The Evaluation of Generated Traffic and ICMP of Juniper, Arista and Cisco in GNS3

Sivangangai Gopinath Ritesh Aswin Raam
[1]II[nd] Semester, I[st] Year, M.Sc. Cloud Computing,
X19154160@student.ncirl.ie *National College of Ireland*

***Abstract*—Virtualization has reached its peak over recent years, the use of virtualization helps us to solve the problem of underutilized resources by forming a virtualization between the user and the hardware components, by this it enables the creation of virtual machines where these are virtual computers that can run in multiple set of platforms on a single set of hardware. Many virtual machines can be created on a single host computer. The virtualization layer creates set of virtual hardware components for the VMs like some computer possess, where there are converted into virtual resources for the virtual machines. Therefore by using this it increases efficiency and enables to perform multi-tasking where we can run multiple computers or operating system on a single set of hardware and it also enables security by isolating them from the core system, it also able to run legacy application which cannot be performed on the normal computer. In this paper, we discuss about network virtualization where we compared 3 market players namely Juniper, Cisco and Arista by forming a basic network topology on an open-source graphical network simulator called GNS3(Graphical network Simulator 3) and captured the ping from one device to other and capture the log for these 3 players and finally conclude which has a better performance.**

***Keywords*- Virtualization, Network Virtualization, Juniper, Arista, Cisco, GNS3.**

I.INTRODUCTION

Virtualization is one of the hot topics over the IT environment over the past few years due to its ability to provide feasible solutions to companies which can increase their productivity by reducing the IT infrastructure costs. And by switching into this the companies where able to monitor their workloads on data centers which reduces their investment over their IT infrastructure and energy consumption cost. One of the main benefits if there is a event of failure the disaster virtualization does the faster recovery of IT resources where it is not supported on the old infrastructures [1], with virtualization there is no longer to troubleshoot complex problems, replacing hardware and monitoring each and everything, by using virtualization it simply allows to clone and apply a new resources without altering the repaired one which saves time for the organization where they can spend time of developing in business-critical application[2].

The use of network virtualization is very essential, it is a method of combining the list of available resources in the network to merge into different physical networks and its replicates the elements of security services and networks in a software container. With the use of network virtualization, the network administrators can change the firewall, logical switches, routers, VPNs and security in a matter of time. It combines hardware and software resources and network functionality into one software-based entity with the help of this. It is proven that network function virtualization can increase the performance, reduced energy consumption and decreased cost compared to that of the traditional hardware-based system. Load balancing can be improved by dividing the local area networks into VLANs and virtual networks. Apart from this an organization can create a logical network even though using the existing hardware, this new network can be completely independent to other virtual network even it uses the same equipment. It maintains complete security of the network and the traffic of each network is kept isolated which avoids from mixing with other resources. Network virtualization offers network segmentation otherwise called as micro-segmentation which offers organization to offer a set of rules between the workloads. Segmentation of the VM-to-VM level allows the execution of a zero-trust policy [4].

In this paper we considered 3 market players in networks virtualization Juniper, Arista and Cisco where each network provides a different set of solutions. And the performance, ping is tested using the network software emulator called as GNS3 is a commercial software which is used to developed basic and complex network topology and generate traffic and do tests on it.

II.PROBLEM DEFINITION AND BACKGROUND

When developing a large set of networks for an enterprise or companies it should be tested first before pushing into production, where this testing will be effective for trouble shooting and different network topology design can be tested. The main problem is that small and SMEs cannot afford these kinds of simulation due to the cost issues and the shortage of equipment's to carry out testing.

So, with the help of free open-source software named GNS3 one can able to develop a different set of networks topology and test the performance, ping and capture log and traffic of the different vendors. So, we perform these set of functions on the top three players namely Juniper, Arista and Cisco [7].

BACKGROUND

The virtualization is a process of virtual environment or software-based representation of networks, storages and servers etc. which enables IT sectors to run more than one sectors. And to reduce the IT infrastructure costs and time there

has been an increase in use of network virtualization which is used to convert the hardware and software resources into a single software entity and on the a developer side if you want a test new software which needed different networks to run is tested using network virtualization, to test this networks and do the performance analysis GNS3 is used.

