POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.org.tr/politeknik

SDN based management platform for intranet services

Yazar(lar) (Author(s)): *Mehmet ÖZDEM[1], Mustafa ALKAN[2]*

ORCID[1]: 0000-0002-2901-2342

ORCID[2]: 0000-0002-8503-9697

Bu makaleye şu şekilde atıfta bulunabilirsiniz(To cite to this article): Özdem M. and Alkan M., "SDN based management platform for intranet services", ***Journal of Polytechnic***, 24(3): 989-995, (2021).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: 10.2339/politeknik.777837

SDN Based Management Platform for Intranet Services

Highlights

- *Open network operating system (ONOS) based software defined network (SDN) platform is developed.*
- *Dynamic VLAN management that can be configured centrally (independent of end devices) is realized.*
- *Central and dynamic bandwidth management is demonstrated as part of the developed platform.*
- *Dynamic access management without an additional security device is performed.*
- *The proposed solution has been tested on a live network.*

Graphical Abstract

Telecom operators experience difficulties in applications such as virtual local area network (VLAN) management, bandwidth management and access management while providing intranet services in traditional networks. In this study, ONOS based SDN platform is developed for intranet services in order to address these problems.

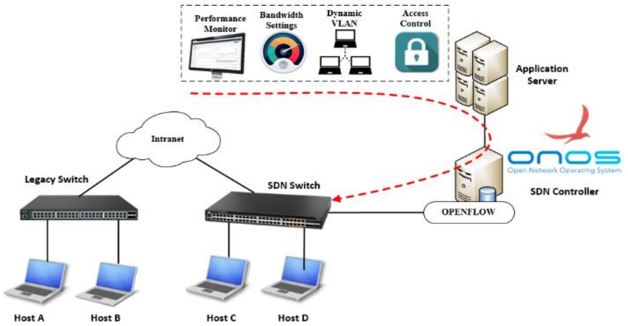

Figure. Demonstration of ONOS based SDN solution with intranet service

Aim

The aim of this study is to show that the SDN platform offers a good alternative to traditional solutions in large-scale intranet networks.

Design & Methodology

In this study, an ONOS based SDN platform, designed for corporate networks to solve the problems of the intranet infrastructure is integrated to the intranet infrastructure of a corporate network. The proposed solution has been tested on a live network. In order to measure the performance of the proposed platform, varying number of traffic flows are created simultaneously so as to compare their performances under varying traffic load. The performance of the proposed ONOS based SDN platform that we have developed is compared with the traditional intranet network.

Originality

None of works considered how to apply SDN paradigm to the intranet network to introduce flexibility and agility to network control. This study differentiates from the existing studies such that an ONOS based SDN platform has been developed and applied to a live intranet network.

Findings

The performance results are approximately equal in both the proposed and the traditional architectures under various traffic load as can be observed from the latency, jitter and packet loss.

Conclusion

The proposed SDN platform provides a good alternative to traditional solutions in large scale intranet networks, minimizing the workload spent by the operators in controlling the network, while achieving cost savings and eliminating vendor dependency. Moreover, performance tests assure that the proposed system behaves stable under various traffic loads and scales well

Declaration of Ethical Standards

The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

SDN Based Management Platform for Intranet Services

Araştırma Makalesi/Research Article

Mehmet ÖZDEM*, Mustafa ALKAN

Faculty of Technology, Electrical and Electronics Engineering Department, Gazi University, Turkey

(Received : 07.08.2020 ; Accepted : 25.08.2020 ; Erken Görünüm/Early View : 26.08.2020)

ABSTRACT

Telecom operators experience difficulties in applications such as virtual local area network (VLAN) management, bandwidth management and access management while providing intranet services in traditional networks. In this study, open network operating system (ONOS) based software defined network (SDN) platform is developed for intranet services in order to address these problems. The developed platform has been integrated onto an existing network and a new topology has been created. In this proposed topology, intranet network elements are connected to the new generation SDN switches instead of the legacy switches. The proposed solution has been tested on a live network. According to test results where the proposed SDN platform is compared with the traditional intranet network in a live network scenario under varying traffic load, the SDN based platform achieved very successful results in terms of latency, jitter, packet loss and flow setup times. Overall, the proposed SDN platform provides a good alternative to traditional solutions in large scale intranet networks, minimizing the workload spent by the operators in controlling the network, while achieving cost savings and eliminating vendor dependency.

Keywords: Intranet services, SDN, ONOS, performance analysis.

