Virtual Router Cisco Performance Analysis on QEMU Hypervisor with Mechanism of Increasing the Number of Routers and Traffic Loads

Allysa Larasati [1], Doan Perdana [2], Gustommy Bisono [3]

School of Electrical Engineering
Telkom University
Bandung, Indonesia.

[1] allysalarasati@students.telkomuniversity.ac.id,
[2] doan.perdana@telkomuniversity.ac.id,
[3] gustommybisono@telkomuniversity.ac.id

Abstract - **Network Function Virtualization, NFV, aims to accelerate the implementation of new network services to support business strategies and revenue growth for the telecommunications sector in particular. In general, NFV aims to replace the function of the existing physical router device into a virtual router device and can be run on any virtualization server. In this study, a combination of Cisco virtual routers are tested on a virtualization platform for: throughput, packet loss, jitter and scalability as additional network hops. The virtualization platform used is a type 2 hypervisor, QEMU (Quick EMUlator), because it is open source and widely used in both educational and enterprise environments. Our results show: i) throughput increases with traffic volume, ii) link speed between host and router has a maximum rate of 1000 Mbps and a maximum recorded throughput of 778.6 Mbps, iii) the jitter parameter test ranged between 0.026 ms to 0.098 ms and met Cisco standards, iv) packet loss parameter was < 1%, v) the packets lost ranged from 0% to 2,471% caused by virtual links created by qemu and the virtual network interface cards, vi) for scalability, the more network hops the lower the performance.**

Keywords - Virtualization, Hypervisor, Network Function Virtualization, QEMU

I. INTRODUCTION

Along with the times, technology also evolved over time, including the very rapid development in the telecommunications industry in Indonesia. This development is inevitable and made the previous one in the form of hardware devices converted into software tools and still have the same function. In addition, this makes the operating system that normally runs in hardware turns into an operating system that runs virtually. And raises a new paradigm in the field of networking, namely Network Function Virtualization (NFV).

NFV is a concept of network architecture that uses virtualization technology that virtualizes all network nodes into building blocks that can be connected to create communication services. The NFV Framework based on the European Telecommunications Standards Institute (ETSI) standard has a definition that is a virtualized, software only entity in the form of a Virtualized Network Function (VNF) that runs on virtual resources created by virtualization layers of a collection of physical devices that form NFV Infrastructure (NFVI) [1].

So far there is no NFV Framework that forms a unified function as a virtualization layer provider and is able to manage all running VNFs. Therefore, to simulate the NFV Framework in accordance with ETSI standards there are several components needed, namely the server as a physical device, the hypervisor as a provider of virtualization layer,

virtual router images as VNF. The server now, can be in physical form or virtual server provided by many cloud providers such as Google Cloud, Digital Ocean, and others.
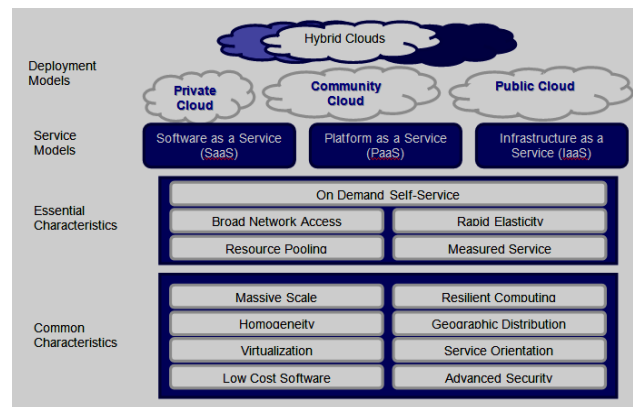

Fig. 1. Cloud Computing according to NIST

Based on research conducted by the market research company NPD Group, explained that Cisco dominates the sale of hyper-converged infrastructure or IT software based on software defined and virtualizes all elements of conventional "hardware" systems [2]. Cisco has also issued several virtual routers such as CSR, IOSXR and others. Cisco CSR is one option that can be used to run on a hypervisor with a 10Gbps license.

Based on the research conducted by Xiao Xiao Bian in the paper "Implement a Virtual Development Platform Based on QEMU" explained that QEMU is a fast and portable hypervisor that can accelerate the deployment process [3]. QEMU is expected to run and show good performance in simulating Cisco CSR.

