A Simulation Environment for enhancing the student experience in advanced networking concepts.

Anjum Zameer Bhat, Imran Ahmed
Department of Computing, Middle East College, Muscat Sultanate of Oman
[azameer@mec.edu.om, imran@mec.edu.om]

Abstract

Several subjects in Computer science necessitate practical and realistic classes in addition to supporting the theoretical underpinning taught to the students. In various subjects' practical exposure & skill is imperative to meet the industry requirements. However, educational establishments can't provide an out-and-out environment for every student to practice. Providing an appropriate Lab for apprentices that bestows desired exposure and feel of a real Network has been a challenging task for every educational establishment. Virtual Labs have been a major milestone and are effectively implemented in numerous colleges and universities throughout the world. In this article, the author is providing a complete setup and functionality of Implementing Virtual Private Networks using virtual Labs to reflect a more realistic and appropriate Networking environment for instructional and educational purposes. Fresh graduates or Diploma holders rarely have practical exposure and experience in deploying and implementing VPNs. Establishing a Virtual Private Network is a cumbersome job, and lack of practical exposure makes it even difficult for a fresher to establish one exclusively for the employer. The Author is providinga guideline for the users so that they can establish Virtual Private Networks using virtual machines. Hencepresenting an environment wherein students can have numerous deployments of VPNs with different features. The students gain the required exposure and develop an understanding of Virtual Private Networks meticulously and pragmatically.

Keywords: VPN simulation model, VPN with Virtual Machines, VPN with VMs, VMs lab model.

1. Introduction

An enormous research and innovation have taken place to facilitate higher education institutions with the latest technological aids(A. Z. Bhat et al., 2021; e-Learning & 2019, 2013; Fadhil et al., 2020). Numerous technologies are used for the enhancement of student experience, academic administration, student support, planning, etc.(Ashaari et al., n.d.; *Big Data for Institutional Planning, Decision Support and Academic Excellence | IEEE Conference Publication | IEEE Xplore*, n.d.; Mkrttchian et al., n.d.; Zameer et al., n.d.). There are however several major have developed Applications & Software in which Virtual Machines & Networks can be built for instructional and didactic use. The Virtual revolutions that have taken place in the recent past, especially in the IT world that has enormously influenced the facilities that are available to students now. Specialized Software Applications are employed at different levels by Networking & Computer Science students in Universities and Colleges (Barrionuevo et al., 2018; Dawson & al Saeed, 2012; Karlov, 2016; Stackpole et al., 2008). Although Virtual Machines have competence for simulating a variety of Network models, it has been observed that the virtual machines are being underutilized especially when using them for instructional purposes. This paper is an effort to demonstrate and exploit the factual potential of virtual machines and their capability to simulate complexnetwork models.

Virtual Private Networks are being established at an extremely high pace in private and Government organizations across the world as the demand for linking branch offices, partners, and collaborations in the organizations has increased(Khanvilkar et al., n.d.; potentials & 2001, n.d.). Virtual Private Network is an efficient, economical, and comfortable technology for organizations to connect their branch offices and partner associations. As the hardware expenditure for implementing the VPNs has significantly decreased over the preceding decade its implementation and deployment have reciprocally & exponentially grown particularly in small to medium-level organizations. As a result, it necessitates imminent network professionals to be fully aware and educated about this mounting and emergent technology(A. Bhat et al., 2016).

On the other hand, providing a pragmatic environment for students to understand the ins and outs of VPNs even with the use of simulators is found to be difficult in most educational establishments. As Virtual Private Networks are thought to be spread over a large geographical area using a public network (internet), simulating such an environment is practically difficult and complex. In many simulators a partial view or idea can be provided to the students for building Virtual Private Networks; however, a complete deployment or a working model is not achieved by using them. In this paper, the author is using "Virtual Machines" with dynamic DNS to simulate Virtual Private Networks.

There is one significant challenge in implementing Virtual Private Networks in Virtual Machines. We need to represent two different networks connected via the public network (internet) in the virtual machine and these two networks should be recognized over a public network by a unique IP without purchasing one from the service provider, as educational institutions cannot purchase

domain names or IP addresses for every student working on the simulator.

