Received: 7 February 2022 | Revised: 18 May 2022 | Accepted: 16 June 2022

DOI: 10.1049/ntw2.12039

IET Networks

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Performance evaluation of software-defined wide area network based on queueing theory

Samaa Adel Ibrahim Hussein[1] | Fayez Wanis Zaki[2] | Mohammed M. Ashour[3]

[1]Electronics and Communications Department of Faculty of Engineering, Mansoura University, Mansoura, Egypt

[2]Faculty of Engineering, Communication Engineering, Mansoura University, Mansoura, Egypt

[3]Faculty of Engineering Mansoura University, Mansoura, Egypt

Correspondence

Samaa Adel Ibrahim Hussein, Electronics and Communications Department of Faculty of Engineering, Mansoura University, Mansoura 35511, Egypt.
Email: samaaadel655@gmail.com

Abstract

Software-defined wide area network (SD-WAN) is part of wider technologies of software-defined networking (SDN). SDN is one of the pivotal network management approaches that abstracts the underlying network infrastructure away from its applications. SDN allows for the centralisation of network intelligence. That allows higher network automation, the simplification of operations, the provisioning, the monitoring, and the troubleshooting. These days, data volume that enterprises and users make is growing rapidly and continuously. As a result, wide area networks are growing increasingly and they are becoming very complicated to manage and monitor using traditional tools. So, many enterprises are interested in developing SD-WAN and benefiting from its advantages. To achieve this goal, a proposed model for the SD-WAN network will be presented based on the queueing theory; then, the proposed model will be analysed using the Quasi-birth–death approach to evaluate traffic behaviour of a proposed queueing model for Poisson distribution in the SD-WAN. Moreover, it compares Poisson to phase type distribution via calculating some parameters that influence traffic behaviour of those distributions in the SD-WAN. The analysis results indicate that the proposed queueing model displays a more accurate SD-WAN controller performance than the existing ones.

1 | INTRODUCTION

Network companies are adopting digital transformation and speedy development technology to raise productivity and decrease costs. The basic function of the wide area network (WAN) was to link customers at the many branches or enterprise headquarters to applications installed on servers in the data centre [1]. Despite the development of technologies used in wide networks with the aim of increasing the security and reliability of the connection, it is lacking in the digital world as applications move out of the data centre into cloud; and users consume these applications that are highly mobile, employing different device sets [2]. Traditional WAN networks mainly depend on data centre infrastructure to provide cloud connectivity, yet that carries the inefficiencies of higher latency, heavy data centre load, and single failure points [3]. Additionally, the traditional WAN faces many challenges such as high bandwidth cost, configuration overhead, and zero-touch deployments that are not possible. Each device is error borne as a result of continuous human interventions and limited automation. Because each vendor has its own system, and it is not allowed any modification. High consumption of network time and resources is due to many operations that take place in the planes of traditional networks [4] and problems of digital electronic wars, which are one of the biggest problems facing traditional networks and cause the destruction of the infrastructure [5]. To solve the limitations of traditional WAN, many companies turned to a centralised model known as software-defined wide area network (SD-WAN), where the SD-WAN can be designed for modern applications and security requirements [6]. Briefly, the SD-WAN is Software-defined Wide Area Network and it is a network that extends over wide geographical areas where software-defined networking (SDN) technology is applied [7]. The software-defined networking technique is applied through decoupling the control plane (The intelligent brain of the network. Its main function is to control the routing of data in the data plane) [8] from the data plane. The data plane is responsible for forwarding traffic to the selected destinations according to the decisions of the control plane [9]. Analysing performance can be made as testing counter values reported while the system is performing various operations. There are some parameters that can be used for analysing SD-WAN such as delay, traffic receive, traffic send, utilisation and throughput [10]. Eventually, Queueing theory is one of the most popular theories used in the computer system, as the queueing theory in general deals with statuses where many processes or jobs wait in line for resources [11]. A few researchers have built queueing models for the SD-WAN by characterising their arrival process as a process subject to Poisson distribution [12]. Many researches focussed on the use of the Open Flow protocol to communicate between the data and control planes [13], since it is an Open Standard protocol, but this protocol is considered an organisational protocol that is not used to transfer configurations [14]. The aims of this paper are as follows:

- Analysing the performance of $M/H_2/1$ queueing model for SD-WAN-based Poisson distribution in arrival process distribution. To achieve this goal, the parameters affecting the behaviour of traffic are studied in the SD-WAN, such as load, throughput, traffic received, delay and utilisation.
- Performing mathematical analysis to the proposed model by using geometric matrix. In the end, a comparison is made between the model built in this paper, which assumes that the arrival process is subject to a Poisson distribution, and a previous study [15], that a model was built with the theory of queues, in which we assumed that the arrival process is subject to a phase type distribution. It is known that the service process in both scenarios is subject to exponential distribution.
- Discussing many of the new features of SD-WAN, through which the problems of traditional networks were overcome.

Closer to our work is the queueing model of SDN-based virtualisation technology and performance measurement where the proposed model of SDN was $M/H_2/1$ [16]. Nevertheless, these studies were carried out over small geographic areas, and they cannot be deployed to a WAN. It is also considered that Ref. [17] is one of the most important research projects that supported the results of this paper, as it compared the process of access based on the exponential distribution and the Poisson distribution in the local network.

1.1 | Queueing theory

According to Ref. [18], Queues occur when there is a contest for bounded resources. The bounded resources can be divided by servers, and the requests are arranged in waiting lists in front of these servers. Clients who request the service are said to 'arrive' at the service facility and place service 'demands' on the resource [19]. The resources are of finite capacity meaning that there is neither infinity of them nor can they work infinitely fast [20]. Modelling and analysing queue systems help to minimise their limitation and maximise the use of the resources. The analysis may predict the expected time to use resources or the expected time to wait for customers in queues [21]. This information is later used to make decisions as to when and how to upgrade the system. Finally, the most important goals of using the theory of queueing are as follows:

- Predicting the system performance, where the prediction is expressed as mean delay or the number of packets waiting in the queueing line to receive a service from the controller, based on first-in, first-out (FIFO) discipline.
- Despite the importance of predicting, the most important goal is to find a better design for the system to improve performance [10].

1.2 | Network performance measurement concept

Network performance is a measure of the quality of service (QoS) of a network. There are many different performance measures such as throughput, delay, utilisation, and response time [17]. The network planner analyses the network in every state and ensures that the network design is optimal while using such diagrams. Network availability is known as network performance. Performance of network is responsible for network latency, routing accuracy, security, and bandwidth. Some monitoring and managing tools assist the administrator in performance optimisation [11].

1.3 | Poisson distribution

The Poisson distribution, widely used in queueing theory, is a discrete probability distribution defined as the probability that a certain number of events will occur in a fixed interval of time if these events occur at a constant, known mean rate, independent of the time since the last event [22]. The Poisson distribution is used for the number of events in other specified intervals such as distance, area or volume [17].

1.4 | Phase type distribution

The phase type distribution is known as a probability distribution consisting of convolution or mixture of exponential distributions [22]. This distribution results from one or more phases of the interconnected Poisson distribution that occurs in series or phases. The sequence in which each of the phases occurs may itself be a stochastic process [23].

1.5 | Related work

Although there are many research studies, academic studies, and industrial applications that are used in the SDN technique, there are still shortcomings in its use across wide geographical distances [9]. To date, analytical SDN modelling research has been studied and analysed in two different ways: queueing theory and network calculus [24]. In this paper, a model of the SD-WAN network is presented upon queueing theory and an analysis of the proposed queueing model is presented. Software-defined networking networks are characterised by flexibility, which allows researchers to study and apply them in various fields and different geographical environments [25] such as Long and Hong [26], proposed, SDN network that has been modelled based on $M^m/\mathrm{M}/1$ and analysed the performance measurement with queueing theory. Samuel and Shamshin [16] presented an Open flow-SDN-based $\mathrm{M}/H_2/1$ queue to help performance measurement that is influenced by the traffic loads and network utilisation. Peng and Qu [27] presented an approach to evaluate SDN controller placement problem efficiently and accurately for WAN by using spectral clustering placement algorithm to partition a large network into different small SDN domains. Y. Goto et al. [19] proposed a queueing model of an OpenFlow-based SDN and provided an analysis of the proposed queueing model. The shortcomings of previous studies and how to solve them and our contributions are presented below:

- Several studies have used queueing theory to model SDN but all previous queueing models have been established for small network topology while our model was built on networks with wide geographical areas (SD-WAN).
- Previous studies relied on network devices (routers and switches) consisting of basic planes of SDN (management, control, and data) and the orchestration plane was neglected, but in our manuscript, this layer was studied. It is considered as one of the most important planes in SDN because it is responsible for the authentication processes between the controllers and the rest of the network devices.
- In previous studies, the OpenFlow protocol was relied on for communication between the control and data planes which cannot be applied to SD-WAN deployments. Therefore, in our study, the OpenFlow protocol was replaced by the NETCONF protocol due to its ability to transfer policies and configurations between planes. Also, OpenFlow is an organisational protocol, it cannot transfer configurations between planes.

2 | SOFTWARE-DEFINED-WIDE AREA NETWORK

2.1 | The proposed network design

The traditional WAN can route traffic from branches to enterprise data centres employing private Multiprotocol Label Switching (MPLS) technology. Companies move the applications out of the data centre and into public clouds such as Microsoft Azure and Amazon Web Services (AWS) [2]. But in traditional WAN shifting, the traffic from branches to the enterprise data centre and later outside to the cloud or Internet and back is inefficient, expensive, and not scalable [10]. Additionally, fast digital conversion of enterprises establishes security needs, cloud and Internet connectivity, WAN management, and application performance [28]. Automation as well as programmability through WAN are needed for improving network performance, redundancy, and visibility as well as reducing complexity [29]. A software-defined-wide area network (SD-WAN) will reduce complication and enhance performance by decoupling control from underlying hardware and assigning it to a centralised software-based controller. The SD-WAN became an important way for companies to decrease deployment cost, release human resources, and get quick, stable, secure communication links [8]. It has been designed for meeting requirements of new companies' applications and quickly increasing security demands.

