UNIVERSITY OF ALBERTA

Master of Science in Internetworking

Capstone Project Report

On

Technical analysis of various vendor SD-WAN offering

By **Jatin Kharub**

Under the supervision of

Mr. Juned Noonari

Introduction

The Internet is the most powerful tool anyone can think of right now. The amount of information available there is simply unthinkable. From learning a piano to watching live matches, there is a vast amount of information and data available. Nowadays, even news reaches fast over the internet than the news channels. Schools have become online, exams are being taken on zoom, and even job interviews are being held on video calls. Without it, companies would shut down, millions would become jobless, and the world would apparently come to a halt. This shows the importance of being connected to the Internet.

WAN is one of the integral parts of Internet deployment. And this project focuses on the technology SD-WAN (Software-Defined WAN), which makes WAN even better. It will involve a detailed study of SD-WAN and will also investigate the various solutions provided by different vendors and will conclude with the study of clouds and their offerings.

About Myself

My name is Jatin Kharub, and I am from a small city (Rohtak) in the center of Haryana, India. From a young age, I was always interested in technology, mobile phones, and computers. I also used to watch shows which focused on technology. So, I decided to go for the science side for my Senior Secondary Education.

After that, I took Computer Science for my bachelor’s and moved to a different state to get admission to a better University. There I learned a lot of things that I wouldn’t have if I had stayed in my hometown. After completing my bachelor’s, I wanted to learn even more, and hence, I decided to do my master’s. I decided to go to Canada because of the quality of education and the opportunities to learn a lot.

Apart from studies, I have always been interested in sports. Even during my Bachelor’s, I was a part of the college and the department soccer team. We participated in many tournaments and even won a few. I was not just limited to soccer. I also played Cricket, Basketball, Badminton, Volleyball, and many other sports. I also like astronomy and similar stuff.

I hope to keep learning even after my studies. I would like to keep myself updated while being on the job. I also intend to keep myself physically fit always as it keeps me motivated to achieve more and more in life.

Acknowledgment

I would like to express my sincere appreciation to all those people who have helped me to get where I am today. I would like to thank my friends who have always motivated me to go higher and higher in life. I would like to thank all my old classmates who have always helped me academically and personally.

I would also like to thank **Mr. Shahnawaz Mir** and **Dr. Mike McGregor** for helping me to select a topic for my project. I also thank all my classmates, staff members, instructors, and professors at the University of Alberta who have helped me for the past two years.

I would also like to thank my mentor **Mr. Juned Noonari** for taking time out of his busy life to help me with my project. Without his knowledge and guidance, this report would not have been possible.

Finally, I would like to thank my family, especially my parents, for supporting and encouraging me in every decision in my life. I can't even imagine what my life would be like without their support.

Jatin Kharub

Abstract

In the world of ever-growing business, it is expected that WANs will provide even better functionalities in the future. WANs have their connection, security, and network information programmed directly into the device. But with a strategy of providing a software overlay for connection provisioning and management, we can improve the deployment and management of a WAN, thus making them more efficient. This strategy is used in Software-Defined WAN (SDWAN) [1].

In the future, we will need networks that provide better QoS, easy network management, and high-cost efficiency. SD-WAN has been the one that is widely regarded as the successor of existing WANs. The main objective of SD-WAN is to simplify networking operations, optimize WAN management and make the network more flexible as compared to the current WANs so that the network becomes more efficient [2].

Table of Contents

Section 1: Software-Defined Networking

1.1 WAN

WAN (Wide Area Networks) have been fundamental in providing internet access across large geographical areas. As mentioned earlier, in today's world Internet is essential even for basic tasks. We have relied on WAN for decades now, and even in the future, we might continue to use WAN with enhanced functionalities.

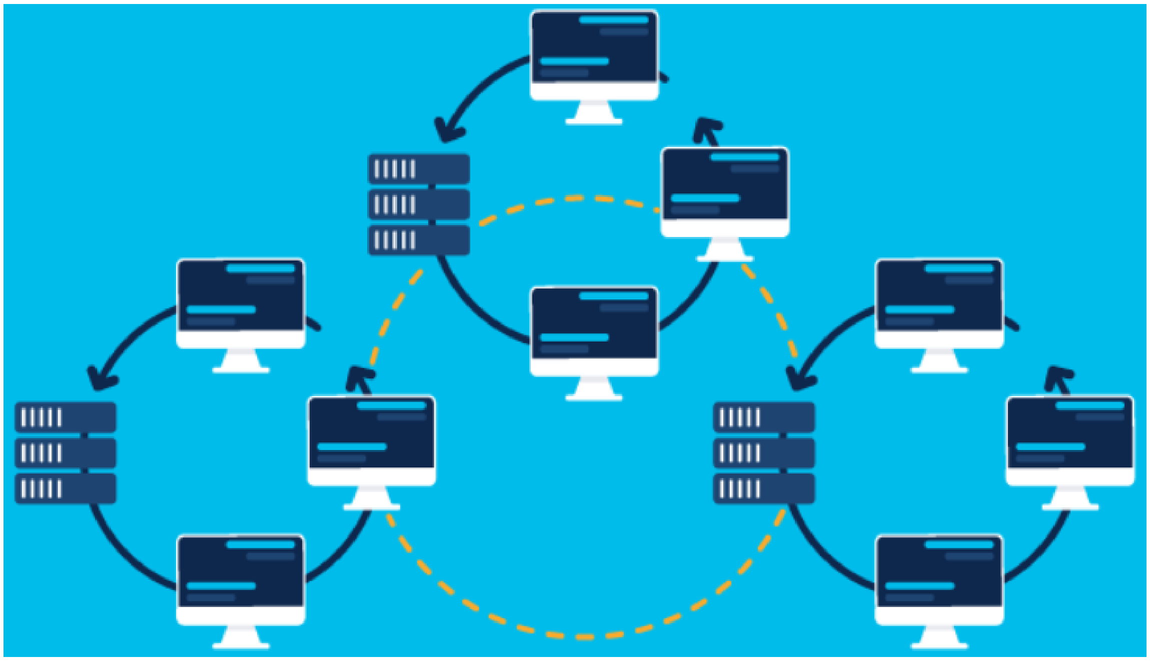


Figure 1: Simple representation of WAN *[3]*

It started in the 1950s when the US Air Force used it for defense in their radar systems. Lots and lots of physical devices like modems, phone lines, telephones were used to establish the connection. Suppose we compare it to today's scenario, many would-be shocked by seeing the amount and sizes of the equipment that they used. But it all laid the strong foundation for what would be used in the future. ARPANET (Advanced Research Projects Agency Network) became the first wide area network. It was the first packet-switching wide area network that implemented the TCP/IP protocol suite. ARPANET connected various universities with each other, namely the University of California, Los Angeles (UCLA), Stanford Research Institute (SRI International), University of California, Santa Barbara (UCSB), and the University of Utah [3].

Jump to the 1970s, the use of WAN mainly consisted of connecting two separate locations in the same city. This was the time when the best option to go for speed was the 9.6 kbps line, and constant improvements were being made regularly to increase the speed. Packet-switched networks led to more efficiency, and it was also economical to use, as they allowed people to pay per usage. Then in the 1990s, various other technologies came into play. Frame Relay, ATM (Asynchronous Transfer Mode), MPLS (Multi-Protocol Label Switching) came into existence and changed the WAN in many ways [4]. We will investigate all these later.

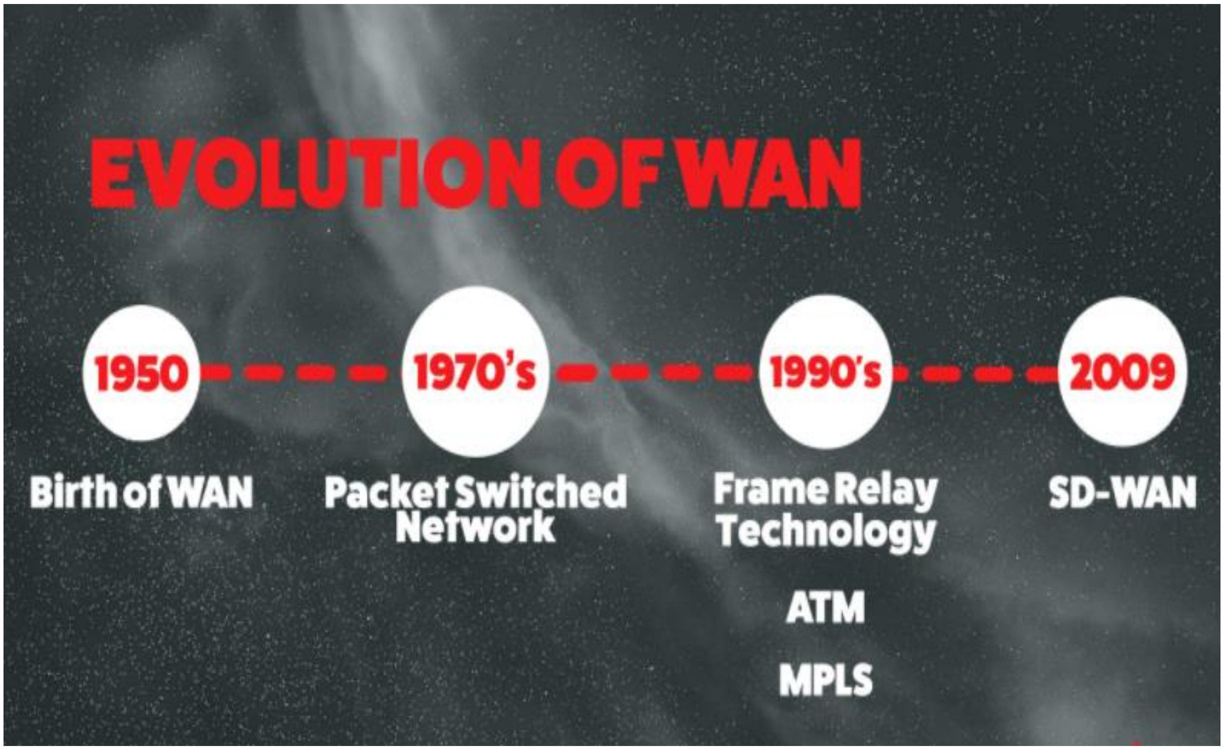


Figure 2: How WAN evolved *[4]*

Now let us have a look at various WAN technologies:

1.1.1 Packet Switching

In simple terms, Packet switching refers to breaking the information into several parts, called packets, before transmission and then transmitting each part separately. These parts are then put together at the destination. Each packet contains a header, which includes information like source and destination IP addresses, the number of packets, and the sequence number. Packet switching makes the transmission more efficient [5].

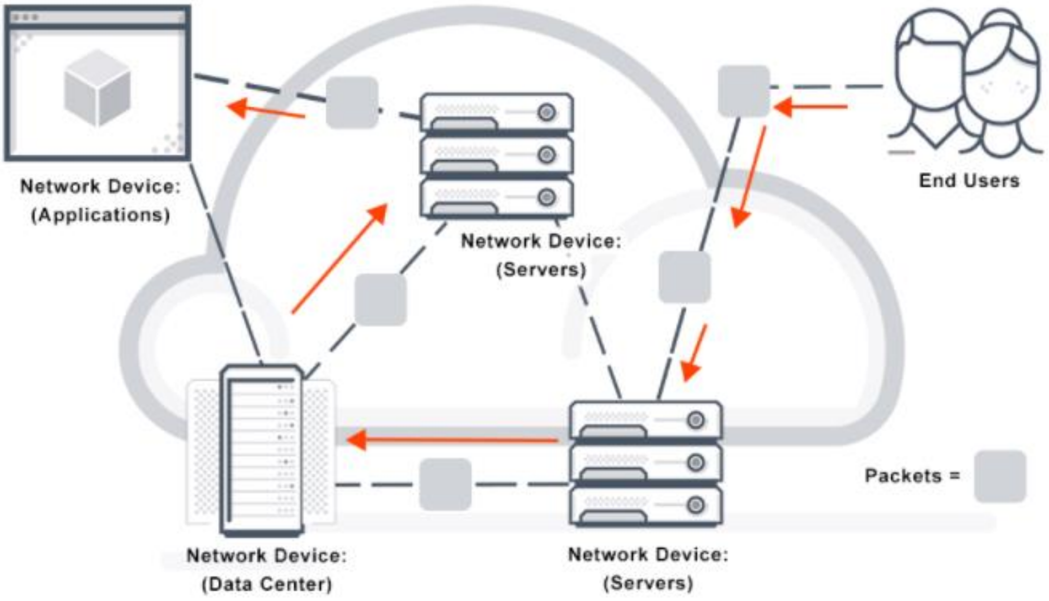


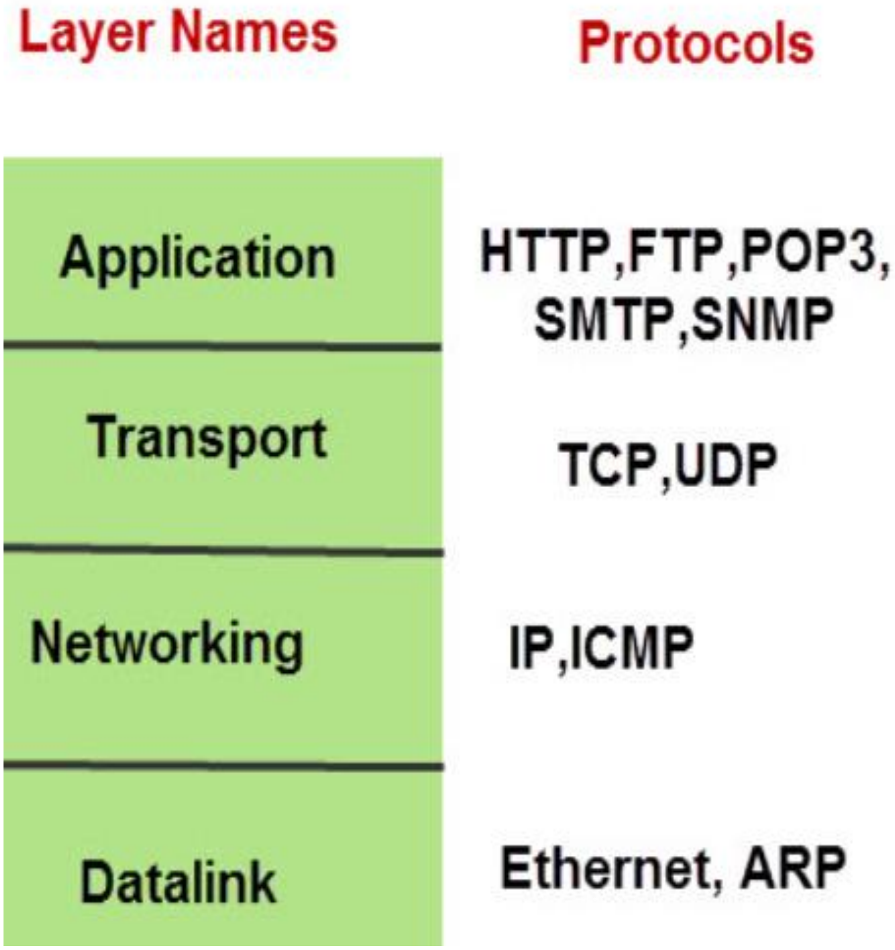
Figure 3: Packet Switching *[5]*

Packet switching can either be Connectionless or Connection-oriented. In Connectionless Packet Switching (also known as Datagram Switching), each packet has a header containing source and destination IP addresses, the total number of packets, and the sequence number. Then the packets are sent, and they may take different paths and may not be sent in order. At the destination, the packets are arranged in the correct order with the help of a sequence number. Whereas in the case of Connection-Oriented Packet Switching, the route is already defined, and the packets are also numbered and assembled. Then the packets are sent in a sequential manner, which eliminates the need for any address information [5].

Packet switching has many benefits. It is efficient as it leads to less network bandwidth usage, less latency leads to more speedy networks. Also, when a path goes down, the packets can reach the destination via a different route. It is also cost-effective and not very complex to implement [5].

1.1.2 TCP/IP Protocol Suite

TCP/IP stands for Transmission Control Protocol/Internet Protocol. This suite contains many protocols which operate at the four layers in TCP/IP model, namely the Datalink layer, Networking layer, Transport layer, and the Application layer. They are used to provide connections to various network devices to each other and the Internet [6].



Layer Names	Protocols
Application	HTTP,FTP,POP3, SMTP,SNMP
Transport	TCP,UDP
Networking	IP,ICMP
Datalink	Ethernet, ARP

Figure 4: TCP/IP Model *[6]*

1.1.3 Router

A router is simply a device that uses an IP address to forward a packet in the network. It is generally called a WAN device as it is used to connect LANs to increase the coverage area to form a wide area network [3].

Figure 5: A router *[7]*

What a router does is simply connect devices together by forwarding data packets between them; it can either be between different devices or even the internet. In today’s words, almost every house has multiple devices. These devices need to be connected to each other and the internet, and this is where the router comes in. In connecting to the internet, even if you want to share files between local devices, a router is also helpful [7].

It must be noted that a router can either be wired or it can be wireless. In the case of a wired router, the connection can only be made by the LAN cable ports, whereas in the case of wireless routers, there is no need for a cable as the name suggests; instead, they have antennae and wireless adapter [7].

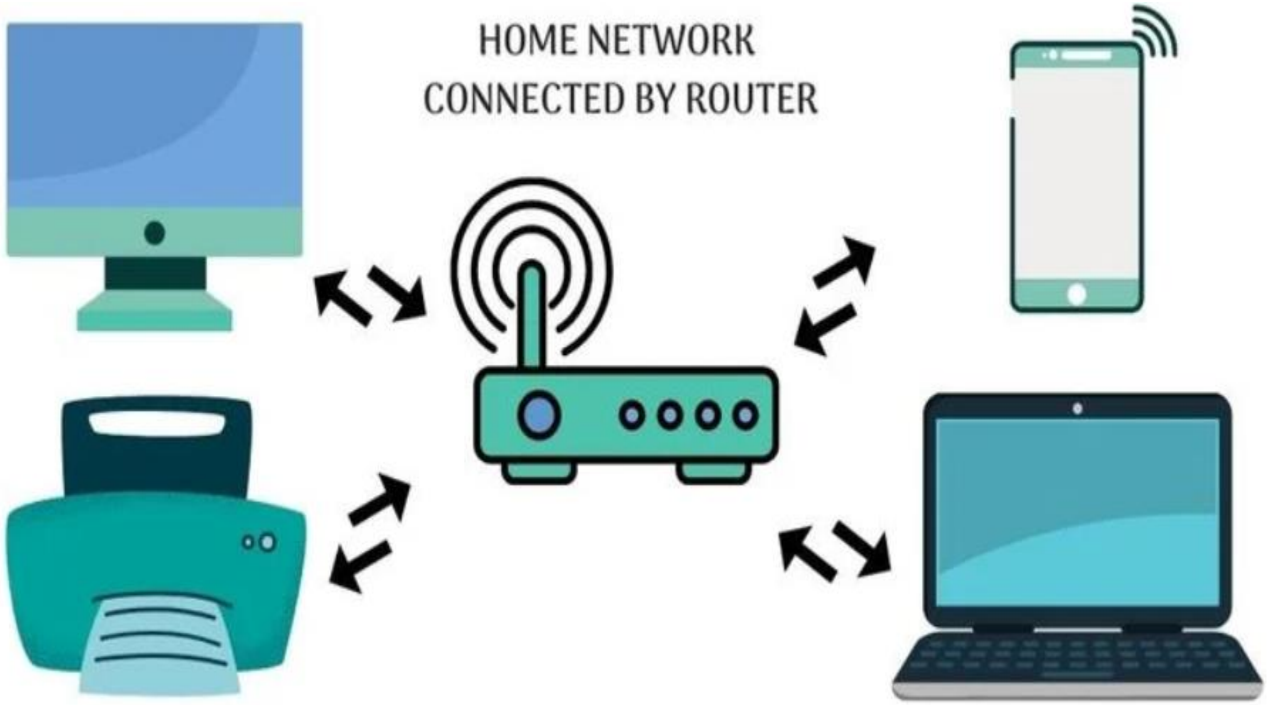


Figure 6: How a router works *[7]*

1.1.4 Overlay Network

When software is used on top of an existing network, it is called an overlay network, which supports the functionalities which are not supported on the existing underlying network. It simply creates a sort of virtual network over another network [3].

It has certain advantages. Firstly, overlay networks make it easier to create and implement protocols conveniently on the web. Also, it increases the flexibility in data routing. And it also enables the addition of a new service or a feature, with no need to reconfigure the whole network or device, and there are also fewer restrictions due to the physical networks. But there are some downsides also. The main problem is the increased complexity. The performance overhead is increased, and the encapsulation and de-encapsulation process leads to an increased number of computations. Also, the physical network does not necessarily adjust to the changes made due to the addition of an overlay network [8].

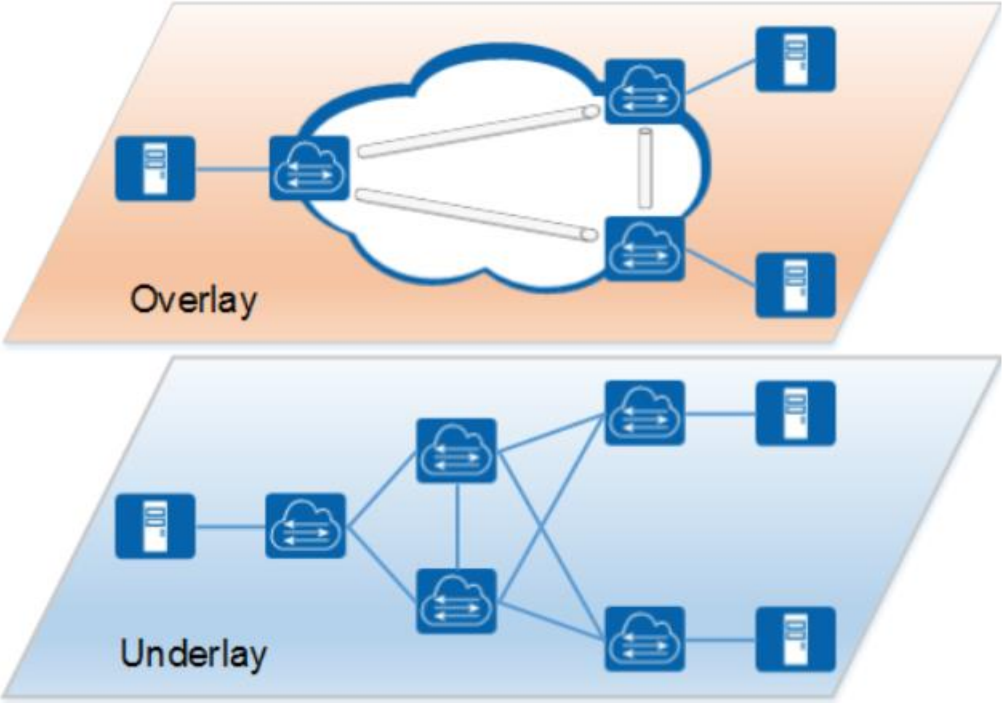


Figure 7: Overlay Network visualization *[9]*

1.1.5 Packet over SONET (PoS)

Packet over SONET is a communication protocol that defines how the communication takes place via point-to-point links when the optical fiber is used along with SONET (Synchronous Optical Network) communication protocols [3].

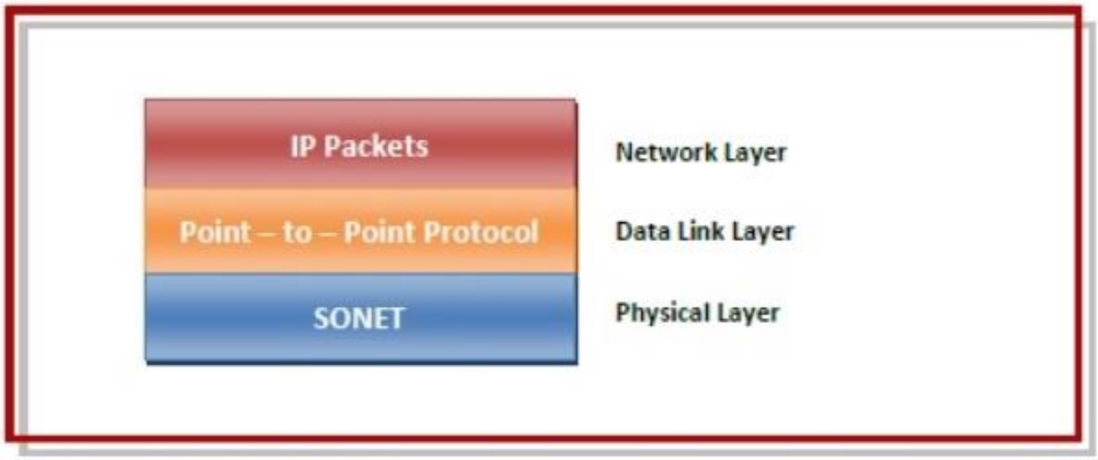


Figure 8: PoS *[10]*

In PoS, PPP (Point-to-Point Protocol), a protocol that is used for transmission between two directly connected devices, runs on IP routers. PPP does the encapsulation of datagram in frames before transmission, which helps in error detection. It also provides Link Control Protocol (LCP) which takes care of the links in transmission. It also provides Network Control Protocols (NCPs) to negotiate the parameters and facilities for the network layer. Applications of PoS include sending a huge amount of data over the internet and transmission of IP packets over WANs [10].

1.1.6 MPLS

Multi-Protocol Label Switching is a technique in which the packets are sent with the help of labels instead of looking into the routing tables for IP addresses. This process makes the transmission faster as the complex routing tables need not be searched. These labels are taken care of by the Label Switch Routers (LSR). It uses Internet Protocol and a router to transfer packets and add an MPLS header to the packets. The header contains Label, Exp (for Quality of Service), Bottom of Stack bit (to determine if the current label is the last one or not), and Time To Live bit (prevents the packet from getting stuck in the network). MPLS does not fit correctly in just one layer, it kind of fits in-between both. Due to this reason, MPLS is a Layer 2.5 protocol [11].

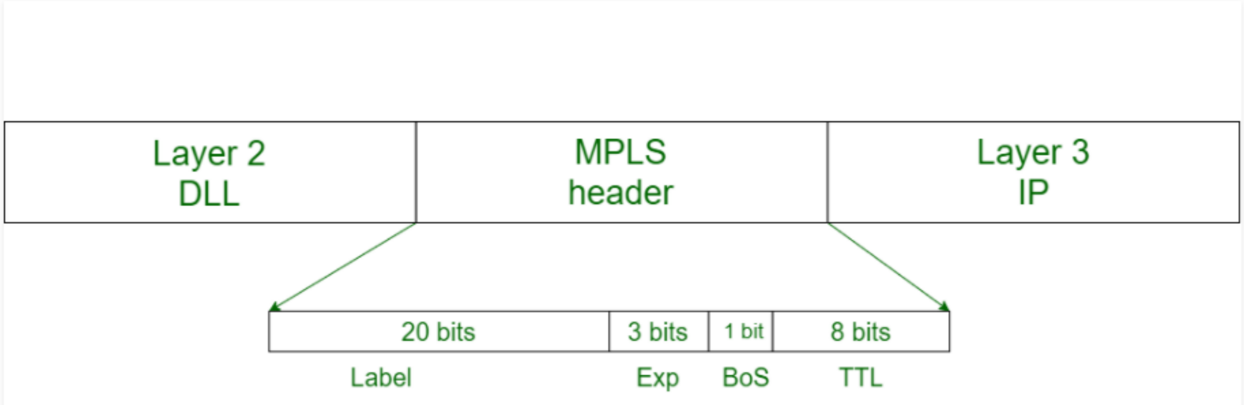


Figure 9: MPLS Header *[11]*

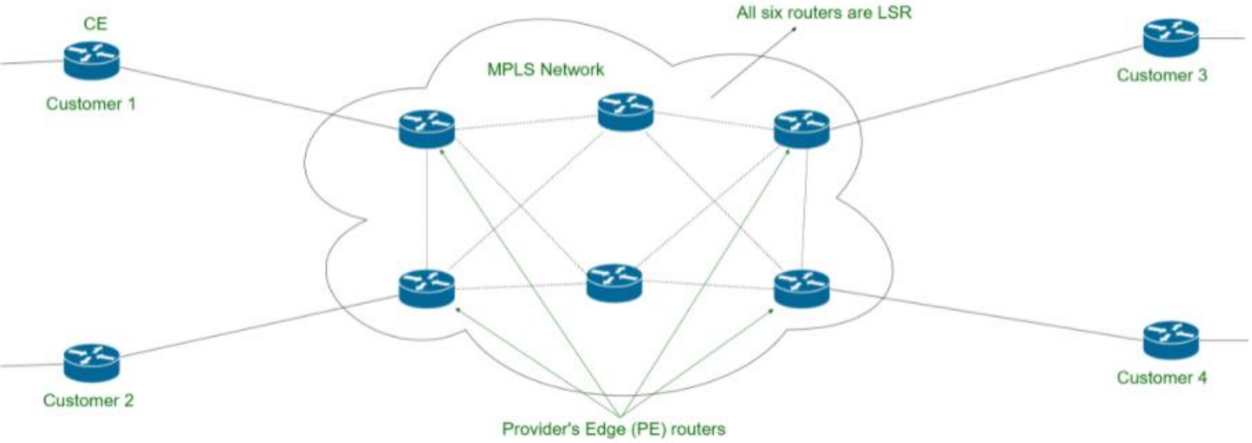


Figure 10: MPLS Network *[11]*

Instead of routing tables, MPLS has Label Forwarding Information Base (LFIB), which helps in forwarding data. When the routers receive a packet, they look at the label and LFIB to forward the packet further [11]. Whenever a packet enters the MPLS 'cloud', the LSR puts a label on it, and as it goes deeper into the network, labels keep on getting stacked one over the other. These labels are then removed in the same order that they were stacked, and the last label is removed when it finally leaves the MPLS network. This is how packets are forwarded using MPLS.

1.1.7 ATM

Asynchronous Transfer Mode is an outdated switching technology that was used to encode the data into fixed-sized cells using asynchronous time-division multiplexing (TDM) [3].

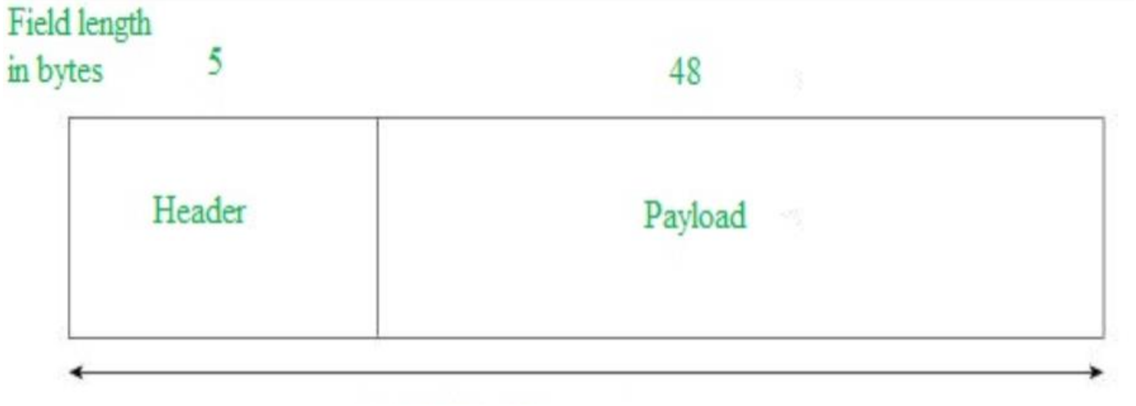


Figure 11: ATM Cell Format *[12]*

As seen from the above diagram, the size of each cell is constant, i.e., 53 bytes.

Now ATM can be of two types, namely UNI (User-Network Interface) and NNI (Network to Network Interface) [12].

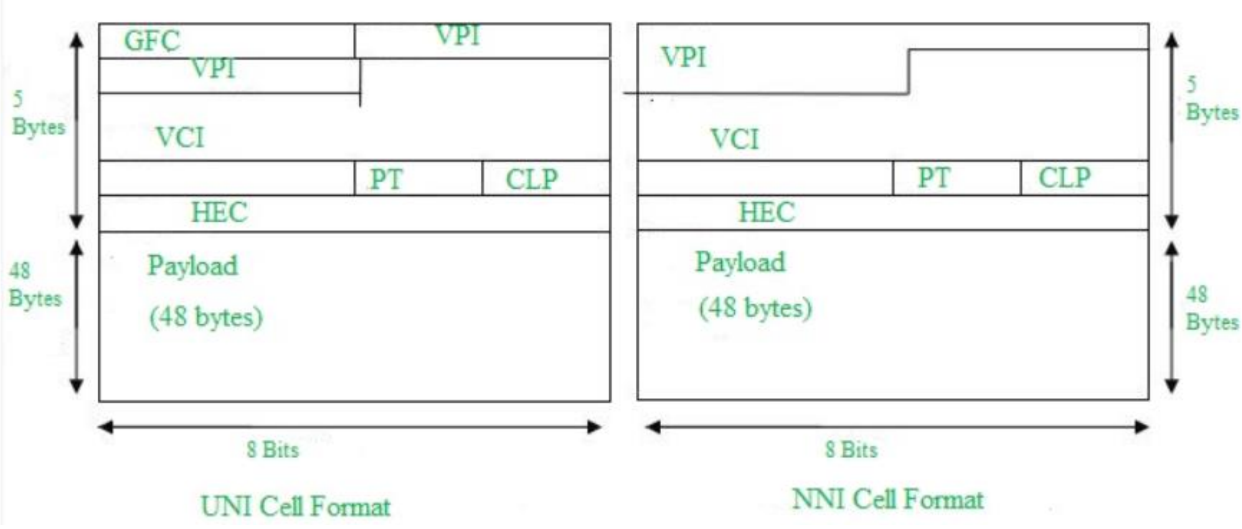


Figure 12: UNI vs NNI *[12]*

As seen from the above diagram, there is a GFC field in the case of UNI but not in NNI. This is the Generic Flow Control field. The main difference between UNI and NNI is that UNI is used for communication between ATM endpoints and ATM switches inside privately-owned networks, whereas NNI is used for the communication of ATM switches with each other [12].