II. BASIC THEORY

A. Cloud Computing

Not something new if we hear about cloud computing in the digital era like this. Cloud computing is often defined as a cloud when we draw an internet network diagram. In general, cloud computing is always associated with virtualization, because all components in cloud computing are virtual. Cloud computing is a model consisting of applications, platforms, and infrastructure that is packaged in cyberspace or the internet where there are services that can be accessed by users / clients as needed such as Software as a service (SaaS), Platform as a Service (PaaS), Infrastructure as A Service (IaaS)[4].

According to the National Institute of Standards and Technology (NIST) cloud computing is a form of service that opens opportunities to be present anywhere, provides convenience, on-demand network access to configurable computing resources, which can be quickly implemented and launched, with minimal management efforts or by using a service provider [5]. The following are 3 service models according to the National Institute of Standards and Technology (NIST):

A1. Infrastructure as a Service (IaaS): IaaS is an IT infrastructure service provided by cloud computing to clients such as storage, memory, processing power, networking components, dbs. This service is assumed as the client hires a virtual server computer whose specifications can be changed easily according to client requirements. Clients are allowed to install the operating system, storage, create firewalls and load balancers as needed and clients can build their own applications as desired.

A2. Platform as a Service (PaaS): Clients can develop applications using application frameworks or application engines extensively and can control these applications. But it cannot control the operating system, hardware, or network.

A3. Software as a Service (SaaS): The client can use the application but cannot create an application, cannot control the operating system, hardware, and network. Applications can be accessed via Web-browser or Web-based interface.

B. Network Function Virtualization, NFV

It is not new if bringing a new service to the network becomes increasingly difficult due to the nature of existing proprietary hardware, and the lack of professionals to integrate services. The concept of **NFV (Network Functions Virtualization**) can be proposed to overcome this problem. NFV changes the way network operators design their infrastructure by utilizing virtualization technology that separates software from hardware platforms for networks that provide faster services [9]. In operator networks, generally every network function is usually run by a software with hardware. Software and hardware in its application are intentionally made to be inseparable and depend on each other. Virtualization can design flexible software. Because NFV can run separately with the hardware. And NFV can be run simultaneously.
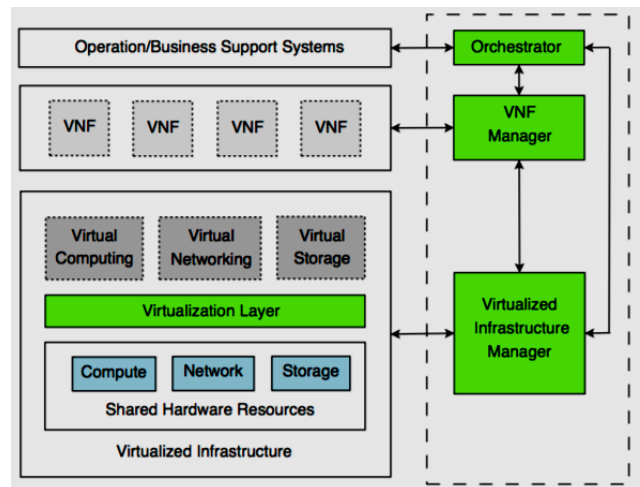

Fig. 2. NFV Architecture [7]

NFV is a concept that was raised to make network functions that can be implemented entirely in software, and then to run on industry-standard hardware. In general, industry-standard hardware points to public servers (e.g. Intel x86) available on the market along with their features (e.g. Ethernet standard switches). With this concept, a network function (e.g. Session Border Controller) can be distributed to operators (only) as software. What this operator needs to do, is just doing the installation procedure on their datacenter infrastructure (just with a standard e.g. rack-mounted / blade-server device that is connected to an Ethernet switch) [6].

B1. The Advantages of NFV:

- Flexible, extensible
- High asset utility
- Can carry out continuous processes (deploy, upgrade)
- Separate / eliminate NF dependence on proprietary devices
- Pure network software (NF) function
- Uses standard virtualization technology
- Can run on commodity / industry-standard hardware

C. Hypervisor

Hypervisor is a foundation for special virtualization or software that causes various operating systems to run simultaneously on a computer. Hypervisor or commonly referred to as Virtual Machine Monitor (VMM)[8]. In general there are two types of hypervisor, first type or Type 1 and second type or Type 2.