Figure 1 illustrates a paradigm SD-WAN deployment scenario. The SD-WAN solution consists of four isolated planes: Orchestration, Management, Control, and Data Plane. Every plane has its own work and responsibilities and is isolated far from the other planes when compared with the traditional WAN; in traditional WAN, each device shares in the data plane (packets forwarding), in the control plane and in the management plane [3]. SD-WAN's parts can be explained as follows:

- ***vManage controller*** is responsible for the Management Plane in the SD-WAN system. It works for gathering network data, turns on analytic controller, and warns on critical events in the SD-WAN fabric paradigm. Additionally, vManage controller is the tool used in creating device templates, push configurations, and is used to do traffic engineering.
- ***vBond*** controller is the Orchestration Plane of the SD-WAN system. It is responsible for the authentication, authorisation and whitelisting of vEdge routers and control/management information distribution.
- ***vSmart controller*** works in the Control Plane of the SD-WAN fabric. It is the intelligence part in the SD-WAN system. It advertises routing, policies, and security. Noting that the vSmart controller is not part of the Data Plane additionally, it does not share in packet forwarding.
- ***vEdge routers*** act in the Data Plane of the SD-WAN fabric. They locate at the WAN border and form the network build and are responsible for establishing network fabric and forwarding traffic.

As shown in Figure 2, each traffic southbound of the vEdge routers can usually be traditional WAN—offices, data centres, and departments, while the traffic northbound of the vEdge routers represents the SD-WAN fabric. Routing information is exchanged between the control and data planes through an Overlay Management Protocol (OMP). Then the routing table is built in the control plane. Finally, the vSmart controller will be announced to other vEdge devices if needed as shown in Figure 3. It is important to note that the protocol responsible for transferring configurations and policies between the control and data planes is Network Configuration Protocol as shown in Figure 4. [3].

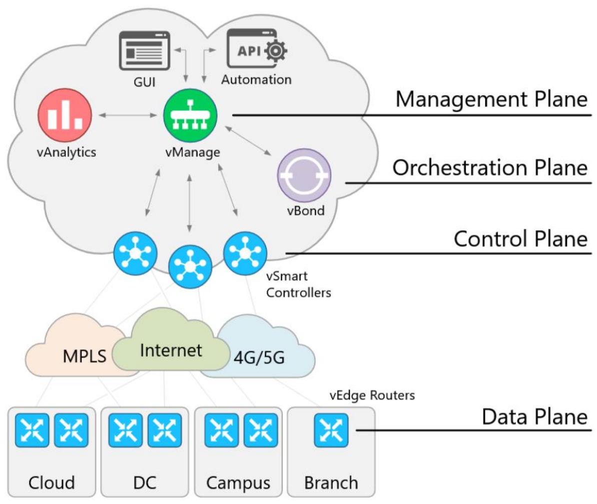

FIGURE 1 Software-defined-wide area network (SD-WAN) components

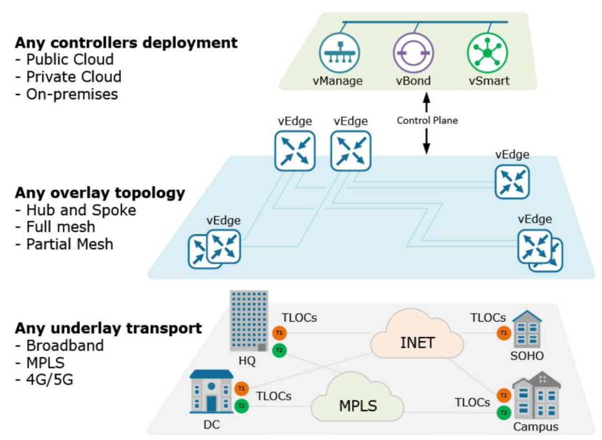

FIGURE 2 Software-defined-wide area network (SD-WAN) fabric

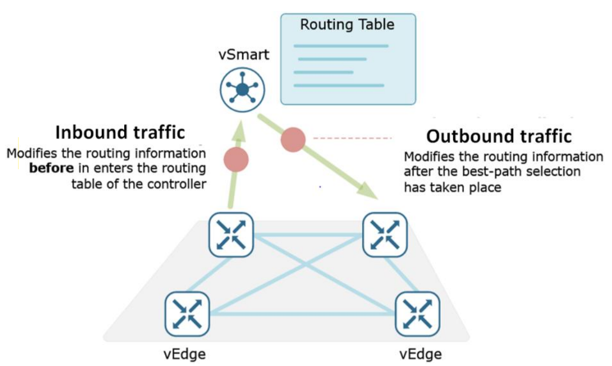

FIGURE 3 Routing process between data and control planes

The vEdge routers connect the cloud data centres, the company's headquarters and its branches to the Internet via different types of high-speed transports such as MPLS, Ethernet, leased line, digital subscriber line (xDSL), and 3 G/4G Long-Term Evolution (LTE). The SD-WAN controller

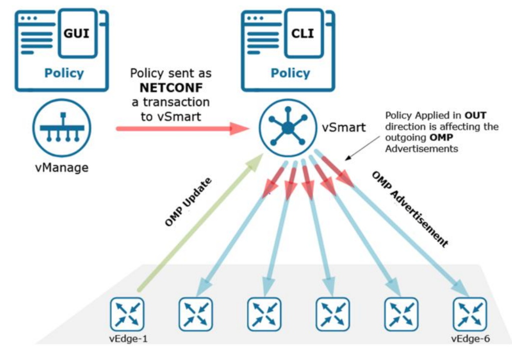

FIGURE 4 Software-defined-wide area network (SD-WAN) policy direction

manages topology, computes path, and secures data and control of policy over network [3]. In this solution, vEdge routers forward packets based on SD-WAN controller decisions that are scheduled in a routing table. A data packet arriving from the network comes to the vEdge router where all packets have a source Internet Protocol (IP) address and a destination IP address. The vEdge router parses the arrival packet for extracting all needful header fields at every protocol layer and lookup of IP destination. As shown in Figure 5, IP destination lookup in the routing table is the first step in the packet forwarding process [3].

- If the destination IP is matched, the action is processed in sequential order, beginning from the lowest sequence number upwards.
- When the match does not happen, the configured entity is subject to the default action configured (by default the vEdge router should send a request to the SD-WAN controller for instructions).

The SD-WAN controller creates the forward decision upon global network vision and pushes it to the vEdge router. Then, the vEdge router can process all packets into the flow based on the decision [3]. Figure 5 explains, in detail, the sequence of operations in the router [3] as follows:

- ***IP Destination Lookup*** The main function of the routers in the data layer is to route data based on the decisions of the controller in the control layer, so the data forwarding process starts with the IP destination lookup step.
- ***Ingress Interface (access control list [ACL])*** Localised policies are usually utilised to make ACLs and attach them to vEdge router interfaces. These policies are used for filtering, marking, and traffic policing.
- ***Application-Aware Routing*** It means it makes a routing decision based on the specified service level agreement characteristics such as packet loss, latency, jitter, load, cost, and bandwidth of a transporter.
- ***Centralised Data Policy*** The centralised data policy is estimated after the previous step and is able to override the AAR forwarding process.

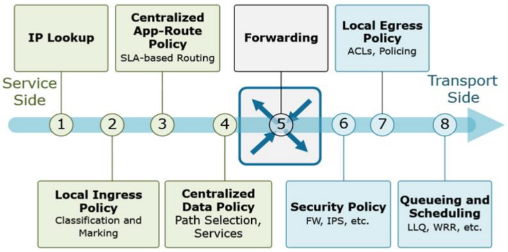

FIGURE 5 vEdge router operations

- ***Forwarding*** In this step, the destination IP is matched with the routing table, and the output interface is determined.
- ***Security Policy*** If there are security services attached to the WAN edge node, they are processed in the following sequence: Firewall, intrusion prevention system, URL-Filtering, and Advanced Malware Protection. The necessary tunnel encapsulations are performed and virtual private network (VPN) labels are inserted.
- ***Egress Interface ACL*** Local policy creates ACLs and applies on egress as well. If the egress ACL reject or manipulate traffic, the modification will be done before the packet is forwarded
- ***Queueing and Scheduling*** Egress traffic queueing services such as Low-Latency queuing and Weighted Round Robin queueing are implemented before the packet leaves.

2.2 | Forwarding packets and behaviour traffic

Forwarding is the transferring of data packets between vEdge routers in the data plane. Once the control plane connections of the SD-WAN network are operating, the traffic streams are spontaneous over the Internet Protocol security (IPsec) channels between vEdge routers. Because the traffic is not sent to or over SD-WAN controller in the control plane, forwarding only passes between the vEdge routers as they send and receive traffic [3]. The routing protocols working in the control plane supply a vEdge router the best path to reach the network that is on the other vEdge router. Briefly, forwarding is carrying the packet, delivering it through the transport link to the remote network, and specifying the action that will take place on the packet [30]. To adjust the packet forwarding flow, a centralised or localised policy can be formulated and applied as shown in Figure 6.

The centralised policies modify the whole structure in a centralised and localised form and give the ability to only a certain device or site. In other words, centralised policy manages the routes over that traffic, which is routed through the network and permits or blocks traffic based on the address, port, and differentiated services code point (DSCP) fields in the packet's IP header. The localised policy controls the inflow of traffic inside and outside of vEdge router's interfaces, which provides features such as QoS and mirroring. In this model, a

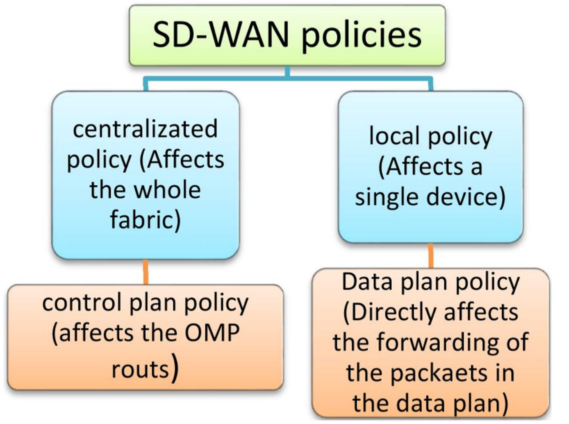

FIGURE 6 Software-defined-wide area network (SD-WAN) policies

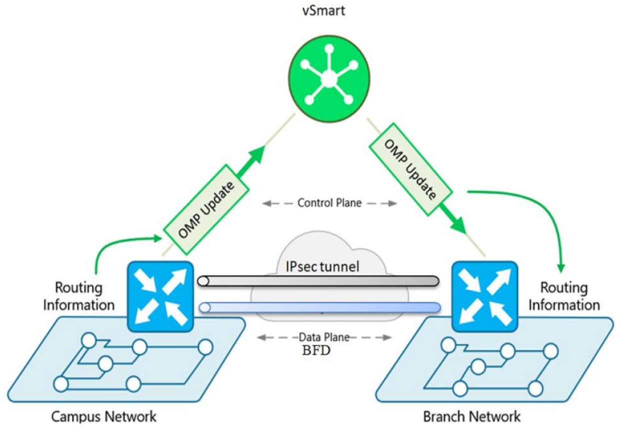

FIGURE 7 Software-defined-wide area network (SD-WAN) protocols

set of routing protocols as well as encrypted channels are used to ensure confidential data transmission as shown in Figure 7 and Table 1.