1. INTRODUCTION

Traditional telecom services highly depend on the physical infrastructures and vendor proprietary hardware. SDN technology is designed to break these types of dependencies, by changing the way networks are built and managed. SDN refers to the concept of separating the control and data planes in the network and defining an open application programming interface (API) between them, of which the OpenFlow protocol is the most prominent example [1]. Thus, SDN control plane directly controls the data plane elements of network like routers, switches, and middle boxes; and the SDN paradigm is becoming more popular in developing network applications that can control the network.

Many tier 1 telecommunication industry vendors have already produced their own proprietary SDN controller solutions, such as Cisco's ACI, Juniper's Contrail, Big Switch's BNC, and Brocade's Vyatta Control. In addition, there are popular open source projects used for SDN research and development, which provide good alternatives to proprietary solutions [2, 3]:

- Opendaylight (ODL) by Linux Foundation [4]
- Open Network Operating System (ONOS) by Open Networking Foundation (ONF) – Initiated by Stanford and Berkeley Universities [5]
- Floodlight by Big Switch [6]
- OpenContrail by Juniper and others [7]

There are various studies on measuring the performance of open source SDN controllers. One of them is the study of performance measurement of the Floodlight SDN controller using mininet [8]. In another study, ODL and ONOS are architecturally analyzed and performance of them are compared [9], [10]. In addition to these, there is a study in which ONOS, ODL, Floodlight and Ryu controllers are compared for their performances by extending previous studies [11]. Yet in another study, popular SDN controllers including ONOS, ODL, and Ryu are evaluated for their performances using Cbench [12]. Finally, architectural guidelines are identified for SDN controllers and several controllers are compared for their performances on latency, thread scalability, throughput and switch scalability in [13].

However, none of these works considered how to apply SDN paradigm to the intranet network to introduce flexibility and agility to network control. This study differentiates from the existing studies such that an ONOS based SDN platform has been developed and applied to a live intranet network. We have also compared our solution to the traditional intranet network in terms of performance and functionality. More specifically, our contributions are listed as follows:

- We have designed an ONOS based SDN platform to manage intranet networks.
- We have determined three scenarios for applying our SDN platform to intranet network and made modifications in the ONOS code to realize these scenarios.
- We have applied our platform to a live intranet network and solved the problems faced in the setup by modifying the existing ONOS code.
- We have compared our SDN based platform with the legacy implementations in terms of performance and functionality.
- The test results justify that SDN can be utilized in controlling intranet networks so as to realize the selected scenarios in these networks, which are not possible in legacy solutions. The usability of SDN is

*Sorumlu yazar (Corresponding Author)
e-mail : mehmet.ozdem@gazi.edu.tr

not limited to these scenarios, which are detailed in Section 2, but can be extended further, which will be covered in the future work.

The organization of the paper is as follows: Section 2 describes the developed ONOS based SDN platform, together with the scenarios implemented to justify the solution. Experiments are detailed in Section 3, and then test results are given. Section 4 concludes the work.

2. ONOS BASED SDN PLATFORM

In this study, an ONOS based SDN platform, designed for corporate networks to solve the problems of the intranet infrastructure, is integrated to the intranet infrastructure of a corporate network. The platform introduces a new application method for policy-based VLAN management, dynamic bandwidth management and dynamic access control management.

Open source based SDN controller ONOS is used in this study, because it is designed to meet the requirements of service providers such as performance, high availability and scalability [14].

Three different scenarios are developed to enable the integration of intranet services such as wired internet, wireless internet and voice service with the developed platform. Features of the developed ONOS based SDN platform are;

- Policy-based dynamic VLAN management
- Policy-based bandwidth management
- Dynamic access management

2.1. Policy-Based Dynamic VLAN Management

In traditional networks, segmentation is usually provided by using VLAN-IDs. Therefore, for each end device that becomes a part of an existing network, a VLAN configuration has to be performed on a L2 switch. To move the end device to another location in the same network, similar definitions need to be done for the new switch port. Hence, it is evident that a serious operational work is needed when management of big networks is considered.

Instead of having static VLAN management on switches as performed in traditional networks, the proposed SDN solution defines a centralized, VLAN independent structure in the network, allowing dynamic management on policies. With the proposed solution, service activation and policies can be applied in real time.

The capture of some packets is presented in Figure-1 in order to better understand how VLAN management is done by using the ONOS based SDN platform. VLANs are assigned to clients according to the source IP addresses, as shown in Figure-1.

