

Functional segments and software defined trends in enterprise networks

Pratiba Deenadhayalan, Ramakanth Kumar Pattar, Vijay Chiranjith Reddy

Department of Computer Science and Engineering, R. V. College of Engineering, Bengaluru, India

Article Info

Article history:

Received Jul 12, 2022

Revised Apr 6, 2023

Accepted Apr 16, 2023

Keywords:

Cloud computing
Enterprise networks
Security
Software defined
Virtualization
Wide area network

ABSTRACT

In the current scenarios most of the business growth comes from the user experience, while using the business applications. Any enterprise network performance depends on the fundamental process of securely serving the user with applications. The network usage patterns have completely changed from just data transfer, voice, and video transmissions to serving entire applications over the networks. With all the modern applications served over the private and public clouds the network resources utilization must be optimized and take full advantage of them which is not possible with current network architectures. The enterprises are currently shifting towards software defined implementation due to many reasons like consistent policy application across the network, run time analytics for troubleshooting the problems and making the network cloud computing ready. Software defined approaches provide centralized security monitoring and control, user data and identity-based segmentation over the network, dynamic recovery from network infrastructure failure and finally virtualization of almost everything. This paper is an overview of the functioning of enterprises in the networking perspective along with current software defined approaches being used in enterprise networking which will soon take over the traditional networks by solving the challenges present in the software defined networking.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Vijay Chiranjith Reddy

Department of Computer Science Engineering, R. V. College of Engineering

Bengaluru, India

Email: rvchiranjith13@gmail.com

1. INTRODUCTION

Enterprise network is the IT infrastructure which serves the communication through physical and virtual networks using the protocols, local area network (LAN), wide area network (WAN), data centers used in the corporate organizations for giving the users access to the network devices and thereby use the applications present in data centers. Distributed applications have become increasingly popular and necessary in the modern world. Enterprise networking solutions provide fast and reliable connectivity among the users and applications along with the security being a crucial factor by controlled access to the company's resources. Enterprise networks are essentially built for serving the business purposes and also give the users access to the application services. The Figure 1 shows the architecture of the enterprise network which consists of areas like LAN, WAN, data centers which connect the users with the applications for business. The process of understanding enterprise network architecture should start from the users trying to access the local area network which in most of the cases is the Campus LAN dedicated to interconnect the devices inside a campus. Users can connect to the LAN using wired or wireless mediums using various devices such as mobile phones, personal computers (PCs), laptops, and internet of things (IoT) devices like video surveillance cameras. Multiple access is a very important requirement that needs to be served by the current traditional enterprise

networks which include campus access, branch access, remote access, and LTE connections. All the campus LANs are then connected to the WAN which is the wide area network. WANs connect an organization's locations to one another, to the locations of other organizations, to external services, and to remote users using the facilities offered by a service provider or carrier, like a telephone or cable company [1].

WAN is a group of LANs in a network spread across a wide geographical area. The WAN after receiving the packets from the LANs passes them to the data centers where the application resides. A data center is a physical facility that enterprises use to house their business-critical applications and information. From centralized on-premises facilities, they advanced to edge deployments, and then to public cloud services. [2]. In most of the companies only the business-critical applications reside in the data center and other services are obtained using the clouds where services are offered by other companies. The packet might be intended for an external service served by the cloud which the data center should handle the request accordingly. The term "cloud computing" describes both the infrastructure and software in the data centers that provide the applications offered as services via the internet [3]. The hybrid cloud services have become more important and users might expect the application resources from hybrid cloud to be served in the enterprise which the current data center must handle. Some user requests might be the information residing over the internet, in that case the request must be sent to the internet and get back the information requested. The multi cloud environment is essential in enterprises where the services requested by the users must be availed from different forms of cloud like public cloud (IaaS), SaaS like Gmail, Office 365, and internet (web).