Type 1: This type is also called bare-metal architecture, a hypervisor that runs directly on the server hardware used to control and manage user hardware and does not require an OS to run it. Included in this type of hypervisor are IBM LPAR (PR / SM), Citrix XenServer, Xen Cloud Platform, VMWare ESX / ESXi.

Type 2: Hypervisor Type 2 is also called Hosted Architecture, a hypervisor that is installed on the operating system used on the server, so the type 2 hypervisor is in the second layer. Included in this type of hypervisor are VMware GSX Server / Workstation, VirtualBox, VritualPC, KVM.
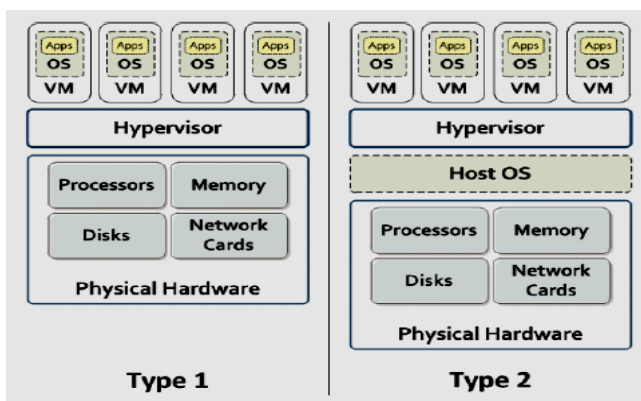

Fig. 3. Hypervisor Type 1 (Left) and Type 2 (Right)

D. QEMU Hypervisor

QEMU is included in the type 2 hypervisor and must run an operating system. QEMU is an emulator engine that is open source, and has two operating modes, that is system mode emulation and user mode emulation.

E. Cisco CSR 1000V

The Cisco Cloud Services Router (CSR) 1000V is a router in virtual form intended for deployment in a cloud data center. Using industry-leading Cisco IOS® Software networks and security features, CSR 1000V enables companies to transparently expand their WAN to external cloud providers and cloud providers hosted to offer enterprise-class network services [11].

F. UDP and TCP

F1. UDP: UDP is a very simple protocol with a minimum overhead, if a process needs to send a message that is relatively small and does not put too much importance on reliability, it is appropriate to use UDP [12]. Sending small messages using UDP requires less interaction between the sender and recipient than when using TCP or SCTP.

F2. TCP: Transmission Control Protocol (TCP) is a type of protocol that allows a collection of computers to communicate and exchange data within a network. TCP is a protocol in the transport layer (seven layers of the OSI reference model) that is connection-oriented and reliable [13].

F3. Iperf: Iperf is software that functions to measure bandwidth and service quality of a network. so that measurement can be done, the iperf is installed point to point, either on the server or client side. Iperf itself can be used to measure performance links from both TCP and UDP [14].