2.3 | New features of SD-WAN

As shown below, SD-WAN fabric consists of a collection of new features that can improve the quality of networks in business-critical applications.

2.3.1 | Application quality of experience (AppQoE)

In the present time, companies' works have become digital. This requires the provision of highly efficient applications to meet with this progress. Figure 8 shows some of the features and applications that motivate us to implement applications in institutions and companies [6].

SD-WAN solution has a collection of abilities that helps in the progress of the Application Quality of Experience (AppQoE) of applications. This collection contains many protocols

TABLE 1 SD-WAN Protocols and channels

SD-WAN protocols	
Protocol name	**Function**
Bi-directional forwarding detection (BFD)	Is used between vEdge routers in the data plane in order to check, to measure the performance of the transport links, and to give information about latency, jitter, and loss on all the transport channels.
Overlay management protocol (OMP)	Is the control plane protocol that runs between the WAN vEdge devices and the vSmart controllers inside a secured tunnel. It is also a full mesh peering between the controllers themselves.
Network configuration protocol (NETCONF)	Is the link between vManage controller, vSmart controller, and vEdge controller to communicate configuration, setting, and policies. NETCONF protocol can work in southbound and northbound interfaces.
SD-WAN channels	
Datagram transport layer security (TLS/DTLS)	Provides a secret channel between the data and control planes.
Internet protocol security (IPsec)	Provides a secret channel between the vEdge in data plane.

Abbreviations: BFD, Bi-directional forwarding detection; NETCONF, Network Configuration protocol; SD-WAN, Software defined-wide area network; WAN, wide area network.

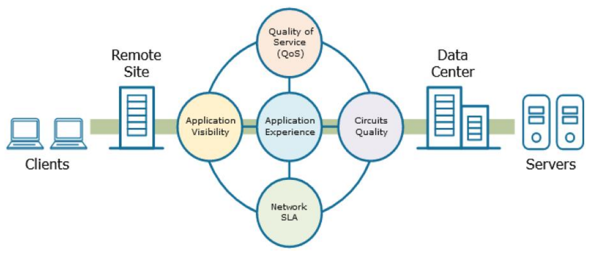

FIGURE 8 Software-defined-wide area network (SD-WAN) tools for improving application experience

that work side by side to improve the performance of applications such as:

A. Bidirectional Forwarding Detection (BFD)

The vEdge routers can use BFD mechanism to investigate and measure the performance of the communication links. Also, it locates the best performing path according to the result of the BFD statics, providing information around latency, jitter and loss on all the communication links [7].

B. Quality of Service (QoS)

Quality of Service is measuring total performance of a service, such as networks or a cloud service. Software-defined-wide area network solution establishes a transport-separate structure, taking advantage of tunnelling techniques such as IPsec that encapsulates and encrypts packets prior to their transmit through all available links on vEdge routers. vEdge routers can copy the DSCP value of the original IP packet into the outer IP header. Through it, particular applications can be scheduled into the correct QoS classes on the service provider side [7] as shown in Figure 9.

C. Forward Error Correction (FEC)

In the FEC feature, we put one parity packet for each group of four packets. In the received device, if one of the four packets is missing, it can be rebuilt according to the parity metadata [7] as shown in Figure 10.

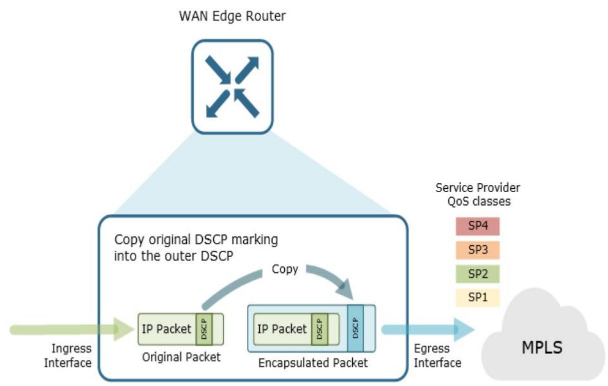

FIGURE 9 Mapping differentiated services code point (DSCP) to service provider classes

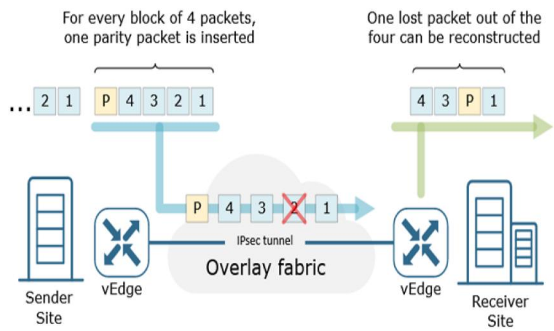

FIGURE 10 Forward error correction

D. Packet Duplication

As shown in Figure 11, packet duplication is utilised to raise application reliability. In a sending device, vEdge router transmits the same traffic stream over several WAN transports that transmit at minimum two copies of each packet. At the receiving device, the vEdge router can recompense for missing

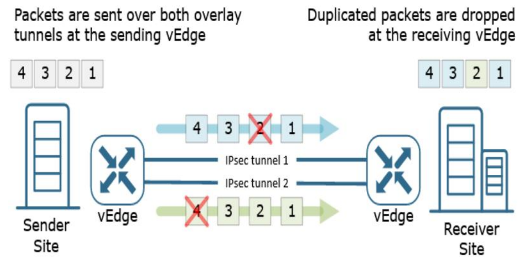

FIGURE 11 Packet duplication

packets by using many copies of the same flow and rejecting unwanted duplicates [30].

E. Fragmentation Avoidance

The SD-WAN consists of many vEdge routers that are connected via several different technologies such as Synchronous Digital Hierarchy, digital subscriber line, Ethernet, LTE and satellite links. Each transport link has a different maximum transmission unit (MTU) value. The tunnelling and IPsec can significantly lower the MTU [30]. Fragmentation fractures bigger packets into segments that can be reassembled later on. It is not recommended to use it because it causes adding latency and jitter in the packet flow. In SD-WAN, the solution is to delete this option by configuring a DF (do-not-fragment) flag in the IP header. The software-defined-wide area network proactively detects the path MTU over the structure and reports on the available MTU as in Figure 12.

F. Software-Defined Application Visibility and Control (SD-AVC)

Software-Defined Application Visibility and Control is used to identify, aggregate, and transfer application data well-arranged to create decisions such as prioritising app traffic using QoS as shown in Figure 13.

G. Application-aware routing (AAR)

Application-aware routing (AAR) is an advantage that can choose the best route for a business-critical application based on a pre-defined policy as shown in Figure 14.

H. Transmission Control Protocol (TCP) Flow Optimisation

The SD-WAN TCP Optimisation feature disconnects TCP communications topically at the vEdge routers and uses TCP Selective Acknowledgement to the best, control the TCP-Window-Size and maximise the throughput through the WAN transports as shown in Figure 15.

2.3.2 | Interconnecting multiple clouds

As shown in Figure 16, some companies end up with a multi-cloud operation just naturally. This typically happens when

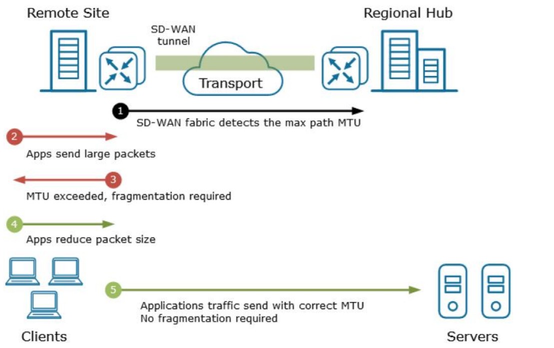

FIGURE 12 Software-defined-wide area network (SD-WAN) path maximum transmission unit (MTU) discovery process

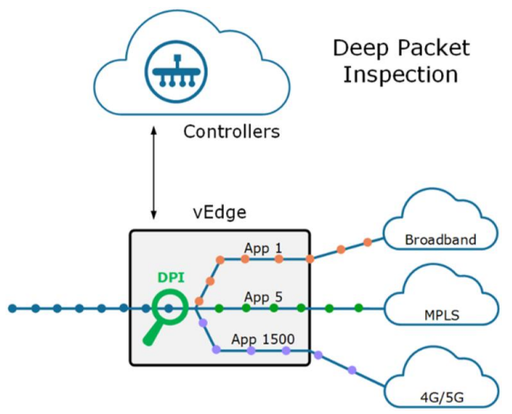

FIGURE 13 vEdge router packet inspection

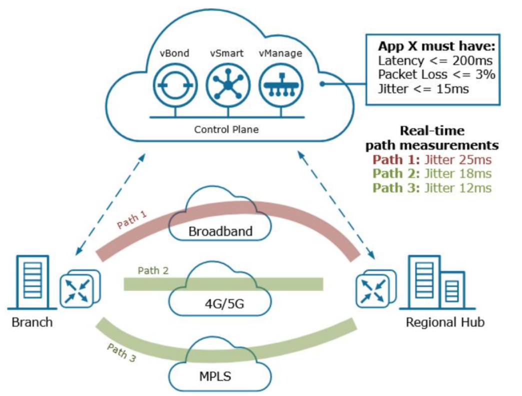

FIGURE 14 Software-defined-wide area network (SD-WAN) application-aware routing (AAR)

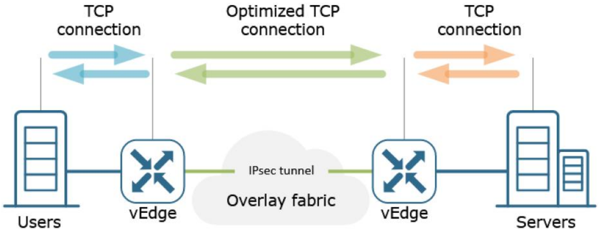

FIGURE 15 Software-defined-wide area network (SD-WAN) Transmission Control Protocol (TCP) optimisation

some departments move workloads into one cloud provider and other departments migrate other apps to a different provider.

Software-defined-wide area network can deploy the enterprise's WAN to the public cloud, in order to link all sites to each cloud in a secure and automated mode [7] as shown in Figure 17.

2.3.3 | Direct internet access (DIA)

As shown in Figure 18 and Figure 19, SD-WAN direct internet access (DIA) is a service that can improve clients' experiment for SaaS applications at far branches by eliminating the performance retrogressions related to backhauling Internet traffic to central data centres [7].

Also, the DIA feature permits forwarding the traffic over a cloud security provider. In this case, the traffic from a special remote branch is forwarded to the cloud security provider through point-to-point IPsec tunnels. The cloud security provider then pushes the traffic through pre-defined security policies and route it out to the Internet as shown in Figure 20.