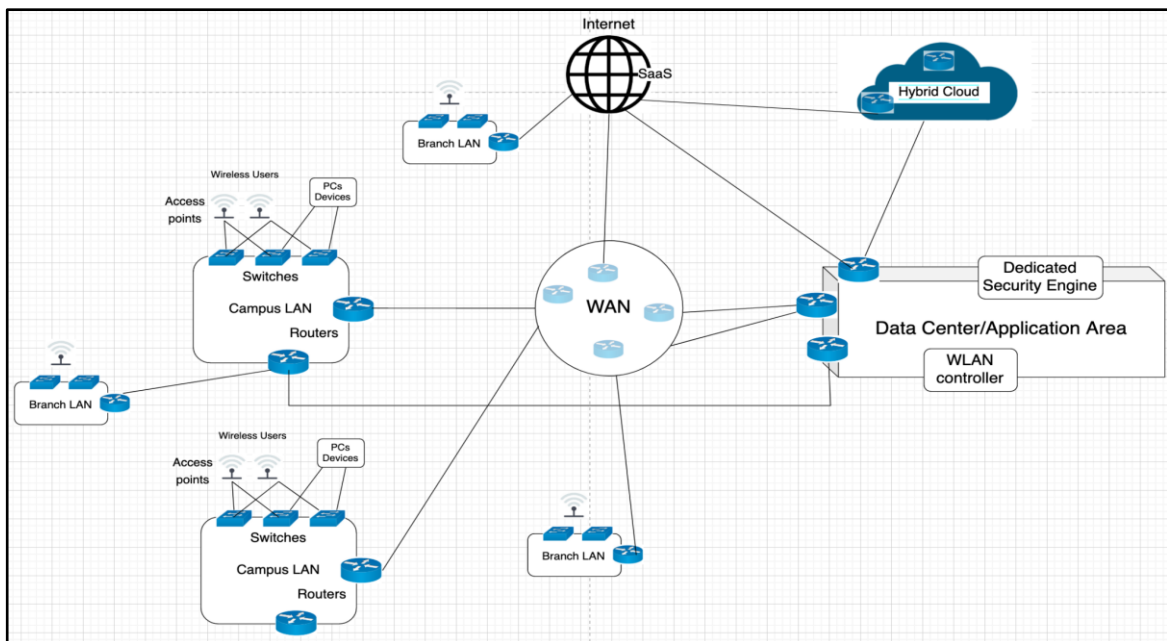


Figure 1. Traditional enterprise network architecture

2. SEGMENTS OF ENTERPRISE NETWORKING

2.1. Local area network (LAN)

The LAN is the connected environment where every campus device gets interconnected with other devices through ethernet and Wi-Fi connections inside the same geographical location. The architecture of the LAN is presented as a hierarchical design model of two types named two tier and three tier. In two tier architecture the distribution layer and core layer are combined and are directly connected to the WAN. In three tier architecture the distribution layer and core layer are separated. The users get connected to the LAN by the access layer switches which are also called edge of LAN and the access layer switches are connected to the distribution layer switches which thereby are connected by the core switches. The core switches are connected to the internet, data centers. Endpoints and users have direct access to the network through the access layer and the distribution layer aggregates the access layers to offer connectivity to the services [4]. For large LAN environments, the core layer provides communication between the distribution layers [4].

2.1.1. Wireless LAN

The wireless communication is done through the air using the radio wave propagations in standard frequency ranges. The access points are used to connect wireless users with the network and act as access edges for the local area network. The communication frame used in a wireless network must be transformed to a different kind and sent to the outside world by the access point, which performs the bridging [5]. The maintenance of ongoing connections as a user switch between various wireless access networks is made possible by handover methods [6]. The network issue might occur from many reasons which include client roaming issues, radio channel inferences, non-Wi-Fi devices inference, access points congestion, network congestion, less coverage of the access points, ap-ap inference [7]-[9]. The roaming itself has to go through many phases such as transfer of client context from one access point to another, retaining the IP address of the client so as to not to break the existing connection, and continuing the communications of the client from the new access point [10].

Techniques like radio frequency triangulation and angle of connection can help the administrator to pinpoint the location of the wireless client and various other IoT devices [11]. The access points emit and receive the radio frequencies containing the data packets in the form of waves. The access points are connected to the access layer switches which forward the packets deep into the network to reach the controller. A WLAN controller is a device for managing the Access points and other centralized benefits can be leveraged using the controller. Access points can be autonomous without the need of a WLAN controller, but in the case of large networks, wireless network management becomes very complex and hard. From the access layer switches the data is sent to the distribution layer switches which are the aggregation point which helps in network scalability, availability and interconnect the access layer switches. The distribution layer reduces the complexity of increasing access layer switches as it requires a smaller number of protocols to operate it and works as an end-to-end solution for LAN connectivity with WAN. The next higher layer of switches is the core layer which connects the multiple distribution layer switches. Connectivity is enhanced by the use of core layer switches where the distribution layer switches can focus on network failure and network control areas [4]. The characteristics of WLAN are physical layer (spectrum modulation techniques), frequency bands (5 Ghz or 2.4 GHz), data rates, operating range and network security [12].

The data is then transferred from core layer switches to the data centers which hold wireless LAN controllers with high processing power. Additionally, security, policy implementation, radio resource management (signal, interference, load, noise, coverage), and seamless roaming can become very easy to manage and implement across the network consistently. Wireless network analytics can become very easily available as the whole traffic is passing through the WLAN controller and the whole picture of network events can be logged and analyzed for any problems in the network, optimization of network usage. The access points are connected to the WLAN controller through control and provisioning of wireless access points protocol (CAPWAP) tunnels [13]. Traditionally all wireless data packets generated from users and also the control traffic packets for the access points are sent through the CAPWAP tunnel. This tunnel is for encapsulating the data from access points and forwarding the packets across the network.

2.1.2. Wireless LAN security

The wired equivalent privacy (WEP) protocol, which is used to safeguard link-level data during wireless transmission between clients and access points, essentially provides the security services [14]. Security service to confirm the communicating client stations' identities. By preventing access to client stations that can't authenticate properly, this gives the network access control. Another goal of security was to stop casual listening from compromising information (passive attack). WEP also aimed to prevent communications from being altered while in transit between wireless clients and the access point during an active attack. The exploitation of static WEP keys, traffic decryption using statistical analysis, active attempts to insert new traffic from unapproved mobile terminals, and dictionary-building attacks are some of the issues with wireless security standards are some other problems of wireless security standards along with not addressing audit, authorization, and non-repudiation security services [14].

2.2. Wide area network (WAN)

For connecting multiple LANs present in different geographical locations the solution is to have a WAN. A country, a continent, or even the entire planet can be covered by a long-distance transmission of information, picture, sound, and video data via WAN [15]. The connections between LANs can either be in the form of switched WAN (router connecting LANs) or leased lines (point-to-point), public telecommunication networks. To establish the link over the communication line from the sending to the receiving device, WANs need data link layer protocols as HDLC, PPP, ATM and frame relay, ISDN and X.25 [15]. Data link layer protocols define how data is illustrated for transmission to distant destinations and the tools used to transfer the data to subsequent network edges. The LANs mostly deal with forwarding the packets

using the switches internally, but when it comes to WAN, the routers are used for communication between the LANs. WAN switching consists of two types such as packet switching (split the packet and send via different paths to target) and circuit switching (fix the path and send all packets) [1]. There are different types of WAN technologies like IPsec VPN, MPLS VPN, ethernet private line (EPL), virtual private LAN service (VPLS), Wavelength. Idea behind all these technologies is to securely transfer the data at high speeds using technologies like Multiprotocol label switching, virtual private network, synchronous optical network (SONET). To deliver layer 2 or layer 3 VPN data networking services, MPLS VPN is a virtual private network constructed on top of a provider's multiprotocol label switching network [16]. IPsec VPN is used to secure the enterprise sites and their connections by making them all present in the same private network [17]. In MPLS TE (traffic engineering), a label switched path, is established for carrying traffic along an explicit path, which may differ from the general destination-based path [18]. The MPLS tagging helps the user data to be partitioned and transferred separately on the network infrastructure based on the tags which gives the enterprise more control over the prioritization of business needs [19], [20]. VPLS provides the facility for remote access making it look like the remote users and branches are still on the same private network where they are actually geographically sparsely dispersed. A packet-switching method called frame relay operates at OSI model layer 2. A virtual circuit is a logical path that is established between two routers. To identify the virtual circuit, frame relay employs a layer 2 address known as the data link connection identifier (DLCI) [19].