GNS3 network software emulator is used to develop a complex and simple networks by downloading different set of switches and routers and developing a network after that the ping is done from one interface to the another to check the time taken and performance of the switches. Wireshark is an open-source packet analyzer which is used to capture logs and do the network troubleshooting which will be downloaded along with the GNS3. The GNS3 is integrated with VMware workstation pro with the GNS3 server inside which otherwise said to be GNS3 VM, it is used to run the set of instructions on the controller from the windows PC, it is integrated because some emulators will not be working on windows. GNS3 GUI basically makes an API call to VMware based on adjustment of size of the RAM and CPUs based on the setting made.

The 3 main market players who were used to do the performance are as follows,
Juniper is a company that provides network products, network security products, SDN (Software Network Technology), and software for network management. The main aim of juniper is to provide virtualized networks to the clients according to their needs in a broader ecosystem of application, storage and computing. Every step of deployment and migrations are taken care by the juniper networks according to their clients wish.

Another important player is Arista networks which is a leading cloud networking and storage-driven cloud networking solutions for large-scale data centers and environments, it provides building a scalable, low latency and high-performance cloud networks. The introduction of Arista EOS (Extensible Operating Systems) is used to control the high-performance data center switches in the virtualized data center with high performance [5].

One of the main players in the field is Cisco systems which is a networking company which allows organizations and companies to adopt to network virtualization that is offered by the company due its flexible software-based computing and storage resource. These services enable networks to be more application-centric and more agile, it also provides a fully integrated architecture by delivering modernized application and services for virtual, physical and cloud environments [6].

III.LITERATURE REVIEW

In [8], there was a distant learning approach proposed for students to learn about the computer networks, their topology and the modeling of LAN (Local area network) and MAN (Metropolitan area network) on their own without the help of teachers to guide them. So, the students use tool called GNS3 which is an open-source software that is used to create and add routers, switches. So, the main aim of the paper is too creating a network topology with different set of routers and switches to analyze the data traffic and they have also used the Wireshark to capture and store generated data packets. So, at the end of the paper the authors stated that students were able to gain basic knowledge virtual networks and the concept of load balancing between routers and other configurations related to networks. Similar approach proposed by Dayanand et al. [9] where network developer use GNS3 tool for the creation of multiple networks, routers and switches in a virtualized environment to reduce the costs and then testing of new networks before release. At the end of the survey the authors stated that the developers where able to create complex network topology and test their performance and traffic generated. The use of GNS3 allows us trouble shoot the own configurations error by troubleshooting them. And for the professional users who use complex set of networks can skip the basic steps and directly switch to complex configurations.

Rodrigo and Mario proposed a paper where an extension is produced to automatically configure the network requirements since as the network topology increases the amount of equipment's of the network is also to be configured. So, for all cisco configurations the automatic extension is proposed which will save time for the developers when developing a complex set of network topologies using the cisco switches and routers. So a extension to GNS3 network virtualizer with the help of perl scripts that can configure files involved in the network automatically which makes easy to develop a network topology. It reads the file and generate Cisco IOS file related to the device. At the end authors stated that by use of these steps the basic configuration when building a complex network and testing those networks and configure a error prone network [10]. A comparison made between Packet Tracer (PT) and GNS3 to find out which performs better and the comparison is made by forming a network topology, a PT is an official cisco software platform used to perform cisco network operations, whearas the GNS3 is a open-source tool where set of images can be downloaded and the networks can be formed. At the end of the paper the author stated that each tools benefit in a specific set of functions like it can be used to create a networking plan that supports external and internal function of the networks and on the other hand GNS3 can check the logic of the network is suitable for the specified purpose. So, the combinations of both tools can solve more complex network problems rather than separately [11].

IV.EXPERIMENT

The benchmarking tool is created to measure the performance of the networks and to capture the traffic generated by each set of switches. Usually these applications are used by the switches or routers to find the execution time and capture the traffic between 2 routers. By using these platforms, we have created a network topology with different set of switches to find out the ping, traffic of each one of them to find which one is efficient compared to other.

This paper will evaluate and measure the performance of Juniper, Arista and Cisco networks by forming a network topology in the GNS3 emulator where we have captured the icmp logs and the traffic between 2 switches is captured using the Wireshark.

The set of steps to be followed for the installation is.

1. Install the GNS3 2.2.12 on the local operating system
2. The VMware Workstation Pro is integrated with the

GNS3 GUI, where GNS3 makes the API call to the VMware and set of instructions can be performed because some of the emulators will not be working on the windows.