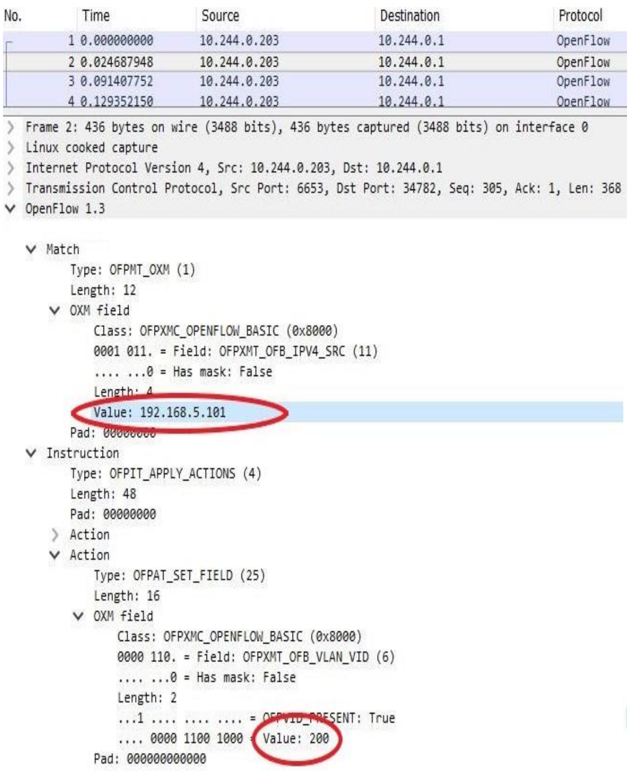

Figure 1. Screen shot of packet capture for VLAN management

2.2. Policy-Based Bandwidth Management

Applying a policy to manage bandwidth in traditional networks entails a lot of operational burden because of the user-based and static configurations on all active end devices. Therefore, it is difficult to update policies for constantly changing needs. In addition, each intervention on live network brings the risk of interruptions due to human error.

In the proposed ONOS based SDN platform, bandwidth policies are available to all end devices in the SDN network as soon as they are defined. While bandwidth policies become applicable in real time, there is no need for new configurations on network devices. An application can create flexible bandwidth policies regarding user and domain names. For instance, different bandwidth policies can be applied to Wi-Fi access points (AP) in the SDN controlled network without the need for an external Wi-Fi administrator. Allocating a certain amount of bandwidth to each intranet user or each intranet device allows efficient use of the network.

The capture of some packets is shown in Figure-2 to indicate how bandwidth management is done by using the ONOS based SDN platform. Bandwidth is assigned to the client according to the source IP address, as shown in Figure-2.

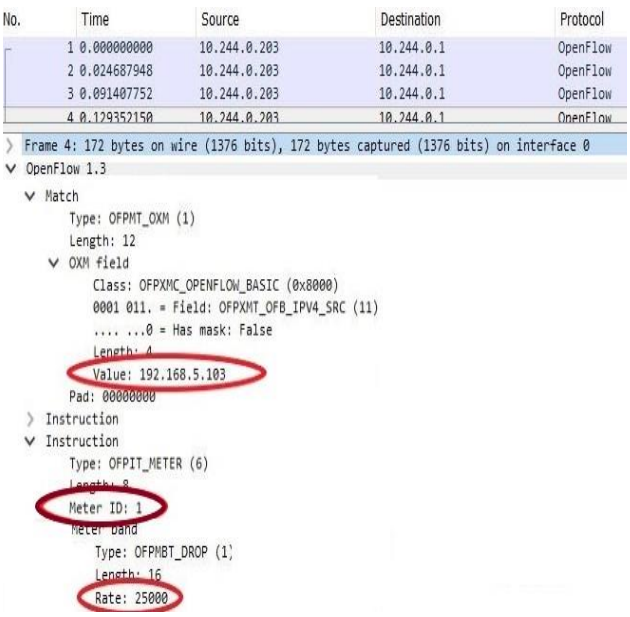

Figure 2. Screen shot of packet capture for bandwidth management

On the contrary of traditional networks where user-based bandwidth management can only be performed statically and manually on each device on the network, users of the proposed SDN solution can be defined centrally and their bandwidths can be dynamically managed without requiring static configuration on each device.