2.3. Data center/multi cloud

Data centers can be considered as the business processing core of the enterprises. Data centers as the name suggests are an integrated collection of computing servers and storage devices capabilities to process and store both application data and network management data. Data centers in most of the enterprises are used to store the business-critical application and data. Typical data centers consist of switches, routers, load balancers, analytics engines, application delivery controllers, network device controllers, and data storage systems. Many segmentation techniques are used in the data centers to separate users from one another and make the business more user friendly and customer centric.

Modern data centers are built to handle applications which use big data, artificial intelligence, machine learning. Only if the applications critical for the business enterprises own the data centers inside the campus. In most of the current enterprises the data centers are in the form of rented spaces of computing and storage infrastructure owned by other companies. Based on the requirements of the business the data centers can be easily scaled up and down. The data centers have the capability to visualize the whole network which makes it very easier for the network administrators while troubleshooting. Any failures or disruption over the network are dynamically handled by the data centers and provide maintainable components in failure events. Recently the infrastructure has been evolved into a multi cloud environment where the applications and data are no longer in the same place. Traditionally, multi-cloud meant using resources from various providers' data centers [21]. The applications are now distributed across many pools of infrastructure all connected by network services making it work as an integrated system, and efficiently utilize the resources. Multi-cloud can take different forms such as hybrid cloud, federated clouds [21]. In order to use traditional cloud computing, an application must be hosted on a virtual machine (VM), which then provides a service to the user [22].

2.4. Security

Whenever the question of security comes it mostly relies on the access and policy of the enterprise. The enterprise network is very business critical and any compromise of the network devices might bring a lot of damage to the company's reputation and business. The whole trust on enterprise sometimes completely depends on how secure the systems are built and maintained in the enterprise. Modern times the security not only should focus on restricting unauthorized access and protecting the company's trade secrets but also protect the crucial customer private data which is also called privacy.

The broadcasting nature of ethernet LANs have fundamentally been designed to provide easy deployment and flexible connectivity but these architectural purposes have been reasons for the security vulnerabilities in current day LANs. The attacker may use the network access for eavesdropping, information manipulation, network availability disruption, or gathering knowledge about the private network topology and network traffic for use in a future assault. Taking control of switches, routers, or servers in the LAN. The ethernet threats include network access, traffic integrity (ARP and DHCP poisoning, man in middle), traffic confidentiality, system security (configurational and architectural issues), DOS as discussed in [23]. When it comes to WAN, the security challenges posed are very different from those posed in LANs and MANs. The wider range of access to the wide area networks has even increased the attacking techniques that could damage the WAN. The network attacks have become more intelligent ranging from flawed DDoS attacks to spoofing attacks, hijacking attacks and zero-day attacks [24]. The data in the cloud can be categorized as data at rest (data stored in cloud storage) and data in transit (data in movement containing sensitive information). Lack of

governance by service providers, insufficient data format standards, a lack of client isolation, insecure or partial data erasure during virtual machine reallocation, and hacked administration interfaces are the security issues with data in cloud computing [24], [25]. The enterprises have a policy database which has the rules and conditions for any connection being made within the enterprise boundary which leads to transfer of data packets both inside and outside. The security appliances are generally aware of these policies and always be looking for any policy violations, breaches or attacks going to happen, happening or has happened. The access to campus LAN can be of any form taking from IoT devices to personal computers, both wired and wireless communications. All the connection standards and protocol format are to be followed based on the policy database before allowing the data packets in or out of the enterprise boundary. Dedicated systems for security purposes are very much required in today's conditions.

3. SOFTWARE DEFINED TRENDS

3.1. Current requirements of networks

The evolution of cloud computing has increased the need for network services and more bandwidth. Because of wireless technology more devices like video surveillance cameras, barcode scanners, LEDs and many other IoT devices are joining the network and it has increased the complexity for traditional networks [26]. The decision-making process can be more simplified by having an overall view of the network and a centralized control over the network.

The automation of network services is very difficult with the traditional networks because of the distributed control over the network by all the switches. There are limitations with the number of MAC addresses that can be stored in the forwarding tables of switches and number of VLANs which can be created. Due to these limitations the network installations and deployments have become very difficult. To prevent forwarding loops, networks are restricted to follow only one path for data communication despite having equally efficient paths available. In case of failure the network should be able dynamically find alternate paths to transfer the data and optimally use the unused network resources. The cloud must now provide a private network for each user and segment data traffic. Network virtualization has become equally important as server and storage virtualizations.

3.2. Traditional vs software defined networking

In traditional networks the control plane and data plane were combined together inside a network device. Control plane is responsible for making the forwarding decisions using the control protocols that affect the forwarding tables and the data plane schedules, buffers, modifies and forwards the packets to the corresponding destination. Control plane is responsible for getting the topology of the network. In software-defined networking (SDN), the control plane is separated from the data plane [26], [27]. The centralized controller is built to control the switches and modify the forwarding tables. This centralized control has opened up the possibility of finding multiple paths to destinations, dynamic response to the events happening in the network, programmable networks, and network virtualization.

Switches have the forwarding tables by which the switches just forward the data based on the match found in the forwarding tables with packet information [27]. In traditional networks each layer 2 and layer 3 switch had to choose between the large number of protocols available and repeatedly do the same tasks at each switch to get the information regarding the topology. The network security can easily be improved with a centralized controller which is not possible in traditional networks where the control plane is distributed among the switches. In traditional networks the hardware appliances are used to get high speeds in matching the forwarding table contents with the packet headers. To assist in making management decisions, SDN monitoring tools should be able to record the information and behavior of the network [28]. In traditional networks the functionalities are implemented in dedicated hardware like application specific integrated circuit (ASIC) [29]. However, this traditional hardware-centric networking has many limitations like packet modification, individual flow statistics, handling the overflow of packets, translation of flow table entries into hardware entries. In traditional networks the programming of the network is not possible directly and has to be done using protocols. Whereas in SDN the northbound APIs are used by the applications to directly program the controller and thereby configuring the network directly.

