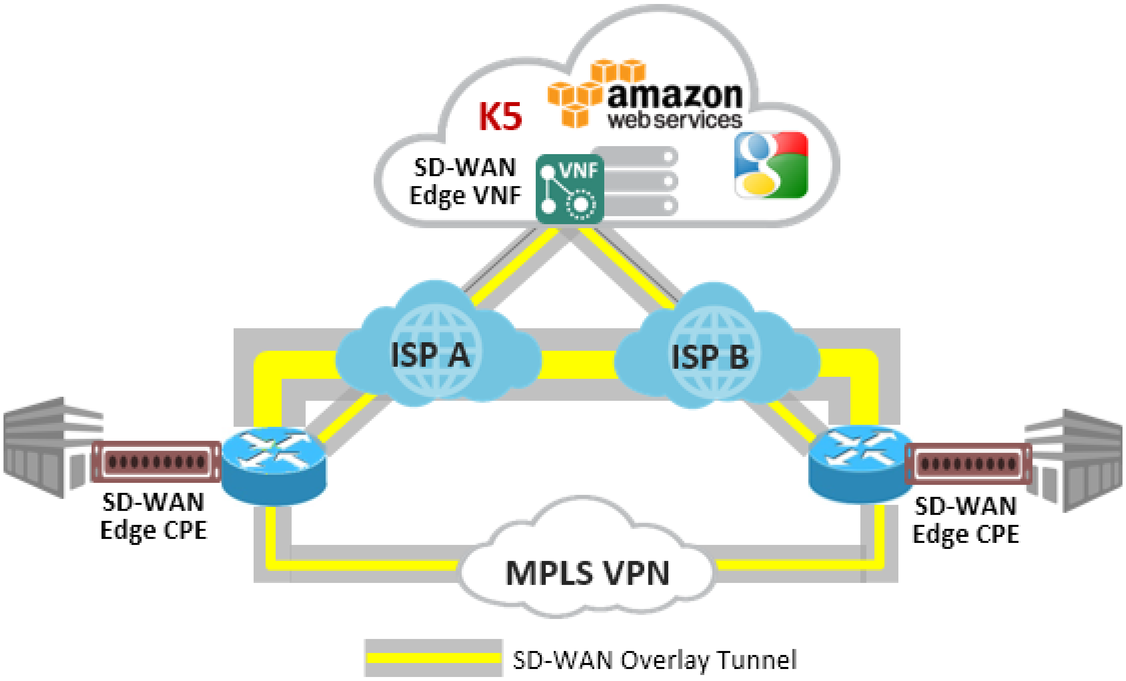

Figure 8 - Use Case for secure connectivity to cloud

3. Use Cases for Placement of SD-WAN Edge and other VNFs

An SD-WAN Edge CPE is the most common implementation since it is the simplest and follows widely established practices deploying a physical appliance at customer premises. Since an SD-WAN Edge can also be implemented as a virtual appliance via a VNF, many interesting possibilities are introduced as to where an SD-WAN service can be extended. As illustrated in ***Figure 9***, the SD-WAN Edge VNF could run on a vCPE at the customer premises similar to how an SD-WAN Edge CPE is deployed. However, in this case, the vCPE could be sized to support the SD-WAN VNF and VNFs delivering additional functions and services.

An SD-WAN Edge VNF could also run on a kiosk or automated teller machine (ATM) in a mall, sports stadium or temporary location providing secure connectivity to data centers or the cloud without requiring additional physical equipment and cabling since the VNF is software. Edge computing infrastructure is another use case where compute functionality is provided much closer to the customer premises in addition to traditional centralized, regional data centers (DC).

As network aggregation points near the edge of the network, e.g., cable modem termination system (CMTS) or broadband network gateway (BNG), become virtualized as one or more VNFs, more compute resources become available for other services or functions. SD-WAN Edge or Gateway VNFs, vCMTSs and vBNGs, and other services or functions delivered by VNFs can be added to these edge computing nodes which act as mini edge data centers. Finally, SD-WAN Edge VNFs running in public cloud environments such as AWS, Google Cloud or Microsoft Azure enable enterprises to extend their inter-site secure SD-WANs up to their virtual private cloud applications.