3. GNS3 is all in one function where open-source packet analyzer Wireshark is installed along with this and list of packages for this performance as well.
4. The set of switches and routers are downloaded in the GNS3 to form and network topology and perform the functions.
5. The Juniper vMX router is installed on the GNS3 simulator.
6. Then for Cisco 7200 and 3725 IOS Router images are downloaded and uploaded on the GNS3 and later the network topology is formed.
7. And then the virtual router Arista vIOS is downloaded uploaded on the GNS3.
8. After network is formed, the solar putty is opened to do the testing by setting the IP address for the different set of switches and it is pinged from one to another to test the performance of each networks.
9. The results are generated and then collected.

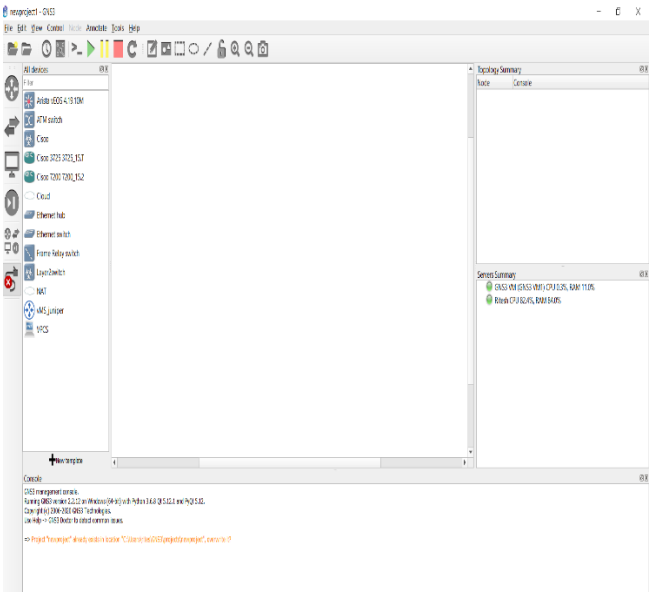

Figure 1: Overview of GNS3

The above diagram shows the overview of GNS3 and set of network switches and routers are downloaded and are seen on the left and on the right 2 green signals, one is the local server and GNS3 VM status is on green color which shows they are connected and ready to go and it also shows the amount of RAM utilized by the systems.

And below diagram shows how the GNS3 looks when integrated with the GNS3 VM. As soon as starting the GNS3 client we can see that GNS3 VM is also automatically starts along with it and it turns to active state.

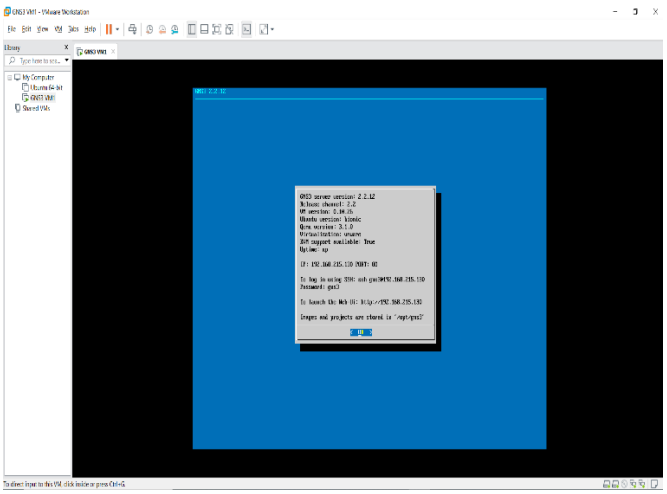

Figure 2: The integration of VMware pro with GNS3

Juniper- Forming a network with vMX router

The basic network is formed by connecting Juniper vMX router which is carrier-grade router that is used to run on JUNOS operating system which is well suited for its network functions virtualization. The vMX is downloaded on Juniper networks official website and uploaded on the GNS3 for forming a network and doing the set of tests and functions.