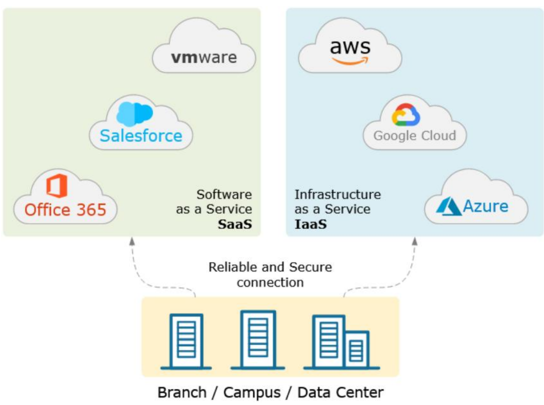

FIGURE 16 Enterprise cloud services

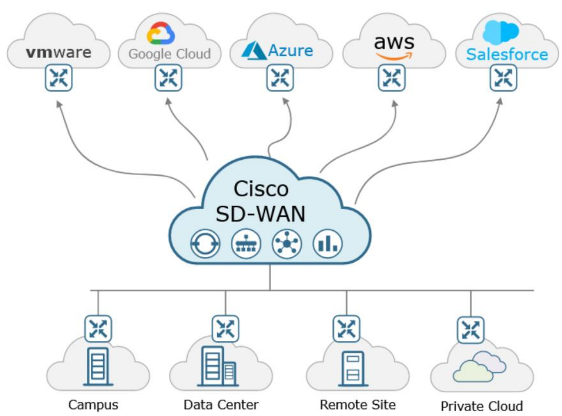

FIGURE 17 Software-defined-wide area network (SD-WAN) as multi-cloud interconnect

2.3.4 | Virtual routing and forwarding (VRF) and virtual private network (VPN)

The original data packet is encapsulated with IPsec, providing encryption and authentication. Figure 21 depicts the SD-WAN header representation [7].

In traditional networking, the most rudimentary forms of network segmentation are Virtual Local Area Networks (VLANs) at layer 2 and virtual routing and forwarding (VRFs) at layer 3. However, these technologies are limited in scope because they are implemented in a locally significant fashion (on a single device per interface) or require complex control plane interactions to work (for example, MPLS-based Border Gateway Protocol L3VPNs). Our SD-WAN design uses a simpler but more scalable approach to network segmentation using two very efficient techniques [7]:

- ➢ Enforcing segmentation at the edges on WAN edge routers.
- ➢ Carrying the segmentation information in the data plane packets by inserting VPN labels that identify the network segment.

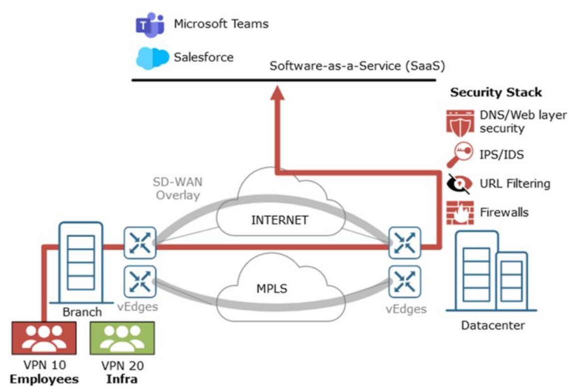

FIGURE 18 Backhauling internet traffic through a data centre

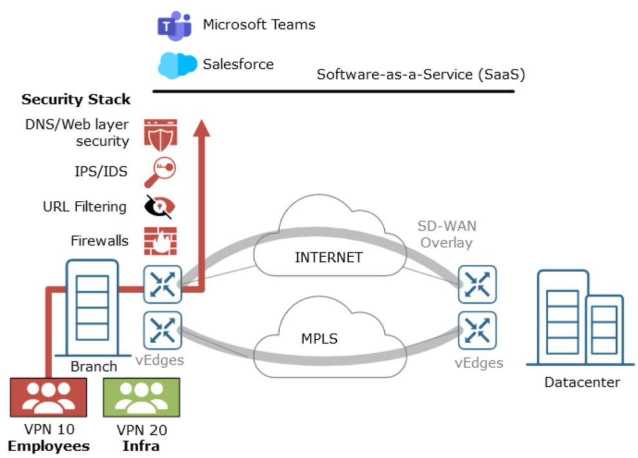

FIGURE 19 Software-defined-wide area network (SD-WAN) direct internet access

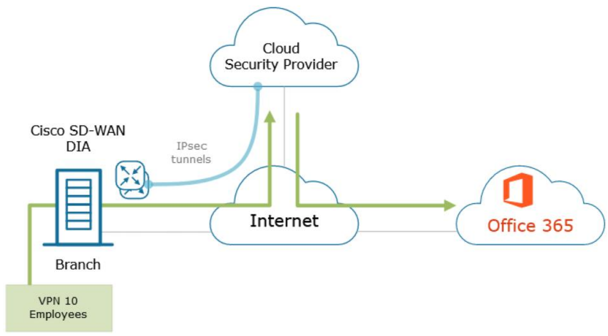

FIGURE 20 Direct internet access (DIA) traffic through a cloud service provider

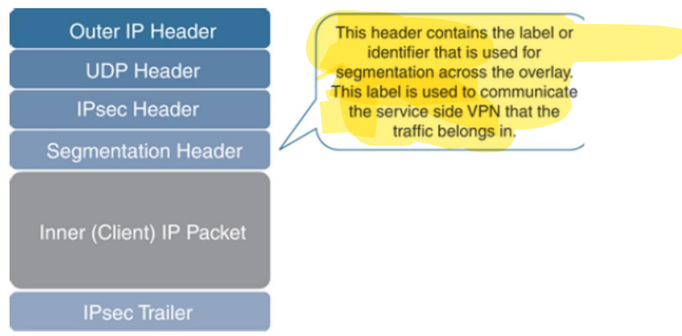

FIGURE 21 Software-defined-wide area network (SD-WAN) packet format

In our SD-WAN solution, the VPN is synonymous with VRF instances from a generic routing perspective. VRFs and VPNs provide a method to separate the control and data plane into different logical parts. Segmentation in the data plane is accomplished by building multiple, isolated routing table instances and binding specific interfaces to those instances. The SD-WAN solution can support diverse topologies unique to each VPN segment or data plane instantiation. Each of these VPN segments is completely isolated from communicating with each other unless the policy allows it. These VPNs are carried in a single IPsec tunnel. According to the structure of the vEdge router shown in Figure (21), the SD-WAN VPNs are divided into many types, the most important of which are as follows:

1. Pre-defined VPNs

As shown in Figure 22 by default, the SD-WAN solution has two pre-defined VPNs that cannot be deleted or modified: Transport VPN 0 and Management VPN 512.

➢ Transport VPN 0

Virtual private network 0 is the pre-defined Transport VPN of the SD-WAN solution. It cannot be deleted or modified [7]. The purpose of this VPN is to enforce a separation between the WAN transport networks (the underlay) and network services (the overlay). Therefore, all WAN links such as Internet and MPLS circuits are kept in VPN 0 as is visualised in Figure 23.

Additionally, vEdge routers must have at least one interface configured in VPN 0 in order to establish the control plane tunnels to vSmart controllers. Each interface that is connected to the WAN must have an IP address, colour, and encapsulation type configured. These parameters are then advertised to the controllers via OMP as part of the Transport Locator route advertisements. Typically, a default route is defined via each WAN interface [7].

2. Management VPN 512

By default, in SD-WAN, VPN 512 is configured for out-of-band management. It is enabled and ready to go out of the box.

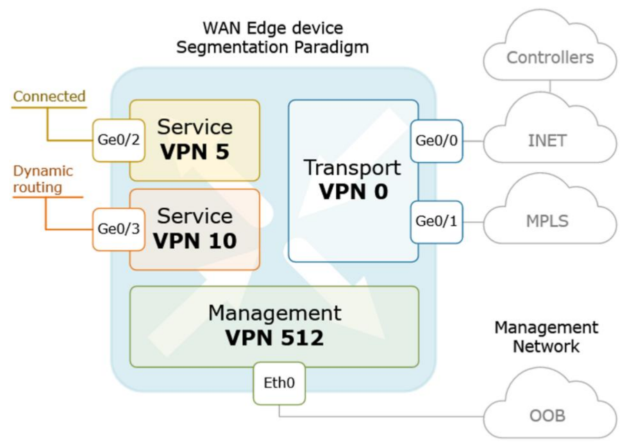

FIGURE 22 vEdge router segmentation

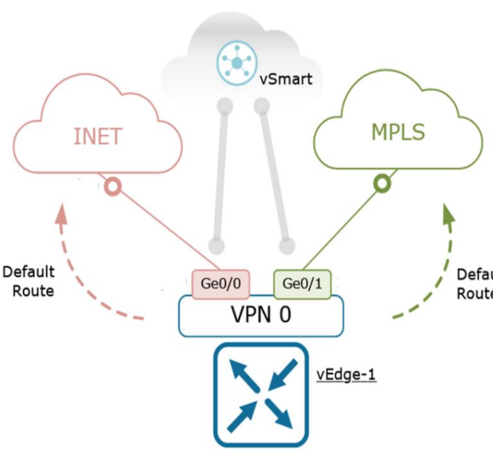

FIGURE 23 Software-defined-wide area network (SD-WAN) transport virtual private network (VPN) 0

3. Service VPNs

As shown in Figure 24, when we want to create an isolated network domain and isolate the data traffic in this domain from the other user networks onsite, we create a new service VPN on the vEdge routers. This VPN is specified by a number different from 0 (Transport) and 512 (Management). Once the

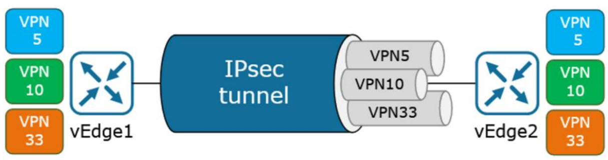

FIGURE 24 Software defined-wide area network (SD-WAN) virtual private networks (VPNs)

network segment is created, you associate interfaces, enable routing protocols, and other network services such as Virtual Router Redundancy Protocol and QoS within this VPN. One important thing to point out is that interfaces associated with user segments must not be connected to WAN transports [30].

As shown in Figure 25, each interface on a vEdge device must be configured in a particular VPN. All prefixes learnt via interfaces or routing instances in a VPN are kept in a separate routing table. When this network information is advertised to the vSmart controller, each prefix is associated with a VPN-ID. In addition, the vSmart controller maintains the VPN context of each prefix [7].