In traditional networks only the switches and routers are used for connections but in SDN, the virtual abstraction of the physical infrastructure is used to create connections and dynamically create network paths without touching the underlying physical infrastructure. The administrator has more control over the traffic flow in SDN as the network view is reviewed at a single point interface. New devices being added to the traditional networks needs to be accessed manually using consoles in the device but in SDN, administrators can program the controller to access the network devices directly wherever it is present in the network. Network virtualization is an abstraction of the physical networks using software [30]. Switching, routing, firewalling, load balancing and VPNs all such services are delivered by software. Network overlays are created by the

software over the physical network. This technique helps in moving virtual machines more easily rather than reconfiguring the whole network [31].

4. SOFTWARE DEFINED ENTERPRISE NETWORKING ARCHITECTURE

The software defined enterprise network has special functional segments in place of traditional functional segments. Figure 2 shows the software defined architecture of an enterprise network with the changes in the LAN and WAN along with their corresponding controllers. The WAN is changed to SD-WAN and the corresponding controller is added to the enterprise network. The campus LAN is changed to software defined LAN where the switches, routers in LAN are configured to be software defined and are not autonomous anymore as they are controlled by the SD-LAN controllers. The wireless connections in traditional networks were managed using access points controlled by the WLAN controllers where both user traffic and control traffic like authentication, mobility, radio resource management, client session management, and image management. were sent to the controllers. But in software defined enterprise networks the management of user data traffic is done directly by the access points through techniques like VX-LANs and only the control plane traffic is sent to the WLAN controller thereby solving the challenges in wireless networks.

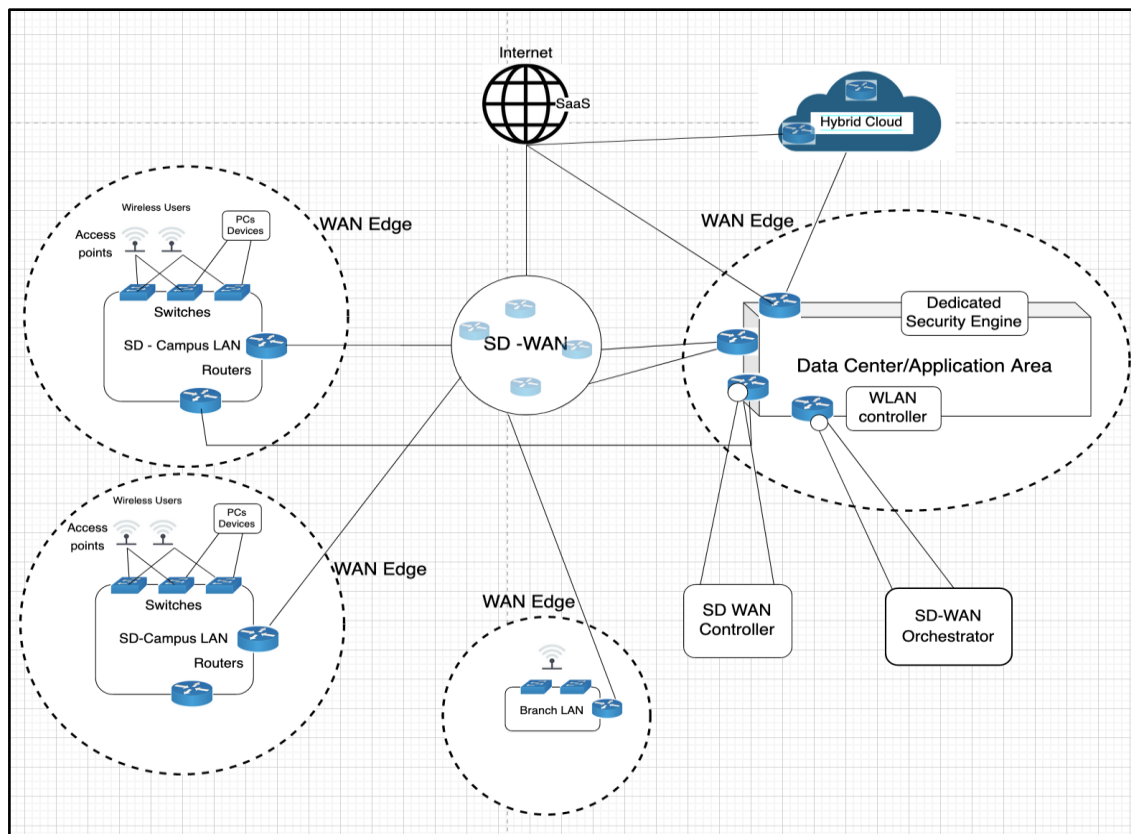


Figure 2. The architecture of software defined enterprise network

4.1. Software defined LAN

In software defined networking the switches are modified to work only for the data plane responsibilities. The centralized controller takes the job of filling the forwarding tables, responding to the control packets, dynamic reaction to the failure events, and simple programming of networks. The SD LAN controller uses the policy-based approach to manage the LAN devices across the network. The LAN controller does the end point device discovery such as laptops, mobile devices and other appliances. The LAN controller is also able to identify the network devices such as switches, and routers which form the infrastructure of the network. One of the important functionalities of the controller is to manage the topology of the network which includes the connections between the user devices and network devices and information regarding the interconnections among the network devices. Figure 3 depicts the SD-LAN containing software defined

switches, software defined controllers, applications in data centers which help the users to program the controller and network policy database which contains the policies of the enterprises provided by the network administrator accessed by the controller to apply them across the network for the corresponding.

