UNIVERSITY OF ALBERTA

Master of Science in Internetworking

Capstone Project Report

On

SD-WAN service analysis, solution, and its applications.

By **Sudhir Yadav**

Under the supervision of

Mr. Juned Noonari

Preface

Software-defined Wide Area Network (SD-WAN) is a modern WAN solution that simplifies network management and provides integration with the cloud. SD-WAN is an application of Software-defined networking. SD-WAN has grown with SDN in recent years and adoption of SD-WAN started when its implementation showed tangible results. SD-WAN adoption has grown in the enterprises and they are reaping the benefits of using SD-WAN over the Traditional WAN technologies.

Let's have a look at how an SD-WAN implementation in a business can be beneficial. To determine that we will be using an example of an organization, we will try to understand why it is beneficial and in some cases critical to adopt the new technology rather than investing in the existing MPLS infrastructure. By transferring these functions to software and a central controller, SD-WAN virtualizes networking services and reduces the complexity of configuring and managing enterprise networks. This new solution can also serve as a replacement for MPLS, which has been in use since the 1990s. As a result, there is a need to analyze these SD-WAN solutions, which is the objective of this Capstone project.

This project will look at one of the most prevalent networking technology in today’s networking world, i.e., Software-Defined Wide-Area Network (SD-WAN). Various vendors have designed and improved their SD-WAN solutions in recent years. The analysis will be based on a review of white papers, vendor documentation and research papers. The goal is to provide a thorough analysis of these SD-WAN Solutions offered by these vendors and to discuss SASE which could be the new best thing to revolutionize enterprise networks.

Table of Contents

List of Figures

1 Software-Defined Networks

Computer Networks consist of three planes Data, Control, and Management plane, as you can see in Figure 1 below. The Data plane is responsible for making forwarding decisions and forwarding traffic. The Control plane is the brain of the network where all the routing protocols are working and is responsible for routing the traffic, which populates the forwarding table for the data plane. The management plane has all the software services which are used to monitor and control the network. When a new network policy is implemented at the management plane, the control plane enforces it, and the data plane executes it [1].

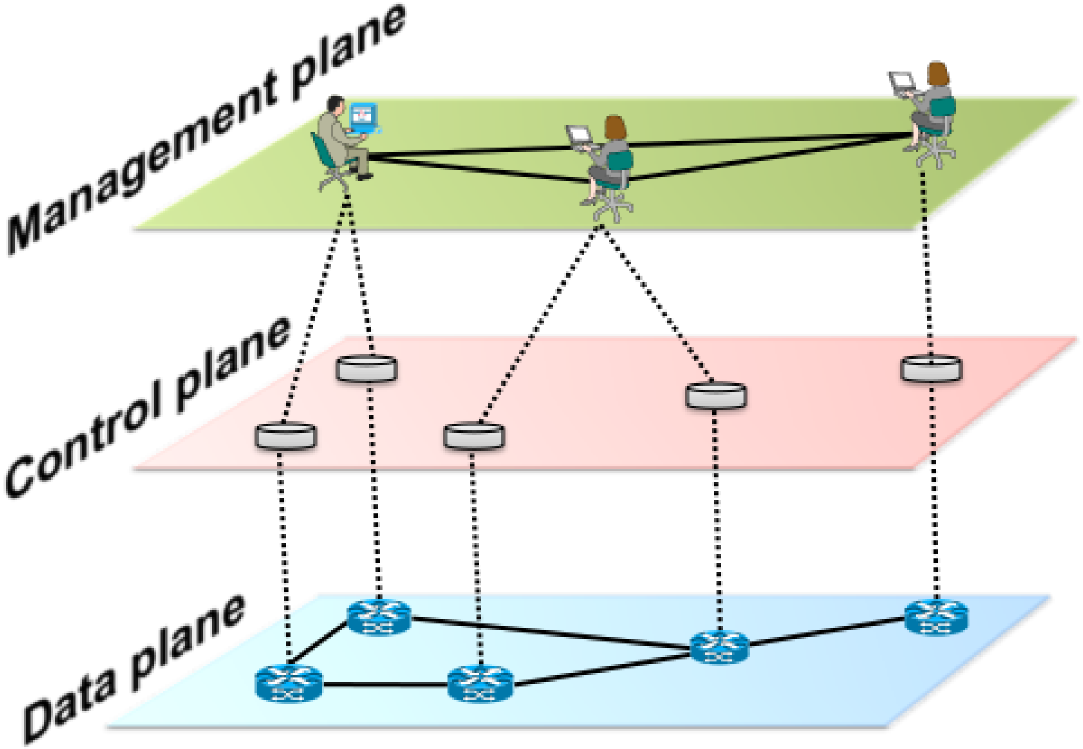


Figure 1: Layered view of the network [1]

1.1 Traditional networking

Traditional networking is hardware-centric networking, which is the fundamental reason why traditional networks are rigid and hard to manage and leaves no room for evolution. We are using these devices, which have their control and data plane coupled together, they have a fixed function, and most of the hardware and software are proprietary, which is a hurdle in the path of innovation.

The decentralized structure and lack of flexibility in the network make it complicated and time-consuming to add new functionalities. We can take the migration of IPv4 to IPv6 as an example, which has been going for almost ten years and still hasn't been fully completed. Also, whenever you need to change any policy or introduce new policies in an existing network, you need to configure that on every device in the network that too, using vendor-specific commands, which is an overwhelming and complex task. Any misconfiguration could result in unexpected network behavior, which can be packet losses, new unintended paths, loss of connectivity, loops in the network, or contract violations. One of the recent events happened at Telstra exchange, where a misconfiguration in the BGP Edge router advertised 500 IPv4 prefixes as of Telstra and resulted in a big chunk of internet traffic routing through their network [1] [2] [3].

Building and maintaining a network infrastructure is significantly costly, which hampers innovation and the addition of new services to combat the lack of in-path functionalities. A small number of vendors offer solutions to provide in-path functionalities and support network management; these solutions are proprietary. These devices have specialized hardware, operating systems, and control programs. Specialized devices like firewalls, Intrusion detection systems, Intrusion prevention systems, and deep packet inspection engines, also called middleboxes. These middleboxes are placed strategically in the network to help with their in-path functionalities to make the network efficient. However, these devices' deployment makes the network design and operation even more complex [1].

1.2 Software-Defined Networking

Software-Defined Networking is Intent-based networking; the term Software-defined networking was originally coined concerning the working of OpenFlow at Stanford University. Where few scientists developed OpenFlow and used it to define data flows of the forwarding devices. It is an idea of decoupling the control plane and data plane from one another, making the network devices simple traffic forwarding devices. Forwarding devices make up the data plane, and the control plane is implemented to an external logically centralized controller. This SDN controller has direct control over the data plane via a well-defined application programming interface (API). A simplified view of an SDN architecture is shown in Figure 2. This separation of the planes makes the network flexible, easier to manage and opens up to evolution and innovation [1] [4].

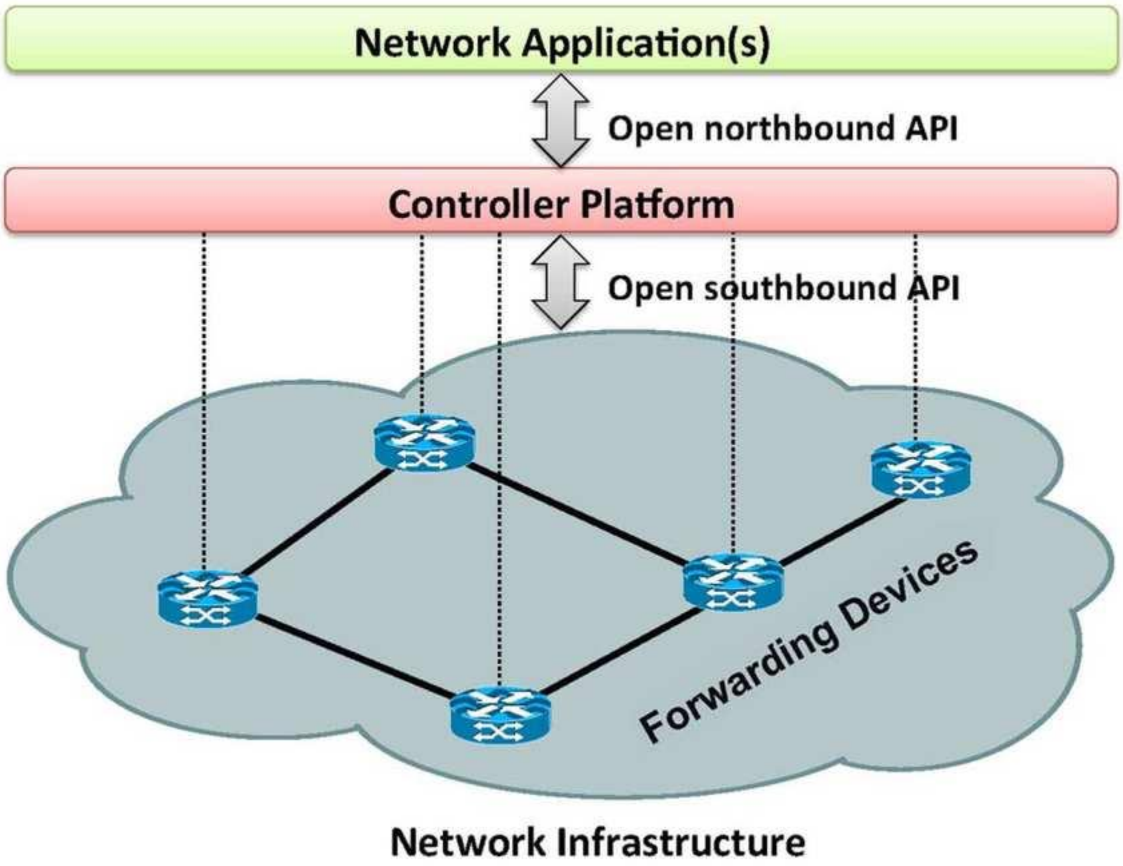


Figure 2: A Simplified view of an SDN architecture [1]

Software-Defined Networking architecture has four pillars that define it in [1], which are: The control and data plane separation, which makes the devices merely forwarding elements.; Flow-based forwarding decisions, flow is a set of packets from source to destination. These flow-based decisions match the traffic, and forwarding devices forward the traffic according to these decisions.; The Control plane is moved to an external logically centralized controller called the SDN controller or Network Operating system. It is a software platform that acts as the strategic control point of the network. It is essentially the brain of the network that handles all the flow control to the underlying network of forwarding devices via Southbound APIs and the management of the network via Northbound APIs.; Network applications that reside above the SDN controller make the network programmable [1] [5].

As Scott Shenker introduced the SDN concept in [6], It can be defined in three fundamental abstractions: (i) distribution, (ii) specification, and (iii) forwarding. The distribution abstraction shields the network applications from the complexities of a distributed state. Which makes the distributed control problem a logically centralized one. It can be realized with a distribution layer, where the layer is responsible for installing control commands on the forwarding elements and providing a global network view to the network applications based on the status information from the forwarding layer. The specification abstraction allows the network applications to express the desired network behaviour without being responsible for implementing it [1] [6].

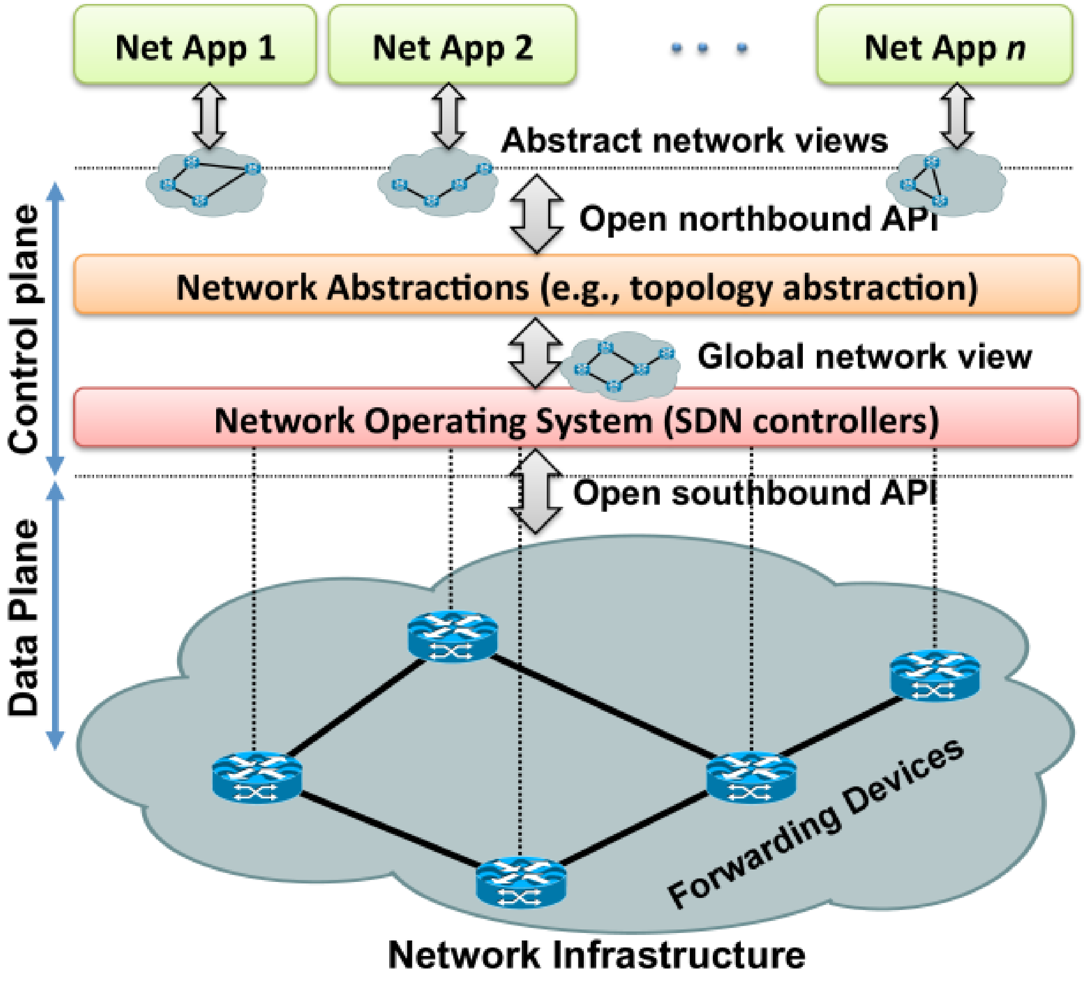


Figure 3: SDN Architecture and its abstractions [1]

Network virtualization and network programming languages can help in achieving this level of abstraction. Network applications can access a much abstract and simpler network model, which is a part of the global network view based on the behavior that needs to be expressed. The control plane needs a flexible forwarding model in the forwarding abstraction because we don't want it to be limited. So the abstraction here can support any forwarding behavior that is desired by the network applications while hiding the underlying hardware. This can be realized with a protocol like OpenFlow. These abstract views are shown in Figure 3 [1] [6].

1.3 Traditional vs Software-defined networking

Traditional network devices have their control and data plane strongly coupled together, making the addition of new functionalities a complex task. Adding new functionality means making changes to the control plane, while the control plane is embedded with the data plane in each device. The new functionalities or features could be introduced via firmware upgrade for every device and can be hardware upgrades in some cases. Hence the solution for this is using middleboxes with specialized and proprietary hardware and software, which can often be very expensive. These devices need to be placed in the network strategically and increase the complexity of the network, which makes it harder to modify the topology, configuration, or functionality of the network [1].

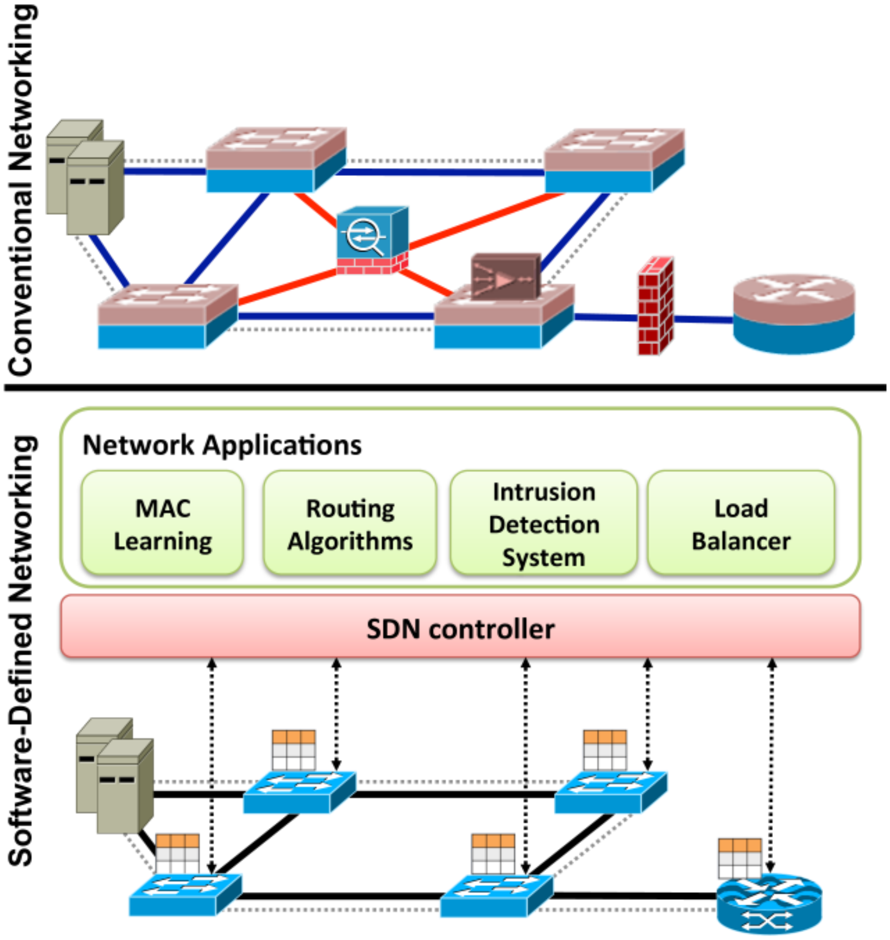


Figure 4: Traditional networking versus Software-defined networking [1]

As we know that SDN decouples the control plane from the data plane, we are no longer limited by the limitation of the traditional network. The only thing that was holding us back in terms of adding new features and functionalities was the distributed control plane. Now that we have a separate and centralized control plane reside in an SDN controller or Network operating system, we can add new functionalities and features much easier than the traditional network. We can introduce these featured middleboxes as SDN controller applications. Figure 4 shows us the striking difference between traditional networking and software-defined networking. The global network view can be shared with all the network applications, which can lead to better and effective policy decisions. Applications are easier to program as they share the same network abstraction provided by the control platform. Applications can be integrated much easier and effectively than earlier [1].

1.4 Software-Defined Networks

Software-Defined Networks has three planes, i.e., Data, Control, and Management plane, just like a traditional network, while here the planes are divided into various layers shown in Figure 5. The Data plane consists of two layers, which are Network infrastructure and Southbound interface. The control plane consists of three layers: Network Hypervisor, Network Operating System, and Northbound interface. And management plane consists of Language-based virtualization, Programming Languages and Network Application. Layers like Southbound interface, Northbound interface, Network operating system and Network applications are always present in an SDN deployment, while other layers are dependent on the type of deployment. Let us discuss the layer from bottom to top [1]:

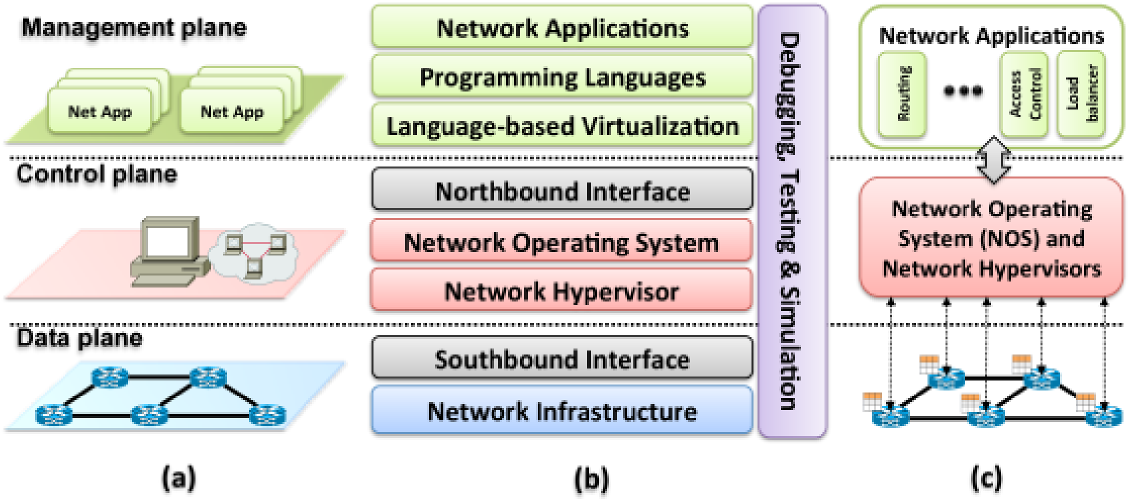


Figure 5: Layered view of Software-defined Networks [1]

Infrastructure Layer: SDN Infrastructure layer consists of a set of network devices, just a traditional network. However, these devices are merely just forwarding devices as they don't have a control plane embedded with their data plane like a traditional network device. They do not have the brain to make autonomous decisions for themselves. That decision-making capability has been moved to an external logically centralized entity, for example, a Network Operating system, as shown in Figure 5 (c). A network operating system communicates with the underlying infrastructure layer using a protocol such as OpenFlow, which is a standard protocol to ensure compatibility between different devices and the network controller. In SDN/OpenFlow, architecture has two elements: the forwarding device and a controller. A forwarding device is a data plane device that can either be a physical device or software. The controller can be software running on a commercial off-the-shelf device. A forwarding device with OpenFlow enabled work with the flow table present at the Controller. The flow table has three parts; the first part matches the incoming packet with the existing flow entries. T second part is executing the action based on the flow entry, and the third to maintain the counter for matching packets' statistics [1].

Southbound Interfaces: Southbound Interfaces, also known as Southbound APIs, connect the forwarding devices with the Controller. They are a bridge between these two entities. OpenFlow is widely accepted as a Southbound API in SDN architecture. It provides communication between forwarding devices and the Controller while being an essential part of the forwarding device. Forwarding devices are OpenFlow enabled, and it provides compatibility and interoperability between the devices and the Controller. However, OpenFlow is not the only Southbound interface;

there are many such as OVSDB [7], OpenState, Hardware Abstraction Layer (HAL), ForCES, and Programmable Abstraction of Datapath(PAD) [1].

Network Hypervisors: Virtualization is a mainstream technology used to create virtual instances of compute resources, storage and network resources. A hypervisor is software that enables users to create these virtual instances over the same hardware resources. Virtualization is what enables the cloud to provide Infrastructure as a Service, where cloud providers create compute to storage instances for their users from a shared pool of resources. One of the important virtualization features is that a virtual machine can be created, migrated, or destroyed on demand. They are making their provisioning easier and flexible. A network hypervisor enables us to create virtual networks and abstract those virtual networks from the underlying hardware network. These virtual networks consist of components like virtualize switches, routers, or firewalls depends on the resource requirement. These virtual instances and components can be provisioned instantly to meet network demand. Hypervisor helps in controlling and managing these instances [1] [8].

Network Operating System: The concept of a network operating system comes from a traditional operating system, which provides a high-level interface to access and control the low-level hardware resources. However, in networking, the devices are being managed and control via lower level and device specifics instructions and commands. Their operating systems are closed and proprietary, i.e. Cisco IOS, Juniper JunOS, etc. A Network Operating system or Controller is one of the important elements of the SDN architecture. It provides abstractions, essential services, and common high-level application programming interfaces. When the operator defines the policies, the Controller generates the configuration for the underlying network hardware. A controller can be centralized or distributed; Centralized Controller is a single multi-threaded entity controlling all the network's forwarding devices. Being a centralized controller, It might not be enough to handle a large network, and the biggest disadvantage of all is the single point of failure. In contrast, a distributed controller provides a much-required redundancy and a scaling capability. This kind of controller is resilient with high availability and less prone to physical failure as there is no single point of failure. These can be independent entities spread across the network controlling their respective segments or a cluster of controllers. In both cases, the impact of a single point of failure is greatly reduced; meanwhile, Scalability and control plane resilience is improved. The high-level interfaces it provides are the Northbound APIs such as REST APIs and programming languages, and it communicates with the underlying network via Southbound interfaces. There are a number of controllers in the market; most of them only support OpenFlow as a southbound API. At the same time, there are few which support a wider range of southbound APIs. OpenDaylight is an example of such a Controller, which supports multiple protocols as a southbound API such as OpenFlow, NETCONF, BGP, SNMP, PCEP, OVSDB, and LISP flow mapping. These protocols co-exist because OpenDaylight provides a service layer abstraction [1] [9].

Eastbound and Westbound APIs are special application programming interfaces required by distributed controllers as shown in Figure 6. The controllers use these APIs for communications and monitoring purposes. As southbound and northbound APIs are essential for the controllers, East/Westbound APIs are also essentials for distributed controllers. These APIs provided interoperability and compatibility between different controllers, which increases the robustness of the system and reducing the probability of common faults [1].

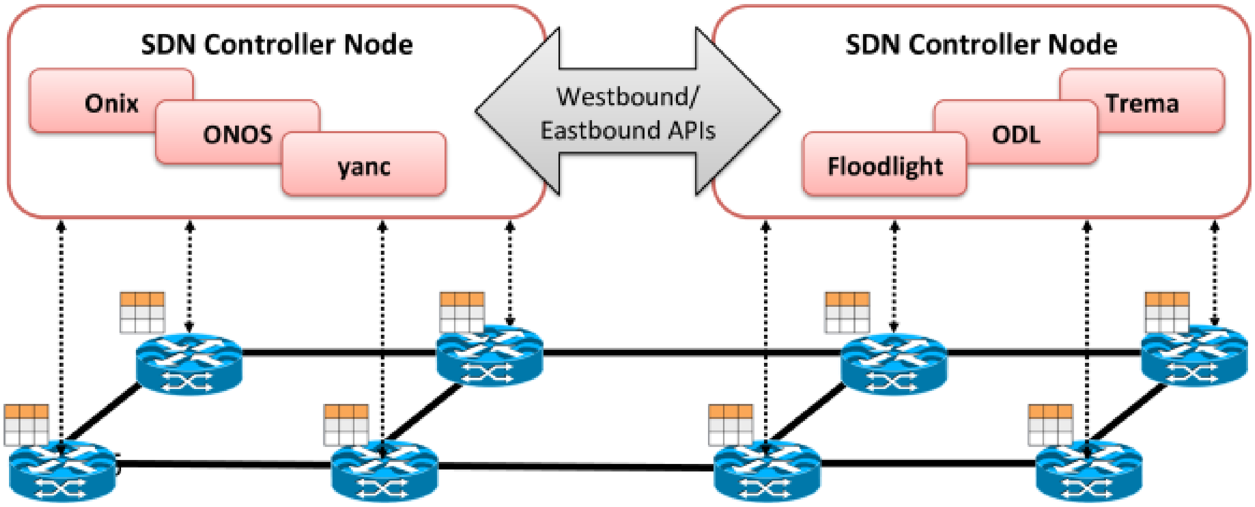


Figure 6: Distributed Controllers [1]

Northbound Interfaces: Northbound interfaces are the high-level programming interfaces provided by the network controller to the upper layers. It is one of the crucial abstractions of SDN architecture second one being Southbound APIs. But there is no widely accepted standard Northbound API as the Southbound API's OpenFlow. As Northbound interfaces are a software ecosystem, not hardware as southbound, these are dependent on the implementation. Though there is no common Northbound API, but an Open and Standard Northbound interface is needed to support and promote portability and interoperability. There is some proposal such as SFNet which is a high-level API and translates the application requirements into service requests, and another proposal was by the Yanc control platform which presents the idea of using the file system as an API. Being a software API, northbound APIs have different functions considering the requirements of different applications. So, it is quite complex to make a single standard northbound API [1].

Language-based Virtualization: Virtualization provides us with modularity and multiple levels of abstraction. When it comes to a programming language solution that can provide us with these features in terms of virtualization, we do not have many options. Pyretic is one of the solutions which offers a high-level abstraction of the network. It creates an abstract network topology with network objects and policies to provide the required services. Another form of virtualization is the static network slicing approach, where the compiler slices the network according to application requirements. This method provides high performance and isolation. In a solution named Splendid Isolation which uses this static network slicing, the network slices have three components, topology, mapping and predicates of packets. Different combination of these combinations was provided to different applications, in order to generate a global network configuration. Isolation among the slices can be achieved using this technique. libNetVirt is also a virtualization solution that creates and manages virtual networks and enables Quality of Service (QoS) capabilities in these virtual networks. It has two layers, the first layer is a generic network interface, and the second layer has technology-specific device drivers i.e., OpenFlow, VPN, MPLS. Over these two layers exist network applications and virtual network descriptions. The OpenFlow driver creates virtual networks that are isolated from each other using rule-based flow tables [1].

Programming Language: Low-level programming languages were being used to program the network for decades. Low-level programming languages does not provide any kind of abstraction; hence their Usage makes the developer stuck at the low-level details of the networks instead of focusing on the real problem. The instruction sets written in low-level languages cannot be re-used due to the lack of interoperability between the devices. On the other hand, High-level language provides an abstraction from the low-level hardware, so the developer can spend less time focusing on the low-level details and more time solving the problem at hand. High-level languages enable higher-level of abstraction, which can be used to program the devices. It provides code reusability, software modularization and promotes network virtualization. Several challenges that exist in SDN can be addressed with a high-level programming language. Writing programs for virtual network topologies were made possible by high-level programming language abstractions. Let's take an example: we can write a program for the abstracted network topology and the programming language will handle the low-level instructions required to enforces that policy on every forwarding device, while we will focus on the abstracted network topology. With this kind of abstraction, developing network applications becomes an easy process. This example will be much complicated to implement with a low-level language [1].

Network Application: Network Applications reside at the top layer in the SDN architecture; these applications are the brains of the network. As the brain of the network, they implement the control logic, which then will be enforced onto the forwarding devices by the Controller as forwarding rules. Take an example of creating a simple route from point A to B; the application will take an abstract of the network topology and instruct the Controller to implement this required route. Then the Controller will install the rules onto the forwarding devices to get the necessary behaviour. Network applications can perform traditional functionalities such as routing, load-balancing and installing security policies. However, SDN enables the network applications to do much more than the standard functions, including reducing power consumption, end-to-end QoS, Network Virtualization, fail-safe and reliability functionalities to the data plane and many more [1].

2 Network Function Virtualization

Network function virtualization is the decoupling of the network functions from the traditional and proprietary hardware. Traditional networks consist of a lot of middle-boxes, which are proprietary hardware appliances. The devices such as firewalls, Intrusion detection systems (IDS), Intrusion prevention systems (IPS), Network address translator (NAT) and so on are the middle-boxes that are responsible for the functionality of the traditional network services. Each of these middle-boxes has a specific function in the network. For example, a firewall is required to protect the network from external threats. These middle-boxes are placed in the traditional network strategically via a complex deployment process. This strategic placement of these middle-boxes results in an increase in the network complexity and rigidity. This deployment process requires a technically trained person with specialized skills and is quite expensive and time-consuming. This deployment process could take weeks and months, which makes it a very long deployment cycle. These middleboxes are proprietary, standalone, and closed, which cause a new set of complex problems if anything goes wrong during or after deployment. This makes launching a new network service in the network infrastructure is a relatively expensive and time-consuming task. Purchase of new middles-boxes and maintenance of the old ones can increase the capital and operational expenses. In some cases, coordination between new and old middle-boxes can be quite complex as they do not always have the same underlying hardware. NFV comes into play to solve this problem, which aims to reduce the time to market, equipment cost and create a scalable and strong ecosystem. NFVI management and orchestration can automate service evaluation and testing, which results in the reduction of time spent on these tasks. NFV enables the network operator and service providers to run network functions as the software on the Commercial off-the-shelf hardware, results in a decrement in the cost of equipment. Lastly, the NFV ecosystem will be built over general-purpose Infrastructure instead of expensive and proprietary infrastructure. Where the virtual network functions are hosted and executed, and better network performance and service provision experience are ensured by orchestrating the virtual network functions and placing them on the network point of presence (N-PoPs) of the network [10].