To overcome this challenge the author is using "dynamic DNS" on either of the connecting networks to uniquely represent the communicating networks on the public network (Internet). Various vendors provide dynamic DNS both free and on an annual subscription fee. After opening a free account with a dynamic DNS provider, thesoftware is used in both communicating networks to keeptrack of changing IPs, avoiding the need of purchasing Static IPs or domain names which certainly have financialimplications and may not be suitable and feasible for educational establishments.

By using the concept of dynamic DNS to represent different networks and locations of Virtual Private networks a student gets a real feel and exposure to implementing Virtual Private Networks which is imperative for the development of skills in imminent professionals.

The model uses five virtual machines (Domain controller, Radius Server, Internet Information Server, VPN Server, and VPN Client machine) which can be built on a single or multiple computer system. The model represents a domain network for an enterprise with the necessary infrastructure for building a Virtual Private Network likea RADIUS server (Remote Authentication Dial-in User Service), a VPN Server, and a domain controller (DC). Allthe above virtual servers represent a single domain network of an enterprise that desires to establish a Virtual Private Network to give remote access to its employees sothat they can log in to the company's network even when they are out of the office. All these Virtual Machines carry the windows 2019 network operating system with all the necessary tools and components required to establish a Virtual Private Network.

A Virtual Machine carrying the Windows 10 Professional operating system is used as a VPN client computer that is connected to a public network (internet) and connects to a Domain network for access to various resources from a remote location.

In both the networks above a Dynamic DNS client software is installed which keeps track of changing IPs and updates it back to both communicating parties so that network packets can be routed to the correct location. In this manner, a Virtual Private Network is formed by usingVirtual Machines.

2. Related Work

A lot of work has been formerly done on augmentation, enhancement, and improvement of Virtual Machines to accommodate and simulate complicated network models. Many paradigms have been provided wherein a simulation or implementation of VPNs can be achieved but how to involve a real public network in the simulation has not been defined.

The complexity of VPN networks lies in the fact that these networks use a public network (internet) to connect several locations or sites of a private network. Simulating or representing a private network in virtual machines is quite common and reasonably easier but representing a public network like the internet in a coherent way that results in the real formation of a Virtual Private Network is very scarce. There has been substantial work done in different virtual machine environments like Microsoft Virtual PC, VMware, etc. but in all of the models, a dummy or a mock network is used to represent the public network.

To understand various aspects of Virtual Private Networks and their dependency on a public network, it is imperative to use a realistic public network so that an in-depth understanding can be achieved of the characteristics, limitations, and advantages of using public networks for connecting different locations of a private network.

The network model presented in this paper is using a public network (internet) to connect two locations of a private network represented by virtual machines. Virtual machines are capable of connecting to the internet; this capability of virtual machines is exploited in this paper to achieve a pragmatic deployment of Virtual Private Networks.

3. Choosing a Virtual Environment

The specified model can be designed in any of the virtual environments which allow the establishment of networks on the Microsoft platform. However, it is always better to choose a virtual environment in which the user is having enough control and knowledge. The virtual environment used in this model is Microsoft Virtual PC.

Microsoft Virtual PC lets you create one or more virtual machines, each running its operating system, on a single physical computer. The virtual machine emulates a standard x86-based computer which includes all the basic hardware components except the processor. By using emulated hardware and the processor in the physical computer, each virtual machine works like a separate physical computer. Because each virtual machine has its operating system, you can run several different operating systems at the same time on a single computer (A. Bhat, Khan, et al., n.d.; Yuan & Strayer, 2001).

A virtual machine can be configured to provide access to the following:

i. Internal network resources.
ii. The Internet and other external network resources.
iii. The local network consists of just the other virtual machines.
iv. The local network consists of the other virtual machines and the host operating system.

Each virtual machine can be set up to use from zero to four network adapters, each of which can have a different configuration.

a. A virtual machine may consist of the following components.
b. A virtual machine window in which the virtual machine runs. Each virtual machine has settings that determine the operating relationship with thehost operating system, such as the amount of RAM allocated for the virtual machine.
c. A virtual machine configuration (.vmc) file that contains all configuration information for a

virtual machine.

d. A file that represents the hard disk of the virtual machine, is known as a virtual hard disk. Virtual hard disks have the extension .vhd. By default, this disk is a dynamically expanding file that grows in size as you install applications or store data on it.

e. Emulated hardware and external devices, including keyboard, mouse, CD, DVD, floppy disk, sound card, ports, printers, and other devices that the virtual machine uses to emulatea physical computer(Enginarlar et al., 2010; Iqbalet al., n.d.).