Now let us look at the different layers of ATM.

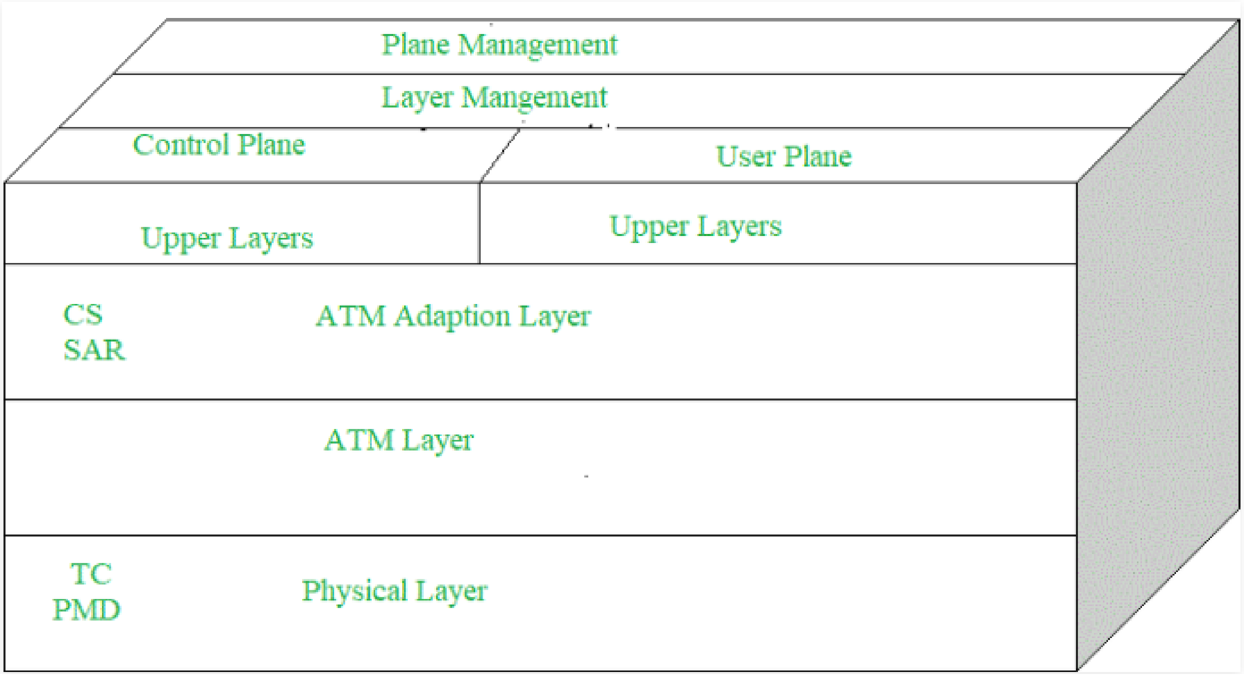


Figure 13: ATM Layers *[12]*

ATM Adaption Layer (AAL) prepares the changing of user data into cells and further into 48-byte payloads while also accepting transmission from higher-layer services, helping them in mapping applications to ATM cells. ATM layer is responsible for taking care of transmission, switching, congestion control, etc., and cell multiplexing and cell relay. The physical layer is used for the conversion of cells into a bitstream, controlling the transmission in the physical medium and packaging the cells into suitable types of frames [12].

ATM supports voice, video, and data communications. Dynamic bandwidth is provided, so there is no problem in case of bursty traffic. Fixed packet size means that traffic is handled efficiently, and the small size of the header means effective bandwidth usage by reduced packet overload. As the name suggests, cells are only sent when necessary, unlike in the case of synchronous lines [13].

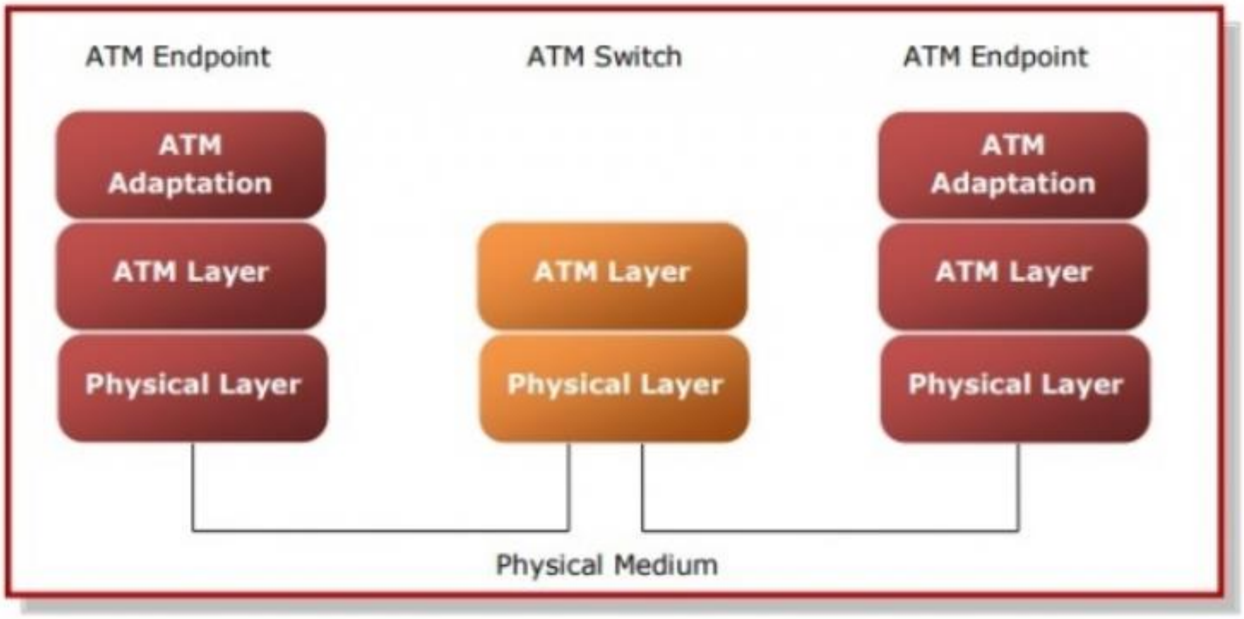


Figure 14: ATM Reference Model *[13]*

1.1.8 Frame Relay

Frame Relay is a protocol that comes under Layer-2 (data link layer) in the OSI model. It is a packet-switching protocol that connects Local Area Networks and is used for data transmission across Wide Area Networks. It contains a congestion control mechanism to reduce congestion, but it lacks error control and flow control mechanisms [14].

Now let us see how a frame relay works. It sets up a virtual connection to connect different LANs, which makes a WAN. The data is then divided into packets, called frames, and these frames are sent between LANs across WAN. The network is set up between the LAN border devices, where each LAN has an access point connecting the LAN to the service provider network, and this access link is the physical link that connects the LAN networks over WAN. There is a frame relay switch whose job is to terminate the access links and provide frame relay services. The router in LAN sends frames over the access link, then the frame relay switch identifies the destination for it by examining the Data Link Connection Identifier (DLCI), as it already has the LAN addresses information for the network. DLCI does the configuration and transmission of frames to the destination LAN frame relay switch, which then transmits the frames to the correct access link and the frames reach their destination. So, multiple LANs are connected to each other via a single shared physical link [14]. The following diagram shows what a frame relay network looks like.

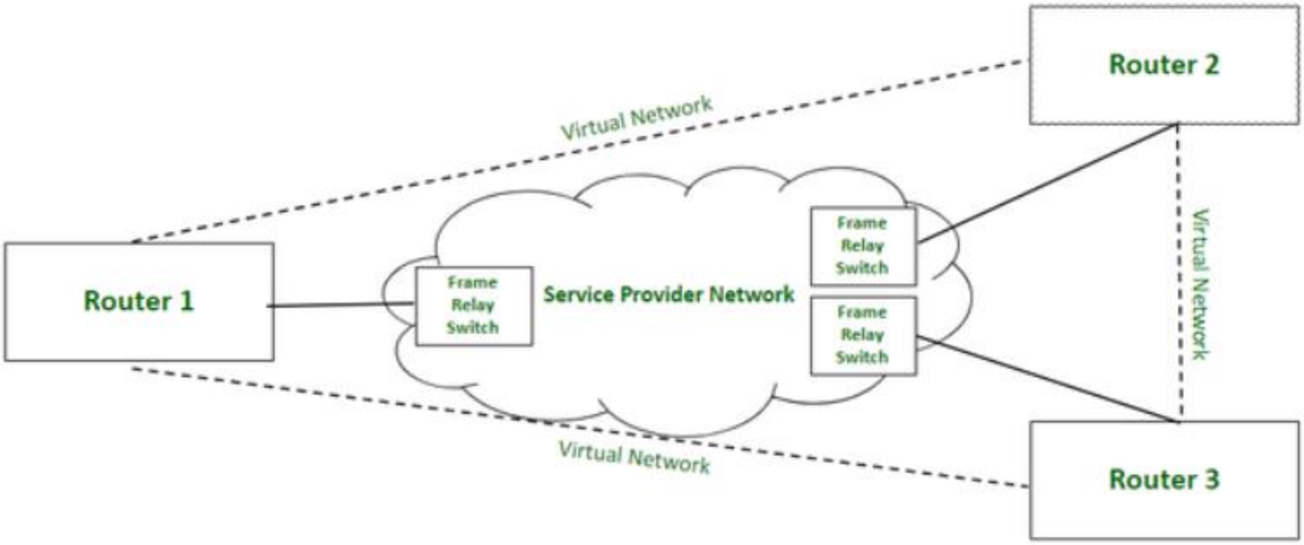


Figure 15: Frame Relay Network *[14]*

As mentioned earlier, there is a provision for congestion control. To identify congestion, there are multiple methods. The first one is FECN (Forward Explicit Congestion Network), which is a part of the frame header. When there is congestion, the frame relay switch of the destination network sets the FECN bit, which tells the destination that there is congestion. The second one is BECN (Backward Explicit Congestion Network), in which, instead of the destination, the source becomes aware of the congestion. In case of congestion, the frame is sent back to the source with a set BECN, and the source comes to know about the congestion, which slows down the transmission process. The third one is DE (Discard Eligibility) which tells the priority to discard the packets. In the case of network overheads, packets with set DE bits are discarded before the ones with unset DE bits [14].

The connections can be of two types, either PVC (Permanent Virtual Circuit) or SVC (Switched Virtual Circuit). In the case of PVC, the connection between the frame relay nodes is permanent and for longer periods of time, unlike SVC, where the connections are temporary and only till the time the nodes are communicating with each other then it is closed. The connections in PVC are static but dynamic in the case of SVC [14].

There are certain advantages of using frame relay networks. The networks generate high speeds, and they are scalable and cost-efficient. Also, there is reduced network congestion, and the connection is secure. But the downsides include delays in packet transfer and a less reliable network. There is no error control mechanism also [14].

1.2 SDN

SDN stands for Software-Defined Networking. It is a technique that uses software to control and communicate with the underlying hardware infrastructure with the help of a centralized server. So, it is different from a traditional network in the sense that the traditional ones control the traffic using hardware, but SDN does so via software [15].

1.2.2 Principles of SDN

There are four principles of SDN. These are:

1. Centralized Management: In the case of a non-centralized network, it is not easy to push updates or compare traffic and performance. SDN takes care of these problems by centralizing the management, which makes it easier to make changes from a centralized server [16].
2. Network Automation: Without automation, while setting up a server, there are many tasks to be done. Allocating CPU, memory, and storage resources, taking care of firewalls, and many more. But SDN takes care of all this by automation. All the network and security parameters are automated, which takes away the need to configure all these manually [16].
3. Network Abstraction: Network abstraction builds on network automation, allowing the services to be delivered in any part of the network. SDN does the abstraction using intelligent software, allowing services to be delivered uniformly anywhere on the network [16].
4. Programmability: SDN provides programmability through APIs, which allows SDN functions to be scripted to make the deployment of workload faster, and the openness of APIs leads to collaboration with other similar programs [16].

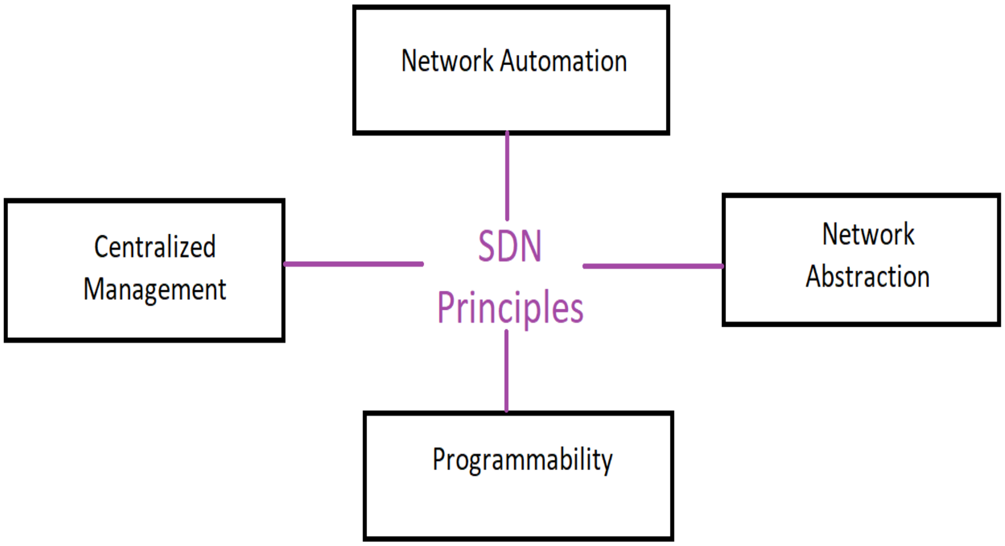


Figure 16: SDN Principles

1.2.1 SDN Architecture

As seen from the following diagram, SDN architecture is a three-tiered architecture. At the top is the Application tier, followed by the Controller in the middle and at the bottom is the Data Plane tier. The Northbound API interface describes the connection with the higher-level component, and its interface present on the controller lets the applications and the management system program the network and request services. There is no standardization for the Northbound API, and the reason for that is the various types of applications above the controller, some of which include managing cloud computing systems and network virtualization schemes [17].

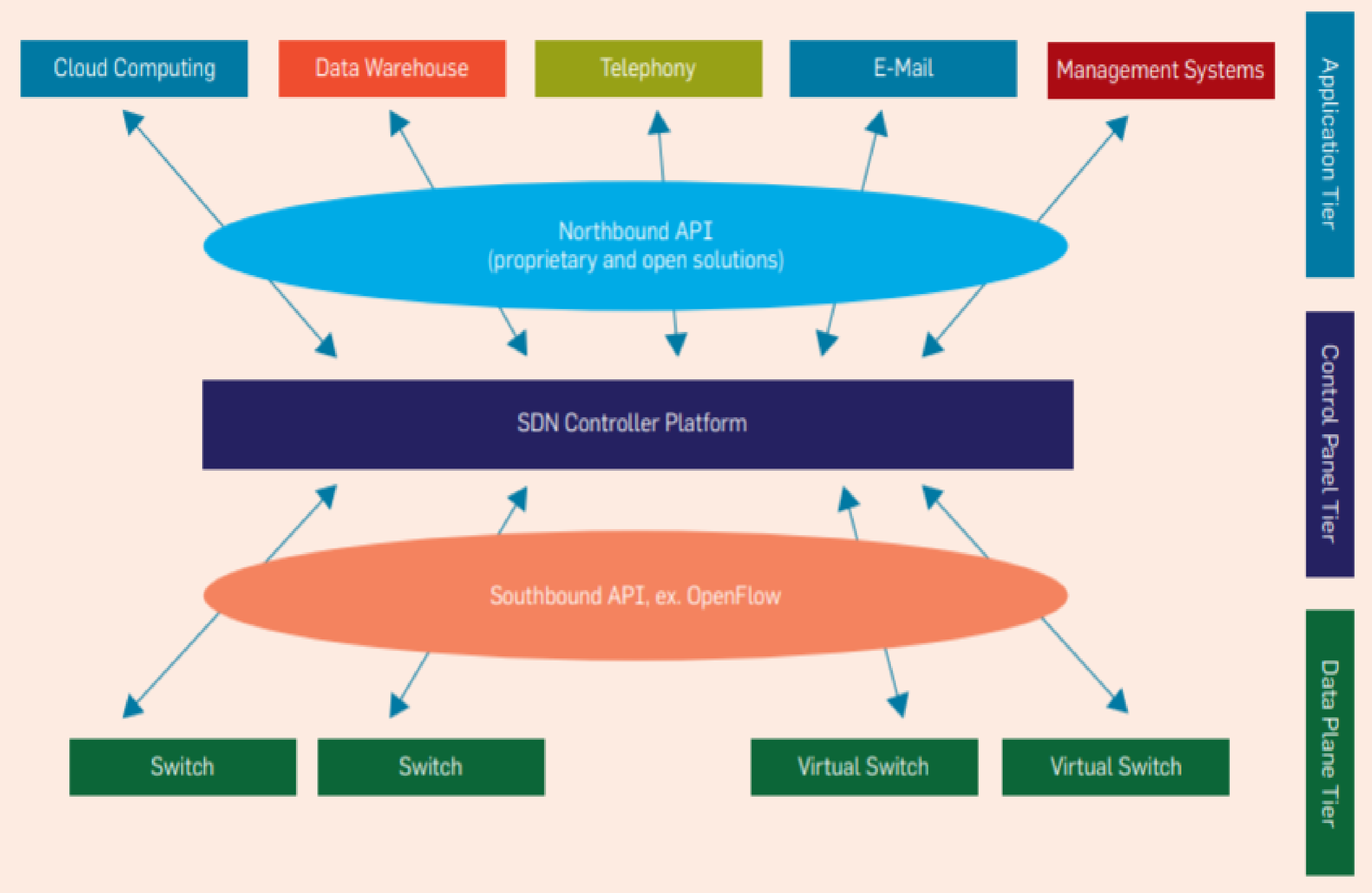


Figure 17: SDN Architecture *[17]*

The Southbound API allows the communication between a specific component in a network and a lower-level component. OpenFlow is the generally used protocol (not necessary) that helps in forwarding the data by defining a set of open commands. The commands provide the routers with the topology of the network, and they can also define the behavior of the switches (both physical and virtual) based on the requests requested via the Northbound APIs [17].

There are three types of fundamental abstractions in SDN, forwarding, distribution and specification. **Forwarding abstractions** hide the details of the underlying infrastructure while allowing the desired forwarding behavior. **Distributed abstraction** protects the applications of SDN from the unpredictability of the distributed state. The third one is the **Specification abstraction**, which allows the network applications to express their desired behavior without being responsible for their implementation [18].

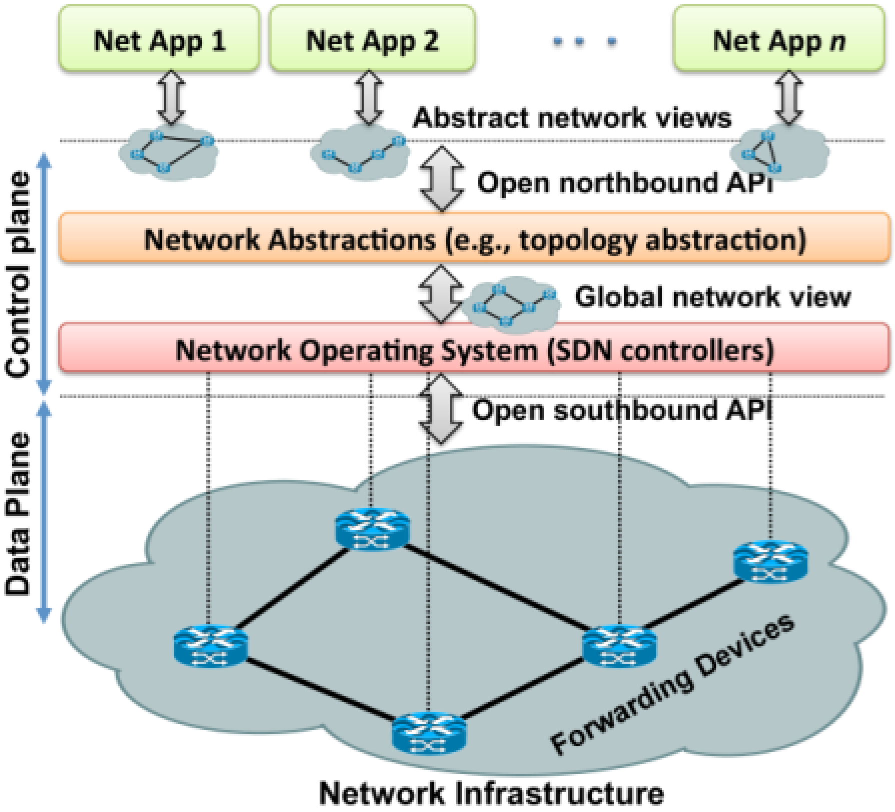


Figure 18: Abstractions in SDN architecture *[18]*

Let us see the layered architecture of SDN and go through them one by one.

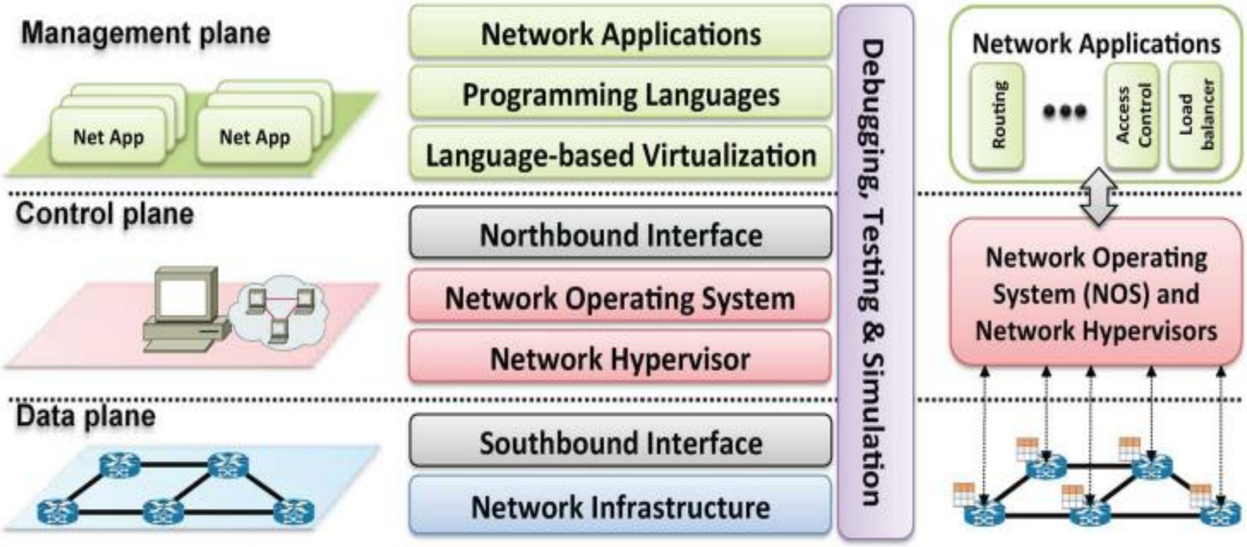


Figure 19: SDN layered architecture *[18]*

Network Infrastructure: This layer contains the various network devices, just like a traditional network. But unlike the traditional devices, they are just forwarding devices as their control and data plane are separated from each other. The NOS (Network Operating System) is responsible for making the decision-making on their behalf using a protocol such as OpenFlow [18].

Southbound Interface: Southbound Interface or the Southbound APIs connects the forwarding devices to the controller, thus acting as the bridge between the two. In SDN architecture, OpenFlow is generally used as the southbound API, which provides communication between the forwarding devices and the controller. OpenFlow is not the only option; other options are also there, like ForCES, ROFL (Revised Open-Flow Library), etc. [18].

Network Hypervisor: Hypervisors let the different virtual machines use the same hardware resources. This is very useful as, due to the popularity of virtualization, the number of virtual servers is way more than the number of physical servers. It enables cloud providers to provide IaaS where users can have their own virtual resources, which leads to the introduction of new revenue and business models, which are very helpful in a lot of ways. These virtual machines can be easily migrated from one system to another and are easily created and destroyed whenever required [18].

Network Operating System/Controller: SDN offers a NOS or a controller which provides centralized control to help in network management and problem-solving. Just like a traditional OS, it provides abstractions, essential services, and APIs to developers. A traditional OS uses a lower-level, device-specific instructions, but in the case of SDN, the developers can ignore the various low-level information. Just like a traditional OS, the lower-level details of the network policies are abstracted by the control platform [18].

These controllers can either be centralized or distributed. A centralized controller is a single entity, and it manages all the network's forwarding devices. The limitation with it is that it has a single point of failure, and it also has limitations in scaling. Some examples the centralized controllers include Maestro, Beacon, Trema, and many more. On the other hand, distributed controllers can scale up easily to meet the network requirements. It can either be a centralized cluster of nodes or a distributed set of elements. Distributed controller overcomes the single point of failure problem of a centralized controller, and scaling issues are not there. Some examples of distributed controllers are HyperFlow, DISCO, Fleet, etc. [18].

There is a special case of interfaces required by a distributed controller called Eastbound and Westbound APIs. Just like the Northbound and Southbound APIs, these APIs are also essential for a distributed controller. These APIs are used by the controller for communication and monitoring purposes. They increase the robustness of the system and decrease the probability of common faults by providing interoperability and compatibility between controllers [18].

The following image shows the Eastbound and Westbound APIs in distributed controllers.

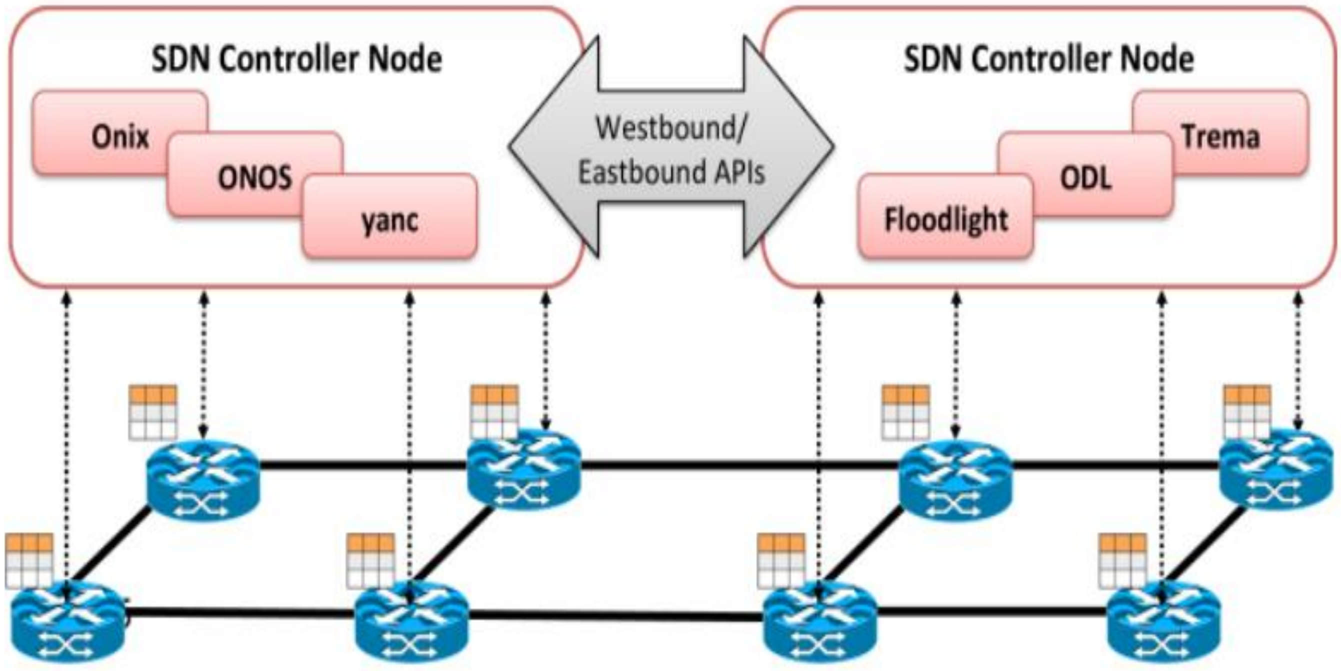


Figure 20: Eastbound and Westbound APIs in Distributed Controllers *[18]*

Northbound Interface: These are the high-level programming interfaces provided to the upper layers by the controller, and it is one of the crucial abstractions of the SDN architecture. Unlike Southbound interfaces, there is no widely accepted standard. Also, these are software ecosystems and dependent on the implementation, unlike the Southbound interfaces, which are hardware. As they have different functions based on the requirements of various applications, it is not easy to make one standard Northbound interface [18].

Language-Based Virtualization: Virtualization provides modularity and different levels of abstraction, but when it comes to a programming language solution that can provide these features, limited options are there. One of them is Pyretic, which creates an abstract network topology with the network objects and their policies. Another approach is the static network slicing approach, where the network is sliced by the compiler based on the requirements of the applications, and it provides high performance and isolation. Splendid isolation uses this approach to make three components called topology, mapping, and predicates of packets. These slices can be used in different combinations for different applications. Another solution is livNetVirt, which creates and manages virtual networks and enables QoS in them. It has two layers, the first one is a generic network interface, and the other one contains technology-specific device drivers (VPN, OpenFlow, MPLS, etc.). There are network applications and virtual network descriptions on the top of these layers. Virtual networks are created by the OpenFlow driver that is isolated from each other using rule-based flow tables [18].

Programming Languages: For decades, low-level programming languages were used to program the network. As there was no abstraction provided in that, developers were not able to focus on the real problems. Instead, they were stuck at the low-level details of the networks. Also, there was no interoperability between the devices, so these low-level languages can not be re-used. But in the case of high-level programming languages, because of the high level of abstraction, users need not worry about the low-level hardware details, and they can focus on their tasks. It enables code-reusability and software modularization. Many existing challenges in SDN can be addressed with a high-level programming language [18].

Network Applications: It is present at the top of the SDN architecture, and these applications are the brains of the network. They implement the control logic, which is enforced on the forwarding devices via the controller. These applications can do functionalities like routing, load-balancing, etc. SDN enables them to do a lot more functions than their standard functions, including reducing power consumption, QoS, Virtualization, fail-safe, etc. [18].

1.2.3 Benefits of SDN

The use of software overlay has certain benefits. Firstly, because it is software-based, the task of manually programming the hardware devices is not required, which allows administrators to control the network, change configurations, increase the capacity of the network from a centralized user interface. This offers more speed and flexibility. Because of this increased speed and flexibility, SDN supports various upcoming technologies like the Internet of Things (IoT), which requires easy and faster data transmission between various remote sites. SDN also offers better security, as it provides more visibility into the whole network, which provides a better picture of security threats [15].

1.3 NFV

Network Functions Virtualization (NFV) refers to the process of virtualizing various services in the network which conventionally run-on hardware, such as a router or a firewall. What this essentially means is that there is no requirement for hardware for each specific function. Rather, these services are bundled as Virtual Machines (VMs) on the hardware [19].

1.3.1 Virtual Machines

One thing mentioned above was Virtual Machine. Let us now see what a Virtual Machine is and why it is useful to us.

VM or a Virtual Machine is like our laptops or computers in the sense that it has a CPU memory and can connect to other devices. The difference is that these Virtual Machines exist as code in the physical servers rather than being physical like the hardware [20].

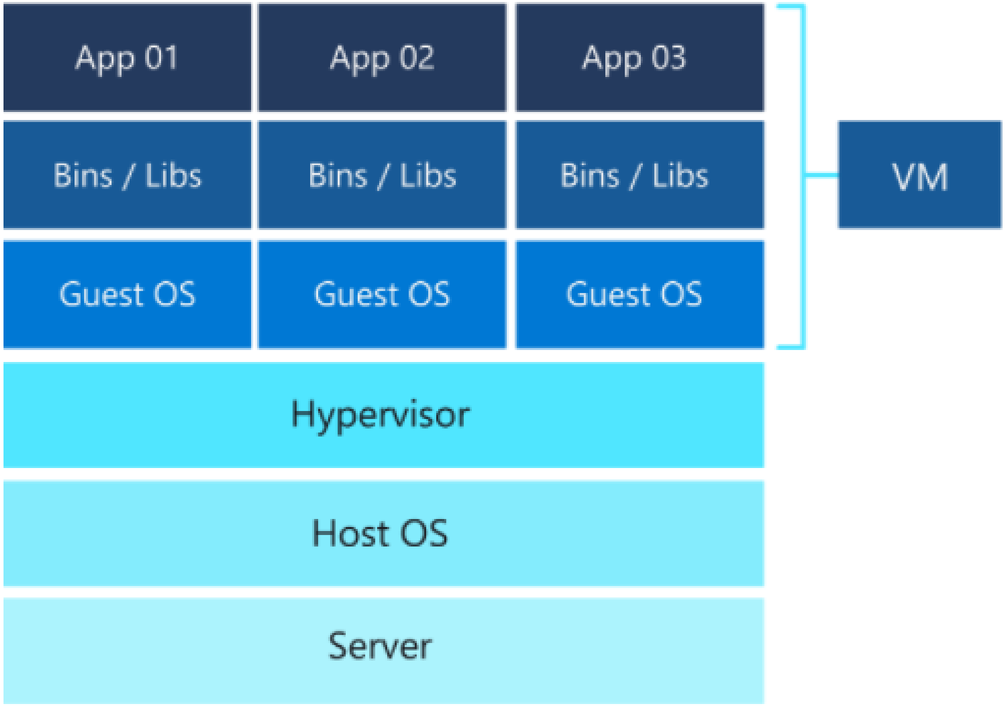


Figure 21: A Virtual Machine *[20]*

The Virtual Machine 'loans' some memory from the physical host (a computer or a remote server) to create a software-based version of the computer and runs in a different environment than the actual system. The Virtual Machine and the host act as two separate systems, and their respective applications cannot interact with each other directly [20].