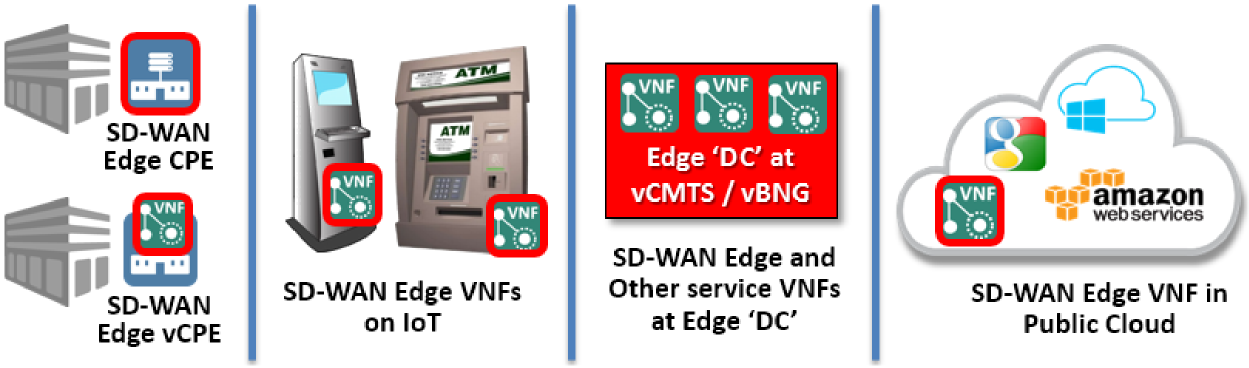

Figure 9 - Interesting possibilities for SD-WAN Edge placement

Conclusion

SD-WAN is the compilation of several networking technologies developed over the years plus newer SDN, NFV and LSO technologies resulting in an agile and flexible virtual network service. Through virtual overlay tunnels, SD-WAN services are decoupled from the underlay transport network. This results in rapid service deployment over any wired or wireless network. SD-WAN services provide much more than connectivity including application-awareness and policy-based packet forwarding. The virtualization of SD-WAN Edges enables SD-WAN services to be delivered beyond traditional 'brick and mortar' buildings, like other WAN connectivity services, and extend secure connectivity to the cloud and other types of devices. Finally, SD-WAN service capabilities, terminology and reference architectures are being defined by MEF Forum which will facilitate and accelerate implementations and service deployments.

Abbreviations

API	application programming interfaces
ATM	automated teller machine
AWS	Amazon Web Services
BB	broadband
BSS	business support systems
CE	Carrier Ethernet
CORD	Central Office Re-architected Datacenter
CLI	command line interface
CPE	customer premises equipment
CSP	communications service provider
DC	data center
DIA	dedicated Internet access
DSL	digital subscriber line
FMO	future mode of operation
IaaS	Infrastructure-as-a-Service
IP	Internet protocol
IoT	Internet of things
ISP	Internet service provider
LSO	Lifecycle Service Orchestration
LTE	long term evolution (4G cellular networks)
MPLS	multi-protocol label switching
NFV	Network Functions Virtualization

NFVI	Network Functions Virtualization Infrastructure
NOC	network operations center
OSS	operational support systems
OTT	over the top
PAYGO	pay as you go
PM	performance metrics
PMO	present mode of operation
PON	passive optical network
QoS	quality of service
RA	reference architecture
SaaS	Software-as-a-Service
SDN	software-defined networking
SD-WAN	software-defined wide area network
TCP	transport control protocol
vBNG	virtual Border Network Gateway
vCMTS	virtual Cable Modem Termination System
vCPE	virtual customer premises equipment
VNF	virtual network function
VNS	virtual network services
VPC	virtual private cloud
VPN	virtual private network
WAN	wide area network

Bibliography & References

Understanding SD-WAN Managed Services: Service Components, MEF LSO Reference Architecture and Use Cases; Ralph Santitoro; MEF Forum

SD-WAN Fundamentals, Use Cases and MEF LSO Reference Architecture, Ralph Santitoro; NFV World Congress (May 2017)

SD-WAN Managed Services, Terminology, Use Cases and Challenges, Ralph Santitoro and Peter Agnew; BrightTalk Webinar

MEF 55 Lifecycle Service Orchestration (LSO): Reference Architecture and Framework, MEF Forum