2.1 What is Network Functions Virtualization?

The concept of Network functions virtualization was proposed by a group of over twenty of the world's largest telecommunications service providers. Telecommunications service providers such as American Telephone and Telegraph (AT&T), British Telecom (BT), Deutsche Telecom (DT) formed an Industry Specifications Group (ISG) within the European Telecommunications Standards Institute (ETSI). ETSI released NFV standards in October 2013; the high-level NFV framework can be seen in Figure 7. The separation of network functions from the hardware proposed by NFV can effectively reduce capital expenses and operational expenses. These network functions can be hosted as virtual machines in the COTS hardware and called virtual network functions. Scaling of virtual machines is done by NFV to handle the data center traffic changes. Software-defined networking and network functions virtualization are related but independent of each other. However, NFV is used in Software-defined networks [1] [11].

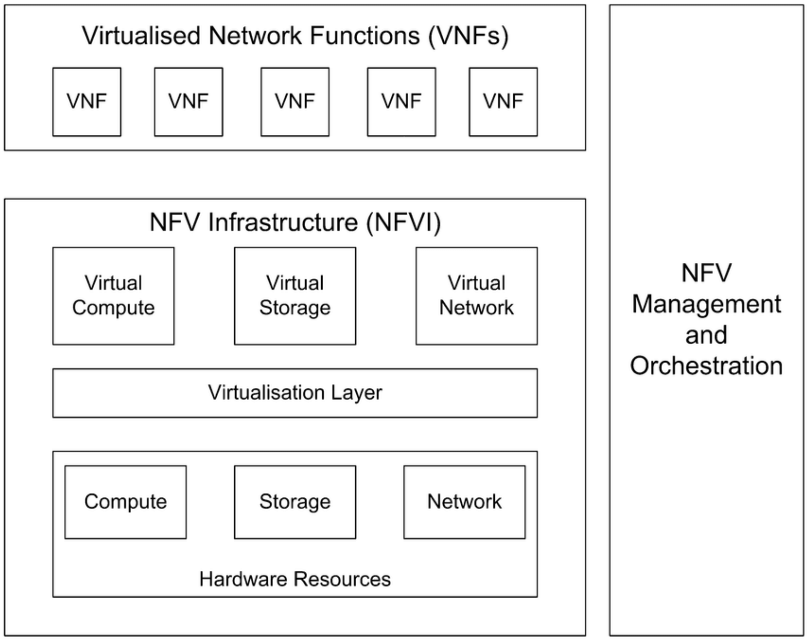


Figure 7: High-level NFV framework [11]

The high-level NFV framework shows that NFV has three significant components, which are Network function virtualization infrastructure (NFVI), Virtual network functions (VNFs) and NFV management and network orchestration (NFV MANO. As Figure 7 above shows us a more high-level NFV framework, below Figure 8 shows us as low-level NFV reference architecture where the NFV components can be further divided into smaller components. Let's discuss these NFV components and their breakdown in detail below [10] [12]:

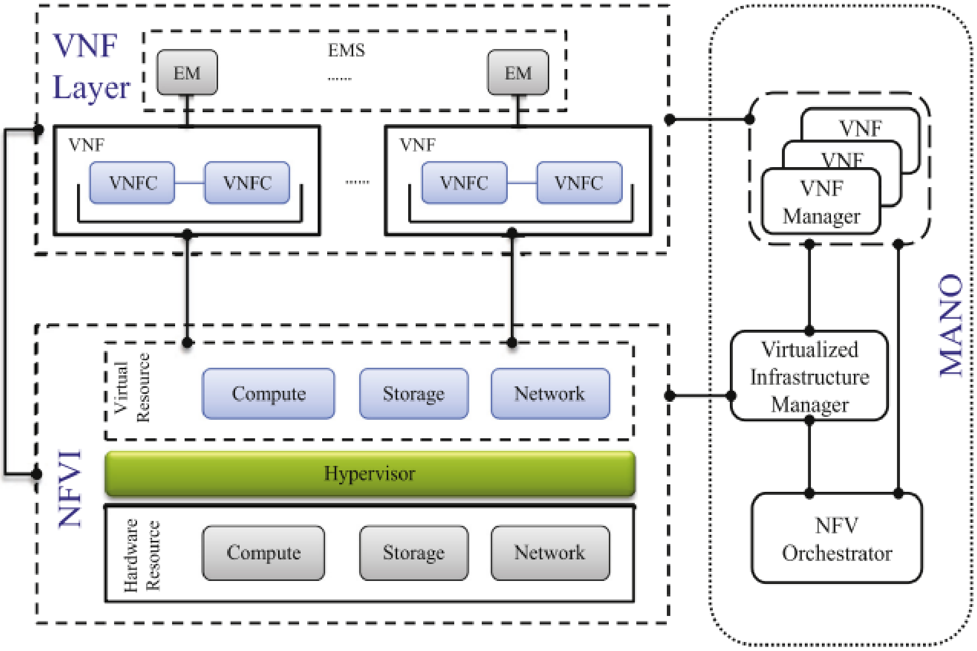


Figure 8: ETSI NFV reference architecture [11] [10]

2.2 Network Function Virtualization Infrastructure

The network function virtualization infrastructure layer provides the essential services need by NFV to function. It has a physical layer where it deploys the general-purpose hardware network devices, resulting in low latency and low network cost. These devices are deployed in distributed locations. These general-purpose hardware network devices are the foundation for the virtualization environment of the NFV. As shown in Figure 8, NFVI is further divided into physical Infrastructure, virtualization layer, and virtualization infrastructure [10].

2.2.1 Physical infrastructure layer

The physical infrastructure layer is composed of general-purpose hardware devices, typically x86 servers. These servers provide compute and storage functionalities. These servers are also known as compute nodes and storage nodes based on the functionality the server provides. Internal interfaces are used to communicate between compute nodes and network elements. The underlying devices can be further divided into the following [10]:

1. **Compute hardware:** Compute nodes managed by the internal instruction set are also referred to as Compute hardware. These are made up of general-purpose hardware servers. These compute nodes can have a single-core or a multi-core processor based on the NFV requirements. There are many types of general-purpose servers available in the market which can be used for compute nodes. Generally, these servers are classified into three categories based on their characteristics [10]:
   - Tower server: A computer built in an upright cabinet can be referred to as a tower server. These servers provide a degree of robustness to prevent damages and reduce possible service downtime. Usually, for NFVI deployment, operators prefer to use branded prebuilt tower servers from brands like Cisco, HPE, IBM etc. However, these tower servers have a large volume and weight, so available floor space can be a constraint while expanding the NFVI. The capital expense and operational expense can also increase as these tower servers are independent of one another and have their own cooling system, I/O devices, etc. [10].
   - Rack server: The servers which are mounted in a server rack are the rack servers. If we compare rack servers to the tower server, a rack can have multiple servers while a tower only has one server. So, the floor space is not a constraint anymore in the expansion of NFVI. These rack servers are mounted in a server rack over one another, which results in consolidations of network resources. 1U and 2U are the current industry standard rack servers, which represent their width and height. 1U rack servers are 19 inches wide and 1.75 inch high, while 2U rack server is 19 inches wide and 3.5 inches high [10] [13].
   - Blade server: Blade servers are evolved from the concept of a rack server. There are two components to blade servers. One is the blade server, which has a processing unit, and the second is the blade enclosure. The blade servers are placed inside the blade enclosure, which makes the blade system. This blade system meets the IEEE standards for the rack unit. Blade servers share certain hardware elements with the other blade servers in the rack and provide more processing power than the tower and rack server in less floor and rack space, making NFVI expansion possible and easy. As NFV workload is mainly compute and networking, a high-density server can be a good choice, which can handle cooling, networking, and

hardware management for the whole set of Compute nodes. A high-density server can be achieved by packing multiple blade servers in a single chassis [10].

  - Hyper-converged solution: This solution involves the consolidation of compute, network, and storage resources in a single device. This mechanism provides high availability, security, and backup. But high convergence characteristics of these devices result in rigid network deployment, configuration, and scaling. Many vendors are using this approach for more I/O-centric NFV workloads [10].

2. **Storage hardware:** Device which is capable of storing information temporarily or permanently are known as storage hardware. Storage-based network functions such as network cache for data processing or video streams use storage hardware for their operation. As a network transfer a large amount of data, we need high speed and high storage servers for data processing and storage. Storage hardware consists of storage servers with large numbers of solid-state disks (SSDs) or hard disk drives (HDDs) with a small amount of compute power and memory. Storage in these servers can be expanded by installing new external disk drives. These storage servers can be used in the following aspects [10]:
    - Direct Attached Storage (DAS): In DAS, that storage is directly connected to the servers with either of these interfaces; Small Computer System Interface (SSCI), Serial Advanced Technology Attachment (SATA), Serial Attached SCSI (SAS), Fibre Channel (FC) or iSCSI. DAS is less expensive, provides better performance and efficient energy use. These storages can only be accessed by the server it is attached to [10] [14].
    - Network Attached Storage (NAS): NAS stores the data at the file level and provides file sharing capabilities among the heterogeneous hosts throughout the network. Shared storage can be access via the ethernet connection. NAS acts as an independent network node with its own IP address. It provides ease of access, high performance at low cost [10] [15] [16].
    - Storage Area Network (SAN): SAN stores the data at the block level and provides access to shared data storage to the hosts. SAN and NAS are similar as they both provide access to the shared storage. However, SAN does at that block-level while NAS does that at a file-level [10] [16].

3. **Networking hardware:** Network hardware consists of the devices capable of performing basic network operations. Usually, these devices are proprietary L2/L3 bare metal switches. But in the NFV ecosystem, these devices are replaced by industry-standard devices, which support OpenFlow or conventional routing protocols or both. Many industry-standard switches are available in the market, i.e., IBM Rackswitch, Juniper QFX series switches. Network interface card (NIC) is also an important component of network hardware, is responsible for network connectivity of compute nodes with other network elements [10].

2.2.2 Virtualization Layer

The virtualization layer is located in between virtual Infrastructure and physical Infrastructure in NFVI. The main goal of this layer is to emulate the physical Infrastructure and provide it as the virtual Infrastructure needed by the virtual machines in the VNF layer. This layer uses the hypervisor to split the physical resource and the virtual machines. These virtual machines have their own necessary peripherals, even though they share the same underlying hardware. The changes in the virtual environment, such as virtual machine removal, installation, online migration, or dynamic scaling, can be supported by the hypervisor. Hypervisors adjust the physical and virtual resources allocated to the virtual machine dynamically by the high-level of portability that can be achieved between virtual machines. Hypervisor's main job is to emulate the hardware resource and provide them as virtual resources to the virtual machines. The mainstream hypervisors used in NFV are the following [10]:

1. KVM: KVM is an open-source hypervisor widely used in Linux based operating systems. It is a type 2 hypervisor, as it works on the top of an OS, i.e., the host OS and runs virtual machines, which are called are guest OS. An extension of KVM known as real-time KVM was developed for time-sensitive workloads. KVM type 2 hypervisor is a virtualization technology that helps in achieving NFV's goal of decoupling network functions from the proprietary hardware and virtualizing them. At the same time, real-time KVM can do the same thing with some rigorous and time-sensitive requirements [10].
2. Xen: Xen is also an open-source hypervisor like KVM, which can simultaneously execute multiple guest OSs. As KVM runs on the host OS, Xen can run directly on the physical machine, making it a type 1 hypervisor. It can run multiple guest OS instances in parallel;

these can be the same or different OSs. These virtual machines do not need virtual resources, as they are aware that they are virtual machines. However, they make special calls to the hypervisor to access the physical resources. Xen supports two types of virtualization, paravirtualization and full virtualization [10].

3. Hyper-V: Microsoft Hyper-V is a commercial hypervisor present in windows servers of Microsoft. It provides a carrier-grade virtualization solution for enterprise data centers or the cloud. Hyper-V is commonly used for enterprise data center workload or for those who want to build the cloud service. It can be installed as a standalone virtualization server. That server can provide a set of management tools that can be used in NFV, such as virtual network manager. Hyper-V can also enable NFV capacities such as tenant isolation and traffic shaping using Hyper-V-based virtual switches [10].
4. ESXi: ESXi is another hypervisor that can be used for virtualization in NFV; it is a type 1 hypervisor. It virtualizes the enterprise-class servers and provides many advanced features for management and administration, such as fault tolerance and high availability. However, it is much more expensive than the hypervisor we discussed earlier, like KVM, etc. NFV can use ESXi as a hypervisor, but its needs to be tuned according to the NFV workload and maximize performance [10].

Apart from Hypervisor technology, Container technology can also be a feasible virtualization solution for NFV. The differences can be seen in the below Figure 9, Hypervisor host application and VNFs, which are isolated from each other. On the other hand, the container does not have a separation between the hosted application and VNFs. By doing this container reduces the overhead compared to the hypervisor [10].

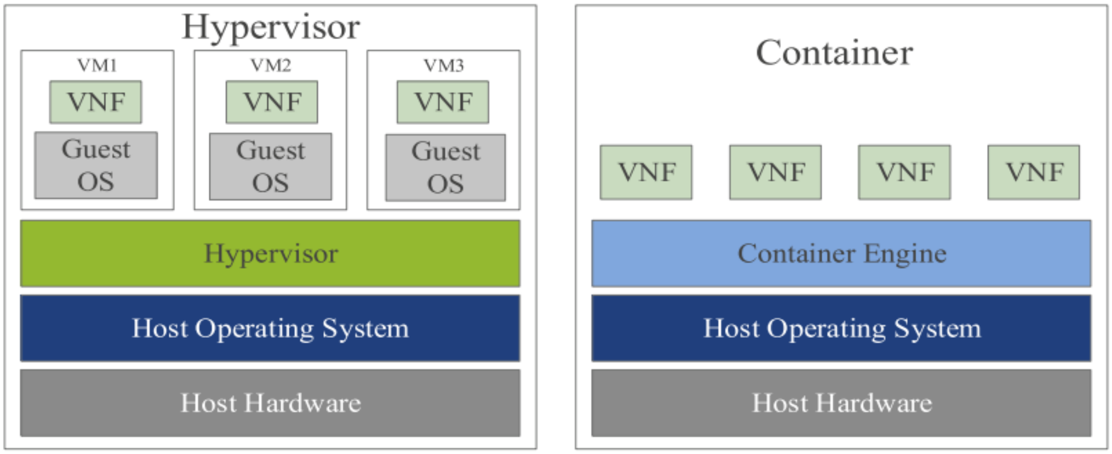


Figure 9: Comparison between hypervisor and container [10]

A container does offer an opportunity to reduce the overhead, but it also introduces potential security issues as the hosts are not isolated from one another. One example of a container is Docker [17], which is an open platform for developing, shipping, and running applications in a virtualized manner. It separates the applications from the Infrastructure, which increases the application delivery time. FlowN is another lightweight container-based virtualization technology designed to address multi-tenancy problems in the cloud. FlowN uses a shared controller instead of a separate one to run tenant applications. Each tenant is provided with a vision that it has its own address space, Controller, and topology. The virtual environment provided by the hypervisor or the container must be equivalent to the hardware environment. Thus, the application and tools virtualized should work in the virtual environment as they work in the hardware environment [10].

2.2.3 Virtual Infrastructure Layer

The virtual infrastructure layer resides just above the virtualization layer; it consists of three components, which are virtual compute, virtual storage, and virtual network. These three components are essential for providing a virtual environment in NFV. These resources are, however, virtual, but they are virtualized from the physical resources [10].

1. Virtual compute: Hardware processing elements are virtualized by hypervisor using specific application programmable interfaces (APIs). By this virtualization, we can achieve virtual compute resources. APIs like libvirt and vCenter is used by hypervisors such as KVM and ESXi, respectively. Both of these API provides management for virtual compute resource. Software-defined compute (SDC) is another compute virtualization technology

by which we can view all the computing resources as one resource pool, and it can move all the computing functions into the cloud [10].

2. Virtual storage: Virtual storage resources can be achievable by virtualizing hardware storage resources. The software for storage management is decoupled from the underlying hardware, which creates a virtual storage resource pool and provides features like snapshots and backup. There is another storage virtualization technology called software-defined storage (SDS), which separates the control and management software from the underlying hardware and enables a virtualized network of storage resources. This storage network creates a single virtual storage entity by connecting several large storage pools [10].
3. Virtual networking: Virtual networking is the virtualization of hardware networking. It enables virtual network environments that connect virtual machines, virtual servers, and other components in it. It consists of software functions like virtual switches and virtual ethernet adapters. We can build a virtual network by connecting various virtual machines and servers. The important component of virtual networking is the virtual switch, which helps in communications between virtual machines using the protocols used by its physical counterpart. One thing we need to be aware of is that virtual machines and servers we are connecting may be running off the same or different hypervisors. There are many open-source and commercial switches available. Let us discuss a few [10]:
    - Linux Open vSwitch (OVS): It is a virtual switch that provides a programmable data plane. The benefit of using OVS is that it can be ported into different environments as it is written in C language. It supports multiple hypervisors such as KVM and Xen. Hence it can be distributed across physical servers. Another feature that makes it portable is that it works without any kernel modules [10].
    - Linux Open Switch: It is an open-source virtual switch that is based on Linux. Compared to OVS, it is deployed at the physical switch instead of the virtualized layer. It provides a fully programmable L2/L3 control plane and controls the real hardware I/O of the physical switch. It enables developers to break the boundaries of the integrated switches by acting as a catalyst in accelerating the transition to disaggregate the network switches. Which makes the network better serves the needs of the customer [10].

- OpenStack Distributed Virtual Router (DVR): It is an OpenStack distributed virtual router which moves the routing functionalities to the compute nodes instead of the network nodes. It helps in isolating the network's failure domain, and it optimizes the performance of the network traffic. It provides routing and gateway functionalities in the distributed architecture and is a supplement to OVS [10].
- Brocade Vyatta 5600 vRouter: It is a carrier-grade router that can reach speed as high as 10+ Gbps. It is proposed by Brocade and has integrated many support features. It can support nearly all general-purpose hardware platforms. It provides low-cost and fast service provisioning with flexible deployment [10].

With all these virtual components of the Virtual infrastructure layer, there are some software-based I/O acceleration methods for the data plane in NFV. NFV performance can be significantly enhanced by the following methods [10]:

1. Data plane development kit (DPDK): It consists of a set of software libraries and drivers, which enables fast processing of the packets. It is expected to improve the processing performance by ten times, and on a processor like intel Xeon, it can achieve around 80 million packets per second. Service providers used to use multiple architectures per workload, but they are shifting all their workload to a standard architecture with DPDK as it ensures scalability, simplification, performance and offers solutions to multi-vendor and multi-function problems. Their various extensions were developed for DPDK to combat its shortcomings. For example, one extension is used to eliminate the network bottleneck caused by DPDK, and another extension is there to provide extended kernel functionality [10].
2. Netmap: Netmap is an API used to enhance packet speed in FreeBSD and Linux. By using the libcap emulation library on top of netmap, we can increase the packet processing performance by five times. It has a very simple data model, which is quite beneficial in its usage in NFV and SDN. This data model let it enables application portability. And the same data model makes it complex to accommodate large-scale networks [10].
3. PF_RING ZC: It is a packet processing framework, which supports packet acceleration in a multi-core environment by using a set of APIs. Packet buffer is used in a multi-core system, where the CPU can access these buffers directly. PF_RING ZC clusters enable the

sharing of data among the processes. It offers a driver with similar capabilities as Netmap, the driver acts transparently, but when the PF_RING ZC application starts, it enables duplication of the packets which are made available for the OS. The regular applications are then unable to send or receive a packet via default OS interfaces. However, the duplication lowers the performance; their many extensions developed for this framework to improve it [10] [18].

4. PFQ: It is a framework built to provide safe and easy processing of the packets. It can also provide high-speed packet processing, but that is not the primary purpose. It uses a domain-specific language to implement algorithms for packet processing and does not rely on any specialized drivers, which can lead to performance degradation [10].

Though ESTI NFV ISG outlined NFVI, it does not provide a full solution for NFVI. That is the reason that vendors build their own NFVI according to their requirements. However, their approach to building the solution might be different, but they still have almost the same components as we discussed above [10].

2.3 NFV management and orchestration layer

NFV Management and orchestration layer that manages and orchestrates all the resources in the NFV ecosystem. ETSI defined NFV MANO for its management and orchestration role in NFV. It handles tasks like VNF life cycle management, network services life cycle management, resource management, etc. It can be broken down into three blocks based on these tasks, which are Virtualized infrastructure manager (VIM), NFV orchestrator (NFVO), and VNF Manager (VNFM). Though they are different blocks, they are implemented as a single entity due to the overlapping in their responsibilities [10].

As the reference architecture of NFV MANO proposed by ETSI NFV ISG has many limitations, many works are offered to overcome these limitations and add new functionalities. Zero-time orchestration, operations, and management (ZOOM) is proposed as a management and orchestration platform; it provided the much-needed security to protect the NFVI, VNF and services across the NFV framework. It also offered business agility in terms of zero-touch provisioning and self-service [10].

OpenMANO is another implementation that focuses on enhancing service provision, unlike Zoom that takes security as its main concern. OpenMANO has three components openmano, openvim, openmano-gui. These three components provide the practical implementation of the ETSI NFV MANO framework. Where openmano is the NFVO, openvim is VIM, and openmano-gui offers a friendly user interface to the operator. The advantage of using OpenMANO is that it provides the much-needed interoperability, and it can work with OpenFlow controllers [10].

Open-Source MANO (OSM), which is hosted by ETSI, is another implementation of the ETSI NFV MANO. As mentioned in the name, its main objective is to provide open-source NFV management and orchestration software. It breaks the NFVO entity into two parts one service orchestrator, which is responsible for end-to-end service provisioning and orchestration, and the second one is resource orchestration, which is responsible for allocating resources to the servers. It also has a VNFM that handles the VNF management and configuration. It leverages the functionalities and efforts of OpenVIM, OpenStack and VMware when it comes to VIM functionalities in OSM [10].

2.3.1 Virtualized infrastructure manager (VIM)

The Virtualized infrastructure manager is responsible for managing and controlling compute, storage, and network resources in the NFVI. Though the virtualized infrastructure manager (VIM) is a specific part of the management and orchestration framework, it can have multiple instances. In general, VIM has two kinds of instances, one where it is used to manage multiple resources and one where it only handles a specific kind of resource. VIM is responsible for the allocated inventory and mapping of virtualized resources to physical resources. This enables the processes like upgrading, allocation, reclamation, and release of the NFVI resources and ensures optimized use of these resources. A repository of NFVI hardware resources (compute, network, storage) and software resources (hypervisors) are also handled by VIM. It enables the features and capabilities discovery for the resources to optimize their usage. By organizing the virtual links, networks, subnets, and ports, it can support VNF forwarding graphs (VNFFG). It ensures access control by managing security policies. Functions like collecting information about performance and faults, management of software images, management of virtualized resources are all handled by the VIM. VIM uses to perform these functions by interacting with the network controller via its southbound interfaces. Open-source MANO (OSM) is an ETSI-based project, which adds functionalities of their VIM component. These functionalities include the usage of OpenVIM for these capabilities and increased interoperability between different components. VIM's importance is visible to Infrastructure as a service (IaaS) provider, as VIM coordinates the hardware resources allocation to deliver network services. Allocation of the resource is done dynamically by VIM, and during the allocation process, it ensures a better and smooth user experience [10] [12].

2.3.2 NFV orchestrator (NFVO)

Network functions virtualization orchestrator, as the name suggests, is responsible for resource orchestration and network services orchestration. NFV Orchestrator is an important component of the NFV MANO framework. It provides interoperability with SDN elements by standardizing the virtual networking functions [12].

Resource orchestration is important in NFV based solutions, which ensures optimal resource usage to provide a required network service. NFVO is responsible for global resources management, which involves allocation and monitoring of the resources used by the given services. NFVO makes it possible by coordinating with the virtual infrastructure manager (VIM), or in some implementations, it directly interacts with NFVI resources. NFVO can manage the resources by interacting with VIM's northbound APIs, or it can directly manage the NFVO resources [10] [12] [19].

Network services are provided by a collection of virtual network functions connected in a particular fashion via virtual links, which is also known as virtual network functions forwarding graph (VNFFG). Network orchestration involves the creation and termination of a network service, modifying the capacity of network services based on the requirement, and updating VNF forwarding graphs. NFVO is responsible for the network services orchestration. NFVO designs and manages various catalogs such as network services catalogs, VNF catalogs and NFVI catalogs. Network services catalogs have the details of network connectivity between the VNFs. VNF catalogs have the details of the VNF resources structure such as CPU usage, memory usage, storage etc. NFVI catalog has the details of the resources available. It is also responsible for the instantiation of the VNFs as a part of network services orchestration, manages the policies for the network services and validates the resources requests. As NFVO provides access to key resource instances, it is a vital component to the NFV Solution as it provides the network services catalogs, VNF catalogs, NFV instances and NFVI resources [10] [12] [19].

2.3.3 VNF Manager (VNFM)

VNF manager is another key component of the NFV MANO architecture; it helps solves the challenges for network management and orchestration faced by the NFV MANO. As the name suggests, it manages the virtual network functions (VNFs). It also provides interoperability with SDN elements by standardizing the virtual networking functions. VNF manager handles the life cycle management of the virtual network functions (VNFs). These operations include instantiation, termination, upgradation, and scaling of the VNFs. The information about the VNF which are deployed should be stored in a template called a virtual network function descriptor (VNFD), which then is stored in the VNF catalog. A VNF Manager can manage either multiple VNF instances or a specific single VNF instance based on the implementation. However, all VNF instances should have a VNF manager managing them. VNF manager accomplishes these operations by interacting with VIM via the available APIs. This interaction involves making a service request to the VIM. There two modes in which the VNFM operates; one is the direct mode, and another is the indirect mode [10] [12] [20].

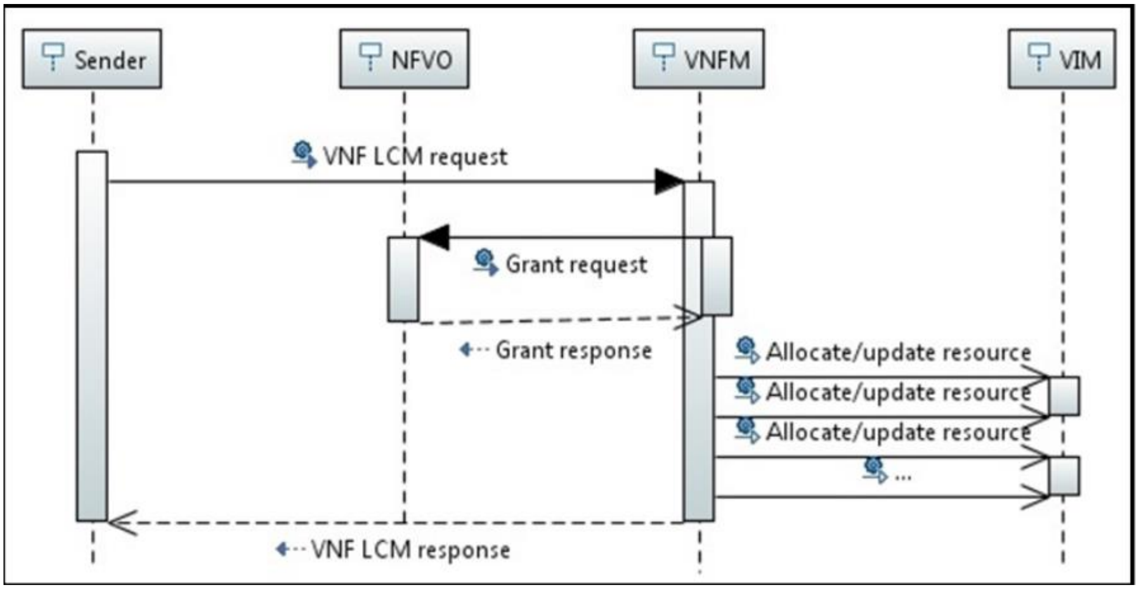


Figure 10: VNFM direct mode of resource request [20]

Figure 10 shows us the direct mode, in which the VNFM sends a "grant request" message to the NFVO, which then in response sends a "grant response" after receiving this grant response, VNFM request the resources directly from the VIM [20] [21].

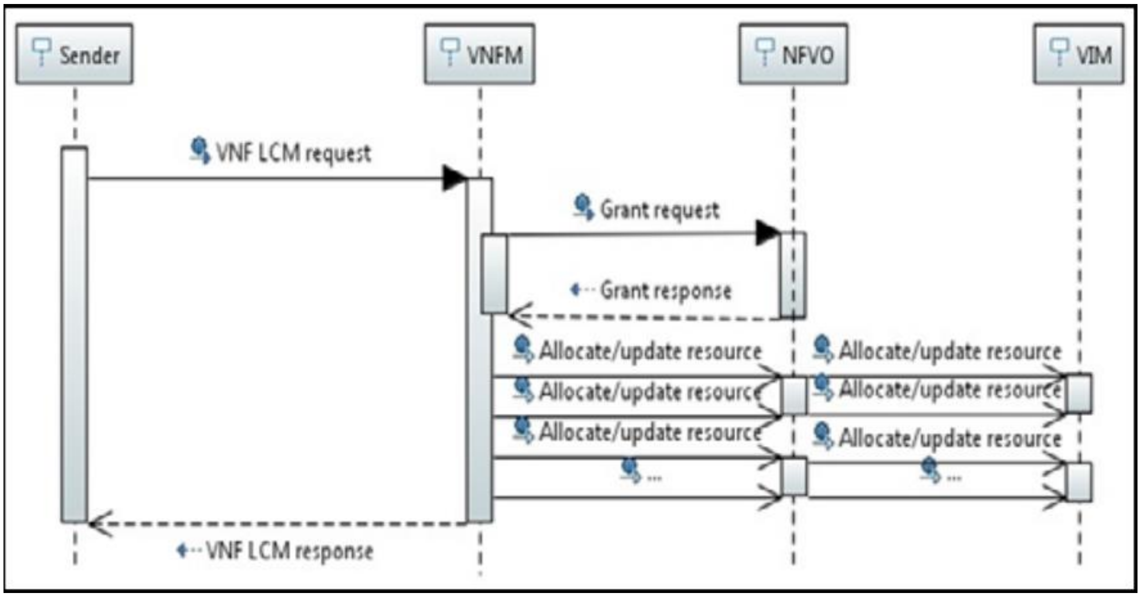


Figure 11: VNFM indirect mode for resource request [20]

Figure 11 shows us the indirect mode, where VNFM does not communicate with VIM directly. VNFM requests the resource via the NFVO, which approves the request and then proxies it to the VIM [20] [21].

