From MPLS to Software-Defined Wide Area Network

David W Mitchell

ICTN 6880

East Carolina University

Abstract

Enterprises and companies have depended on private networks, such as private T1 access to MPLS service for their bandwidth performance. The high cost of these services has encouraged the technology industries to develop some cheaper solutions as technology evolved. The support of more demanding real-time applications were limited due to the high cost of these private networks. A simple 1.5Mbps T1 circuit could cost more than $400 or more per month. Most companies or enterprises relied on these costly secured private networks to provide high availability and high performance. The ever-changing technology evolution has provided a way for enterprise and companies to move or lease their applications to a cloud based data center.

The demand for more resources that are accessible rapidly helped to bring about the software defined network. Software defined networks (SDN) have provided companies with the ability to control and manage the network by a central software platform that is separate from the hardware. Software defined networks helped to introduce Software Defined Wide Area Networks (SD-WAN) as a way to extend the software defined networks to branches. SD-WAN allow companies to use a cost-effective transport such as Internet, MPLS, wireless and broadband. It provides a way for companies or enterprises to add resources with existing devices and circuits. This cost-effective solution is starting to attract various businesses as they look for ways to decrease their headcount and budgets. In this paper, we will examine the components of SDN, components of SD-WAN, and the benefit for adapting both in a future technology solution. We will also look at possible challenges associated with SDN and SDWAN. The purpose is aimed to educate the reader about SDN and SD-WAN technologies.

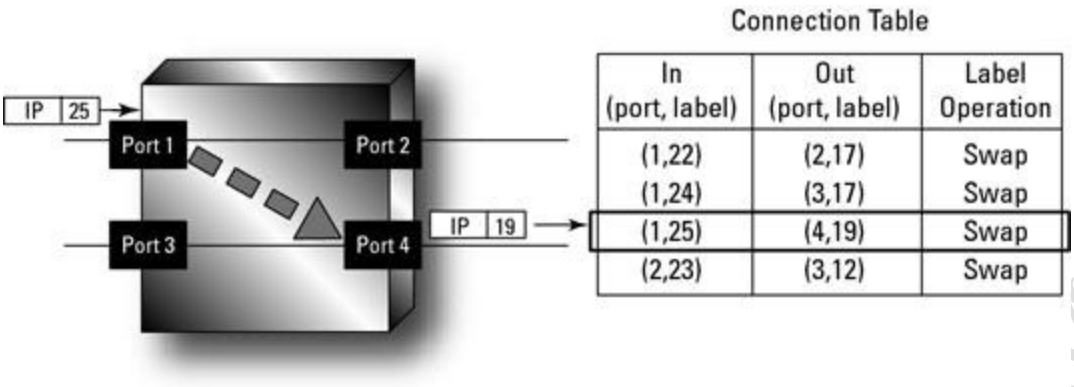
TABLE OF CONTENTS

MPLS

Most IT and telecommunication professionals consider Multiprotocol Label Switching (MPLS) as a type of service provided from a carrier. MPLS is a technique that delivers anything from IP VPNs and optical services to metro Ethernet services (Johnson, 2007). Telecommunication carriers build multiprotocol label switching backbones but do not provide MLPS service. The label in MPLS is between layer 2 (data link) and layer 3 (network) headers (SDX Central, 2017). MPLS can be best summarized as a layer 2.5 networking protocol.

Multiprotocol label switching does not mandate a single control protocol in a control plane (Winter, 2011). MPLS uses control plane protocol such as Label Distribution Protocol or Resource Reservation Protocol. The label-switched form the control-plane protocol that is distributed between routers. These LSPs transport layer 2 payloads across the core network (Metz, Barth, & Filsfils, 2007). The control plane overhead can sometimes impose technical and operational challenges for service providers (Metz, Barth, & Filsfils, 2007). The fast rerouting has made MPLS a more robust option.

In a traditional IP network, routers determine the next hop based on its routing table and forwards the packet to the next hop. MPLS finds the final destination router instead of routing to the next hop. It finds a pre-determined path, called label-switching paths (LSPs), to the final router (Goralski, Gadecki, & Bushong, 2017). The router then applies a label based on that information. The label is removed at the final destination router, then the packet is delivered via normal IP routing (Steenbergen, 2016). Figure 1 illustrates the router examines the label once it arrives at port 1. The numeric identifier associated with the LSP allows the router to lookup in its MPLS routing table the next hop (Goralski, Gadecki, & Bushong, 2017).



Connection Table

In (port, label)	Out (port, label)	Label Operation
(1,22)	(2,17)	Swap
(1,24)	(3,17)	Swap
(1,25)	(4,19)	Swap
(2,23)	(3,12)	Swap

Figure 1: A label connection table for MPLS

The diagram shows that the lookup outbound port is port 4. This process is repeated at the next LSP.

MPLS has an excellent quality of service that allows businesses most important traffic to flow. Voice over IPs are critical services used in businesses today. MPLS provides a reliability that is essential to maintaining a quality of real-time protocol like VoIP. The isolated packets from the LSP allow MPLS to be reliable. MPLS providers are able to assign a higher priority to certain network traffic (SDX Central, 2017). Figure 2 illustrates an example of multiprotocol label switching network used in enterprise companies today.