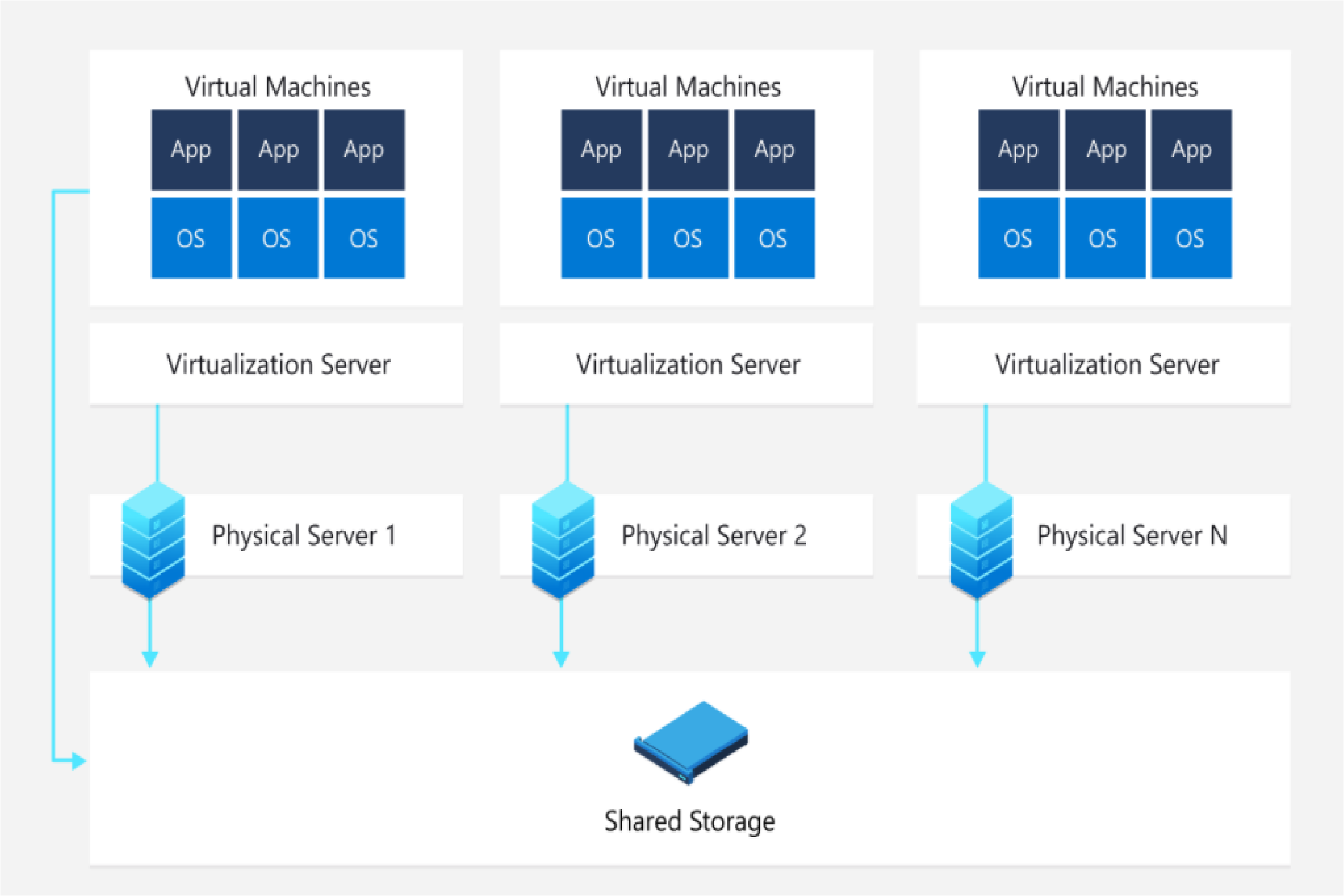


Figure 22: How a VM shares memory *[20]*

The above image shows how memory and resources are provided to the virtual environment by the host. Now let us see some benefits of Virtual Machines.

The fact that the host system and the Virtual Machine remain separated from each other is of great use. We can use this to run different operating systems on various Virtual Machines simultaneously (like running Ubuntu on Windows 11) or different versions of the same operating system as the host. This feature makes them flexible and portable, and because of this, there are certain benefits of using Virtual Machines [20]. Let us look at these benefits one by one.

- Cost: With Virtual Machines, you can run various virtual environments from one physical system. This means that the cost of the physical hardware is comparatively lower in the case of not using Virtual Machines, as maintenance costs are significantly low [20].
- Speed and Agility: Setting up a Virtual Machine is relatively fast and easy than setting up another physical system [20].
- Low Downtime: The Virtual Machines are very conveniently moved from one VM Manager to another on a separate machine, making them a great choice for backup for the scenario when the host system goes down [20].

- Scalability: With Virtual Machines, it is easier to add more servers to manage the workload among various VMs. This directly results in more efficient performance of applications [20].
- Security: Because of the separate environment, we can run applications that are not fully trusted on the Virtual Machines and hence avoid any harm to the host system [20].

Because of all the benefits listed above, there are multiple uses for Virtual Machines. These include creating and linking applications to the cloud, testing new Operating Systems used as a testing environment for developers, backing up, examining data that has been infected with viruses or malware, and using applications or software on an Operating System that they were not designed for [20].

1.3.2 NFV Approach

NFV introduces Virtual Machines in the already existing hardware. Traditionally, when a new function in a network needs to be added, a new appliance must be deployed. But with Network Functions Virtualization, there is no need to get new hardware. Instead, we can simply set up a virtual machine in the already present system [21].

The following image illustrates the difference between the classic network approach and the approach used by NFV.

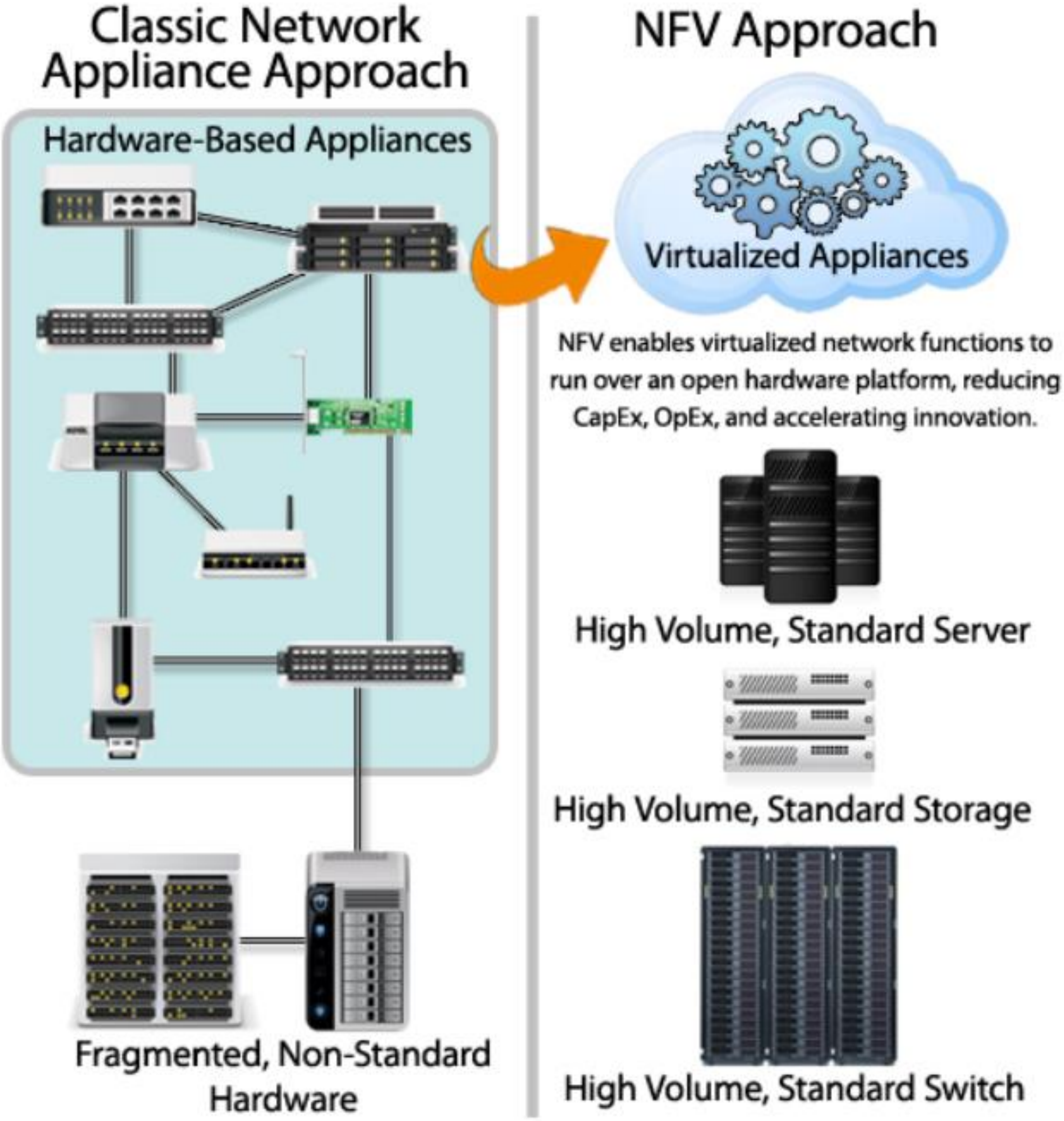

Classic Network Appliance Approach
Hardware-Based Appliances
Fragmented, Non-Standard Hardware
NFV Approach
Virtualized Appliances
NFV enables virtualized network functions to run over an open hardware platform, reducing CapEx, OpEx, and accelerating innovation.
High Volume, Standard Server
High Volume, Standard Storage
High Volume, Standard Switch

Figure 23: Classic Approach vs NFV Approach *[21]*

1.3.3 NFV Architecture

Now let us have a look at the architecture of Network Functions Virtualization.

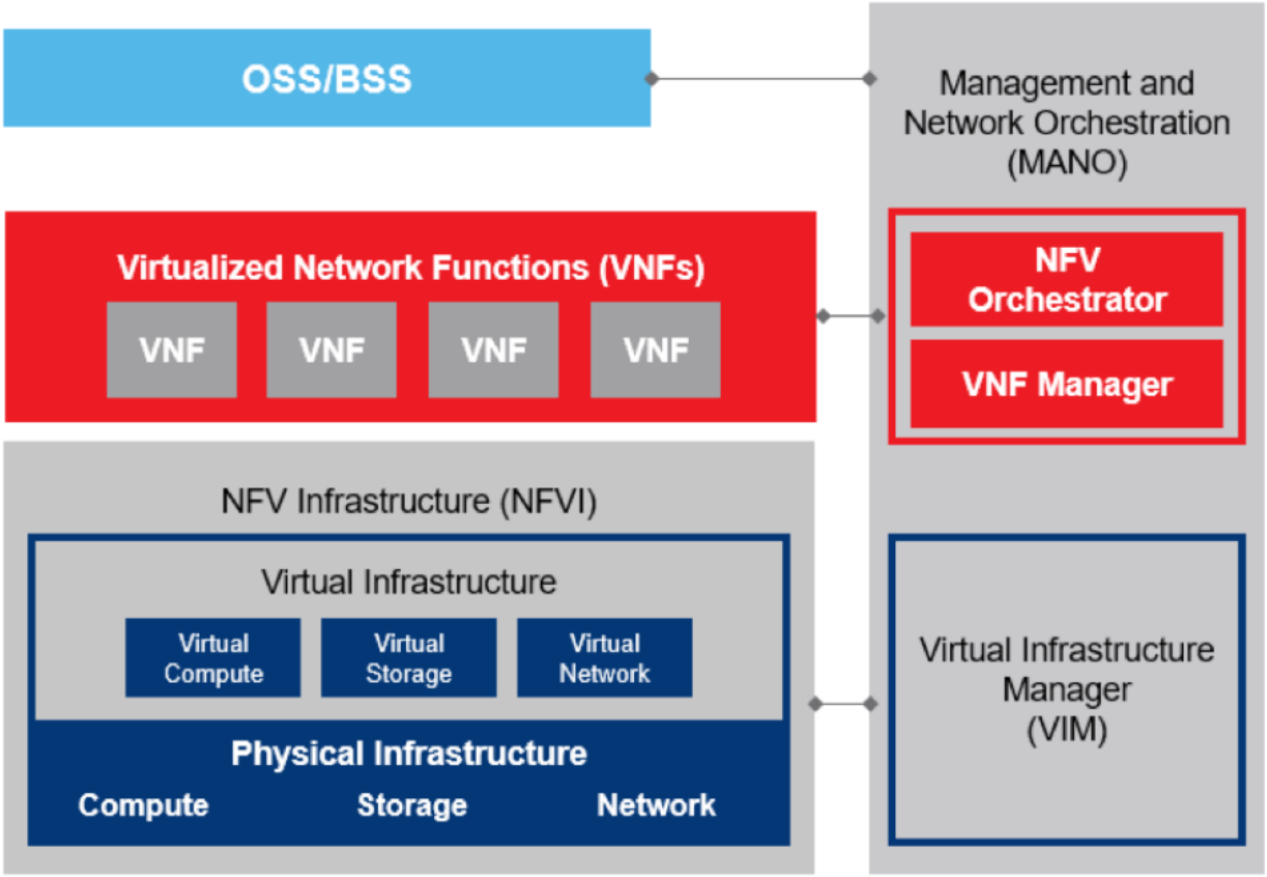


Figure 24: NFV Architecture *[22]*

As seen from the above diagram, there are three main components of NFV architecture. Let us see them one by one.

The first one is **Virtual Network Functions (VNFs)**. These refer to the devices or elements in the network that have been virtualized, like a router or a firewall. For example, when we virtualize a router, it becomes Router VNF [23].

The next component is the **NFV Infrastructure (NFVI)**. NFVI provides the required physical resources like compute, storage, network, and software which helps in the deployment and management of VNFs. The virtualization layer is provided by NFVI, sitting just on top of the hardware and abstracting its resources. These resources are then partitioned and provisioned logically, which then supports the Virtual Network Functions [22].

The last is **Management and Network Orchestration (MANO)**. It is further divided into three components. The first one is the **NFV Orchestrator**, which is used to handle VNF onboarding, managing, and validating resources, managing the lifecycle, and authorizing the NFVI resource requests. The next one is the **VNF Manager**, which is used to control the VNF lifestyle management of VNF instances. The last one is the **Virtual Infrastructure Manager (VIM)**, which is used in controlling and managing the resources (compute, storage, and network) in NFVI [22].

There is also a block at the top of the diagram showing **OSS/BSS**. It stands for Operation Support System/Business Support System. OSS is used in the management of network, fault, configuration, and service, while BSS is used in the management of customers, products, orders, etc. [23].

1.3.4 Benefits of NFV and working with SDN

As mentioned above, NFV separates the various functions in a network from the physical system. This partitioning leads to an increase in the overall flexibility, which leads to certain benefits. Firstly, it directly leads to less physical space needed by the infrastructure. This also leads to a reduction in cost related to purchasing the hardware as well as the cost of maintaining it, and the lifecycle of the hardware increases. Less hardware also means reduced power consumption by the network and is less costly to maintain. Finally, it also means it is more convenient to upgrade our network [21].

Although NFV and SDN are not the same things, they have their own similarities. In both technologies, we go for virtualization and network abstraction, but the process is not quite similar. In SDN, the target is to achieve a centrally manageable and programmable network by separating the network forwarding functions and the network control functions from each other, whereas in NFV, network functions are abstracted from the physical host [19].

But this does not mean that they cannot work together; rather, it is very beneficial to use them together. NFV provides the infrastructure, and SDN can run software on it. Depending on the required goal, we can use them together. The resulting network would be a lot more flexible programmable and will use the resources in a very efficient manner [19].

1.4 vCPE

To understand vCPE, let us first see what a CPE is. CPE stands for Customer Premises Equipment, which can be any equipment or device like a router, firewall, gateway, etc., which runs on the customer's side, and which provides a particular service. Traditionally, while installing a CPE, dedicated hardware is needed on the customer's premises to run the CPEs, making their functionality hardware-based [24].

But now, instead of providing dedicated hardware, the same services provided by CPE are delivered using the software-based approach. Routing, switching, security, and all the networking functions are provided using virtualization with the help of Virtual Network Functions (VNFs) [24].

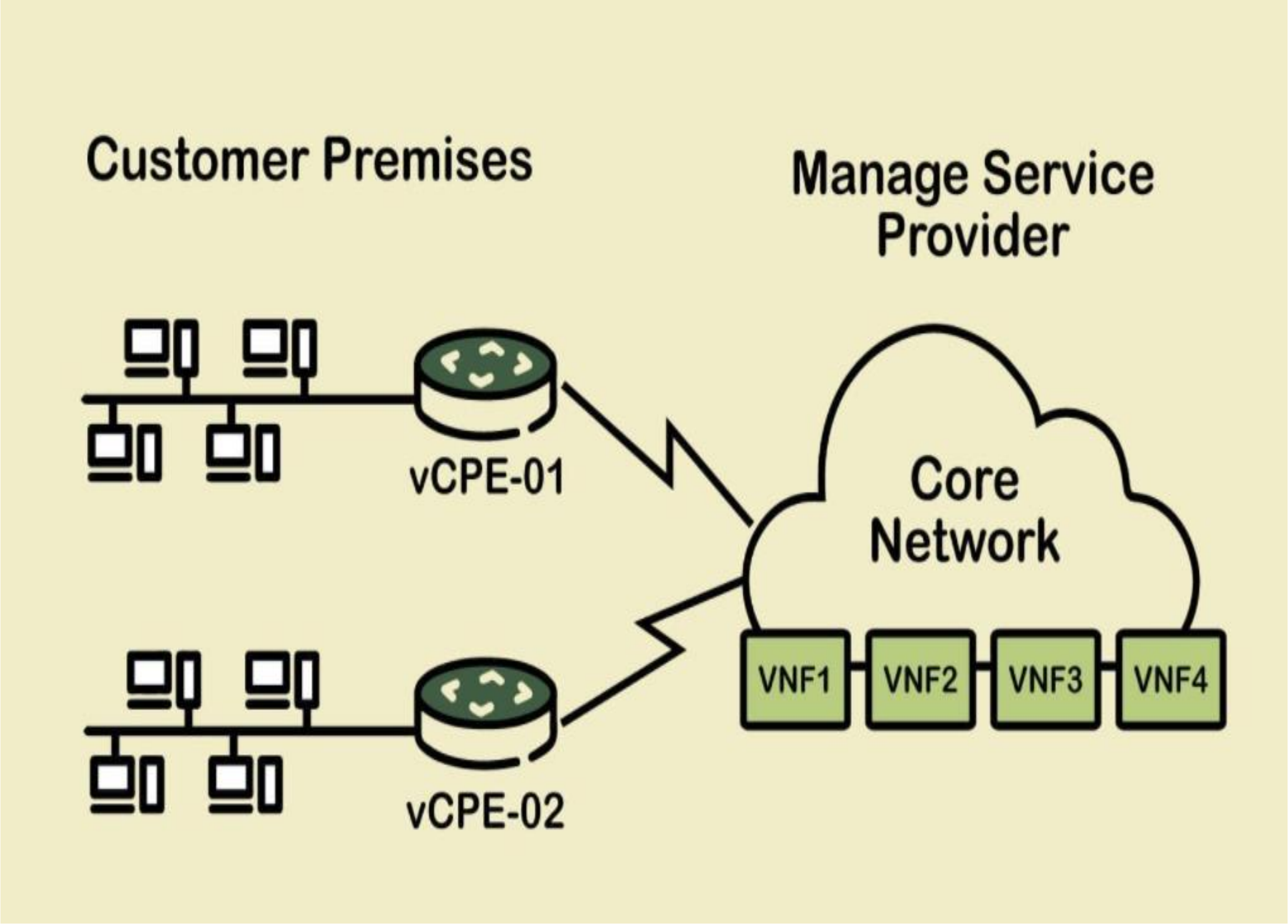


Figure 25: vCPE *[24]*

1.4.1 Working of vCPE

The concept of virtualization, when added to the CPE, has a huge impact on the way things work. Instead of being hardware-based, the functionality now becomes software-based [24]. Let us see what it looks like.

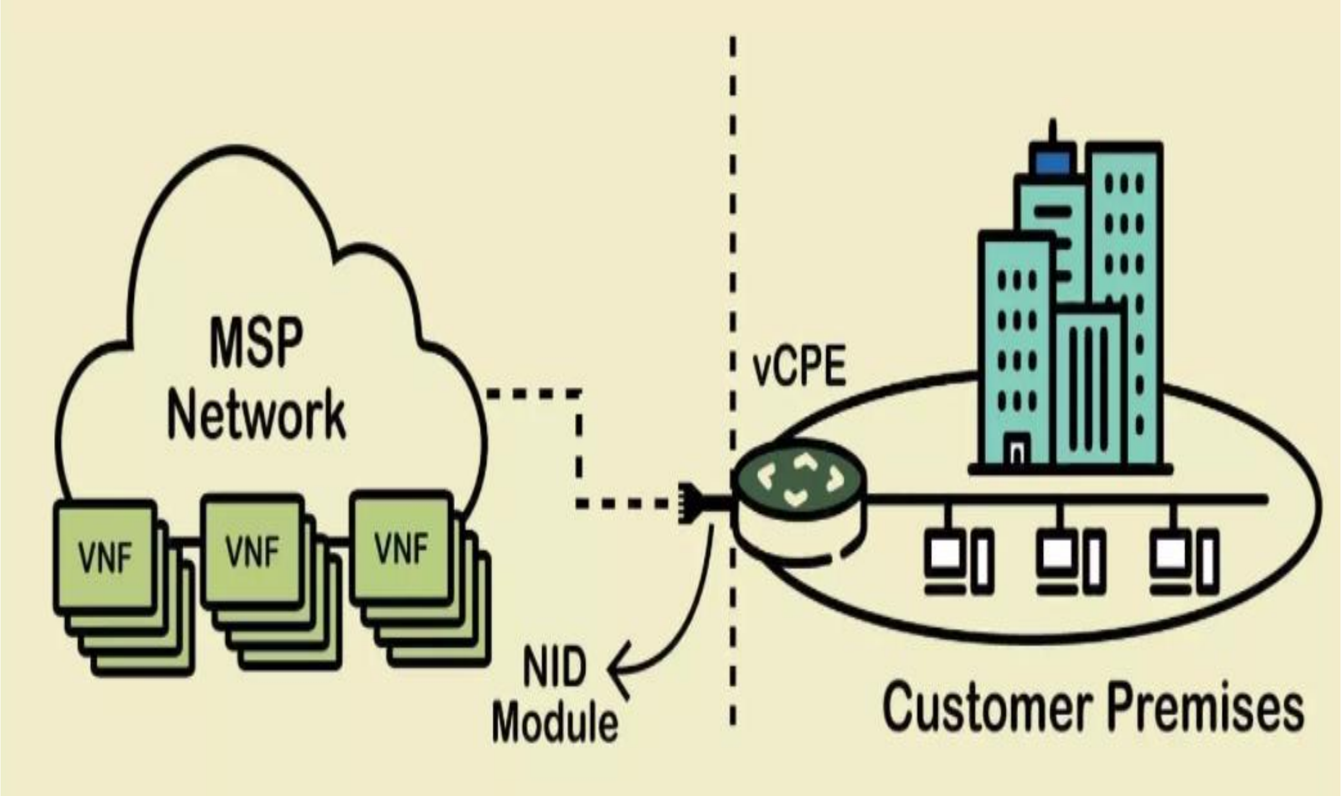


Figure 26: Working of vCPE *[24]*

As seen from the above diagram, the service provider on the left side uses Virtual Network Functions (VNFs). These VNFs are used to provide different network services like routing, session management, malware detection, etc. [24].

The service provider provides the network functions to the customer by pushing them into the hardware on the customer's side. The NID modules (Network Interface Device) are used as the interfaces between the customer premises and the service provider network. So, it is the VNFs that play a major role in the working of vCPE [24].

1.4.2 Benefits

With vCPE, all the network services are provided by software instead of hardware. This approach leads to certain benefits. Let us have a look at them:

- Fast and Easy: Because of the vCPE approach, the service providers can deploy, upgrade, and remove unwanted elements from the network remotely, which is both fast and convenient [24].
- Scalability: Virtualization leads to evenly distribution of resources with customers to provide better supply, and it is also helpful in scalability when the network grows [24].
- Low cost: Software-based approach leads to fewer requirements for the hardware. This directly leads to a reduction in costs related to deploying, installing, and managing hardware [24].

- Centralized UI: Because of virtualization, there is no need to have multiple hardware devices. Instead, we can have one centralized user interface for management and monitoring purposes [24].
- Flexibility: Virtualization has led to the creation of new algorithms and services that could not be provided by the hardware-based approach, thereby making the network a lot more flexible [24].

1.5 SD-WAN

When we combine the concepts of SDN with a WAN, we get SD-WAN. A centralized controller is used to manage SD-WANs, which sends policy information to all the devices connected to it. The use of software lets the professionals configure devices on the network edge remotely, so they do not have to configure them manually, and even if they must do it manually, the task is reduced considerably [25].

1.5.1 SD-WAN Architecture

WAN poses many challenges for various organizations, including the high cost of network circuits' complexities of configuring, monitoring, and managing them. Although WAN optimization has helped to certain degrees, there is still a demand for more [26]. The following image shows how a traditional WAN works.

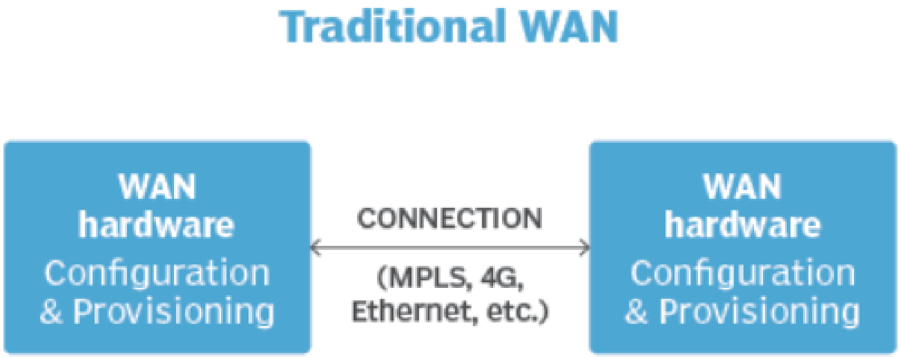

Traditional WAN
WAN hardware
Configuration & Provisioning
CONNECTION
(MPLS, 4G, Ethernet, etc.)
WAN hardware
Configuration & Provisioning

Figure 27: WAN overview *[26]*

But in the case of SD-WAN, a software overlay is introduced, which eases the task of professionals by allowing them to do all the required tasks (configuring, monitoring, managing, securing, etc.) remotely; they don't have to be physically present there. This is very helpful when the locations are hard to reach. Also, there is a lot of abstraction and automation, which centralizes the network control. When we abstract the transport layer from hardware to software, we can prioritize the traffic. This allows us to use broadband and wireless (which are cheaper) along with the expensive MPLS connections. All these factors combined lead to an environment that is way more flexible and efficient [26].

The following diagram shows the SD-WAN overlay.

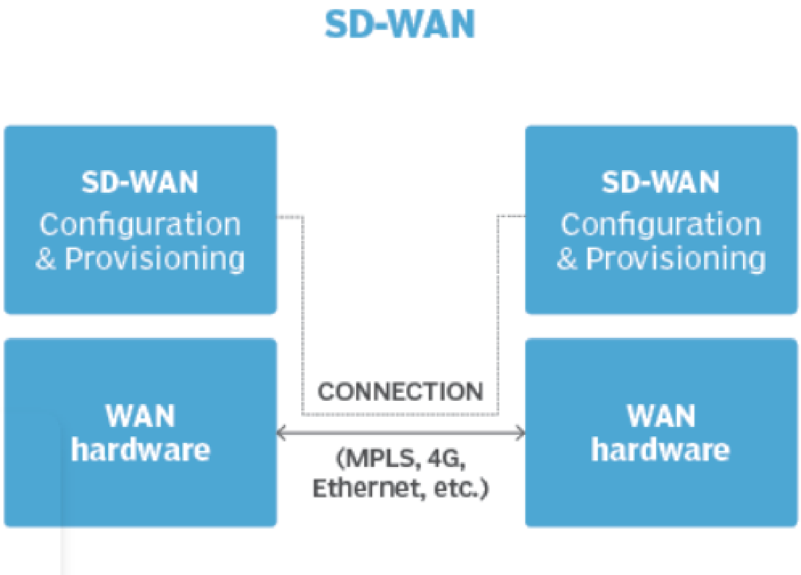

SD-WAN
SD-WAN Configuration & Provisioning
SD-WAN Configuration & Provisioning
CONNECTION
WAN hardware
WAN hardware
(MPLS, 4G, Ethernet, etc.)

Figure 28: SD-WAN Overlay *[26]*

Not just the overlay another term used a lot is the controller, which is a client that is used to direct data flow between two points. Apart from that, it is also used to distribute policies related to network and security to connected devices [26].

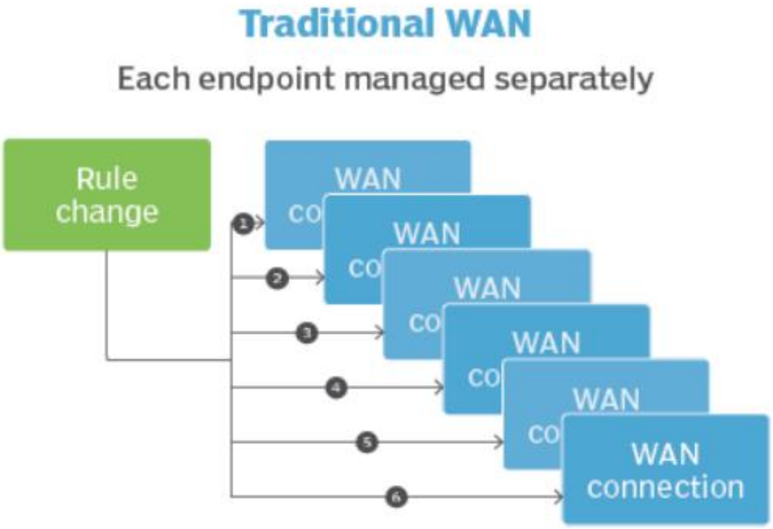


Figure 29: WAN without controller *[26]*

The above image shows what a traditional WAN looks like without a controller. Now let us see how different SD-WAN looks with the introduction of a controller.

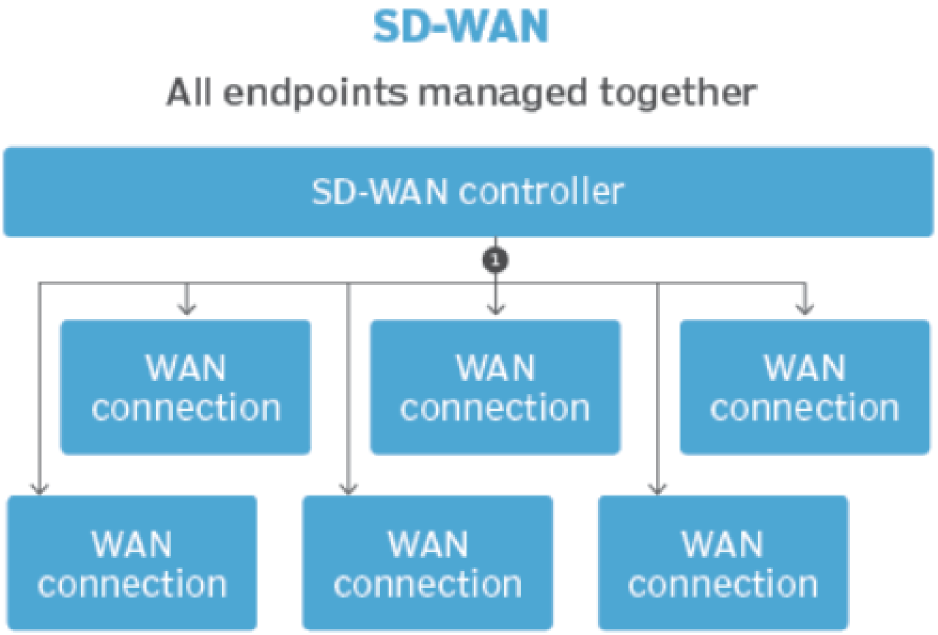


Figure 30: SD-WAN controller *[26]*

As can be seen from the two figures, the introduction of a controller makes SD-WANs more flexible than traditional WANs.