2.4 Virtual network function layer

The virtual network function layer is the top layer in the ETSI NFV architecture. It consists of the Virtual network functions, which replace the physical network functions. VNFs can be connected to create virtual network environments. VNFs run on the virtual machines over the Infrastructure provided by the NFVI. These VNFs provide network functionalities as software that were used to be provided by proprietary and dedicated hardware middle-boxes. In the case of VNF, COTS hardware is used at the NFVI layer to host the VNFs. VNFs present in the VNF layer are isolated from each other, and every VNF is consists of multiple VNF components (VNFC). These components are managed by Element Management (EM). There is various element management in a single domain that makes up an element management system (EMS). EMS is a part of the VNF layer, which collaborates and exchanges VNFs related information with VNFMs to manage the VNFs. Chaining of multiple VNFs can be done based on enterprise requirements, where the VNFs are in a different location and are selected dynamically to make a service chain. There exists a high level of diversity in the VNFs, as every functionality provided a middlebox can be virtualized as a VNF. Due to this diversity, there are different types of implementations of these VNFs. We can see Table 1 below with the current VNF products and solutions provided by different vendors [10].

Vendors	Product/Solution	Description
Infoblox [22]	virtual secure Domain Name System (DNS) [22]	An expansion solution of the original DNS which reduces the business and operation risk during the network transition to NFV and SDN.
NEC [23]	NFV C-RAN [23]	A cloud-based RAN with automate L2/L3 functions adding and removing for NFV to meet the traffic demand in NFV.
NFWare [24]	virtual carrier-grade NAT [24]	Centralized network addresses translator.
Oracle [25]	IMS Session Delivery [25]	An agile IMS solution for delivering consumer VoIP and VoLTE services.
Red hat [26]	Linux-Atomic host [26]	A lightweight platform support running applications in Linux containers.
6wind [27]	Virtual Accelerator [26]	Accelerating packet processing for virtual network infrastructure in NFV.
	Turbo IPsec[26]	A software Virtual Private Network (VPN) appliance deployed on COTS servers in bare mental environment with the same functionality of the legacy IPsec VPN gateways.
Cisco [28]	Virtual Port Channel [28]	Allowing physical links between two devices to appear as a single port channel to a third device.
	Virtual Managed Services [28]	A cloud native solution for delivering new software defined WAN services to business customers.

Ericsson [29]	Virtual Router [29]	A carrier-grade software system which offers network operators the ability to deploy services with high agility and performance.
	vEPC [29]	Virtualized Evolved Packet Core networks.
Juniper [30]	vMX series edge router [30]	Revolutionary carrier-grade virtual routing for enterprises and service provider networks.
	vSRX integrated virtual firewall [30]	A virtual firewall designed for enterprises and service providers to achieve capabilities of firewall security and automation in a virtual machine.
Nominum [31]	N2 [30]	A virtual communication platform depending on browsers.
	Vantio CacheServe [30]	A DNS solution which integrates the N2 platform.
F5 [32]	Policy Enforcement Manager [32]	Optimizing and monetizing networks with context-aware policy enforcement.
	Local Traffic Manager [32]	Application delivery with programmable Infrastructure in a reliable secure and optimized way.
	Virtual Edition [32]	Deploying software-defined application service in hybrid virtual and cloud environments.
Metaswitch [33]	Perimeta Session Border Controller [33]	Carrier-grade virtualized network function which supports large scale communication security.
	Clearwater [33]	IP Multimedia Subsystem in cloud computing.
	Voice over LTE [33]	A VoLTE solution built from the ground up using cloud native service methodologies.
Brocade [34]	virtual Mobile Analytics [34]	Brocade network visibility platform for end-to-end mobile networks.
	SteelApp Traffic Manager [34]	A leading virtual application delivery platform for virtual environments or cloud.

	Vyatta 5600 vRouter [34]	Networking industry leader in virtual router with high performance and scalability.
	virtual Application Delivery Controller [34]	A software based VNF solution for fast reliable application delivery across the virtual and cloud platforms at massive scale.

Table 1: Various VNF products and solutions [10]

With the increasing number of VNFs, we need an automated solution to build and manage these VNFs. One such example is Click, which can build network functions that are flexible and configurable. There are software-based functions like packet processing and forwarding, which are available in Click. Functions like IPFilter, IP/UDP/TCP rewriter are some examples available to provide functionalities of firewall and NAT, respectively. However, click is used to simulate the NFV environment in a number of researches. ClickOS is proposed as an improvement over click due to its limitations. ClickOS provides a high-performance and virtualized software platform with functions varied from the firewall to carrier-grade NAT. Click and ClickOS are two lightweight platforms in this category, as there many other open-source and commercial platforms available for building and managing VNFs [10].

2.4.1 Virtualization Technologies

Generally, there are two kinds of implementation for VNFs, the first is using a virtual machine environment, and the second one is using container-based virtualization. Former uses the virtualization technologies such as KVM, XEN, Hyper-V etc. and provide an isolated VM environment for the VNFs. In contrast, the latter uses container technologies such as Docker and provide only necessary elements for virtualization and no isolation. Many technologies evolve using these two technologies, which can be seen in Figure 12 and described as follows [10]:

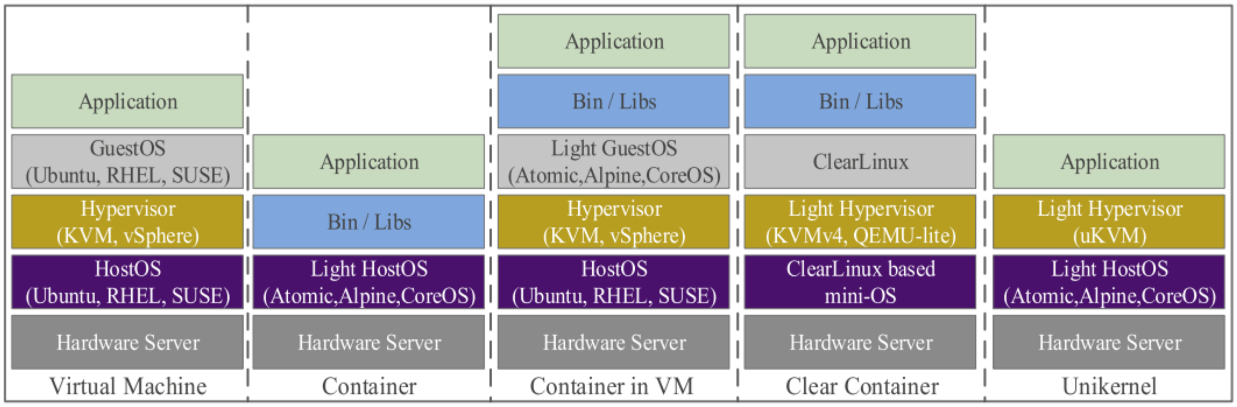


Figure 12:Various types of VNF implementations [10]

Virtual Machine: As we can see in Figure 12, the VNF applications are being run on the Guest OS, which is running in a virtual machine on top of the hypervisors (KVM, Xen, vSphere, etc.). The hypervisor is running in a host OS environment that runs on the physical hardware. Virtual machine technology is a commonly used environment for VNFs [10].

Container: The container is using a light host OS to virtualize and install the required libraries instead of installed an entirely new OS, i.e., guest OS. VNF execution in a container is simplified as the container running on a single compute node shares the same kernel. Though scalability is not an issue in containers, security is. As kernel sharing among the containers can result in security and isolation issues [10].

Container in VM: Container in VM, as the name suggests it is running a container in a virtual machine. By using this, we can leverage both technologies' benefits, VNFs are running in the containers, so their execution is simplified, and the container is running in a virtual machine, so the VNF are isolated from one another to some extent. But then comes performance and scalability, container promises both, but this approach does not guarantee that. This approach is used for NFV, where it does not require high performance [10].

Clear container: It is a project that originated at Intel; the idea behind this is similar to that of the previous approach container in VM. But their implementation is different as it is using a lightweight hypervisor, e.g., KVMv4, QEMU-lite and Clear Linux are being used as the host OS, which is a lightweight OS. This approach is leveraging the functionalities of a container but on a lightweight host, OS, which boosts the boot time and the image size is reduced. The size of the VM is also greatly reduced to make the VNF environment a container instead of a VM. Usage of the container is popular, so NFV development can leverage this approach [10].

Unikernel: Unikernel is another approach, which uses the library operating system. They do not offer a full guest OS; however, they offer the libraries to connect the VNF. This approach is beneficial in terms of boot time and size and is similar to the container approach. Though it is a good approach for NFV, before running any new VNFs, we must recompile them and considering the number of VNFs we can have; it can be a big disadvantage for this approach [10].

3 Legacy WAN Networking Model

A computer network that connects multiple local area networks (LANs) across a large geographical area is known as a Wide area network (WAN). It can be private, or a public WAN; private WANs connect businesses while public WANs connect smaller LANs. The world's largest WAN is the internet as a whole, and it connects the small LANs via internet service providers (ISPs). When it comes to a private WAN, It connects the headquarters site and remote branch sites of a business, which are distributed over a large geographical area. The purpose of WAN is to enable communication between smaller networks from different geographical locations to each other. Figure 13 shows us a simple WAN diagram [35].

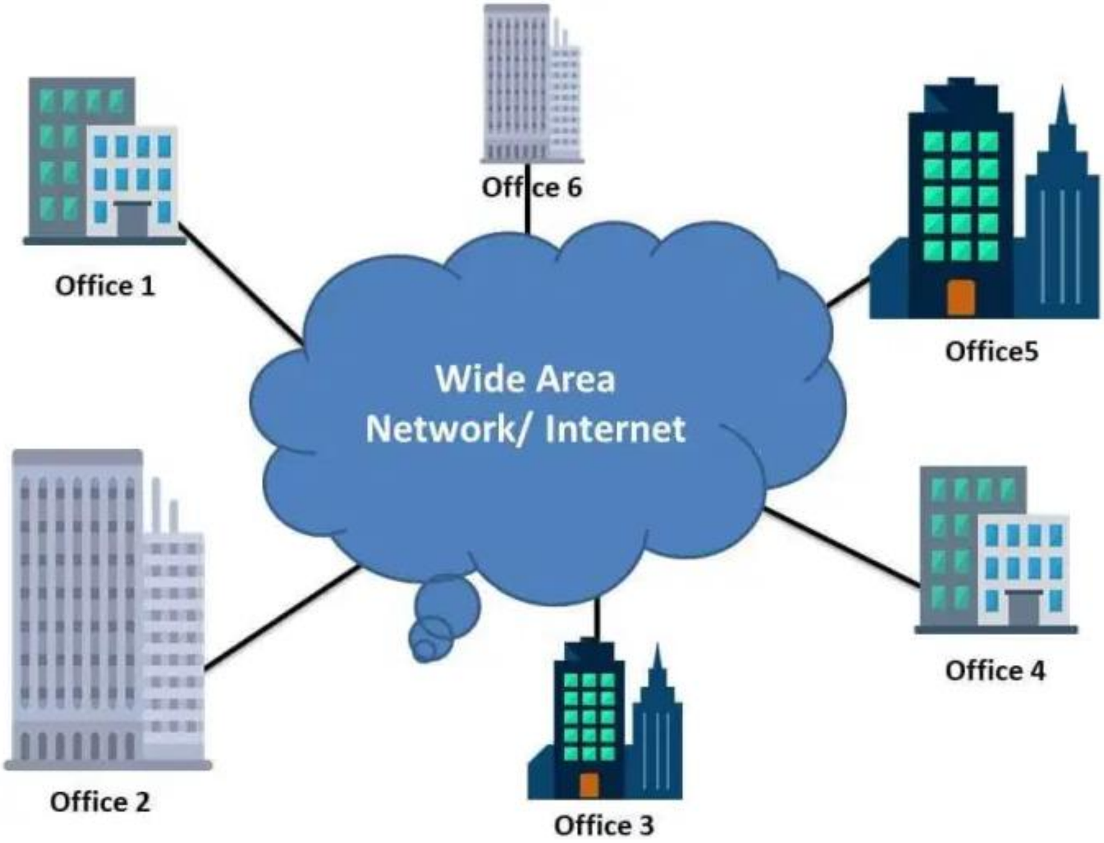


Figure 13: Wide area network diagram [35]

Since the early days of computer networking, Wide area networks have been around. Though now WAN connectivity options include leased lines, Multi-protocol label switching (MPLS), broadband and satellite, but in the early days, WANs were based on circuit-switched telephone lines. This changed the transmission rates drastically from 2400bps in the early days to 40 Gbps and 100Gbps today. This evolution led to an increase in the number of devices connected to the networks. This enables the enterprise to use applications that require high bandwidth, such as video conferencing and large backups. WAN links are provided by the service providers to customers; these links can be shared between the customers or can be dedicated to a specific customer. Dedicated links are point-to-point links for a specific customer. These links are expensive and used to send priority and delay-sensitive traffic. There are various WAN link connection options, as shown in Figure 14. For Private WAN infrastructure, service providers provide either dedicated point-to-point links, circuit or packet-switched links. These links have their own WAN protocols. WAN protocols are the set of rules which define network communication over WAN links. These WAN protocols work on layer 2 of the OSI model. For dedicated WAN access, the WAN protocols available are T1/E1 and T3/E3, which provide point-to-point connectivity. Switched access includes circuit and packet-switched links. Circuit-switching protocols include Public Switched telephone network (PSTN) and an Integrated service digital network (ISDN). The use of circuit-switching has been shadowed by packet-switching as it provides better performance and transmission rates. X.25 is one of the earliest WAN protocols used to deliver WAN traffic over the WAN links using packet-switching exchanges. After X.25 comes Frame Relay, Asynchronous Transfer Mode (ATM) and Multi-protocol label switching (MPLS) protocols for packet-switched links. Nowadays, MPLS is being used to carry traffic over WAN links, As it provides multiple additional functions than the other packet-switching protocols. For public WAN infrastructure, service providers offer internet access via Broadband services, which uses DSL or cable links. To secure WAN traffic over open internet links, a technique known as tunnelling is used. In a tunnelled connections, the network data and protocol information are encrypted and encapsulated in IP packets and sent to the destination via open internet. When those packets arrive at the destination, it stripes the IP header and decrypts the data, then forwards it for further processing. Virtual private networks are commonly used to tunnel the traffic over the open internet from one site to another. There are many options shown in Figure 14, though only packet-switched and broadband links are used widely than other technologies as only they can meet the current business workload requirements [36] [37] [38] [39].

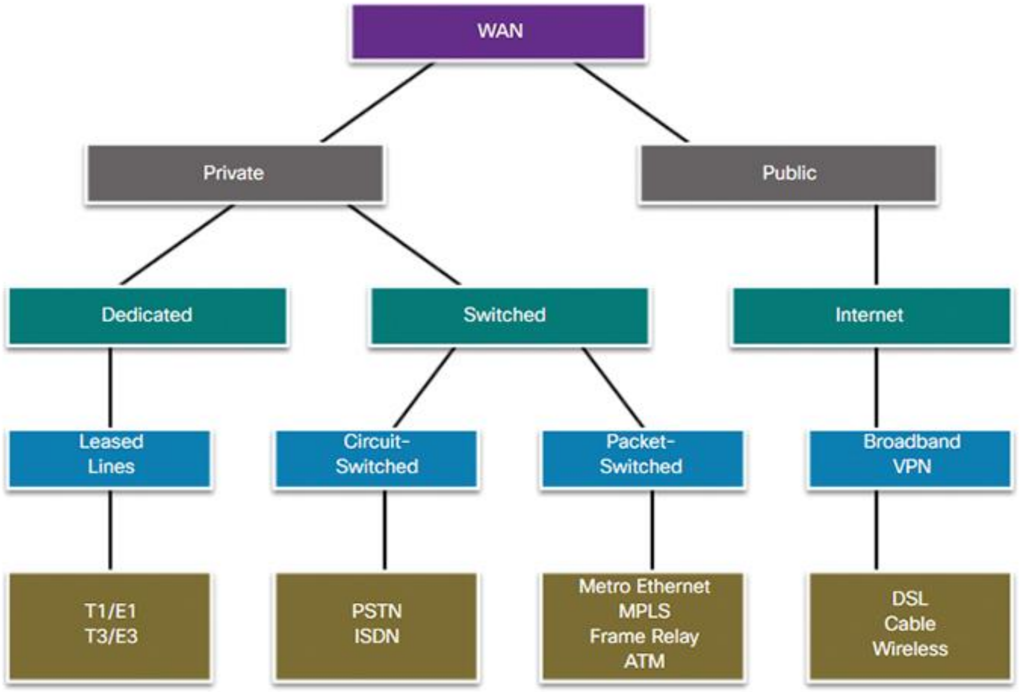


Figure 14: WAN link connection options [38]

3.1 Multi-protocol Label Switching (MPLS)

Multi-protocol label switching is a packet-switching protocol, which uses labels to forward the packets instead of IP addresses. It is a connection-oriented and scalable protocol, which is independent of any packet forwarding technology. It provides functionalities such as quality of service (QoS) and optimization of network resources. MPLS provides an improvement over traditional packet forwarding and mitigates the disadvantages of IP forwarding. It can support a multi-customer environment using Virtual routing and forwarding (VRF), which keep data of different customer isolated from one another. MPLS also provides a functionality known as Any Transport over MPLS (AToM). AToM is based on pseudowires, which carries Layer 2 frames and emulates as a tunnel [40] [41].

In the traditional OSI model, MPLS sits in between layer 2 and layer 3, as layer 2 has protocols like SONET and Ethernet, which encapsulate IP packets into data frames and carry them over point-to-point WAN links. Layer 3 has an Internet protocol that uses its addressing to route packets. MPLS, however, can be summarized as layer 2.5 networking protocol as it exists in between L2 and L3, as shown in Figure 15 [40] [41] [42].

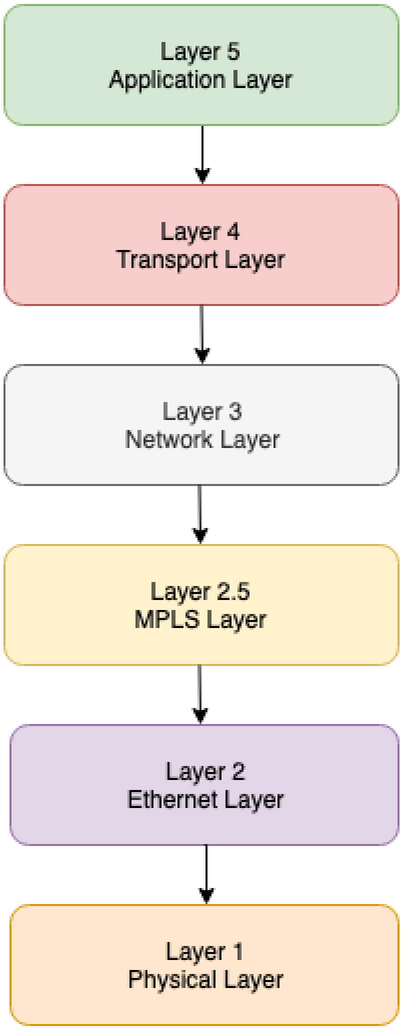


Figure 15: MPLS in OSI model [43]

Packet forwarding in traditional IP networks is done by IP lookup; it is a process of analyzing the IP header of the packet and then look for the next hop in the routing table and forwarding the packet to that next hop. This process is performed at every router from source to destination. In MPLS, When the packet reaches the first MPLS router, it will do the IP lookup to find the destination router instead of the next-hop and then find a pre-determined path to the destination MPLS router. The router then applies a label to the packet based on the pre-determined path. The routers in the path will use that label information to look into the MPLS table and forward the packet until it reaches the destination MPLS router. The destination MPLS router removes the label and delivers the packet via normal IP routing. The router functionality of the intermediate routers is being reduced to switching functionality as the router only analyzes the MPLS header instead of the IP header, which saves time and router resources. [42].

3.1.1 MPLS Architecture

MPLS network is a switched network which consists of multiple Label switching router (LSR), where the path is pre-determined based on the source and destination. These paths are called Label-switched paths. A label switching router (LSR) is a fundamental component of an MPLS network. There are multiple flavours of LSRs like ingress router, egress router, transit router and penultimate router, as shown in Figure 16 [42].

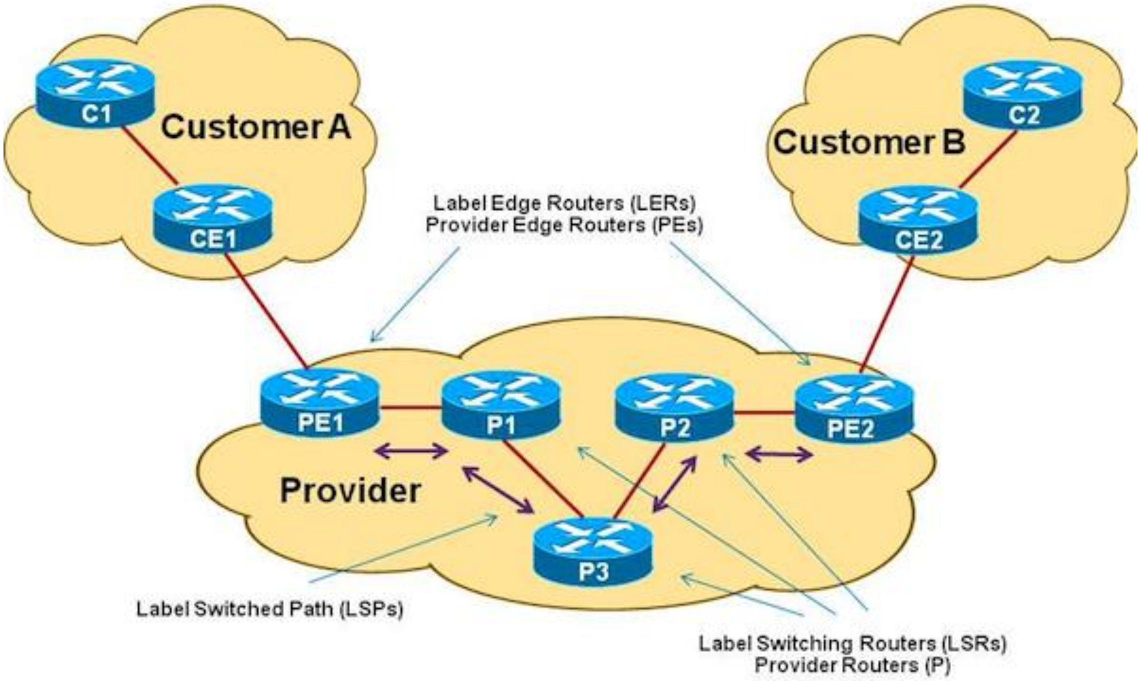

C1
Customer A
CE1
Label Edge Routers (LERs)
Provider Edge Routers (PEs)
Customer B
C2
CE2
PE1
P1
P2
PE2
Provider
P3
Label Switched Path (LSPs)
Label Switching Routers (LSRs)
Provider Routers (P)

Figure 16: MPLS Components [44]

- Label Switched Path (LSP): The label switched path is a path the packet follows through the MPLS network from the Ingress router to the Egress router. MPLS signalling protocols like LDP, BGP or RSVP-TE set up the LSP. Ingress routers prefix Mpls label onto the incoming packet based on the forwarding equivalence class (FEC) and forwards the packet to the next router in the Mpls network; these LSR will swap the label and forward it until it reaches the Egress router, which pops the label off and forwards it based on the layer 3 header. The path followed by the packet is LSP, and these LSPs are unidirectional and point-to-point. Redundancy can be introduced by adding secondary and tertiary LSP in case the primary LSP fails [45] [46].

- Ingress Router: This router is connected with the customer network and is an LSP entry point for any incoming IP packet. It is responsible for encapsulating the IP packet with the MPLS header. After encapsulating the packet, it forwards it to the next-hop router in the LSP. It decides the forward equivalence class (FEC) of the packet and then applies the label on the packets. Ingress router is also known by many other terms such as Edge LSR, Label Edge Router (LER), Provider Edge (PE) [47].
- Transit Router: It is responsible for forwarding packets using labels and swapping of labels. When it receives the packet, it checks the label in the MPLS header and looks for the label switched path (LSP) next-hop label in the MPLS forwarding table, it forwards the packet to the next hop after swapping the old label with the new label. This router, also known as Label switching router (LSR), Core Mpls router, provider router (P) [47].
- Penultimate Router: This router is present adjacent to an Egress router and the second-to-last router in the LSP. As the next-hop to this router is an Egress router in the LSP, there is no need for an MPLS header. So it performs a process known as Penultimate hop popping (PHP), which is removing the MPLS header from the packet before sending it to the Egress router. Hence the router is named as Penultimate router. However, this is an optional option that can be introduced during MPLS implementation and a much-needed function in some cases [47].
- Egress Router: This router is the last router in the LSP as it the exit point of the LSP. The packet comes to this router either with an MPLS header or without it, which depends on whether PHP is enabled in the MPLS network. This router forwards the packet to the next hop via normal IP routing after performing an IP lookup [47].
- MPLS header: MPLS header consists of four fields, as shown in Figure 17. When an MPLS edge router receives a packet, it appends a 32-bit MPLS header to the packet and forwards it to the next router in the MPLS network. This MPLS header resides in between Layer 2 and Layer 3 headers [43].

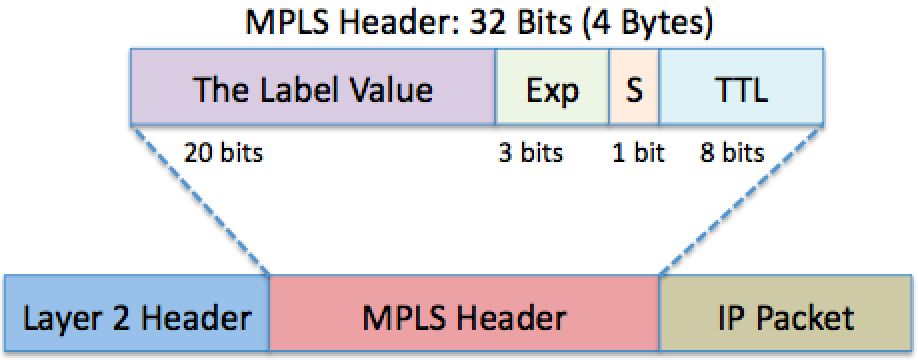


Figure 17: MPLS header [43]

- Label Value: This 20 bits field has the Label value; this value can range from 0 to 1048575. Where 0 to 15 are reserved for by IETF, This label value is stored in the MPLS forwarding table of the Label switched routers [43].
- Experimental: This 3 bits field is used for Quality of service. This field has been renamed to Traffic Class field [43].
- Bottom of the Stack (BoS): This field is set to 1 for the last MPLS header when MPLS headers are stacked over one another [43].
- TTL: This an 8 bits time to live field, just like in the IP header. Its maximum value can 255, and this field is decreased by one at each router [43].

- Label Stacking: Encapsulating an MPLS packet inside another MPLS packet is known as Label stacking. It is called a stack because we are adding an MPLS header on top of an existing MPLS header, and it functions in Last in first out (LIFO) mode. This stack results in nested tunnelling of MPLS packets. When these packets are transported through one hop to another, only the top MPLS header is checked until an egress router pops it off. The bottom of the Stack bit mentioned in the MPLS header section above is used to represent the bottom MPLS header when all the headers are popped off, and only the bottom header is left [48] [49].
- Label Distribution protocols: When a packet enters the MPLS network, it is labelled by the Ingress router and then forwarded to the LSR. The LSR in the MPLS network will swap the labels, and when it reaches the egress router, the label is popped off the packet. For the distribution and management of these labels, label distribution protocols such as LDP and

RSVP-TE are used. Commonly LDP is used for label distribution in MPLS VPN as RSVP-TE is used for MPLS traffic engineering (MPLS TE) [42] [49]:

- Label Distribution Protocol (LDP): The label distribution protocol is defined by IETF and has three primary operations, which are discovering LDP neighbors, forming LDP adjacencies and advertising labels. It discovers and forms an adjacency with LDP neighbors in the MPLS networks and automatically generates locally significant labels. It advertises the labels with its neighbors, which enable the MPLS routers to build and maintain the LSPs. LSPs are built based on the underlying routing information which is obtained by Interior Gateway Protocol (IGP). It creates a local binding for every IP prefix entry in the routing table, which enables the building of two databases label information base (LIB) and label forwarding information base (LFIB). LIB is a part of the control plane which maintains a table of IP prefixes and their local and outgoing labels and is used by LDP to distribute labels. LFIB, a part of the data plane, is created using LIB and used in forwarding labelled packets. LDP uses multicast with IPv4 address 224.0.0.2 and UDP port 646 for LDP neighbor discovery, and for exchanging the labels, it uses TCP unicast with the same port. It also offers MD5 authentication between LDP neighbors. However, LDP needs the Peers to be directly connected, for the peers that are not directly connected, Targeted-LDP (T-LDP) is used. T-LDP uses unicast for LDP neighor discovery instead of multicast LDP [49] [50].
- Resource Reservation Protocol-Traffic Engineering (RSVP-TE): RSVP-TE is an extension of the Resource reservation protocol used for MPLS traffic engineering. As named, it supports resource reservation for applications across the network. RSVP performs two functions; one is that it reserves resources for the application traffic, and another one is label distribution. It signals a path through the TE tunnel from the ingress to the egress router for quality of service purposes. The ingress router then computes the path to the egress using bandwidth and other constraints [49].

3.1.2 MPLS L3VPN

MPLS provides Layer 3 Virtual Private Network service, which provides Layer 3 intersite connectivity between customer sites. This Layer 3 VPN is possible by using MP-BGP and VRFs in an MPLS network [51].

Virtual Routing and Forwarding (VRF) is a technology that allows multiple routing instances on a single router simultaneously. VRF can be applied to a particular interface to tag or mark that traffic. It enables the separation of customer routes and forwarding information using multiple forwarding tables for a specific customer. That provides controlled and private intersite connectivity between customer sites [51].

Multiple protocol Border Gateway Protocol (MP-BGP) is an extension of Border Gateway Protocol. It allows the distribution of various types of address families in parallel. It enables route sharing between the provider edge (PE) routers with special address families. Extended Communities provided by MP-BGP helps in advertising the customer information and VRF properties attached to the routes [51].

3.1.2.1 L3VPN Model

Let's see how L3VPN works by taking a simple example:

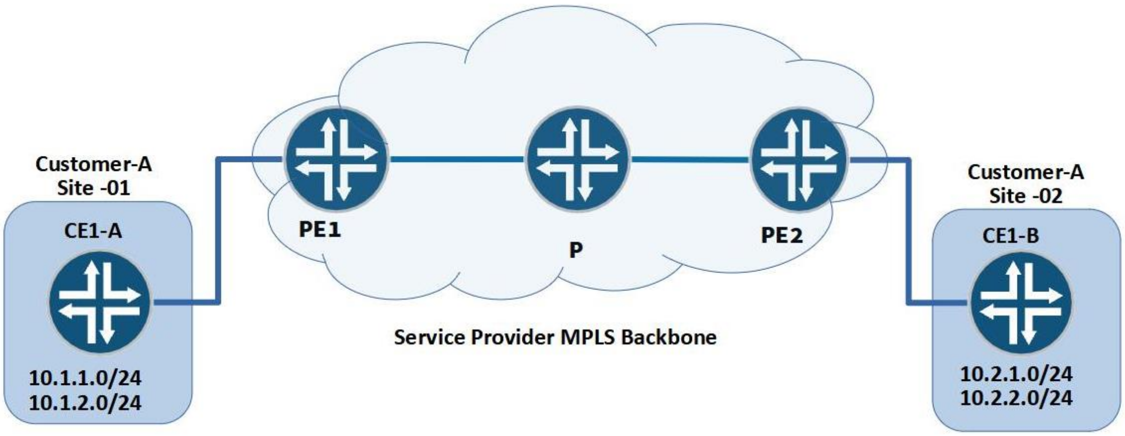


Figure 18: MPLS L3VPN Basic Connectivity

We have customer A who has two sites, SITE-1 and SITE-2. These two sites are connected via a service provider MPLS network. Here we will focus on the MPLS network and the working of L3VPN in the service provider MPLS network instead of focusing on the Customer sites. Let's assume that both customer sites are connected with their respective provider edge (PE) router with some routing protocol, as shown in Figure 18. PE1 here is the provider edge at the service provider side, which can have multiple customers connected to it [51].