The domination of wireless networks by IP Services are expected to drive up bandwidth requirements (Shah, 2005). This has caused some carriers to shift some backhaul endpoints to IP and transport the traffic using multilink point-to-point protocol connections. MPLS networks were used to evolve the backhaul networks with transports such as TDM and IP (Shah, 2005). Wireless carriers would need to migrate their core networks to MPLS if they plan to offer IP-VPN.

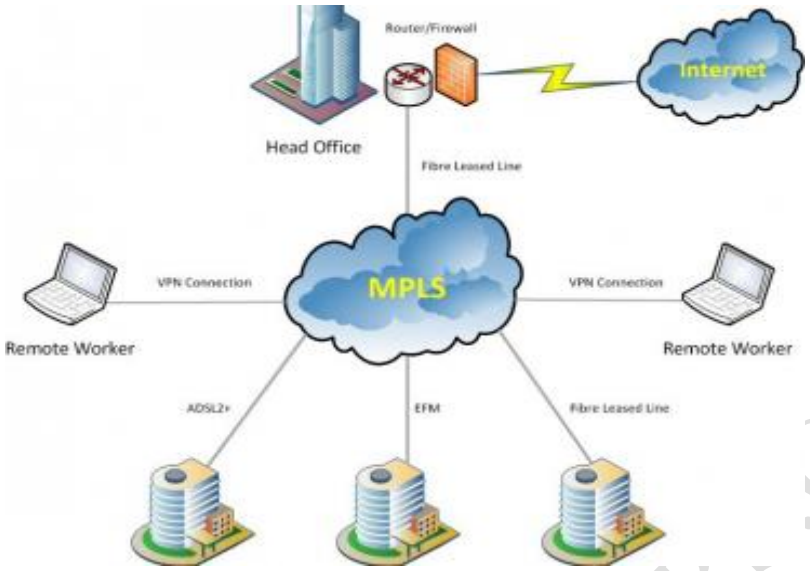


Figure 2: A multiprotocol label switching network.

MPLS Disadvantages

One downside of MPLS is the bandwidth cost. Large enterprise businesses typically pay $300 - $600 per megabits per second (Mbps) a month for a cooper connectivity (Gottlieb, 2012). The cost for a fiber MPLS connectivity at a customer's premise would range from $60 - $200 per megabits per second a month. The high cost of MPLS has driven technology gurus to start developing other cheaper reliable techniques similar to MPLS.

Another downside of MPLS is the carrier must play a role in configuration of the network. For example, the provider would be responsible for the routing of data within their MPLS cloud if you are using static routing on your network (Drake, 2013). Dynamic routing would work on most networks, but you should keep in mind that dynamic and static routing must work together in routing MPLS traffic. MPLS would not be the ideal solution for your network if you want total control of your network. (Drake, 2013).

The last drawback with MPLS is the security. MPLS networks does not offer data protection and vulnerabilities could be introduced in the network with improper implementation (Drake, 2013). Encryption should be introduced between connecting routers to ensure hardening of your network devices. A spoke and hub network with one to one connection between sites could provide more security than MPLS. Technology evolutions have helped to increase security using new cloud based software-defined networking. One of the new technologies developed recently is software-defined networking (SDN).

Software-Defined Networking

Managing networks have become innovative over the past few years with the development of software-defined networking (Feamster, Rexford, & Zegura, 2013). Software-defined network focuses on the separation of the control plane of the network to make decisions about the flow of packets through the network from the data plane (Rouse, Software-defined Networking, 2017). Software-defined network is sometimes considered an architecture approach, not a specific product that has been thought of as virtualizing data center networks (Butler, 2017). "Virtualization, cloud, mobility, and now the Internet of Things (IoT) have exposed the limitations of traditional network architectures and operational models," according to Mehra and Casemore in their SDN Forecast published in 2016 (Mehta, 2016). SDN plays a role in shaping the next-generation of networks and MPLS. SDN provides methods to manage physical and virtual network devices. Software-defined network separates the network's control logic from the underlying routers and switches.

Software defined networking provides a solution for network administrators to manage various equipment, such as switches, firewalls, and load balancers. Traditional networks have the

control plane and data plane inside the proprietary hardware (Badotra & Singh, 2017). Software-defined networking allows the separation of the control plane from the data plane. The control plane has direct control over the data plane as the brain of the network. The elements in the data plane can be manipulated as needed without having to configure each element individually (Badotra & Singh, 2017).

Plane Separation

Control, data and management planes are not bound to the network devices because of the network planes in software-defined network. The separation of the control plane and data plane are recognized by well-defined programming interface between the devices and the SDN controller (Kreutz et al., 2014). The well-defined application programming allows the controller to have direct control over the state in the data plane element. The principles of SDN include forwarding of traffic, separation of concerns and the implementation of switching hardware. The separation makes it easier to create and introduction abstractions in the networking (Kreutz et al., 2014). Figure 3 illustrates the different planes in a software-defined network from EtherealMind. SDN planes are separated by removing control discussion from the forwarding hardware and programming the forwarding hardware through an open interface (Lin, Wang, & Luo, 2016).