Therefore, separate route tables provide network segmentation on a single device. However, the question is how to populate this isolated routing information across the overlay domain. At the packet forwarding level, WAN edge routers will insert a new VPN label field in each IP packet. This label will identify the network segments that the packets belong to. The process is visualised in Figure 4. When we configure a new VPN on a vEdge router, it will associate a label to it. The WAN Edge device will then advertise this label along with the VPN-ID to the vSmart controller via OMP. The controller itself will then redistribute this VPN-ID mapping to other vEdge routers in the network. The remote vEdge routers in the network will then use these labels to send traffic to the appropriate VPNs, similarly to label switching in MPLS. Because the control plane is completely separated from the data forwarding plane, the SD-WAN allows us to define different topologies per VPN. As shown in Figure 26, typical topology types are full-mesh, partial-mesh, hub-and-spoke, and point-to-point.

Software defined-wide area network topologies are important because some applications may benefit from going via the shortest possible path, for example, VoIP works best in full-mesh topologies. On the other hand, some segments of the network might benefit from controlled connectivity topology such as hub-and-spoke [7].

2.3.5 | SD-WAN and cloud

- ➢ Software-as-a-Service (SaaS) As shown in Figure 27, SaaS application is simply an enterprise-degree business application, which is usually utilised through the Internet [7]. The most common SaaS applications in these days are Microsoft Office 365, Google Workplace, and Salesforce. The work requirements are to make sure that these SaaS applications are available 24/7 but it cannot be achieved

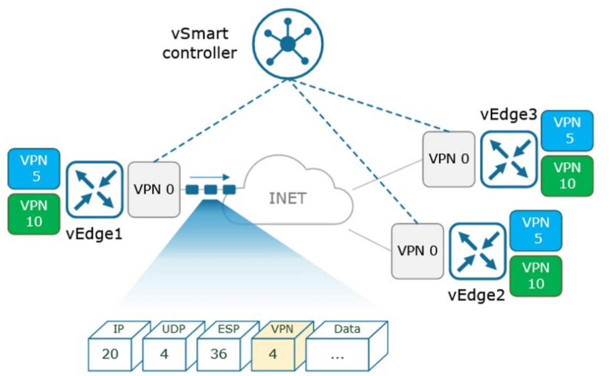

FIGURE 25 Software-defined-wide area network (SD-WAN) virtual private network (VPN) labels

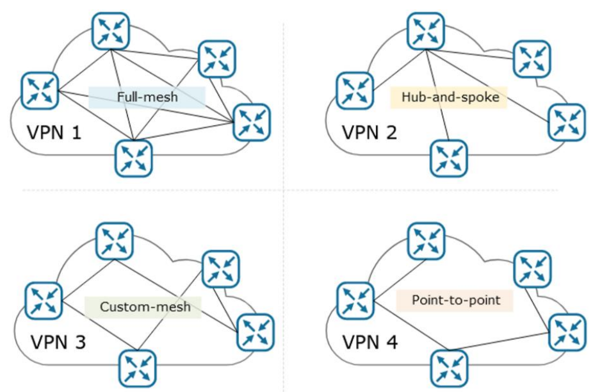

FIGURE 26 Software-defined-wide area network (SD-WAN) arbitrary topologies

with the traditional WAN path of traffic through MPLS circuits to the data centre. Because this paradigm is costly, high delay causes a bandwidth bottleneck at the data centre WAN links. This leads to main problems related to single-point-of-failures, complexity [30]. Briefly, SaaS uses real-time, accurate analytics for each application to direct clients to the best-performing route for optimal application performance.

- ➢ Infrastructure as a Service (IaaS)

Infrastructure as a Service is a virtualised computing infrastructure, provisioned and managed through the Internet and it is used to host and deliver enterprise applications. Infrastructure as a Service has several advantages compared to the on-premise data centre infrastructure such as:

- ➢ It can expand and shrink according to business requirements.
- ➢ It significantly decreases the time to market.
- ➢ It reduces capital expenses and ongoing costs.
- ➢ It has the best security on-premise.

The common IaaS providers are AWS, Microsoft Azure, and Google Cloud (GCP). Each cloud provider has various connectivity and provisioning models. One of the most famous

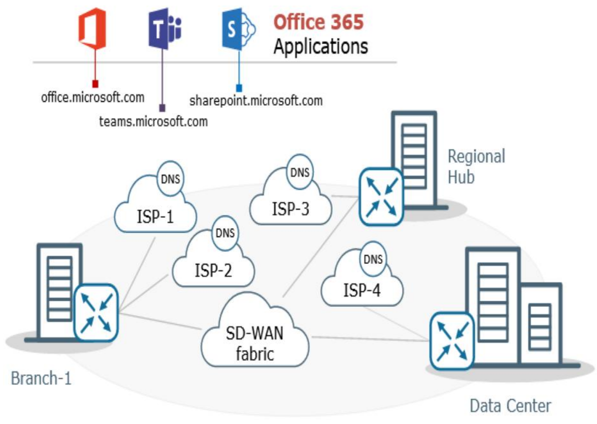

FIGURE 27 Cloud for SaaS topology

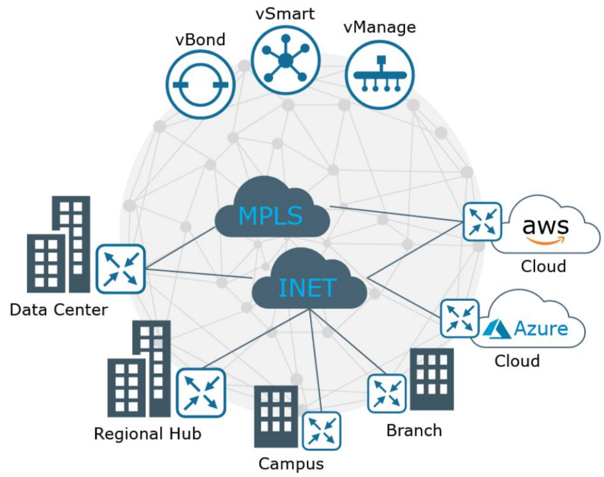

FIGURE 28 Cloud for infrastructure as a service (IaaS)

IaaS is the Cloud onRamp owned by Cisco [3] as shown in Figure 28:

Cloud can be known as collection of capabilities that expand the SD-WAN overlay structure to a public cloud paradigm. This design permits far sites, campuses, and data centres inside the SD-WAN overlay structure to benefit by advantages such as AAR to select the best path to install the applications hosted inside a public cloud provider such as AWS, Azure, or GCP.

3 | MATHEMATICAL ANALYSIS OF QUEUEING MODEL

The main element of the SD-WAN network is a vSmart controller which provides the control information to vEdge router in branches. Packets arrive from vEdge router to SD-WAN controller at the system to be served. When the controller is idle, a packet is served immediately. Otherwise, an arriving packet joins waiting in queues. If the vSmart controller completes serving a packet, the item departs. When there are packets waiting in the queue, one is soon dispatched to the vSmart controller [17].

3.1 | Queueing model of SD-WAN controller

The data in the network is transmitted as a series of packet flows in network traffic. In SD-WAN deployments, a centralised controller is responsible for several of the vEdge routers and receives a flow of packets from each of them. As mentioned earlier, the vEdge router will send packets to the SD-WAN controller for each new stream. Finally, the SD-WAN controller sends down the response to all vEdge routers over the flow path. Conforming with analysis, it may be described as the packet processing of the SD-WAN controller of the queueing model M/M/1 with these assumptions:

a. Arrival process at the SD-WAN controller as a Poisson flow with the arrival rate λ.
b. The service of the SD-WAN controller subjects to the service rate μ.
c. The packet processing time of SD-WAN controller adjusts to exponential distribution.

In line with queueing theory, it may be realised that the average waiting time of a packet in the SD-WAN controller is as follows:

$$\overline{W}_{(c)}(k) = \int_0^\infty t w_{(c)} dt = \frac{p_0 \rho_1^k}{\mu_c k \cdot k! \left(1 - \rho_{(c)}\right)^2} + \frac{1}{\mu_c} \tag{1}$$

where $\rho_1 = \frac{\lambda_{(1)}}{\mu_{(1)}}$, $\rho_{(c)} = \frac{\lambda_{(c)}}{n\mu_{(c)}} < 1, p_{(0)}$ in (2):

$$p_{(0)} = 1 - \rho_{(c)} = 1 - p_{(k)} = \left(\sum_{i=0}^{k-1} \frac{\rho_1^i}{i!} + \frac{\rho_1^k}{k!} \frac{1}{1 - \rho_{(c)}} \right)^{-1} \tag{2}$$

where p_k denotes stationary probability $p_k = (1 - \rho)\rho^k$ and utilisation $\rho = \lambda/\mu$.

3.2 | Queueing model of vEdge router

All packets sent from the SD-WAN controller to the vEdge routers are represented by queueing service packets with probability α. A packet can receive service at rate μ_1, and the probability $(1-\alpha)$ receives service at rateμ_2. The services provided by the SD-WAN controller may be initial connection, Zero-Touch Provisioning, configuration phase and flows, and packets sent by the vEdge router are forwarded in the form of arrival queueing packets. The $M/H_2/1$ queue model is used and this means that the arrival process consists of one phase. This follows a Poisson law at rate λ, whereas packets may not match any flow entries. In this case, the vEdge router will send a packet into the SD-WAN controller to take the appropriate action or the vEdge router will be asked for configurations from the SD-WAN controller. The action may be for providing the vEdge router with the required configurations, drop packet, forward packet to SD-WAN controller, and sending an update of routing table to vEdge router or forwarding packet to the specified destination port. Assume that all packets take their service and come out based on *the FIFO* principle. Network Configuration Protocol and OMP will be used to communicate between the control and data planes in the Southbound Interface of SD-WAN, where they provide mechanisms to install, to manipulate, to perform traffic forwarding and to delete the configuration of network devices. It also reduces the given time to the management of network device configuration. Figure 29 shows messages exchanged between the SD-WAN controller and vEdge router.

In line with the above, the arrival process is generated upon a *Poisson distribution* at rate λ, while the service process is represented by a two-phase *hyper-exponential distribution* with service rate μ_i and α_i as shown in the following Figure 30.