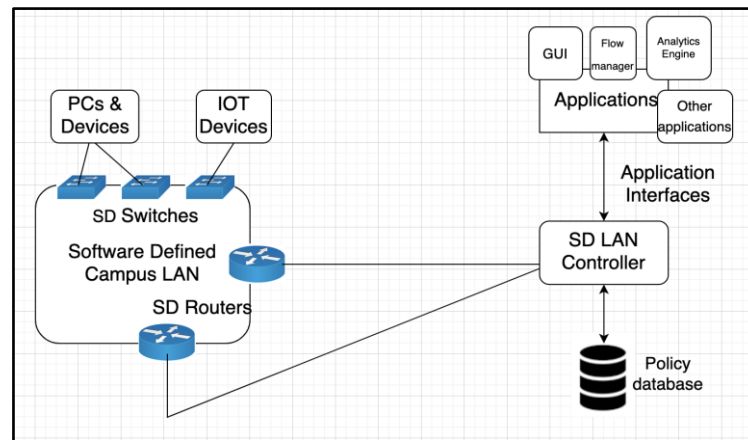


Figure 3. The software defined LAN architecture

Devices the northbound interfaces present above the controller allow the network administrator to program the network according to the requirement and also a single point graphical user interface backed control can be achieved through the software defined controller. The application programs the controller to respond to network topology changes like link failures and new device addition, traffic redirection for inspection, security related tasks, finding the best suitable paths between two network devices [32]. With the help of the LAN controller and the northbound applications, the end user business policies and group-based policies such as employee-based policies, IoT devices policies can be applied across the network without having to manually configure each network device [33], [34].

The group-based segmentation can be achieved by techniques such as MPLS VPN, VPLS, GRE, and CAPWAP [35]. The SD LAN controller collects the traffic flow data among the network devices and stores it in the database. The southbound interfaces help the controller to program the software defined switches and program them according to application requirements. Using Artificial intelligence and machine learning, the stored flow data can be processed and the statistical analysis will be produced based on which the network devices and their inter connections can be effectively managed. The statistical analysis information can be shown in dashboards or graphs which is very helpful while debugging and optimizing the network performance.

4.2. Software defined-WAN (SD-WAN)

In SD-WAN the network devices operating are the router which work at layer 3 and connect the LANs. The SD-WAN layers are the control layer which autonomously implements and supervises network functions, the data layer manages bandwidth and forwarding abstraction and the application layer offers services that allow internet service providers and developers to specify the network requirements for such services to be provided [36]. Using an SD-WAN controller the routers in the WAN are controlled and are only used for forwarding the packets across the network based on the routing tables. The routing tables are now filled by the controllers by considering the global view of the network. Earlier the routing process was complex and time consuming, but with the introduction of SD-WAN the routing is managed by the central controller. With the central global view of the network the controller can dynamically find alternate paths in case of any MPLS leased line failover. The resilience had made the current SDN approaches more used by enterprises in business-critical applications. SD-WAN lets the enterprises utilize various multiple network transport services to increase the bandwidth and transfer data safely without latency and network failure. The data based on its characteristics is transferred in the corresponding type of bandwidth. For example, the LTE, MPLS, internet transport services can be split among the log data, latency sensitive data like voice and video, control data respectively [36]. In case of failure in one of the transport services, SD-WAN can use redundant paths even in different transport services. Regardless of the type and quantity of WAN connectivity at the branches, SD-WAN establishes an overlay network connecting all enterprise branches via IPsec tunnels. For instance, a branch can simultaneously deploy an MPLS private link, an Internet link, and LTE, and SD-WAN can

aggregate all the link bandwidth to boost the branch's overall throughput. SD-WAN also gives the analytics for the traffic flows for performance optimization and easy troubleshooting, monitoring of QoS for prioritizing business critical data traffic, network device monitoring, secure access management are the additional capabilities of SD-WAN. Virtual networks also called as overlays are created over the physical network to improve the network utilization and quickly create connections between end points. The network controller, which is programmed in such a way that it has a complete view of the network architecture, oversees continuously assessing the status of the links and dynamically determining which route should be used to send the data [37]. The challenge in traditional WAN was that it was not aware of the application and could not prioritize packet transfer through links at real time. The application aware routing (AAR) is the focal point of every SD WAN implementation. It is a feature that allows a user to specify the permitted levels of packet loss, jitter, delay, and bandwidth usage for an application [38]. Because of the SD-WAN, there are various types of controller deployment models such as cloud deployment, service provider deployment and on-premises deployment. A framework for business policy is offered by SD-WAN Orchestrator for corporate governance and service security policies. The management level is a high-level abstraction for handling configuration, debugging, monitoring, insights, forecasts, correlations, reporting, and notifications. It also includes centralized and unified policy management [39].

The SD-WAN provides the enterprises with zero touch provisioning, where multiple sites or branches can be provisioned remotely in a secure way. This zero-touch provisioning solves the problems such as high IT cost, business time consumption, inconsistent configurations in network devices. With SD-WAN, all management functions-including configuration, monitoring, and troubleshooting-are centralized through a single management interface. To give enterprise branches quicker access to the cloud, a cloud-delivered SD-WAN delivers globally dispersed cloud gateways that are located at the doorstep of the major SaaS/IaaS/PaaS providers. Overall installations and setups are made simpler because only one tunnel needs to be built from cloud gateways to each cloud provider, which will be shared by all the branches, rather than a full mesh between branches and cloud providers.

4.3. Wired vs wireless SDN

In general, distributed control issues in wireless networks are difficult to break down into simple, isolated functionality (i.e., tiers in traditional networking designs). Due to the shared wireless radio transmission medium, typical control issues in wireless networks require resource allocation decisions to be made at multiple layers of the network protocol stack that are inherently and tightly coupled. In contrast, in software-defined commercial wired networks, routing at the network layer can be focused on independently. Additionally, in most of the current implementations of this concept, SDN is accomplished by removing control decisions from the hardware, such as switches, and enabling hardware, such as switches and routers, to be remotely programmed through an open and standardized interface and relying on a centralized network controller to define the behavior and operation of the network forwarding infrastructure.