III. SYSTEM DESIGN AND IMPLEMENTATION
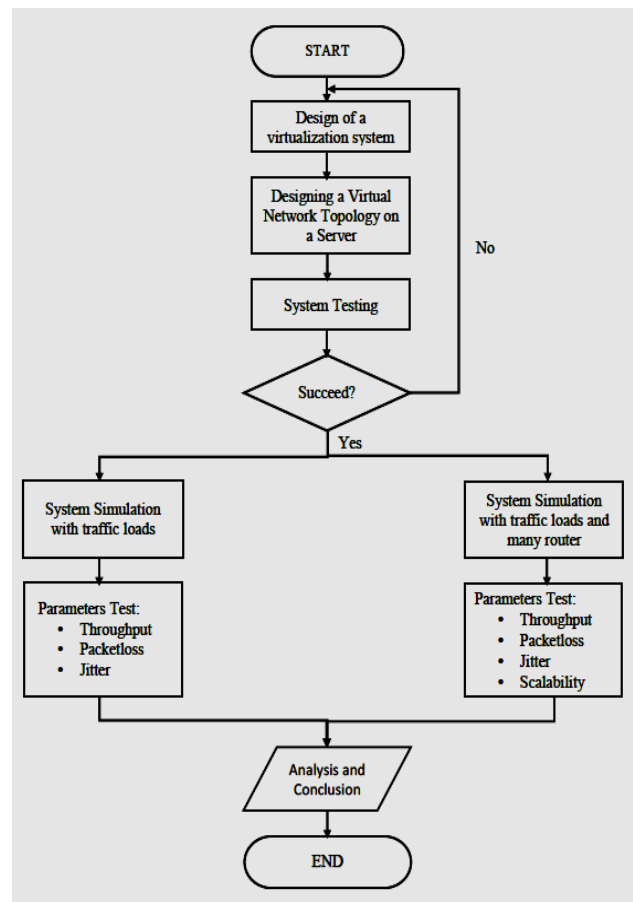
A. Flowchart System

Fig. 4. Flowchart System

In Figure 4 describes the design of a virtual system on a virtual platform using the QEMU hypervisor. In this virtual system the scenario that will be done is to design the virtual system and then combine it with the topology. In the topology there is a host server, client host and Cisco Vrouter.

B. Implementation Support Needs

The need to support this design is divided into two types, namely hardware and software.

B1. User: In the implementation of this final project, one user runs the hypervisor manager application with the following specifications:

TABLE I. USER SPECIFICATIONS

Spesifikasi	User
Processor	Intel Core i5
RAM	8 GB
Storage	250 GB
speed	1.6 GHz

B2. Server: In the implementation of this final project, one server from Google Cloud will be used to run the hypervisor and web manager with the following specifications:

TABLE II: SERVER SPECIFICATIONS

Spesifikasi	Server
Processor	Intel Xeon Kabylake 8 Cores
RAM	32 GB
Storage	500 GB

3. Ubuntu 16.04.
4. Cisco CSR 1000V Virtual Router + license 10Gbps.
5. QEMU as a Hypervisor.
6. EVE-NG as QEMU web manager.
7. iperf and iperf3

C. Designing a Virtualization System

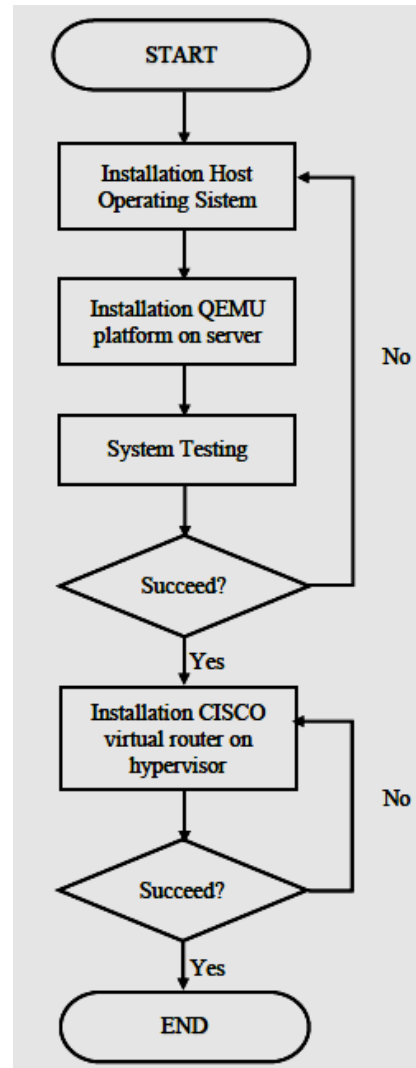The design process is shown in figure 5.

Fig. 5. Designing a Virtualization System
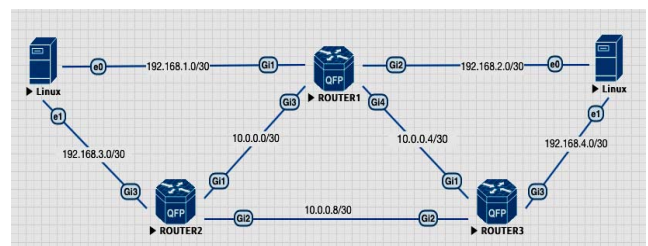
D. System Topology

Fig. 6. System Topology

In this final project the system topology consists of a virtual server, virtual environment, and 2 hosts. The sender host device is connected in real time with a virtual router, and in it there are virtual router devices and virtual hosts. Host sender is used to run the hypervisor manager application and retrieve data.