As has been previously indicated, Figure 5 demonstrates packet forwarding of a vEdge router. The vEdge router caches arrival packet in the input queue and transmits it one by one to the input port. In detail, the vEdge router parses all packets to extract its destination IP fields. Then the destination IP is used for looking up in the routing tables to match an entry. When the lookup fails, the vEdge router sends a request including packet information to its SD-WAN controller and waits for a response from the controller. If detention IP is matched, the packet is moved to the output port after applying ingress ACL. Finally, the packet is put into the egress queue to wait for transmitting [31]. The packet forwarding of the *ith* vEdge router can be described as the queueing model M/M/1 upon these assumptions:

- Packet arrives at the *ith* vEdge router as Poisson distribution with the rate λ_i
- Packet routing time of the i^{th}vEdge router conforms with a hyper-exponential distribution with the rate μ_i in (3) and the variance $\sigma(s)^2$ in (4), where the μ_i represents the rate of the *jth* step in the i^{th}switch and s denotes steps of packet routing in vEdge router.

$$\mu_i = \frac{1}{\sum_{j=1}^{s} \frac{1}{\mu_i}} \tag{3}$$

$$\sigma(s)^2 = \sum_{j=1}^{s} \frac{1}{\mu_i^2} \tag{4}$$

According to Little's law in (5), it is possible to obtain the average waiting time of packets W_q [22] in the *j*th vEdge router as follows:

$$L_q = \lambda W_q \tag{5}$$

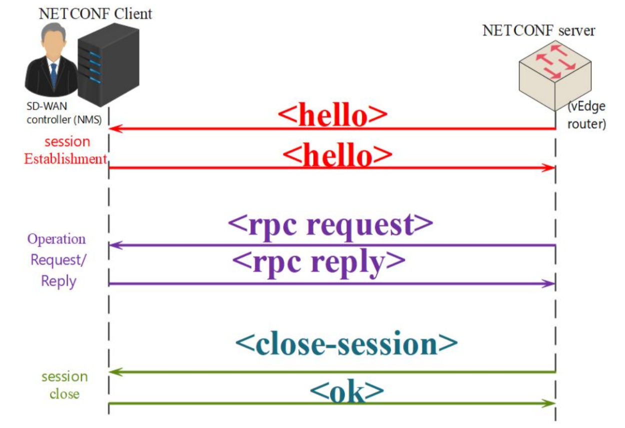

FIGURE 29 Messages between software-defined-wide area network (SD-WAN) controller system and vEdge router

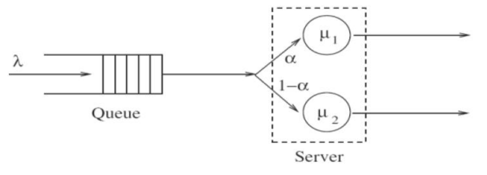

FIGURE 30 Queueing model of vEdge router

$$W_q = \frac{L_q}{\lambda} = \frac{\lambda}{\mu(\mu-\lambda)} = \frac{\rho}{\mu-\lambda} \tag{6}$$

where L_q denotes Mean Queue Length and $\rho = \lambda/\mu$ is the point utilisation system.

The *service process* will be subject to hyper-exponential disruption law and denoted by X (.) on [∞, 0); as its representation is (γ, S) in which γ is a raw vector dimension that denotes initial probability and S is a square matrix that denotes service process, the transition rate matrix of service processes is as follows:

$$S' = \begin{pmatrix} -\mu_1 & \mu_1 & 0 \\ 0 & -\mu_2 & \mu_2 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} S & S^0 \\ 0 & 0 \end{pmatrix},$$ and the initial probability distribution γ is given as $(\alpha(1-\alpha)0) = (\gamma\ 0)$. The probability density function of the service process is given as

$$f_X(x) = \alpha_1\mu_1 e^{-\mu_1 x} + \alpha_2\mu_2 e^{-\mu_2 x}, x \geq 0 \tag{7}$$

While the cumulative distribution function is

$$F_X(x) = \alpha_1(1-e^{-\mu_1 x}) + \alpha_2(1-e^{-\mu_2 x}) \tag{8}$$

3.2.1 | Analysis of queueing model of vEdge router

According to the above, $M/H_2/1$ queueing systems can be solved by Quasi-birth–death as the following [22]:

I. Construct the block sub-matrices as it was mentioned in section 2, arrival packets consist of one phase while the service process has two phases. The Q generator matrix can be associated with $M/H_2/1$ queue by $\pi Q = 0$ [32], and the transition matrix is given as

$$Q = \begin{bmatrix} B_{00} & B_{01} & 0 & 0 & \dots & 0 \\ B_{10} & A_1 & A_2 & 0 & \vdots & 0 \\ 0 & A_0 & A_1 & A_2 & \cdots & 0 \\ 0 & 0 & A_0 & A_1 & A_2 & \vdots \\ 0 & \vdots & \ddots & \ddots & A_1 & 0 \\ 0 & 0 & \vdots & \vdots & \vdots & 0 \end{bmatrix}$$

Where π is the steady state distribution, B_{00}, B_{01}, and B_{10}, denote initial conditions, A_0 represents service completions at the rate of $\alpha_i\mu_i$, A_2 represents arrival completions at the rate of λ, and A_1 super-diagonal elements represented service completions at a rate of $(\lambda+\mu_i)$. The transition rate matrix for the $M/H_2/1$ model is given as

$$\mathbf{Q}= \left[\begin{array}{c|cc|cc|cc|c} -\lambda & \alpha\lambda & (1-\alpha)\lambda & 0 & 0 & 0 & 0 & \cdots \\ \hline \mu_1 & -(\lambda+\mu_1) & 0 & \lambda & 0 & 0 & 0 & \cdots \\ \mu_2 & 0 & -(\lambda+\mu_2) & 0 & \lambda & 0 & 0 & \cdots \\ \hline 0 & \alpha\mu_1 & (1-\alpha)\mu_1 & -(\lambda+\mu_1) & 0 & \lambda & 0 & \cdots \\ 0 & \alpha\mu_2 & (1-\alpha)\mu_2 & 0 & -(\lambda+\mu_2) & 0 & \lambda & \cdots \\ \hline 0 & 0 & 0 & \alpha\mu_1 & (1-\alpha)\mu_1 & -(\lambda+\mu_1) & 0 & \cdots \\ 0 & 0 & 0 & \alpha\mu_2 & (1-\alpha)\mu_2 & 0 & -(\lambda+\mu_2) & \cdots \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots \end{array}\right]$$

where

$$A_0 = \begin{pmatrix} \alpha\mu_1 & (1-\alpha)\mu_1 \\ \alpha\mu_2 & (1-\alpha)\mu_2 \end{pmatrix}, A_1 = \begin{pmatrix} -(\lambda+\mu_1) & 0 \\ 0 & (\lambda+\mu_2) \end{pmatrix},$$

$$A_2 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, B_{00} = (-\lambda), B_{01} = (\alpha\lambda(1-\alpha)\lambda),$$

$$B_{10} = \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix}$$

The transition rate diagram for the $M/H_2/1$ queue is illustrated in Figure 31:

II Form Neuts' R matrix: To find the Neuts' R matrix, $\pi Q = 0$ is applied and it solves the following equations as illustrated:

$$R = -A_2 A_1{}^{-1} - R^2 A_0 A_1{}^{-1} = -V - R^2 W \tag{9}$$

where $V = A_2 A_1{}^{-1}$ and $W = A_0 A_1^{-1}$. This means that the successive substitution procedure proposed by Neuts, Let, $R_0 = 0$, $R_{k+1} = -V - R_k{}^2 - W$, $k = 1, 2, 3, \ldots$

III Solve the boundary equations as shown:

$$(\pi_0 \quad \pi_1)\begin{pmatrix} B_{00} & B_{01} \\ B_{10} & A_1 + RA_0 \end{pmatrix} = (0, 0)$$

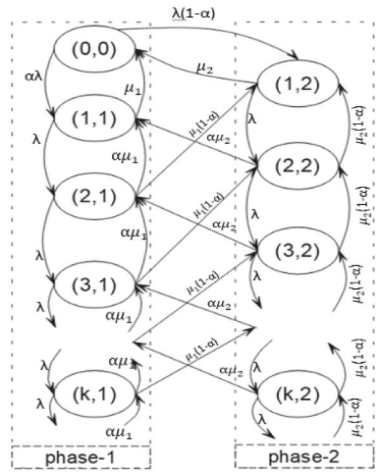

FIGURE 31 Transition diagram for the $M/H_2/1$ queue

where $\pi_i = \pi_1 R^{i-1}$, $i = 2,3,\ldots$ to obtain a unique solution, being set $\pi_0 = 1$ given as follows:

$$1 = \sum_{i=0}^{\infty} \pi_i u = \pi_0 u + \sum_{i=1}^{\infty} \pi_1 R^{i-1} u = \pi_0 u + \sum_{i=0}^{\infty} \pi_1 R^i u = \pi_0 u + \pi_1 (I - R)^{-1} u \tag{10}$$

IV Generate successive components of the solution by using the MATLAB package as shown in Ref. [22] to find sub-blocks of the stationary probability vector.

4 | PERFORMANCE MEASUREMENT

From the previous conclusions, the proposed queue model is stable; the number of packets does not increase indefinitely—as the mean arrival rate λ is less than the mean service rate μ. This means that the SD-WAN system is stable [33] when arrival rate is less than the service rate based on the system utilisation factor that should not be less than one: $\rho < 1$, where: $\rho = \lambda / C\mu = 0.030006 = 3\%$, λ denotes the arrival rate, and C is the number of the server and μ is the service rate [34]. A queueing system can be analysed for the purpose of studying the behaviour of the system and make the most of its resources. There are many parameters that affect the system performance:

4.1 | Waiting time or delay

Delay is one major performance measurement in telecommunication networks. In computer network, the delay is the time a packet waits in a queue until it is served. The waiting time of packets in queue SD-WAN system can be calculated as shown:

a. Let stationary probability vector πbe given by the equation (11):

$$\pi = (\pi_0, \pi_1, \pi_2, \ldots, \pi_k) \tag{11}$$

$$\rho = \frac{\lambda}{\mu} < 1 \tag{12}$$

$$\pi_0 = 1 - \rho \tag{13}$$

$$\pi_k = (1-\rho)\rho^k \tag{14}$$

where π_k is the probability of k packets in the ith vEdge router.

$$\begin{aligned} L &= \sum_{k=0}^{\infty} k\,\pi_k = \sum_{k=0}^{\infty} k(1-\rho)\rho^k \\ &= (1-\rho)\sum_{k=0}^{\infty} \mathrm{k}\,\rho^k = (1-\rho)\ \rho^k \sum_{k=0}^{\infty} \mathrm{k}\,\rho^{k-1} \end{aligned} \tag{15}$$

b. The mean number of packets in the queueing system can be computed as given in equation (15):

Assuming that the system is stable, then $\varrho < 1$.

$$\sum_{k=0}^{\infty} k\rho^{k-1} = \frac{\partial}{\partial\rho}\left[\sum_{k=0}^{\infty}\rho^k\right] = \frac{\partial}{\partial\rho}\left[\frac{1}{1-\rho}\right] = \frac{1}{(1-\rho)^2} \tag{16}$$