If PE1 uses a single routing and forwarding table for all those customers, it could potentially send the traffic from one customer to another. To prevent this, we use Virtual Routing and forwarding (VRF) technology, which enables us to create multiple instances of routing and forwarding tables. We can assign a specific VRF to a particular customer. With which the PE can maintain a separate table for each customer [51].

PE1 and PE2 are MP-BGP neigbhors; PE1 has to advertise these customer routes to PE2. For PE2, there no mechanism to filter and check these routes unless these routes are marked. The advertising PE1 attach an export Route Target (RT) with these routes, now the PE2 on the other side filter these routes based on the marking and advertise them to the customer site. This route-target is an extended community attribute supported by MP-BGP. MP-BGP enables PE1 and PE2 to send this extended community with these advertised routes [51].

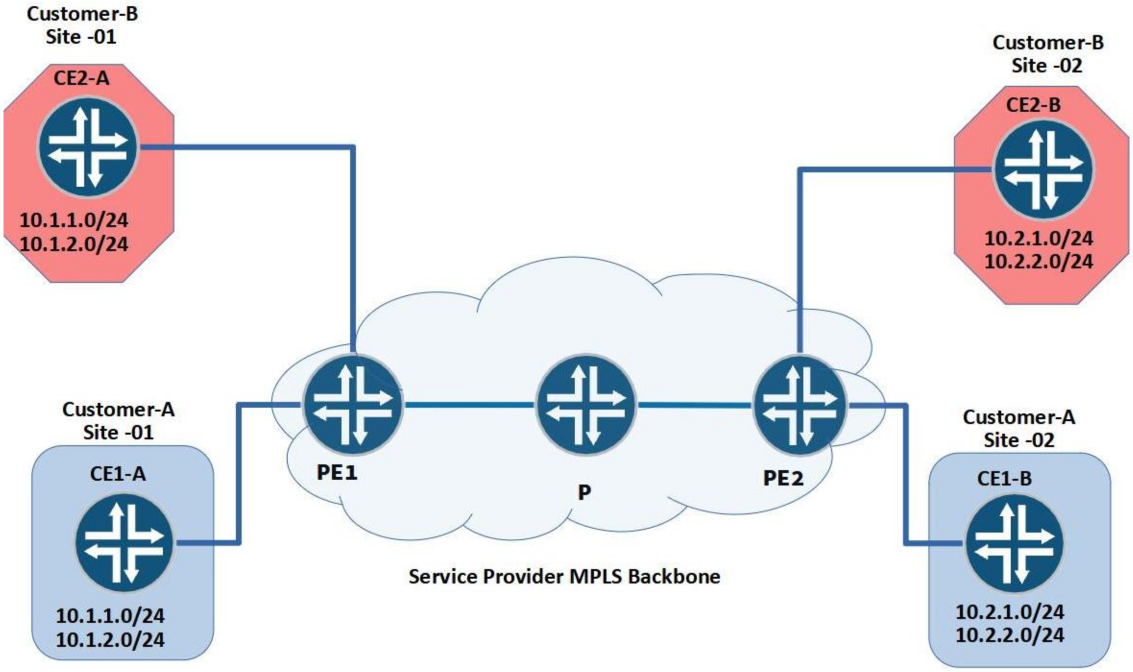
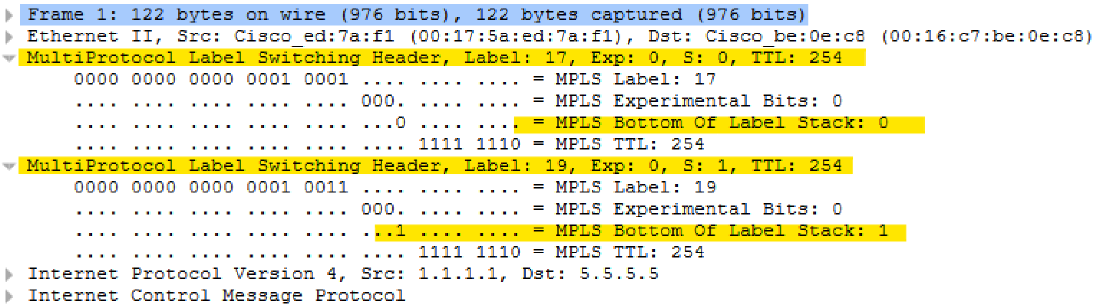


Figure 19: MPLS L3VPN with Multiple Customers

In the same scenario, let's assume that another customer's sites peered up with the PE1 and PE2, with the same IP addressing scheme as Customer-A, as shown in Figure 19. A unique route distinguisher is used to make the IP address unique VPN-IPv4 addresses. Route Distinguisher is a 6-byte value specified in two formats, *as-number:number* or *ip-address:number*. Former uses 2-byte AS number and 4-byte number value while that latter uses 4-byte IP address and 2-byte number value. The IP address can be any IP address of the device within the VPN. MP-BGP supports multiple address families; it helps advertise these VPN-IPv4 addresses from PE1 to PE2 and vice versa. Now that provider edge routers have all the routes from the customers. When the traffic flows from PE1 to PE2 or vice versa, the packet will include two labels; the first one will be the VPN label, which helps the provider edge router in the identification of the next hop for the destination, and the top label will the LSP label to get the traffic through the MPLS network. BGP will distribute these VPN labels as it distributes the VPN-IPv4 routes. These labels can be seen in Figure 20 [51].



```
▸ Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
▸ Ethernet II, Src: Cisco_ed:7a:f1 (00:17:5a:ed:7a:f1), Dst: Cisco_be:0e:c8 (00:16:c7:be:0e:c8)
▾ MultiProtocol Label Switching Header, Label: 17, Exp: 0, S: 0, TTL: 254
      0000 0000 0000 0001 0001 .... .... .... = MPLS Label: 17
      .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
      .... .... .... .... .... ...0 .... .... = MPLS Bottom Of Label Stack: 0
      .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
▾ MultiProtocol Label Switching Header, Label: 19, Exp: 0, S: 1, TTL: 254
      0000 0000 0000 0001 0011 .... .... .... = MPLS Label: 19
      .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
      .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
      .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
▸ Internet Protocol Version 4, Src: 1.1.1.1, Dst: 5.5.5.5
▸ Internet Control Message Protocol
```

Figure 20: MPLS L3VPN Wireshark Capture

3.1.2.2 L3VPN Properties

We have seen an L3VPN model in the previous subsection 3.1.2.1. The properties of L3VPN are as follows:

- Virtual Routing and Forwarding (VRF) is used for separating Customer routing and forwarding tables [51].
- Route-target is used to filter the routes received at the Provider edge routers [51].
- MP-BGP is used in between Provider Edge routers, and it needs to be a full mesh [51].
- Route-distinguisher is used to distinguish between overlapping IP addresses and make them unique VPNv4 addresses [51].

- MP-BGP uses an extended community to share Route-target information and uses the VPNv4 address family to distribute VPNv4 routes [51].
- Provider edge maintains routes only for the customers connected to it [51].
- Provider (Core) routers do not have to maintain any customer routes at all [51].
- The service provider handles the customer routing, and the Customer does not have to care about its routing [51].
- For any new site deployment, the customer only needs to peer the new site's customer-edge router with the provider edge router. No expertise or configuration required from the customer and no changes are required at any other existing network sites [51].
- Provides two types of connectivity models [51]:
    - Any-to-Any
    - Hub and spoke

3.2 Virtual Private Networks

A virtual private network (VPN) is a service that provides an online connection that is secure and encrypted. Using the VPN, we can connect a remote office or a remote worker over a shared public network to an organization's private network. VPN creates an encrypted tunnel for the data to pass through within the public network. VPN provides an alternative to WAN technologies such as leased lines, frame relay and ATM and helps reduce the cost that comes with traditional leased lines. VPN provides confidentiality, integrity, and authentication over an untrusted network like the internet. Confidentiality is provided by using encryption to encrypt the data between two endpoints. Encryption is done using symmetric key encryption, where both endpoints use the same key for encrypting and decrypting the data. Another method is asymmetric key encryption, which also knows public-private key encryption. A pair of the public and the private key is generated, and the public key is being shared between the endpoints. The data is encrypted using the private key and then send to the receiver, where it used the sender’s public key to decrypt the data. Asymmetric encryption, however, makes things complicated and slow. It is not feasible for large data transfer and will bottleneck the performance of the link. Symmetric encryption works faster and better than asymmetric, but the sharing of symmetric keys over the internet in cleartext can cause security issues. That is why in IPsec VPN, asymmetric encryption is used for the creation of tunnels, and a shared secret is generated for data encryption and decryption. The integrity of the data is also ensured in a VPN. Hashing is used for maintaining the integrity of the data. A hash is computed before transferring the date and appended to the data packet. At the receiver, the hash is recomputed with the data and matched against the hash provided in the data packet. If the hash matches, that means the data's integrity has not been compromised. Authentication is provided in VPN by pre-shared keys and digital certificates. These methods are used to confirm the identity of both endpoints. The encryption method, Hashing algorithm and Authentication methods are negotiated at the beginning of the VPN connection for the whole duration of the connection [52].

Remote-access VPN: Remote-access VPN is between a single host and a network access server at the organization's data-center. It enables the user to use the organization's resources from his home internet connection. There are two main components for a remote-access VPN are network access server and VPN client software. A remote-access VPN creates a virtual and temporary tunnel between the host and the organization's private network. This tunnel goes through the public internet, and data sent via this tunnel is secured with encryption and authentication protocols. Some examples of Remote-access VPNs are SSL VPN, SSH VPN and more [53].

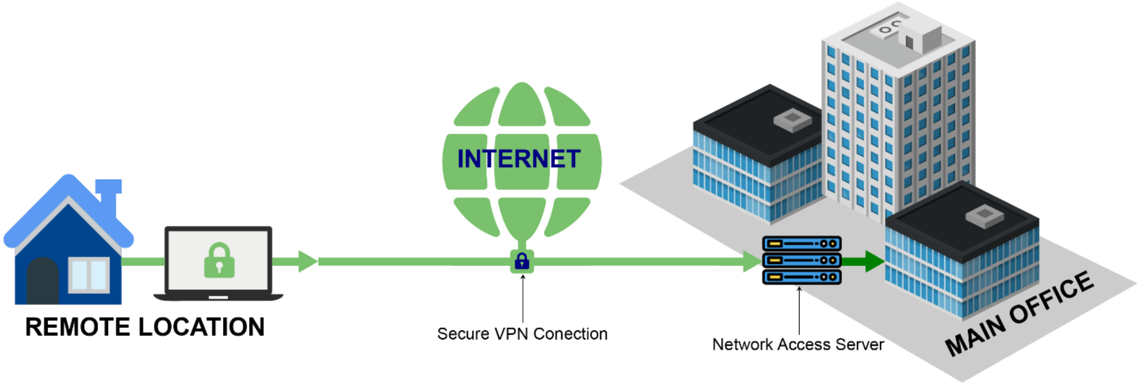


Figure 21: Remote-access VPN [54]

Site-to-site VPN: Site-to-site VPN provides a secured link between two VPN gateways of an organization over the internet. Data shared through this link is encrypted, and this link enables sharing of resources between the sites. Organizations with numerous geographically dispersed locations use site-to-site VPNs to securely connect the sites to the HQ site over the public internet, as shown in Figure 22. These VPNs provide an encrypted tunnel from one site to another, VPN gateways are responsible for encryption and decryption of data going and coming through the tunnel. Example of site-to-site VPN is MPLS L3VPN, IPsec VPN, DMVPN, etc. Site-to-site VPNs are widely used VPNs when it comes to connecting multiple branches of an organization [55].

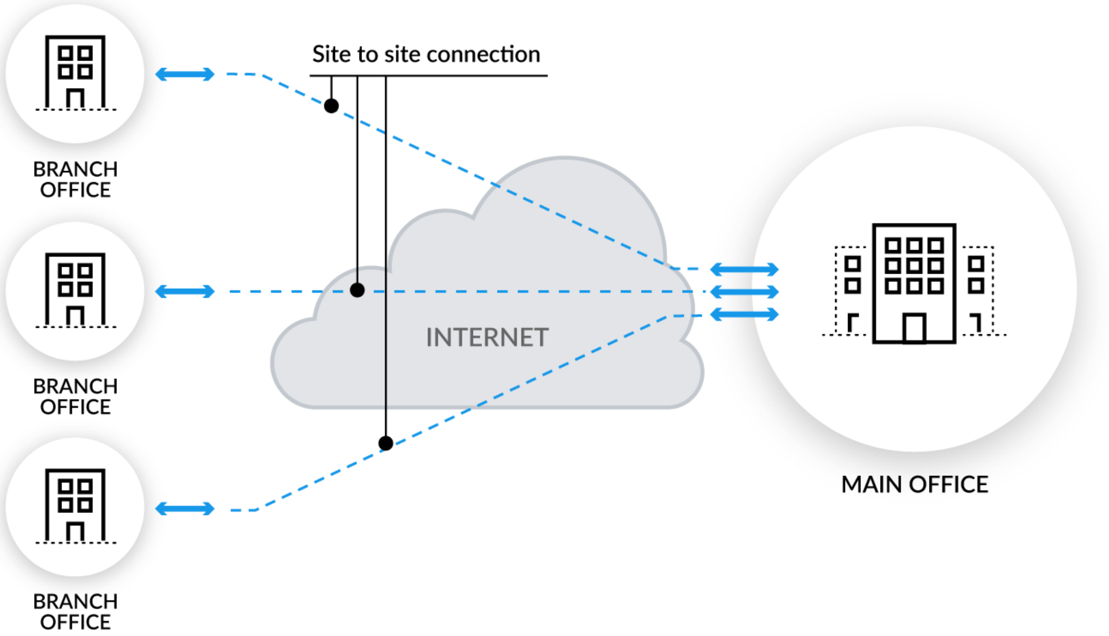


Figure 22: Site-to-site VPN [55]

Benefits of Site-to-site VPN:

- These VPNs can handle mission-critical traffic like VoIP communication as they require low latency and quality of service [56].
- VPN client is not required at the host PC to connect to the VPN. The connection is handled by the VPN gateways at each site [56].
- Encryption/decryption is handled by the VPN gateways instead of the host PC like remote-access VPN [56].

3.3 Use Case

ACME Corp. is an organization with over a few hundred employees and a single location in Edmonton, Alberta. There are few departments in the organization, namely HR, Accounts, IT, Legal and Security. In terms of network infrastructure, they are using a single Layer 2 switch on each floor of the building to connect all the users. In this layer 2 switched network, they use

VLANs on their Layer 2 switches to keep the traffic separated from other departments. VLAN is a great technology to divide a network into multiple networks logically. As the company grows, the number of departments increases and they create more VLANs in their existing network for each newly added department. With this organization's continuous growth, they opened five branch sites, one in Edmonton, one in Calgary and three in Toronto. These sites are also using layer 2 switches for the connectivity and VLANs for the departments.

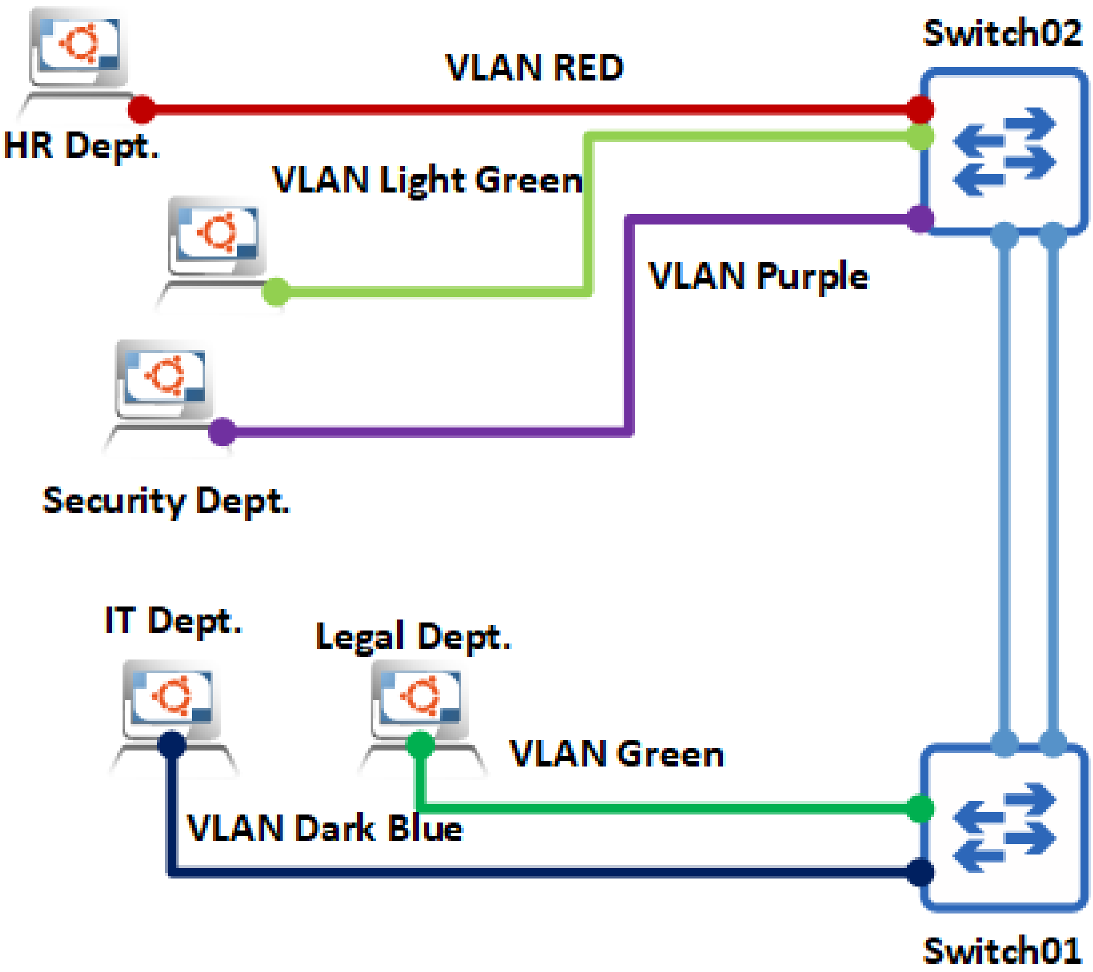


Figure 23: ACME's early single-site network

Now that ACME Corp. has five remote branch sites and one Head Office, it needs to connect these sites to its Head Office. Multiple technologies can be used to provide this connectivity, such as ISDN, Frame Relay and others. These are Layer 2 technologies that use switches to provide connectivity between branch sites of an organization. The service provider providing this connectivity has to provide dedicated VLANs on its service provider switches for each site. If we take this into account, the service provider just consumed five VLANs on its switch. The switch has a limit of 4096 VLANs only and keeping in mind that the service provider is also serving multiple customers, this method does not scale well. Switches' limitation limits this solution. Though the service provider can install other switches in its network, it will increase the capital expenses.

ACME Corp. now has a data-center at its head office with some hosted applications and servers. The organization has moved to the Layer 3 network instead of layer 2. Older connectivity provided by the service provider might work, but it is not scalable. Then comes MPLS and its L3VPN; it requires a Customer edge router at ACME Corp. head office and remote sites. Assuming that the service provider has a provider edge (PE) router near all ACME remote sites and head office locations. The service provider now provides L3VPN as a service to provide connectivity of all remote locations to the head office of ACME Corp. All the remote sites are now connected to the head office location, and the head office is sharing the routes with every remote location. This solution uses Layer 3 connectivity, every remote location can use private IP addresses, and those IP addresses and routes will be shared with corresponding locations. By that remote location can access the servers and applications hosted at the head office data-center.

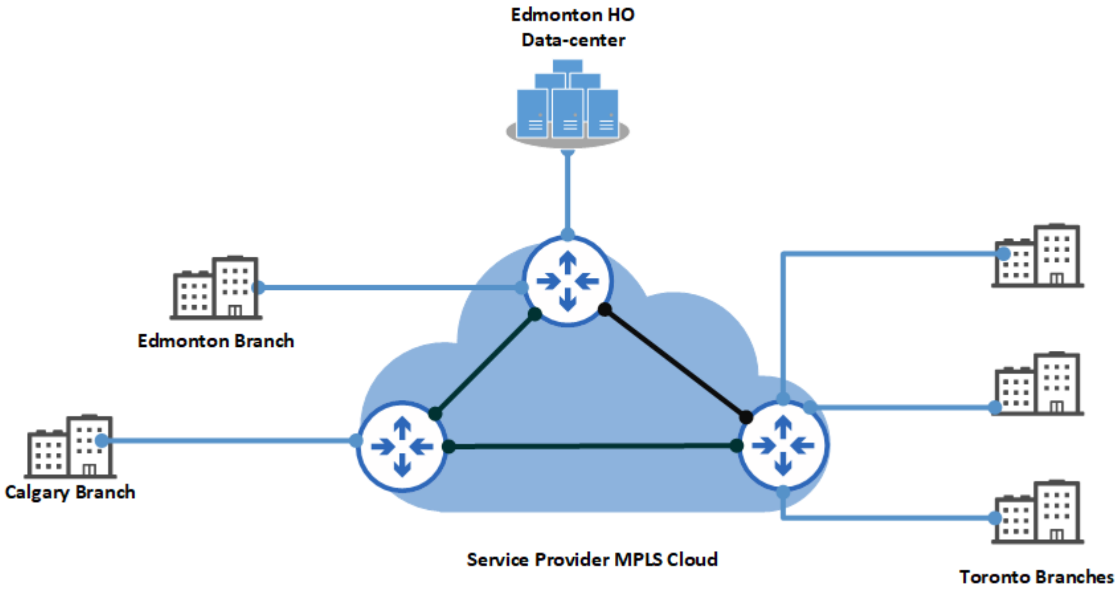


Figure 24: ACME MPLS Connectivity with branch sites

Assuming that the service provider provides the same service to other customers, the Provider Edge routers will separate the customers' traffic by using VRFs, and MP-BGP protocols were discussed in subsection 3.1.2.1. Some benefits of this approach are as follows:

- It provides support for overlapping private addresses used by customers at their locations.
- New site deployment requires configuration and peering to that site’s Customer Edge only.
- The service provider handles the routing for the customer. No routing expertise is required at the customer end.
- This solution is easy to scale with the customer and the service provider perspective.

We have discussed the benefits of this approach. Let us see how it adapts to new changes at the customer end. ACME Corp. is a growing organization with a few international remote locations in Europe and Asia. In this case, If the service provider ACME is using for its domestic network connection is available near the remote international location, then it is pretty easy to peer that remote location to the PE at the service provider end. However, that is not the case all time as a country’s geography binds the service provider's operations, and they might not have a presence internationally.

One of the solutions, in this case, is that the service provider goes into an agreement with an international service provider to provide service to a specific international location, which will provide an expensive dedicated link. And in turn, it will increase the capital and operational expenses of ACME Corp.

Another solution is to have an internet connection at both locations and use a Virtual private network to connect that international remote location to the head office, ensuring data integrity and authentication. Using this approach, ACME Corp. can now provide remote access to its employees.

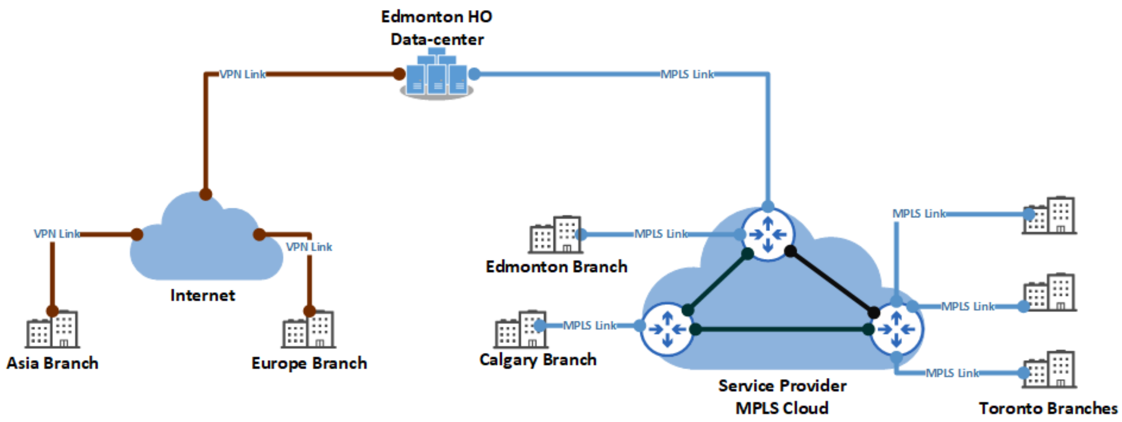


Figure 25: ACME's MPLS and VPN connectivity with remote branch sites

The current position of ACME Corp. is shown in Figure 25 and as follows:

- ACME Corp. using MPLS L3VPN to connect to its five domestic remote locations to the head office.
- ACME Corp. has two international sites in Europe and Asia; It uses a Virtual private network to connect them to the head office.
- ACME Corp. now provides remote access to its employees.
- All ACME Corp. remote sites are using the Head office's internet connection for their internet connectivity.
- With the continuous growth of cloud services, ACME Corp has started using cloud applications and shifted some of its non-critical applications to the cloud.

Network challenges ACME Corp. facing with the continuous growth are as follows:

- ACME does not have complete control of its IP routing, as the service provider is handling it.
- ACME is using a Hub and Spoke model. This means remotes sites have to go through the head office to communicate with any other remote site called backhauling of traffic, which is an inefficient use of the links and puts an unnecessary load on the links.
- Similar backhauling is experienced when remote sites use cloud applications; the traffic goes to the head office and then go through the middleboxes then to the cloud.
- Lack of quality of service of critical application traffic such as voice and video.
- Existing MPLS infrastructure is incapable of integrating with cloud services.

- Expensive and time-consuming new site deployments take around a few weeks to deploy a new MPLS connection for a remote site.

These are the limitation faced by ACME Corp. with legacy WAN technologies; we will continue this case study with a new solution named Software-defined Wide area network (SD-WAN). We will see how it provides solutions to ACME Corp's challenges, facing legacy WAN technologies and the new challenges this new approach introduces.

4 Software-defined Based WAN

As the name suggests, software-defined WAN is a Wide Area Network that leverages the principle of Software-defined Networking to simplify traditional Wide Area Network operations. Traditional WAN is a hardware-centric network, while Software-defined WAN like SDN is an Intent-based network. SD-WAN is abstracted from the underlying hardware network and enables a secure virtualized overlay independent of the underlying network. This overlay and abstraction enable SD-WAN to carry the application traffic independent of the physical network. That means SD-WAN can work over multiple links no matter if they are MPLS, LTE or Broadband internet [57] [58].

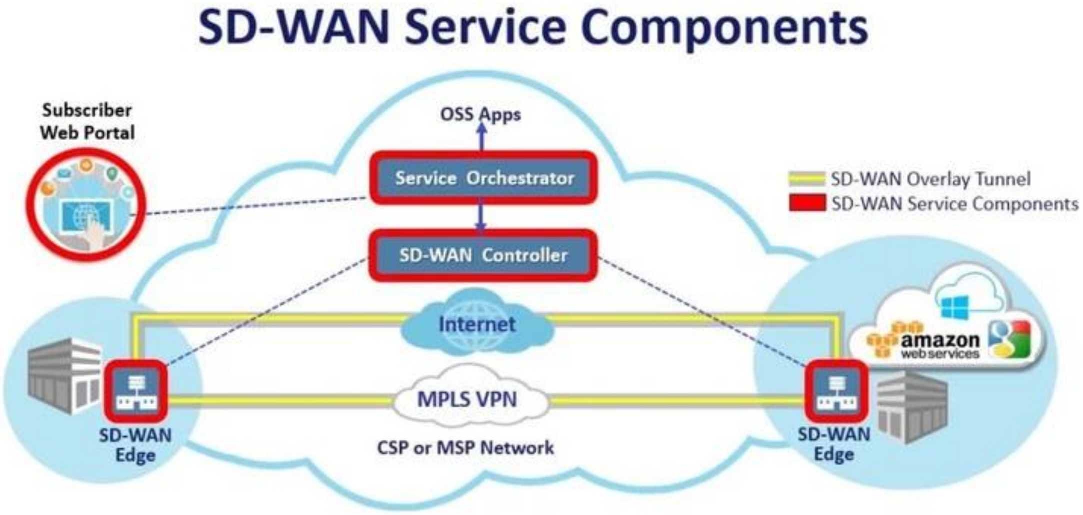


Figure 26: SD-WAN Service Components [57]

As it uses the SDN principle of decoupling the control and data plane, it has a similar structure as a software-defined network, which consists of an SD-WAN edge, SD-WAN orchestrator, and SD-WAN controller as seen in Figure 26. These components are connected in the network and provide a virtual and simple network overlay. SD-WAN edge is a network function present at the network endpoint or the branch sites, a virtual application, or a physical device. The SD-WAN Controller is a logically centralized control unit that provides a management interface to control the network, where policies are created. SD-WAN orchestrator is a virtualized brain of the network that manages the network and executes the Controller's policies. As businesses and enterprises are moving applications to the cloud, and usage of SaaS is increasing, traditional WAN technologies are having a hard time providing a better cloud application performance and user experience. SD-WAN provides a solution to this challenge, as it is designed to support cloud applications and provide better cloud application performance and user experience. As shown in Figure 26, SD-WAN is working over the internet and MPLS links. It one of the characteristics of SD-WAN to work with multiple links. This characteristic plays an important role in application performance optimization as all the cloud services can be reached through the internet links instead of backhauling to the data center via MPLS links. This not only improves cloud application performance but also provides efficient utilization of given links [57].

SD-WAN uses commercial off-the-shelf devices in terms of physical infrastructure, which are also called white-boxes. These white-boxes simplify network management as they are not vendor-specific and can host a variety of network functions. These functions can be routing, switching, firewall, IPS, IDS, DNS, among other network functions. This use of network functions and white boxes significantly reduces the network's complexity makes it more flexible and agile [57] [58].

4.1 SD-WAN Architecture

Traditional WAN relies on private and expensive MPLS links; however, with SD-WAN, we have flexibility in terms of types of links we can use. As the organizations are adopting cloud services, they expect a quality user experience and good application performance. Traditional WAN is struggling to provide better application performance and user experience. The main reason for this problem is that it is dependent on the private and expensive MPLS links and backhauls all the internet traffic from the remote branch sites to the central data center for processing and then send it to the cloud providers. All the traffic from the branch sites is required to go through the centralized services. Branch sites rely on the central data center for their internet connectivity as sometimes their existing internet links are unreliable. This backhauling is the most inefficient use of the MPLS links and can lead to increased latency and degraded links. Here comes SD-WAN in the picture; its ability to work with heterogeneous networks is a significant advantage over traditional WAN. It can utilize the links provided at the remote branch sites efficiently, and in some cases, it can even replace the existing private WAN links. Using SD-WAN services, we can send the cloud application traffic directly to the cloud service providers via the internet links at the branch site instead of going through the central data center. However, there is a certain type of traffic that needs to be backhauled to the data center, such as E-mail traffic and other critical application traffic. SD-WAN does all this by using business policies, as it prioritizes the traffic based on the policies defined. SD-WAN provides three types of SD-WAN architecture that can be used by the organizations to implement SD-WAN services into their network [58]:

4.1.1 On-premises SD-WAN

On-premises SD-WAN architecture is where SD-WAN edge device is present at the remote branch sites, and the centralized orchestrator is present at the central data center. These SD-WAN edges can be a physical device or virtual software hosted on commercial off-the-shelf hardware. In this architecture, SD-WAN's purpose is to augment the existing private network, and by using SD-WAN, we can increase the bandwidth, efficiently use the WAN links, and optimize the overall network performance. These SD-WAN edge devices present at the branch sites use the instructions provided by the orchestrator hosted at the central data center. These devices use MPLS for their connectivity instead of any cloud gateway. This architecture is best suited for the organization which hosts their application instead of using cloud application [57] [59].