Now let us put the whole architecture of SD-WAN together in a single figure. There are a total of 3 layers, namely the Data layer, Control layer, and Application layer [2]. Let us look at them one by one.

The **Data layer** takes care of bandwidth virtualization and data forwarding. Bandwidth virtualization refers to the full utilization of the available bandwidth by putting together the various network links that are going to one location into a resource pool available for all various applications and different services. The available bandwidth is then provided to forward the data using a distributed set of network elements that are used in forwarding the data. Both the bandwidth virtualization and data forwarding get their commands through interfaces (for example, OpenFlow) from the network controller in the upper layer [2].

The **Control layer** serves many purposes, and these are separately implemented and managed. This enables us to develop, modify, debug, and remove them (if needed) without having any impact on others, making it economical. Also, these functions can be connected with each other to create various new services, hence, making it more flexible [2].

Application layer allows application developers to be more involved in the network control through network expression and application expression, as required by the different purposes of various applications. There are countless applications in the market today, and the number is increasing day by day, and their requirements are also different. For example, a video streaming application will have different requirements than a security application. Application expression lets the application developers declare their strategies to handle the various requirements, and the network expression allows them to list the different networking requirements [2].

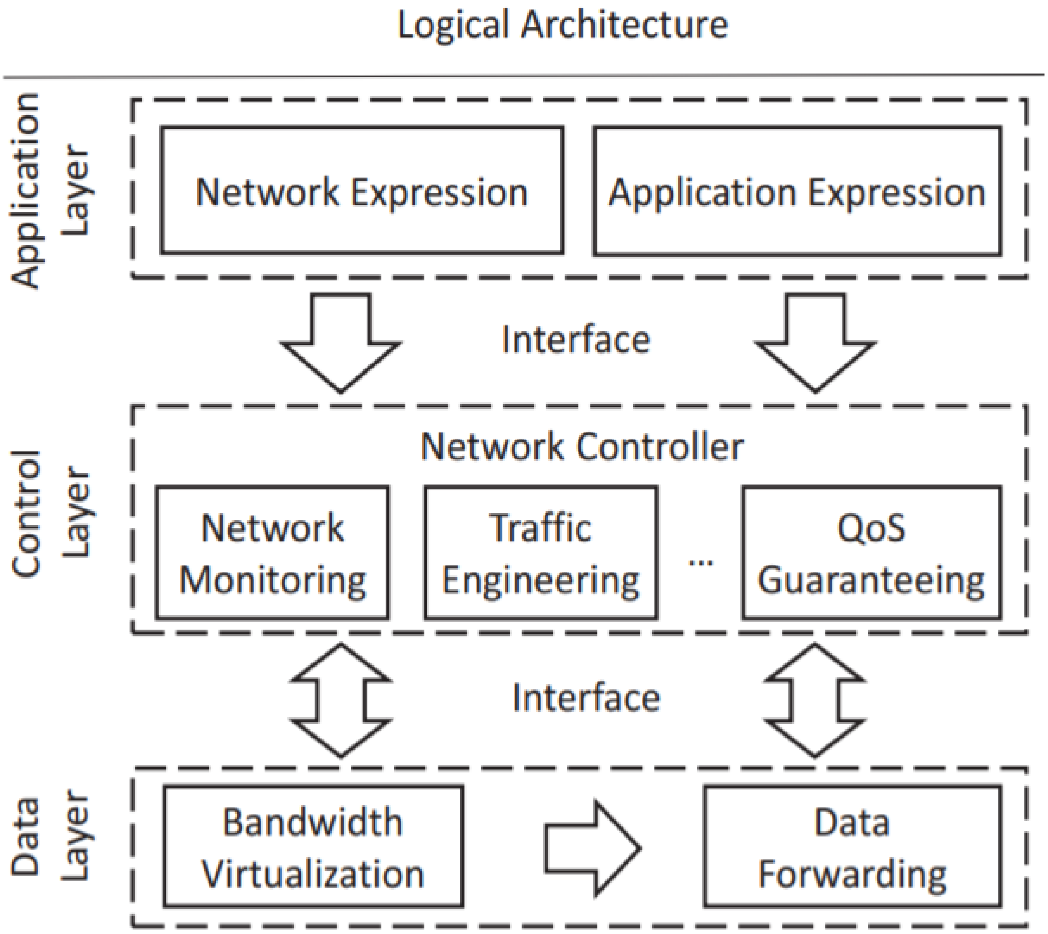


Figure 31: SD-WAN Logical Architecture *[2]*

The diagram above is the logical architecture of SD-WAN, and the one below is the physical architecture.

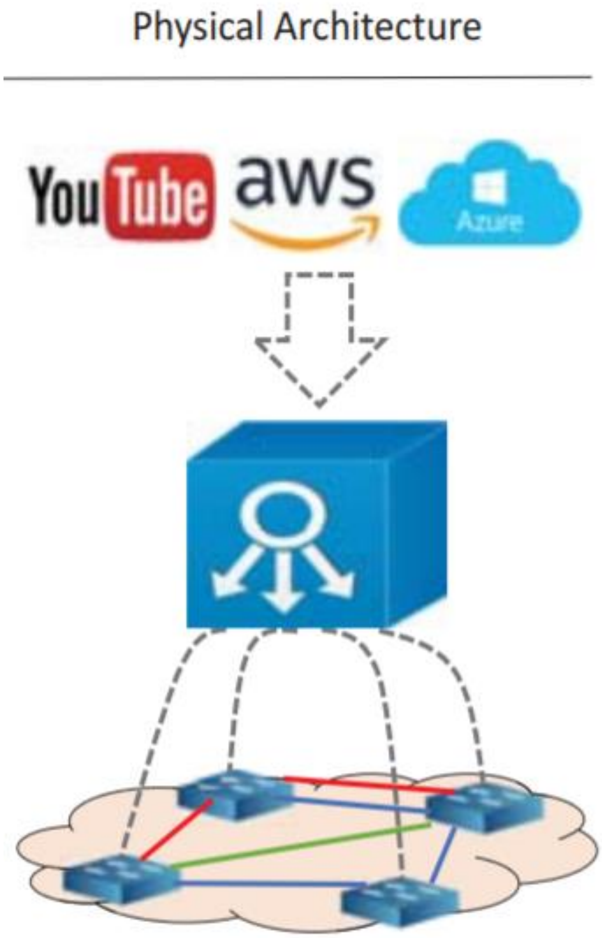


Figure 32: SD-WAN Physical Architecture *[2]*

The SD-WAN architecture can be of three main types. The first one is **On-Premises SD-WAN**, where the SD-WAN hardware is on-site, and no cloud is used. This makes it ideal when sensitive information is there that cannot be sent over the internet. The second one is **Cloud-Enabled SD-WAN**, which connects the hardware infrastructure to the virtual clouds, providing a better experience with the cloud-native applications. The third one is **Cloud-Enabled with Backbone SD-WAN**, which connects the network to a nearby PoP (Point of Presence), which allows traffic to switch from public to a private connection, making it more secure and consistent [27].

1.5.2 Why SD-WAN over WAN

As mentioned previously, the one thing that differentiates SD-WAN from a traditional WAN is the software overlay. This software overlay this introduction of software overlay provides a lot of advancement in the current WANs, making them more flexible, convenient to manage, and efficient.

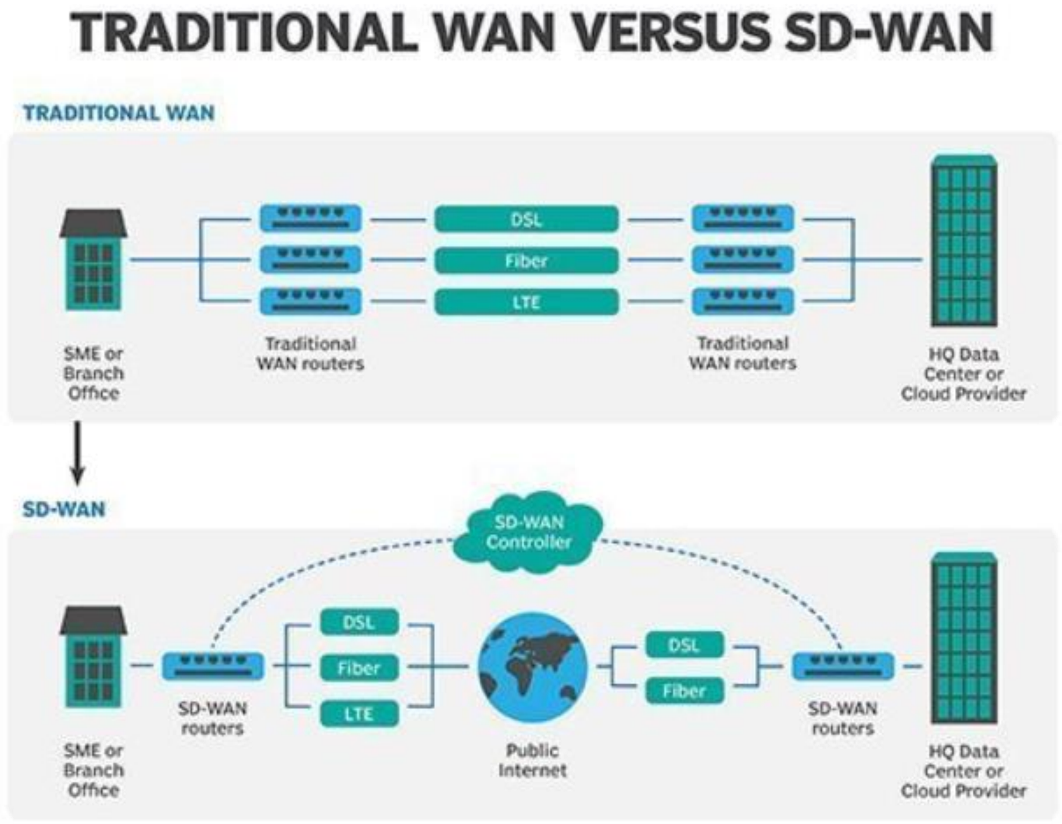


Figure 33: WAN vs SD-WAN *[1]*

The above diagram shows how different an SD-WAN looks from a conventional WAN. Now let us make a bullet list of key differences between the two.

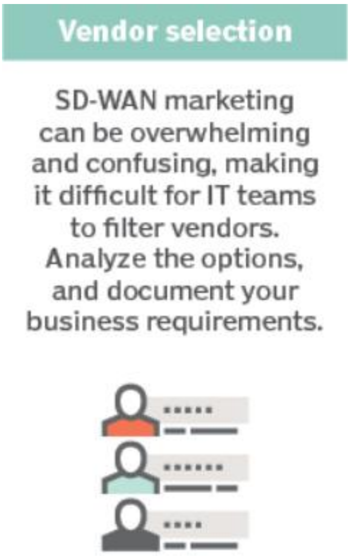
- Traditional WANs provide a hardware approach for their management, but SD-WANs do all of that with the help of a software approach [28].
- SD-WAN provides better flexibility than current WANs [28].
- When we need to do configuration, or if we need to scale up our network, WAN takes a lot longer time than SD-WANs [28].
- SD-WAN provides provision for automation, which allows network configuration to be done automatically without human intervention [28].
- SD-WAN provides higher-speed connectivity at lower costs than traditional WANs [28].
- Traditional WANs first connect to an intermediate hub and then to the cloud, whereas SD-WANs access the applications directly, which is hosted in a cloud. So, in the case of cloud applications, SD-WANs provide better performance [28].
- In the case of traditional WANs, because of the hardware, the data centers are limited in their capabilities to cope with the connections to multiple cloud platforms. This is not the case with the SD-WANs [28].
- SD-WANs simplify the complexities of conventional WANs, which involve management and configuration [28].

- SD-WANs provide a more secure VPN than conventional WANs. Also, features like firewall, WAN optimization, etc., which normal WANs fail to fully integrate, are provided in SD-WANs [28].

1.5.3 SD-WAN Challenges

While we have looked at all the benefits that are provided by SD-WAN, it is also important to look at its downsides of it. In this section, we look at some of the concerns or challenges that are related to SD-WANs.

- Vendor Selection: The first thing that comes to mind is the name of the company whose product you want to buy. There are various SD-WAN solutions available in the market and selecting one of them can be a little bit of a headache.



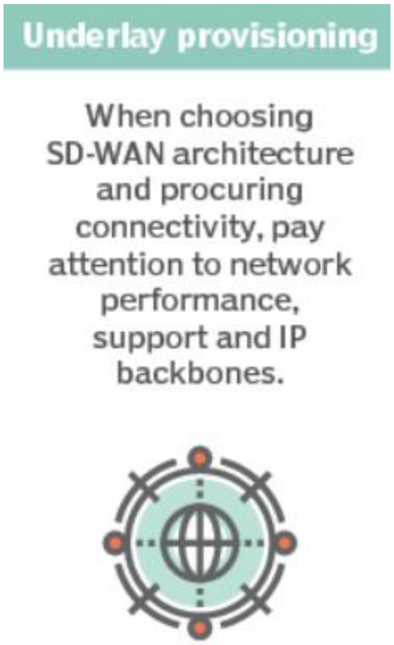
Vendor selection

SD-WAN marketing can be overwhelming and confusing, making it difficult for IT teams to filter vendors. Analyze the options, and document your business requirements.

Figure 34: Vendor Selection Challenge *[29]*

The various solutions available in the market put a little bit of a burden on the shoulders of IT teams. They now must decide which product to opt for based on a few things, for example, analysis of their user workflows, existing contracts, and many more [29].

- Underlay Provisioning: This challenge involves a discussion about which underlay service provider is the best choice for a company and whether to go for a single IP backbone or a multi-ISP approach [29].



Underlay provisioning

When choosing SD-WAN architecture and procuring connectivity, pay attention to network performance, support and IP backbones.

Figure 35: Underlay Provisioning Challenge *[29]*

- Cloud Connectivity: Connection to clouds is needed in almost every company by the IT teams, and there are three options to go for. In the first one, cloud access is in-built into the architecture itself and uses the cloud as the backbone. The second one involves delivery into the cloud environment via public gateways or private backbones. In the third one, the onus is on the customers for the deployment within their local cloud data center, hence involving a simple ad-hoc architecture [29].

Cloud connectivity

Most enterprises require cloud access to public cloud environments. Evaluate each vendor's strategy for providing this access.

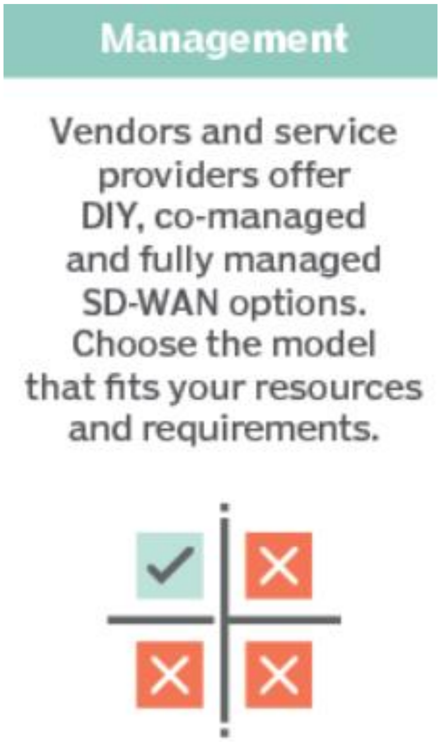
Figure 36: Cloud Connectivity Challenge *[29]*

- Cost reduction: For every business, cutting costs is one of the most important elements. In the case of SD-WAN, certain choices have an impact on the overall cost to the company. These choices should not be made just to make the initial cost lower but by keeping the overall benefit of the business in mind [29].

Cost savings with SD-WAN don't always show as quantifiable figures on the budget. Look at overall business benefits as well.

Figure 37: Cost reduction Challenge *[29]*

- Management: There are three ways in which SD-WAN can be deployed, DIY (Do It Yourself), co-managed and fully managed. The decision should be made based on certain factors, like ownership status, requirements, and many more [29].



Management

Vendors and service providers offer DIY, co-managed and fully managed SD-WAN options. Choose the model that fits your resources and requirements.

Figure 38: Management Challenge *[29]*

Section 2: SD-WAN Solutions

In this section, we will look at the SD-WAN solutions in the market provided by different vendors. When SD-WAN came, different vendors came up with their own solutions, and hence, there were a lot of choices for enterprises to choose from. So now, let us look at a few of the top ones and compare them with each other.

2.1 Cato SD-WAN

The first one that we will explore is the solution provided by Cato Networks. Before that, let us take a brief look at the company itself.

Cato Networks Ltd. was founded on 1st February 2015 by Gur Shatz and Shlomo Kramer, and it is based in Israel. Shlomo Kramer is the co-founder of Check Point Software Technologies and Imperva, and Gur Shatz is the co-founder of Incapsula. Cato provides networking and security platforms to establish the connection among various endpoints securely [30].

Figure 39: Cato Networks Ltd. *[30]*

Cato Networks uses 34 technology products and services (HTML5, jQuery, etc.) and about 66 technologies for their website (Viewport Meta, iPhone/Mobile Compatible, etc.) [30].

The main emphasis by **Cato SD-WAN** is on the edges and the core, mainly on the edges. On the edges, Cato Sockets are used to provide connection to the Internet and MPLS services. The job of these Sockets is to monitor traffic in real-time and decide which link is to be used based on the application policies. If needed, fail-over and fail-back are done automatically [31]. These Cato Sockets are available in two models, X1500 and X1700. X1500 is used in branch offices, whereas the X1700 model is used in data centers, and both models are regularly monitored and updated by Cato's NOC (Networks operations Center) [32].

2.1.1 Cato SD-WAN Operations

The SD-WAN operation by Cato Networks can be divided into various points. Let us go through them one by one.

- Link Aggregation: Cato supports multiple links aggregation for MPLS and different Internet circuits like fiber, cable, 4G, 5G, etc., and enhances capacity and resiliency by balancing the traffic across links. And in case of a link fail-over, Cato automatically switches the traffic to the next best selection instantly. Also, the management policies are customizable, so we can prioritize the applications for enhanced performance. Fail-back also occurs according to the already configured timers, which makes sure that the network is not disrupted [32].

- Dynamic Path Selection: There is a provision for Policy-based Routing (PbR), where the best link is selected based on predefined rules. Jitter, latency, and packet loss of the link are monitored by the Socket. Based on these, we can prioritize applications to different links based on their priority [32].
- Application Identification: The Deep Packet Inspection (DPI) engine provided by Cato can identify many applications and an even greater number of domains. This, combined with some third-party engines and ML (Machine Learning) algorithms, creates a huge data warehouse. All of this provides a detailed insight into traffic analytics [32].
- Bandwidth Management and QoS: Using the Bandwidth Management rules, the applications which are more critical always get the required capacity, and other applications get served on the best-effort approach, making it very efficient for business purposes. These rules can be created or changed at each level by the administrators [32].
- Packet Loss Mitigation: To reduce the effect of packet losses, the detection is done not at the destination but at the nearby Point of Presence (PoP). The Cato Sockets instantly detects the packet loss, changes the traffic link, and swaps back to the primary link accordingly. Also, packet duplication can be enabled on an application basis, which duplicates only the application packets on both the links of an active-active connection. The thing to notice here is that only the packets of the selected applications are duplicated, not for all, which leads to better utilization of bandwidth [32].

- BGP Integration: Cato provides routing protocol integration with which there is no need to manually configure static paths for the connection between established and the SD-WAN infrastructure when organizations decide to go for SD-WAN integration on their already established network. Cato Clouds can make routing decisions in real-time based on the current configurations and by leveraging the routing information of BGP, which leads to even better flexibility in gradual deployments [32].

2.1.2 Features of Cato SD-WAN

Now let us look at some features of SD-WAN provided by Cato.

- Management Application: A single pane of glass is provided by Cato for the management of networking and security infrastructure, and not just a visual image. Rather, the users are provisioned to configure, manage, and troubleshoot their networks. By interacting with the single pane of glass, detailed statistics for each option can be accessed [32].
- Real-time Analytics: Cato has included real-time network analytics, which provides information about jitter, latency, packet loss, throughput, and many more. This helps in the troubleshooting process and helps in determining the quality of experience by providing a Mean Opinion Score (MOS) [32].
- Event Discovery: Event Discovery organizes multiple events related to network and security, putting them in a single timeline, which can be queried easily. Cato takes care of the data warehouse, and the benefit of this is that it leads to a hierarchy of events, and complex queries can be built easily [32].

- Zero-touch Deployment: With zero-touch deployment, IT teams need not be present on the site. Instead, only power and an IP address (static or dynamic) must be provided to the Sockets, and when they get on the Internet, they get connected to the nearest Cato PoP and get self-configured [32].
- Meshed Topologies and Scaling: Different applications require different topologies based on their work. With Cato, all the network configurations are allowed providing customers with better control. Also, there is no scaling limitation on the network size or the topology [32].

- High Availability: Using the Virtual Router Redundancy Protocol (VRRP), Cato provides primary and secondary sockets leading to a non-stop connection, even if a Socket fails, with fast and simple deployment without any recurring charge [32].

Cato just does not stop at the SD-WAN. It is just the first step of a bigger picture. Next comes SD-WAN as a Service, which converges the edge, the global backbone, and a full network security stack into a cloud platform known as SASE (Secure Access Service Edge), thereby extending the capacity of SD-WAN even more [33]. Let us now have a look at what SASE is and what benefits it provides.

2.1.3 Cato SASE

SASE or Secure Access Service Edge is a platform where SD-WAN and various network security point solutions are converged into a single unified cloud service. These point solutions include FWaaS, CASB, SWG, and ZTNA, and we will look at them later. Traditionally, things were a little bit complex as these point solutions were managed separately, which meant more cost and complexity [34].

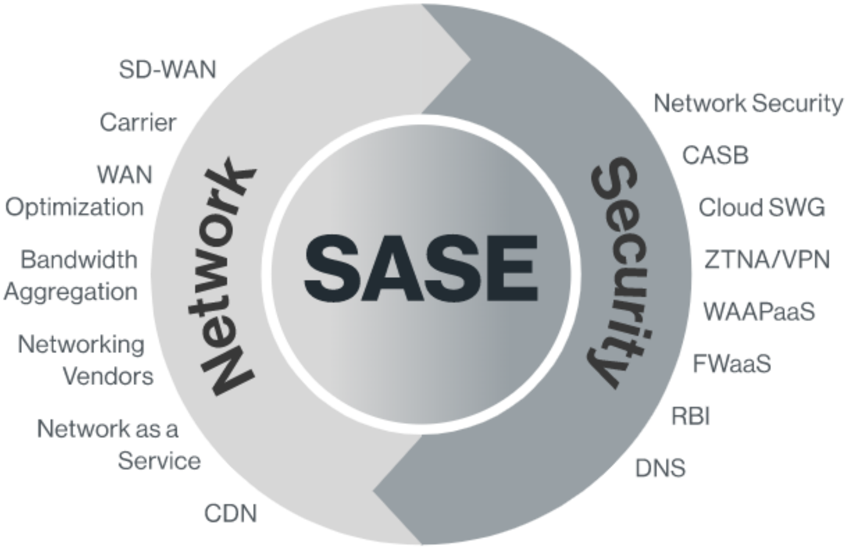


Figure 40: Secure Access Service Edge (SASE) *[34]*

Let us now have a look at the **components of SASE** one by one.

- SD-WAN: The first component is the Software-Defined WAN. Its capabilities are leveraged by SASE to provide various network services [34].
- FWaaS: It stands for Firewall as a Service. FWaaS is included in SASE for businesses to extend a full network security stack if required [34].
- ZTNA: Zero-Trust Network Access helps in securing application access to users, with a zero-trust policy in which the access to applications gets adjusted dynamically, based on details like user identity, location, device, etc. [34].
- CASB: Cloud Access Security Broker is useful to deal with the threats involved with cloud computing. SASE takes care of the complexity associated with the integration between CASB and other point solutions [34].
- SWG: Secure Web Gateway helps in protecting users from various threats from the web, and with SASE, protection is given to users at all locations without the need of maintaining policies among various point solutions [34].
- Unified Management: In SASE, a single pane of glass helps users in monitoring and managing all the network and security solutions with ease [34].
- Global Private Backbone: It is the globally distributed network of more than 70 Points of Presence connected to each other by multiple T-1 carriers with cloud-native software [34].

With all the components mentioned above, there are certain benefits of SASE. Firstly, it leads to fast and better performance. Secondly, with the full security stack and a unified policy, the security is optimum. And lastly, because there is no complexity, there is no need for CAPEX (Capital Expenditure). There are just Operational Expenses (OPEX) to keep the business operational [34].

2.1.4 Why Cato

Let us see from a future business point of view. The traditional SD-WANs do not fully support the business needs by themselves. This is due to the fact that to fully cope with the future business needs, IT professionals have to secure across all edges on the global scale, and the traditional SD-WANs leaves the IT professionals with the complexity of managing various point products, as well as relying on the rigid MPLS links to provide secure and high-performance connectivity, which becomes costly [33].

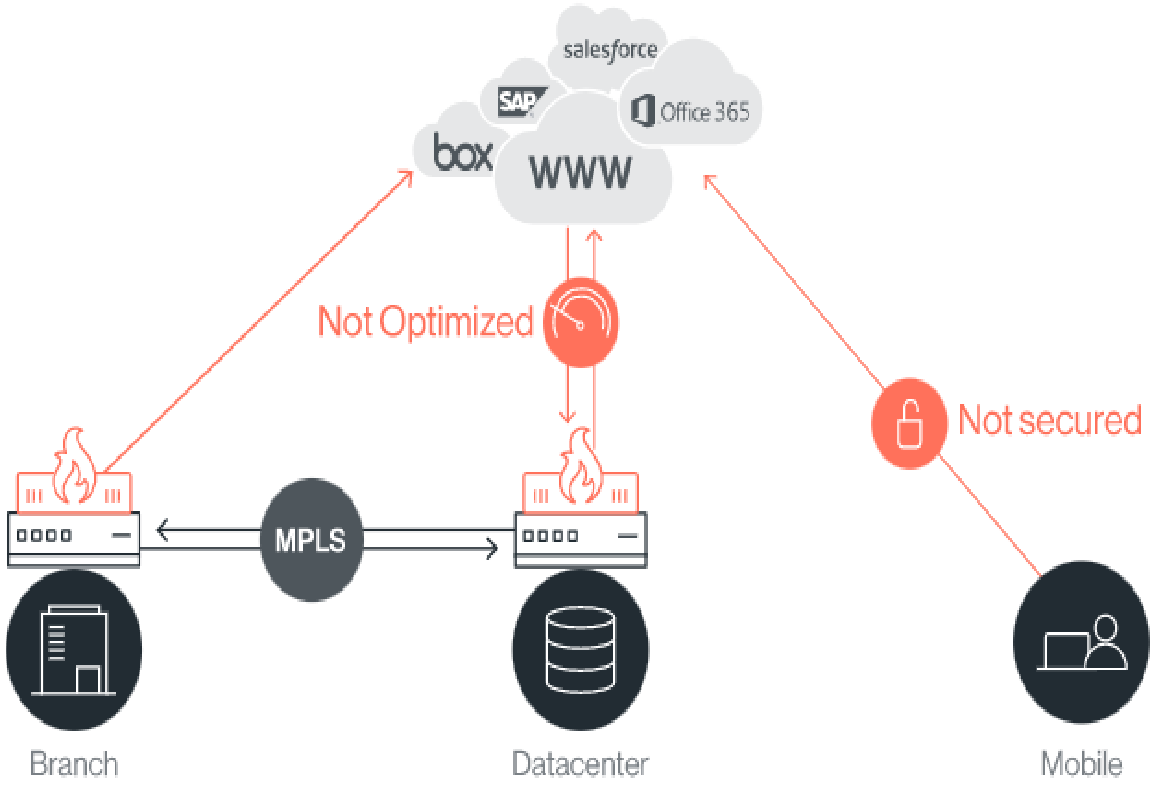


Figure 41: SD-WAN Complexity *[33]*

Cato Networks provides the solution for this problem. As mentioned previously, Cato converges the SD-WAN, global backbone, full network security stack, and support for cloud and mobile. This helps not only in reducing the costs due to MPLS but also in removing the need to provide multiple point products. So, the cost and complexity associated with maintaining them are not there [33].

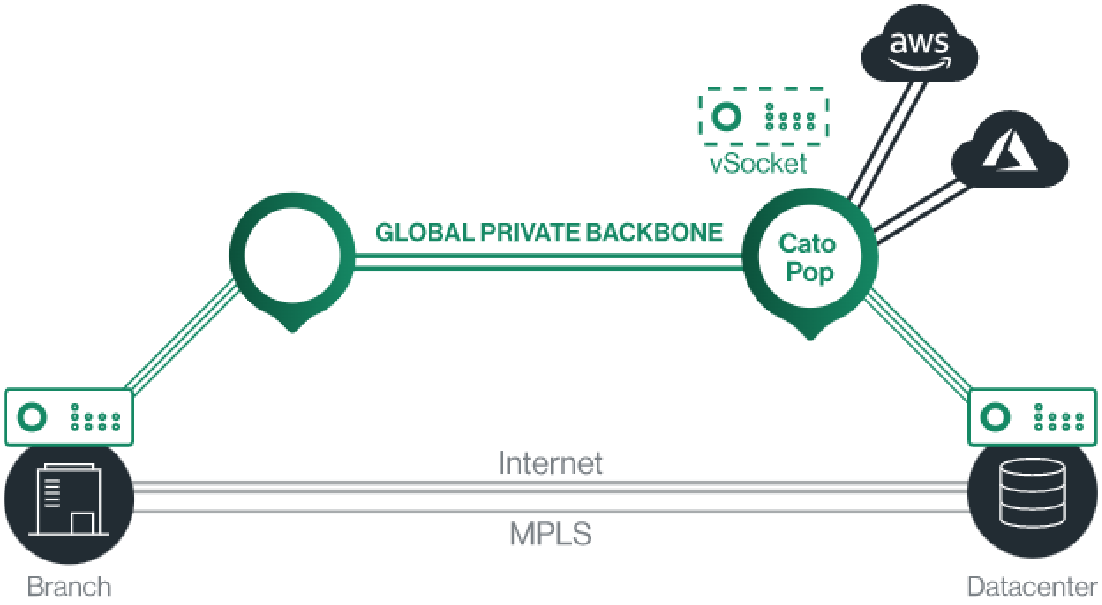


Figure 42: Cato Cloud-Native Architecture *[33]*

2.2 Aryaka SD-WAN

Founded in 2009 by a group of entrepreneurs, the emphasis was to provide an infrastructure experience that is simple in operation and is highly responsive to adjust to the growing needs of the business. The name is derived from Sanskrit, which roughly means noble or truthful. Over the years, Aryaka has become very popular and has office locations in many major countries of the world, including the USA, UK, India, China, Singapore, and the Netherlands [35].

Figure 43: Aryaka *[35]*

The **SD-WAN** service in **Aryaka** is provided by integrating a global Layer 2 network and SD-WAN, providing Network as a Service. Aryaka provides VPN connections to their globally distributed Point of Presences to connect to the Layer 2 backbone, so only an internet connection is required for the customers [36]. In 2019, Aryaka revised its SD-WAN product, saying that it now has a multi-cloud architecture, and SD-WAN was expanded not just for global but also for regional deployments [37].

2.2.1 SmartServices Platform

The SD-WAN in Aryaka is managed by a platform called SmartServices Platform, which is software-based and consists of 6 services, namely SmartManage, SmartConnect, SmartOptimize, SmartCloud, SmartSecure, and SmartInsight [37]. Let us see them one by one.

1. <u>SmartManage</u>
   We can look at this from two angles. From a physical point of view, it consists of the network's PoPs, connections, and the ANAPs (Aryaka Network Access Points), and from a virtual point of view, it takes care of automation and orchestration [37].
   Aryaka uses a tool called ANMC (Aryaka Network Management and Control) for automation and orchestration, and for monitoring, Aryaka uses Aryaka EagleEye. EagleEye has the full visibility of the network and can perform analytics functions which helps it to identify issues in the network before they can have any impact. So, SmartManage is the foundation of the network [37].
2. <u>SmartConnect</u>

   This service uses SD-WAN to connect the branches, remote locations, and data centers of an organization and the organization itself to various cloud service providers. So, SmartConnect connects and manages the SD-WAN connections among multiple nodes within an organization [37].

SmartConnect provides end-to-end connection securely by managing the first and last mile circuits as part of its secure SD-WAN with an MPLS-like private network core. SmartConnect also provides provision for bandwidth bursting to handle traffic spikes which provide optimum user experience [37].

3. SmartOptimize

   SmartOptimize is used by SmartConnect to make sure that the traffic is optimized and compressed so that the services are provided on demand. Intelligent edge optimization, multi-segment transport optimization for TCP, CIFS (Common Internet File System), advanced redundancy removal for uncompressed and unencrypted traffic, application acceleration for SSL, and SMB (Server Message Block) makes sure that the traffic in WAN gets optimized [37].

   A part of SmartOptimize called LinkAssure makes sure that link aggregation is performed and the complexity in the network is reduced. So LinkAssure takes care of load balancing, path selection, and single/dual-link packet loss recovery through error correction algorithms [37].

4. SmartCloud

   SmartCloud makes sure that the customers are connected to the cloud. Customers can connect to several clouds' IaaS (Infrastructure as a Service) and SaaS (Software as a Service) services. In the cloud, customers can connect to SaaS applications using cloud acceleration capabilities, reducing latency and packet loss [37].