From (17) the mean number of packets in the SD-WAN system can be obtained as follows:

$$L = (1-\rho)\frac{\rho}{(1-\rho)^2} = \frac{\rho}{1-\rho} = \frac{\lambda}{\mu-\lambda} \tag{17}$$

c. The Mean Queue Length L_q can be defined as the number of packets waiting [22] in the arrival queue and it is given as follows:

$$\mathrm{L_q} = \sum_{\mathrm{k}=1}^{\infty} \mathrm{k}\ \pi_{\mathrm{k}} - \sum_{\mathrm{k}=1}^{\infty} \pi_{\mathrm{k}} = \frac{\rho}{1-\rho} - \rho = \frac{\rho^2}{1-\rho} = \rho\,\mathrm{L} \tag{18}$$

Thus

$$\mathrm{L_q} = \rho\,\mathrm{L} = \mathrm{L} - \rho \tag{19}$$

d. Finally, the average Waiting Time W_q can be computed based on Little's law in equation (5) as follows:

$$W_q = \frac{L_q}{\lambda} = \frac{\lambda}{\mu(\mu-\lambda)} = \frac{\rho}{\mu-\rho} \tag{20}$$

4.2 | Sojourn time or response time

Sojourn time is the full time it takes to react to a request for service. If the sending time is ignored, the sojourn time is the total of the service time and wait time. Service time is the time taken to complete a required work or service [16]. The wait time is how much time the packet has to wait in an arrival queue before being serviced. In other words, sojourn time is the time that a packet spends in the system from the moment of its arrival queue to the moment of its leave from the controller, also known as response time [22]. It can be evaluating the response time as follows:

$$\mathrm{T} = \frac{\mathrm{L}}{\lambda} = \frac{1}{\mu(1-\rho)} \tag{21}$$

4.3 | Traffic intensity (utilisation ρ)

The utilisation ρ is known as the part of time that the SD-WAN controller is busy [17]. In this paper, λ can point to the arrival rate of packets and μ is the service rate; thus, the utilisation ϱ is equal to λ/μ.

$$\rho = \frac{\text{arrival rate}}{\text{service rate}} = \frac{\lambda}{\mu} \tag{22}$$

If there are many controllers, then

$$\rho = \frac{\text{arrival rate}}{\text{number of controller} \times \text{service rate}} = \frac{\lambda}{C\mu} \tag{23}$$

4.4 | SD-WAN system throughput

The throughput of SD-WAN system is equivalent to its leaving rate; it defines the average number of packets processed per unit time. If all packets arriving can be served and depart from the system, then the throughput equals the arrival rate. The throughput is given by:

$X = \lambda$ if system has one controller; otherwise, $X = \mathrm{C}h$.

Performance measurement [22] of the proposed $M/H_2/1$ queueing system is shown in [16] Table 2.

5 | EMULATION AND SIMULATION

In our previous research work [15], similar experiments were carried out but phase type distribution can be used for the arrival rate of packets from the vEdge router to the SD-WAN controller system; while in the present work, it is assumed that the arrival rate is Poisson distribution. The size of the message used in both scenarios must be constant and the service time at the server ought to be exponential

TABLE 2 Performance measurement of software-defined-wide area network (SD-WAN) system

Property	Equation	Value
Check the stability of system by utilisation Factor (ϱ)	Condition $\rho = \frac{mean\ \lambda}{mean\ \mu} = 0.030006 < 1$, system is stable	System is stable
Queue notation	$M/H_2/1$	
The average response time or sojourn time	$T = L/\lambda$	$T = 0.030852$ (ms)
Throughput	$X^{`} = C$ (number of server)$\times\mu \times \rho$	$X^{`} = 3.52$ pps
Average queueing time W_q	$W_q = L_q/\lambda = \lambda/\mu(\mu{-}\lambda) = \rho/\mu{-}\lambda$	$W_q = 2.5498 \times 10^{-5}$

distribution, where models ph/ph/C and $M/H_2/C$ were applied to a proposed SD-WAN network. The result of both studies has the same asymptotic shape [17]. Also, as shown in Figure 32, a simulation of the proposed model was made using Java Modelling Tools to solve the system in order to test the stability of the system and study the parameters affecting the performance of the system.

In addition, network emulation was done using emulated virtual environment-next generation (EVE-NG) as shown in Figure 33. The purpose of this emulation is to help develop proficiency in deploying, managing and monitoring the SD-WAN solution. The emulation steps are as follows:

i. https://www.eve-ng.net/ → EVE-NG is the virtualisation platform where you create and run virtual machines and virtual appliances.
ii. www.cisco.com → Cisco SD-WAN Images → Select a Software Type: [vEDGE Router, vManage Software, vSmart Software].
iii. Deployment of virtual software as shown in Table 3
iv. Deployment of vManage at Management plane, vBond controller at Orchestration Plane, vSmart controller at the control plane, and vEdge in data planes as the following:
   - Deploy the virtual machine for the controller.
   - Bootstrap and configure the controller
   - Manually install the root certification authority certificate on the controller.
   - Add the controller to manage.
   - Generate, sign, and install the certificate onto the controller.
v. Deployment of vEdge router (data plane)

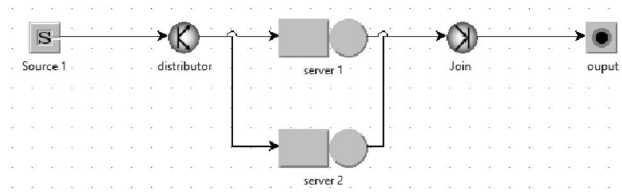

FIGURE 32 Simulation of software-defined-wide area network (SD-WAN) system by java modelling tools (JMT)

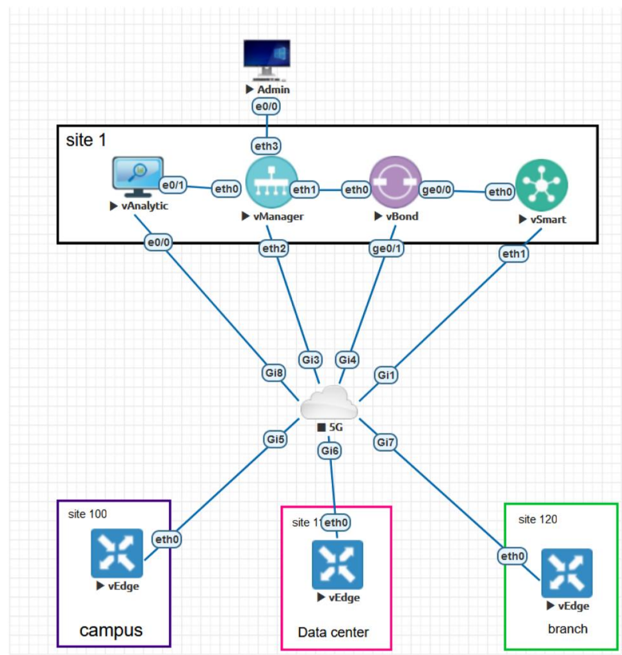

FIGURE 33 Emulation of software-defined-wide area network (SD-WAN) topology

6 | PERFORMANCE MEASUREMENT RESULTS

- Utilization ρ

In Ref. [15] shows the utilisation for the phase type distribution arrival rate. As can be seen, the utilisation for Ref. [15] is $5.7191 \times 10^{-4} = 0.057\%$, while average utilisation in this paper for Poisson distribution arrival rate is $0.03 = 3\%$. According to Table 2 and Figure 34, Poisson distribution had a higher utilisation compared to phase type distribution.

- Throughput

Also, Ref. [15] shows that the throughput for the phase type distribution arrival rate is 41.8638 pps when 5.7191×10^{-4} Also, Figure 35 indicates that this is different for Poisson distribution arrival rate where the average throughput is 1.4998 pps, and phase type distribution had a higher throughput compared to Poisson.

TABLE 3 Software-defined-wide area network (SD-WAN) image

Virtual machine	RAM	HDD	vCPU	Description
vManage controller	64 GB	1 TB	1	Management plane
vSmart controller	64 GB	1 TB	1	Control plane
vDatabase-redundancy	64 GB	2 TB	1	Management plane
vBond controller	64 GB	1 TB	1	Orchestration plane
vAnalytics controller	64 GB	1 TB	1	Management plane
vEdge router	4 GB each one	4 GB	3	Data plane

Abbreviation: HDD, Hard disk drive.

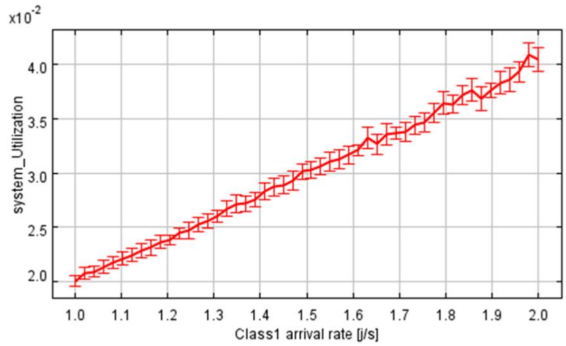

FIGURE 34 Average utilisation for Poisson distribution

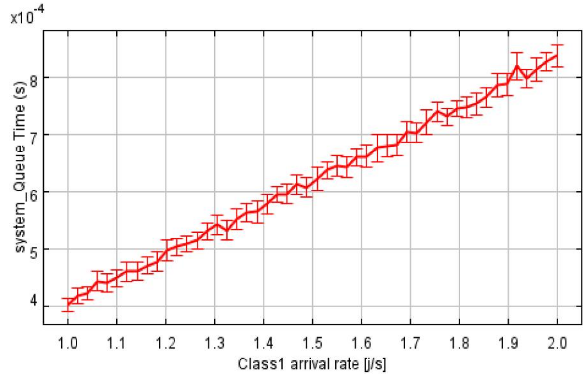

FIGURE 36 Average queue time for Poisson distribution

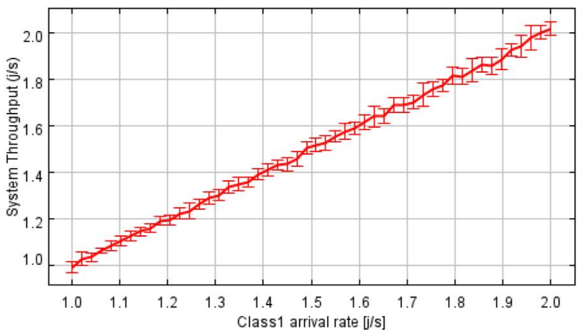

FIGURE 35 Average throughput for Poisson distribution

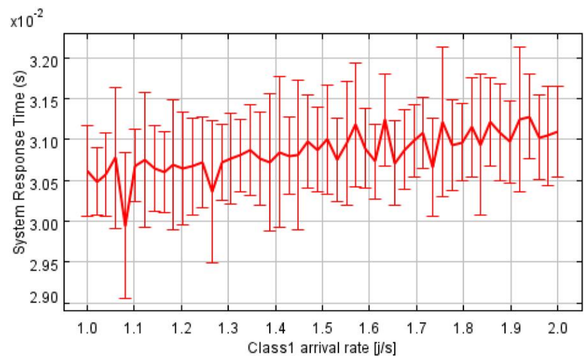

FIGURE 37 Average response time for Poisson distribution

- Queueing time

Additionally, Ref. [15] shows the delay for phase type distribution is 1.7006 $\times$ 10^{-7} ms, and the delay for Poisson distribution is 4.01 $\times$ 10^{-4}. Table 2 and Figure 36 illustrate that the delay in Poisson distribution is higher than that in phase type distribution.