2.4

IV. ANALYSIS AND RESULTS

This chapter discusses the analysis of the test results with predetermined scenarios and parameters, by implementing Cisco VRouter on the Qemu hypervisor. The Ubuntu 16.04 operating system is used as the operating system host to run tests on the Qemu hypervisor. Testing using iperf and iperf3 applications with the parameters tested are throughput, packet loss, jitter and scalability. Tests on the parameters of throughput, packet loss, and jitter are tested by running Cisco VRouter and two hosts as recipients and senders of packets that are streamed to Cisco VRouter. Scalability parameters are tested in the same way except that the addition of Cisco VRouter in each test is done. Scalability testing is carried out up to a maximum of three VNF due to limited resources from the server used. Each test is carried out 30 times of data collection and the average is taken.

A. Throughput, Jitter, and Packetloss Testing

This test uses two hosts as a server and client to stream traffic and one vRouter as a link between the two hosts.
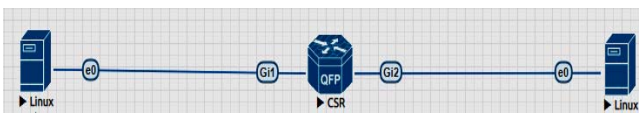

Fig. 7. Test Topology Throughput, Jitter, and Packetloss

The iperf tools work by flowing traffic in accordance with the bandwidth desired by the user so that for testing throughput, jitter, and packet loss has a large amount of traffic flowed from 100 Mb to 1000 Mb at intervals of 100 Mb. This is based on the ability of the vNIC hypervisor link which has a maximum link capacity of 1000 Mbps or commonly called Gigabit Ethernet. Each test is obtained by flowing TCP and UDP traffic from one host to another through Cisco vRouter for 30 attempts every second.
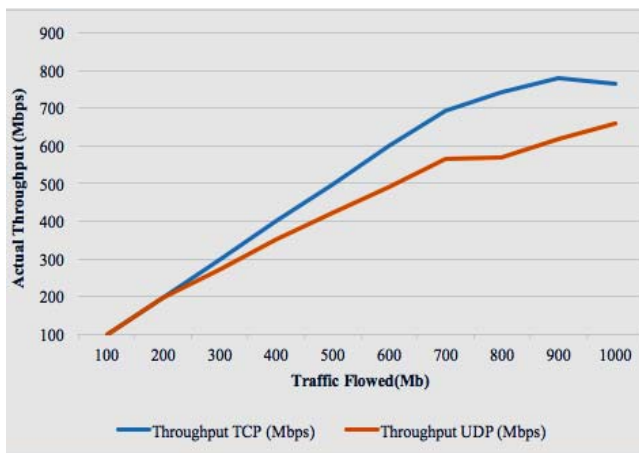
A1. Throughput

Fig. 8. Graph of throughput testing results

TABLE III: TABLE OF THROUGHPUT TESTING RESULT

Taffic (MB)	Throughput TCP (Mbps)	Throughput UDP (Mbps)
100	99.810	99.983
200	199.100	198.833
300	299.333	274.100
400	399.133	350.433
500	498.733	424.300
600	599.167	490.333
700	694.233	567.200
800	740.867	570.600
900	778.600	618.533
1000	766.633	657.833

In Fig 8, it can be seen that throughput has increased according to the amount of traffic flowed. The maximum link between host and router has a maximum capacity of 1000 Mbps with the maximum throughput recorded is 778.6 Mbps. The limited throughput is caused by the features of the hypervisor, the ability of vCPU to process data, and the ability of Cisco VRouter software in data buffering. Throughput can be increased by applying the interface bonding mechanism or combining two or more different links on the host and router, but Cisco VRouter does not support these features so that the mechanism cannot be applied.
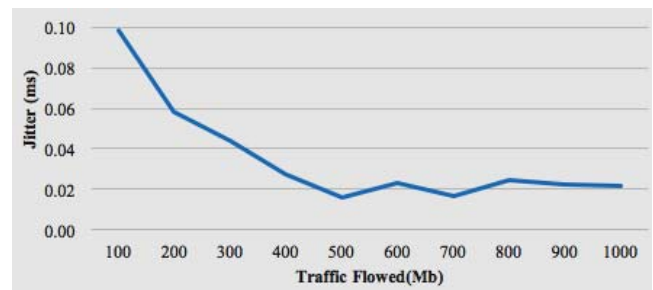
A2. Jitter