   Customers can also connect to various popular IaaS like AWS, Google, etc., using the Cloud Direct Connect feature in the SmartCloud, and these connections are very fast due to Aryaka PoPs' regionally distributed links. And if the number of cloud users becomes too large, SmartCloud has a tool called the Cloud Transport gateway, which optimizes and manages the traffic [37].

5. SmartSecure

   SmartSecure does the job of making sure that security is in place, using firewalls in network access points and site segmentation. Partnership with Zscaler and Palo Alto Networks has made the cloud environment even more secure [37].

   Aryaka's private network core has partitioned connections between customers, making sure that the data is encrypted. This private network core in Aryaka also provides protection against Distributed Denial of Services (DDoS) attacks [37].

6. SmartInsight

   SmartInsight has high visibility of the network and provides detailed insights to the customers. MyAryaka cloud portal provided this visibility of the infrastructure of SD-WAN and applications which are generating the traffic. This helps the organizations in identifying issues and making sure that the SLAs (Service Level Agreements) are met [37].

SmartManage performs its analytics in SmartInsight, helping organizations to decide the resources they will need and how much, based on the trends provided by the analytics [37].

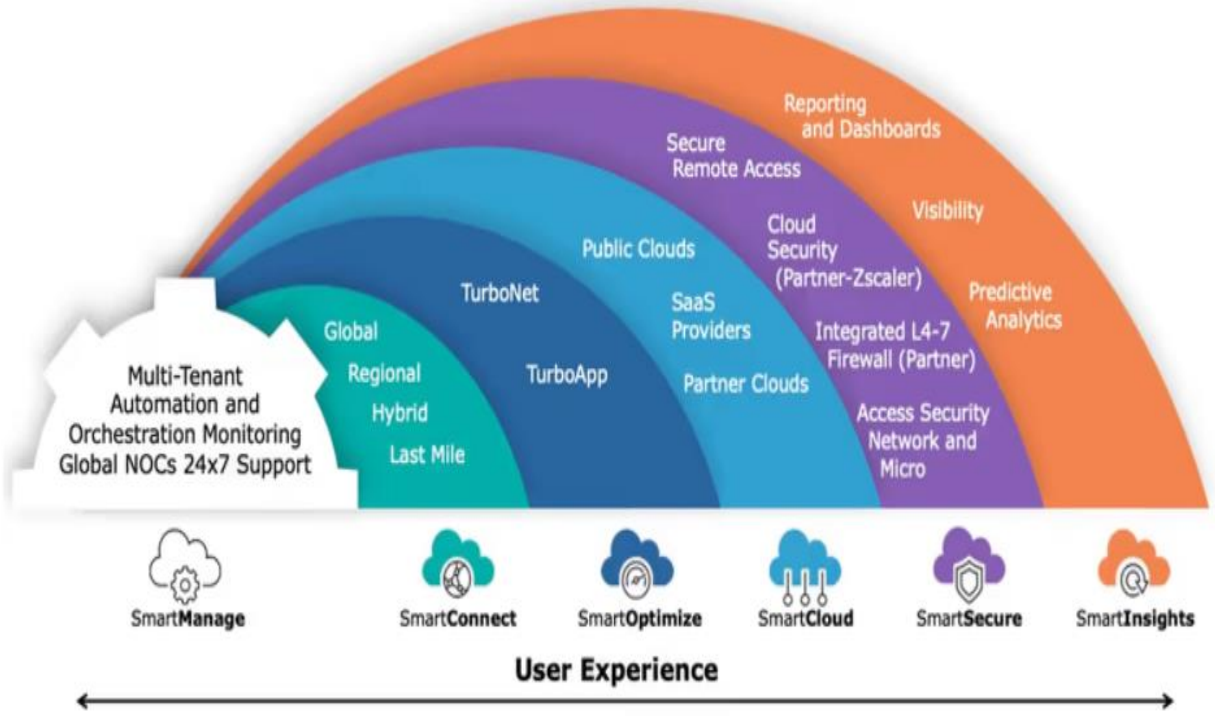


Figure 44: Aryaka SmartServices Platform *[37]*

In December of 2021, Aryaka announced that it would bring a new Layer 3 private core with the aim of lowering the cost even more [38].

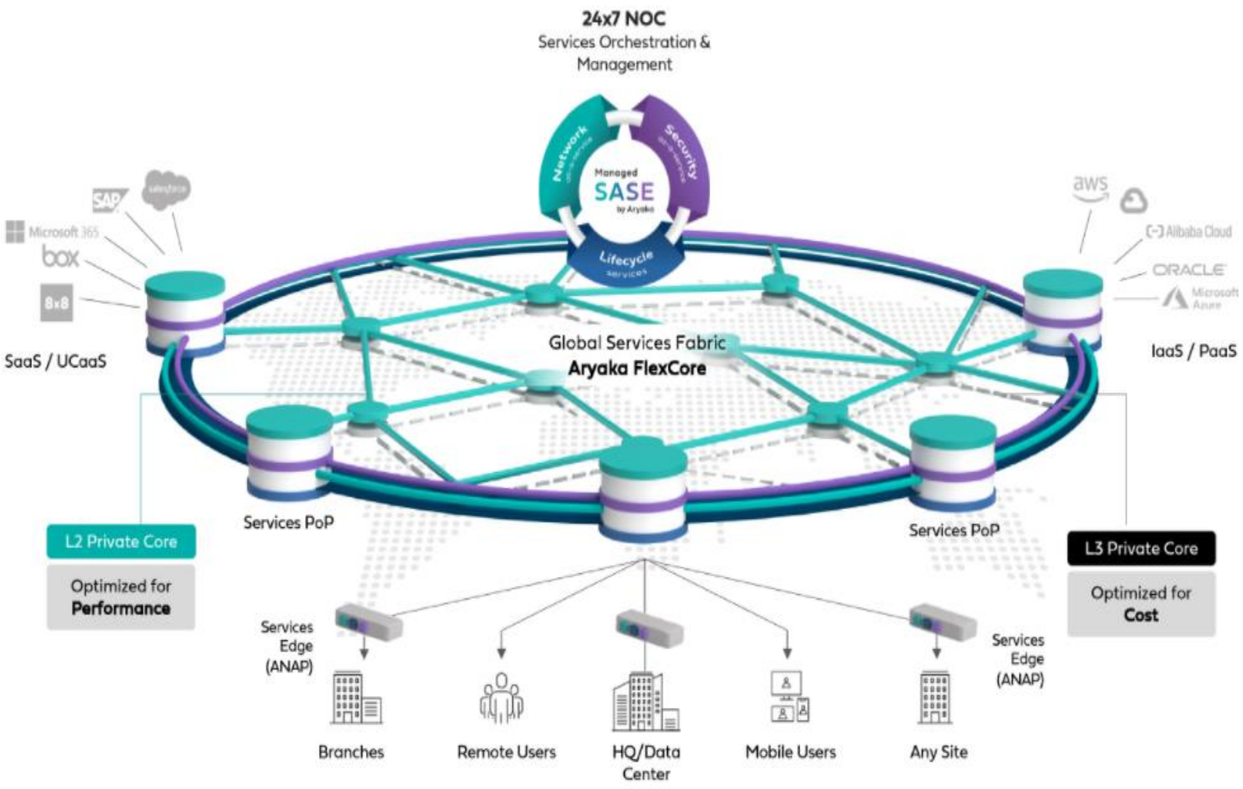


Figure 45: FlexCore with L2 and L3 private cores *[38]*

2.2.2 Capabilities of Aryaka SD-WAN

Now let's use some core capabilities of Aryaka's SD-WAN:

- All in one Managed Service: A complete SD-WAN service that connects enterprise sites, hybrid workers, and cloud workloads, as well as world-class service, support, and a comprehensive set of service level agreements that are appropriate for the cloud-first era [39].
- Aryaka FlexCore^{TM}: Aryaka's FlexCore L2 and L3 backbone network has optimum performance and has more than 40 PoPs present across the globe serving businesses with low latency [39].
- Link, App, and WAN Optimization: SmartConnect is a proprietary end-to-end application and network optimization solution [39].
- White-Glove and Co-Management Options: The SD-WAN services are provided with global service deliveries, and customers have the choice to select integrated support and white-glove services [39].
- MPLS Interworking & Hybrid WAN: The FlexCore network backbone provides easy and smooth integration of connectivity options for existing MPLS, site-to-site internet, and public internet paths [39].
- Last Mile Services: Aryaka makes procurement and management of last-mile services very easy and makes sure end-to-end network management coverage is provided. Reliable connectivity is ensured by providing dedicated professional

support, 24x7 link monitoring coverage, and intelligent link availability technologies [39].

Aryaka came up with expanded SD-WAN offerings recently, namely SmartConnect Pro and SmartConnect EZ. Aryaka adopted the “T-shirt sized pricing” into the SmartConnect offering to simplify the quoting, deployment, consumption, change management, and tracking. It would use the 5 T-shirt sizes, S, M, L, XL, and XXL. The SmartConnect Pro supports the existing L2 private core and connects it to the T-shirt-sized consumption and packaging. The SmartConnect EZ does the same with the L3 private core and is cheaper than the traditional overlay SD-WAN or Enhanced Internet and can be combined with last-mile services for better deployment. Having the same underlying architecture (PoP-based), customers are provided with flexibility when engaging with one another or even changing to other service [38].

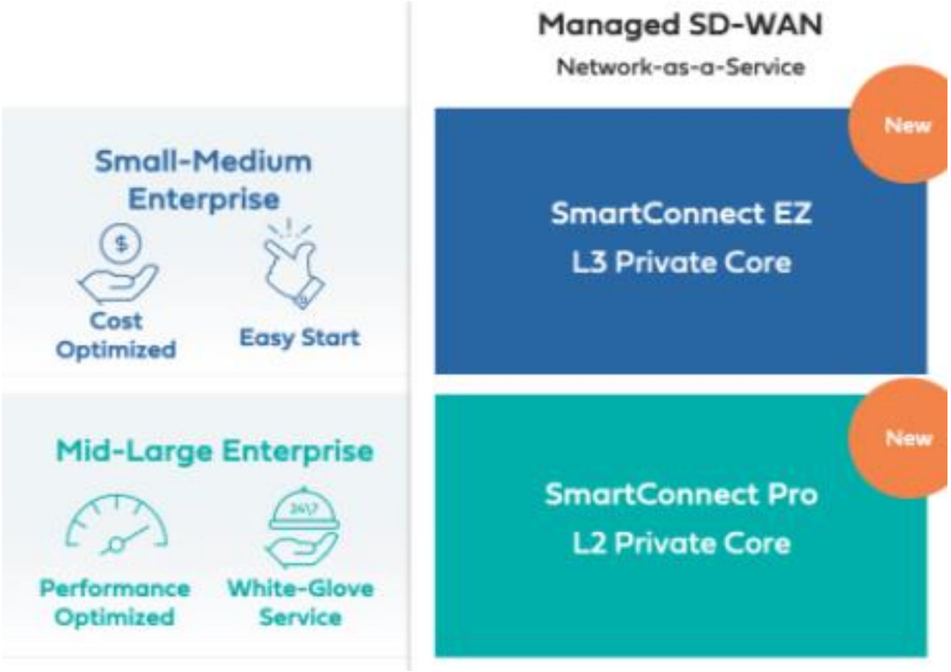


Figure 46: SmartConnect EZ and SmartConnect Pro *[38]*

2.2.3 Benefits of Aryaka

The benefits of opting for Aryaka’s SD-WAN solution include a delightful experience for the customers, better performance by the applications, and flexibility [39]. From a business point of view, these benefits are very helpful, and Aryaka is arguably one of the best SD-WAN providers in the market right now.

2.3 Cisco SD-WAN

In the field of global networking, Cisco is the leader as around 85 percent of traffic goes through Cisco's systems. Founded in 1984 by two computer scientists from the same university (Stanford University), Cisco has become a multi-national corporation. Thousands of employees are associated with Cisco in more than 115 countries. Cisco is the concrete foundation of many service providers, businesses, government agencies, institutions, and many more [40].

Figure 47: Cisco *[40]*

The SD-WAN comes in two solutions from Cisco, namely **Cisco Meraki** and **Cisco Viptela**. Cisco took over Meraki in 2012, and the motive behind that was to improve the WLAN and cloud networking business. The more popular one is Viptela, which was acquired by Cisco in 2017 and delivered advanced routing, segmentation, and security for enterprises in their networks and internetworks. Cisco took its own existing platforms and solutions and integrated them with the cloud-first network management, orchestration, and overlay network technologies of Viptela [41].

2.3.1 Cisco Cloud-Scale Architecture

Cisco developed a cloud-scale architecture, which meets the various complex requirements of enterprises via three key areas, which are Advanced application optimization, Multi-layered security, and Simplicity [42].

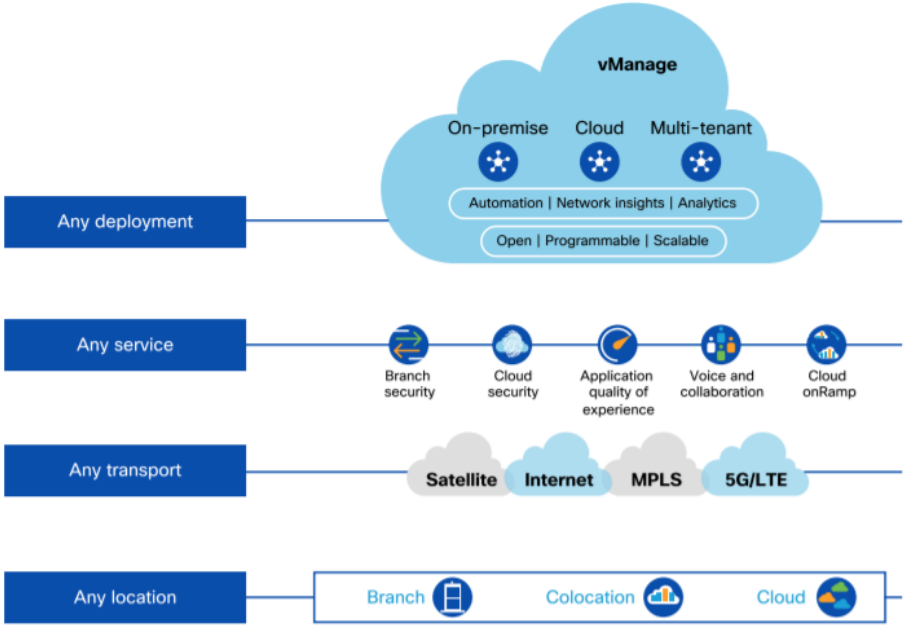


Figure 48: Cloud-Scale Architecture of Cisco SD-WAN *[42]*

The cloud-delivered solution of Cisco can be divided into four planes. These are the Data plane, Control plane, Management plane, and Orchestration plane [42]. The following image shows the four planes and how SDN is integrated into WAN.

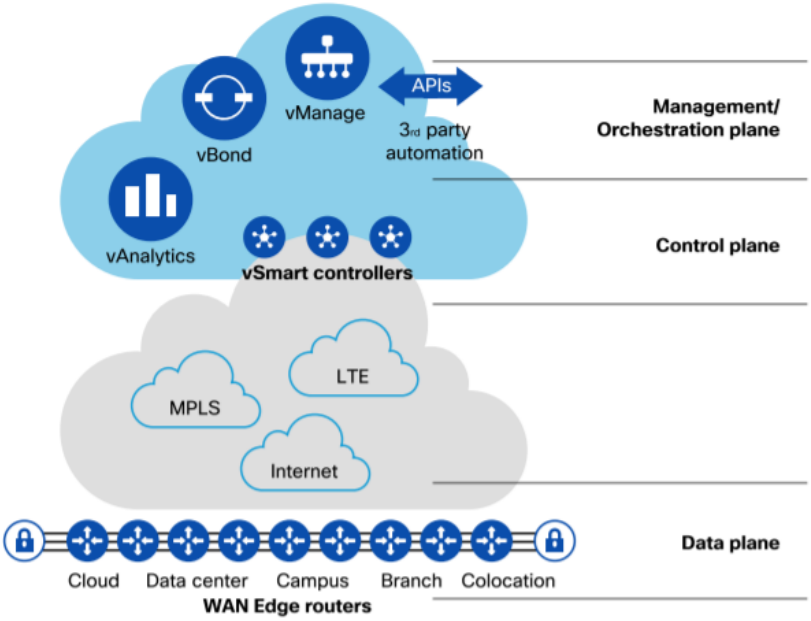


Figure 49: Cisco SD-WAN layers *[42]*

2.3.2 Components of Cisco SD-WAN

There are four key components in the Cisco SD-WAN solution. These include Cisco vManage, Cisco vBond, Cisco vSmart, and Cisco WAN Edge routers [42]. Let us look at them one by one.

1. Cisco vManage: Cisco vManage is the UI, and it lets the IT professionals do the configuration, provisioning, troubleshooting, and monitoring of the connections among various nodes in the organization's WAN. It resides in the management plane and is a single dashboard offering the controlling options. Based on the requirements, both single-tenant dashboards and multi-tenant dashboards are available [41] [42].
2. Cisco vBond: Cisco vBond is present in the orchestration plane and provides zero-touch provisioning. It also facilitates authentication, distributing control and management information, and NAT (Network Address Translation traversal). When a router is not configured, vBond onboards it into the SD-WAN, it understands the network and provides this information to other components [42].
3. Cisco vSmart: It resides in the control plane and is the part that does the 'thinking', enforcing the policies established on the vManage. The routing information of a branch when it comes online is exchanged with the vSmart controller. Based on the policies set earlier, the routing information is shared with different locations determining how the communication between them will take place. It uses a protocol called OMP (Overlay Management protocol) for exchanging information between the sites and vSmart [42].
4. Cisco WAN Edge routers: Cisco WAN Edge routers are part of the SD-WAN overlay fabric. They are managed through vManage and can be present in various positions, like a branch, campus, data center, or the cloud itself. They can either be deployed on the hardware or the virtual platforms. Hardware ones include the cisco vEdge routers, ISR (Integrated Services Router) 1000 and 4000 series, and the ASR (Aggregation Services Router) 1000 series, whereas the virtual ones include CSR (Cloud Services Router) 1000v and the vEdge Cloud router. SD-WAN overlay is created by the WAN Edge routers to form the IPSec (Internet Protocol Security) tunnels among one another. Also, a control channel is created between these routers and every control element with which they receive configuration, provisioning, and routing information [42].

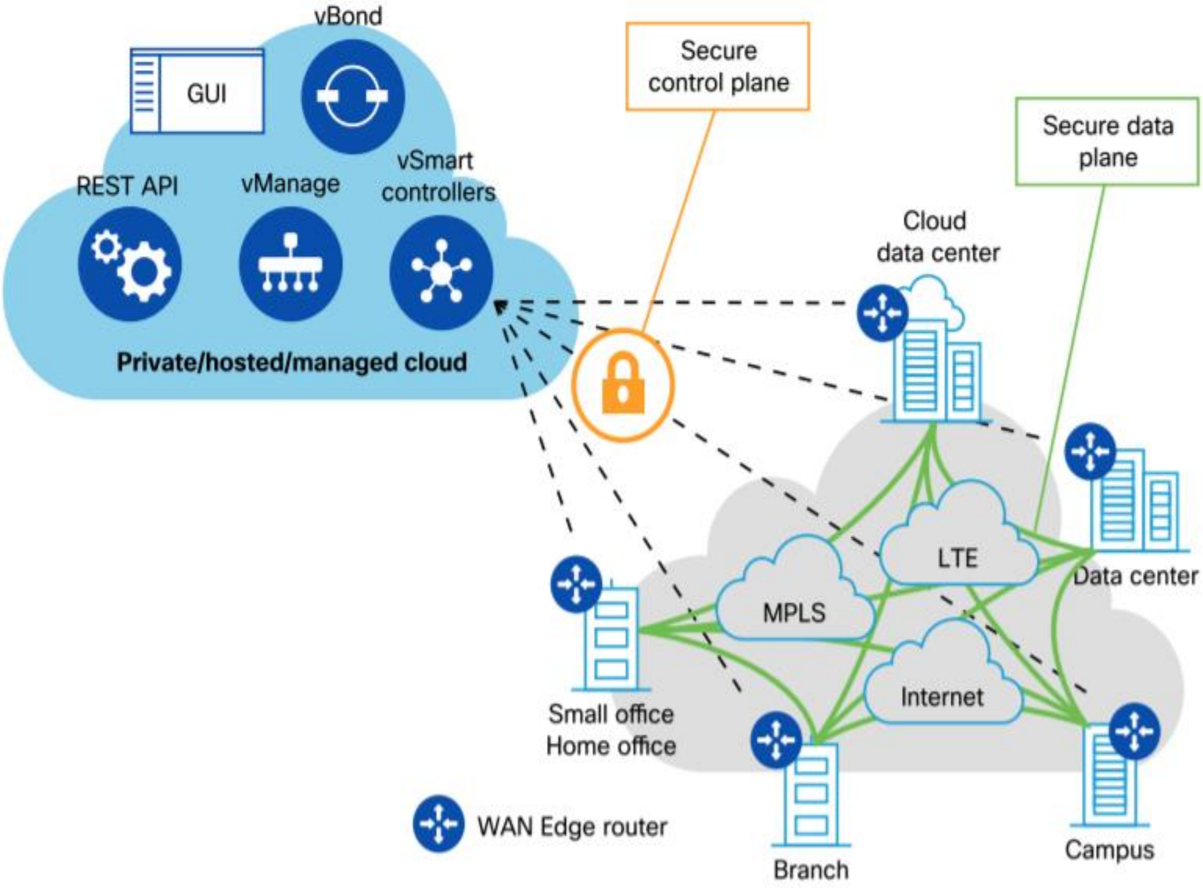


Figure 50: Cisco SD-WAN components *[42]*

Earlier, we named a protocol called **Overlay Management Protocol (OMP)**. It is the protocol that runs between the vSmart controllers and the Edge routers and manages the overall network. OMP makes sure that control plane information is exchanged securely between the vSmart controllers and the Edge routers, and by default, a full mesh topology between the WAN Edge routers is allowed, which allows each of these routers to directly connect to other Edge routers [42].

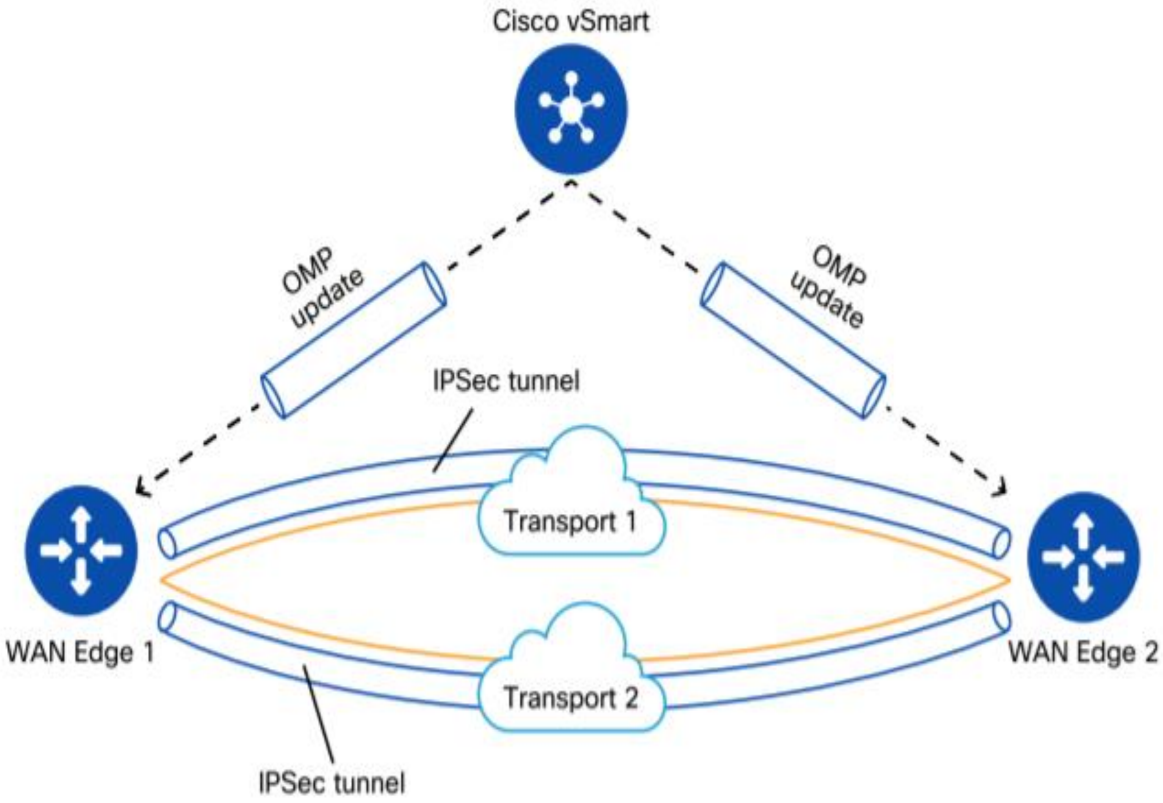


Figure 51: Overlay Management Protocol *[42]*

2.3.3 Benefits of Cisco SD-WAN

Let us now look at some key benefits of the Cisco SD-WAN solution:

- Connection to the cloud: With Cisco SD-WAN, connection to the applications in the cloud is very convenient. With the Cloud onRamp for SaaS (Software as a Service) and IaaS (Infrastructure as a Service), connections to certain applications are optimized, and services are provided as a part of the SD-WAN overlay [42].
- Security: To make the infrastructure more secure, strong defense mechanisms are present inside the Edge routers, including a Stateful application firewall, IPS/IDS (Intrusion Protection and Detection), URL filtering, Cisco AMP (Advanced Malware Protection), tunneling to secure gateways in the cloud vis third parties, and much more [42].
- Application Experience: To provide optimum user application experience, Cisco provides QoS, FEC (Forward Error Correction), packet duplication, application-aware routing, TCP optimization, and Cloud onRamp. These further include more features like DPI (Deep Packet Inspection), traffic prioritization, packet duplication feature, and many more [42].

- Management and Operations: Automated management and simplified operations are two of the key points provided by Cisco SD-WAN. To manage, monitor, and troubleshoot, a single pane of glass is there in Cisco vManage. Network information like availability, performance, anomalies, etc., can also be viewed by a SaaS-based service called vAnalytics [42].

2.4 Juniper 128 SD-WAN

Juniper Networks was founded in 1996, and it is headquartered in a city in California called Sunnyvale. Juniper has become one of the major companies in technologies involving Cloud, WANs, Artificial Intelligence, and many more. Juniper provides support to most of the top global companies, service providers, cloud providers, universities, banks, and many more institutions. Juniper has thousands of employees and has a global reach via more than 100 locations spread across 50 countries [43].

Figure 52: Juniper Networks *[43]*

The **SD-WAN** solution provided by **Juniper** is driven by Artificial Intelligence (AI). Along with AI, Juniper has its Juniper Mist Cloud and Session Smart Routers. A little over a year after acquiring **128 technology** (in 2020), Juniper used their Smart Session Routers and now has connected them to its Mist Cloud. All these combined provide an unmatched experience to the customers, along with various insights and automation, thus lowering the complexity of the network [44] [45].

Juniper's SD-WAN solution is made using their first-ever tunnel-free, session-based architecture, with zero trust security. The tunnel-free technology helps in reducing bandwidth consumption and thereby increases the overall performance of the applications. Zero trust security makes sure that security and performance are maintained by providing deny-by-default, global access control, per-hop authentication, and adaptive encryption. This leads to an improvement in SLAs (Service Level Agreements) and a very enhanced experience for the customers [44].

2.4.1 Benefits of AI in Juniper SD-WAN

It was mentioned before that Juniper uses Artificial Intelligence in its SD-WAN solution. Let us see some benefits that AI provides to this product.

- Templating: It allows professionals to configure and deploy their devices, services, and policies quickly via automation. Thus, it is a very helpful tool for scaling purposes, eliminating various inconsistencies and minimizing the headache that comes with configuration [46].
- Adaptive Encryption: This makes sure that proper encryption takes place without reducing the overall performance by minimizing the headend infrastructure which

supports IPsec tunnels. This makes sure that the user experience remains optimum [46].

- Inflow Performance Monitoring: Juniper’s SD-WAN solution measures performance in-band or inflow with the session itself and does all this using a very small amount of bandwidth. This is a different technique from other vendors and provides more accurate performance data, thus giving better visibility of the network performance [46].
- AI-Powered WAN Assurance: With Juniper’s solution for SD-WAN, various network issues and insights can be viewed and solved even before the user notices them. AI-Powered WN Assurance provides instant insights, identifies network issues, and reduces the meantime to repair [46].
- Session Capture: This lets us track a specific packet across the network, hop by hop, thus providing the exact data that is required. A tool called the Session Capture tool is used to do this by performing session-based captures across multiple routers and executing trigger-based automated captures [46].

2.4.2 Products of Juniper SD-WAN

Juniper’s AI-driven SD-WAN provides multiple products in the market right now. Let us have a look at each of them one by one.

- Session Smart Router

  The key features of this Session Smart Router include application-aware routing, fail-safe service delivery, orchestration, automation, zero-trust security, and a centrally Mist Artificial Intelligence Cloud-managed option. All these features lead to more agile, secure, and resilient connections in the WAN [47].

  These features make the router very flexible, providing many benefits. These benefits include unparalleled user experience, reduction in cost, providing better visibility and insights, zero-trust security, helping in scalability, a more responsive network, better application awareness and control, and centralized Cloud Management. These benefits provided by the Smart session Router really take SD-WAN to a whole new level [47].

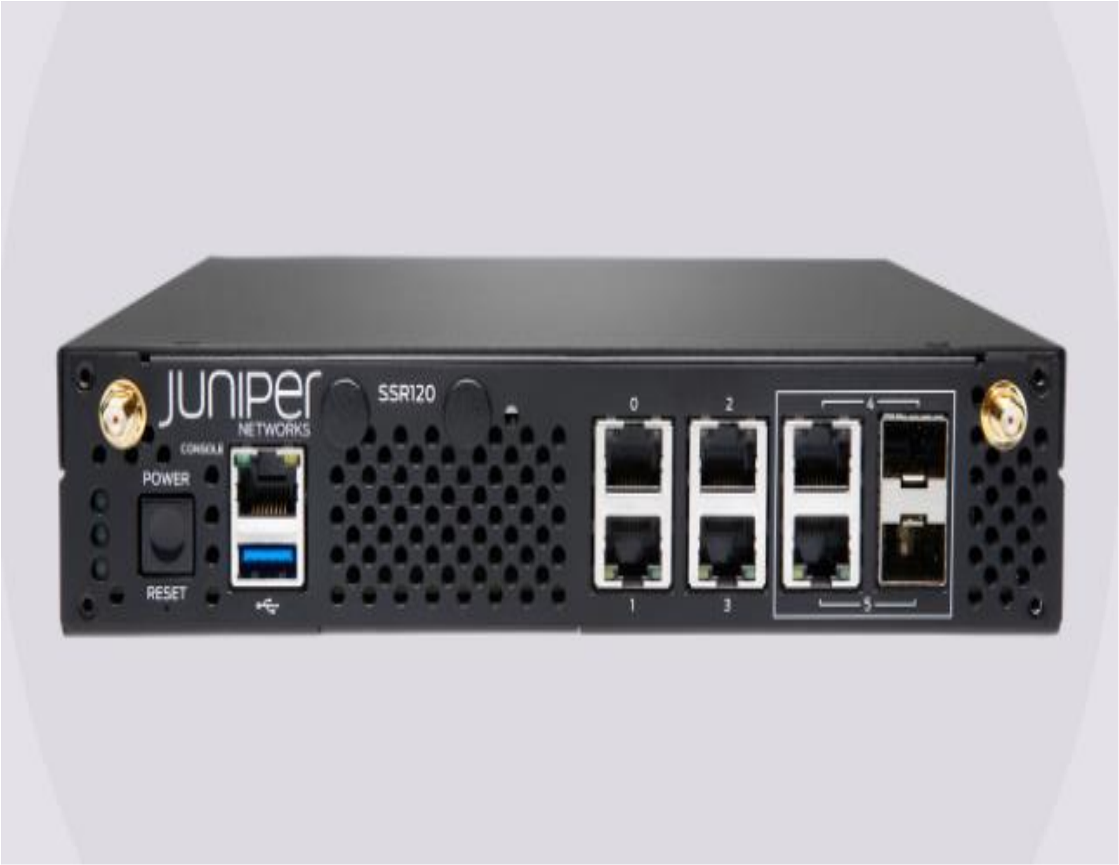


Figure 53: Smart Session Router *[47]*

- Marvis VNA

  It is the Virtual Network Assistant (VNA) in the SD-WAN product and provides a conversational interface that uses natural language to understand the user's intent. It can provide recommendations or even take action when it encounters an issue. It provides real-time insights and easy troubleshooting to improve service delivery. Other features include anomaly detection within SLEs (Service Level Expectations), accurate root cause analysis (using Bayesian Interface), an android application for network visibility, determining the scope, and self-driving actions framework [48].

- Mist WAN Assurance

  It is the cloud offering by Juniper and provides easy deployment, better visibility, and less mean time to repair various issues. It monitors and enforces SLEs (Service Level Agreements). It is also responsible for automatically identifying misconfiguration in the gateways and interfaces and correcting them. Some other features include AI-driven application insights centralized Cloud-based onboarding (with zero-touch provisioning and templates) [49].