2.3. Dynamic Access Management

In traditional networks, cross-segment network access is controlled by firewall policies or access control lists (ACL). For this reason, it is not possible to control the access of end devices in the same network segment. Especially, denial of service (DoS) type attacks on end device cannot be prevented, so they may affect the other devices in the same network segment.

In the proposed ONOS based SDN platform, flows are handled according to the flow rules defined by the SDN controller, therefore the access of end devices are subject to the rules defined, irrelevant of the location of the devices. Policy rules and device accesses can be managed without being dependent to VLAN definitions. There are also MAC, IP or port-based access controls. It is important to provide access to third parties in intranet network. Connections to the network can be provided to enable this type of user authorization and detailed permission operations. Service levels and permission levels can also be changed dynamically.

The capture of some packets is shown in Figure-3 to indicate how access management is done by using the ONOS based SDN platform. As an example, access to a specific IP address is denied in Figure-3.

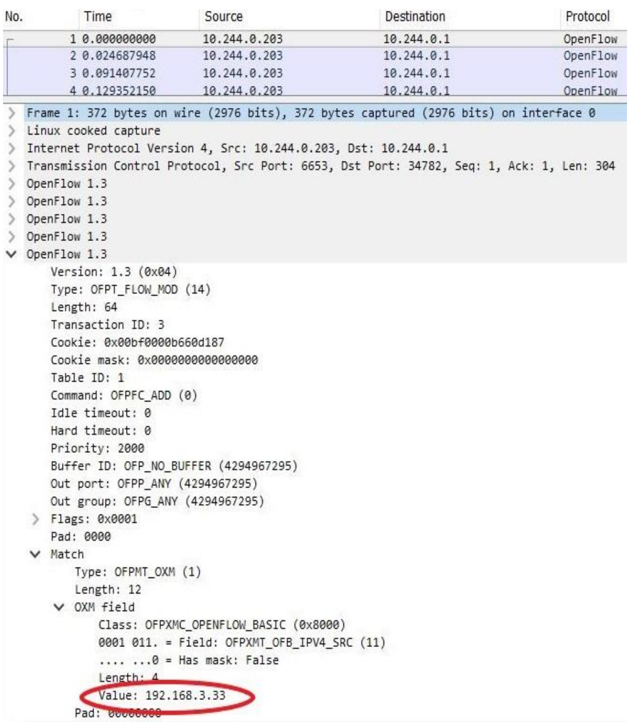

Figure 3. Screen shot of packet capture for access management

Dynamic access management features include access control in L2, L3, L4 layers, access blocking with domain name and dynamic configuration. In order to make these type of access blockings in a traditional network, a firewall has to be added. In this study, unlike traditional structures, instead of using an additional firewall, policies are determined centrally on the SDN controller. Thus, relevant access policies can be implemented across the entire intranet network, independent from the end devices.

2.4. System Architecture

Figure-4 shows the ONOS based SDN solution, which includes three main layers as shown in Figure-5. In the physical layer of the SDN network, the switches managed by the ONOS based SDN controller support the OpenFlow protocol. The main function of switches is to ensure the transmission of traffic to the end devices in the data plane in accordance with the flow rules defined by the SDN controller on the control plane. In the control layer, the SDN controller provides the management function through the OpenFlow protocol between the edge switches. SDN provides a solution where applications regarding control and data planes can easily be implemented via open and programmable interfaces. Different types of applications can be present on the application layer, such as dynamic VLAN assignment, bandwidth management, performance management, statistics display, as well as network access control (NAC).