Fig. 9. Graph of Jitter testing results

TABLE IV: TABLE OF JITTER TESTING RESULT

Traffic (MB)	Jitter (ms)
100	0.098
200	0.057
300	0.043
400	0.040
500	0.031
600	0.037
700	0.036
800	0.026
900	0.041
1000	0.027

In Figure (4.3) 9, jitter varies with a range of values between 0.026 ms - 0.098 ms. Based on the jitter standard determined by Cisco, the jitter value that can be calculated is jitter <30 ms. Thus, the test jitter value meets the standards set by Cisco and is feasible to run various services such as online gaming, VoIP, and real time video streaming services.
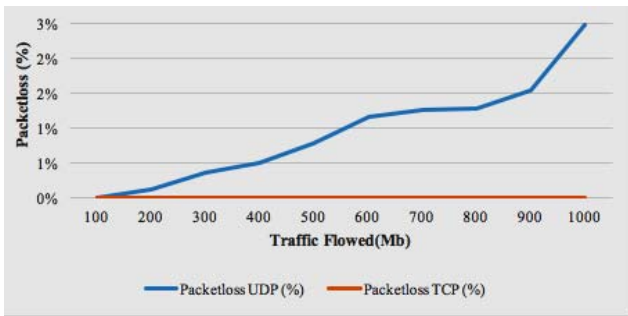
A3. Packetloss

Fig. 10. Graph of Packetloss testing results

TABLE IV: TABLE OF PACKETLOSS TESTING RESULT

Traffic (MB)	Packetloss TCP (%)	Packetloss UDP (%)
100	0	0.000%
200	0	0.121%
300	0	0.374%
400	0	0.500%
500	0	0.790%
600	0	1.160%
700	0	1.262%
800	0	1.288%
900	0	1.541%
1000	0	2.471%

Based on the standards specified by Cisco, the packet loss value that can be received to run various services is <1%. If you see the packetloss test results in table IV, the packet loss value ranges from 0% - 2,471%. This can be caused by the ability of a virtual network interface card (vNIC) on a bad Qemu hypervisor, or a virtual link between a bad vNIC and causing very high packet loss.

B. Network Scalability Testing

This test is intended to test the quality of the Cisco vRouter network when there is an increase in hop or the number of vRouter on the network. The parameters that are specified are throughput, jitter, and packet loss that will be compared when running one vRouter, two vRouter, and three vRouter with the topology in Figure 11 (4.5). The testing scheme for the two vRouter and the three vRouter is done the same as the test on one vRouter.
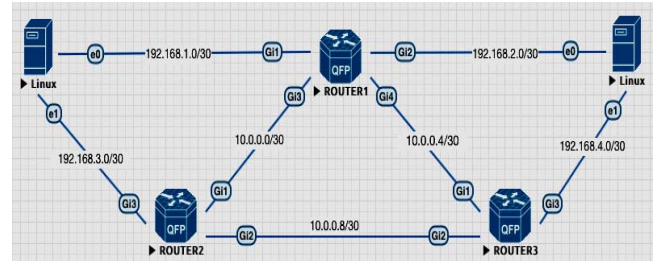

Fig. 11. Network scalability testing topology

B1. Throughput Testing of the Number of Routers

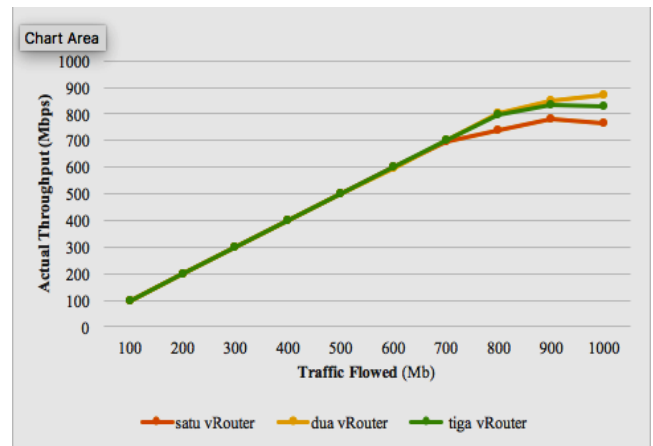Fig. 12. Graph of TCP throughput testing results on the number of routers

Based on the results of testing TCP throughput, there is no decrease in throughput results even though the number of hops increases on the network. In addition, there is a maximum increase in throughput when two vRouter and three much different when one vRouter is run.