2.4.3 Benefits of Juniper

The benefits provided by the Juniper SD-WAN solution are many. Firstly, the overall user experience is exceptional through various AI-driven insights, automation, and actions. Customizable SLEs, anomaly detection, event correlation, fast fault isolation/resolution are some other features. It has its own AI-driven Virtual Network Assistant called Marvis, which provides various functionalities like deep insights and troubleshooting actions. Machine learning is used to provide advanced threat prevention services, making the network a lot more secure. Juniper products integrated with its partners provides services that are unmatched in the market right now, making Juniper one of the best SD-WAN providers right now [50].

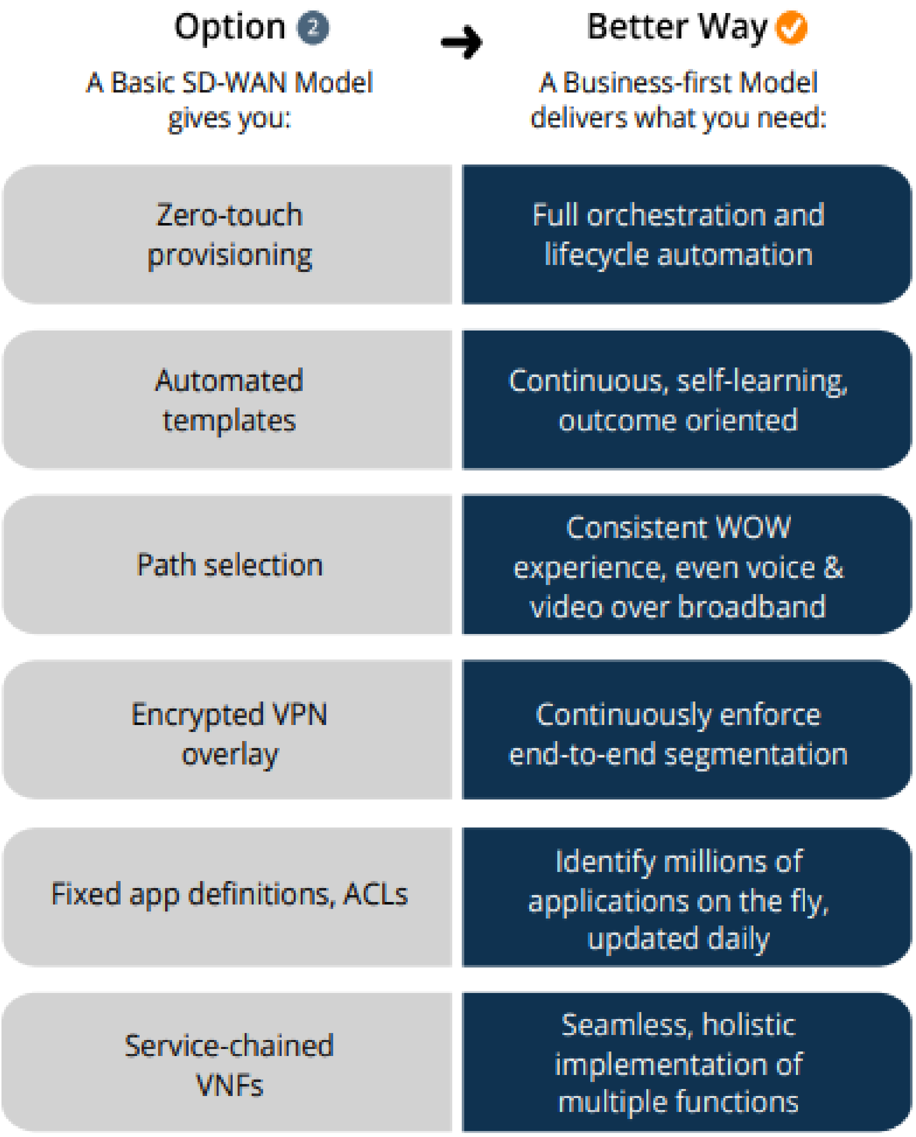
2.5 Silver Peak SD-WAN

Founded in 2004 in California, Silver Peak is a company that delivers WAN products, like WAN optimization or SD-WAN. It is a global company and has partnerships with various big companies like Dell, VMware, etc. In 2020, it was acquired by HPE (Hewlett Packard Enterprise), and now it is a part of another HPE acquired company, Aruba Networks [51].

Figure 54: Silver Peak *[51]*

The **SD-WAN** product by **Silver Peak** is now sold under **Aruba** Networks. The platform is provided by the Aruba EdgeConnect SD-WAN, and it is different from other SD-WAN products in the way that other products' main emphasis is on various abilities like centralized management, dynamic path selection, zero-touch provisioning, encryptions, etc., while the solution provided by Silver Peak/Aruba Networks focusses on providing Business-First Networking Model, which is a little bit different than the normal models, and provides some benefits over them [52].

The following image illustrates these differences.



Option 2 A Basic SD-WAN Model gives you:	→	Better Way ✓ A Business-first Model delivers what you need:
Zero-touch provisioning		Full orchestration and lifecycle automation
Automated templates		Continuous, self-learning, outcome oriented
Path selection		Consistent WOW experience, even voice & video over broadband
Encrypted VPN overlay		Continuously enforce end-to-end segmentation
Fixed app definitions, ACLs		Identify millions of applications on the fly, updated daily
Service-chained VNFs		Seamless, holistic implementation of multiple functions

Figure 55: Basic SD-WAN model vs Business-First model *[52]*

2.5.1 Aruba EdgeConnect Platform

The Aruba EdgeConnect platform is comprised of three products, namely Aruba EdgeConnect, Aruba Orchestrator, and the Aruba Boost [53]. Let us see them one by one.

1. Aruba Edgeconnect

It is the SD-WAN appliance deployed at the branch sites creating the network overlay. Its key features include **business intent overlays** (to provide various services like QoS, transport, security, etc.), **path conditioning** (to overcome the problem of dropped and out of order packets), **tunnel bonding**, **first-packet iQ application classification** (to identify applications on the first packet to select the correct path), **cloud intelligence**, **secure**

internet breakout (to eliminate bandwidth wastage and provide better performance), **UTM** (Unified Threat Management, the defense system which provides advanced Intrusion Detection and Prevention), **better segmentation** (with the Aruba ClearPass integration), **zone-based stateful firewall**, **SASE integration** (with trusted partners like Zscaler, McAfee, Netskope, etc.), **routing** (supporting L2 and L3 protocols), **high availability** (HA to protect from various failures), **zero-touch provisioning** and **WAN hardening** (to deny entry for unauthorized traffic) [53].

Figure 56: Aruba EdgeConnect *[53]*

2. Aruba Orchestrator

The Aruba Orchestrator provides full visibility and control over the WAN by providing an interface to define, assign, and enforce various policies centrally across the WAN via single-screen administration. It also provides real-time visibility and monitoring of the network, also providing automation and continuous control. Centralized orchestration of different network functions, which includes SD-WAN routing, segmentation, application visibility, control, etc., is also there [54].

3. Aruba Boost

Aruba Boost is an optional feature whose main task is to accelerate applications so that they perform better, the effect of latency is minimized, and make sure that the available bandwidth is maximized. This leads to an improvement in application response times. Also, data compression and deduplication make sure that the duplicate data is not retransmitted, which accelerates applications that are data sensitive. It also provides its services in the cloud by deploying them in Infrastructure as a Service (IaaS). Centralized visibility and control lead to flexibility and rapid time-to-service [55].

2.5.2 Benefits

Let us now look at some of the key benefits provided by this SD-WAN:

- Business-Driven

It follows the top-down business policies, making it ideal for enterprises, as they can ensure that the applications are delivered to the users in a way that they can prioritize their different business needs. Various resources in the network are utilized in a way that matches the business criticalities of different applications [52].

- Quality of Experience
  It makes sure that both end-users and the IT staff enjoy the optimum experience through the continuous learning, adaptation, and automation provided by the platform. With various features like path conditioning, Aruba Boost, centralized orchestration, automation, and many more, users experience a high quality of services, and the IT teams can make changes, do troubleshooting, and do other tasks with convenience [52].
- Continuous Adaptation
  With Machine Learning, the network becomes self-driven, and the applications change themselves when some features are added or when the IP addresses used by the applications are updated. This eliminates the need to use any application without doing anything manually. With continuous monitoring and analytics, any change in the conditions is detected, and their responses are triggered in real-time [52].
- Unified Platform
  All the different systems and services like SD-WAN, firewall, WAN optimization, etc., are unified in a single platform that is centrally managed, providing convenience. Also, all the hardware, software, and cloud delivery models are interoperable, which provides flexibility and fast deployment. Aruba also partners with other enterprises through service chaining, and it supports the broadest security and cloud partner ecosystem with other leaders in security, cloud, and service providers [52].

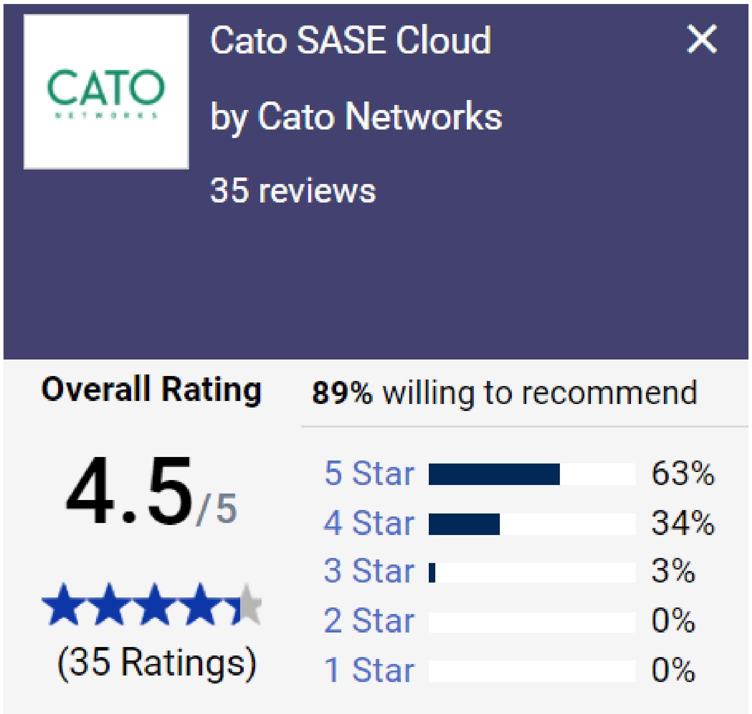
Business-Driven
Highest Quality of Experience
Continuous Adaptation
Unified Platform

Figure 57: Benefits of Aruba EdgeConnect SD-WAN Platform *[52]*

2.6 Comparisons

Let us now compare these SD-WAN solutions with each other. Based on the verified reviews provided by Gartner, which is a well-known platform for comparisons among various technologies, the top-rated product among the mentioned SD-WAN vendors is provided by **Juniper Networks**. Out of 5, it received an unmatched 4.9 stars. It was followed by Aruba EdgeConnect SD-WAN (4.8), then Cisco Viptela SD-WAN (4.7), Aryaka (4.6), and the last one with 4.5 is Cato [56]. Let us see each one of them in brief.

Starting with **Cato**, let us see some pros and cons that were mentioned in the reviews. It is reliable, easy to set up and configure, secure, and provides excellent connection and support. But some reviews mentioned its lack of integration with 3rd parties, some beta packages were buggy, and the single-sign-on integration is not up to the mark, giving it an overall score of 4.5 out of 5 [57].



Cato SASE Cloud

by Cato Networks

35 reviews

Overall Rating

4.5/5

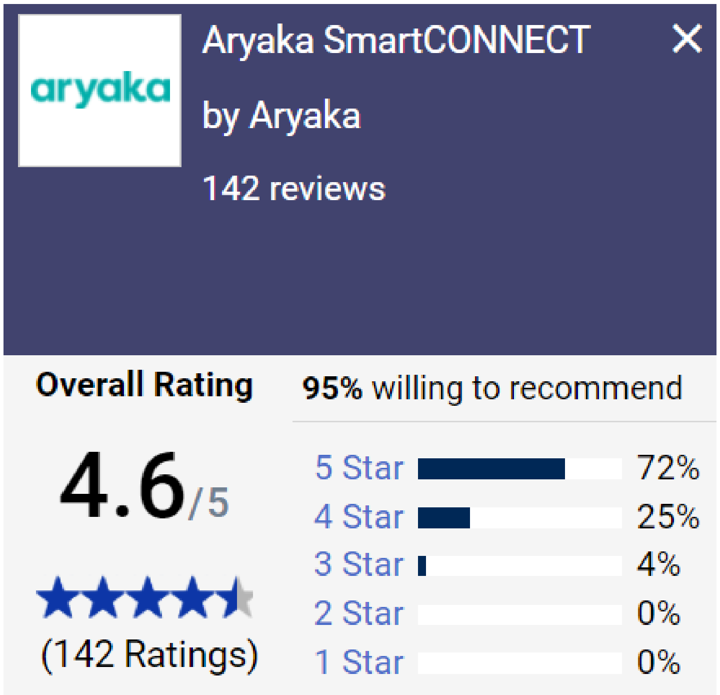
(35 Ratings)

89% willing to recommend

5 Star	63%
4 Star	34%
3 Star	3%
2 Star	0%
1 Star	0%

Figure 58: Cato ratings *[56]*

The next one is the **Aryaka** SD-WAN product. Its simplicity in everything is highly praised, and the reviews regarding latency, security, cloud connection, end to end connectivity are also positive. However, there were mixed reviews regarding help desk support, and the cost was also a bit higher. Out of 5, it scored 4.6 overall [58].



Aryaka SmartCONNECT

by Aryaka

142 reviews

Overall Rating

4.6/5

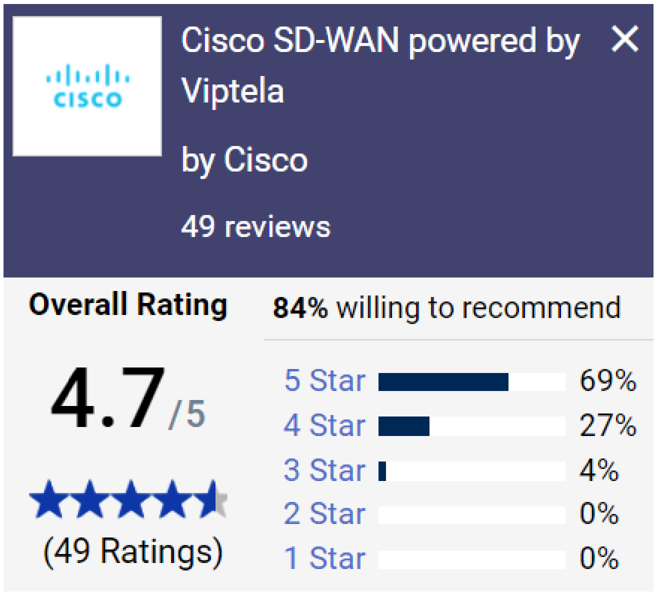
(142 Ratings)

95% willing to recommend

5 Star	72%
4 Star	25%
3 Star	4%
2 Star	0%
1 Star	0%

Figure 59: Aryaka ratings *[56]*

Now comes the solution provided by **Cisco Viptela**. The biggest benefit mentioned was that it would work on existing routers and lines, which is great in cost-saving and scaling. Zero-touch deployment and its central controller have been praised. However, some concerns regarding the complexity are there, and some reviews suggested that Cisco should focus on one SD-WAN product only, as multiple products could cause some confusion. Also, some minor issues with vManage are there, taking its overall score to 4.7 out of 5 [59].



Cisco SD-WAN powered by Viptela

by Cisco

49 reviews

Overall Rating

4.7/5

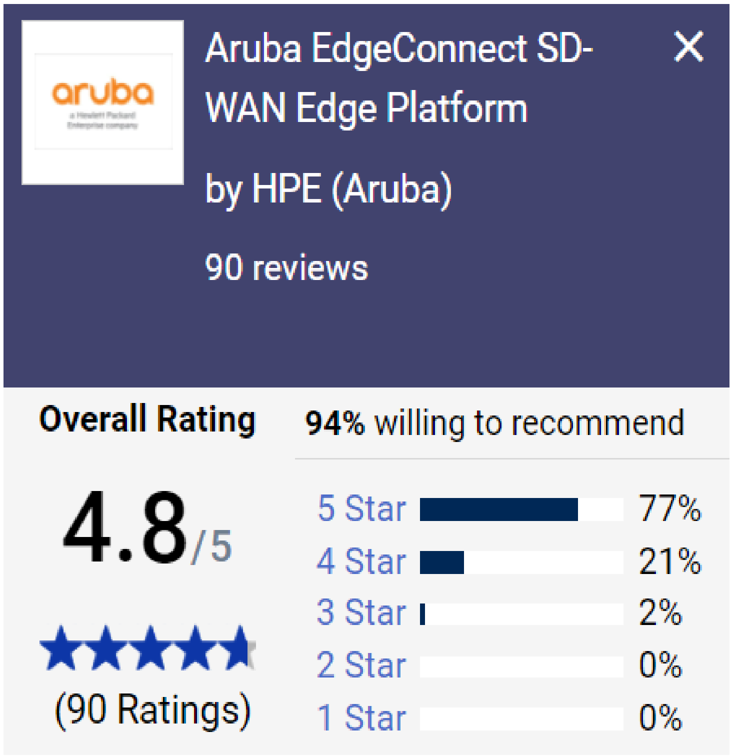
(49 Ratings)

84% willing to recommend

5 Star	69%
4 Star	27%
3 Star	4%
2 Star	0%
1 Star	0%

Figure 60: Cisco Viptela ratings *[56]*

Next is the **Silver Peak** solution, which is owned and distributed by **Aruba**. Almost everything, including controls, support, customization, flexibility, reliability, simplicity, zero-touch deployment, etc., is excellent. There's a little overhead with very frequent upgrades, and some concerns are there regarding the firewall. But overall, it is an excellent product with a rating of 4.8 out of 5 [60].



Aruba EdgeConnect SD-WAN Edge Platform

by HPE (Aruba)

90 reviews

Overall Rating

4.8/5

★★★★★

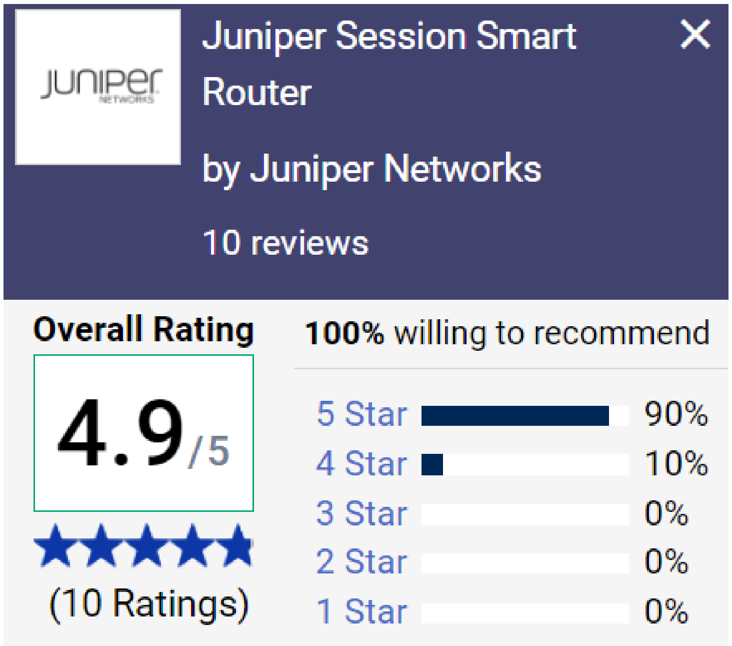
(90 Ratings)

94% willing to recommend

5 Star	77%
4 Star	21%
3 Star	2%
2 Star	0%
1 Star	0%

Figure 61: Aruba SD-WAN platform ratings *[56]*

Juniper comes out as the winner in this list of vendors. Its flexibility, user experience, speed, security, and everything else has been praised. The tunnel-free approach is exceptional, and there is no overhead in using IPSec. However, there are some small issues, like no forward error correction, limited topology view, little learning curve, and little time to adjust to the web UI. These cons are not very significant, and Juniper scores a brilliant 4.9 stars out of 5 [61].



Juniper Session Smart Router

by Juniper Networks

10 reviews

Overall Rating

4.9/5

★★★★★

(10 Ratings)

100% willing to recommend

5 Star	▇▇▇▇▇▇▇▇▇	90%
4 Star	▇	10%
3 Star		0%
2 Star		0%
1 Star		0%

Figure 62: Juniper SD-WAN ratings *[56]*

Section 3: Cloud Solutions

3.1 Cloud

Cloud simply constitutes the data servers over the Internet and the various software and databases running on them. These servers are located globally, and clouds enable users to access the same files and applications from any device. This is very beneficial from a business point of view as they don't have to maintain their own physical servers. Instead, they can simply take the help of cloud vendors, which reduces their costs and overheads. Also, clouds make it possible for companies to go international, as their customers can access their services from any part of the world [62].

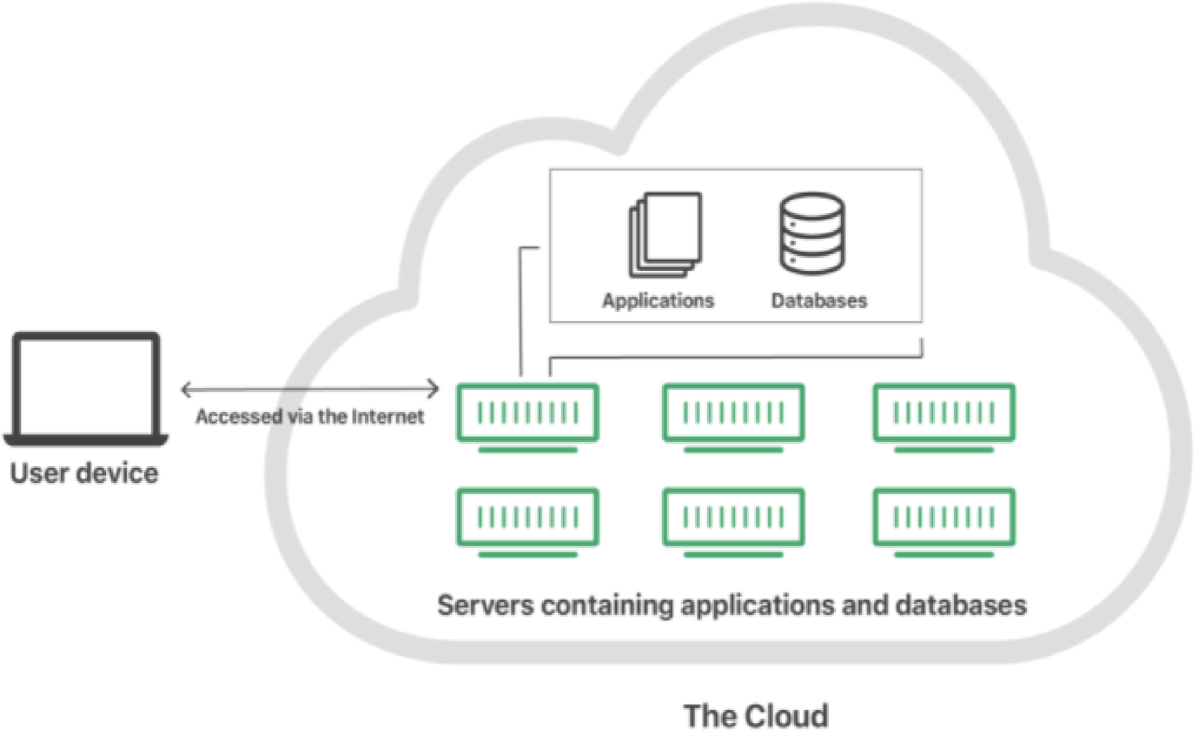

Applications
Databases
User device
Accessed via the Internet
Servers containing applications and databases
The Cloud

Figure 63: How a cloud looks like *[62]*

The above diagram shows how we can visualize a cloud.

Let us see how clouds can be deployed.

- **Private cloud:** This is the type of cloud (a server, a data center, or a network) that belongs to a single organization only; no other organization has access to their private cloud [62].

- **Public cloud:** This cloud is shared by multiple organizations via multitenancy. Its services are run by an outside vendor, and the servers can either be present in one or multiple data centers [62].
- **Hybrid cloud:** This includes a combination of both public and private clouds, like using a public cloud for some services and a private cloud for others [62].
- **Multi-cloud:** Multi-cloud deployments usage of multiply public clouds. It can be a hybrid cloud, and the reverse can also be true [62].

3.1.1 Cloud Networking and its benefits

Cloud networking refers to the connection between various network resources with the help of the cloud. It has become very famous since its inception that in 2019, 9 in 10 companies were already using cloud services. This number will keep on going up as more and more companies will shift to cloud networking in the coming years [63].

In simple terms, for an IT professional, cloud computing refers to the process of designing, configuring, managing, and fine-tuning various network resources to set up networks. These network resources can be virtual routers, VPNs, virtual firewalls, data connectivity, load balancers, virtual bridges, virtual adapters, and many more [63].

Based on the requirements, a choice can be made whether to go for cloud-enabled networking or cloud-based networking. In the case of cloud-enabled networking, the network infrastructure is on-site, but the services and resources provided are present in the cloud. It means that the core part of the network is on the premises, but its management, monitoring, maintenance, security services are done via the cloud. But in the case of cloud-based networking, the entire network, including all the resources and the physical hardware, is in the cloud, which provides connectivity between the various applications and resources in the cloud [64].

Some of the benefits of using cloud networking include:

- **Low Cost:** Because there is no need to buy servers and hardware, the overall cost is reduced considerably [63].
- **Minimum Downtime:** All the cloud resources related updates are handled by the service provider, which means the network teams have one less task to worry about, and the information regarding downtime is provided in advance, which gives the network teams plenty of time to take care of it [63].
- **Scalability:** All the business requirements can be assessed, and the required modifications can be made easily using cloud networking, which is great for scaling purposes [63].
- **Productivity:** As the service provider takes care of lots of resources-related stuff, the network teams can focus on other technical needs to increase their productivity [63].
- **Resilience and Elasticity:** With cloud networking, it is ensured that resiliency is maintained if properly planned and consistent performance is provided [63].
- **Security:** With regular security testing, built-in firewalls, redundancy strategies, and regular security updates, the cloud offers secure networks [63].

3.1.3 Cloud Computing

The terms cloud networking and cloud computing are often confused with each other and used interchangeably. However, these are two different terms with different meanings. Cloud networking deals with the various network resources and how they are handled in the cloud. Cloud computing, on the other hand, deals with the various applications and services (like storage, software, database) in the cloud [63].

Cloud computing is done via virtualization, by creating virtual machines. This makes the hardware even more efficient as multiple virtual machines can run on a single hardware system, meaning one server can act as multiple servers, reducing cost in the process [62].

There are three main service models of cloud computing, namely SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service) [62].

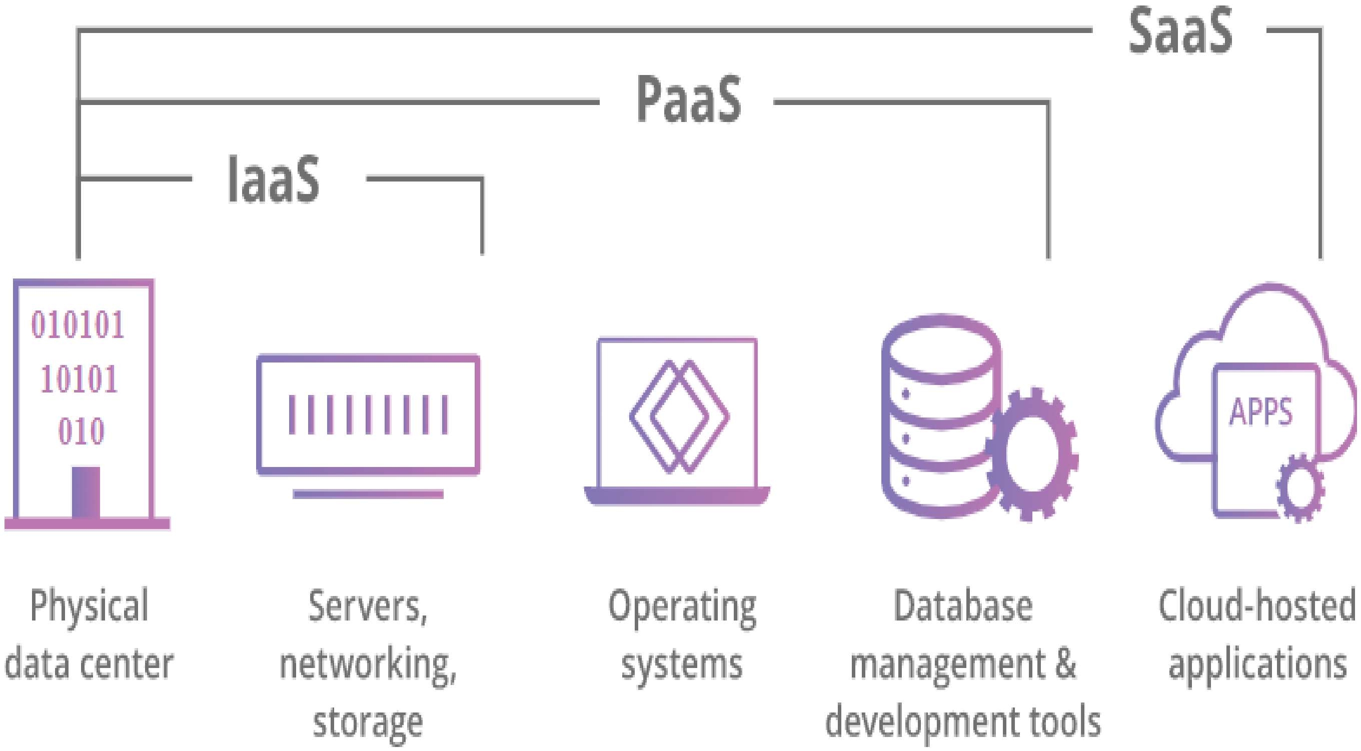

SaaS
PaaS
IaaS
010101
10101
010
APPS
Physical data center
Servers, networking, storage
Operating systems
Database management & development tools
Cloud-hosted applications

Figure 64: Main service models of cloud computing *[62]*

SaaS provides applications on the cloud servers, and users need not install these applications on their devices. **PaaS** provides resources for building an application (like development tools, infrastructure, OS, etc.), and the company only needs to pay for these resources, not for the whole application. **IaaS** lets the companies rent the servers and the storage, and then these companies use them to build their applications [62]. Recently, many more models have been introduced, but these three remain the most popular ones.

3.1.4 CSP SD-WAN Solutions

As more and more companies are heading towards SD-WAN, at first, it was kind of a threat to the CSPs, but now they have taken it as an opportunity and have added the concepts of SD-WAN into their offerings, and some have taken the help of other vendors to include the various functionalities of SD-WAN into their managed solutions. They are using NFV architecture to build their SD-WAN solutions and are using the NaaS (Network as a Solution) model in their offerings [65].

NaaS is a type of cloud service model which allows the customers to rent the different network services available in the cloud from a cloud vendor in which they do not have to establish their own network infrastructure. Like other cloud models, it removes the requirement to buy expensive hardware. It makes the network more flexible, scalable, accessible from anywhere in the world, requires less maintenance, is secure and reduces the overall cost considerably [66].

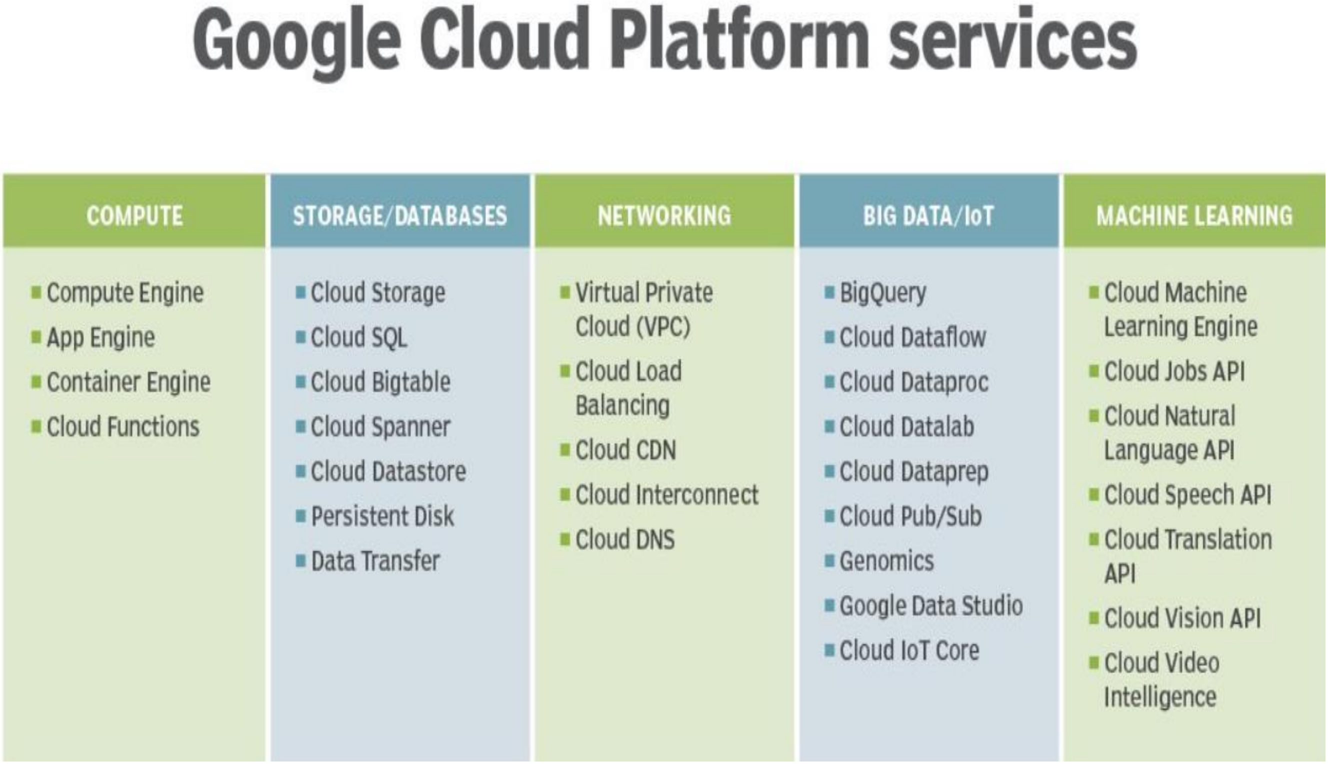
There are three choices when it comes to deploying SD-WAN, DIY (Do-It-Yourself), NaaS, or managed service option. In DIY, the customers take care of the planning, designing, implementing, and managing of their resources. NaaS allows them to be free from these responsibilities but gives them the option for management via a portal. In the case of managed service, an MSP (Managed Service provider) takes care of the implementation and provides functionality to the customers using which they can monitor their network and make changes if required [65].