The part of the network that carries signaling traffic is the control plane. The control plane is responsible for routing traffic. It is considered the brain of the device that makes decisions about traffic flow. The control plan functions include system configuration, management, and exchange of routing table information. The topology information is exchanged with other routers in the router controller. It will construct a routing table based on routing

protocols such as OSPF, BPG and RIP. The packets are processed by the router to update the routing table information. In tradition networks a layer 3 device operates its own control

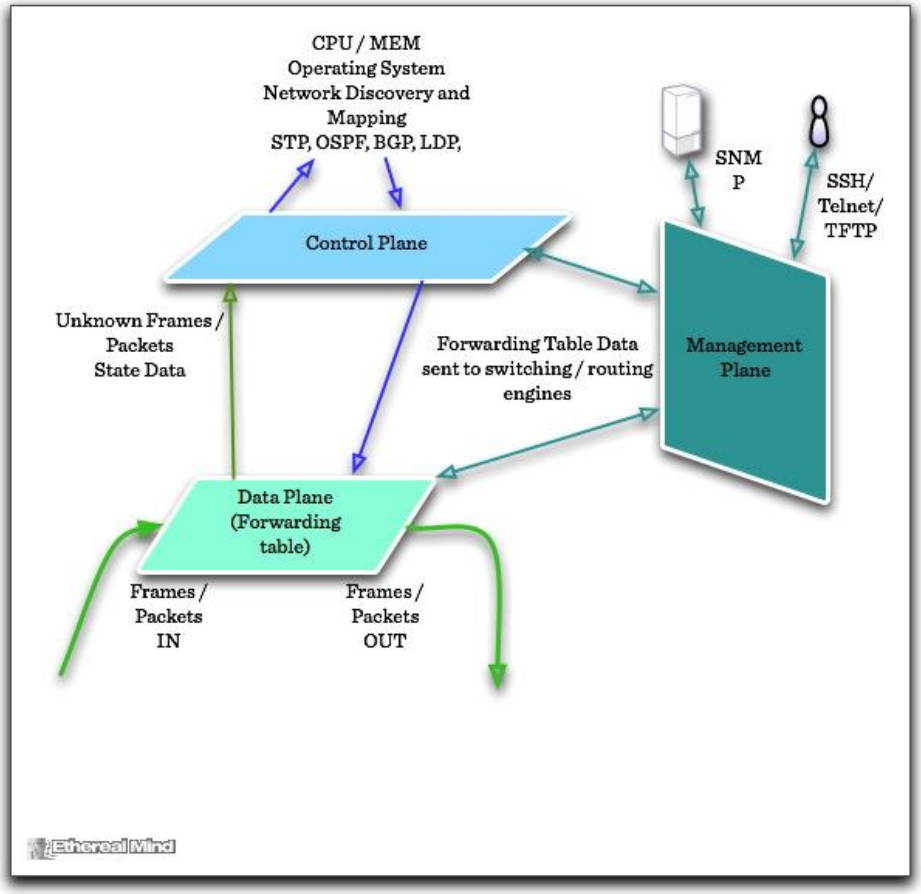


Figure 3: Software-Defined Networking Planes

plane. The control plane would not be able to obtain a complete view of the network since it operates individually. In software defined networking, the control plane is separated for management and programming. This allows quick changes with VLANs, routing, traffic flow and quality of service. The changes would happen within minutes because software defined network reduced the need to independently configure each device.

The data plane enables data transfer to and from clients while handling multiple conversations through multiple protocols (Rouse, TechTarget, 2013). The data plane is known as the forwarding plane, user plane or carrier plan because it is part of the network that carries user traffic (Rouse, TechTarget, 2013). It forwards traffic to the next hop along the path to the selected destination network. The data plane manages the filtering, quality of service, encapsulations, and queuing (Salisbury, 2012). It operates in the fast path to keep up with performance needs of core network and data centers. Software-defined networks allow companies to move toward generic hardware for processing in the data plane. This brings us to the management plane.

The management plane ensures that the network is running optimally by communicating with the network device operational plane. The management plane allows configuring, monitoring and handling of the entire software defined networks. (Montoya-Munoz, Casas-Velasco, Estrada-Solano, Ordonez, & Caicedo Rendon, 2017). Protocols such as telnet, SSH, and SNMP are used to monitor and troubleshoot. SDN has offered a newer management protocol called OpenFlow.

OpenFlow

The centralized controller uses OpenFlow as a southbound protocol to direct the flows between nodes on the network (Jacobs, 2013). OpenFlow is used for managing southbound interface of the generalized SDN architecture. OpenFlow configuration protocol establishes the relationship between switches and controllers. It provides software-based access to flow tables that instruct routers and switches how to direct network traffic (Jammal, Singh, Shami, Asal, & Li, 2014). It provides a basic set of management tools that can be used to control features such as

packet filtering. Switches and routers that use the OpenFlow protocol are offered by networking hardware vendors such as Cisco, IBM and HP. The switches come in OpenFlow only and OpenFlow hybrid. All packets are processed by the OpenFlow pipeline in OpenFlow-only. OpenFlow hybrid switches support normal ethernet and OpenFlow operations.

OpenFlow Controller

The controller maintains all the network protocols and policies. It distributes the appropriate instructions to the network devices (Jammal, Singh, Shami, Asal, & Li, 2014). The switch flow table is managed by adding and removing flow entries over the secure channel using the OpenFlow protocol. The network intelligence is centralized by the control. The switch may establish communication with multiple or single controllers.

Multiple controllers will add redundancy in the case that one of the connections fail. A switch can continue to operate in OpenFlow mode if one controller connection fails. The hand-over is managed by the controller, enables fast recover, and load balancing (Jammal, Singh, Shami, Asal, & Li, 2014). The goal of multiple controllers is to help synchronize controller hand-offs.