Fig. 13. Graph of UDP throughput testing results on the number of routers

TABLE V: TABLE OF UDP THROUGHPUT TESTING RESULTS ON
THE NUMBER OF ROUTERS

Traffic (Mb)	1 vRouter (Mbps)	2 vRouter (Mbps)	3 vRouter (Mbps)
100	99.983	99.937	99.970
200	198.833	196.900	196.800
300	274.100	267.233	270.167
400	350.433	339.367	346.733
500	424.300	401.700	420.933
600	490.333	471.400	478.867
700	567.200	522.933	552.267
800	570.600	575.567	596.933
900	618. 533	601.900	618.800
1000	657.833	647.200	620.600

Based on the results of the UDP Throughput test, the resulting pattern is similar to the TCP Throughput testing, that is there is no significant decrease in results even though the number of hops increases. The maximum throughput value is 657,833 Mbps. This shows that, although the link capacity provided by the vNIC hypervisor is 1 Gbps, the resulting throughput is unable to reach or approach its ideal maximum capacity on both the TCP and UDP protocols. Many factors can cause this to happen, one of which is the limited ability of vNIC from Qemu and is unable to produce maximum throughput. There is no significant degradation in this parameter. Therefore, throughput is not degraded if the number of hops on the network increases to three routers. Of course, the results will be different if the addition is done by more than three routers.

B2. Jitter Testing of the Number of Routers

TABLE V. TABLE OF TCP THROUGHPUT TESTING RESULTS ON
THE NUMBER OF ROUTERS

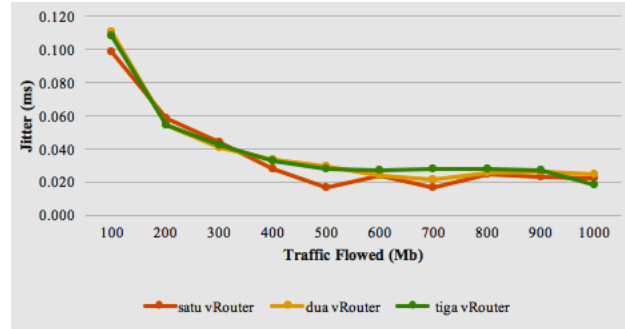| Traffic (Mb)	1 vRouter (Mbps)	2 vRouter (Mbps)	3 vRouter (Mbps)
100	99.810	99.773	99.773
200	199.100	199.100	199.100
300	299.333	299.200	299.333
400	399.133	400.067	398.933
500	498.733	499.600	499.833
600	599.167	598.033	599.733
700	694.233	698.967	699.700
800	740.867	799.567	799.267
900	778.600	849.133	835.233
1000	766.633	873.133	829.267

Fig. 14. Graph of Jitter testing results on the number of routers

TABLE VI. TABLE OF JITTER TESTING RESULTS ON THE NUMBER
OF ROUTERS

Traffic (Mb)	1 vRouter (ms)	2 vRouter (ms)	3 vRouter (ms)
100	0.099	0.111	0.108
200	0.058	0.054	0.054
300	0.044	0.041	0.042
400	0.027	0.033	0.032
500	0.016	0.029	0.028
600	0.023	0.024	0.027
700	0.017	0.021	0.028
800	0.025	0.025	0.027
900	0.023	0.026	0.027
1000	0.022	0.024	0.018

In figure 15 (4.8), the jitter value is maintained and meets Cisco standards which is below < 30ms even though there is an additional number of hops on the network. One factor that causes the jitter value not to be affected is the absence of transmission loss that only occurs when the link uses electrical cables or optical cables such as damping and bending. The jitter parameter is the most stable parameter of the results and is very good. Although there are additional hops or routers, the jitter value remains good and is not affected by the addition of the hop.
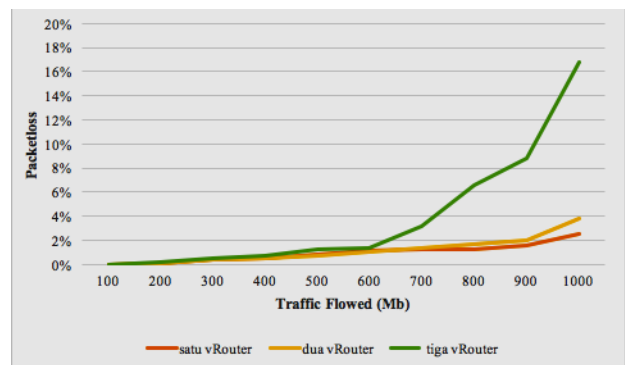
B3. Packetloss Testing of the Number of Routers