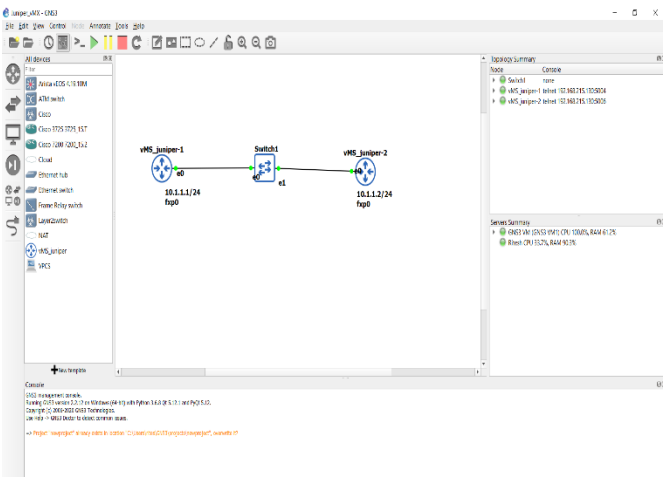

Figure 3: Basic network topology using Juniper

Above diagram shows how the network is created by adding 2 set of Juniper vMX connected with the ethernet switch which runs the virtual environments. After forming the network, it is started to do performance and capture of logs. The IP address for each router is assigned and then VLANs are created on the switch. And then ping is done to check the icmp and ttl of each switch to diagnose the communication issues of each server and difference in ping latency for each router is calculated.

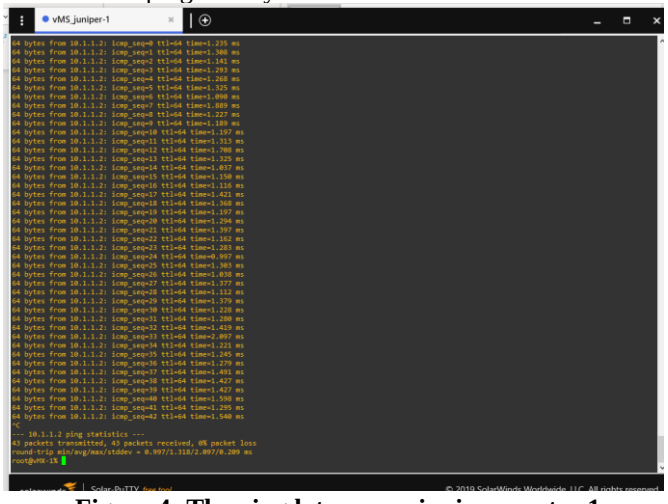

Figure 4: The ping latency on juniper router 1

The above diagram shows the ping latency which is done from switch 1 for the switch 2 to check the performance and it is stated that there was a 0 percent of packet loss which we calculated for 43 packets and estimated time taken is less 2 MS.

The below diagram shows the amount of time taken to ping the switch 1 across from the switch 2. Both the values show that similar amount of taken is taken by both the switches in the network.

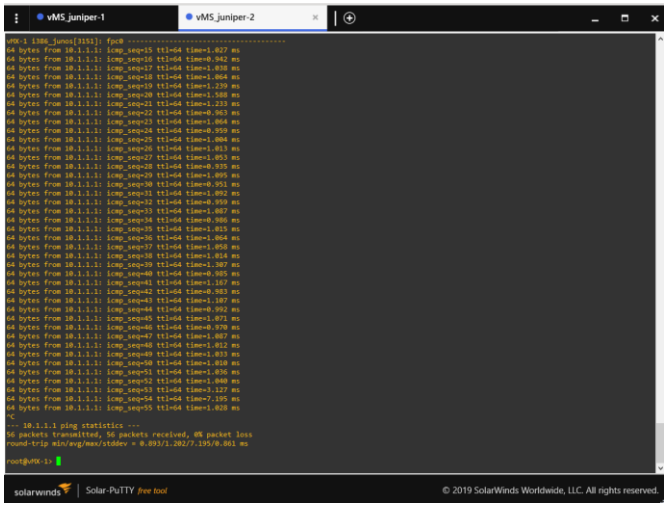

Figure 5: The ping latency from router 1 from router 2

Arista- Network formation using Arista vEOS

The network topology is formed using 2 different Arista vEOS which is a software used to satisfy the business needs of companies which is a switch operating system. Similar to juniper a network is created by downloading the arista switches into the GNS3 environment and then VLAN and IP address is created by starting the network.