OpenFlow Protocol

The OpenFlow switches contain group tables and multiple flows. The flow tables contain many flow entries. The entries are used to perform packet look-up and forwarding (Jammal, Singh, Shami, Asal, & Li, 2014). The switches can make forwarding decisions for packets by maintaining a flow table. An exact match check on a field of the packet is performed on the

OpenFlow switch. Some corresponding instructions are executed if the packet matches a flow entry in the flow table.

Flow entries that point to group requires additional processing. The group table offers additional methods of forwarding such as multicast and link aggregation. The group entry is a group identifier, a group type, counters and a list of action buckets (Jammal, Singh, Shami, Asal, & Li, 2014). Each action bucket contains a set of actions to be executed.

Benefits of SDN

Software-Defined Networking has several benefits to the legacy network architectures. SDN provides flexibility and simplification to the inflexibility and complexity of the traditional network. Enterprise companies are provided with the ability to control their networks programmatically and to scale them without affecting performance (Jammal, Singh, Shami, Asal, & Li, 2014). SDN simplifies network management by eliminating the complexity of the infrastructure layer. The flow control is abstracted to give administrators the power to define network flows that meet connectivity requirements (Jammal, Singh, Shami, Asal, & Li, 2014).

Software-Defined Networking provides programmability on the control plane that allow changes to be implemented throughout the network hardware on a secure channel. This allows an administrator to integrate new devices into the existing architecture (Jammal, Singh, Shami, Asal, & Li, 2014). The SDN controller's traffic engineering is improved for network operators using video traffic. It provides additional benefits to network operators of reducing congestion hot spots (Jammal, Singh, Shami, Asal, & Li, 2014).

Network Virtualization

Software-Defined Networking allows the managing of data centers. The growth of virtual machines has provided significant scalability issues for data center (Jammal, Singh, Shami, Asal, & Li, 2014). The user experience is interrupted when moving virtual machines on traditional network architecture. An application of software-defined networking called network virtualization has provided an opportunity for hyper-scale data centers.

Network virtualization is a service that provides multiple logical networks decoupled from a single physical network (Chowhury & Boutaba, 2009). Network virtualization allows service providers to manage end-to-end service on virtual network for end users. Network virtualization separate the role of traditional Internet Service Providers into infrastructure providers and service providers. The infrastructure providers manage the physical infrastructure. The service provider aggregate resources from multiple infrastructure providers to create the virtual networks (Chowhury & Boutaba, 2009).

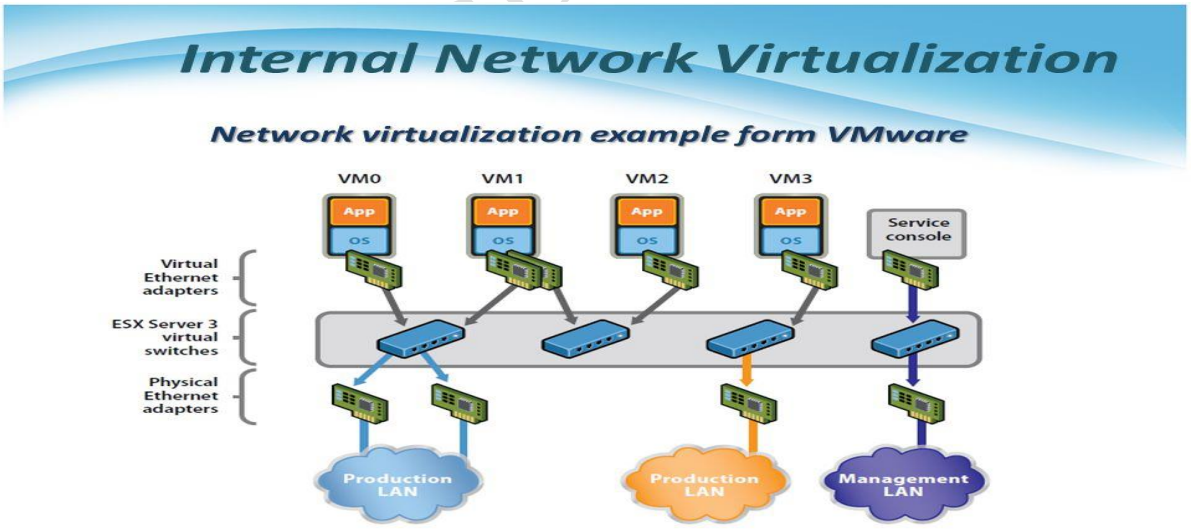


Figure 4: VMware Network Virtualization.

Figure 4 illustrates an example of network virtualization from VMware. Virtualization allows network hardware and services to be implemented as software (Li & Chen, 2015).

An example of external virtual network is VLAN technology. VLAN allows many logical networks to operate on one VLAN-capable switch (Bigelow, 2017). Scott Gorcestr, president of Moose Logic stated, "internal virtual networks would be the facilities built into virtual server host software such as Microsoft Hyper-V, Citrix XenServer and VMware products" (Bigelow, 2017). Network virtualization can be applied within virtual servers to create synthetic networks between virtual machines (Bigelow, 2017).

Network virtualization provides cost savings, efficiency and flexibility. According to Dave Sobel, CEO of Evolve Technologies, "the objective of virtualization is to get more utilization out of the hardware" (Bigelow, 2017). A virtual environment eliminates the need to add switch ports that require cabling and connection. Logical switch ports are created in a virtual environment. This allows more virtual switch ports to be connected to other logical switch ports quickly.