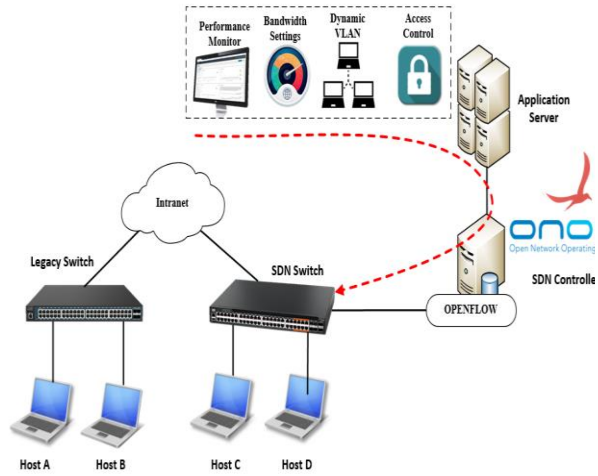

Figure 4. Demonstration of ONOS based SDN solution with intranet service

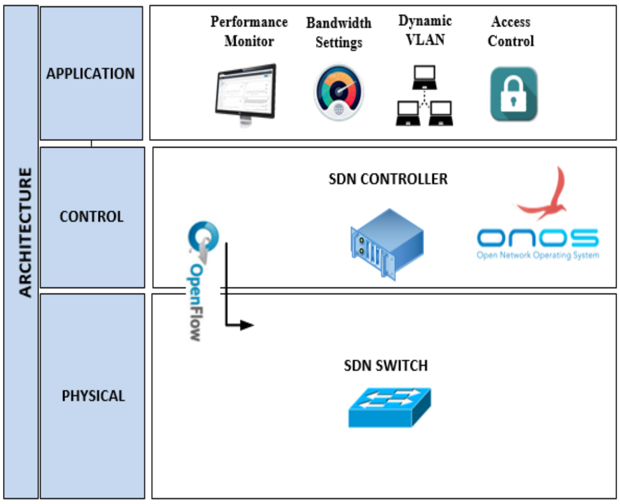

Figure 5. Architecture of ONOS based SDN solution with intranet service

This study is based on an open source SDN controller, ONOS, which is used to control the SDN enabled switches in the intranet network. ONOS is modified in the study, so as to solve the problems observed during the work, which are listed below:

- Problems in setting up flow rules for mobile hosts when the proposed platform is used together with the traditional solution and hosts move back and forth between these networks
- Problems in keep-alive flows between the IP Telephone and the Call Manager
- Problems in flows of the devices that are moved to a different port on the same switch
- Problems caused by broadcast ARP messages coming from traditional network, when the proposed platform is used together with the traditional solution and the ARP messages received overwrite host locations
- Problems caused by flows that are not deleted after removing an host connected to a legacy switch that is also connected to the SDN Switch

3. EXPERIMENTS

In this section, first the experimental setup is presented with functional description and details of the test scenario. After measurement procedure is defined, the results are presented, which show that the solution works as intended, and scales well under varying traffic loads.

3.1. Experimental Setup

Experimental setup for traditional intranet network is shown in Figure-6. This setup includes L2 switches, L3 aggregation switches, routers for internet access, dynamic host configuration protocol (DHCP) servers, firewalls (FW), wireless local area network controllers (WLC) and domain name server (DNS). On the L2 switches, there are end devices such as the computer, IP telephone, test probe, Iperf client, Iperf server and access point (AP) that make up the intranet.

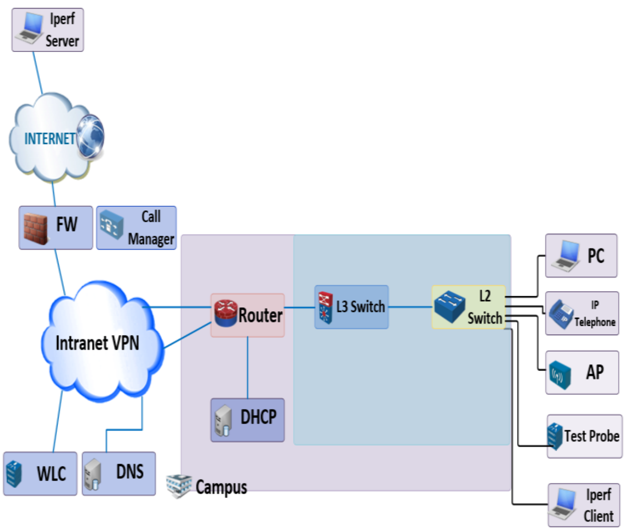

Figure 6. Experimental setup for traditional intranet network

Physical test topology of the developed SDN platform is demonstrated on Figure-7 and it can be observed that L2 switch is replaced by the SDN controller and SDN switch. This platform is integrated and installed on the live network. Devices such as computers, IP Telephones and access points are directly connected to SDN switch. Intranet services (wired internet, wireless internet, voice) provided with these devices are tested on live network. Service flow details can be observed in Figure-7.

The SDN controller is physically connected to the L3 switch. For wired internet service, the traffic from the computer reaches the internet after accessing through sequentially the switches, routers and then firewalls. IP phone, on the other hand, passes through switches and comes to the call manager equipment where the call is provisioned and managed. Finally, the traffic coming from the AP is directed to the wireless local area network controller and it reaches to the internet after it is managed by firewall. Control plane traffic, (signaling of all services), is centrally controlled by the SDN controller.