In wireless networks, where network nodes must make distributed, optimal, cross-layer control decisions at all layers to maximize network performance while keeping the network scalable, dependable, and simple to deploy, this inescapably necessitates a high-speed backhaul infrastructure, which is typically not available. These wireless-specific issues are obviously unsolvable by SDN approaches.

4.4. Challenges in software defined enterprise networking

The controller being a centralized control system the whole network can be compromised using a single controller and the new technologies, code, application interface for the working of controllers can become the reason for the network security threats [40]. With the network virtualization made more easier by SDN, the new network segments being created on the fly can have different risks and threats which need to be managed by the software defined approaches and network administrators. With the rise of the number of networking devices communicating with the controller for forwarding decisions and other configurations the number times the data being transferred between the network devices and controller increases rapidly. The delay between the communications can cause a serious performance degradation as the networking devices are waiting for the controller's policy instructions more time than working for packet transfers [41]. The solution is to bring more intelligence to the data plane devices so that the communications with the controller decreases. Another form of latency comes from the data centers which are located at far distances and in [42] the solutions to reduce this latency using geographically distributed mini data centers is discussed. The controllers in SDN are the single points of failure in the current network scenarios. For network path failure the solution is to have redundant paths for communication between the controller and networking devices so that even if the communication channels are blocked for any reason, the alternate paths can become active and serve the purpose. For controller device failure the solution is to have back up processing power so that whenever the controller is not able to server the huge number of requests from the network devices, the backup processing

power can be used. In case of controller complete breakdown, the standby controllers need to be introduced for which the data in the previous controllers needs to be copied and used for consistent controller communications.

There is a limit to the number of devices a single controller can handle by itself. As the number of devices getting added to the organization network, the controller becomes a bottleneck [40], [43]. The solution is to have more controllers talking to each other to control the multiple devices. The SDN adoption is not going to happen within a short time as the legacy networks have been used more dependently for business to be active all over the world. Hence the interoperability between the legacy devices and software defined devices is also an important [40]. The solution is to have devices hybrid to both SDN and legacy devices, which can work with new protocols specifically introduced for the interoperability purpose. The networking issues of cloud computing include security, reliable communication, virtualization, resource allocation, interoperability [44]-[46]. In SD-WAN the challenges posed are distributed control planes, traffic engineering and network monitoring for traditional mechanisms, low-latency routing, data plane fault tolerance, data plane load balancing, internet scale attacks [47]-[49].

4.5. Challenges in SDN migration from traditional enterprise networks

The migration from traditional networks typically involves challenges like identifying the network requirements, initial preparations for migrations, actual assessment of the results, phase wise migrations. There are options available for migration based on the device types in network like all the network devices controlled by the controller, some devices being controlled and hybrid devices which can switch from traditional to software defined implementations. The Stanford University SDN Migration and the Google's SDN migration gives the details into verification and flexibility of SDN. Prioritizing the core demands of the network, deploying software into network devices for them to be compatible with software defined approaches, validation of the results for the SDN implementations if they are really helping to solve the network issues and business difficulties are useful for SDN migration [50]. Examines the effectiveness of SDN in various topologies and connection failure scenarios [51]. The complexity, flexibility, and possible functionality and capabilities of two SDN architectures-OpenFlow and ProGFE were examined in [52].

5. CONCLUSION

The usefulness of SDN in clouds and data centers is primarily found in its capacity to offer additional functionalities such network virtualization, resource provisioning automation, and the development of new services on top of provisioned network resources. For instance, cloud applications and services can get network topology, keep track of underlying network circumstances like failures, and start and modify connectivity. Throughput and round-trip-time (RTT) performance comparisons have been provided and discussed. Instant provisioning, improved resource planning, and adaptability are problems caused by virtualization and cloud computing, but they can be resolved with the help of SDN's control paradigm. The differences in the software defined solutions provided by different vendors must be considered while using the devices in the enterprises. Standard APIs must be built in the servers to communicate with controllers and for controllers to communicate with the network devices, in an efficient and clear manner to program the network with more control and quickly. It's observed that SDN flexibility does sacrifice raw performance while increasing overhead for a more complicated feature. Network virtualization can become as important as server and storage virtualizations for the better serving of business-critical applications.

REFERENCES




- [1] S. Tanenbaum, "Network hardware: wide area networks," *Computer Networks*, Pearson Education India, 2011, pp. 11-13.
- [2] C. Wu and R. Buyya "Cloud computing," *Cloud Data Centers and Cost Modeling: A Complete Guide to planning, designing and building a cloud data center*. Morgan Kaufmann, 2015, doi: 10.1016/B978-0-12-801413-4.00001-5.
- [3] D. C. Marinescu, "Introduction," In *Cloud computing: Theory and practice*. introduction, Elsevier, MK, Morgan Kaufmann Publishers, pp. 1-17, 2013, doi: 10.1016/B978-0-12-404627-6.00001-4.
- [4] M. H. Ferdous, M. Murshed, R. N. Calheiros, and R. Buyya, "Network-aware virtual machine placement and migration in cloud data centers," *In Emerging research in cloud distributed computing systems*, pp. 42-91, IGI Global, 2015, doi: 10.4018/978-1-4666-8213-9.ch002.
- [5] S. Ali and K. Mohan, "A survey on IEEE 802.11 wireless LAN technologies," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, no. 10, October 2015.
- [6] Z. Chen, Z. Luo, X. Duan, and L. Zhang, "Terminal handover in software-defined WLANs," *EURASIP Journal on Wireless Communications and Networking*, 2020, pp. 1-13, doi: 10.1186/s13638-020-01681-w.
- [7] Z. Zhong, P. Kulkarni, F. Cao, Z. Fan, and S. Armour, "Issues and challenges in dense WiFi networks," In *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 947-951, IEEE, 2015, doi: 10.1109/IWCMC.2015.7289210.
- [8] J. Dhankhar, "Research issues and challenges in wireless networks," *International Journal of Engineering and Management Research (IJEMR)*, vol. 4, no. 3, pp. 381-384, 2014.