Benefits [59]:

1. Load-balancing of ISP and MPLS links.
2. Improved WAN applications performance and real-time traffic shaping.
3. Automatic failover and improved disaster recovery via alternate links.

4.1.2 Cloud-enabled SD-WAN

In cloud-enabled SD-WAN architecture, SD-WAN edges are hosted at the premises but are connected to the cloud gateway via an internet connection. The cloud gateway has a direct connection to some major cloud providers, which increases the overall cloud application performance and user experience. This approach is getting the benefits of the on-premises in addition to cloud application performance. In this architecture, if the branch has multiple Internet and MPLS links, SD-WAN makes efficient use of those networks and provides automatic failover, which can immediately switch links if the existing link is facing any problems without any interruption to users [57] [59].

Benefits [59]:

1. Improved performance of cloud applications via the cloud gateways.
2. The reliability of the cloud application improved because of cloud gateways.
3. Load balancing between provided links.
4. Improved WAN applications performance and real-time traffic shaping.
5. Automatic failover and improved disaster recovery via alternate links.

4.1.3 Cloud-enabled with Backbone SD-WAN

This architecture is the same as the cloud-enabled SD-WAN, but it has a backbone provided by the SD-WAN service provider. In this, the SD-WAN edge is hosted on the branch as usual, but it connects to the nearest SD-WAN service provider's Point of presence (POP), which ensures low latency, packet loss, jitter, and high reliability through the service provider's private network backbone. This backbone is directly connected to the major cloud application providers as well. This backbone not only improves the performance of the cloud application but also improves the performance of the real-time traffic [57] [59].

Benefits [59]:

1. Private backbone improves the overall performance of the network and real-time applications.
2. Improved performance of cloud applications via the cloud gateways.
3. The reliability of the cloud application improved because of cloud gateways.
4. Load balancing between provided links.
5. Improved WAN applications performance and real-time traffic shaping.
6. Automatic failover and improved disaster recovery via alternate links.

4.2 SD-WAN Features

- **Virtualization of Network:** As we all know, Software-defined WAN is abstracted from the network hardware and operates on its virtual network overlay with its components. The virtual network is independent of the underlying hardware network and making it much more flexible. It enables SD-WAN to utilize multiple links between a branch and data center or SaaS service provider despite their types, i.e., MPLS links, LTE, Broadband. In a traditional scenario, Branches backhaul their entire traffic regardless of nature to the data center, which results in increased latency, congestion in the link and poor application performance. With SD-WAN, which can use multiple links at the branch and the DC, it prioritizes the traffic and utilizes all the available links. It can use the MPLS for critical traffic destined to the data center and can use LTE or Broadband for application traffic destined for the cloud provider, using application traffic segmentation. It uses the links smartly, and when it senses that the link's performance is degrading, it switches over to the other available links. It also makes installing new links also easier due to the abstraction of software and hardware [58].

- **Service Delivery Simplification:** SD-WAN simplifies the service delivery with its architecture and abstraction by the use of Network Function Virtualization. SD-WAN used commercial off-the-shelf devices; these white-boxes can host many network functions. The Traditional WAN model uses middleboxes whenever a new service was needed. Installation and placement of these middleboxes are critical and makes the network more complex. These installations are prone to mistakes and failures. SD-WAN simplifies it and makes it easier to install any needed network function that can reside either on the Customer premises equipment or the cloud. This method of service delivery takes much less time than the traditional one [58].
- **Interoperability:** SD-WAN provides interoperability, which means it can work and co-exist with the existing network infrastructure. SD-WAN can be deployed in existing network infrastructure and can interoperate using the available application programming interface. The abstraction in SD-WAN enables this interoperability as it separates the control plane and the data plane [58].
- **Vendor Neutral Hardware:** SD-WAN enables the use of Vendor-neutral and cost-effective hardware. It is the result of control and data plane decoupling, which allows the use of standard hardware for the data plane. For the control plane, Network functions can be delivered remotely via the cloud or can be hosted on commercial and cost-effective off-the-shelf hardware. This provides cost-effective advantage to SD-WAN over traditional WAN [58].
- **Monitoring:** SD-WAN enables monitoring of the whole network, including remote sites and service providers, that provides overall visibility of the network and its performance.

This performance monitoring and the Controller's policies enable smart decisions about the application traffic and resources available [58].

- **Zero-touch deployment:** Zero-touch deployment means that the devices provided by the vendor are plug n play (PnP) devices. This essentially means that enterprises and businesses do not have to worry about the cost of a specialized IT person at every branch they provision. A person with no IT skill can deploy these PnP SD-WAN edge devices at the branch by just plugging the power and the network cable. Usually, in traditional WAN, a specialized IT person needs to visit the branch site to provision any WAN service, which includes installation and configuring the device with the initial setup. But with SD-WAN devices, there is no need for all that hassle [60].
- **Automation:** Automation is basically automating the required process. In SD-WAN, there are two types of automation that are required, one is at the customer level, and another one is at the service provider level. So, for the customer level, automation means managing the life cycle of deployed devices and services. This includes installation, configuration, upgrading, operations, and monitoring; all these processes are automated in SD-WAN. For example, if a new device is deployed at a branch site, to configure that device network administrator only needs a prebuilt template in the dashboard and then assign it to the branch via a click. That will assign the required business policies and configuration to the branch device [60].

  From the perspective of a service provider, automation means having REST APIs in the orchestrator. These REST APIs will help in managing the business policy framework of each customer via the service provider orchestrator, which makes installing, configuring, operating, and managing a customer's WAN via the software dashboard [60].

- **Cloud usage enablement:** SD-WAN is cloud-enabled, as it supports and optimizes cloud application performance. It does it by leveraging the benefit of having multiple links on a branch site and uses the internet link to transfer the cloud application traffic to its cloud SD-WAN gateway. As we know, many service providers provide a cloud gateway that is connected to major SaaS service providers. Traditional WAN lacks this feature, though it can be configured to enable cloud usage, which will raise the cost to the point, that it is not feasible and efficient to do that; on the other hand, SD-WAN provides this service at a much lower cost.

- **Deployment models:** As we discussed in the last section about the SD-WAN architecture, SD-WAN provides us with three types of basic deployment methods. These deployment methods provide a level of flexibility to the customers. Each of these methods has its own benefits, and the customer can leverage these benefits based on their business requirement. For example, for customers who have no cloud usage and security of the data is paramount, premises only SD-WAN will work perfectly in that case. However, if the customer uses the SaaS service providers and has sensitive data as well, cloud-enabled with backbone SD-WAN is the best choice, which will not only optimize cloud traffic but also provide security by sending the sensitive data via the MPLS link and keep that link free from the cloud traffic by reducing the cloud traffic backhauling to the data center unless absolutely needed [60].
- **Business level policy orchestration:** In traditional WAN, the network administrator will configure each box at a time. However, SD-WAN enables him to create a template with the rules and policies that are required, for example, routing, quality of service, firewall, and so on. That template can be valid for many sites, which he can configure with a single click. For example, for enabling quality of service, he just needs to click a checkbox that "enable quality of service". When it comes to business policies, the first thing we need to know about these that they are context-driven, these policies do not need to go at a packet level, and they have high-level constructs. For example, setting the priority of any application traffic from low to high, it can be done with a click. After those, high-level constructs will handle packet-level implementation [60].
- **Multi-tenancy with operational support:** SD-WAN provides multi-tenancy, which is a key element in managed SD-WAN for service providers. Multi-tenants for customers means that they are using application segmentation to ensure a secure environment. However, for service providers, it means how it manages multiple customers from a single orchestrator and while managing the customers, it provides them with their own Wide area network instance [60].
- **Traditional protocol support:** SD-WAN provides interoperability with traditional hardware networks. Enterprises that have a traditional WAN network can install an SD-

WAN environment, which can support the languages and traditional protocols. It will be able to integrate with the third-party hardware, even though it can be proprietary itself, as it provides easy implementation and migration from the traditional WAN instead of fully replacing and ripping all of it. The benefit of this feature is that the enterprise can ease in with the SD-WAN usage and slowly move to replace its traditional Infrastructure [60].

- **AI-enhanced troubleshooting:** Artificial intelligence (AI) plays an important role in SD-WAN. As we know, troubleshooting network issues can be a tedious task that takes a significant amount of time and technically skilled labor. Human errors are the reasons for most unplanned network downtime. Though automation does eliminate human errors, it cannot completely eradicate them as a human can make errors while doing the automation. Usage of AI in SD-WAN provides a proactive solution to this networking challenge and removes human error completely. AI learns from the network behaviors, rules and policies and can make decisions based on these rules, policies and network behaviors. An AI-powered network can help to reach the network to its full potential and efficient use. It monitors the network and can detect the smallest of the problem before it impacts the business. SD-WAN is there to provide centralized management in the network; however, AI has fault prediction which enables the network administrators to anticipate problems. These networks that are AI-driven also known as smart networks, can analyze how the network, application performance and security are being impacted by certain events. Using that information, they provide intelligent recommendations and decisions, which can be adapted must faster than humans and improves the overall network performance. These smart networks save the cost and the time which we spend doing troubleshooting manually [61].
- **Security:** Network administrators with SD-WAN can centrally manage and orchestrate the elements into the network; Security is one of them. SD-WAN provides better security than traditional WAN. SD-WAN virtualizes the security functions like other functions, So, when the time comes for updating or upgrading, the network administrator just needs to update or install the software instead of installed a new device in the network. SD-WAN uses IPsec-based VPNs universally, as SD-WAN has to use the internet in addition to private MPLS links. VPN is a key element for SD-WAN security and is the least requirement to secure the traffic over the public internet. It provides visibility to the

network administrator, which traditional WAN does not provide. The network administrator can monitor the network and ensure the security elements and policies if they are running correctly. SD-WAN makes segmentation of application traffic possible; this segmentation is based on the application traffic characteristics and network policies. We know SD-WAN creates virtualized network overlays; segmentation leverage that functionality and creates its virtual network in the virtualized network overlay. By doing that, separates the different application traffic and makes the network much more granular. Micro-segmentation is another approach that can segregate the traffic based on the workload, which helps in segregating sensitive traffic from the regular traffic. Another key element of SD-WAN security is the next-generation firewall. This is a virtual firewall that performs deep packet inspection; it has multiple VNFs running in it, such as application awareness, intrusion detection and prevention, antivirus and many more. SD-WAN can place security functions wherever they are needed for the application. Network function virtualization made this feature possible, among others. Service chaining of security functions is used to build multiple security levels, for example, using multiple security functions such as firewall, IDS, anti-malware and IPS [60] [62].

4.3 SD-WAN Solutions

Many SD-WAN vendors provide SD-WAN solutions and products. Every vendor provides products with its own set of solutions and tools. Gartner, a research organization, publishes a yearly report named “Magic quadrant for WAN edge infrastructure.” It provides a detailed analysis and review of the various vendors in the WAN-Edge market. Figure 27 shows us the magic quadrant graph for WAN-edge infrastructure released by Gartner in September 2020 [63].

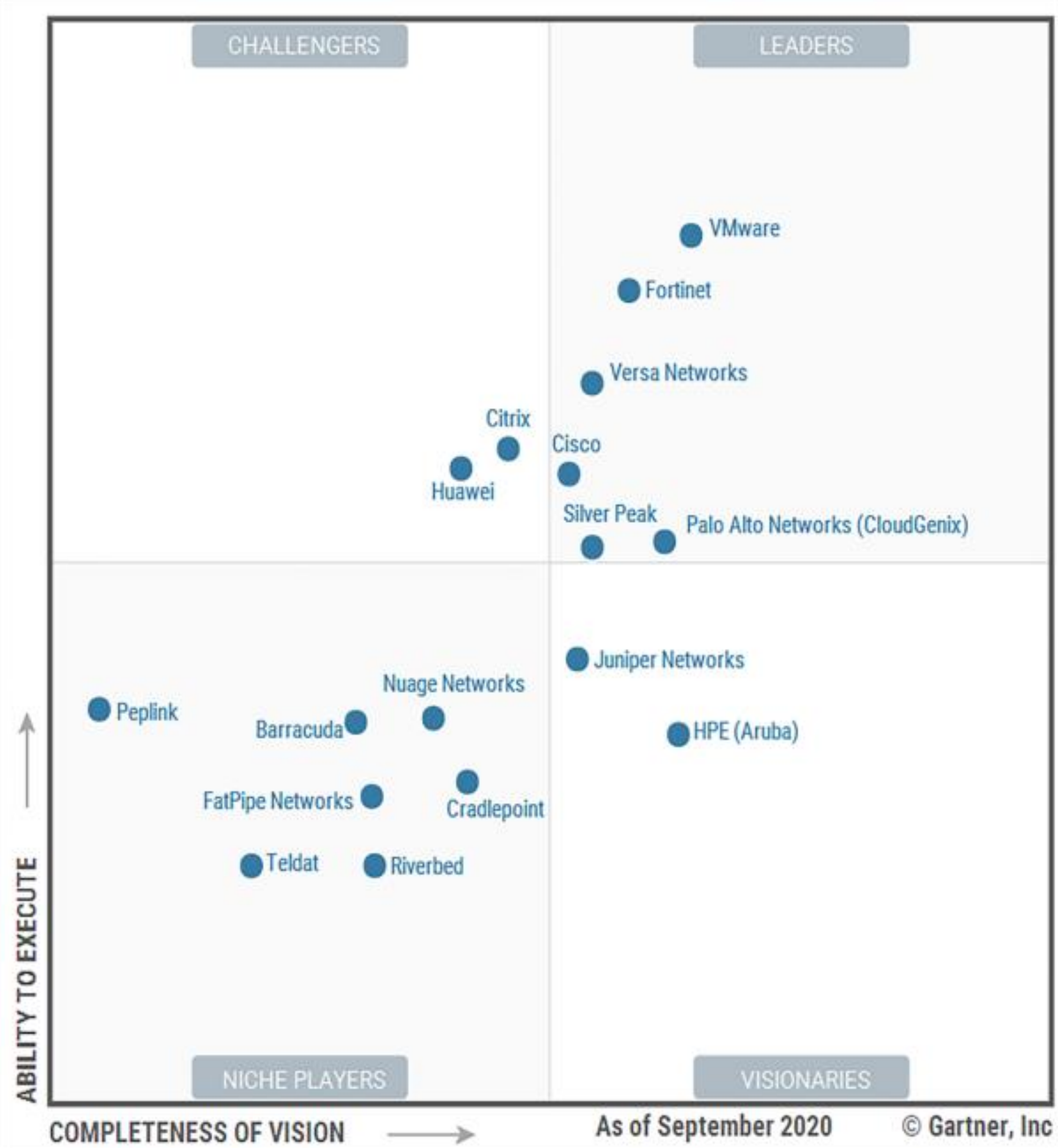


Figure 27: Magic quadrant for WAN-Edge infrastructure (2020) [63]

Gartner divides its magic quadrant graph into four quadrants, namely leaders, visionaries, challengers, and niche players. These quadrants are based on two things, the ability to execute and the completeness of vision. As shown in Figure 27, vendors such as Silverpeak, Cisco, Fortinet, Versa Networks and Palo Alto networks (Cloudgenix) are the leaders in the field of SD-WAN solutions. There are other vendors such as Juniper Networks and HPE (Aruba), which are visionaries, Citrix and Huawei, which are the challengers in the field and other vendors such as Barracuda, Riverbed, and others are niche players in the SD-WAN solutions field [63].

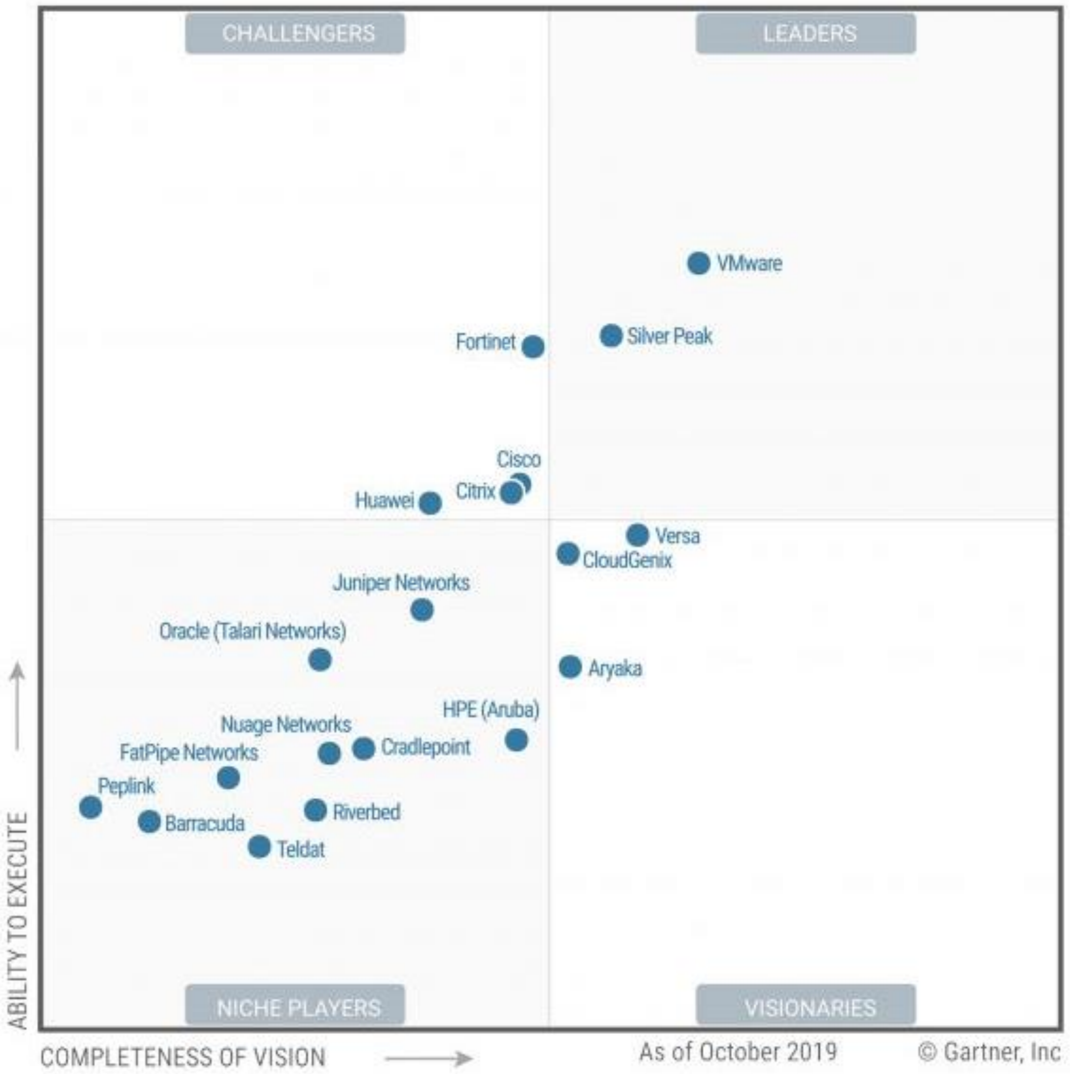
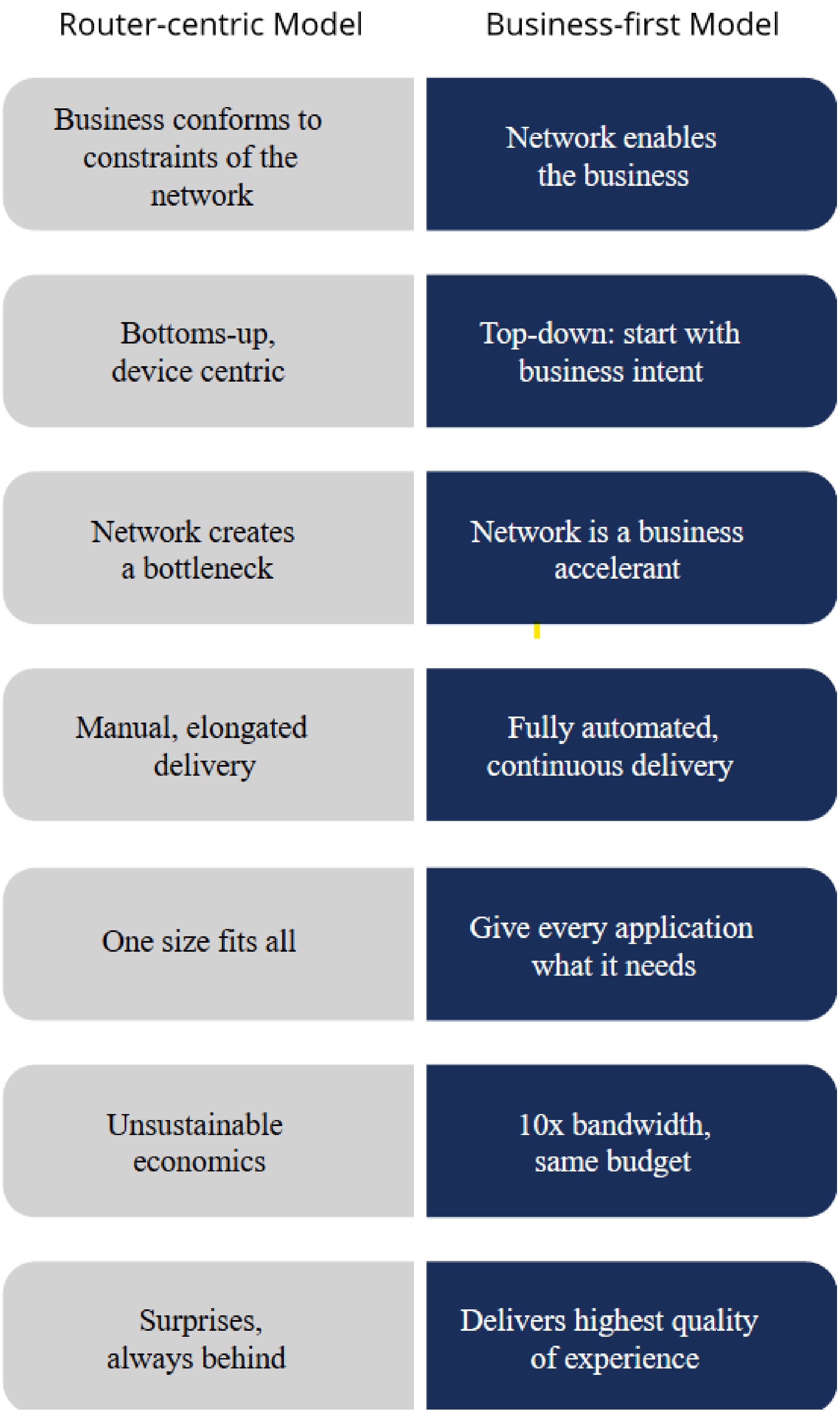


Figure 28: Magic quadrant for WAN-Edge infrastructure (2019) [64]

If we compare the magic quadrant released by Gartner in 2020 to the one published in 2019, we can see a striking difference, as there were two leaders in 2019 and 2020, there four as Cisco and Fortinet are no longer the challengers [63].

4.3.1 Silver Peak SD-WAN solution

Silver Peak is a leader for the last two years in Gartner's magic quadrant. It ranked third in the market in the first quarter of 2020 by a research firm Dell'Oro. It follows a business-first approach instead of the old router-centric approach; the difference is shown in Figure 29 [65] [66].



Router-centric Model	Business-first Model
Business conforms to constraints of the network	Network enables the business
Bottoms-up, device centric	Top-down: start with business intent
Network creates a bottleneck	Network is a business accelerant
Manual, elongated delivery	Fully automated, continuous delivery
One size fits all	Give every application what it needs
Unsustainable economics	10x bandwidth, same budget
Surprises, always behind	Delivers highest quality of experience

Figure 29: Router-centric vs business-first model [66]

The router-centric model follows a bottom-up approach where applications and businesses conform to network-imposed constraints. However, the business-first model follows a top-down approach, as shown in Figure 29. Business' intent directs the network operations instead of the other way around in this business-first approach. Benefits of the Business-first approach are [66]:

Lifecycle Orchestration and Automation: It provides full lifecycle management and orchestration of the WAN function. A change can be implemented centrally in the WAN based on business requirements. The time required for the change implementation has been drastically reduced [66].

Self-learning: Self-learning is essential in providing optimal application performance and experience. The continuous monitoring of the network enables self-learning of the network states. Which helps in delivering optimal application performance. The network detects and remediates network congestion and impairments to do so [66].

Consistent QoS: SD-WAN enables the use of multiple kinds of transport, be it MPLS, LTE or broadband. Monitoring and managing transport services intelligently gives the ability to overcomes common network problems like jitter, packet loss, and latency. This helps in delivering a high level of quality of service in case of any transport service impairment [66].

Silver Peak SD-WAN product is Unity EdgeConnect SD-WAN solution. Unity EdgeConnect SD-WAN solution consists of Unity EdgeConnect appliance, Unity Orchestrator and an optional WAN optimization solution named Unity Boost. These devices, as shown in Figure 30, help to achieve a business-first networking model with the focus on SaaS applications and IaaS data centers, which are crucial business tools. Each Unity EdgeConnect device in Figure 30 shows us a branch site of the organization [63] [65] [67].

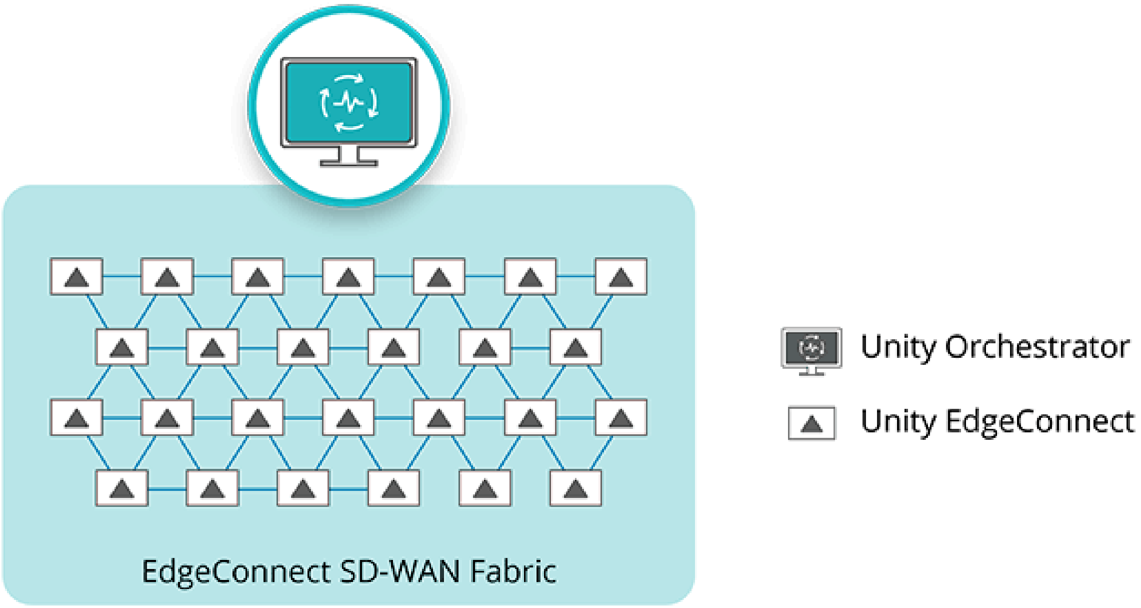


Figure 30: Silver Peak SD-WAN Solution Components [68]

Unity Edge appliances: The appliances are installed at the remote branches, can either be a physical device or a virtual one. They help customers to move over a broadband WAN by providing secure and virtual network overlay. There are plenty of features these appliances provide; these features are as follows [65] [67]:

- It follows a plug n play deployment model, which enables it to be deployed at any branch site in a matter of seconds. It can automatically connect itself with other instances of Silver Peak devices at the data center and the cloud [67].
- It provides virtual network overlays, which can be defined and abstracted from the underlying transport services, which enables quality of service, failover characteristics and many other features for every different network overlay. Based on the business intent, these different overlays can be mapped with different applications [67].
- Forward error correction and packet order correction are the function which EdgeConnect devices provide for better resiliency over broadband links. There are measures called ultra-resilient packet delivery, which make use of multiple links available at the site. This is done by using parity packets which can rebuild the packets lost in the transmission [69].
- Per-packet load balancing is another feature provided by EdgeConnect appliances. This is accomplished by sending a number of packets over multiple links, and then the order is corrected at the destination EdgeConnect appliance and maximizing data transfer [69].

- When we have more than one physical transport service available like MPLS, Broadband or LTE, in case of a link failure, application interruption can be eliminated as other links are there to transport the traffic and switch over between the links is automatic [67].
- It provides a security feature called WAN hardening, which provides encrypted tunnels from one edge to the other. It uses 256 AES encryption to encrypt these tunnels, hence securing all the SD-WAN traffic [67].
- It provides a zone-based firewall, where end-to-end secure zones can be created based on application groups, user groups or virtual overlays; these zones can be managed and orchestrated centrally [67].
- A proprietary service called First-packet iQ application classification is provided by this appliance. It identifies the application based on the first packet in the transmission and then sent the trusted traffic to the internet and unknown traffic to the data center security devices [67].
- Simplified service chaining with a friendly user interface is provided by this appliance, which enables automation and accelerated integration between different security services [67].

Unity Orchestrator: Unity orchestrator provides visibility over legacy and cloud applications. It offers control over the Unity EdgeConnect appliances installed at remote branches and secures the SD-WAN traffic with its business intent policies. It is a virtual machine that can be hosted on hardware or hosted as a service in the Silver Peak cloud. Below the features provided by Unity Orchestrator [65] [67] [68]:

- It offers flexible deployment options:
    - It can be deployed as a virtual machine as a part of on-premises deployment [68].
    - It supports private cloud deployment, where it can be deployed as a virtual instance [68].
    - It provides cloud-hosted deployment, where Silver Peak provides a cloud-hosted orchestrator to the enterprises as a service [68].
- It offers administration of the network by a single screen; all the business intent policies can be implemented through that single screen [68].

- It defines granular security policies and centrally orchestrates them; it also offers simplified service chaining for next-generation security devices [68].
- Real-time monitoring is another feature that it provides. It monitors the network and provides network statistics and details about application and web traffic [68].
- It makes the Unity EdgeConnect appliance's deployment easy and fast [68].

Unity Boost: It is an optional WAN optimization feature that Silver Peak provides. It includes the following features [67]:

- It eliminates the repetitive transmission of duplicate data by using data compression and deduplication. It does this by inspecting the packets at the byte-level and storing the content in the local and remote data stores. Then it analyses the fingerprints of the new packet's data and matches it with the local data stores [67].
- It offers acceleration techniques that significantly improve application performance response time across the WAN. By reducing the effects of latency on application performance. It is done by transmitting the data as quickly as possible to the Silver Peak appliance and not wait for the TCP acknowledgments when the TCP window is full [67].