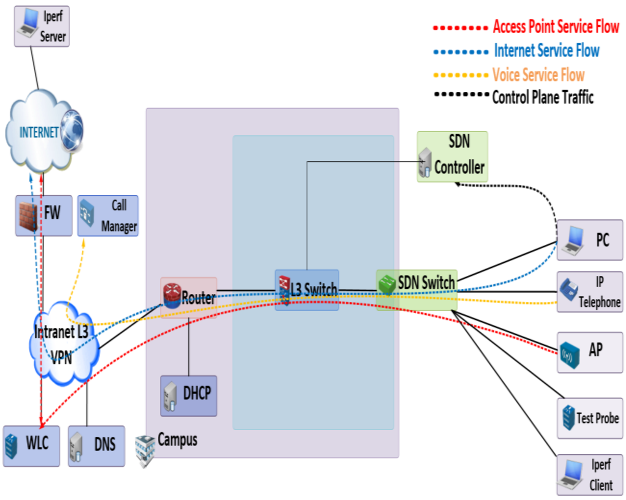

Figure 7. Experimental setup for developed intranet network

The elements used in the setup are shown in Table 1.

Table 1. Network equipment used in the setup and their features.

Network Equipment	Features
SDN Controller	• Xeon E5-2620 v4 2.1GHz,20M Cache,8.0GT/s QPI, Turbo • 1x 16GB DDR4 • 4x 1GE
SDN Switch	• 48 x 1GE • 4 x 10 Gigabit SFP+ • 16 Gbps switching capacity • 2 GB DDR3
L2 Switch	• 48 x 1GE • 4 x 10 Gigabit SFP+ • 16 Gbps switching capacity • 64 MB DRAM
L3 Switch	• 24 x 1GE • 12 x 10 Gigabit SFP+ • 32 Gbps switching capacity • 128 MB DRAM
Router	• 24 x 1GE • 16 x 10 Gigabit SFP+ • 1,8 Gbps Switching Capacity

	• 512 MB DRA
DHCP	• Windows DHCP Server
WLC	• Supports up to 500 access points • 8 x Gigabit SFP
DNS	• Windows DNS Server
Firewall	• Supports 10M concurrent sessions
Iperf client	• Generating flows by using Iperf tool
Iperf server	• Receiving flows by using Iperf tool
Test probe	• Measuring latency, jitter, packet loss

3.2. Measurement Procedure

In order to measure the performance of the proposed platform, varying number of traffic flows (i.e. 1000, 2000, 5000, 10000, and 20000) are created simultaneously using Iperf, each of which has lasted for 400 seconds. These flows are created between the Iperf server and client nodes, on the proposed platform as well as the traditional intranet so as to compare their performances under varying traffic load, as shown in Figure-6 and Figure-7. Performance measurements (latency, jitter, packet loss) are done by the test probe by sending ICMP packets to the Iperf server node.

In addition to that, flow setup time, which is defined as the duration between the reception of the first packet of the flow at the switch and the completion of the packet forwarding [15], is measured during the tests under varying traffic load. In order to measure this metric, the outgoing packet traffic from both the Iperf client and the SDN switch is captured and then compared to each other. The time difference between the outgoing packets of the Iperf client and the SDN switch determines the flow setup time.

3.3 Results

The performance of the proposed ONOS based SDN platform that we have developed is compared with the traditional intranet network, as described in the previous section. As can be observed from the latency, jitter and packet loss figures shown in Figure-8, Figure-9, and Figure-10, respectively, the performance results are approximately equal in both the proposed and the traditional architectures under various traffic load.

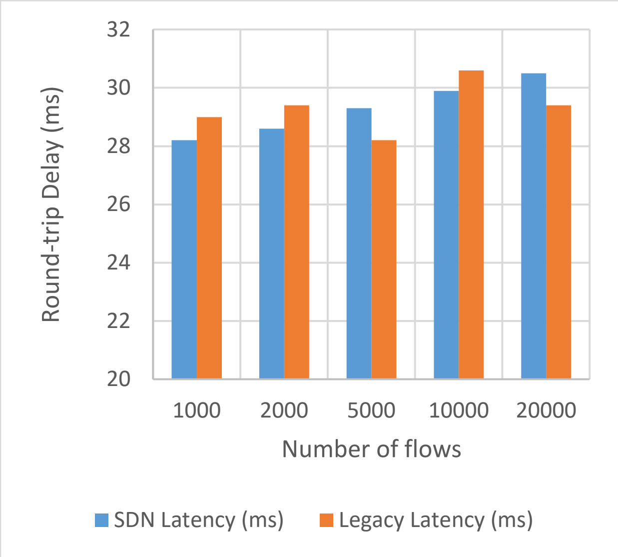

Figure 8. The performance comparisons between the proposed and traditional architectures (Latency)

Therefore, it is clear that the ONOS based SDN platform, in which open source components are utilized so as to realize a vendor independent low cost solution, can be used to control large scale intranet networks. The results justify that the proposed solution is a good alternative to traditional intranet networks, which are typically vendor dependent and have high cost.