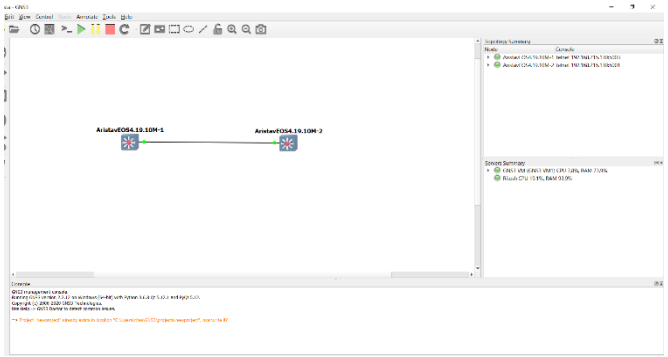

Figure 6: The network of Arista vEOS

The above diagram shows the 2 arista switches have been created and the network is formed between these to compare the performance and time taken while pinging one and another in the solar putty by assigning and VLAN and IP address for each switches on the console and running the tests.

The below diagram shows the ping function, which is called from one switch to the another, the 5 packets have been transmitted with the rate of 0 packet loss and the total time taken by these 5 packets was around 272ms where the exponential weight average is ipg/ewma is around 68.004/53.139ms and the round trip time is for min/avg/max/mdev is 24.001/35.201/72.004/18.661 ms respectively.

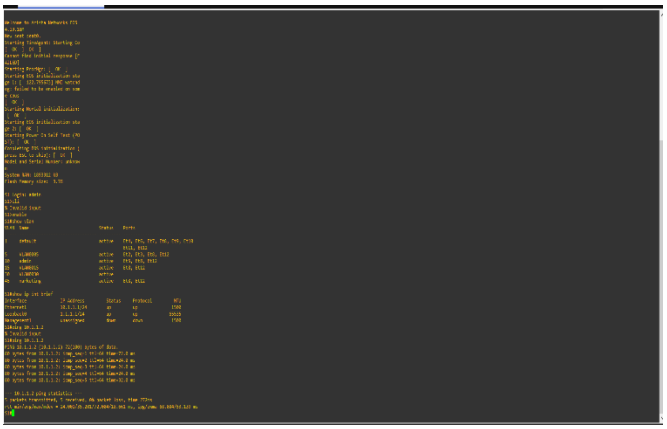

Figure 7: Ping latency from router 1 to router 2

The below diagram shoes the capture of ping latency from switch 2 to the switch 1.

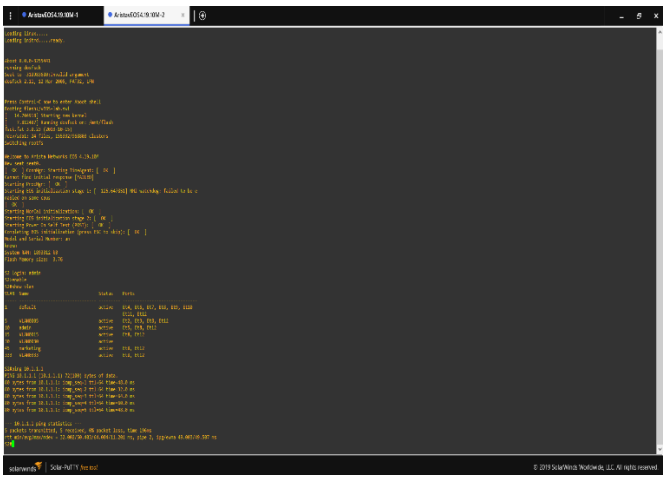

Figure 8: Ping latency from router 2 to 1

The above latency shows there was not a much of a difference compared while pinging from 2 to 1, as similar there were 5 packets transmitted with 0 packet loss and time consumed is 196ms and the rtt min/avg/max/mdev is 32.002/50.403/64.004//11.201ms respectively and the ipg/ewma is 49.003/49.507 which is slightly high compared to that of switch 1.

Cisco – Forming a network topology using Cisco 3725 and Cisco 7200 switch

In this same like other steps, we have uploaded the images of routers namely Cisco 3725 and 7000 in the GNS3 platform, and then these routers are connected along with the ethernet switch and the network is started to assign the ip address and capture the ping and time taken by each switch.