Fig. 15. Graph of Packetloss testing results on the number of routers

TABLE VII. TABLE OF PACKETLOSS TESTING RESULTS ON THE NUMBER OF ROUTERS

Traffic (Mb)	1 vRouter	2 vRouter	3 vRouter
100	0.000%	0.004%	0.000%
200	0.121%	0.104%	0.153%
300	0.374%	0.345%	0.451%
400	0.500%	0.550%	0.684%
500	0.790%	0.756%	1.228%
600	1.160%	1.055%	1.375%
700	1.262%	1.306%	3.122%
800	1.288%	1.689%	6.607%
900	1.541%	2.026%	8.827%
1000	2.471%	3.798%	16.803%

Based on the results of packet loss testing on the number of hops shown in the figure and table above, there is a very high packet loss value when three vRouters are executed or when the network has a number of three hops. This can occur due to congestion on one of the links between the three hops. One way that can be done to reduce packet loss is by increasing the link capacity of each hop, but this cannot be done due to the limited features of Qemu.

V. CONCLUSION

We conclude that with a maximum ideal link of 1000 Mbps the maximum throughput is 778.6 Mbps. Moreover, the results of testing the jitter parameters, the results are obtained between a range of 0.026 ms. 0.098 ms and meet the standards specified by Cisco that is <30ms jitter. Based on the results of the package parameter test results obtained with a range between 0% s.d. 2.471% and has not met the standard set by Cisco, with the packet loss <1%. This is due to the ability of virtual devices from QEMU. Meanwhile, according to the results of scalability testing with the addition of the number of hop networks, there is a decrease or degradation of the greatest performance in packet loss parameters.

REFERENCES

[1] Thekkedath, Balamurali., 2013. Network Function Virtualization For Dummies.

[2] https://www.crn.com/slide-shows/virtualization/ 300086946/the-top-6-hyper-converged-infrastructure-brands-of-q1-2017.htm/3

[3] X. Bian, "Implement a Virtual Development Platform Based on QEMU," 2017 International Conference on Green Informatics (ICGI), Fuzhou, 2017, pp. 93-97.

[4] Sofana, I., 2012. Cloud Computing Teori dan Praktik. Bandung, Informatika.

[5] Mell, P. and Grance, T., 2009. Draft nist working definition of cloud computing-v15. 21. Aug 2009, 2, pp.123-135

[6] Han, B., Gopalakrishnan, V., Ji, L. and Lee, S., 2015. Network function virtualization: Challenges and opportunities for innovations. IEEE Communications Magazine, 53(2), pp.90-97.

[7] Eueung Mulyana. "Buku Komunitas SDN-RG". Bandung. Published by GitBook

[8] Ajimangun Lintang Mas. Perancangan Dan Analisis Performansi Layanan Iaas Pada Private Cloud Dengan Cloud Platform Cloudstack, 2013.

[9] European Telecommunications Standards Institute. 2013. Network Functions Virtualisation (NFV); Use Cases. GS NFV 001 (V1.1.1).

[10] http://www.qemu.org/

[11] https://www.cisco.com/c/en/us/products/routers/ cloud-services-router-1000v-series/index.html#~stickynav=2

[12] I. Sofana, Cisco CCNA & Jaringan Komputer, Bandung: Informatika, 20

[13] Putra, M.A.P., Perdana, D., Negara, R.M., Performance analysis of data traffic offload scheme on Long Term Evolution (LTE) and IEEE 802.11AH, Telkomnika (Telecommunication Computing Electronics and Control) , 2017.

[14] Riski Muktiarto, N.A., Perdana, D., Negara, R.M., Performance analysis of mobility impact on IEEE 802.11ah standard with traffic pattern scheme, International Journal of Communication Networks and Information Security, 2018.

.