- [9] Nishi, "Research issues and challenges in wireless networks:an overview," *International Journal of Innovative Science and Research Technology*, vol. 3, no. 5, May 2018.
- [10] H. Ahmed and H. Hassanein, "A performance study of roaming in wireless local area networks based on IEEE 802.11r," *In 2008 24th Biennial Symposium on Communications*, 2008, pp. 253-257, doi: 10.1109/BSC.2008.4563250.
- [11] V. Osa, J. Matamales, J. F. Monserrat, and J. L. Bayo, "Localization in wireless networks: the potential of triangulation techniques," *Wireless Personal Communications*, pp. 68, 2012, doi: 10.1007/s11277-012-0537-2.
- [12] M. Dahiya, "Evolution of wireless LAN in wireless networks," *International Journal on Computer Science and Engineering*, vol. 9, pp. 109-113, 2017.
- [13] P. R. Calhoun, M. P. Montemurro, and D. Stanley, "Control and provisioning of wireless access points (CAPWAP) protocol specification," *RFC 5415*, 2009, pp. 1-155, doi: 10.17487/rfc5415.
- [14] V. K. Gandhi, "A study on wireless lan fundamentals, architecture, benefits and its security risks," *Indian Streams Research Journal*, vol. 4, no. 8, Sept 2014.
- [15] M. S. Mazhar, "Comparative study of WAN services and technologies in enterprise business networks," *International Journal of Computer Science and Telecommunications*, vol. 10, no. 3, May 2019.
- [16] L. L. Peterson and B. S. Davie, "Advanced internetworking," In *Computer Networks: A systems approach*, pp. 354–365, Morgan Kaufmann Publishers, an imprint of Elsevier, 2011.
- [17] S. Bhattarai and S. Nepal, "VPN research," (Term Paper), 2016, doi: 10.13140/RG.2.1.4215.8160.
- [18] R. Q. Shawl, R. Thaker, and E. J. Singh, "A review: multi protocol label switching (Mpls)," *International Journal of Engineering Research and Applications*, ISSN: 2248-9622, vol. 4, no. 1, pp. 66-70, January 2014.
- [19] H. Kaur and R. K. Gurm, "Comparative analysis of WAN technologies," *International Journal of Computer Science Trends and Technology*, vol 3, no. 5, Sep-Oct 2015.
- [20] M. A. Ridwan *et al.*, "Recent trends in MPLS networks: technologies, applications and challenges," *IET Communications*, 2020, doi: 10.1049/iet-com.2018.6129.
- [21] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," *Future Generation Computer Systems*, vol. 79, Part 3, pp. 849-861, 2018, doi: 10.1016/j.future.2017.09.020.
- [22] J. Smith, R. Nair, and J. E. Smith, "Introduction to virtual machines," In *Virtual Machines: Versatile platforms for systems and Processes*, pp. 1–10, 2005, doi: 10.1016/B978-155860910-5/50002-1.
- [23] T. Kiravuo, M. O. Alassafi, R. Walters, and J. Manner, "A survey of ethernet LAN security," *Communications Surveys and Tutorials*, IEEE, vol. 15, pp. 1477-1491, Jan. 2013, doi: 10.1109/SURV.2012.121112.00190.
- [24] Y. Luo, "Analysis of wide area network security technology system," *Proceedings of the 2017 5th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering*, 2017, doi: 10.2991/icmmce-17.2017.42.
- [25] A. Albugmi, M. O. Alassafi, R. Walters, and G. Wills, "Data security in cloud computing," *2016 Fifth International Conference on Future Generation Communication Technologies (FGCT)*, London, UK, 2016, pp. 55-59, doi: 10.1109/FGCT.2016.7605062.
- [26] A. O. Jefia, S. I. Popoola, and A. A. Atayero, "Software-defined networking: current trends, challenges, and future directions," *presented at proceedings of the International Conference on Industrial Engineering and Operations Management Washington DC*, Sept 27-29, 2018.
- [27] B. N. Astuto, M. Mendonça, X. N. Nguyen, K. Obraczka, and T. Tuletta, "A survey of software-defined networking: past, present, and future of programmable networks," *Communications Surveys and Tutorials, IEEE Communications Society*, vol. 16, no. 3, p. 1617, IEEE 2014, doi: 10.1109/SURV.2014.012214.00180.
- [28] A. Hakiri, A. Gokhale, P. Berthou, D. C. Schmidt, and T. Gayraud, "Software-defined networking: challenges and research opportunities for future internet," *Computer Networks*, vol. 75, pp. 453-471, 2014, doi: 10.1016/j.comnet.2014.10.015.
- [29] T. G. Robertazzi, "Software-defined networking," In *Introduction to Computer Networking*, pp. 81–85, 2017, doi: 10.1007/978-3-319-53103-8_7.
- [30] N. Chowdhury and R. Boutaba, "Network virtualization: state of the art and research challenges," *Communications Magazine*, IEEE, vol. 47, no. 7, pp. 20–26, July 2009, doi: 10.1109/MCOM.2009.5183468.
- [31] A. Wang, M. Iyer, R. Dutta, G. N. Rouskas, and I. Baldine, "Network virtualization: technologies, perspectives, and frontiers," in *Journal of Lightwave Technology*, vol. 31, no. 4, pp. 523-537, Feb. 2013, doi: 10.1109/JLT.2012.2213796.
- [32] V. Panagiotopoulou, "Controller-based WLAN design and evaluation," 2015, doi: 10.13140/RG.2.2.30468.88964.
- [33] M. Jammal, T. Singh, A. Shami, R. Asal, and Y. Li, "Software defined networking: State of the art and research challenges," *Computer Networks*, vol. 72, pp. 74-98, 2014, doi: 10.1016/j.comnet.2014.07.004.
- [34] E. Udo, E. Isong, and E. Nyoho, "Software defined networking framework for campus network management," *International Journal of Computer Science and Network*, vol 9, no. 4, Aug 2020.
- [35] D. Terefenko, "A comparison of multiprotocol label switching (MPLS) and OpenFlow communication protocols," *M.S. thesis, Distributed and Mobile Computing, Institute of Technology*, 2018, doi: 10.13140/RG.2.2.14457.98404.
- [36] J. Bustamante and D. A. Pesantez, "Comparative analysis of Cybersecurity mechanisms in SD-WAN architectures: A preliminary results," *IEEE Engineering International Research Conference (EIRCON)*, pp. 1-4, Oct. 2021, doi: 10.1109/EIRCON52903.2021.9613418.
- [37] C. J. Diaz, L. Andrade-Arenas, J. G. Arellano, and M. A. Lengua, "Analysis about benefits of software-defined wide area network: a new alternative for wan connectivity," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 1, 2022, doi: 10.14569/IJACSA.2022.0130188.
- [38] P. Iddalagi, "SD WAN – its impact and the need of time," *Journal of Ubiquitous Computing and Communication Technologies*, vol. 2, pp. 197-202, 2020, doi: 10.36548/jucct.2020.4.002.
- [39] F. Aldeeb and A. A. Ahmed, "Software defined wide area network SD-WAN: principles and architecture," *4th International African Conference on Current Studies*, Oct 2021.
- [40] M. Paliwal, D. Shrimankar, and O. Temburne, "Controllers in SDN: a review report," in *IEEE Access*, vol. 6, pp. 36256-36270, 2018, doi: 10.1109/ACCESS.2018.2846236.
- [41] V. Shamugam *et al.*, "Software defined networking challenges and future direction: a case study of implementing SDN features on OpenStack private cloud," In *IOP Conference Series: Materials Science and Engineering*, vol. 121, no. 1, p. 012003. IOP Publishing, 2016, doi: 10.1088/1757-899X/121/1/012003.
- [42] M. Mathur and M. Madan, "Software defined cloud mini data centers – an effort towards reduction in latency mini cloud traffic delivery," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 12, pp. 20–26, 2019, doi: 10.35940/ijitee.I2483.1081219.
- [43] B. Sokappadu, A. Hardin, A. Mungur, and S. Armoogum, "Software defined networks: issues and challenges," *2019 Conference on Next Generation Computing Applications (NextComp)*, 2019, pp. 1-5, doi: 10.1109/NEXTCOMP.2019.8883558.