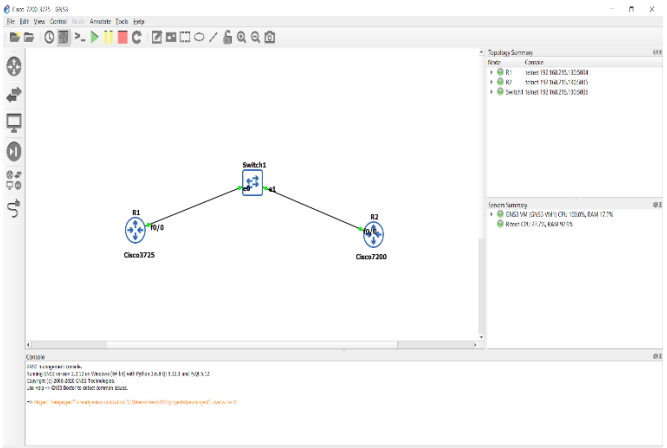

Figure 9- Network formation by connection the 2 switches

Above diagram shows the basic network formed by connecting the 2 switches.

Figure 10: Checking the connectivity of 7200 from 3725

The above diagram shows the ping of Cisco 3725 router, where the connectivity between Cisco 3725 and 7000 is tested by checking the success rate of both the routers. In this we where able to find the success rate is 100 percent and the round-trip min/avg/max is 1/1/4ms.

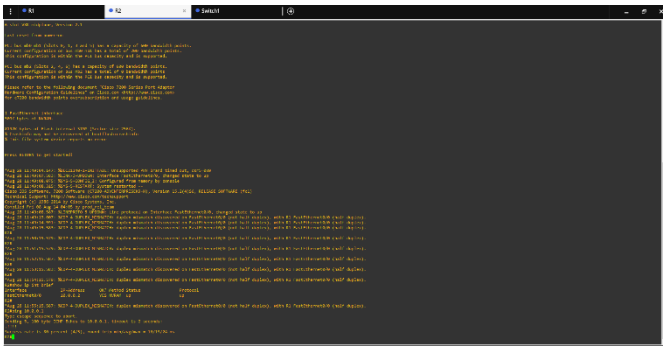

Figure 11: Checking the connectivity of 3725 from 7200

Same like the above process the connectivity is checked from the router 2 and it has been found that the success rate is off 80 percent where 4 packets have been called out of 5 and the round-trip min/avg/max is 16/19/24ms respectively which is slightly high and success rate is less compared to that of 3725 router.

Capturing the traffic between 2 routers using Wireshark tool on GNS3

GNS3 provides an inbuilt Wireshark software which is an open-source packet analyzer which is used to capture logs, traffic and network troubleshooting. For each player, the logs are capture by starting the capture command in the GNS3 where it opens the Wireshark software and capturing traffic between serial link takes place which can be stored in the hardware for later analysis.

The below diagram shows the capture of traffic between 2 set of routers between Juniper vMX 1 and Juniper vMX 2, while pinging from one device to another the Wireshark shows the traffic the amount of packets and the time taken and the source where it is generated and which type of protocol it is running and the length is also shown.

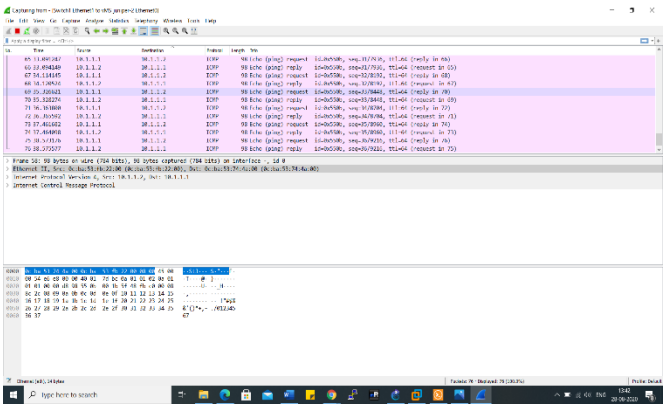

Figure 12: Capturing the traffic between 1 and 2 using Wireshark

Capturing traffic in Arista:

The below diagram show the traffic capture between the 2 arista switches when the connection request is made by the calling the respective IP address the request and the reply time is displayed along from which and destination it is generated along with protocol.