4.3.2 VMware SD-WAN solution

VMware is a leader in Gartner's magic quadrant 2020; It provides SD-WAN solutions with VeloCloud products. VMware acquired VeloCloud in December 2017, which expanded its SD-WAN offerings. VMware SD-WAN solution provides network operators and application owners with a cloud-delivered solution ensuring application performance and availability with low networking costs. It enables traffic steering, which selects the best path for each application by combining multiple links. This ensures consistent application performance and minimizes the effects of quality issues and outages. It delivers high-performance and reliable branch access to cloud services, Software-as-a-services (SaaS) based applications and private data-centers while supporting application growth, simplified branch implementation and network agility. For SaaS applications, it ensures optimal performance without traffic backhauling. It also provides features like Virtual private networks and per-packet load-balancing for encrypted traffic. VMware SD-WAN monitors and measures the health of the links and reacts to any issues with proper actions.

With all these features, it gives the network operator full management and visibility of the network if needed [63] [70].

VMware SD-WAN solution offers VMware SD-WAN Edge appliances, VMware SD-WAN gateways, and VMware SD-WAN orchestrator and controllers, as shown in Figure 31. A VMware SD-WAN deployment starts with its SD-WAN Edge device, and these devices are placed and installed at locations such as branch locations and the data-center. The device in the data-center will be a larger device and act as a hub, connections from the SD-WAN edge devices will be aggregated at the hub. Optimization is delivered close to the cloud, which connects to the cloud-hosted applications in this model. This eliminates the need for backhauling traffic over private MPLS links.VMware SD-WAN Edge devices are easy to install as they are auto-configured [71] [72].

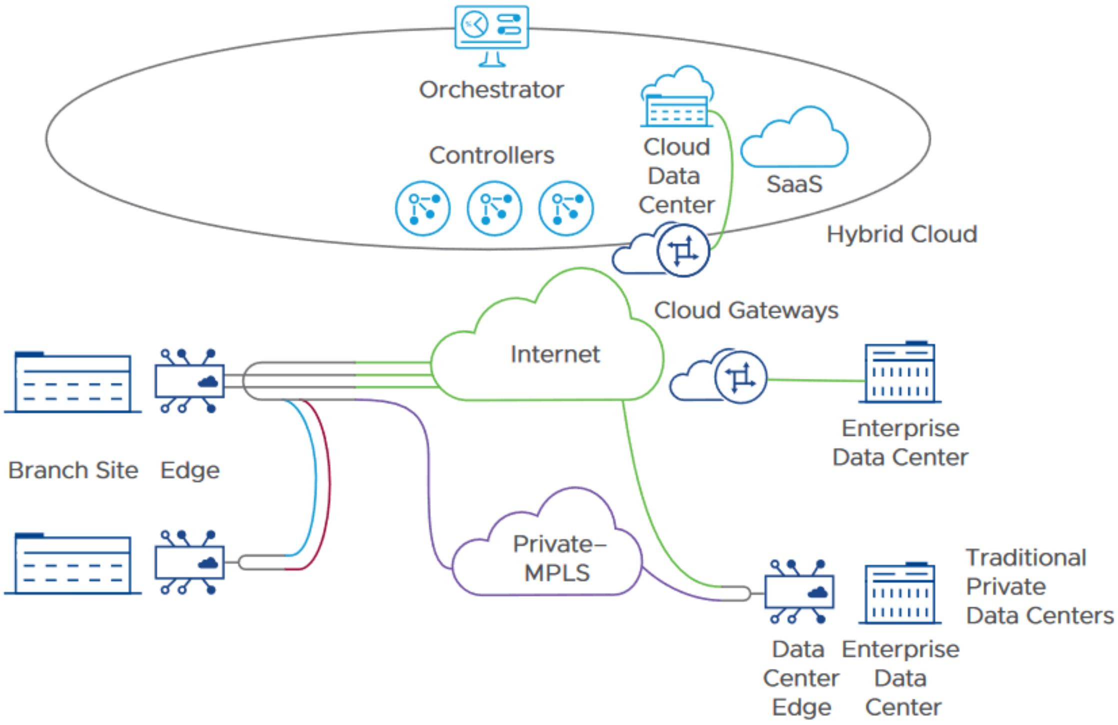


Figure 31: VMware SD-WAN architecture [73]

VMware SD-WAN Edges: VMware SD-WAN edge appliance can be a physical device or a virtual VNF software. The physical device offers easy to install SD-WAN edge devices with WAN, LAN and wireless LAN connectivity. SD-WAN edge as VNF software can be hosted on x86 customer premises equipment (CPE), which provides the same features as the physical one.

Generally, COTS hardware is used to host virtual SD-WAN edge. These Edge devices, as mentioned above, are auto-configured that makes them easy to install. Another benefit of SD-WAN edge devices is that their deployment costs much lower than a traditional router. These devices determine the best routes, support OSPF and BGP, apply business policies and replace traditional routers with their high available capability [71] [74] [72].

VMware SD-WAN gateways: These SD-WAN gateways support multitenancy and are deployed by VMware at the top-tier network point of presence (N-PoP). These gateways provide security services, traffic optimization and access to the private data center and the public cloud. VMware SD-WAN edge connects to its nearest VMware SD-WAN gateway, and the gateway handles the traffic after that point. The communication between the gateway and edge is secured with IPsec. This makes the user closer to the cloud, which enables better SaaS application performance [71] [74].

VMware SD-WAN Orchestrator and controllers: SD-WAN orchestrator can be a virtual machine hosted on a cloud, or it can be hosted on-premises. It is a management portal that manages all the SD-WAN edge devices hosted at the branch sites. It provides centralized policy management, orchestration of the data flow through the network and provision network-wide business policies to meet the business requirement. It allows the provisioning of virtual network services at a branch location with a single click. Controllers are distributed alongside the gateways and provide the distribution of routing information in the network [71] [74] [75].

Features of VMware SD-WAN solution:

- Flexible deployment models are provided by VMware SD-WAN Solution, which includes On-premises SD-WAN, Cloud only SD-WAN, and Cloud hybrid SD-WAN [74].
- WAN circuits are continuously monitored, which enables Zero-touch deployment. It allows dynamic optimization by continuously monitoring link and path quality [74].
- Dynamic path selection is enabled by its proprietary technology named VMware SD-WAN Dynamic Multipath Optimization, which consists of application recognition, automatic-link monitoring, auto-configuration of link characteristics, routing, and quality of service setting [74].
- Dynamic application steering is another feature provided by the VMware SD-WAN solution. It can recognize the applications based on the priority and their network

requirements. Then it can steer the application traffic via the optimal links for better application performance [74].

- On-demand Remediation, which includes error correction, jitter buffering, and local retransmit is enabled by the VMware SD-WAN solution. This remediation can be applied on a specific link on-demand for a single point of failure links or if all available links are facing degradation. It can only be applied for priority application traffic [74].
- Single click service delivery simplifies service deployment at branches. Services can be provisioned for remote branches by a single click, which will activate native VMware services and third-party VNFs [74].
- It enables smart quality of service, as it has the quality of service policies set as default out of the box. It automates the quality of service configuration and bandwidth allocation [74].
- It continuously monitors and assesses the performance of critical applications in the network. This analysis provides comprehensive statistics about application behaviour on any given physical transport [74].

4.3.3 Fortinet SD-WAN Solution

Fortinet is a leader in Gartner's magic quadrant 2020; It offers a Fortinet secure SD-WAN solution. Fortinet is a network security company and in the market for making cybersecurity products such as firewalls, intrusion prevention, etc. Fortinet is now providing a secure SD-WAN solution in those Fortigate firewalls as a service. It offers a Fortigate appliance with networking and security software on that appliance. This Fortigate appliance can be a physical proprietary CPE, or It can be a virtual machine that can be hosted on a universal customer premises equipment (uCPE). This appliance is capable of running VNFs and is managed by an orchestrator in Fortimanager. Fortinet SD-WAN solution consists of multiple components. The components that make up the Fortinet secure SD-WAN solution are FortiGate, FortiManager, FortiAnalyzer and FortiDeploy. FortiGate is the core of the Secure SD-WAN solution that runs on FortiOS. FortiManager delivers management and orchestration functions. FortiAnalyzer and FortiDeploy are responsible for delivering the solution as a whole. Secure SD-WAN architecture components are shown below in Figure 32 [76] [77].

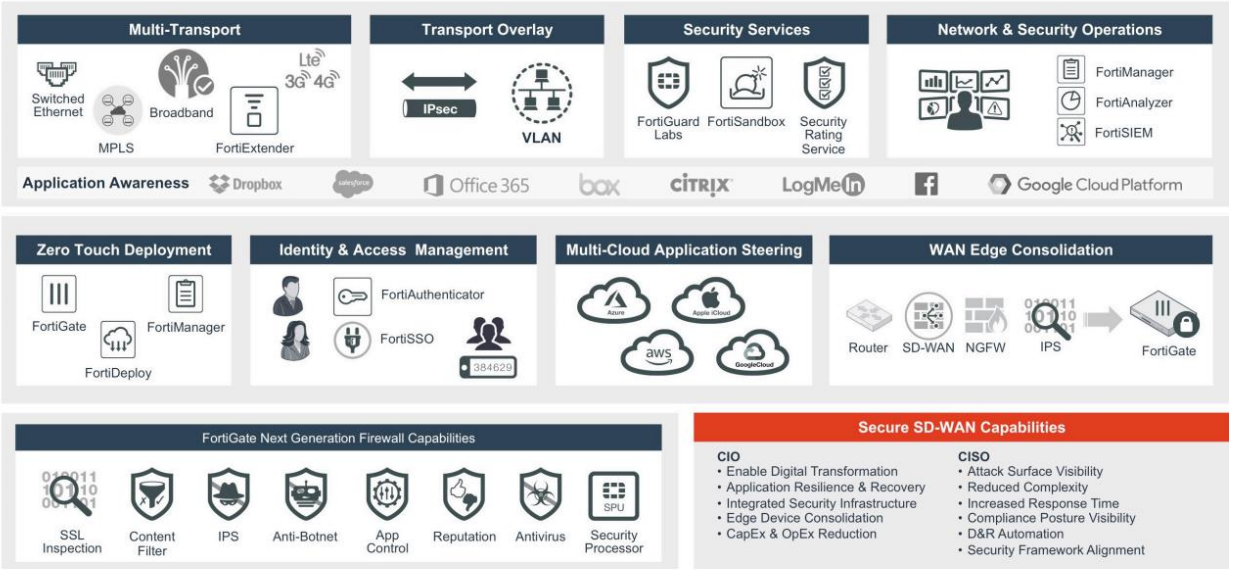


Figure 32: Fortinet SD-WAN architecture components [76]

FortiGate: FortiGate is the SD-WAN CPE and Next-Generation Firewall that is deployed at the branch sites and Data-center. It runs on a proprietary operating system FortiOS, the basic component of the Secure SD-WAN solution. It delivers advanced security features, SD-WAN capabilities, and routing protocol support. The features of FortiGate include SSL Inspection, Antivirus, Anti-Botnet, Application control, WAN optimization via protocol optimization, packet priority and VPN pairing. For small deployments, FortiGate acts as a management, control and data plane. It’s the distributed deployments in which it utilizes the full spectrum of Secure SD-WAN components [76].

FortiManager: It provides central management and orchestration of Secure SD-WAN edge devices. It can be deployed either on-premise or the cloud. Irrespective of location, it maintains connectivity with each FortiGate device. It presents a single-pane-of-glass view into the global network and monitors network SLAs. It provides templates for configuring security policies and SD-WAN policies. It is the sole requirement for controlling the entire deployed network. It supports APIs and security fabric connectors, which delivers seamless integration with the workflow of any organization. It plays a key role in the zero-touch deployment of branch edge devices [76].

Fortinet Secure SD-WAN provides a single device Fortinet NGFW which replaces the WAN routers, WAN optimization devices, and security devices. Fortinet Secure SD-WAN delivers many features, which are as follows [78]:

- Fortinet Secure SD-WAN provides zero-touch deployment with its edge appliances. These appliances are plug n play; after plugging the device, it contacts FortiCloud to connect to FortiDeploy. FortiDeploy connects the edge device to the FortiManager after authenticating the edge device [78].
- Fortinet secure SD-WAN solution provides integrated NGFW capabilities in its FortiGate appliances. Capabilities like SSL inspection, Content filtering, IPS, Anti-Botnet, etc., are baked into a single appliance that is capable of routing as well. The purpose-built security processor in the appliance enables Fortigate parallel path processing. That is done without any degradation in performance and at the same cost [76].
- Fortinet NGFWs are powered by their new system on chip 4 (SOC4) application-specific integrated circuit (ASIC). This new chip provides faster application awareness and steering to these appliances. By defining SLA based on the applications, Fortigate can steer the traffic based on the priority of the application [78].
- Fortinet NGFW enables a highly efficient deep secure socket layer (SSL) and transport security layer (TLS) inspection. Fortinet secure SD-WAN can identify and classifies application traffic with the help of an application control database that houses more than 5000 application signatures and is regularly updated by Fortiguard labs. This identification can be made via the first packet, and it can also identify encrypted cloud traffic. These inspections enable SD-WAN to route the traffic efficiently [78].
- Packet shaping capabilities enable Secure SD-WAN solution to provide a better quality of service for business-critical application traffic, i.e., video or voice traffic. This can be achieved by the preferential ordering of critical application traffic and rate-limiting non-critical application traffic across the virtual WAN link [76] [78].
- Automatic failover is enabled by the multipath technology, which switches over to the next best link in case of primary link failure. This switch over reduces the interruption and downtime for end-users [78].

- Forward error correction is used to enhance data reliability and user experience. It is a WAN path remediation technique that helps overcome packet loss and errors during transmission [78].
- Per packet, load balancing is available in the Secure SD-WAN solution for applications that require greater bandwidth. Fortigate Edge appliances make use of multiple links and create tunnels with other edge appliances. Which they use to maximize the number of packets through the tunnels, and these packets are reordered at the destination edge appliance. This helps in achieving greater bandwidth [78].
- Low latency multi-cloud access is another feature provide by secure SD-WAN as Fortinet NGFW is available as a virtual machine on major cloud service providers. An internet link can be used to create a secure connection from branch edge appliances to cloud edge appliances. It leverages its in-built security functions in providing secure access to cloud applications with low latency [78].
- True single pane of glass management provides full visibility into the network and provides details of all the deployed secure SD-WAN enabled Fortinet NGFWs. FortiManager, the secure SD-WAN orchestrator, simplifies workflow and policy management with few clicks. A full mesh overlay link for all the deployed devices is built and managed by the orchestrator for secure connectivity [77] [78].

4.3.4 Cisco SD-WAN Solution

Cisco emerged as a leader in Gartner's magic quadrant 2020. Cisco offers two SD-WAN solutions, one is Cisco SD-WAN powered by Viptela, and the second is Cisco SD-WAN Powered by Meraki. Viptela solution includes Viptela operating system or IOS XE platform with vManage, while Meraki solution has MX appliances with orchestration. The more popular and mainstream SD-WAN solution is the one powered by Viptela, which includes vSmart Controller, vManage, WAN Edge routers (vEdge or IOS XE routers), and vBond Orchestrator. Cisco SD-WAN solution with its components is shown in Figure 33 [63] [79] [80].

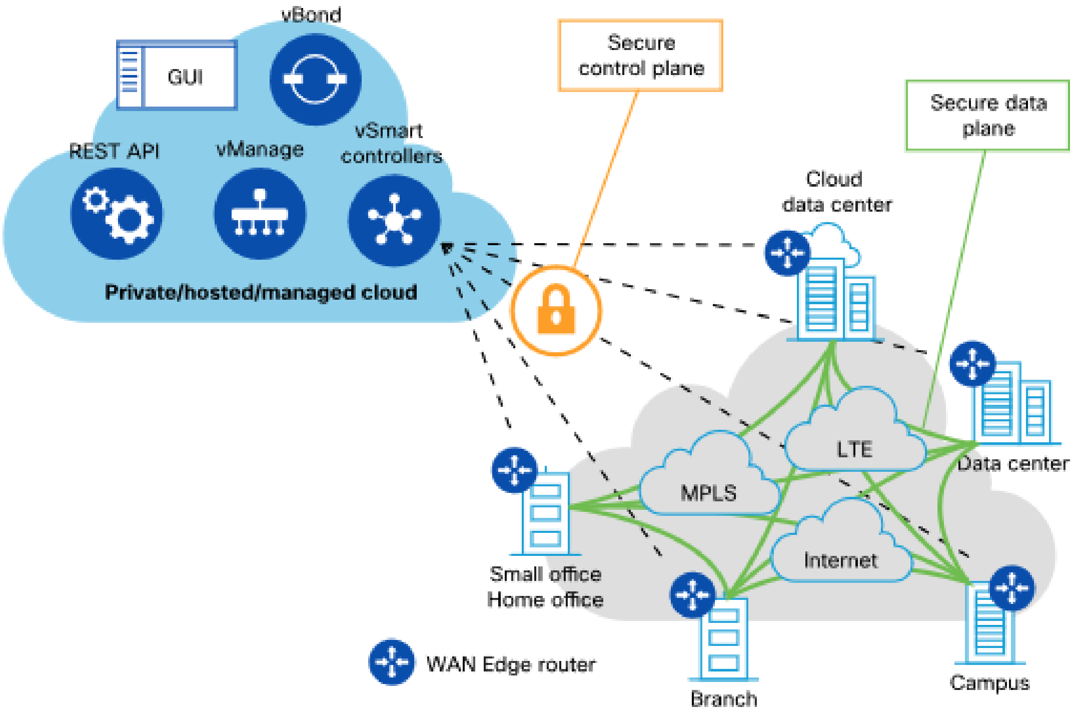


Figure 33: Cisco SD-WAN Solution Components [81]

Cisco WAN Edge routers: Cisco WAN edge routers are installed at the branch site, data center or in the cloud. These WAN Edge routers are available as physical devices like Viptela OS' vEdge router or IOS XE platform routers such as Aggregated Service Routers (ASRs) and Integrated Service Routers (ISRs). The virtual platform is also available for Cisco WAN edge routers such as Cloud service routers (CSRs) and vEdge cloud routers. These virtual routers can be deployed on any x86 hardware using hypervisors like KVM or VMware ESXi. These virtual platforms are also available as virtual instances with major cloud service providers. For SD-WAN overlay, WAN edge routers create IPsec tunnels with other WAN edge routers. WAN edge router establishes a control channel with a vSmart controller to receive configuration, provisioning and routing information [81].

Cisco vSmart: Cisco vSmart controller is the brain of the network. It is responsible for enforcing the business policies defined in vManage. Initially, when a device comes online at a branch site, its routing information is shared with vSmart controllers. Then, depending on the business policies applied, this information is forwarded to the other branch sites. Overlay Management Protocol (OMP) is used to exchange information between branch sites and Cisco vSmart [81].

Cisco vBond: Cisco vBond controller makes zero-touch provisioning possible. It is also responsible for device authentication, distribution of control and management information, and NAT traversal. The vBond controller is responsible for the onboarding of new devices installed at the remote sites. It shares the network information among other devices after understanding the network [81].

Cisco vManage: Cisco vManage provides a single pane of glass control and management interface for the underlying network. It offers a single or multitenant dashboard, depending on the customer's requirement. Network administrators can perform a number of functions like monitoring, troubleshooting, configuration and provisioning via the vManage dashboard. It provides a rich set of REST APIs which user-defined automation and integration into orchestration systems or tools [81].

Overlay Management Protocol (OMP): Overlay management protocol is used in Cisco SD-WAN to manage the overlay network. OMP enables the secure exchange of control plane information between WAN edge routers and vSmart controllers, shown in Figure 34. This control plane information includes route prefixes, next-hop routes, crypto keys, and policy information. By default, OMP allows a full mesh topology between the WAN edge routers [81].

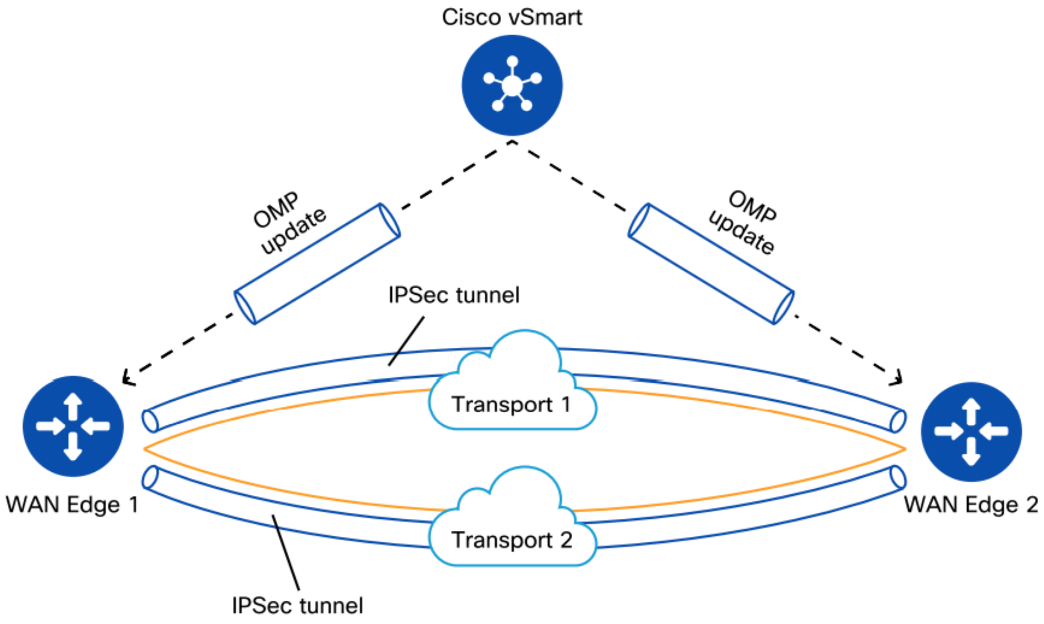


Figure 34: Overlay Management Protocol [81]

Features of Cisco SD-WAN solution:

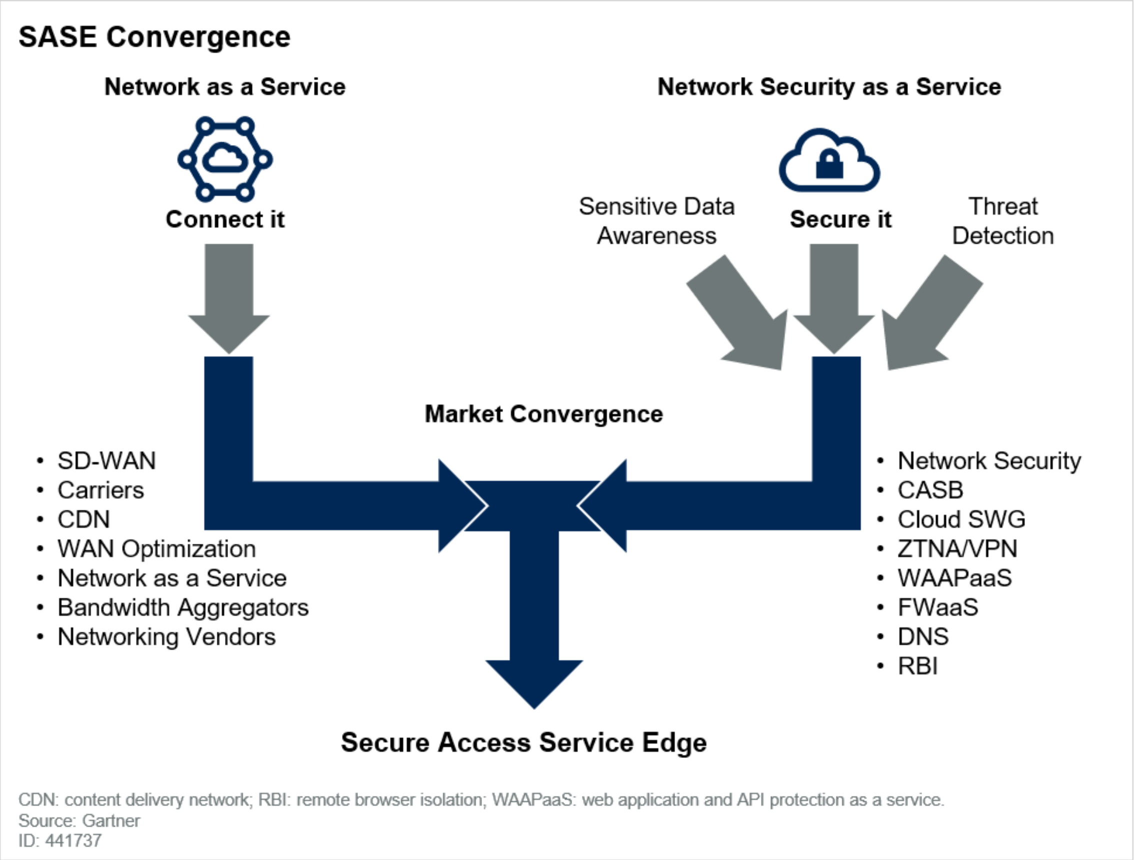
- Cisco WAN edge routers have the deep packet inspection (DPI) inspection integrated into them, which provides application visibility. DPI engine can classify more than 1500 applications by leveraging multiple technologies. After application classification, policies can be enforced to prioritize critical applications [81].
- Forward Error Correction feature in Cisco SD-WAN delivers critical traffic over unreliable WAN links. FEC can recover packets lost during transmission from source to destination. This is done by using parity packets for every predefined packet group. The receiving WAN Edge can recover the lost packet using the parity packet. It eliminates the need for retransmission and preserves application performance [81].
- Packet duplication is another feature that can be used application data over multiple links, so if there is any packet lost on any link, that can be recovered from the duplicate packets received over the other links. It increases application reliability [81].
- TCP optimization is enabled in Cisco SD-WAN. TCP selective acknowledgment (SACK) is used to prevent unnecessary retransmissions, and it maximizes throughput by larger TCP window sizes are used [81].
- Cisco SD-WAN provides secure direct internet access. It eliminates traffic backhauling which improves the internet experience for branch users and reduced WAN costs [81].
- Cisco WAN Edge features an Application-aware firewall, which can inspect traffic and provide features like URL filtering, IPS/IDS, Advanced Malware Protection (AMP), and DNS security [81].
- Cisco vManage provides REST APIs, which can be used for extracting details information about the state of the network. These APIs are compatible with traditional tools such as Syslog, SNMP, and Netflow. These APIs can also be leveraged by users for user-defined automation. Third-party domain controllers can also leverage these APIs to deliver an end-to-end operational experience for monitoring, management, configuration and troubleshooting [81].

4.4 Secure Access Service Edge

Secure Access Service Edge (SASE) is the term coined by the research and analysis firm Gartner. It is a cloud-based framework to secure WAN. It combines comprehensive WAN capabilities with cloud-native security functions such as Secure web gateways (SWGs), cloud access security brokers (CASBs), firewall as a service (FWaaS) and zero-trust network access (ZTNA). The traditional network is centered around the organization's data-center, while the focal point of the network with SASE is the cloud. SASE provides anywhere, anytime secure access to the cloud applications and services. SASE is particularly significant for organizations that witnessing the following changes [82] [83]:

- Increase in remote workers that are working outside of the organization's network [83].
- Increase in usage of IaaS and SaaS services by the users and organization [83].
- The traffic and workload are shifting from the data-center to the cloud [83].
- Sensitive data is shifting from the data-center to the cloud [83].
- The Traffic destined to the data-center is shrinking [83].

These changes are the characteristics of a modern cloud-centric digital business, which disrupts the traditional network functioning. The reason being traditional networks are focused on the data-center that has all the security functions. The users, devices and network capabilities require secure access everywhere in these cloud-centric digital businesses. SASE proposes a change in the paradigm by providing secure access irrespective of the location of the users or the applications. It addresses users and devices; a branch location for SASE is where the multiple users are concentrated. SASE uses cloud-native security functions like SWGs, CASBs, FWaaS and ZTNA. We can see SASE convergence in Figure 35 below [83].



CDN: content delivery network; RBI: remote browser isolation; WAAPaaS: web application and API protection as a service.
Source: Gartner
ID: 441737

Figure 35: SASE Convergence [83]

There are two components to SASE, which are Network as a Service and Network Security as a Service. Software-defined WAN is used to connect and manage remote branch sites of an organization that could be geographically dispersed. It provides features like WAN optimization, Quality of service, network automation and monitoring. It also provides security between the remote sites and the data-center and a low-cost alternative to traditional MPLS links. Though SD-WAN minimizes traffic backhauling, it still backhauls critical and sensitive traffic to the data-center for security and inspection purposes. We need security for the sensitive and critical data at the Edge, instead of the data-center, which requires backhauling and impact application performance. The other challenge SD-WAN faces is that the SD-WAN fabric lacks the security and access controls for the network in the cloud environment. Security functions like CASBs, Cloud SWGs, ZTNA, FWaaS and others provide a solution to this problem. These security functions provide security at the traffic entry point. This gives us SASE, using SD-WAN to provide network-as-a-service and cloud-native security functions to provide network-security-as-a-service. SASE enables dynamic policies that are based on the identities of users, devices or applications.

In SASE, the data-center is not the center of the architecture, and the users can access it as an internet-based service like other cloud-based services. The identities are coupled with the network capabilities and access. The network services and security policies are delivered and enforced dynamically, solely based on the identity of the entity [83].

Let us analyze the three scenarios from [83] and see what SASE provides in terms of security and connectivity:

The first scenario is about a salesperson Sue, who needs to access Salesforce CRM after hours via the Wi-Fi on her managed device. This managed device is also used for casual internet browsing. SASE here delivers Wi-Fi protection, malware inspection, SaaS optimized and accelerated connection with DLP to Salesforce. And for internet browsing, it provides SWG with DLP [83].

The second scenario is about a contractor, Jorge, and He needs to access an enterprise web application. This application is hosted in an enterprise data-center. SASE here will provide restricted access to specific locations, ZTNA, use WAAP services to protect the web application and inspect encrypted traffic for sensitive data loss [83].

The third scenario is about a set of wind turbines, which needs access to the edge-computing-based network and compute for data analytics on sensor data. They also need to stream the results on AWS without the location of the turbines. SASE here will deliver low-latency ZTNA access for turbines to edge computing resources, API protection and encrypted connection to AWS while hiding their IP addresses. The edge computing resources should be protected by FWaaS provided by SASE [83].

These scenarios are using different functions from the SASE stack, as shown in Figure 36. SASE is enforcing dynamic security and network access policies based on identity in each scenario. In the first scenario, Sue needs access to a SaaS application. Network services like Quality of service, Path selection, and SaaS acceleration are provided to optimize the application performance and user experience. While security services are Threat prevention and detection, DNS and Wi-Fi protection, UEBA, SWG, and sensitive data discovery are provided to secure the access. The services provided are relevant in the context of the first scenario. For the second scenario, network access services like Cost, Geo Restrictions are provided, and security services like DLP, Web application firewall and web application and API protection, ZTNA, Sensitive data discovery and

Network traffic encryption and decryption are provided. These services are relevant in Jorge's context as he needs to access a single web application that is hosted in the data-center. The services like QoS or SaaS acceleration are out of context in this scenario, while scenarios one and two are both using sensitive data discovery as it is relevant in both cases. In the third scenario, a set of turbines need access edge-computer-capabilities and AWS. The services like Latency Optimization, Path selection, and traffic Shaping are delivered for network access and security services like Web application firewall/ web application and API protection, Firewall as a service, ZTNA, Network traffic encryption and decryption and privacy are delivered for secure access. In this scenario, we have seen an overlap of services that were used in scenario one, like Path selection, and scenario two, like Web application firewall/web application and API protection and ZTNA. In these scenarios, we have seen that SASE eliminates the security perimeter, which is a legacy security and network access approach and introduces dynamic creation of policies based on identities and usage, regardless of the location of the entities or the location of network resources [83].