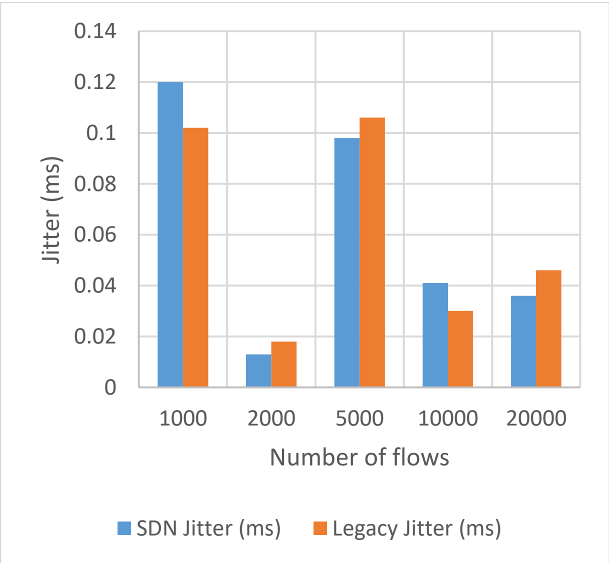

Figure 9. The performance comparisons between the proposed and traditional architectures (Jitter)

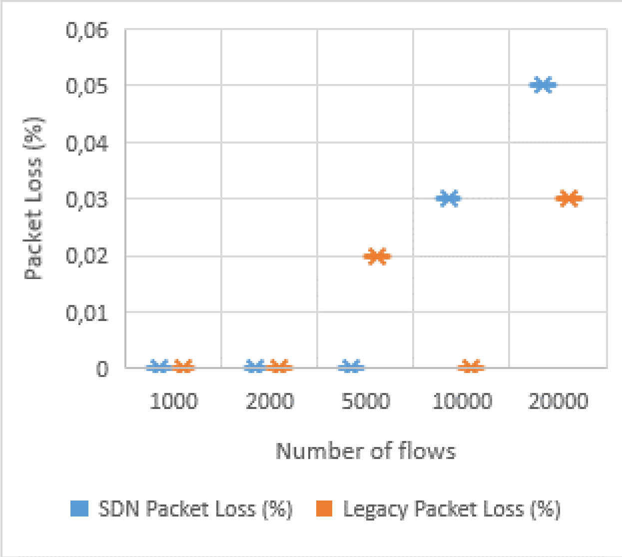

Figure 10. The per
formance comparisons between the proposed and traditional architectures (Packet Loss)

Average flow setup times, as measured for varying number of simultaneous flow, are depicted in Figure- 11. As can be noted from the values shown, the proposed platform scales well under heavy traffic, resulting in less than 250 ms of total flow setup time for 20000 simultaneous flows. Also, it can be calculated that the flow setup times per flow are between 8 and 14 microseconds.

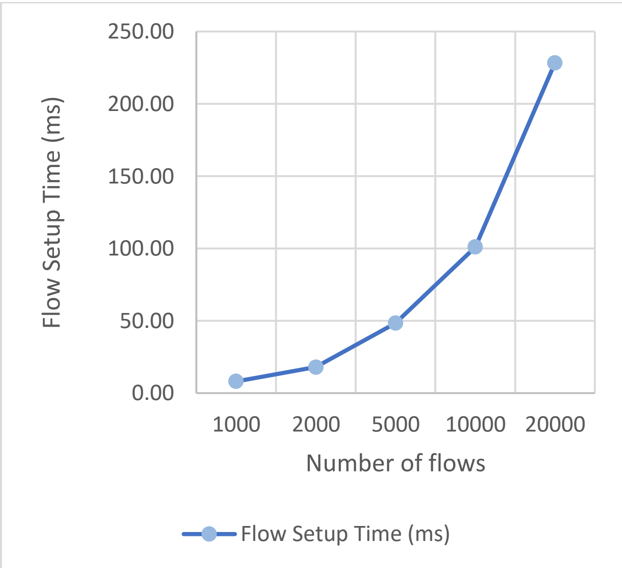

Figure 11. Flow setup times spent in setting up OpenFlow rules for simultaneous flows received