Investing in advanced analytics is a major factor, as it will help in providing more security to the network and provide various insights. Although there are firewalls and encryptions, some attacks like DDoS can happen, but real-time analytics can take care of such attacks. So, CSPs are now offering these analytics with their products [65].

Clouds have become an important part of SD-WAN offerings. All the solutions that we have mentioned previously offer cloud services. Cato has its own SASE cloud, Aryaka offers SmartCloud, Cisco developed its own cloud-scale architecture, Juniper has its own Mist cloud, and Aruba provides cloud services vis third parties (like AWS).

3.2 GCP

GCP stands for Google Cloud Platform. It was launched in 2008, and it is a suite of Google’s public cloud computing services. GCP consists of several services, including compute, storage, networking, ML (Machine Learning), big data, IoT (Internet of Things), cloud management, security, and developer tools [67] [68].



Google Cloud Platform services

COMPUTE	STORAGE/DATABASES	NETWORKING	BIG DATA/IoT	MACHINE LEARNING
■ Compute Engine ■ App Engine ■ Container Engine ■ Cloud Functions	■ Cloud Storage ■ Cloud SQL ■ Cloud Bigtable ■ Cloud Spanner ■ Cloud Datastore ■ Persistent Disk ■ Data Transfer	■ Virtual Private Cloud (VPC) ■ Cloud Load Balancing ■ Cloud CDN ■ Cloud Interconnect ■ Cloud DNS	■ BigQuery ■ Cloud Dataflow ■ Cloud Dataproc ■ Cloud Datalab ■ Cloud Dataprep ■ Cloud Pub/Sub ■ Genomics ■ Google Data Studio ■ Cloud IoT Core	■ Cloud Machine Learning Engine ■ Cloud Jobs API ■ Cloud Natural Language API ■ Cloud Speech API ■ Cloud Translation API ■ Cloud Vision API ■ Cloud Video Intelligence

Figure 65: Major GCP Services *[68]*

As of now, GCP provides its services in 88 different zones spread across 29 regions. Zone refers to the area where the GCP resources are deployed, and they are grouped into regions, which are separate areas [67] [69].

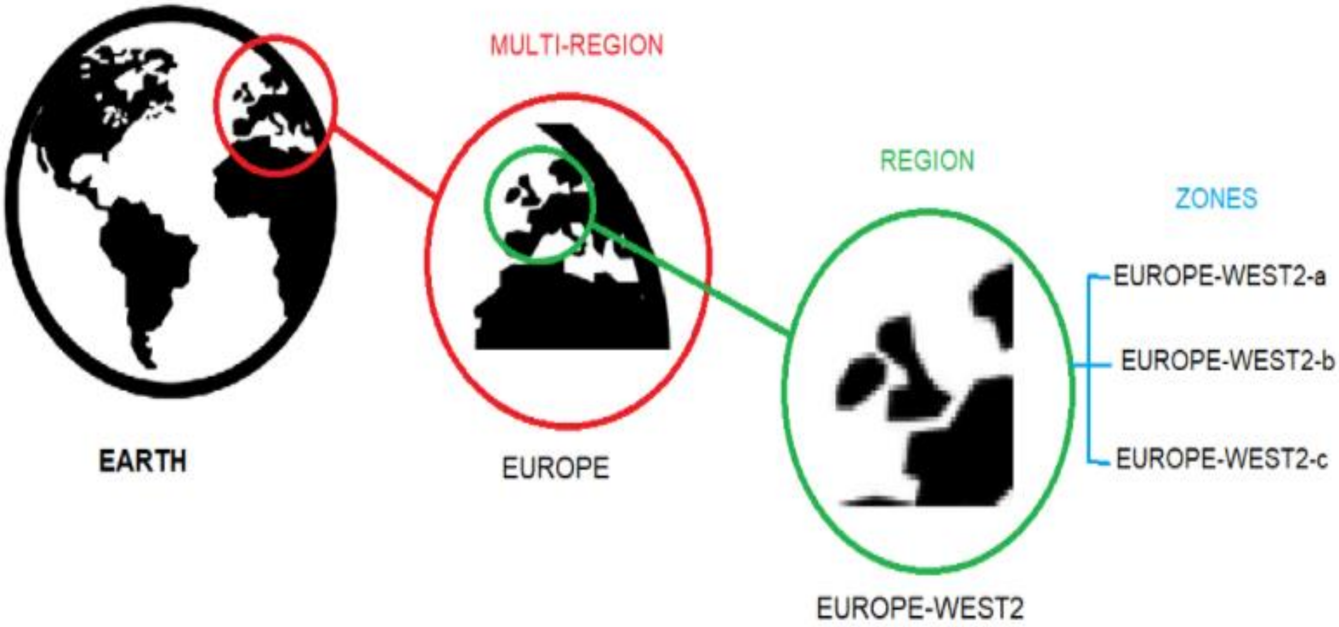


Figure 66: Regions vs Zones *[69]*

3.2.1 GCPs Core Cloud Computing Products

Although there are many elements that make up the Google Cloud Platform, there are four core components. These are:

1. Google Compute Engine: It is the IaaS offering that provides virtual machines to users [68].
2. Google App Engine: It is the PaaS offering that allows the software developers to gain access to scalable hosting, and it basically helps in developing various software products [68].
3. Google Cloud Storage: It is a storage platform that allows storing large amounts of data in cloud servers, which can be accessed from anywhere in the world [70].
4. Google Container Engine: It is the orchestration and management system for the Docker containers running in the public cloud [68].

Apart from the above-mentioned core components, some others are:

- Google BigQuery Service: It is a service with which users can analyze their business efficiently for Big data, and it can also store huge amounts of data [70].
- Google Cloud Dataflow: The cloud data flow helps users in managing the consistent parallel data-processing pipelines [70].
- Google Cloud Job Discovery: This component of GCP helps users in finding jobs and other business options [70].

- Google Cloud Test Lab: This provides various devices (physical and virtual) in the cloud to users where they can test their applications to get some insights about them [70].
- Google Cloud Endpoints: It helps the users in the development and maintenance of a secure application program interface that runs on the GCP [70].
- Google Cloud Machine Learning Engine: It helps users in developing various models and structures to better utilize ML abilities [70].

3.2.2 Benefits of GCP

The various advantages of using the Google Cloud Platform includes:

- Users only need to pay the money when they are using the platform, and some special discounts are also provided when they use their services for a longer period [70].
- The data and information stored in the cloud can be accessed from anywhere in the world [70].
- GCP provides excellent performance to its users. Fast load time and quick web responses provide excellent services, and GCP also integrates well with the hardware configurations to provide a very good cloud experience [70].
- It rolls up updates and security patches very frequently, making the product better with every update [70].
- All the data and other stuff are kept safe by encrypting and securing the servers, cloud platform, and networks using excellent security measures. So, GCP provides outstanding security [70].

3.3 OCI

Oracle Cloud Infrastructure (OCI) was initially released in 2016, and it is a suite of Oracle Cloud. It was initially named ‘Oracle Bare Metal Cloud Services’ and was later named OCI in 2018, and it is also known as Oracle’s Generation 2 Cloud [71].

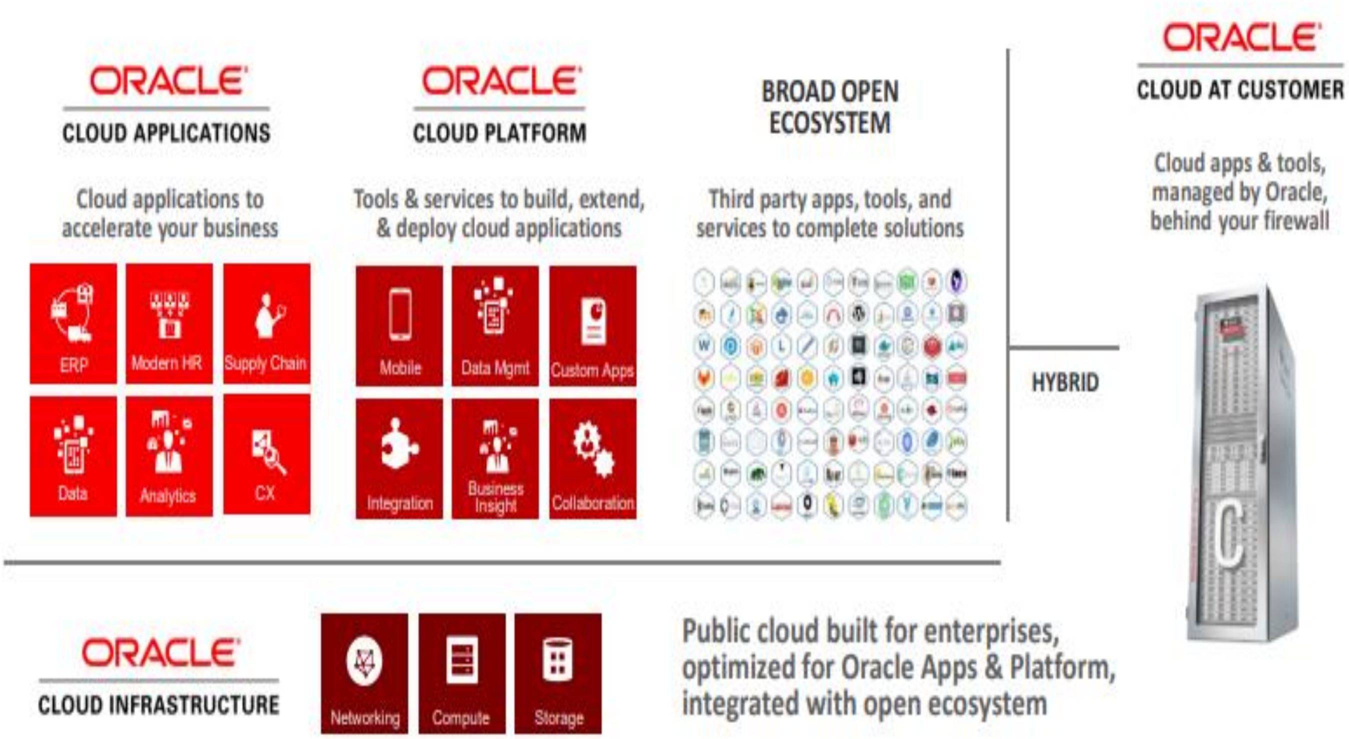

ORACLE
CLOUD APPLICATIONS
Cloud applications to accelerate your business
ERP
Modern HR
Supply Chain
Data
Analytics
CX
ORACLE
CLOUD PLATFORM
Tools & services to build, extend, & deploy cloud applications
Mobile
Data Mgmt
Custom Apps
Integration
Business Insight
Collaboration
BROAD OPEN ECOSYSTEM
Third party apps, tools, and services to complete solutions
HYBRID
ORACLE
CLOUD AT CUSTOMER
Cloud apps & tools, managed by Oracle, behind your firewall
ORACLE
CLOUD INFRASTRUCTURE
Networking
Compute
Storage
Public cloud built for enterprises, optimized for Oracle Apps & Platform, integrated with open ecosystem

Figure 67: OCI Strategy *[72]*

OCI has integrated the public cloud’s benefits with the controls, predictivity, and security provided by the infrastructure present on the site, which delivers excellent performance services. Their strategy is to provide the best experience to customers with an open and broad environment that can provide services in both the cloud and on-premises or a combination of the two [72].

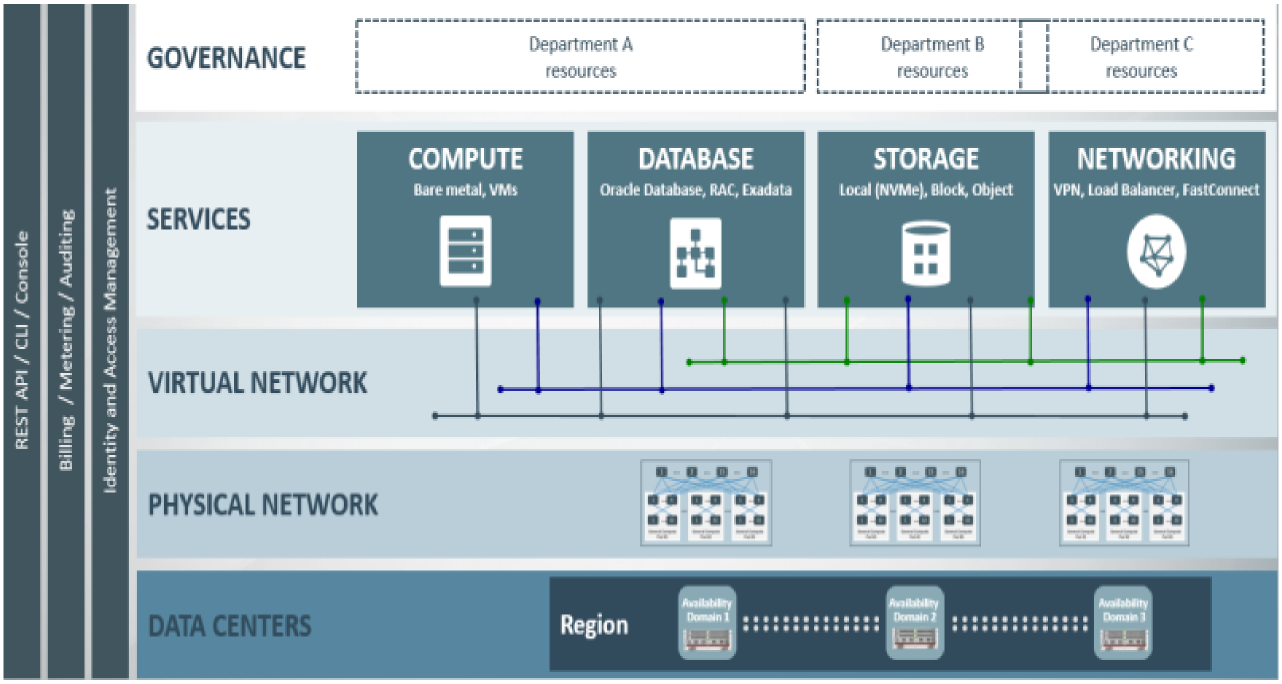


Figure 68: OCI overview *[72]*

OCI is the world's first platform that implemented off-box network virtualization. It takes network and input/output virtualization out of the software stack and then lays it in the network, which results in an elastic, self-serving, pay-as-you-go physical host. Also, with the off-box network virtualization, any bare metal host can run side-by-side with any class of systems, using the same APIs. Normally, the hypervisor (hardware virtualization layer) is relied upon to take care of the network virtualization, but with the off-box network virtualization, the network virtualization runs directly on the hardware as the hypervisor layer gets removed. This results in increased performance by the network. Also, as isolation is provided, security is increased by the fact that in the event of breaching of hypervisor layer, the attack remains contained to that virtual network only; all the other virtual network remains unaffected by that threat [72].

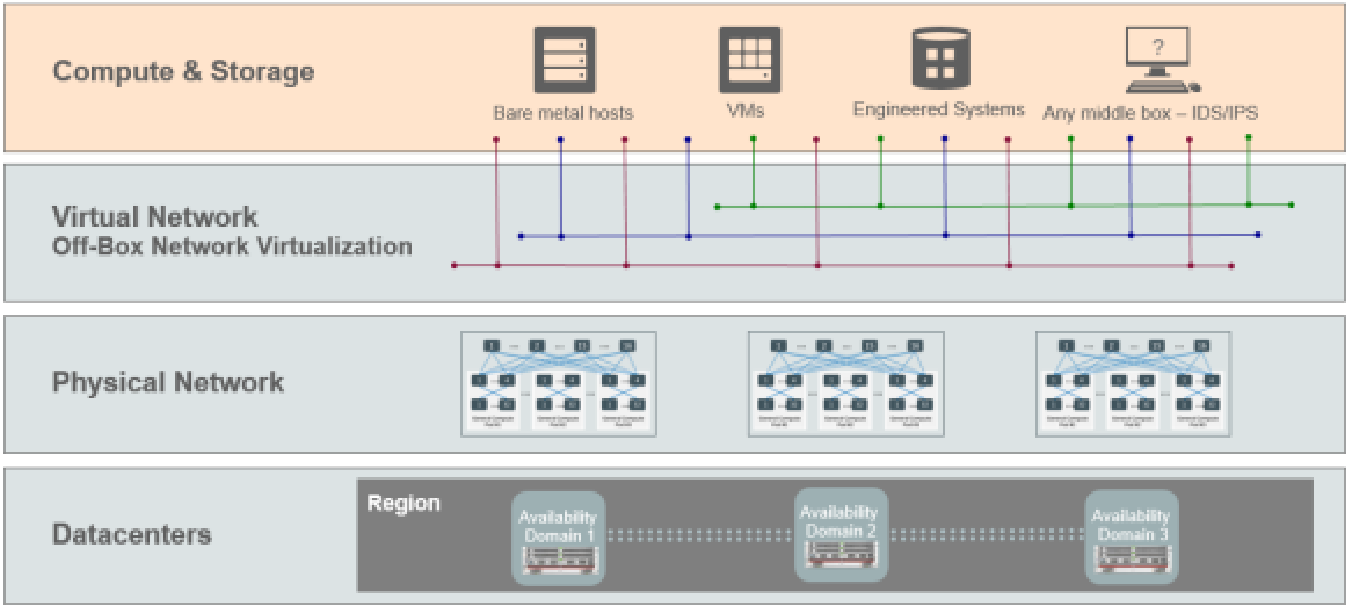


Figure 69: Off-box network virtualization *[72]*

3.3.1 Regions and Availability Domains (AD)

- OCI is hosted in regions, which are located in different metropolitan areas
- Availability Domains (AD) are isolated from each other and are fault tolerant
- Multiple ADs can be used to ensure high availability and protect against resource failure
- Some resources are AD specific, such as an instance and the storage volume attached to it

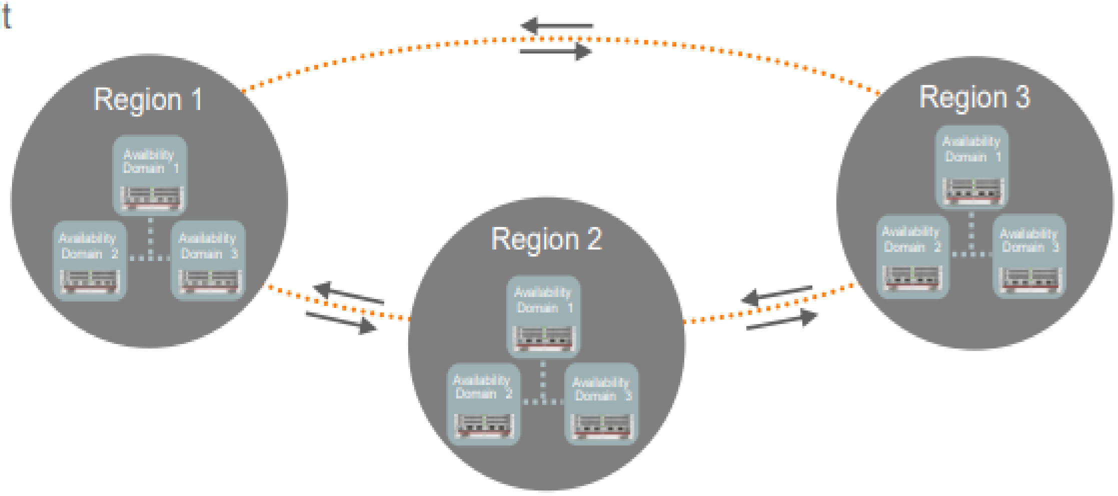


Figure 70: Regions and Availability Domains (AD) *[72]*

As the above image illustrates, different regions are kept independent and separated from each other by large distances. Multiple ADs can be there in one region, which ensures high availability and provides protection from failures, and these ADs are kept isolated from each other [72].

3.3.2 OCI Offerings and Services

Oracle Cloud Infrastructure offers a lot of services, including the following:

- **Storage**: OCI provides huge storage services, including block volumes, archive storage, and object storage, and these services can activate databases, content, and applications with the same APIs and protocols [73].
- **Network**: OCI provides fully connected end-to-end secured networks, which support existing as well as new networks [73].
- **Compute**: OCI offers virtual machine instances to take care of the compute services according to the workload, and we can rent bare metal servers and bare metal GPU servers when needed [73].
- **Database**: It helps in the deployment of Oracle databases in the cloud environment, which can be done using granular controls and data security for real-time applications [73].
- **Load Balancing**: Through load balancing, the traffic gets routed automatically across the Availability Domains (ADs), and it also provides fault tolerance [73].
- **Governance**: Oracle Cloud Infrastructure helps its customers in the process of auditing and in IAM (Identity and Access Management). Users are provided with access management checks, data integrity checks, and traceability by the OCI [73].
- **Ravello**: Ravello assists in the deployment of the user's existing workloads on the Oracle Cloud Infrastructure without making any changes to the network, storage, or the VMs [73].
- **Fast Connect**: With Fast Connect, users can connect to the cloud networks privately [73].

3.3.3 Oracle Cloud Infrastructure benefits

OCI offers many benefits to its customers. These include:

- When an organization has already made an investment in on-premises products, it does not mean that they will face any tough challenges while moving to the cloud. All the mitigation tasks, including virtualization, server setups, storage setups, etc., can be done with or without the help of Oracle's experts [74].
- OCI's bare metal servers have the capabilities to process large data sets in real-time. This produces high-performing and scalable databases and other related products. Also, these servers can take care of multiple terabytes per instance using NVME storage (Non-Volatile Memory Express). These factors result in the excellent performance of applications that are mission-critical [74].

- OCI separates the computing resources from the networking resources. It also provides built-in firewalls, multi-factor authentication, data encryption, and other security measures to provide an infrastructure that is highly secure [74].
- Oracle is always available to assist the organizations that need any kind of help in migrating to the cloud with OCI, with their highly skilled and qualified experts [74].
- When an organization opts for OCI, it does not mean that they are stuck with just one vendor. OCI supports cross-cloud support, meaning it can work with other cloud providers. Both Oracle and non-Oracle workloads can run together as Oracle Cloud Infrastructure supports interoperability. Also, OCI supports open-source technology, and it can be joined with DevOps and IT tools from other vendors and supports both Windows and Linux servers. So, OCI provides a very open architecture [74].

3.4 Azure

Azure or Microsoft Azure is the cloud computing service provided by Microsoft. It came into existence in 2008 and provides all the three main models (SaaS, PaaS, IaaS) of cloud computing. It supports various programming languages, frameworks, and tools of Microsoft as well as third-party products and provides hundreds of services [75].

Azure follows a series of steps to provide its fundamental guidance, right from the architecture to the implementation [76]. The following flow chart shows these steps.

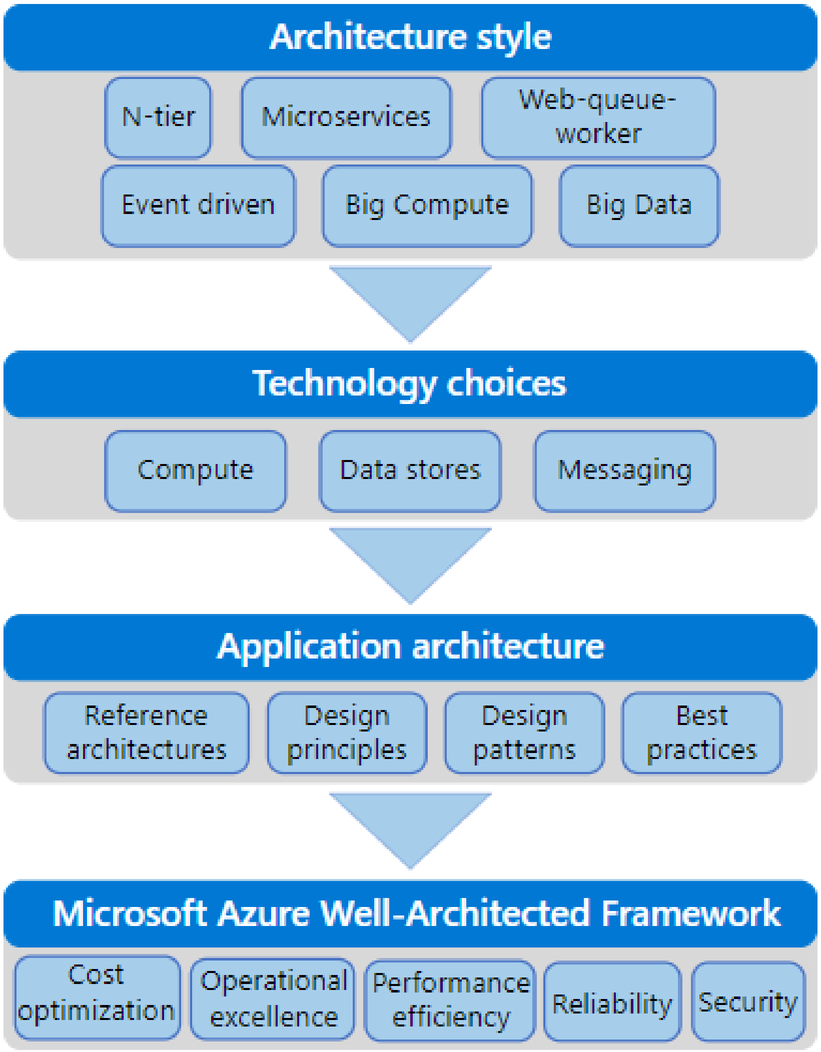


Figure 71: Azure application architecture fundamentals guidance *[76]*

The first step is selecting the kind of architecture from various choices which will be best suited to the requirements. According to the selected style, we can select the core technology pieces (compute, data storage, messaging). More choices will have to be made later, but these three are the most important ones. After that, the design comes next. As different applications will have different requirements, the designs will be different. At last, the five pillars are there (Cost Optimization, Operational Excellence, Performance Efficiency, Reliability, and Security) to complete the cloud application [76]. The following image shows these five pillars to form the Azure Well-Architected Framework.

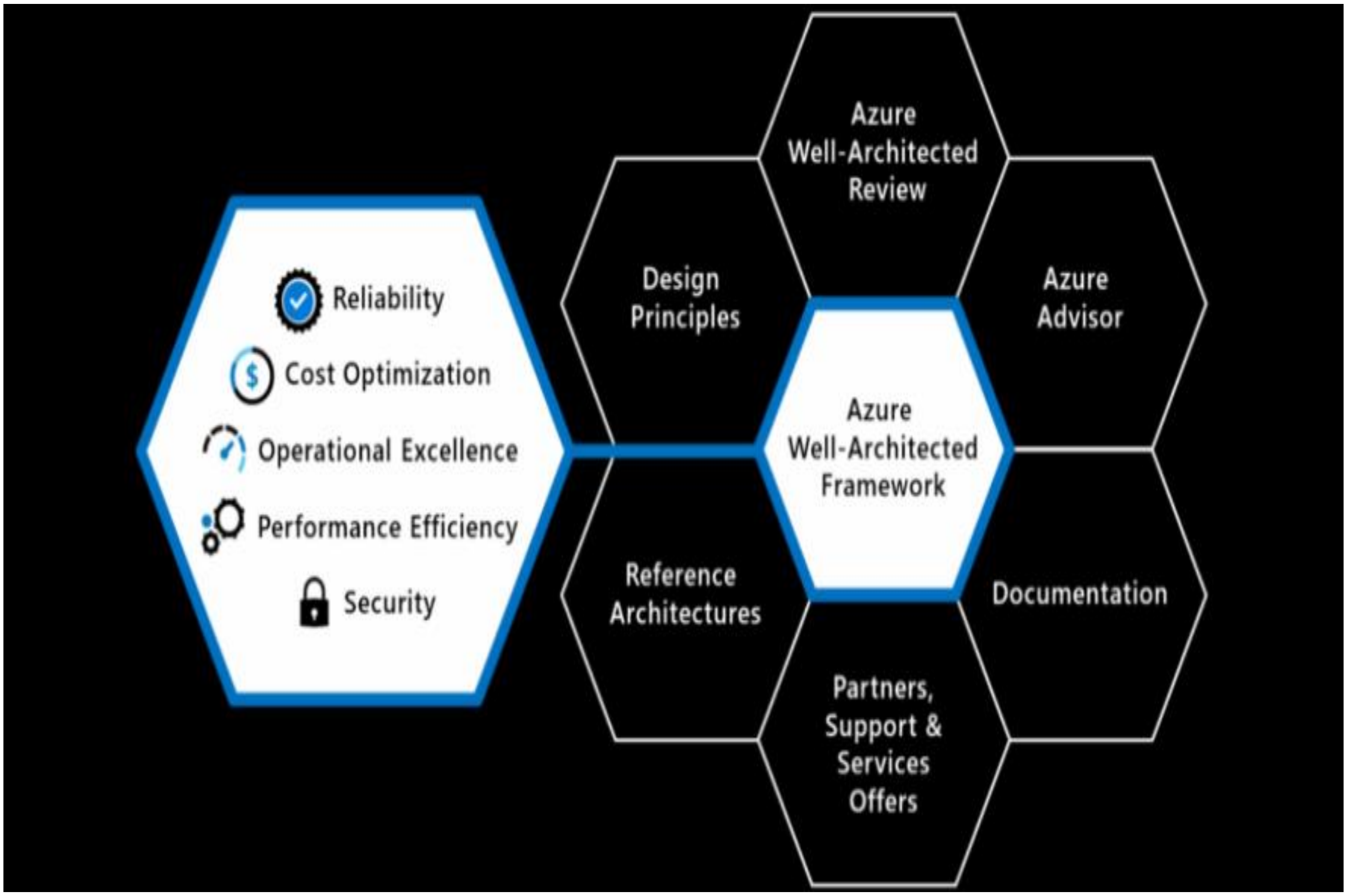


Figure 72: Azure Well-Architected Framework *[77]*

Let us see the functions of these pillars now. **Reliability** makes sure that the system will recover in case of failures and will continue to work. **Cost Optimization** does the cost management to deliver the maximum value. **Operational Excellence** takes care of the various operations and processes to keep the application running in production. **Performance Efficiency** provides the capability to the system in adapting to the changes in load. At last, **Security** provides protection from various threats to the application and data [77].

3.4.1 Microsoft Azure Offerings

MS Azure provides several services in various categories. Some of them are:

- Compute: Compute services helps in the deployment and management of virtual machines and provide remote application access support [78].
- Mobile: Mobile products aids in the development of cloud applications for mobile devices. They also provide notification services, tools for building APIs, support for back-end tasks, and many more [78].

- Web: Web services help to develop web applications and, in their deployment. Other features for search, API management, content delivery, notification, and reporting are also there [78].
- Networking: Networking takes care of virtual networks, connections, gateways, traffic management, diagnostics, load balancing, DNS hosting, and provides protection against DDoS attacks [78].
- Storage: Large amounts of cloud storage are provided for structured as well as unstructured data. Support for big data projects, persistent storage, and archival storage is also provisioned [78].
- Analytics: These services provide features for real-time analytics, big data analytics, data leaks, ML, BI (Business Intelligence), IoT, data streams, and data warehousing [78].
- Media and CDN (Content Delivery Network): These services provide streaming on-demand, digital rights protection, indexing and encoding, and media playback [78].
- Identity: These services provide authorization protection of encryption keys and other information which is sensitive [78].
- Security: It helps in identifying and responding to security threats in the cloud and in managing the encryption keys and sensitive stuff [78].
- Migration: These services provide aid to organizations when they decide to shift from local data centers to the Azure cloud by providing estimated costs and by helping in the migration process [78].
- Management and Governance: These help in the management of Azure deployment by providing certain tools for backup, recovery, compliance, automation, scheduling, and monitoring [78].

3.4.2 Benefits of Azure

There are various benefits of using Azure, including:

- Microsoft focused on the word ‘speed’ in a different way. They focused on how quickly new applications can be deployed, how fast we can scale up, how quickly we can recover from failures, and so on. With various fully automated solutions and many built-in tools, users can save a lot of time as they need not build everything from scratch [79].
- More resources can be accessed, and extra ones can be reduced in the Azure cloud environment with a few clicks. Companies can move between different service level tiers, backup can be done in multiple places around the world, and its applications support all languages and frameworks, making Azure stand out in its flexibility [79].
- Azure provides an end-to-end suite of services in creating an overall infrastructure. Everything from start to finish can take place inside a single environment through the concept of a fully unified delivery pipeline [79].
- With Azure, backing up the data in the cloud is very easy, and you need not own any servers to keep the data safe, and it can be accessed in no time. It also

provides virtual testing, which provides you with the information needed to make changes in your application [79].