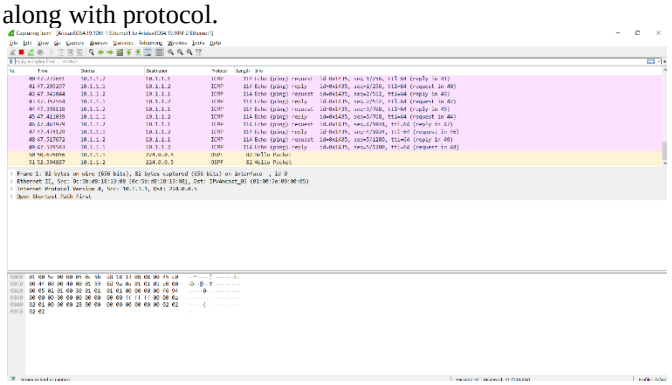

Figure 13: Capturing the traffic between Arista vEOS

Capturing traffics in Cisco

The same set of procedures where followed in cisco 3725 and 7200 switches by capturing the traffic by calling one and other assigned IP address.

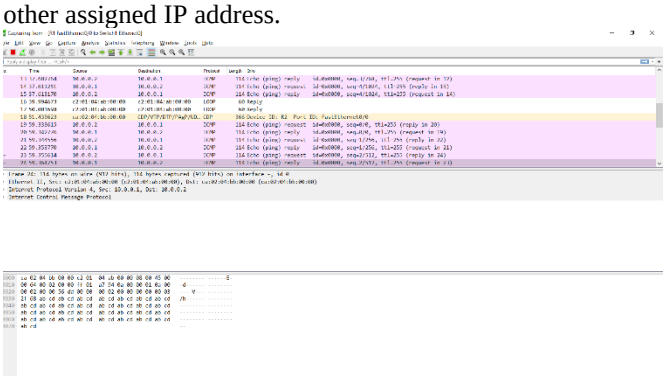

Figure 14: Capturing the traffic between 2 switches of Cisco Networks

In this we perform the traffic capture for 2 different set of switches by calling the IP address on and other. So we were able to get request and reply of each address called upon, there where total of 5 packets where we got ping for a total of 10 and the request and reply time is also calculated and the source and destination of each address from which it is called upon is also shown and considered.

At the end the request and response time for Cisco networks is very low, time taken is very less which makes it faster compared to that of Arista and Juniper, Juniper takes more time compared to other market players.

V SECURITY

The suggestions have been given by user to the latest version of Junos as they possess some set of vulnerabilities where some of them share a same set of passwords which makes easy for the attacker take full access over the software and there is also a serious attack (CVE-2019-0029) where which can be a breach to the Splunk server in which the information's can be accessed. And there has been a set of flaws in advanced firewalls in SRX series proposed by Juniper where it ends in giving full control for the attackers where they have been resolved in the further releases by the company [12].

Arista networks have known for its best security standards across every product they have produced. The Product Security Incident Response Team (PSIRT) responds to the security issues faced by each customer while accessing the product and respond with the possible solution within a short period of time. The collaboration of Arista with Forescout provides zero trust to the customers which provides continuous monitoring and mitigation. These provides complete device availability which provides awareness to the customers like what is happening in the network environment. The DNSSEC (Domain name system security extensions) is not enabled which is used to protect the network from forged DNS data by using public key cryptography. It is one which protects the company's data from third parties from forging the data's which ensures domains identity [13].

Cisco is one of most leading networks which provides complex security solution to their client, they provide complex security which is vulnerable to any kind of security problems. Since the cisco routers are accessed everywhere there are some set of breaches and attacks made like remote attacks made in Cisco 1001-X router that takes away every set of data and commands sent through. And there is a set of weakness found in SOAP API endpoint which gives access to the remote attackers to overcome the authentication over the set of breached devices and the same applies to REST API as well. Most of the attackers go for the network switches which carries the set of information internally within a network. The switches provided by the cisco networks must be patched carefully, since most vulnerable devices does not consist of auto-update which needs manual configuration to get protections [14].

VI. ANALYSIS AND CONCLUSION

In this paper we have considered network virtualization due to it reduce operation costs, infrastructure-less services, security protocols and automation services and by combining the existing hardware into a single virtual network. In this paper we have done the testing by forming a basic network topology on an open-source software emulator called GNS3 which is used to test the set of networks. Three important market players in the networking field have been considered namely Juniper, Arista and Cisco networks where the switches and routers is downloaded on the GNS3 platform and the networks is formed and Wireshark tool is a in-built function provided by GNS3 which is used to monitor and capture traffics and logs for troubleshooting problems. The VLAN is created and then IP address is assigned for each set of switches.