4. CONCLUSIONS

Nowadays, operators are having difficulties in managing their existing large-scale networks and intranet services running on these networks. Many network operations are performed manually, comprising vendor dependent high cost hardware. In this study, an ONOS based SDN platform is developed to solve these problems of operators. Thanks to the scenarios realized as part of the developed platform, the following features are supported and demonstrated:

- Dynamic VLAN management that can be configured centrally (independent of end devices)
- Central and dynamic bandwidth management
- Dynamic access management performed via ONOS controlled SDN switches without an additional security device

After comparing the performances of the traditional intranet network and the ONOS based SDN solution developed in this study, it became evident that the developed solution provided a good alternative to traditional solutions in large scale intranet networks. Moreover, performance tests assure that the proposed system behaves stable under various traffic loads and scales well. As a conclusion, by using the developed SDN platform in place of traditional solutions, it is possible to minimize the workload spent by the operators and therefore to reduce the required human effort significantly, while achieving cost savings and eliminating vendor dependency.

DECLARATION OF ETHICAL STANDARDS

The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

AUTHORS' CONTRIBUTIONS

Mehmet Özdem: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Supervision, Writing - Original Draft, Data Curation

Mustafa Alkan: Writing - Review & Editing, Visualization, Project administration

CONFLICT OF INTEREST

There is no conflict of interest in this study.

REFERENCES

[1] McKeown N., Anderson T., Balakrishnan H., Parulkar G., Peterson L., Rexford J., Shenker S., Turner J., "OpenFlow: Enabling innovation in campus networks", ***ACM SIGCOMM Computer Communication Review***, 38(2): 69-77, (2008).

[2] Bondkovskii A., Keeney J., van der Meer S., Weber S., "Qualitative comparison of open-source sdn controllers", ***IEEE Network Operations and Management Symposium***, 889-894, (2016).

[3] Koponen T., Casado M., Gude N., Stribling J., Poutievski L., Zhu M., Ramanathan R., Iwata Y., Inoue H., Hama T., Shenker S., "Onix: a distributed control platform for large-scale production networks", ***9th Usenix Symposium on Operating Systems Design and Implementation***, 351-364, (2010).

[4] Internet: Linux Foundation, The OpenDaylight Platform, https://www.opendaylight.org, 06.06.2020.

[5] Internet: Open Network Operating System (ONOS), https://wiki.onosproject.org/display/ONOS/Wiki+Home, 20.05.2020.

[6] Internet: https://sdxcentral.com/networking/sdn/definitions/what-is-floodlight-controller/, 15.07.2020.

[7] Internet: http://www.opencontrail.org/a-blueprint-for-building-the-opencontrail-community/, 18.07.2020.

[8] Abdullah T., "Testing of floodlight controller with mininet in SDN topology", ***ScienceRise***, 5 (2): 68-73, (2014).

[9] Yamei F., Qing L., Qi H., "Research and comparative analysis of performance test on SDN controller", ***2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI)***, 207-210, (2016).

[10] Suh D., Jang S., Han S., Pack S., Kim M. S., Kim T., Lim C. G., "Toward highly available and scalable software defined networks for service providers", ***IEEE Communications Magazine***, *55*(4):100-107, (2017).

[11] Mamushiane L., Lysko A., Dlamini S., "A comparative evaluation of the performance of popular SDN controllers", ***2018 Wireless Days (WD)***, 54-59, (2018).

[12] Salman O., Elhajj I. H., Kayssi A., Chehab A., "SDN controllers: A comparative study", ***Electrotechnical Conference (MELECON)***, 1-6, (2016).

[13] Shah S. A., Faiz J., Farooq M., Shafi A., Mehdi S. A., "An architectural evaluation of SDN controllers", ***IEEE International Conference on Communications (ICC)***, (2013).

[14] Leenheer M. De, Tofigh T., Parulkar G., "Open and programmable metro networks", ***Optical Fiber Communication Conference and Exhibition (OFC)***, Th1A.7, (2016).

[15] Kumari A., Chandra J., Sairam A. S., "Optimizing flow setup time in software defined network", ***10th International Conference on Communication Systems & Networks (COMSNETS)***, 543-545, (2018)