- Microsoft spends more than a billion dollars every year to provide better security. It has security control in the hardware as well as the firmware and has cybersecurity experts to assist customers if they need any help. Azure sends frequent notifications to upgrade or enable new security features. Azure's Security Center also monitors the security standing of users and provides them with certain tips to secure their data, and determines if a threat can occur or not [79].

3.5 AWS

Amazon Web Services is a part of Amazon and provides solutions in cloud computing that are both cost-effective and scalable. It provides on-demand platforms for cloud computing and APIs to its customers on a pay-as-you-go basis. In the year 2002, AWS services were launched, and it consisted of web services only. Cloud computing services were launched four years later, in 2006. Today, AWS offers hundreds of services and products to its users; some of them are offered directly, while many are provided through APIs to be used in the applications. According to Synergy Group, in 2017, AWS owned one-third of all the cloud [80] [81].

All kinds of enterprises and organizations are using AWS in developing, deploying, and hosting applications. These include startups, government, established companies, and many more. The number crosses 1,000,000, and some of the big ones are Netflix, Coinbase, Adobe, Airbnb, Johnson & Johnson, Hitachi [81].

Just like Azure has its own Well-Architected Framework, so does AWS. But in the case of AWS, there are six pillars, one extra than the one in Azure. This framework includes domain-specific lenses, various labs, and the AWS Well-Architected Tool, and it describes certain key concepts, design principles, and best architectural practices to design and run workloads in the cloud [82]. The six pillars in the framework are:

- Operational Excellence: Focuses on running and monitoring systems, as well as on the continuous improvement of processes and procedures by providing automated changes, responding to events, and defining certain standards [82].
- Security: It provides protection to information and the systems, and it includes data confidentiality, data integrity, managing user permissions, and establishing controls to look for security events [82].
- Reliability: It includes distributed system design, recovery planning, and adapting to the changes to focus on correct performance by the workloads and quick recovery from failures [82].
- Performance Efficiency: It provides structured and streamlined allocation of resources. It includes selecting the right type and size of resources, performance monitoring, maintaining efficiency, and many more [82].
- Cost Optimization: Its objective is to reduce the overall cost by understanding timely spending, funds control, selecting the right type and quantity of resources, and scaling without overspending [82].
- Sustainability: This pillar's focus is on minimizing the impacts of cloud workloads on the environment. Responsibility model, understanding impact, maximizing utilization to minimize resources are some of its elements [82].

AWS Well-Architected Framework has AWS Well-Architected Lenses and a tool called AWS Well-Architected Tool. The lenses extend the guidance to a specific domain, like Machine Learning, data analysis, IoT, hybrid networking, etc., and multiple lenses can be used together. The AWS Well-Architected Tool helps to review the state of applications and workloads [82] [83].

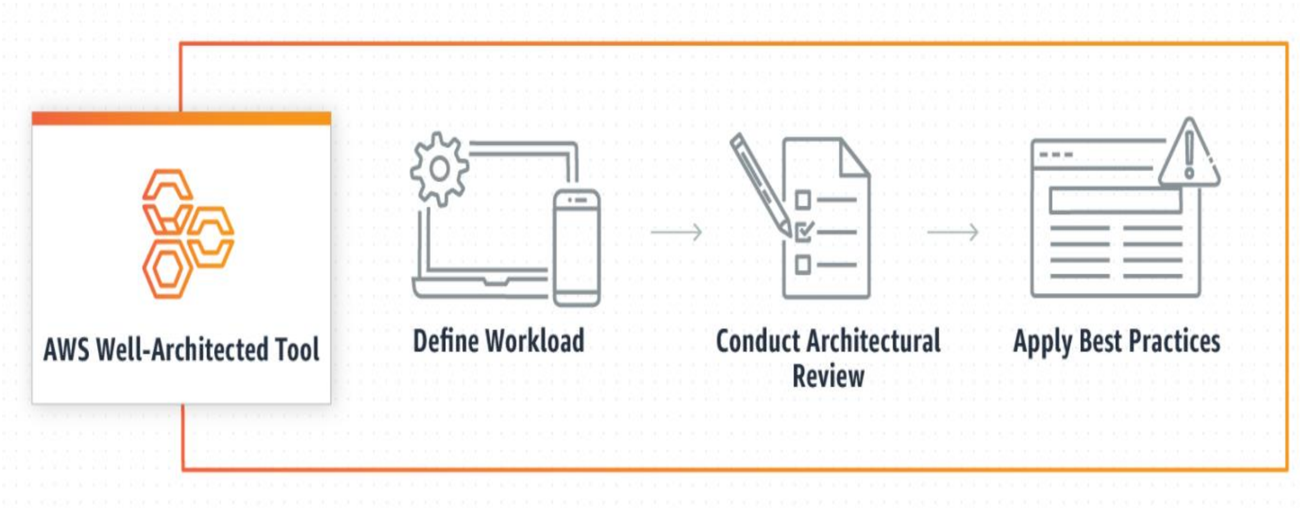


Figure 73: Working of AWS Well-Architected Tool *[83]*

The AWS Well-Architected Tool provides free architectural guidance by providing access to knowledge and practices which are used by the AWS solutions architects. It allows us to monitor the status of various workloads, helps in deciding the next steps for improvement, and helps in their implementation. New reviews are initiated when needed, which makes sure continuous improvement is there in the architecture. At last, it also helps in the customization of our reviews by helping us create custom lenses to measure the workloads of the entire organization [83].

3.5.1 Services by AWS

The key services of AWS include:

- Compute: These help in the building, deploying, and scaling of applications in the cloud. AWS Elastic Compute Cloud (EC2) and AWS Lambda are two examples. AWS EC2 enables developers to rent virtual machines when needed, and AWS Lambda is a serverless service that helps in program execution without managing servers [81].
- Storage: It is the data storage service of AWS. Example Amazon Simple Storage Service (Amazon S3) and Amazon Elastic Block Store (Amazon EBS). Amazon S3 is used for online data backup and provides storage via web service interfaces. Amazon EBS is the storage used mainly by the EC2 instances for primary storage [81].
- Database: This service provides cheap, secure, and scalable databases in the cloud. DynamoDB is a database service that provides a multi-region and durable database with built-in security, backup, and restore features. RDS (Relational Database Service) is another example. It helps developers in operating and scaling a database in a very simplified manner [81].
- Networking and content delivery: It provides a secure cloud platform and connection of physical networks to private virtual networks. Virtual Private Cloud (VPC) helps in deploying AWS resources into the cloud. Route 53 is another

example that provides help to route software by translation of the text into IP addresses [81].

- Security tools: This service makes sure the environment is not compromised by providing only required access to authorized people. It contains tools like IAM (Identity Access Management) which maintains secure access to AWS services, and KMS (Key Management Service), which lets users in the creation and management of encryption keys [81].
- Developer tools: It includes tools like CodeStar and Code Build and helps users in automatically building, deploying, and running an application source code. CodeStar provides a single space where developers can develop, build, and deploy applications, and Code Build compiles the code, does the execution, and provides ready-to-deploy artifacts [81].
- Management tools: It provides tools that help in cost optimization, minimizing risks, and automation of resources to increase the overall efficiency, like Cloud Watch and Cloud Formation. Cloud Watch is a monitoring tool that provides access to the operational data (in the form of logs), and Cloud Formation lets users monitor all the AWS resources in one place and lets the developers manage the infrastructure either in a text file or as a template [81].

3.5.2 Benefits of AWS

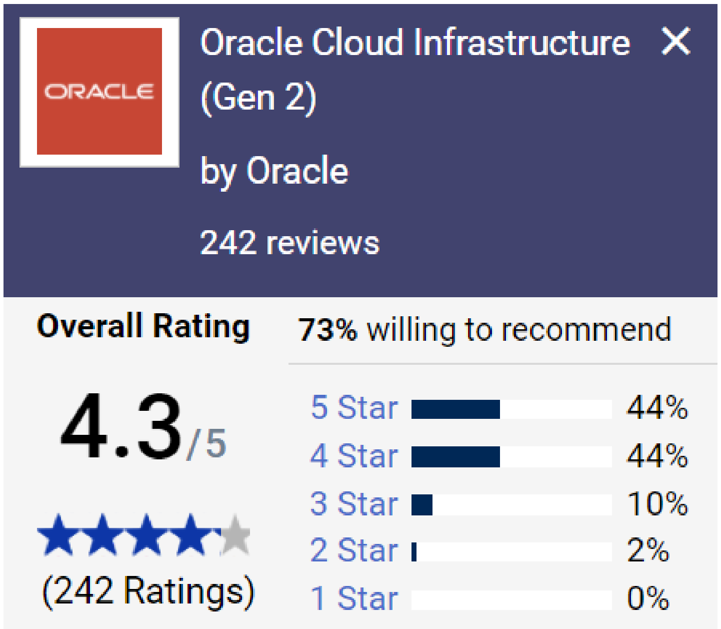
Certain benefits of using AWS include:

- Easy to use: AWS has its own Management Console and well-documented web services APIs, which allows companies to host the applications in a very quick and secure manner [84].
- Flexibility: There is support for all operating systems, programming languages, web application platforms, and other services. This leads to overall flexibility and helps in the migration process [84].
- Low cost: Payment needs to be done only when we use the resources. There is no need to sign any long-term contracts or make any commitments [84].
- Reliability: Over the years, Amazon has set up and maintained a global infrastructure for AWS that is highly reliable, scalable, and secure [84].
- Scalability and Performance: Scaling up or down is very easy using the tools provided by AWS, auto-scaling, and ELB (Elastic Load Balancing). Amazon’s infrastructure also provides resources on-demand to make sure that optimum performance is maintained [84].
- Security: AWS has an end-to-end approach that is made highly secure by various physical, operational, and software protective measures [84].

3.6 Comparisons

Let us now make the comparison between GCP, OCI, Microsoft Azure, and AWS. The comparison will be based on the reviews provided by Gartner, which gives overall ratings out of 5. These reviews are the verified ones, and based on these reviews, Google Cloud Platform scored 4.5, Oracle Cloud Infrastructure scored 4.3, Microsoft Azure scored 4.4, and Amazon Web Services scored 4.5. Although the ratings of GCP and AWS might be the same, if we break it further down, it is seen that AWS performed better. It shows that AWS performed a bit better than GCP, by the number of 5 starts given and the number of reviews [85]. Let us have a look at them one by one.

The one with the lowest rating out of the four is Oracle Cloud Infrastructure, with a score of 4.3 out of 5. It provides easy migration and monitoring services, provides high performance, is reliable, and is easy to configure. However, it lacks proper documentation and integration with third parties. Also, it is not very user-friendly, not much flexible, and the support staff is not as good as it should be [86].



Oracle Cloud Infrastructure ✕
(Gen 2)

by Oracle

242 reviews

Overall Rating

4.3/5

★★★★☆

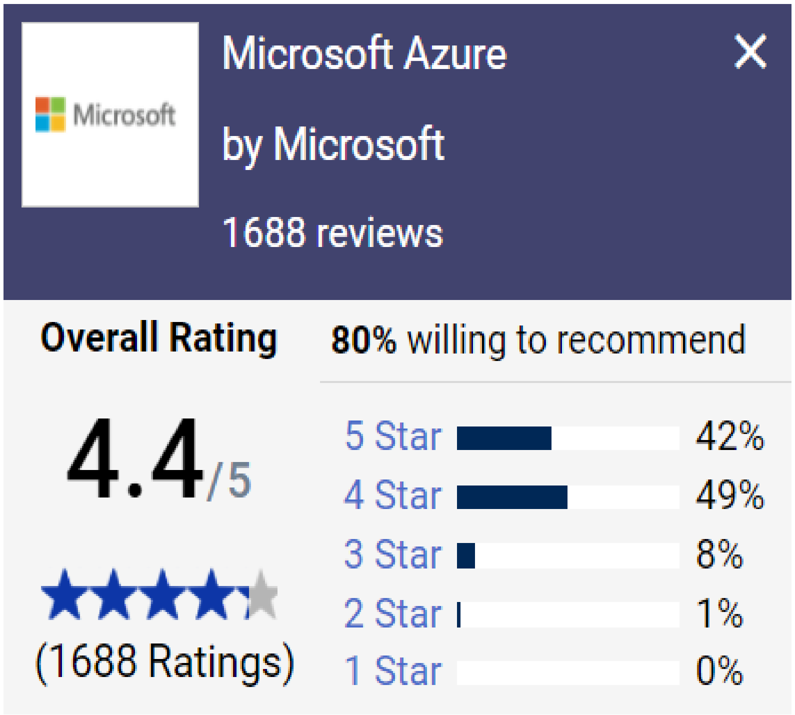
(242 Ratings)

73% willing to recommend

5 Star	44%
4 Star	44%
3 Star	10%
2 Star	2%
1 Star	0%

Figure 74: OCI ratings *[85]*

The next one is Microsoft Azure. It provides fast, secure, scalable, and reliable services, which is its strongest point. It is also user-friendly, and the features of application testing, deploying, and managing are excellent. But it becomes somewhat slow when integrated with products that are non-Microsoft. The billing process also seems a bit confusing, as the pricing is not very transparent. All these factors combined give Azure a rating of 4.4 [87].



Microsoft Azure

by Microsoft

1688 reviews

Overall Rating

4.4/5

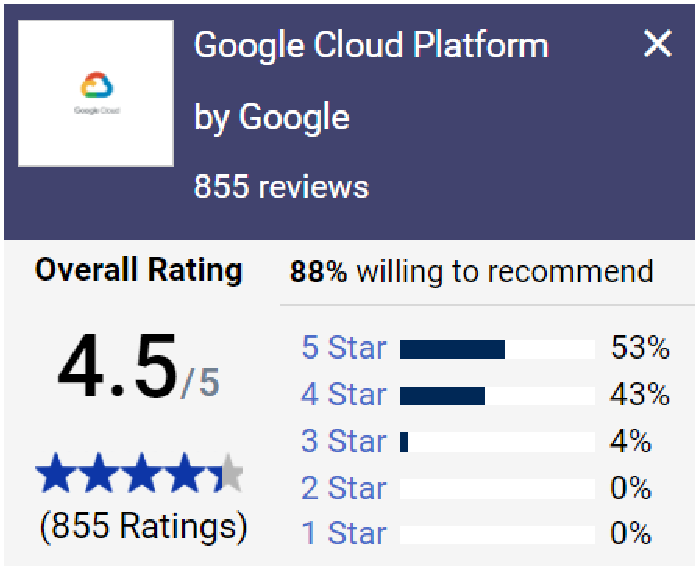
(1688 Ratings)

80% willing to recommend

5 Star	42%
4 Star	49%
3 Star	8%
2 Star	1%
1 Star	0%

Figure 75: MS Azure ratings *[85]*

Next comes the Google Cloud Platform. It is fast and provides regular updates. It follows a project-based approach, which is quite helpful as the resources are grouped together in a project. It also provides a free version, which is generally enough for small usage for individuals. However, the paid services are generally more expensive than AWS. Sometimes, some issues arise when integrating with other non-Google products, and documentation can be better. Overall, it scores 4.5 [88].



Google Cloud Platform

by Google

855 reviews

Overall Rating

4.5/5

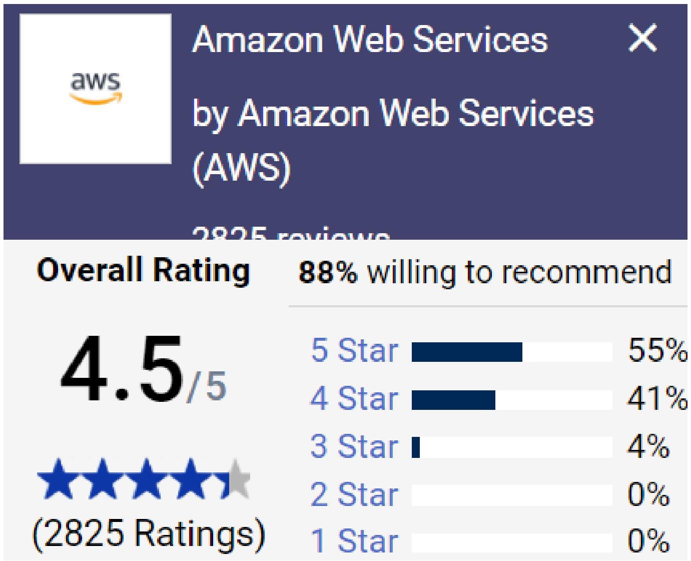
(855 Ratings)

88% willing to recommend

5 Star	53%
4 Star	43%
3 Star	4%
2 Star	0%
1 Star	0%

Figure 76: GCP ratings *[85]*

AWS comes out on top as the leading vendor in the cloud. It is the most popular, secure, and robust public cloud platform. Everything is well documented, and the pay-as-you-go feature generally proves to be cost-efficient. It is highly scalable, reliable, and easy to use. But it can be a bit complex for new users, and the pay-as-you-go feature can sometimes become a little bit expensive [89].



Amazon Web Services

by Amazon Web Services (AWS)

2825 reviews

Overall Rating

4.5/5

(2825 Ratings)

88% willing to recommend

5 Star	55%
4 Star	41%
3 Star	4%
2 Star	0%
1 Star	0%

Figure 77: AWS ratings *[85]*

References

[1] J. Fruehe, "Traditional WAN vs. SD-WAN: How do they compare?," TechTarget, [Online]. Available: https://www.techtarget.com/searchnetworking/answer/Traditional-WAN-vs-SD-WAN-How-do-they-compare.

[2] Z. Yang, Y. Cui, B. Li, Y. Liu and Y. Xu, *Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities,* Valencia, Spain: IEEE, 2019.

[3] Cisco, [Online]. Available: https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html#~what-it-is.

[4] Apcela, [Online]. Available: https://www.apcela.com/blog/the-evolution-of-wan/.

[5] AVI Networks, [Online]. Available: https://avinetworks.com/glossary/packet-switching/.

[6] Steve, "The TCP/IP Model and Protocol Suite Explained for Beginners," 29 November 2019. [Online]. Available: http://www.steves-internet-guide.com/internet-protocol-suite-explained/.

[7] M. Ellis, "How Does a Router Work? A Simple Explanation," MakeUseOf (MUO), 20 October 2021. [Online]. Available: https://www.makeuseof.com/tag/technology-explained-how-does-a-router-work/.

[8] N. Cranford, "Overlay networks explained," RCR Wireless, 18 April 2018. [Online]. Available: https://www.rcrwireless.com/20180418/fundamentals/overlay-networks-explained.

[9] Huawei, [Online]. Available: https://support.huawei.com/enterprise/fr/doc/EDOC1100023542?section=j015&topicName=overview.

[10] S. Sam, "Packet over SONET," Tutorials Point, 29 March 2019. [Online]. Available: https://www.tutorialspoint.com/packet-over-sonet.

[11] A. K. Sahni, "Multi Protocol Label Switching (MPLS)," Geeks for Geeks, [Online]. Available: https://www.geeksforgeeks.org/multi-protocol-label-switching-mpls/.

[12] N. Agarwal, "Asynchronous Transfer Mode (ATM) in Computer Network," Geeks for Geeks, [Online]. Available: https://www.geeksforgeeks.org/asynchronous-transfer-mode-atm-in-computer-network/.

[13] K. Chavan, "Asynchronous Transfer Mode (ATM)," Tutorials Point, 13 March 2019. [Online]. Available: https://www.tutorialspoint.com/asynchronous-transfer-mode-atm.

[14] A. Saxena, "How does Frame Relay Work?," Geeks for Geeks, [Online]. Available: https://www.geeksforgeeks.org/how-does-frame-relay-work/.

[15] VMware, [Online]. Available: https://www.vmware.com/topics/glossary/content/software-defined-networking.html.

[16] S. Chakrabarty, "THE 4 PRINCIPLES OF SOFTWARE-DEFINED NETWORKING," Govloop, 21 March 2016. [Online]. Available: https://www.govloop.com/4-principles-of-software-defined-networking/.

[17] K. Kirkpatrick, *Software-defined networking*, 2013.

[18] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, *Software-Defined Networking: A Comprehensive Survey*, IEEE, 2015.

[19] "What is NFV?," Red Hat, 16 August 2019. [Online]. Available: https://www.redhat.com/en/topics/virtualization/what-is-nfv.

[20] "What is a virtual machine (VM)?," Microsoft, [Online]. Available: https://azure.microsoft.com/en-ca/overview/what-is-a-virtual-machine/#overview.

[21] "What is Network Function Virtualization (NFV)," Blue Planet, 13 July 2016. [Online]. Available: https://www.blueplanet.com/resources/What-is-NFV-prx.html.

[22] A. Leonhardt, "Defining The Elements of NFV Architectures," Equinix, 17 October 2019. [Online]. Available: https://blog.equinix.com/blog/2019/10/17/networking-for-nerds-defining-the-elements-of-nfv-architectures/.

[23] F. Khan, "A Cheat Sheet for Understanding “NFV Architecture”," Telco Cloud Bridge, [Online]. Available: https://telcocloudbridge.com/blog/a-cheat-sheet-for-understanding-nfv-architecture/.

[24] "vCPE, Virtualizing the CPE," Lanner, [Online]. Available: https://www.lanner-america.com/blog/vcpe-virtualizing-cpe/.

[25] A. Irei and J. English, "SD-WAN (software-defined WAN)," TechTarget, [Online]. Available: https://www.techtarget.com/searchnetworking/definition/SD-WAN-software-defined-WAN.

[26] S. Gittlen, "SD-WAN explained: Ultimate guide to SD-WAN architecture," TechTarget, 26 April 2021. [Online]. Available: https://www.techtarget.com/searchnetworking/SD-WAN-explained-The-ultimate-guide-to-SD-WAN-architecture.

[27] M. Lessing, "SD-WAN Defined: What is SD-WAN (Software-Defined Wide Area Network)?," SDxCentral, 10 February 2021. [Online]. Available: https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/.

[28] S. Jena, "Difference between Traditional WAN and SD WAN," Geeks for Geeks, [Online]. Available: https://www.geeksforgeeks.org/difference-between-traditional-wan-and-sd-wan/.

[29] R. Sturt, "5 common SD-WAN challenges and how to prepare for them," TechTarget, April 2021. [Online]. Available: https://www.techtarget.com/searchnetworking/tip/5-common-SD-WAN-challenges-and-how-to-prepare-for-them.

[30] Crunchbase, [Online]. Available: https://www.crunchbase.com/organization/cato-networks.

[31] SD-WAN experts, [Online]. Available: https://www.sd-wan-experts.com/cato-networks/.

[32] "Cato Edge SD-WAN," Cato Networks, [Online]. Available: https://www.catonetworks.com/cato-sase-cloud/cato-edge-sd-wan/.

[33] "SD-WAN as a Service," Cato Networks, [Online]. Available: https://www.catonetworks.com/sd-wan/sd-wan-as-a-service/.

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

[35] Aryaka, [Online]. Available: https://www.aryaka.com/about-us/#about.

[36] SD-WAN experts, [Online]. Available: https://www.sd-wan-experts.com/aryaka/.

[37] C. Craven, "What is the Aryaka Networks Managed SD-WAN Approach?," SDxCentral, 12 February 2020. [Online]. Available: https://www.sdxcentral.com/networking/sd-wan/definitions/aryaka-managed-sd-wan/.

[38] S. Kiran, "Aryaka's SD-WAN and SASE solutions – What's new and why should you care?," Aryaka, 7 December 2021. [Online]. Available: https://www.aryaka.com/blog/aryakas-sd-wan-and-sase-solutions-whats-new-and-why-should-you-care/.

[39] Aryaka, [Online]. Available: https://www.aryaka.com/managed-wan-services/.

[40] Cisco, [Online]. Available: https://www.cisco.com/c/en_au/about/who-is-head.html.

[41] "What is the Cisco SD-WAN Approach?," SDxCentral, 25 August 2017. [Online]. Available: https://www.sdxcentral.com/networking/sd-wan/definitions/cisco-sd-wan/.

[42] A. Rohyans, A. Shaikh, C. B. Rajaram, D. Klebanov, D. Kumar, G. Cornett, H. Malik, K. Ghodgaonkar, M. Arunachalam, N. Pitaev, T. Carlson and Z. Aziz, "Cisco SD-WAN Cloud scale architecture," Cisco, [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.

[43] Juniper Networks, [Online]. Available: https://www.juniper.net/us/en/company/profile.html.

[44] "Managed AI-driven SD-WAN," Juniper Networks, [Online]. Available: https://www.juniper.net/us/en/solutions/sd-wan/managed-sd-wan.html.

[45] T. Mann, "Juniper Takes On Cisco, Aruba With Fully Mist-ified SD-WAN," SDxCentral, 18 January 2022. [Online]. Available: https://www.sdxcentral.com/articles/news/juniper-takes-on-cisco-aruba-with-fully-mist-ified-sd-wan/2022/01/.

[46] Juniper Networks, [Online]. Available: https://www.juniper.net/us/en/dm/sd-wan-hero.html.

[47] "Juniper Session Smart Router," Juniper Networks, [Online]. Available: https://www.juniper.net/us/en/products/routers/session-smart-router.html.

[48] "Marvis Virtual Network Assistant," Juniper Networks, [Online]. Available: https://www.juniper.net/us/en/products/cloud-services/virtual-network-assistant.html.

[49] "Juniper Mist WAN Assurance," Juniper Networks, [Online]. Available: https://www.juniper.net/us/en/products/cloud-services/wan-assurance.html.

[50] "Juniper SD-WAN," Network Screen, [Online]. Available: https://www.networkscreen.com/SD-WAN.asp.

[51] "Silver Peak Systems," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Silver_Peak_Systems.

[52] "Making the shift to a business-first networking model," Aruba Networks, [Online]. Available: https://www.arubanetworks.com/assets/so/SO_Business-First-Networking-Model.pdf.

[53] "ARUBA EDGECONNECT SD-WAN EDGE PLATFORM," Aruba Networks, [Online]. Available: https://www.arubanetworks.com/assets/ds/DS_Spec-Sheet_EdgeConnect-Solution-Enterprise.pdf.

[54] "Aruba Orchestrator," Aruba networks, [Online]. Available: https://www.arubanetworks.com/products/sd-wan/edgeconnect/orchestrator/.

[55] "Aruba Boost Unified WAN Optimization on-demand," Aruba Networks, [Online]. Available: https://www.arubanetworks.com/products/sd-wan/edgeconnect/boost/.

[56] "Aruba EdgeConnect SD-WAN Edge Platform vs Aryaka SmartCONNECT vs Cato SASE Cloud vs Cisco SD-WAN powered by Viptela vs Juniper Session Smart Router," Gartner, [Online]. Available: https://www.gartner.com/reviews/market/wan-edge-infrastructure/compare/product/aruba-edgeconnect-sd-wan-edge-platform-vs-aryaka-smartconnect-vs-cato-sase-cloud-vs-cisco-sd-wanpowered-by-viptela-vs-juniper-session-smart-router.

[57] "Cato SASE Cloud Reviews," Gartner, [Online]. Available: https://www.gartner.com/reviews/market/wan-edge-infrastructure/vendor/cato-networks/product/cato-sase-cloud/likes-dislikes.

[58] "Aryaka SmartCONNECT Reviews," Gartner, [Online]. Available: https://www.gartner.com/reviews/market/wan-edge-infrastructure/vendor/aryaka/product/aryaka-smartconnect/likes-dislikes.

[59] "Cisco SD-WAN powered by Viptela Reviews," Gartner, [Online]. Available: https://www.gartner.com/reviews/market/wan-edge-infrastructure/vendor/cisco/product/cisco-sd-wanpowered-by-viptela/likes-dislikes.

[60] "Aruba EdgeConnect SD-WAN Edge Platform Reviews," Gartner, [Online]. Available: https://www.gartner.com/reviews/market/wan-edge-infrastructure/vendor/aruba/product/aruba-edgeconnect-sd-wan-edge-platform/likes-dislikes.

[61] "Juniper Session Smart Router Reviews," Gartner, [Online]. Available: https://www.gartner.com/reviews/market/wan-edge-infrastructure/vendor/juniper-networks/product/juniper-session-smart-router/likes-dislikes.

[62] "What is the cloud? | Cloud definition," Cloudfare, [Online]. Available: https://www.cloudflare.com/en-ca/learning/cloud/what-is-the-cloud/.

[63] S. Petryschuk, "What is Cloud Networking?," Auvik, 12 February 2021. [Online]. Available: https://www.auvik.com/franklyit/blog/cloud-networking/.

[64] "What is cloud networking?," Citrix, [Online]. Available: https://www.citrix.com/solutions/app-delivery-and-security/what-is-cloud-networking.html.

[65] J. Metzler, "HOW ADVANCED ANALYTICS DIFFERENTIATES CSP SD-WAN SOLUTIONS," Kentik, [Online]. Available: https://assets.ctfassets.net/6yom6slo28h2/5jv7bImhLOcOe6gM4Q6UKQ/3294d034cece65b385150fa7704ef746/kentik-sd-wan-whitepaper.pdf.

[66] "What is NaaS (network-as-a-service)?," Cloudfare, [Online]. Available: https://www.cloudflare.com/en-ca/learning/network-layer/network-as-a-service-naas/.

[67] "Google Cloud Platform," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Google_Cloud_Platform.

[68] S. J. Bigelow, "Google Cloud Platform (GCP)," TechTarget, [Online]. Available: https://www.techtarget.com/searchcloudcomputing/definition/Google-Cloud-Platform.

[69] S. Kevadiya, "What is Google Cloud Platform (GCP)?," Geeks for Geeks, [Online]. Available: https://www.geeksforgeeks.org/what-is-google-cloud-platform-gcp/.

[70] G. Saran, "Introduction To Google Cloud Platform," Whizlabs, [Online]. Available: https://www.whizlabs.com/blog/google-cloud-platform/.

[71] "Oracle Cloud," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Oracle_Cloud.

[72] A. Nagaraj and J. Garcia, "Oracle Cloud Infrastructure Fundamentals," Oracle, September 2017. [Online]. Available: https://www.oracle.com/webfolder/technetwork/tutorials/ocis/ocis_fundamental/OC-Infra-Funda_sg.pdf.

[73] A. Mathur, "Introduction to Oracle Cloud," Geeks for Geeks, [Online]. Available: https://www.geeksforgeeks.org/introduction-to-oracle-cloud/.

[74] A. Hunter, "Oracle Cloud Infrastructure and its Key Benefits," Parallels, 10 August 2020. [Online]. Available: https://www.parallels.com/blogs/ras/oracle-cloud-infrastructure/.

[75] "Microsoft Azure," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Microsoft_Azure.

[76] "Azure application architecture fundamentals," Microsoft, 11 February 2022. [Online]. Available: https://docs.microsoft.com/en-us/azure/architecture/guide/.

[77] "Microsoft Azure Well-Architected Framework," Microsoft, 3 January 2022. [Online]. Available: https://docs.microsoft.com/en-us/azure/architecture/framework/.

[78] S. J. Bigelow, "Microsoft Azure," TechTarget, [Online]. Available: https://www.techtarget.com/searchcloudcomputing/definition/Windows-Azure.

[79] L. Kner, "Top 5 Benefits of Microsoft Azure," HP, 2 April 2020. [Online]. Available: https://www.hp.com/us-en/shop/tech-takes/top-5-benefits-microsoft-azure.

[80] "Amazon Web Services," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Amazon_Web_Services.

[81] "What Is AWS(Amazon Web Services): Services, Applications, Advantages and More," Simplilearn, [Online]. Available: https://www.simplilearn.com/tutorials/aws-tutorial/what-is-aws#storage.

[82] "AWS Well-Architected," Amazon, [Online]. Available: https://aws.amazon.com/architecture/well-architected/?wa-lens-whitepapers.sort-by=item.additionalFields.sortDate&wa-lens-whitepapers.sort-order=desc.

[83] "AWS Well-Architected Tool," Amazon, [Online]. Available: https://aws.amazon.com/well-architected-tool/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc.

[84] "Benefits at a Glance," Amazon, [Online]. Available: https://aws.amazon.com/application-hosting/benefits/.

[85] "Amazon Web Services vs Microsoft Azure vs Google Cloud Platform vs Oracle Cloud Infrastructure (Gen 2)," Gartner, [Online]. Available: https://www.gartner.com/reviews/market/public-cloud-iaas/compare/product/amazon-web-services-vs-azure-vs-google-cloud-platform-vs-oracle-cloud-infrastructure-gen-2.

[86] "Oracle Cloud Infrastructure (Gen 2) Reviews," Gartner, [Online]. Available: https://www.gartner.com/reviews/market/public-cloud-iaas/vendor/oracle/product/oracle-cloud-infrastructure-gen-2/likes-dislikes.

[87] "Microsoft Azure Reviews," Gartner, [Online]. Available: https://www.gartner.com/reviews/market/public-cloud-iaas/vendor/microsoft/product/azure/likes-dislikes.

[88] "Google Cloud Platform Reviews," Gartner, [Online]. Available: https://www.gartner.com/reviews/market/public-cloud-iaas/vendor/google/product/google-cloud-platform/likes-dislikes?marketSeoName=public-cloud-iaas&vendorSeoName=google&productSeoName=google-cloud-platform.

[89] "Amazon Web Services Reviews," Gartner, [Online]. Available: https://www.gartner.com/reviews/market/public-cloud-iaas/vendor/amazon-web-services/product/amazon-web-services/likes-dislikes.