SDN Impact

Software-defined networking is taking over other parts of the computing industry. More devices are moving towards the software-defined path with logic implementation in their software over standard processors (Jain & Paul, 2013). SDN Network infrastructures are shared by a many number of entities in cloud computing. The networks of tomorrow will be more programmable than today with technologies such as SDN and SDN-WAN. Programmable capable devices will become the common feature of all hardware in the future (Jain & Paul, 2013). Table 1 shows the management requirement for a traditional network versus a software-

defined network. SDN represents a landmark because we are witnessing computer network development happening outside private industry boundaries (Wickboldt, et al., 2015). Software-defined wide area networks (SD-WAN) have extended software-defined networking over enterprise branch offices.

Management Requirements	Traditional Networks	Software-Defined Networks
Bootstrap and configuration	Set well known protocol parameters	Configure customized and ever-changing software, setup forwarding and control plane connectivity
Availability and resilience	Configure alternative routes in case of link failure	Configure forwarding devices behavior in case of failure in the connection with control plane
Network programmability	Not required	Control versioning, coordinated deployment, and verification of network software.
Performance and scalability	Bandwidth assignment and reservation, Quality of Service configuration and enforcement.	Monitor performance of network application, adjust connection quality between forwarding and control planes.
Isolation and security	Control network access, prevent intrusion, spoofing and Denial of Service.	Grant isolation to network applications, prevent eaves-dropping of control traffic
Flexibility and decoupling	Adjust the management of higher level protocols.	Adapt management functions along with management interfaces, coordinate management information within plane or among management systems.
Network planning	Access capacity and performance needs, choose a network topology.	Plan the disposition of controlling elements in relation to forwarding elements.
Monitoring and visualization	Track resource utilization, identify outages and trigger alarms	Trace functional parameters of novel applications, visualize jurisdiction of network controllers.

Table 1. Traditional network versus software-defined networking management.

Software-Defined Wide Area Networks

The advantages of software-defined networking are no longer limited to data centers because of software-defined wide area networks (SD-WAN). SD-WAN provides a software abstraction to create a network overlay and decouple network software services (Uppal, Woo, & Pitt, 2015). This abstraction allows administrators to control and manage their networks easier. The overlay provides an interface across different physical components to ease the network administration.

Software-defined wide area networks separate the functionality into a data and control plane. The data plane carries application and user data. The control plane is responsible for making packet routing decisions. One logical instance of the control plane serves multiple instances of the data plane (Uppal, Woo, & Pitt, 2015). The data plane contains its own control plane in a traditional network. The separation of layers has many benefits:

- The control plane provides management of a more diverse set of data plane components.
- Agility is increased as intelligence is moved from data plane into programmable control plane.
- It enables the communication between the control plane and data plane components using OpenFlow protocols.
- It enables applications to program the network as an abstraction with application-programming interface.

SD-WAN provides a secure overlay that is independent of the transport components. SD-WAN can provide even better security than traditional dedicated WAN services such as

Multiprotocol Label Switching (MPLS) at a cheaper cost (Wood, 2017). SD-WAN is thought of as an overlay architecture that connects infrastructure as a service, software as a service and remote locations. MPLS connections may be the dedicated circuits used to carry traffic through the SD-WAN device. In this case, the service provider MPLS circuit already provides a secure connection. The downside is MPLS circuits are very expensive. SD-WAN solutions use technology like IPSEC VPN, IKEv2 with certificates, and end-to-end encryption using AES256 (Wood, 2017). SD-WAN has a single, multi-tenant management tool for handling application policies across all connections. SD-WAN provides the security at a cheaper cost than the MPLS.

SD-WAN Deployment

There are different deployment options for connecting SD-WAN to enterprise branch offices. SD-WAN offers different flexible link options for accessing cloud application or data center. Traditional networks reply solely on MPLS protocols. Figure 5 illustrates some of the SD-WAN deployment options.