4. Challenges

Many challenges were faced while constructing the network model but the primary among them was the challenge of representing each location of a private network in a virtual machine by a unique IP. As in real Virtual Private networks, each location of a private network must be represented by a unique IP address allocated by the ISP. Typically these IP addresses are available at an annual subscription reimbursement and all the organizations deploying Virtual Private Networks procure these IPs or domain names to symbolize different locations of the organization distinctively on a public network (internet).

As with the growing demand for the domain name, there is a substitute used quite frequently by the organizations i.e. Dynamic DNS. A dynamic DNS unlike DNS can point to a dynamic IP address that changes over a while and these changes are monitored and accordingly updated and communicated to the clients or locations using them. Dynamic DNS is comparatively available at a lesser annual subscription fee and can easily be booked from theinternet. There are various vendors available in the market from where we can purchase a Dynamic DNS. Moreover,many of the vendors provide a free Dynamic DNS without any annual subscription, just one needs to create an account on the vendor's website which is just as easy as creating an email account. We can specify multiple locations of our network and all those will be assigned a dynamic DNS by the vendor. A specialized application should be running at each network location to keep track of the changing IP in the Dynamic DNS, this application is usually provided by the vendors and can be downloaded easily from the internet.

5. Design

Virtual Private Networks accomplish different tasks as appropriate to the requirements of a particular organization. As Virtual Private Networks use a public network to communicate between multiple locations, security is the prime concern. As a result, there are various protocols available that provide security to the data flowing through a public network by encrypting and encapsulating the data.

A complex Virtual Private Network may contain many specialized VPN-enabled routers which are responsible for enforcing different VPN protocols to ensure the security and integrity of the data passing through a publicnetwork. These specialized routers are designed toaccommodate numerous VPN tunnels which represent a dedicated link or a connection to a remote location. These routers are completely compatible with all the advanced protocols defined, necessary for the establishment of a Virtual Private Network. We can implement the Virtual Private Networks without the use of these specialized devices as many of the platforms or network operating systems do provide a facility for establishing VPN and include the set of protocols required for the establishment of a Virtual Private Network. Windows Server 2019 provides all the necessary components for the establishment of a VPN. Instead of using expensive special purpose VPN-enabled routers, we can have a computer system with Windows Server 2019 doing the same job. The typical infrastructure of VPN established using Windows 2019 Server includes.

1. Four windows server 2019 computers representing a Domain controller, Remote Authentication Dial-in User Server, Internet Information Server, and a VPN Server.
2. Window XP Professional computer representinga VPN user.

The same can be represented using virtual machines using the following infrastructure. The infrastructure for theVPN network consists of five Virtual Machines performing the following services(Gupta et al., 2009).

a. A Virtual Machine running Windows Server 2019 that is acting as a domain controller, aDomain Name System (DNS) server, a Dynamic Host Configuration Protocol (DHCP) server, and a certification authority (CA).

b. A Virtual Machine running Windows Server 2019 that is acting as a Remote Authentication Dial-In User Service (RADIUS) server.

c. A Virtual Machine running Windows Server 2019 that is acting as a Web and file server.

d. A Virtual Machine running Windows Server 2019 that is acting as a VPN server.

e. A Virtual Machine running Windows 10Professional with SP2 that is acting as a VPN client.

The five virtual machines performing the services listed above are

i. A Domain controller is a machine running Active Directory Services for the organization. This machine is configured to be a DHCP server so that IP addresses can be assigned to the host machines automatically. This machine will have one network interface card configured to be connected to the local network. The machine is having a local IP address of 172.16.0.1 with a subnet mask 255.255.255.0 configured.

ii. The second virtual machine will be configured asa RADIUS Server. This machine is used to authenticate VPN users to have access to the company's network. The computer is installed with Windows Server 2019 and an internet authentication service is configured on this server. In addition, this server is registered in the Active Directory so that it is authorized to authenticate

all dial-in users for Active Directory access. This machine is configured with one network interface card connected to the local network. The computer will be a member of the domain network of the organization. The machine is having local IP address 172.16.0.2 with subnet mask 255.255.255.0.