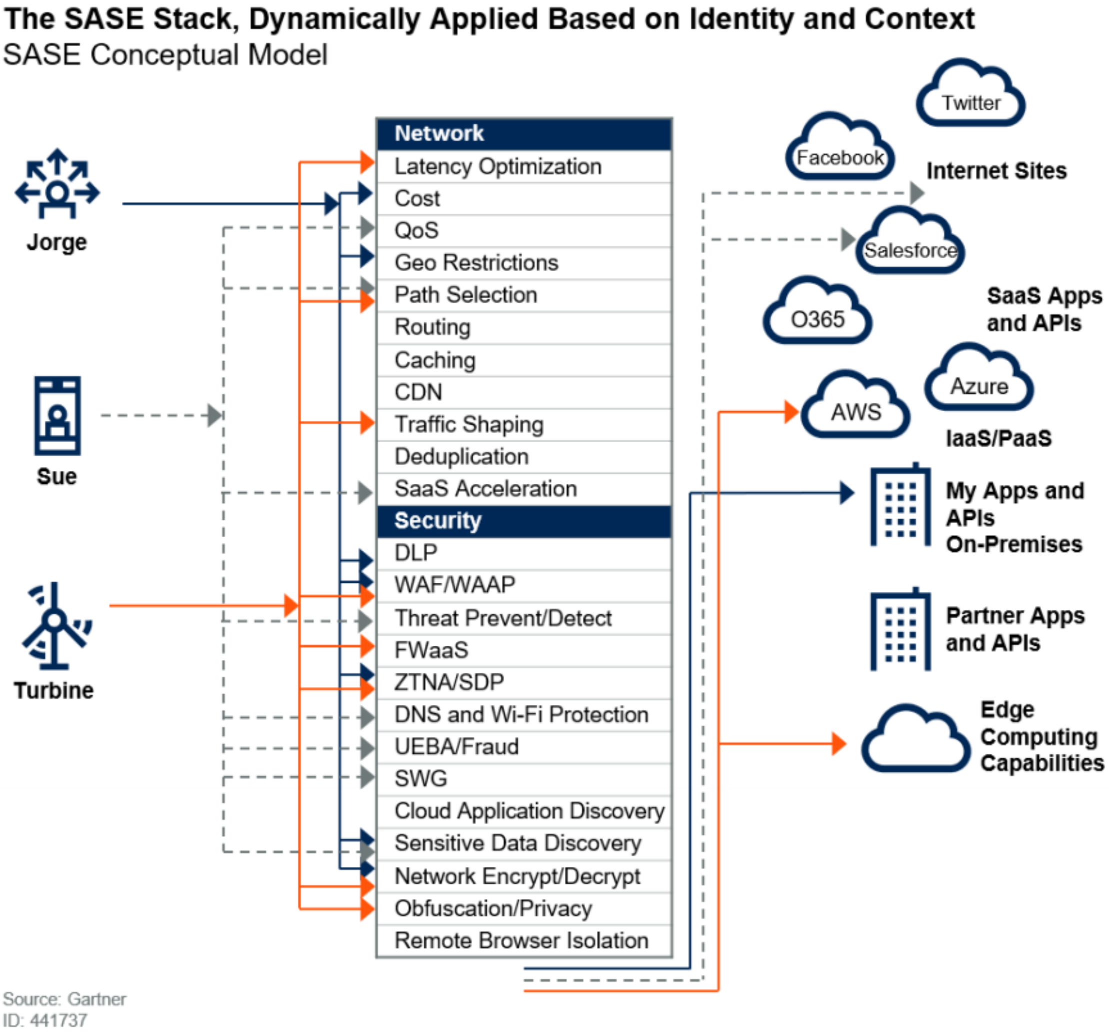


Figure 36: SASE stack [83]

SASE offers the following benefits [83]:

- SASE offered by a single vendor can reduce the complexity and cost associated with network management and security. As it will reduce the number of vendors, the number of the physical and virtual appliance being used at the branch locations. Which ultimately results in lower operational and capital expenses in the long term [83].
- SASE enables the organizations to provides secure access to their resources to the vendors and third-party contractors. This eliminates the need for legacy DMZ architecture [83].
- SASE vendor will be able to deliver latency-optimized routing across the points of presence worldwide. It is beneficial for latency-critical traffic VoIP, Video and web conferencing. SASE's high bandwidth backbone can be used based on the policies enforced [83].

- SASE offers ease of use, as with proper implementation. The number of agents required is reduced to a single agent or device. This enables access policy enforcement without user interaction. This improves the user experience [83].
- With SASE, updates for new threats and policies do not require new deployments of hardware or software. This reduces the operational overhead if we compare it with traditional WAN and allows quicker adoption of new capabilities [83].
- One of the SASE's components is Zero-trust network access. By using this approach, SASE provides better security and policy enforcement based on the user or device identity. SASE provides end-to-end encryption of the entire session as it assumes the network is untrusted [83].

4.4.1 SASE Security Functions

SASE's core security functions consist of the following:

Cloud Access Security Broker: A Cloud access security broker (CASB) is a cloud security solution, which acts as an intermediary between the users and the cloud service providers. The increased usage of Software-as-a-Service, Infrastructure-as-a-service, and platform-as-a-service environment increase the risk which is addressed by CASB. It protects sensitive data so businesses can use the cloud services safely and securely. It extends the reach of security policies beyond the on-premises infrastructure. CASB ensures that the traffic between the corporate network and the cloud service providers complies with the security policies enforced by the organization. One of the vital abilities of CASB is that it can provide insight into cloud application use. This can be done across multiple cloud service providers. With this insight, it can identify unsanctioned use of the cloud application. Identification of high-risk applications, high-risk users and other risk factors can be accomplished with CASB autodiscovery. It also provides services like device profiling, encryption, security access controls, credential mapping and single sign-on.

CASB offers the following functionalities [84] [85]:

- It provides Firewall functionality, which enables malware identification and prevents malicious traffic from entering the corporate network [84].

- Authentication and Authorization is another functionality CASB has. It verifies user credentials and provides access to the resources based on those credentials [84].
- It offers web application firewall functionality to prevent malware from breaching security at the application level [84].
- It offers Data loss prevention (DLP), which prevents the transmission of sensitive data outside of the corporate network [84].

Secure Web Gateway: A secure web gateway is a solution that protects the enterprise from unauthorized traffic and web-based threats. It is the gateway between the user and the internet and applies and enforces acceptable corporate policies. It prevents malware and viruses from breaching the corporate network. This web gateway allows approved users to access approved resources. Another function of a web gateway is that it prevents the leaking of sensitive information out of the corporate network. Secure web gateways are installed at the edge of the network. It can be a software component or a hardware device. All the traffic to and from the user must pass through the gateway so that the gateway can monitor the traffic. It monitors the traffic for malicious code, use of web application and URL connection made by the user. This gateway can filter URLs based on the known website list, and all other and unknown websites and known malicious website access will be blocked by the gateway. The gateway maintains two lists, i.e. whitelist and blacklist. Whitelist consists of all the known and approved websites while the blacklist c [86]onsist of the known malicious websites that are blocked. These list filters are applied to all the incoming and outgoing traffic. Similar to URL filtering, data going out of the network can be monitored. The restriction can also be applied at the application level, where some functions are known and approved, and some are blocked. For example, functions like uploading on a SaaS application can be blocked [86].

Some features of Secure Web Gateway beyond URL filtering and data filtering are:

- The gateway should be able to perform the inspection of SSL encrypted traffic. This enables the comparing all the traffic to the threat lists available and then analyzing the traffic to check if it consists of any malicious code or content that poses a threat to the network [86].
- Data loss prevention is another feature where the gateway should scan the documents shared or uploaded out of the network for any sensitive data [86].

- It should Scan and filter all the information to and from social media [86].
- It should provide support for protocols like HTTP, HTTPS, and FTP [86].
- To deliver the best threat prevention and remediation, it should integrate with an anti-malware solution that can detect zero-day threats [86].

Zero Trust Network Access: Zero trust network access (ZTNA) is a part of the zero-trust model. The term zero-trust was introduced by an analyst at Forrester Research 2010. This model is a security framework that enforces strict user and device authentication throughout the network. This model suggests that no user should be trusted even if they are allowed on the network as they can be compromised. Instead of authentication the user or device for a network perimeter, they are authenticated throughout the network. It used identity-based authentication to establish trust and provide access. It keeps the network location hidden and provides IT and Security teams with centralized control. It secures network access and detects anomalous behavior based on location, time and attempts to access any restricted resource. The zero-trust model support micro-segmentation that enables network resource restriction so potential threats can be contained. It also enables granular policies, which include role-based access to secure sensitive resources and data [87].

Some features of ZTNA are:

- It protects an organization's data and provides restricted access [87].
- It enables lower breach risk and threat detection time [87].
- It delivers improved visibility into the network traffic [87].
- It offers increased control in a cloud environment [87].

Web Application and API Protection as a Service: Web Application and API protection is a security tool designed to protect web applications and APIs. It analyzes incoming traffic and resides on the public side of the web application. WAAP service works are application layer, and below are the key capabilities of a comprehensive WAAP service [88]:

- It monitors and protects the web application from a wide variety of attacks, which can be possible by the Next-Generation Web Application Firewall [88].
- It identifies and blocks attacks from malicious bots while allows access to the known bot traffic [88].

- It delivers real-time attack protection for web applications [88].
- It offers protection against denial-of-service attacks, which makes the web resources unavailable for legitimate traffic by overwhelming them with high request volumes [88].
- It prevents and protects the applications and resources from any abusive behaviour that can negatively impact the resources [88].

Firewall as a Service: Firewall as a service (FWaaS) refers to the firewall that resides in the cloud and offers advanced layer 7 capabilities, such as URL filtering, access controls, advanced threat prevention, intrusion prevention systems (IPS) and DNS security. FWaaS offers a cloud-based logical and scalable firewall that can be accessed irrespective of the location. These firewalls are delivered and maintained by cloud service providers. This eliminates the use of perimeter firewalls. This simplifies the organization’s IT infrastructure. The benefits of firewall-as-a-services are as follows [89] [90]:

- FWaaS enables unified and consistent security policy enforcement, as organizations can now send all their traffic through one of their firewalls [90].
- FWaaS is a cloud-based resource, and its deployment is not limited by the location like the physical firewalls [90].
- FWaaS offers scalability over the physical firewalls as it is a cloud resource and can be quickly expanded to accommodate growing traffic requirements [90].
- FWaaS delivers improved flexibility than the physical firewalls, as organizations can adapt to the surges in the network easily [90].
- FWaaS brings a cloud-based intrusion prevention system, which delivers always-on threat protection and coverage irrespective of the connection type or location [89].
- Inspection of user traffic includes SSL traffic, provides full visibility into applications, users and internet connections [89].
- FWaaS delivers better DNS security and control, which is the first line of defence. It provides optimized DNS resolution that delivers a better user experience and cloud application performance [89].

Remote Browser Isolation: Remote browser isolation (RBI) is also referred to as web isolation. It is an advanced cybersecurity technique that provides an additional layer of protection for users. It reduces the device’s attack surface by separating the browsing activity from the endpoint. The browsing is done in a remote browser in the cloud, and the webpage is rendered to the user. The user just receives the pixels instead of the traffic or any active content from the webserver. This method keeps the malicious code away from the user's device, thereby protecting users and their devices. The benefits of Remote browser isolation are [91]:

- Risky web content can be access safely, as it isolates the users from the web applications and web traffic. It delivers safe rendering of the web content on the endpoint [91].
- It offers protection from targeted attacks hidden in the web pages, downloadable web content and vulnerable plugins [91].
- The ability of a web page to exfiltrate data or compromise a user's machine has been eliminated.
- It reduces risk and minimizes policy complexity so that organizations can implement more open policies for internet access [91].

4.4.2 SASE vs SD-WAN

SD-WAN is an application software-defined networking that uses network virtualization and virtual network overlay to connect and manage the remote branch sites. The focus is to connect the branch sites to the head office's data center. SD-WAN is not built with the cloud as its focus, though it can easily be integrated with the cloud. On the other hand, SASE's focus is on the cloud, and it has a distributed architecture. Where SD-WAN's focus was to connect the branches to the head office's data center, SASE focuses on the endpoints, either a single user or a branch site, and connects them to the service edge. SASE software stack runs on the service edge, consisting of a network of distributed points of presence. SASE provides a cloud-based service that combines the SD-WAN approach and security functionalities. SASE looks at the Wide Area network differently than SD-WAN does. SASE network fabric is made up of Vendors' point of presence (PoPs). SASE uses SD-WAN features like bandwidth optimization and traffic prioritization. SASE uses security agents on an end user's computer or the cloud to make these network decisions, unlike SD-WAN, which uses virtual devices distributed throughout the WAN [82].

SASE's point of presence forms the architecture's service edge, and the SASE stack runs on the service edge. SASE uses private cloud or public cloud to provide the point of presence. Optimal routes for the traffic are determined by SASE software. It is a distributed architecture that is different from SD-WAN, centred around the organization’s data-center. However, SD-WAN does provide cloud integration, but it more of a feature than a vital element. Though it has a similar approach to SASE, which is Cloud-enabled deployment, requires the user to connect to the virtual cloud gateways through the internet [82].

The focus of SASE is to provide secure access to the distributed resources for the network and its users. Private data-centers, colocation facilities and the cloud are used for resource distribution. The security tools reside on the user’s device and the cloud as security agents and have security and networking decision-making capabilities. Security in SD-WAN is delivered via third-party vendors. Security is not the main focus of SD-WAN. However, it depends on the vendor providing the solution. Some SD-WAN solution does have security baked into the solution, for example, Fortinet SD-WAN Solution. SD-WAN does provide flexible connectivity and monitoring of branch locations with the central headquarters. Security tools reside in the CPE located at the offices, and the networking decisions are made by the virtualized network devices distributed throughout the WAN [82].

SASE networks use security functions like firewalls, SWGs, CASBs and zero-trust access. SASE runs these functions in parallel, and When the traffic is opened up for inspection, it is inspected by these functions at once. There is passing of traffic in between these functions, which save a lot of time. However, SD-WAN uses point solutions and service chaining. Point solution is an individual security function that handles one type of threat. SD-WAN uses multiple point solutions to enforce security policies. The traffic is inspected by the point solutions one at a time. The point solutions open up the traffic, inspect it, then forward it to the other point solution after closing the traffic. This process is followed until the traffic is passed through all the point solutions [82].

4.4.3 Cato Networks SASE Platform

Cato Networks SASE platform provided the first implementation of the SASE framework in 2019. Cato offered a solution that converged SD-WAN, a global private backbone and network security stack with distributed network PoPs. It provided many security services coupled with the benefits of SD-WAN. As shown in Figure 37, the Cato network's SASE solution has the cloud at the center of the network. This private cloud backbone provides connectivity regardless of the source can either be a branch, remote host or data center. SASE is a framework that utilizes SD-WAN principles and technologies with cloud-native security functions. SASE provides WAN capabilities such as cloud optimization, WAN optimization, Global route optimization and self-healing architecture. In terms of security functions, it has Next-generation Firewalls (NGFW), Secure Web Gateways (SWGs), advanced threat prevention and, cloud and mobile security. This private cloud backbone provides encrypted connections from the source to the destination [82] [92] [93].

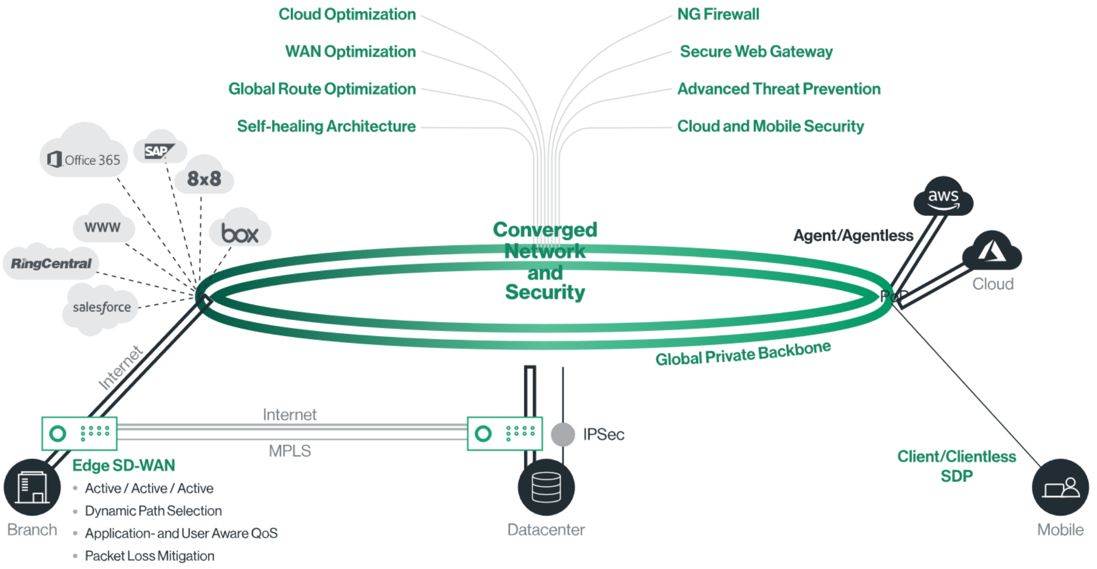


Figure 37: Cato Networks SASE Cloud [92]

Components of Cato Networks SASE Platform:

Cato Socket: It is the SD-WAN edge device that is used for branch offices and data-centers. Cato sockets have all the SD-WAN edge functions such as link aggregation, dynamic path selection, application identification, bandwidth management, routing protocol integration and packet loss mitigation [92].

Next-Generation Firewall: Cato provides Next-generation firewalls that enable capabilities like Application awareness, LAN segmentation, user awareness, WAN and internet traffic protection. NGFW provides granularity in terms of network policies and rules. Classification of application can be done with the first packet without SSL inspection. NGFW’s deep inspection engine takes information from the network metadata and uses the Cato research Labs application database to correlate the data and classify the application. IAM (Identity Access Management) and RBAC (role-based access control) capabilities are used for user awareness [92].

Secure Web Gateways (SWGs): It provides the capability to control and monitor the access to websites for the users. Cato provides predefined URL categories, and the customer can add their own to the list [92].

Anti-Malware: Malware detection and prevention, Deep packet inspection, and true filetype detection are elements of Cato’s anti-malware service. It has a multi-feature engine that reviews digital signatures with existing information in the database on suspicious sites and attack methods. This engine is kept up to date with the global threat intelligence database. Cato also partnered with SentinelOne, which can identify and block unknown malware using Machine learning and artificial intelligence. Encrypted and unencrypted traffic is inspected and blocked if necessary. The actual filetype can be determined by the true filetype detection, which detects the true type of file without considering the file extension or content header. It is a handy and useful tool to combat the evasion tactics that mask the high-risk filetypes. All these services function in parallel during traffic inspections. Parallel inspection is the critical element of SASE services [92].

Intrusion Prevention System: IPS in Cato SASE platform is multi-layered and prevents attacks and network scans with behavioral analysis. Cato SASE's IPS services are protocol validation, behavioral signatures, reputation feeds, malware communication, geolocation, and network behavioral analysis. IPS validates the packets conform to the protocols and reduces the chances of an attack from exploits. IPS can search for deviations from the network or user behavior. Reputation feeds are the collection of Cato’s and other intelligence feeds. IPS uses network behavioral analysis and reputation feeds to stop any outbound traffic from reaching command and control servers. The geolocation feature in IPS can be used to block traffic from any specific country or location [92].

Global PoP Network Backbone: Cato has a distributed network of PoPs, which are capable of running a cloud-native software stack. This stack can run all security functions and network services. Multiple customers can connect to a single PoP. These PoP uses IPsec tunnels to connect to a Cato Socket located at the customer location or a device that is capable of using IPsec tunnels, i.e., a remote user computer. The connection between the PoPs is encrypted. Cato PoPs has routing algorithms that factor in the flow of traffic, and it enables WAN optimization as one of the networking services through a Cato Socket [92].

Features of Cato Networks SASE platform:

- Cato provides a global private backbone, which enables reliable and affordable connectivity for its customers. With which customer can easily connect their Data-center to their WAN [92] [94].
- TCP efficiency is improved by WAN optimization and advanced TCP congestion control, which increases data throughput for users and branch sites [94].
- It provides end-to-end encryption built-in in all communications with AES256 tunnels [95].
- Cato enabled secure remote access with easy deployment and integration with the Active Directory and access management [96].
- Cato enables and provides Security as a service, including access control across the network and advanced threat prevention [95].
- Access control across the network capabilities is enabled by the Next-generation firewalls (NGFW) and Secure web gateways (SWGs). They provide granular control and full application awareness. Access control, monitoring is allowed by SWGs, and NGFW enables inspection of packets to provide full application awareness [95].
- Advanced thread prevention includes anti-malware and Intrusion prevention systems. Both services inspect the traffic in the cloud. Inspection of TLS-encrypted traffic is also enabled at Cato Pops [95].
- Managed threat detection is also provided by Cato networks in their SASE solution. Cato's SOC Teams enabled Managed Threat Detection and Response Service (MDR). They analyze and verify suspicious activities and inform the customer. It reduces the requirement for the customer to employ skilled personnel for this process [95].

4.4.4 Cisco SASE platform

Cisco SASE platform includes integration of technologies from Umbrella, Viptela and Duo security. Umbrella provides the security aspects of the SASE, Viptela provides the networking connectivity to connect the users to the network, and Duo security helps the user to securely access the resources in the cloud. Cisco SASE architecture is shown below in Figure 38 [97].

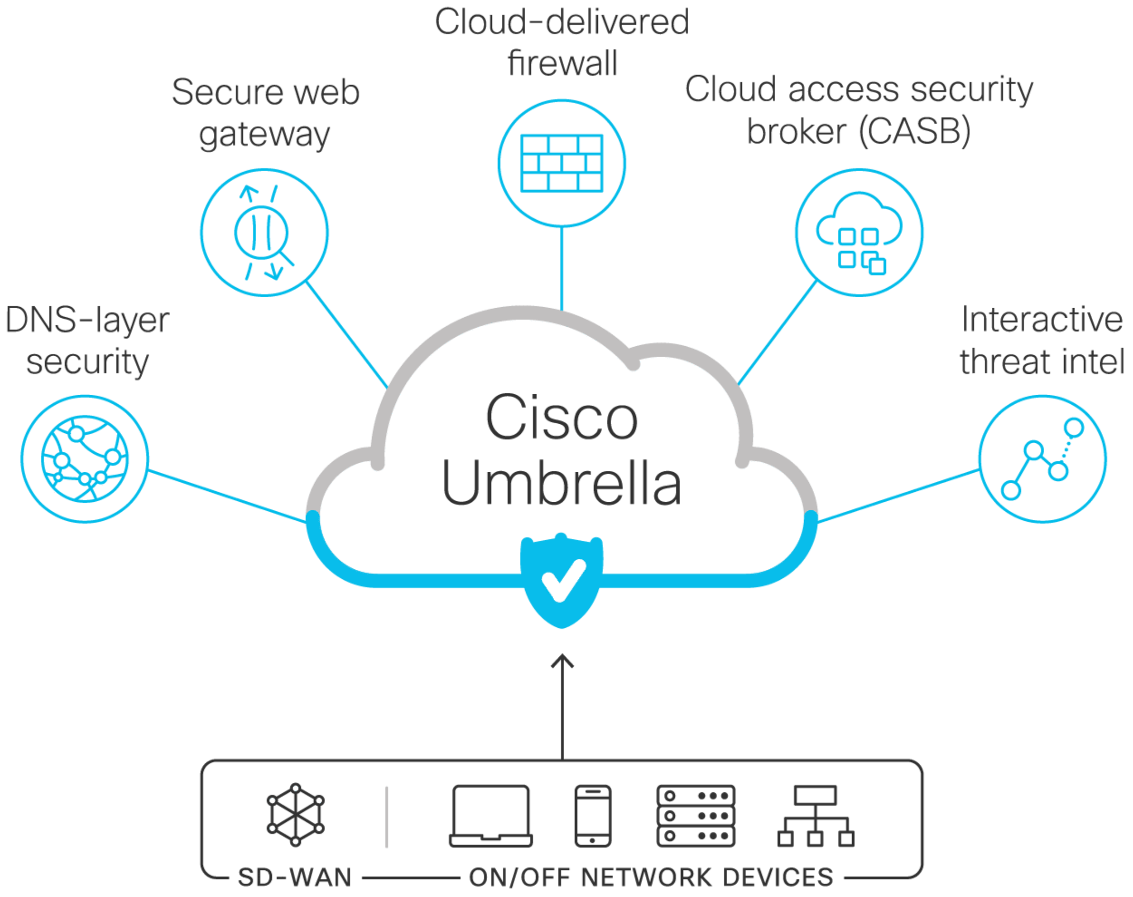


Figure 38: Cisco SASE Architecture [98]

The components of the Cisco SASE platform are:

The secure Internet Gateway: Umbrella provides a secure internet gateway (SIG) with a single cloud-native stack integrated with all the security services. The services include Domain name system security, full proxy secure web gateway (SWG), control access security broker (CASB) and a cloud-delivered firewall. Parallel inspection of traffic being a vital element of SASE architecture, Umbrella runs all the functions at once during traffic inspection [82].

Cisco Umbrella's DNS security: DNS-layer is the first line of defence, as mentioned by cisco. DNS resolution is the first step in accessing the internet. DNS Security here works at DNS and IP layer, so the requests to malware, ransomware, phishing, and botnets can be blocked before the connection is established. DNS layer security enables deeper inspection of traffic via antivirus engines and advanced malware protection software. It provides visibility to the organizations to the cloud applications accessed by their users. The granularity enables the organization to determine if the applications are blocked, a potential risk or safe to use. [82]

Cloud-based Secure Web gateway: Umbrella SWG scans all the traffic coming and going through it. It enables SSL decryption, which helps to identify hidden attacks. Access to specific file types or specific activities in the application can be blocked for the users. SWG can also block traffic based on the destination, which might go against organization compliance policies. SWG can also provide a detailed report that includes URLs, network identities, action taken and external IP address accessed [82].

Cisco Umbrella's CASB: CASB offers granularity in terms of applying policies and provides application awareness. Granularity here means blocking or allowing a specific application for a specific individual or a group [82].

A firewall in the cloud: It enables visibility of the traffic passing through it. All the outbound traffic heads to the firewall because it works on layer 3 and layer 4, and all the traffic activity is logged in the firewall. IPsec tunnel is used to send the traffic to the firewall [82].

Networking Via Viptela: Viptela is Cisco's SD-WAN product discussed in subsection 4.3.4. Cisco SASE platform uses Viptela for its connectivity from the source to the cloud. Viptela can be used to route traffic to and from the network edge, which is a vital part of SASE. Network PoPs are the edge location where SASE services are delivered [82].

Duo Security and Zero Trust Access: Umbrella is integrated with zero-trust technology from Duo security. That implements a multi-factor authentication in order to access the Organization's SASE network. This ensures security and certainty that employee's credentials have not been compromised. This is the result of following the zero-trust approach, where all the traffic and sources of the traffic are suspect even if the source is a reliable employee. Here the source has to go through several steps to verify their identity, and then access will be provided. Moreover, to ensure that the devices in the network are not compromised, real-time device health monitoring is performed. Access policies provide a level of granularity where policies or access can be defined based on user location, type of device being used, along with other contextual information [82].

4.4.5 SASE Use Cases

Let’s discuss some SASE use cases:

Use Case 1: When it comes to geographically dispersed branch locations, for organizations such as banks or retail stores, the data need to traverse to the security stack hosted at the hub location for security and examination purposes. If the applications are hosted at the hub location, then this justifiable, however, if the organization is utilizing cloud applications or web applications, this creates performance issues. For an example of a retail store business based in Toronto that has remote stores all over Canada, one such store is located in Vancouver that had to contact its head office in Toronto to process a single transaction. Let analyze the situation here, A person is buying something in the retail store and using his credit card at the retail store. The bank which issues the credit card is located in Vancouver just like the retail store. The traffic needs to reach Toronto by traversing the whole country from West Coast to the East Coast. And then the traffic will go back to the bank in Vancouver which will then authorize the transaction. All that just for processing a single transaction. Now imagine a similar situation with real-time applications, this could lead to high latency, which can result in poor application performance. Real-time applications are dependent on seamless and low latency connections [99].

SASE will connect this Vancouver store with the enterprise applications via secure tunnels while connecting with vendors locally and enhancing the application performance and user experience. This setup requires Universal customer premise equipment (uCPE) and the cloud features like cloud access security broker (CASB) and DDoS mitigation [99].

Use Case 2: In geographically diverse organizations, which include remote branch locations and an increasing number of remote workers. Remote workers connect to the organization using a VPN to use private resources and access cloud applications. For example, ACME corp. has few branches all over Canada, and has an increasingly remote workforce due to the coronavirus pandemic. This workforce needs to access the data-center hosted applications and cloud applications. With legacy WAN, They need to connect to their hub location via a VPN and then access the resource hosted at the data center and the cloud traffic will also follow the same route to the data center and exit from there to the internet. We can see two main issues here, one is the degraded performance of cloud applications through backhauling and another is the security as they are a prime target for attacks. Both of these issues can be addressed by SASE. SASE advocate that the cloud should be the focus of the network. Remote users will have security agents installed in their devices, which will connect them to SASE's many network point-of-presence around the globe. The user device will form a secure connection to the network point-of-presence, after that the traffic will be handled by the SASE backbone. The required features here are zero-trust network access(ZTNA), firewall-as-a-service(FWaaS), cloud access security broker (CASB) and cloud secure web gateway (CSWG).

Use Case 3: SD-WAN makes the network simple and eliminates the scalability limitation, however it makes security a complex issue. SD-WAN advocate for DIA (Direct Internet Access) which results in an increased number of broadband connections and internet access points to SD-WAN sites. SD-WAN devices lack an inherent native-security stack which is required to harden the connection to the Internet. SASE can be used in this case as well, in a business where security is paramount. For example, A Medical system, where they have clinics all over the city. All the clinics are connected directly to the internet. With the existing solution, they might not be facing performance issues but they need a secure connection to the internet. SASE can address this issue and define a secure means to connect to the internet. SASE addresses connectivity, security and routing for the enterprises [99].

4.5 Use Case

As we discussed in our case study in subsection Use Case3.3, we have faced a few challenges and limitations with the legacy WAN technologies. Let us revisit the challenges ACME Corp. was facing:

- ACME does not have complete control of its IP routing, as the service provider is handling it.
- ACME is using a Hub and Spoke model. This means remotes sites have to go through the head office to communicate with any other remote site called backhauling of traffic, which is an inefficient use of the links and puts an unnecessary load on the links.
- Similar backhauling is experienced when remote sites use cloud applications; the traffic goes to the head office and then goes through the middleboxes then to the cloud.
- Lack of quality of service of critical application traffic such as voice and video.

- Existing MPLS infrastructure is incapable of integrating with cloud services.
- Expensive and time-consuming new site deployments take around a few weeks to deploy a new MPLS connection for a remote site.