- Response time

Also, Ref. [15] shows the response time for phase type distribution is 0.0029 ms while Poisson distribution is different where the response time is 0.030852 ms. As shown in Table 2 and Figure 37, Poisson had a higher response time than that of phase type distribution.

In the following Table 4, an explanation of the difference between ph/ph/C and M/H_2/C by studying a number of factors affecting the network, such as utilisation network, throughput, delay, waiting time of system, response time and queueing size in the system [18].

7 | CONCLUSION

With the traditional WAN developing to cloud networking, companies are significantly moving applications to the cloud. This design permits users to scale globally, push business agility, and benefit financially from the flexible consumption models of the cloud framework. Cloud networking gives information technology the flexibility to deploy applications

TABLE 4 Comparison between ph/ph/C and M/H_2/C

Parameter	$ph/ph/C$ (arrival process is phase type distribution)	$M/H_2/C$ (arrival process is Poisson distribution)
Utilisation ρ = arrival rate/service rate [18]	$\rho = 5.7191 \times 10^{-4} < 1$	$\rho = 0.03 < 1$
Throughput	41.8638 *pps*	$X^{`} = 1.4998$ pps
Queueing time	$E\,[W_q] = 1.7006 \times 10^{-7}$ ms	$W_q = 4.01 \times 10^{-4}$
Response time and queueing size in system	E[T] = 0.0029 ms	$T = 0.030852$ ms

globally, without compromising on performance and scale. This modification has brought about a whole new set of requirements for security, policy implementation, management, and more. Companies are faced with limitations such as management and operational complexities, inconsistent policy and security, disparate consumption models, and poor application experience. A software-defined WAN (SD-WAN) model addresses these limitations with a cloud, normalised approach that provides scalability, automation, and agility while reducing operational costs. In addition, performance analysis of the queueing model is highly significant to study the behaviour of the network and the parameters affecting it, such as delay and response time, where it affects the utilisation and throughput of the network. The proposed model should be characterised by less delay and high throughput. In this paper, we presented an $M/H_2/1$ queueing model for the SD-WAN network, and a simulation of the network was done using EVE-NG emulator. Also, a comparison was also made between our phase type distribution in our previous study and poison distribution. Then, we analysed the two proposed models to study the behaviour of traffic and get best results in terms of delay, utilisation, throughput, and response time. The results indicate that phase-type distribution performs better than Poisson distribution in this topology where the phase-type distribution queueing model is higher throughput, but it has less delay and less utilisation, also lower response time in phase-type distribution.

8 | FUTURE WORK

There are several distributions which were not studied to date such as beta distribution, gamma distribution, binomial distribution, geometric distribution, negative binomial distribution and discrete uniform distribution. Also, other parameters may be used such as traffic send, data loss and jitter. In our future plans, we will try to study some of these distributions and apply them to SD-WAN solution and cloud networks in an attempt to link networks to the cloud and make the most of its resources and reduce the problems of delay, confusion and packet loss.

CONFLICT OF INTEREST

The author declares no conflict of interest.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analysed in this study.

ORCID

Samaa Adel Ibrahim Hussein https://orcid.org/0000-0002-7598-3334

REFERENCES

1. Kandula, S., et al.: Calendaring for wide area networks. In: Proceedings of the 2014 ACM Conference on SIGCOMM, pp. 515–526 (2014)
2. Rajagopalan, S.: A study on MPLS vs SD-WAN. In: Computer Networks, Big Data and IoT, pp. 297–304. SpringerSingapore (2021)
3. Jason, G., Dana, Y., Dustin, S.: Cisco Software-Defined Wide-Area Networks: Designing, Deploying, and Securing Your Next Generation WAN with Cisco SD-WAN. Cisco Press (2020)
4. De, D., et al. (eds.) Nature Inspired Computing for Wireless Sensor Networks. Springer (2020)
5. Spezio, A.E.: Electronic warfare systems. IEEE Trans. Microw. Theor. Tech. 50(3), 633–644 (2002)
6. Yang, Z., et al.: Software-defined wide area network (SD-WAN): architecture, advances and opportunities. In: 2019 28th International Conference on Computer Communication and Networks (ICCCN), pp. 1–9. IEEE (2019)
7. Sheng, C., Bai, J., Sun, Q.: Software-Defined Wide Area Network Architectures and Technologies. CRC Press (2021)
8. Manel, M., Habib, Y.: An efficient mpls-based source routing scheme in software-defined wide area networks (SD-WAN). In: 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), pp. 1205–1211. IEEE (2017)
9. Troia, S., et al.: SD-WAN: an open-source implementation for enterprise networking services. In: 2020 22nd International Conference on Transparent Optical Networks (ICTON), pp. 1–4. IEEE (2020)
10. Harchol-Balter, M.: Performance Modeling and Design of Computer Systems: Queueing Theory in Action. Cambridge University Press (2013)
11. Atefi, K., et al.: Traffic behaviour of local area network based on M/M/1 queuing model using Poisson and exponential distribution. In: 2016 IEEE Region 10 Symposium (TENSYMP), pp. 19–23. IEEE (2016)
12. Shalimov, A., et al.: Advanced study of SDN/Open Flow controllers. In: 9th Central and Eastern European Software Engineering Conference in Russia, pp. 1–4. Russian, Moscow (2013)
13. Shang, Z., Wu, H., Wolter, K.: An Open Flow controller performance evaluation tool. In: 15th European Workshop on Performance Engineering, pp. 235–249Paris (2018)
14. Open Flow Switch Specification, Open Networking Foundation, Version 1.5.1 (Protocol version 0x06). https://opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf
15. Adel, S., Wanis, F., Ashour, M.: Mathematical Model for Forwarding Packets in Communication Network IET Network (2022). First published: 16 February 2022. https://doi.org/10.1049/ntw2.12035
16. Muhizi, S., et al.: Analysis and performance evaluation of SDN queue model. In: International Conference on Wired/Wireless Internet Communication, pp. 26–37. SpringerCham (2017)
17. Sadeghi, M., Barati, M.: Performance analysis of Poisson and exponential distribution queuing model in local area network. In: 2012 International Conference on Computer and Communication Engineering (ICCCE), pp. 499–503. IEEE (2012)
18. Munir, B.S., et al.: Novel approach to improve qos of a multiple server queue. Int. J. Commun. Netw. Syst. Sci. (01), 83–86 (2010). https://doi.org/10.4236/ijcns.2010.31012

19. Goto, Y., et al.: Queueing analysis of software defined network with realistic open flow–based switch model. Comput. Network. 164, 106892 (2019). https://doi.org/10.1016/j.comnet.2019.106892
20. Bolch, G., et al.: Queueing Networks and Markov Chains: Modeling and Performance Evaluation with Computer Science Applications. John Wiley & Sons (2006)
21. Nweke, L.O., Wolthusen, S.D.: Modelling adversarial flow in software-defined industrial control networks using a queueing network model. In: 2020 IEEE Conference on Communications and Network Security (CNS), pp. 1–6. IEEE (2020)
22. Stewart, W.J.: Queues with phase-type laws: Neuts' matrix-geometric method. In: Probability, Markov Chains, Queues, and Simulation, pp. 444–474. Princeton University Press (2009)
23. Luh, H., Xu, Z.Z.: PH/PH/1 queueing models in mathematica for performance evaluation. Int. J. Oper. Res. 2(2), 81–88 (2005)
24. Durner, R., Blenk, A., Kellerer, W.: Performance study of dynamic QoS management for OpenFlow-enabled SDN switches. In: 2015 IEEE 23rd International Symposium on Quality of Service (IWQoS), pp. 177–182. IEEE (2015)
25. Nunes, B.A.A., et al.: A survey of software-defined networking: past, present, and future of programmable networks. IEEE Commun. Surv. Tutorials 16(3), 1617–1634 (2014)
26. Yao, L., Hong, P., Zhou, W.: Evaluating the controller capacity in software defined networking. In: 2014 23rd International Conference on Computer Communication and Networks (ICCCN), pp. 1–6. IEEE (2014)
27. Xiao, P., et al.: The SDN controller placement problem for WAN. In: 2014 IEEE/CIC International Conference on Communications in China (ICCC), pp. 220–224. IEEE (2014)
28. Kobayashi, M., et al.: Maturing of Open flow and software-defined networking through deployments. Comput. Network. 61, 151–175 (2014). https://doi.org/10.1016/j.bjp.2013.10.011
29. Natarajan, S., Ramaiah, A., Mathen, M.: A software defined cloud-gateway automation system using Open flow. In: 2013 IEEE 2nd International Conference on Cloud Networking (CloudNet), pp. 219–226. IEEE (2013)
30. Scott, E., Patrick, G.: CCNP and CCIE Enterprise Core & CCNP Enterprise Advanced Routing Portable Command Guide. Cisco Press (2020)
31. Zhao, J., et al.: Modeling and optimization of packet forwarding performance in software-defined WAN. Future Generat. Comput. Syst. 106, 412–425 (2020). https://doi.org/10.1016/j.future.2019.12.010
32. Marcel, F.N.: Phase-type probability distributions. In: Encyclopedia of Operations Research and Management Science, pp. 1132–1134. SpringerBoston (2013)
33. Shang, Z., Wolter, K.: Delay Evaluation of Open Flow Network Based on Queueing Model (2016). arXiv preprint arXiv:1608.06491
34. Baba, Y.: Algorithmic methods for Ph/Ph/1 queues with batch arrivals or services. J. Oper. Res. Soc. Jpn. 26(1), 12–32 (1983)

How to cite this article: Ibrahim Hussein, S.A., Zaki, F.W., Ashour, M.M.: Performance evaluation of software-defined wide area network based on queueing theory. IET Netw. 11(3-4), 128–145 (2022). https://doi.org/10.1049/ntw2.12039