iii. The third virtual machine is a computer running Windows Server 2019 and Internet Information Services (IIS). It provides Web and file server services for intranet clients. This particular machine is optional and specifically designed for providing web and file services to intranet clients. A VPN can be established without the use of this machine if we don't want to give web services to our clients. This machine is configured with one network interface card connected to the local network and it will be a member of the domain network of the organization. The machine is having an IP address of 172.16.0.3 with subnet mask 255.255.255.0

iv. The fourth virtual machine is a computer running Windows server 2019 that provides VPN server service to internet clients. This machine is configured with routing and remote access. In addition, various protocols necessary for the establishment of the VPN are configured in the machine as this machine will be responsible for routing the packets to the destination and embedding security to the data traveling on the public network. This machine is configured with two network interface cards, one connected to the local network and another connected to the public network (internet). One network interface card will be having local IP address configured as 172.16.0.4 with subnet mask 255.255.255.0. The second network interface card will be given an IP assigned by the vendor of the dynamic DNS. The dynamic DNS used in this model has been registered from "no-IP" which is a renowned vendor for dynamic and static IPs.

v. The fifth virtual machine is configured with Windows 10Professional SP2. This machine represents the VPN user. This machine does not have any connection with the local network or the domain network of the organization. The machine is directly connected to the internet and is configured with the IP address assigned by the dynamic DNS vendor. A dial-in connection is established/configured in this virtual machine so that the VPN network can be connected on demand and the VPN user can get access to the resources of the organization's network from any remote location. After the connection is dialed it asks for the user name and password and if correctly entered the user is given access to the resources of the organization's network. The user can thus connect to the company's database, access shared files & folders, can get access to network printers and all other resources which may be available to any network user of the organization.

6. Dynamic DNS Functionality and Implementation

The dynamic DNS used in this model is provided by a well know vendor for Dynamic & Static DNS "no-IP". "no-IP"also issues free accounts so that people can benefit by using the services for different purposes. After opening the account and defining various settings for the dynamic DNS like DNS names of various locations etc. an application is to be installed at each location that keeps track of changes in the IP addresses of that location. In thismodel "NO-IP Dynamic Update Client" application isinstalled on the VPN server as well as on the VPN client computers. NO-IP DUC is a program that monitors the machine's IP address and notifies the dynamic DNS system when it changes. Appropriately DNS name alreadyregistered by us points to a new IP address updated to it bythe Dynamic update client program and hence a location can always be uniquely identified and data packets can besent or received from that location using a public network(internet)(Cheung et al., n.d.; Pappas et al., n.d.; Wilkinsonet al., n.d.). The concept of dynamic DNS is used in numerous realistic VPN implementations by small organizations which do not want to spend too much moneyon the VPN infrastructure and want to avoid theexpenditure of purchasing a static IP or a domain name. As the services of dynamic DNS are provided at very lowcosts that suit many small-scale organizations, even a fewof the organizations use a free account that needs to be renewed after every three months however renewal process is very easy and can be done online by sending a simple mail to "no-IP". One more difference between a paid account which is available at an annual subscription fee and a free account is that in case of any disturbance inthe services of the free account, "no-IP" will neither be responsible and nor any service will be provided in that regard; however, in case of paid accounts company takes responsibility of any disturbances in the services and assists in case of any fault in the account. The free accountof dynamic DNS is automatically stopped if the service isnot being used continuously for one month; however paid services are not stopped even if the account is inactive fora considerably long period.

The free services of dynamic DNS are well suited for experimental and instructional purposes and can be beneficial for small companies which do not require large data transfers between multiple locations and do not need to be constantly connected.

7. Results

An experiment was conducted on virtual machines established on a single physical computer system as well as virtual machines established on two physical computer systems and the results were successful in both. A Virtual Private Network was successfully simulated and represented by the virtual machines in both cases. In the first experiment, all virtual machines were accommodated

on a single physical computer, and internet access was provided to the VPN server and VPN client virtual machines with dynamic update client software running on both. The client machine was successfully able to establisha connection to the domain network and access various resources of the network. A network drive was mapped from the VPN client computer to a shared folder on the organization's network. In the second experiment VPN client machine was established on a separate physical computer and all other virtual machines were established on a separate computer system, in this case as well VPN client computer was successfully connected to the domain

network and accessed all the resources available on the network.