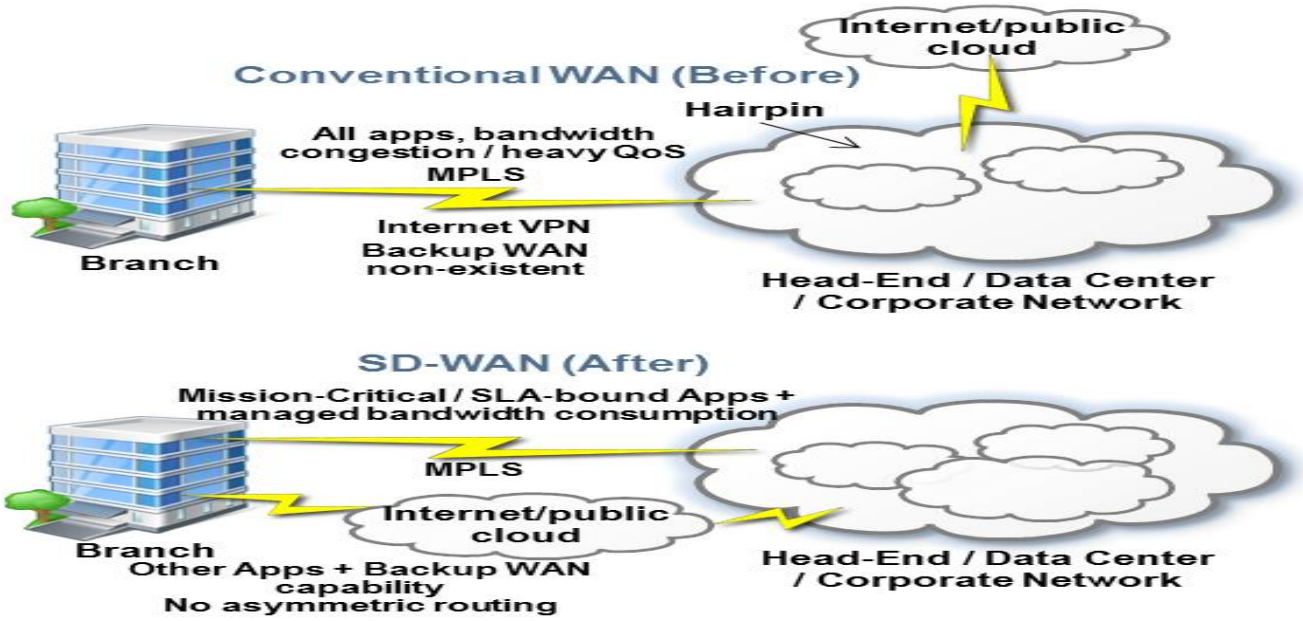


Figure 5: Traditional WAN versus SD-WAN deployment.

SD-WAN helps to fully leverage broadband links as part of the enterprise WAN while maintaining performance and reliability. One deployment option includes using any combination of wireless 4G, broadband and fiber links. These connections provide a reliable and secure connections to public cloud services using SD-WAN (Uppal, Woo, & Pitt, 2015). SD-WAN can steer application on a per-packet basis in the middle of active sessions with two connection links. This helps to improve the performance and reliability of the applications. SD-WAN performs Forward Error Correction to mitigate the performance issue.

Another deployment option is to use hybrid WAN combinations such as Internet and private WAN links. Private WAN can be very costly and provide a slower speed. SD-WAN provides utilization of the links without having to manually route the protocols (Uppal, Woo, & Pitt, 2015). According to Gartner Andrew Lerner, the hybrid SD-WAN offers a number of benefits including reduce WAN costs; simplified and improved management orchestration of WAN traffic and devices; improved and unified visibility and monitoring traffic; and better security. It often relies on the SD-WAN's intelligence to distribute the traffic. Figure 6 illustrates a hybrid SD-WAN connection using MPLS and broadband.

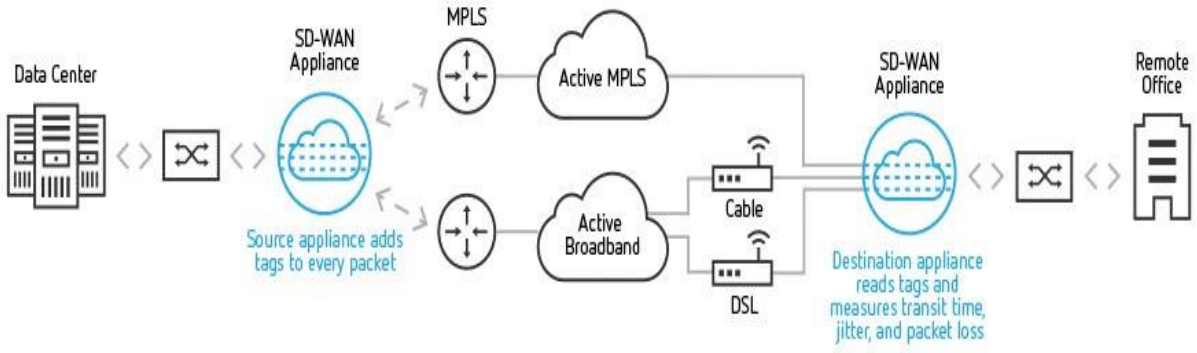


Figure 6: Hybrid SD-WAN deployment.

Benefits of SD-WAN

The first benefit of SD-WAN deployment is a reduced cost. A large cost is involved in connection geographically disparate branches using dependable and secure traditional connections like MPLS lines (Bouk, 2017). SD-WAN reduces the expense while providing the same reliability and security as a traditional MPLS line. Service providers can use MPLS, Internet, LTE, wireless, broadband or other methods to optimize bandwidth usage at the least possible cost (Dey, Dhir, & Kumar, 2016). WAN upgrade costs are reduced with the options to mix private MPLS and broadband links. The cloud gateway-based SD-WAN architecture eliminates the need for data center upgrades or redesign cost (Uppal, Woo, & Pitt, 2015).

Another benefit of SD-WAN deployment is the improvement of provisioning times. Gartner estimated there is a 50-80% reduction in the time it takes to provision network changes due to the simplified configuration, orchestration and rapid provisioning of an SD-WAN solution (Lerner & Rickard, 2017). SD-WAN also enables automated provisioning, leading to faster activation of branches. SD-WAN offers a zero-touch provisioning that allows quick branch deployment and time to accessibility as all deployment functions are managed from the central IT branch.