The analysis are made capturing the ping latency and the amount of reply and response time taken is considered when calling a IP address from one switch to the another and the time taken to do the set of requests and the icmp logs is also considered. At the end of the analysis it is stated that each set of networks possessed a different set of response time and comparatively Cisco performed well compared to other in terms of less packet loss and the reply and request time is also less compared to that of Juniper and Arista. Whereas in Juniper the round trip min, max average time ranges around 1 to 10ms, and request and response time when the network function is also comparatively high that of Cisco and in terms of Arista there was a 0 packet loss but the total time taken was high around 270ms which is comparatively high compared to the other market players.

We are not able to propose a specific set of players from the above findings since all three performances were unique and only some set of differences were found. From my point of view, Cisco networks perform consistently compared with other players on the market. Thus, forming a virtualization network using Cisco networks would be a better option to provide a flexible solution and better experience to the customers.

REFERENCES

[1] "Benefits of Virtualization - Thrive," Thrive, 11-Jan-2018.[Online].Available:https://thrivenextgen.com/benefits-of-virtualization

[2] S. Brown, "What Are the Benefits of Virtualization?," www.rutter-net.com. [Online]. Available: https://www.rutter-net.com/blog/what-are-the-benefits-of-virtualization

[3]https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutionbrief/partners/intel/vmware-why-businesses-adopting-network-virtualization-white-paper.pdf

[4] "Advantages of network virtualization impress, but hurdles remain," SearchServerVirtualization. [Online]. Available: https://searchservervirtualization.techtarget.com/feature/Advantages-of-network-virtualization-impress-but-hurdles-remain.

[5] Sabeesh, "What is Network Virtualization?," Arista Networks, 24-Oct-2017. [Online]. Available: https://www.arista.com/en/solutions/network-virtualization . [Accessed: 28-Aug-2020].

[6]"2020. [online] Available at: <https://www.sdxcentral.com/networking/virtualization/definitions/what-is-cisco-network-virtualization/> [Accessed 28 August 2020].

[7] "What is GNS3- and Why do You Need it?," All Consuming, 18-Nov-2016. [Online]. Available: https://www.allconsuming.net/what-is-gns3-and-why-do-you-need-it/ . [Accessed: 28-Aug-2020].

[8] P. Gil, G. J. Garcia, A. Delgado, R. M. Medina, A. Calderón and P. Marti, "Computer networks virtualization with GNS3: Evaluating a solution to optimize resources and achieve a distance learning," 2014 IEEE Frontiers in Education Conference (FIE) Proceedings, Madrid, 2014, pp. 1-4, doi: 10.1109/FIE.2014.7044343.

[9] D. Lal N, B. Ghorbani, and S. Vaghri, “A SURVEY ON THE USE OF GNS3 FOR VIRTUALIZING COMPUTER NETWORKS.”

[10] R. Emiliano and M. Antunes, "Automatic network configuration in virtualized environment using GNS3," 2015 10th International Conference on Computer Science & Education (ICCSE), Cambridge, 2015, pp. 25-30, doi: 10.1109/ICCSE.2015.7250212.

[11] M. Steve, K. Baker, and M. Vega-Herrera, “A Comparison of Network Simulation and Emulation Virtualization Tools.”

[12] “Juniper releases barrage of security fixes for security, networking devices,” Help Net Security, 11-Jan-2019. [Online]. Available: https://www.helpnetsecurity.com/2019/01/11/juniper-security-updates/#:~:text=The%20batch%20of%20fixed%20Juniper. [Accessed: 28-Aug-2020].

[13] “Arista Networks Recent Data Breaches and Security Report,” www.upguard.com. [Online]. Available: https://www.upguard.com/security-report/arista . [Accessed: 28-Aug-2020].

[14] M. Cooney, “Cisco issues critical security warnings its Data Center Network Manager,” Network World, 03-Jan-2020.[Online].Available:https://www.networkworld.com/article/3512041/cisco-issues-critical-security-warnings-its-data-center-network-manager.html . [Accessed: 28-Aug-2020].