However, errors can occur in establishing connectivity from the client computer to the organization's network if dynamic DNS is not getting updated or there is any error in the dynamic update client application installed on the VPN server virtual machine or VPN client virtual machine. In addition to that dynamic update, the client application should always be running in both virtual machines to get the latest update of any changes in the IP address from any side. The connectivity problem has also been noticed if there is any error with the dynamic DNS account established on the email specified by the applicant; many email accounts do not communicate the updated information to the "no-IP" dynamic DNS host which can cause problems in the communication. If the users take care of the above reasons for a possible error, the connection is stable and can be maintained for long sessions of data transfer and information access without any complications.

8. Conclusion

There are numerous cloud-based models available for the didactic purpose(A. Bhat et al., 2021; A. Bhat, Kameshwari, et al., n.d.; A. Bhat, Singh, et al., n.d.). Cloudcomputing has recently been used for several educational purposes(A. Z. Bhat et al., 2021; Singh et al., n.d.). This research study takes an entirely different approach so that realistic exposure is provided to students in establishing Virtual Private networks. The established Virtual Private Network is completely stable and can be used as a model by the students to understand how Virtual Private Networks are established, the components and tools used to establish the VPN, the necessary infrastructure required for the deployment of Virtual Private Network, various types of services and facilities which can be allotted to theVirtual Private Network clients, pragmatic exposure to understand the situations in which a company may opt for establishing a Virtual Private Network, practical understanding of benefits gained by the deployment of Virtual Private Networks, the confidence of building the Virtual Private Networks exclusively and independently. In addition, students will understand the limitations of a public network which is only possible while realistically implementing the Virtual Private Networks.

Acknowledgements

We are extremely thankful to Almighty Allah for bestowing us strength, intellect, and health to carry out this research work. We are certainly very thankful to Middle East College for the continued support that they provide for research activities. We are extremely thankful to everyone that has laid a helping hand in this research study.The academicians, students, colleagues, and others without whom this research study would not be possible. We are also truly thankful to our families, friends, and supporters for their support and cooperation.

References

Ashaari, M., Singh, K., Abbasi, G., … A. A.-… F. and S., & 2021, undefined. (n.d.). Big data analytics capability for improvedperformance of higher educationinstitutions in the Era of IR 4.0: A multi-analytical SEM & ANN perspective.*Elsevier*. Retrieved September 1, 2022,from https://www.sciencedirect.com/science/article/pii/S0040162521005527

Barrionuevo, M., Gil, C., Giribaldi, M., Suarez, C., & Taffernaberry, C. (2018). Virtualization in education: Portable network laboratory. *Communications in Computer and Information Science*, *790*, 90–98. https://doi.org/10.1007/978-3-319-75214-3_9

Bhat, A., Kameshwari, L., International, B.S.-2020 I. 5th, & 2020, undefined. (n.d.).MathCloud: a discrete cloud implementation to enhance learning experience in mathematics. *Ieeexplore.Ieee.Org*. https://doi.org/10.1109/ICCCA49541.2020.9250875

Bhat, A., Khan, M., Research, I. A.-J. of S.,& 2021, undefined. (n.d.). The Enhancedavailability agility Centralized Management and benefits with vCenter &vMotion a reflection. *Jsr.Org*. RetrievedSeptember 15, 2022, from https://jsr.org/index.php/path/article/view/ 1466

Bhat, A., Shuaibi, D. al, International, A.S.-2016 5th, & 2016, undefined. (2016).Virtual private network as a service—Aneed for discrete cloud architecture.*Ieeexplore.Ieee.Org*. https://doi.org/10.1109/ICRITO.2016.7785012

Bhat, A., Singh, B., International, A. S.- 2017 6th, & 2017, undefined. (n.d.). Learning resources as a service (LraaS) for Higher Education Institutions in Sultanate of Oman. *Ieeexplore.Ieee.Org*. RetrievedSeptember 10, 2022, from https://ieeexplore.ieee.org/abstract/document/8342486/

Bhat, A., Singh, B., & Mohsin, T. (2021). *Cloud Implementation to Assist Teachers ofEnglish to Speakers of Other Languages in HEI's in Sultanate of Oman*. https://osf.io/2q8kg/download

Bhat, A. Z., Singh, B., & Fadhil, T. (2021).*Role of Cloud Computing to Support BigData and Big Data Analytics for EducationPar Excellence*. 327–337.