Security is even better with SD-WAN solutions. Traditional WAN solutions handle security through multiple appliances at each branch. SD-WAN provides a security solution in a single box and at a lower cost. A Gartner study estimates worldwide spending on information security will reach $90 billion in 2017, an increase of 7.6 percent over 2016, and top $113 billion by 2010 (Forni & Meulen, 2017). SD-WAN solutions have encryption capabilities that protect access and assets on a corporate network. SD-WAN provides AEW 256 encryption to ensure data

integrity. The communication is secured using IPsec. The controllers in SDN have a global network view which provides the greatest security advance over traditional networks (Dabbagh, Hamdaoui, Guizani, & Rayes, 2015). SD-WAN can increase your network security segmenting the network. SD-WAN technology makes it possible to limit the damage done by an attack by limiting the manageable area and immediately alerting you to the problem (Brown, 2016). Segmenting the branch helps to prevent any attack from spreading across the enterprise. Traffic in one segment is limited to the source and destination within that segment. The built-in fail-overs allows the problem to be fixed without the end user ever noticing an alert of failure.

Software-Defined Security

Software-defined security (SD-security) accompanied with SD-WAN offers additional security to an SD-WAN solution. SD-security offers the same security features and functionality a company would expect from hardware-based network security devices (Mehta, 2016). The difference in SD-security is the security is served via software instead of hardware. Software-defined security allows enterprise IT to deliver a layered security service for branch offices. SD-security provides advance functions such as secure web gateways and next-generation firewalls. The software in SD-security allows enterprise to replace the proprietary appliances with high-performance software systems (Mehta, 2016).

Software-defined security is an architectural approach to compliance and protection that abstracts controls away from physical elements. The security mechanisms are abstracted from the security device and set inside the software defined security controller of the control layer (Darabshe, et al., 2015). The autentication process and all security controls occur at the control

layer. Security abstraction means all controls must be completely non-dependant on hardware, topologies, or physical location.

Software-defined security principle of security orchestration is satisfied by automated, dynamic and centrally managed composition of individual controls into integrated security services. Security orchestration maintains alignment between security requirements and control implementation through provisioning. It manages the composition deployment, and management of individual components into more complex security systems. Security orchestration is considered to be a higher order function than simple control automation. A key advantage of orchestration is the ability to rapidly create and maintain numerous security environment that are aligned with higher-level business needs while keeping pace with migration and reconfiguration needs. Security orchestration reduces the potential for error associated with deploying multiple control systems across multiple application or infrastructure environments (What CSOs Need to Know about Software-Defined Security, 2014).

SD-WAN and Internet of Things

Internet of Things (IoT) fit very well in the SD-WAN framework. IoT is basically connecting any device to the Internet. The sensors in IoT would respond to endpoint as the IoT gateway is located with the SD-WAN edge device. Cloud services could be inserted into the SD-WAN framework (Uppal, Woo, & Pitt, 2015). The numbers of the IoT market range from $16 billion in 2016 to $1.29 trillion by 2020. SD-WAN is expected to exceed $9 billion by 2021 (Wexler, 2017). SD-WAN represents the backbone for Internet of Things. It provides the support that allows automatic systems to function. SD-WAN solutions provide visibility and control for

enterprise IoT technology. SD-WAN solutions ensures IoT devices and their applications would not be impacted by packet loss.

Conclusion

The high cost of private ethernet circuits such as Multiprotocol Label Switching (MPLS) has driven the technology industries to adopt a cheaper solution called Software-defined wide area network (SD-WAN). Software-defined wide area networks provide the security and reliability of a multiprotocol label switching at a much cheaper price. SD-WAN offers better security than MPLS with more flexibility. All companies may not immediately switch from MPLS to SD-WAN because they are more familiar with the inter-working of MPLS. However, a hybrid SD-WAN solution will influence enterprise branches to sample the network connection because they would be able to keep their current MPLS and add a redundant cheaper connection. That is what mostly attracts these enterprise branches to adopt a SD-WAN solution. SD-WAN is expected to change the way service providers and enterprise branch offices adopt technology at a cost within their budgets.

References

Badotra, S., & Singh, J. (2017). A Review Paper on Software Defined Networking. *International Journal of Advanced Research in Computer Science*, 29-36.

Bigelow, S. J. (2017, 09 26). *Network Virtualization Explained*. Retrieved from TechTarget: http://searchitchannel.techtarget.com/feature/Network-virtualization-explained

Bouk, J. (2017, July 14). *5 True Business Benefits of SD-WAN*. Retrieved from Cass Information Systems, Inc: http://www.casstelecom.com/blog/5-true-business-benefits-of-sd-wan

Brown, L. (2016, September 30). *How Secure is Software-Defined WAN*. Retrieved from CTC Technologies: http://www.ctctechnologies.com/sd-wan-and-your-security/

Butler, B. (2017, July 19). *What SDN is and where it's going*. Retrieved from Network World: https://www.networkworld.com/article/3209131/lan-wan/what-sdn-is-and-where-its-going.html

Chowhury, N. K., & Boutaba, R. (2009). A Survey of Network Virtualization. *Computer Networks*, 862-876.

Culver, T., Black, C., & Goransson, P. (2016). *Software Defined Networks: A Comprehensive Approach.* Morgan Kaufmann.

Dabbagh, M., Hamdaoui, B., Guizani, M., & Rayes, A. (2015). Software-Defined Networking Security: Pros and Cons. *IEEE Communication*, 73-79.

Darabshe, A., Al-Ayyoub, M., Jararweh, Y., Benkhelifa, E., Vouk, M., & Rindo, A. (2015). *SDSecurity: A Software Defined Security Experimental Framework.* Irbid: Jordon University of Science and Technology.