- [44] J. Moura and D. Hutchison, "Review and analysis of networking challenges in cloud computing," *Journal of Network and Computer Applications*, vol. 60, pp. 113-129, ISSN 1084-8045, 2016, doi: 10.1016/j.jnca.2015.11.015.
- [45] P. Paul and P. S. Aithal, "Cloud security: an overview and current trend," *International Journal of Applied Engineering and Management Letters (IJAEML)*, vol. 3, no. 2, pp. 53-58, ISSN: 2581-7000, 2019, doi: 10.47992/IJMTS.2581.6012.0070.
- [46] S. Mishra and M. Alshehri, "Software defined networking: research issues, challenges and opportunities," *Indian Journal of Science and Technology*, vol. 10, no. 7, pp. 1-9, 2017, doi: 10.17485/ijst/2017/v10i29/112447.
- [47] O. Michel and E. Keller, "SDN in wide-area networks: A survey," *2017 Fourth International Conference on Software Defined Systems (SDS)*, Valencia, Spain, 2017, pp. 37-42, doi: 10.1109/SDS.2017.7939138.
- [48] R. A. AlSolami, R. H. AlJabali, and R. A. Obeid, "A holistic review of SD-WAN security challenges," *International Journal of Computer Applications*, vol. 176, no. 33, pp. 20-23, 2020, doi: 10.5120/ijca2020920398.
- [49] A. Rajendran, "Security analysis of a software defined wide area network solution," *Data Communication Software: Electrical Engineering, Aalto University School of science, Espoo*, July 13, 2016.
- [50] P. Goransson, C. Black, and T. Culver, "Genesis of SDN," In *Software defined networks a comprehensive approach*, pp. 39-56, 2016, doi: 10.1016/B978-0-12-804555-8.00003-X.
- [51] T. L. Huang, G. L. Wu, X. Huang, and N. Hansen, "Characterization of Si particles and their effects on and recrystallization in a nanostructured cold rolled Al-1% Si alloy," In *IOP Conference Series: Materials Science and Engineering*, vol. 89, no. 1, p. 012028. IOP Publishing, 2015, doi: 10.1088/1757-899X/557/1/012028.
- [52] A. Gelberger, N. Yemini, and R. Giladi, "Performance analysis of software-defined networking (SDN)," *Proceedings of the 2013 IEEE 21st International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems*, pp. 389-393, Aug. 2013, doi: 10.1109/MASCOTS.2013.58.

BIOGRAPHIES OF AUTHORS






Dr. Pratiba Deenadhayalan    is working as an Assistant professor in Computer Science and Engineering department at RVCE. She received her Ph.D. degree from VTU. She has published over 40 research papers. She has worked on various research and consultancy projects sponsored by Cisco, Citrix and Samsung. She can be contacted at email: pratibad@rvce.edu.in.



Dr. Ramakanth Kumar Pattar    is a Professor and HOD in the Computer Science and Engineering department at RVCE. His research interests are digital image processing, pattern recognition and natural language processing. He has published over 100 research papers. He has executed several funded research and consultancy projects sponsored by DRDO, ISRO, AICTE, GE India Pvt. Ltd, CABS, HP, and Nihon Communication Solutions Pvt. Ltd. He can be contacted at email: ramakanthkp@rvce.edu.in.



Vijay Chiranjith Reddy    is currently pursuing his B.E. degree at R.V. College of Engineering in the department of computer science and engineering. Has worked on projects related to deep learning and machine learning. He has received a certificate of excellence in a student program offered by SAMSUNG for working on recommender systems. His areas of interest are deep learning, machine learning, web development, and computer networks. He can be contacted at email: rvchiranjith13@gmail.com.