https://doi.org/10.1007/978-981-33-4604- 8_26
Big data for institutional planning, decision support and academic excellence | IEEE Conference Publication | IEEE Xplore. (n.d.). Retrieved March 15, 2022, from https://ieeexplore.ieee.org/abstract/document/7460353
Cheung, C., Yuen, M., … A. Y.-I. C. on, &2003, undefined. (n.d.). Dynamic DNS for load balancing. *Ieeexplore.Ieee.Org*. Retrieved September 15, 2022, from https://ieeexplore.ieee.org/abstract/document/1203676/
Dawson, M. E., & al Saeed, I. (2012). Useof open source software and virtualizationin academia to enhance higher educationeverywhere. *Cutting-Edge Technologies inHigher Education*, *6*(PARTC), 283–313. https://doi.org/10.1108/S2044-9968(2012)000006C013/FULL/HTML
e-Learning, S. H.-O. J. of D. E. and, & 2019, undefined.(2013).Technological advancements in education 4.0. *Tojdel.Net*. https://tojdel.net/journals/tojdel/volumes/to jdel-volume07-i01.pdf#page=70 Enginarlar, E., Li, J., & Meerkov, S. M. (2010). *Virtual machines*. https://doi.org/10.1007/s00291-004-0187- 1
Fadhil, T., Anjum, M., Bhat, Z., Ahmed, I.,& Khan, M. S. (2020). Systematic Approach for Development of Knowledge Base in Higher Education. *Journal of Student Research*. https://doi.org/10.47611/jsr.vi.999Gupta, V., Gavrilovska, A., Schwan, K., Kharche, H., Tolia, N., Talwar, V., & Ranganathan, P. (2009). GViM: GPU- accelerated virtual machines. *Dl.Acm.Org*. https://dl.acm.org/doi/abs/10.1145/151913 8.1519141
Iqbal, A., Pattinson, C., on, A. K.-2015 W. C., & 2015, undefined. (n.d.). Performance monitoring of Virtual Machines (VMs) of type i and II hypervisors with SNMPv3. *Ieeexplore.Ieee.Org*. Retrieved September 15, 2022, from https://ieeexplore.ieee.org/abstract/document/7415127/
Karlov, A. A. (2016). Virtualization in education: Information Security lab in yourhands. *Physics of Particles and Nuclei Letters*, *13*(5), 640–643. https://doi.org/10.1134/S1547477116050289
Khanvilkar, S., Magazine, A. K.-I. C., & 2004, undefined. (n.d.). Virtual private networks: an overview with performance evaluation. *Ieeexplore.Ieee.Org*. Retrieved September 15, 2022, from https://ieeexplore.ieee.org/abstract/document/1341273/
Mkrttchian, V., Gamidullaeva, L., … A. F.-I. J. of, & 2021, undefined. (n.d.). Big dataand internet of things (IoT) technologies'influence on higher education: current stateand future prospects. *Igi-Global.Com*.Retrieved September 1, 2022, from https://www.igi-global.com/article/big- data-and-internet-of-things-iot- technologies-influence-on-higher-education/284475
Pappas, A., Hailes, S., Symposium, R. G.-L. C., & 2002, undefined. (n.d.). Mobile host location tracking through DNS. *Ee.Ucl.Ac.Uk*. Retrieved September 15, 2022, from https://www.ee.ucl.ac.uk/lcs/previous/LCS2002/LCS072.pdf
potentials, R. V.-I., & 2001, undefined. (n.d.). Virtual private networks. *Ieeexplore.Ieee.Org*. Retrieved September 15, 2022, from https://ieeexplore.ieee.org/abstract/document/913204/
Singh, V., Marcel, R. ·, Durgesh, W., Mishra, K., Amit, ·, Shikha, J., & Editors, M. (n.d.). Multimedia cloud for highereducation establishments: a reflection. *Springer*. Retrieved September 10, 2022,from https://link.springer.com/chapter/10.1007/ 978-981-13-2285-3_81
Stackpole, B., Koppe, J., Haskell, T., education, L. G.-… technology, & 2008, undefined. (2008). Decentralized virtualization in systems administration education. *Dl.Acm.Org*, 249–253. https://doi.org/10.1145/1414558.14146