Dey, R., Dhir, A., & Kumar, A. (2016). *SD-WAN for Service Providers: Threat or Opportunity.* Price water house Coopers LLP.

Drake, K. (2013, January 17). *Pros vs. Cons of an MPLS Network*. Retrieved from Ongoing Operations: https://ongoingoperations.com/2013/01/17/mpls-network-pros-cons/

Feamster, N., Rexford, J., & Zegura, E. (2013). The Road to SDN. *Acmqueue*, 1-21.

Forni, A., & Meulen, R. (2017, March 14). *Gartner says Detection and Response is Top Security Priority for Organizations in 2017*. Retrieved from Gartner: https://www.gartner.com/newsroom/id/3638017

Goralski, W. J., Gadecki, C., & Bushong, M. (2017). *The Function of Labels in MPLS Networks.* Wiley.

Gottlieb, A. (2012, April 19). *Next-Generation Enterprise WANS*. Retrieved from Network World: https://www.networkworld.com/article/2222196/cisco-subnet/why-does-mpls-cost-so-much-more-than-internet-connectivity-.html

Jacobs, D. (2013, April). Retrieved from OpenFlow configuration protocols: Understanding OF-Config and OVSDB: http://searchsdn.techtarget.com/tip/OpenFlow-configuration-protocols-Understanding-OF-Config-and-OVSDB

Jain, R., & Paul, S. (2013). Network Virtualization and Software Defined Networking for Cloud Computing: A Survey. *Cloud Networking and Communications*, 24-30.

Jammal, M., Singh, T., Shami, A., Asal, R., & Li, Y. (2014). Software defined networking: State of the art and research challenges. *Computer Networks*, 78-80.

Johnson, J. T. (2007, March 29). *MPLS Explained*. Retrieved from Network World: https://www.networkworld.com/article/2297171/network-security/network-security-mpls-explained.html

Kreutz, D., Ramos, F. M., Verissimo, P., Rothenberg, C. E., Azodomolky, S., & Uhlig, S. (2014). Software-Defined Networking: A Comprehensive Survey. *Institute of Electricial and Electronic Engineers*, 1-10.

Lerner, A., & Rickard, N. (2017, March 23). *Market Guide for WAN Edge Infrastructure*. Retrieved from Gartner: https://www.gartner.com/doc/reprints?id=1-3X6W6KF&ct=170404&st=sb

Li, Y., & Chen, M. (2015). Software-Defined Network Function Virtualization: A Survey. *IEEE*, 2542-2550.

Lin, S.-C., Wang, P., & Luo, M. (2016). Control traffic balancing in software defined networks. *Computer Networks*, 260-272.

Mehta, K. (2016, December 12). *SD-WAN is Wonderful, But Should Be Accompanied by SD-Security*. Retrieved from SDX Central: https://www.sdxcentral.com/articles/contributed/sd-wan-wonderful-should-accompanied-sd-security/2016/12/

metz, C., Barth, C., & Filsfils, C. (2007). Beyond MPLS ... Less Is More. *IEEE Internet Computing*, 72-76.

Montoya-Munoz, A. I., Casas-Velasco, D. M., Estrada-Solano, F., Ordonez, A., & Caicedo Rendon, O. M. (2017). A YANG Model for a vertical SDN Management Plane. *IEEE*, 1-6.

Rouse, M. (2013, March 12). *TechTarget*. Retrieved from Data Plane: http://searchsdn.techtarget.com/definition/data-plane-DP

Rouse, M. (2017, October 11). *Software-defined Networking*. Retrieved from Techtarget Network: http://searchsdn.techtarget.com/definition/software-defined-networking-SDN

Salisbury, B. (2012, September 27). *NetworkStatic*. Retrieved from The Control Plane, Data Plane and Forwarding Plane in Networks: http://networkstatic.net/the-control-plane-data-plane-and-forwarding-plane-in-networks/

SDX Central. (2017, October 7). Retrieved from SD-WAN vs. MPLS: The Pros and Cons of Both Technologies: https://www.sdxcentral.com/sd-wan/definitions/sd-wan-vs-mpls-pros-cons-technologies/

Shah, N. (2005). Carrier Migration From ATM to MPLS: Why, When and How. *Business Communications Review*, 26-30.

Steenbergen, R. A. (2016). *MPLS for Dummies.* Chicago: nLayer Communications, Inc.

Uppal, S., Woo, S., & Pitt, D. (2015). *Software-Defined WAN For Dummies.* West Sussex: John Wiley & Sons Ltd.

Wexler, S. (2017, May 8). *SD-WAN Steps Up as an IoT Enabler*. Retrieved from CIO: https://www.cio.com/article/3193880/networking/sd-wan-steps-up-as-an-iot-enabler.html

(2014). *What CSOs Need to Know about Software-Defined Security.* San Francisco: CloudPassage.

Wickboldt, J. A., Paim de Jesus, W., Isolani, P. H., Both, C. B., Rochol, J., & Granville, L. Z. (2015). Software-Defined Networking: Management Requirements and Challenges. *IEEE Communication*, 278-284.

Winter, R. (2011). The Coming of Age of MPLS. *IEEE Communication Magazine*, 78-82.

Wood, M. (2017). How to make SD-WAN secure. *Network Security*, 12-14.