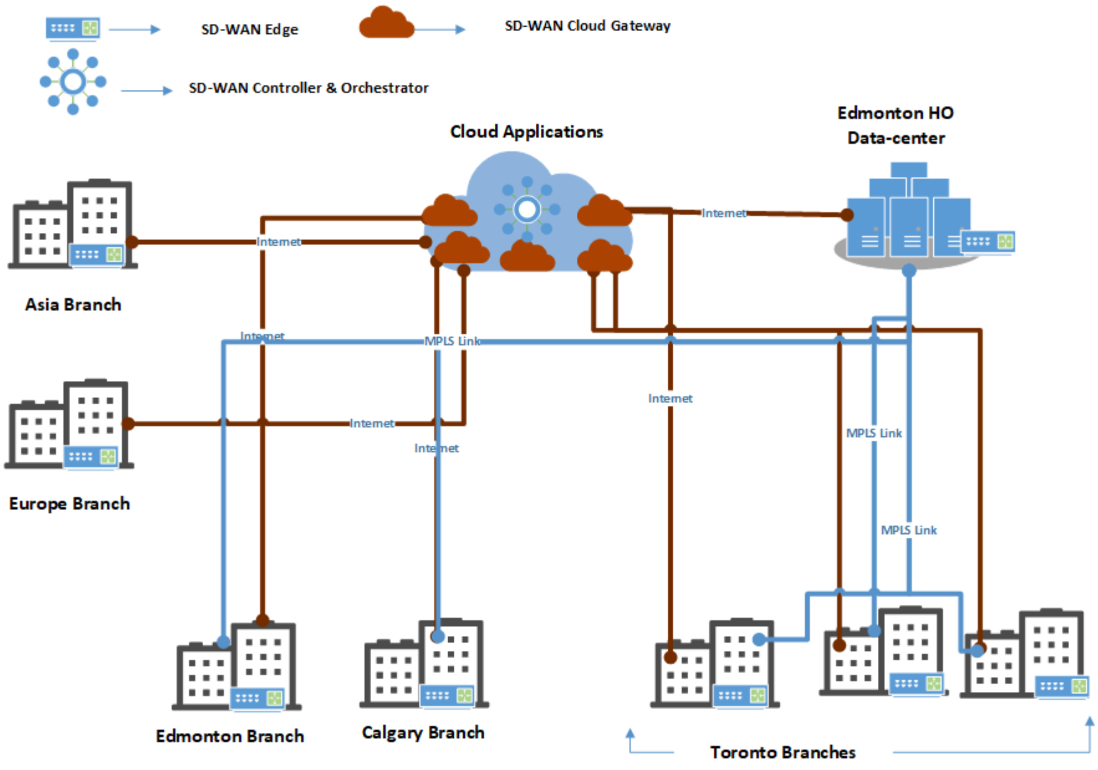


Figure 39: ACME SD-WAN Network

In SD-WAN, There are three types of architecture to choose from. However, for the sake of this case study, we are going with Cloud-enabled SD-WAN. SD-WAN's essential components are SD-WAN edge device, SD-WAN controller and SD-WAN orchestrator. SD-WAN Cloud gateway is also required in cloud-enabled SD-WAN. SD-WAN edge device is the Customer premises equipment, either a physical device or a virtual one.

ACME Corp. has a data-center at its head office, where are all servers and applications are hosted. It can either purchase a physical device from the SD-WAN Service provider or purchase Commercial-of-the-shelf equipment and run a virtual image of the CPE on the device. It needs to install an SD-WAN controller and SD-WAN orchestrator either at the data-center or in the cloud. However, the cloud should be the preference as the On-premises controller and orchestrators are limited by geography while the cloud provides geographical redundancy. Now that the head office is all set up, It needs to ship an SD-WAN edge device to its remote locations and provide an internet broadband connection at the sites that don't have one. These Edge devices are plug n play devices. Hence no expertise is required to install these devices. Once powered on and connected to an internet link, it will secure a connection with the SD-WAN controller, as shown in Figure 39. These SD-WAN edge devices will use their nearest SD-WAN cloud gateway to connect to the SD-WAN controller. All that's left is doing the configuration on the SD-WAN orchestrator via the graphical user interface. Any policy applicable on all sites or a specific set of sites can be applied within minutes with a few clicks. It's all ACME Corp. needs to do to be SD-WAN enabled. All five domestic remote sites have the Edge device installed with a broadband internet connection and have a secure connection with SD-WAN controller and SD-WAN Cloud-gateway. Edge devices at the domestic site use two links provided, which are MPLS and Broadband. The international sites in Europe and Asia have also installed edge devices; these devices have secured connection with SD-WAN controller and SD-WAN Cloud-gateway.

Now that ACME Corp. has moved to SD-WAN, let us see what type of benefits and solutions SD-WAN is providing:

- SD-WAN enables remote sites to use multiple links, i.e., MPLS, LTE, or broadband, and enable link redundancy.
- SD-WAN provides quality of service for critical traffic such as video and voice with appropriate policies applied.
- Now that all ACME Corp sites are SD-WAN enabled, Backhauling can be minimized as the Cloud application traffic will directly be sent to the SD-WAN cloud gateways. IPsec secures this transmission, and it optimized application performance. Backhauling will only be required for critical application traffic, which needs extra security measures if enabled by the organization.
- With Backhauling minimized, sites can communicate with each other without using the links inefficiently.
- ACME Corp. will be able to monitor and manage its network and IP routing.
- SD-WAN is integrated with the cloud and provides zero-touch deployment with its plug n play SD-WAN edge devices.

- SD-WAN edge device provides Next-gen firewall services at the site, which enable secure communication.
- The cost of deploying a new site and time consumed has been significantly dropped compared to MPLS deployments.

We now know the benefits received by ACME with its SD-WAN enablement. Let’s take a look at the limitations and challenges ACME still facing:

- Backhauling of traffic to the head office is still required in case of critical application traffic.
- SD-WAN uses point solutions in terms of security functions; when it comes to traffic inspection, the traffic flows from one security function to the next. Results in extra time added to the response.
- SD-WAN lacks cloud-native security tools.

To combat above mentioned limitations, the SASE framework can be used at ACME Corp. It is already using the SD-WAN solution. SASE provides the necessary security functions and features that reduce or nearly eliminate backhauling. One of the primary purposes of backhauling traffic to the data center is to process the traffic through security devices such as firewalls, IDS, IPS and other devices. SASE provides these functions in the cloud. The only thing ACME Corp. needs to do is purchase the SASE solution from a SASE vendor. ACME Corp. can now connect its remote sites, head office’s data center and remote user to the Point of Presence of the SASE vendor. The requirement of this design is the reachability of every site to reach the point of presence. ACME Corp. can even get rid of its Costly MPLS links if they want to. As discussed in the above subsection, 4.4 SASE provides their cloud backbone with a globally distributed network of points of presence.

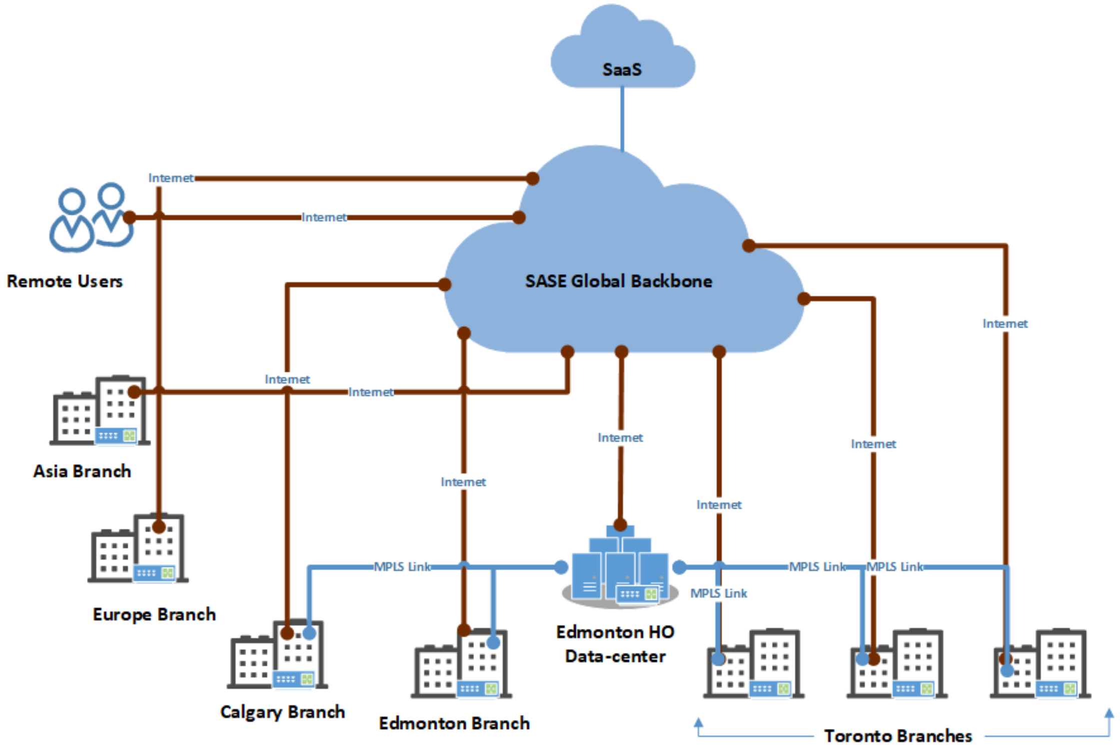


Figure 40: ACME SASE Network

These PoPs connect with the source and other PoPs with IPsec tunnels. ACME Crop.'s remote sites have the CPE installed at their location to connect to their nearest point of presence and access ACME's SASE network, as shown in Figure 40. The remote workers will have the security agents installed on their devices, connecting to the nearest point of presence and authenticating the user with their credentials. SASE vendors also implement multi-factor authentication where a zero-trust security approach is being used. Traffic inspection will be done in the cloud-native software security stack. These security functions work in parallel instead of work as point solutions like in the SD-WAN solution.

Benefits of enabling SASE framework in ACME Corp.:

- ACME is using the SASE cloud backbone that reduces the cost of operation and capital cost. ACME can opt to replace the expensive MPLS links with cheap broadband links.
- The globally distributed network of PoPS enables secure mobility making remote working easy and secure.
- SASE provides better and faster security with its cloud-native security tools.
- Branches and mobile users can access cloud applications securely.

5 Conclusion

Wide area networks are essential as they provide the ability to communicate data over a large geographical distance. WANs enabled the development of data communication technologies and helped in overcoming distance limitations. Legacy WAN technologies enabled communication between two fixed locations. Earlier these technologies supported point-to-point communication, but innovations like circuit and packet switching provided the flexibility for the communication to be dynamic and supported growing networks. MPLS became a popular WAN technology that provided Hub and Spoke model which enabled connectivity of all the branches to the central data center instead of having point-to-point connections. This provided the missing scalability for ever-growing enterprise networks. The use of VPNs also provided a way for the remote workers to connect with branches and access applications hosted in the data-center. However, with increased usage of cloud applications and services, All the traffic for the cloud was backhauled to the central data-center. This backhauling is required to examine the traffic by security equipment hosted at the data-center. This created a problem, MPLS links are expensive and backhauling of all cloud traffic to the data-center and then forwarding it to the cloud resulted in inefficient use of expensive MPLS links.

To address the limitations faced by Legacy WAN technologies such as MPLS and VPNs, SD-WAN comes into the picture. The SD-WAN is a use case of Software-defined networking which came into existence in the 2000s. SD-WAN market moved past the hype phase after implementations started showing tangible results, early adoption of SD-WAN were started in 2017. Multiple SD-WAN vendors exist in the market which offers SD-WAN solutions, as discussed in subsection 4.3. Software-defined WAN proposed decoupling of data and control plane of the network and provided virtual network overlays. It provided secure communication over any type of link either be MPLS, Broadband or LTE. It gave the flexibility of deployment to the enterprises with its different deployment models. Moreover, it provided centralized management of the enterprise network while reducing capital expense and operational expenses. SD-WAN solution has become quite popular in recent years giving the advantages it provides over legacy WAN technologies. SD-WAN solution enable the use of multiple links, intelligent traffic transmission and provide unified policy-driven management. With the global network control SD-WAN provides, large enterprises which are scattered over the large geographical area can better manage their network and resources. SD-WAN has eliminated the scalability and other limitations which come with legacy WAN technologies. SD-WAN triumph over legacy WAN technologies, when it comes to cost and network efficiency, as it provided Network-as-a-Service.

As we compare MPLS and SD-WAN, it is not a fair comparison. As MPLS is a technology that connects the branches with the traditional WAN approach. SD-WAN disrupted that traditional WAN functioning by offering features like centralized management and cloud integration. It has not quite “Replaced” MPLS, however, it utilizes any given transport regardless of its nature, it can MPLS link, broadband or LTE. MPLS provides connectivity while SD-WAN enables a virtual network overlay solution with centralized management using existing connectivity. Replacing MPLS links is totally up to the enterprises, and most of them opt for it because MPLS links are expensive and SD-WAN vendors advocate for replacing MPLS for the same reason.

As we have seen, SD-WAN focuses on connecting enterprise networks to the central data-center. In 2019 Gartner coined the term Secure Access Service Edge (SASE), which made the cloud its focal point in the network instead of the enterprise data-center. The focus has then shifted from SD-WAN toward SASE, as it becomes the driving force for network innovation. As discussed in subsection 4.4 and 4.4.2, SASE is a cloud-based framework to secure WAN. There are two major components to SASE Network-as-a-service and Network Security-as-a-service. SD-WAN is an enabler for SASE as it provides Network-as-a-Service. While network security-as-a-service is enabled by multiple technologies like Cloud SWG, CSAB, FWaaS and many more. SASE advocates putting the cloud at the center of the network. That can make the network securely accessible around the globe to remote branches and workers. The main difference between SD-WAN and SASE is that SD-WAN provides security functions as point solutions while SASE provides security-as-a-service with cloud-native security stack and parallel processing of security functions. SASE Providers are offering a full-fledged cloud-native platform to the enterprises, SD-WAN vendors are developing their SASE platforms, as discussed in subsection 4.4.3 and 4.4.4.

When comparing SD-WAN and SASE, SD-WAN is a solution that decouples network management from the hardware and simplifies a network, while SASE is a cloud-based approach to secure WAN with SD-WAN and cloud-native security stack. Both serve different roles in the enterprise network, where SASE focuses on secure access for the remote workers and the cloud. SD-WAN can be used by enterprises that are looking to simplify their network control and management. The introduction of SASE and the unexpected Coronavirus pandemic has slowed SD-WAN's growth. The pandemic has increased the number of remote workers and with this increase, there is a growing security concern. SASE plays a pivotal role here, as it enables secure the communication of remote workers to the enterprise resources and cloud applications.

Concluding this report, I would state that SASE is relatively new in comparison to SD-WAN and SD-WAN is essential to the SASE platform. Enterprises will keep adopting either SASE or SD-WAN to replace their traditional WAN based on their business requirements. The technological world is everchanging, and we see new technologies developed now and then. We will see a steady growth of SASE and SD-WAN in the near future.

6 Works Cited

[1] D. Kreutz, F. M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," *Proceedings of the IEEE,* vol. 103, no. 1, 2015.

[2] IBM Services, "SDN Versus Traditional Networking Explained," IBM, 09 August 2019. [Online]. Available: https://www.ibm.com/services/network/sdn-versus-traditional-networking.

[3] Mark Duffell, "An update on our September 30 BGP issue," Telstra Exchange, 2 October 2020. [Online]. Available: https://exchange.telstra.com.au/an-update-on-our-september-30-bgp-issue/.

[4] K. Greene, "TR10: Software-Defined Networking," Technology Review, 24 February 2009. [Online]. Available: http://www2.technologyreview.com/news/412194/tr10-software-defined-networking/.

[5] SDxCentral Staff, "What Is an SDN Controller? Definition," SDx Central, 08 October 2019. [Online]. Available: https://www.sdxcentral.com/networking/sdn/definitions/what-is-sdn-controller/.

[6] S. Shenker, "The Future of Networking, and the Past of Protocols - Scott Shenker," Open Networking Summit, 25 October 2011. [Online]. Available: https://www.youtube.com/watch?v=YHeyuD89n1Y.

[7] B. . Pfaff and B. . Davie, "The Open vSwitch Database Management Protocol," , 2013. [Online]. Available: https://tools.ietf.org/html/rfc7047. [Accessed 8 12 2020].

[8] M. Rouse and M. McNickle, "Network Hypervisor," TechTarget, June 2013. [Online]. Available: https://searchnetworking.techtarget.com/definition/network-hypervisor.

[9] M. Casado, "Origins and Evolution of OpenFlow/SDN - Martin Casado," Open Networking Summit, 25 October 2011. [Online]. Available: https://www.youtube.com/watch?v=4Cb91JT-Xb4.

[10] B. Yi, X. Wang, K. Li, S. k. Das and M. Huang, "A comprehensive survey of Network Function Virtualization," *Computer Networks*, vol. 133, 2018.

[11] ETSI GS NFV-MAN 001 , "Network Functions Virtualisation (NFV);Architectural Framework," 2014. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf.

[12] C. Craven, "NFV 101: Networking Foundations Guide," sdxcentral, Denver, 2019.

[13] Wikipedia, "Rack unit," Wikipedia, December 2020. [Online]. Available: https://en.wikipedia.org/wiki/Rack_unit.

[14] M. Rouse and J. A. Miller, "direct-attached storage (DAS)," Techtarget, April 2018. [Online]. Available: https://searchstorage.techtarget.com/definition/direct-attached-storage.

[15] M. Rouse and G. Kranz, "network-attached storage (NAS)," Techtarget, July 2019. [Online]. Available: https://searchstorage.techtarget.com/definition/network-attached-storage.

[16] A. Bednarz, "What is a SAN and how does it differ from NAS?," Networkworld, February 2018. [Online]. Available: https://www.networkworld.com/article/3256312/what-is-a-san-and-how-does-it-differ-from-nas.html.

[17] "Docker," Docker, [Online]. Available: https://www.docker.com/.

[18] S. Gallenmüller, P. Emmerich, F. Wohlfart, D. Raumer and G. Carle, "Comparison of Frameworksfor High-Performance Packet IO," Technische Universität München, Department of Informatics, München, 2015.

[19] D. K. S, "NFV Orchestrator (NFVO)," Cloudify Network, July 2017. [Online]. Available: https://cloudifynetwork.com/nfv-orchestrator-nfvo/.

[20] N. Vyakaranam, "VNF Manager (VNFM)," Cloudify Network, August 2017. [Online]. Available: https://cloudifynetwork.com/vnf-manager-vnfm/.

[21] Nokia, "ETSI VNF resource request options: Direct versus indirect mode explained," Nokia, Espoo, 2016.

[22] Infoblox, [Online]. Available: https://www.infoblox.com/.

[23] NEC, [Online]. Available: www.nec.com.

[24] NFware, [Online]. Available: https://nfware.com/.

[25] Oracle, [Online]. Available: https://www.oracle.com/index.html.

[26] Redhat, [Online]. Available: https://www.redhat.com/en.

[27] 6wind, [Online]. Available: https://www.6wind.com/.

[28] Cisco, [Online]. Available: https://www.cisco.com/.

[29] Ericsson, [Online]. Available: https://www.ericsson.com/en.

[30] Juniper Networks, [Online]. Available: https://www.juniper.net/us/en/.

[31] Nominum, [Online]. Available: https://www.akamai.com/us/en/about/news/press/2017-press/akamai-completes-acquisition-of-nominum.jsp.

[32] F5, [Online]. Available: https://www.f5.com/.

[33] Metaswitch, [Online]. Available: https://www.metaswitch.com/.

[34] Brocade, [Online]. Available: https://www.broadcom.com/.

[35] A. Jahejo, "Wide Area Network | Advantages and Disadvantages of WANs," Computer Network Topology, [Online]. Available: https://computernetworktopology.com/wide-area-network/.

[36] B. Mitchell, "What Is a Wide Area Network (WAN)?," Lifewire, August 2020. [Online]. Available: https://www.lifewire.com/wide-area-network-816383.

[37] J. Fruhlinger and K. Shaw, "What is a WAN? Wide-area network definition and examples," Networkworld, 2020. [Online]. Available: https://www.networkworld.com/article/3248989/what-is-a-wan-wide-area-network-definition-and-examples.html.

[38] Cisco Networking Academy, "WAN Concepts," Cisco Press, 2017. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=2832405&seqNum=5.

[39] B. Vachon and R. Graziani, "Introduction to WANs," in *Accessing the WAN, CCNA Exploration Companion Guide,* Pearson Education, 2008.

[40] M. A. Ridwan, N. A. M. Radzi, W. S. M. W. Ahmad, F. Abdullah, M. Jamaludin and M. Zakaria, "Recent trends in MPLS Networks:Technologies, Applications and Challenges," *IET Research Journals,* vol. 14, no. 2, 2019.

[41] N. Weinberg and J. T. Johnson, "What is MPLS: What you need to know about multi-protocol label switching," Networkworld, March 2018. [Online]. Available: https://www.networkworld.com/article/2297171/network-security-mpls-explained.html.

[42] R. A. Steenbergen, "MPLS for Dummies," nLayer Communications, Inc., [Online]. Available: https://archive.nanog.org/sites/default/files/tuesday_tutorial_steenbergen_mpls_46.pdf.

[43] M. Tripathi, "Multiprotocol Label Switching(MPLS) Explained," towards data science, August 2019. [Online]. Available: https://towardsdatascience.com/multiprotocol-label-switching-mpls-explained-aac04f3c6e94.

[44] INE, "MPLS Components," INE, [Online]. Available: https://blog.ine.com/2010/02/20/mpls-components.

[45] W. J. Goralski, C. Gadecki and M. Bushong, "Label Switching and Label-switched Paths (LSPs)," Dummies, [Online]. Available: https://www.dummies.com/programming/networking/juniper/label-switching-and-label-switched-paths-lsps/.

[46] Wikipedia, "Multiprotocol Label Switching," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching#Operation.

[47] W. J. Goralski, C. Gadecki and M. Bushong, "Types of Label Switching Routers," Dummies, [Online]. Available: https://www.dummies.com/programming/networking/juniper/types-of-label-switching-routers/.

[48] New H3C Technologies Co., "MPLS Technology White Paper," 2020. [Online]. Available: https://downloadcdn.h3c.com/en/202007/24/20200724_5098585_99-book_1316585_294551_0.pdf.

[49] L. D. Ghein, MPLS Fundamentals, Cisco Press, 2006.

[50] Wikipedia, "Label Distribution Protocol," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Label_Distribution_Protocol.

[51] I. Minei, "Tutorial: BGP/MPLS Layer 3 VPNs," TeamNANOG, June 2016. [Online]. Available: https://www.youtube.com/watch?v=VvHk4-lOMwA.

[52] Cisco Press, "IPSec VPN WAN Design Overview," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/IPSec_Over.html.

[53] A. Spadafora, "Remote access VPN: what are they, how do they work and which are the best," Techradar, March 2020. [Online]. Available: https://www.techradar.com/vpn/remote-access-vpn.

[54] Greyson Technlogies, "Remote Access VPN Guide," Greyson Technologies, March 2020. [Online]. Available: https://www.greyson.com/remote-access-vpn-guide/.

[55] Palo Alto, "What Is a Site-to-Site VPN?," Palo Alto, [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn.

[56] P. Kirvan, "Remote access vs. site-to-site VPN: What's the difference?," techtarget, 2020. [Online]. Available: https://searchnetworking.techtarget.com/answer/How-do-site-to-site-VPN-configuration-and-remote-access-VPNs-vary.

[57] M. Lessing, "What is SD-WAN (Software-Defined Wide Area Network)?," SDx Central, 10 March 2020. [Online]. Available: https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/.

[58] Sanjay Uppal; Steve Woo; Dan Pitt, Software-Defined WAN For Dummies®, 2nd VMware Special Edition, Hoboken, New Jersey: John Wiley & Sons, Inc., 2018.

[59] M. C. Smith, "The 3 types of SD-WAN architecture," Networkworld, 25 August 2017. [Online]. Available: https://www.networkworld.com/article/3219653/the-3-types-of-sd-wan-architecture.html.

[60] M. Wood, "SD-WAN Manifesto: Eight Critical Characteristics for Building an SD-WAN," Sdxcentral, 7 October 2016. [Online]. Available: https://www.sdxcentral.com/articles/contributed/sd-wan-manifesto-eight-critical-characteristics-for-building-an-sd-wan/2016/10/.

[61] Z. Kerravala, "The coming together of SD-WAN and AIOps," Network World, 24 March 2020. [Online]. Available: https://www.networkworld.com/article/3533437/the-coming-together-of-aiops-and-sd-wan.html.

[62] C. Craven, "What is SD-WAN Security? Definition," sdxcentral, 07 January 2020. [Online]. Available: https://www.sdxcentral.com/networking/sd-wan/definitions/what-is-sd-wan-security/.

[63] J. Forest, A. Lerner and N. Singh, "Magic Quadrant for WAN Edge Infrastructure," Gartner, 23 September 2020. [Online]. Available: https://www.gartner.com/doc/reprints?id=1-248C06C6&ct=200924&st=sb.

[64] D. Hughes, "Silver Peak Named a Leader in 2019 Magic Quadrant for WAN Edge Infrastructure," Silver Peak, [Online]. Available: https://blog.silver-peak.com/2019-gartner-sd-wan-edge-magic-quadrant.

[65] SDxCentral Studios, "What is the Silver Peak SD-WAN Approach?," SDxCentral, 25 September 2017. [Online]. Available: https://www.sdxcentral.com/networking/sd-wan/definitions/silver-peak-sd-wan-approach/.

[66] Silverpeak, "Making the Shift to a Business-First Networking Model," Silverpeak, [Online]. Available: https://www.silver-peak.com/resource-center/making-shift-business-first-networking-model.

[67] Silver Peak, "Unity EdgeConnect SD-WAN Edge Platform," Silver Peak Systems, Inc, 2020. [Online]. Available: https://www.silver-peak.com/sites/default/files/infoctr/silver-peak-datasheet-unity-edgeconnect-sd-wan-solution.pdf.

[68] Silver Peak, "Unity Orchestrator," Silver Peak Systems, Inc, 2019. [Online]. Available: https://www.silver-peak.com/sites/default/files/infoctr/sp-datasheet-unity-orchestrator-solution-0419.pdf.

[69] Tech Field Day, "Silver Peak Unity EdgeConnect SD-WAN Overview," Tech Field Day, January 2016. [Online]. Available: https://www.youtube.com/watch?v=y3uFxfZ111A.

[70] VMware Inc., "VMware SD WAN," 2020. [Online]. Available: https://wan.velocloud.com/rs/098-RBR-178/images/sdwan-542-vmware-sdwan-by-velocloud-overview-so-1020.pdf.

[71] C. Craven, "What is the VMware SD-WAN Approach?," SDxCentral, 7 November 2019. [Online]. Available: https://www.sdxcentral.com/networking/sd-wan/definitions/vmware-sd-wan/.

[72] Velocloud by VMware, "Cloud Delivered Simplifies SD-WAN," [Online]. Available: http://wan.velocloud.com/rs/098-RBR-178/images/sdwan-822-cloud-delivered-simplifies-sdwan-so-0220.pdf.

[73] VMware Inc., "A Guide to SDN, SD-WAN, NFV, and VNF," [Online]. Available: https://sdwan.vmware.com/content/dam/digitalmarketing/velocloud/en/documents/208805aq-so-vcloud-guide-sd-wan-nfv-vfn-uslet-web.pdf.

[74] VeloCloud by VMware, "Enterprise WAN Agility, Simplicity, Performance with SD-WAN," VMware Inc, 2019. [Online]. Available: https://sdwan.vmware.com/content/dam/digitalmarketing/velocloud/en/documents/brief-enterprise-wan-agility-simplicity-performance.pdf.

[75] VMware, "VMware Hands-on Labs - HOL-2039-01-NET," VMware Inc, [Online]. Available: https://docs.hol.vmware.com/HOL-2020/hol-2039-01-net_html_en/.

[76] Fortinet, "Fortinet Secure SD-WAN Reference Architecture," Fortinet, 2019. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/document-library/ra-sd-wan-reference-architecture.pdf.

[77] Tech Field Day, "Fortinet SD-WAN Architecture & Demo," Tech Field Day, February 2019. [Online]. Available: https://www.youtube.com/watch?v=lS1F5gsyIAI.

[78] Fortinet, "The Network Leader’s Guide toSecure SD-WAN," Fortinet, 2019. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/ebook/eb-network-leaders-guide-to-SD-WAN.pdf.

[79] SDxCentral Studios, "What is the Cisco SD-WAN Approach?," SDxcentral, August 2017. [Online]. Available: https://www.sdxcentral.com/networking/sd-wan/definitions/cisco-sd-wan/.

[80] SDxCentral Studios, "What Is the Viptela SD-WAN Approach?," SDxCentral, September 2017. [Online]. Available: https://www.sdxcentral.com/networking/sd-wan/definitions/viptela-sd-wan-approach/.

[81] Cisco, "Cisco SD-WAN," Cisco, 2019. [Online]. Available: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf.

[82] C. Craven, "SASE 101," 2020. [Online]. Available: https://www.sdxcentral.com/security/definitions/sase-101-getting-started-guide/.

[83] N. MacDonald, L. Orans and J. Skorupa, "The Future of Network Security Is in the Cloud," Gartner, 2019.

[84] D. Sullivan and M. Bacon, "cloud access security broker (CASB)," TechTarget, [Online]. Available: https://searchcloudsecurity.techtarget.com/definition/cloud-access-security-broker-CASB.

[85] McAfee, "What Is a CASB?," McAfee, [Online]. Available: https://www.mcafee.com/enterprise/en-ca/security-awareness/cloud/what-is-a-casb.html.

[86] McAfee, "What Is a Secure Web Gateway?," McAfee, [Online]. Available: https://www.mcafee.com/enterprise/en-ca/security-awareness/cloud/what-is-secure-web-gateway.html.

[87] S. Gittlen, "What is zero trust? Ultimate guide to the network security model," TechTarget, [Online]. Available: https://searchsecurity.techtarget.com/definition/zero-trust-model-zero-trust-network.

[88] Signal Sciences, "The Ultimate Guide to Web Application and API Protection (WAAP)," Signal Sciences, [Online]. Available: https://www.signalsciences.com/glossary/web-application-api-protection/.

[89] Zscaler, "What is Firewall as a Service?," Zscaler, [Online]. Available: https://www.zscaler.com/resources/security-terms-glossary/what-is-firewall-as-a-service.

[90] Checkpoint , "What is Firewall as a Service (FWaaS)?," Check point software technologies, [Online]. Available: https://www.checkpoint.com/cyber-hub/network-security/firewall-as-a-service-fwaas/.

[91] Zscaler, "What is Remote Browser Isolation?," Zscaler, [Online]. Available: https://www.zscaler.com/resources/security-terms-glossary/what-is-remote-browser-isolation.

[92] C. Craven, "What is the Cato Networks SASE Platform?," sdxcentral, June 2020. [Online]. Available: https://www.sdxcentral.com/security/sase/definitions/what-is-cato-networks-sase-platform/.

[93] Cato Networks, "Secure Access Service Edge (SASE)," Cato Networks, [Online]. Available: https://www.catonetworks.com/sase.

[94] Cato Networks, "Global Private Backbone," Cato Networks, [Online]. Available: https://www.catonetworks.com/cato-sase-cloud/global-private-backbone-3/.

[95] Cato Networks, "Security as a Service," Cato Networks, [Online]. Available: https://www.catonetworks.com/cato-sase-cloud/enterprise-grade-security-as-a-service-built-directly-into-the-network/.

[96] Cato Networks, "Optimized and Secure Remote Access," Cato Networks, [Online]. Available: https://www.catonetworks.com/cato-sase-cloud/optimized-and-secure-remote-access/.

[97] C. Craven, "What is the Cisco SASE Platform?," sdxcentral, June 2020. [Online]. Available: https://www.sdxcentral.com/security/sase/definitions/what-is-cisco-sase-umbrella-viptela-and-duo/.

[98] Cisco Umbrella, "Secure Access Service Edge (SASE)," Cisco, 2020. [Online]. Available: https://umbrella.cisco.com/trends-threats/secure-access-service-edge-sase.

[99] J. Cavanaugh, "Top 5 SASE use cases balance network connectivity, security," TechTarget, January 2021. [Online]. Available: https://searchnetworking.techtarget.com/tip/Top-5-SASE-use-cases-balance-network-connectivity-security.