****

**KCA UNIVERSITY**

**BSD 2201 - NETWORK SCIENCE THEORY**

**ASSIGNMENT 1**

**KAMAU SAMUEL**

**19/02761**

SOFTWARE DEFINED NETWORKS

# Abstract

Networks are controlled by software applications which are called Software Defined Networking (SDN) controllers. Traditional network controllers are tedious and it is hard to manage old, rigid commands and consoles.

A key requirement of SDN is speed and automation which is not possible in traditional network controller. In a traditional network controller, we require a lot of administrative work. So it requires a lot of administrative work. SDN is an open technology and it is more flexible to the previous technology and network system.

It has more interoperability functions and it has greater innovation in it. It gives a cost effective solution which also gives most important advantage.

# I Introduction

Software defined networking can be said to a new paradigm which separates network control logic from data (traffic) forwarding [1,2]. It centralizes all traffic management decisions in the SDN controller.

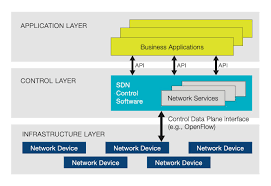
The primary benefit of this approach is that it allows real time and dynamic updating of traffic forwarding policies in network fabric infrastructure and due to real time programmability availability of SDN, we can also change the role of individual network devices.

For e.g., a forwarding switch to a forwarding firewall or just a firewall by remotely changing the traffic management primitives implemented in respective switches.

## Software-Defined Networking

In SDN, the control plane runs in a logically centralized controller. Additionally, the controller typically controls multiple routers across the network and often, the control program exerts control over all the routers in the network [2,3]. Thus facilitating network-wide control.

The separation of data and control allows a network operator to build a network with commodity devices where the control resides in a separate control program. This refactoring allows us to move from a network where devices are vertically integrated and making it very tough to innovate to a network where the devices have open interfaces that can be controlled by software.



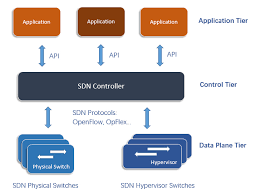
The two essential concepts behind SDN are **abstraction** and **automation**. By abstracting the network service required for an application into a network policy, applications are freed from underlying low level complexity and empowered to program their network connectivity. SDN automates the manual time intensive request based provisioning model. The network policy instantiates new application configuration tasks automatically replacing a laborious expensive process possibly hundreds of times a day.

Nuage networks virtualized services platform unleashes the full power of SDN.

# II. SDN FOR ENTERPRISE NETWORKS

Today, a wide range of business applications inside enterprises are being used over a network. In addition to ordinary companies, IT infrastructure is now utilized across various fields such as education and hospital facilities.

Secure Enterprise SDN (or SES) from AT (Allied Telesis) reduces the cost associated with network operation and management and enhances security by relating the applications and networks utilized in enterprises and various other industries.



SES, based on Openflow, dynamically determines the access policy of enterprise network by getting various information from enterprise applications. T

Secure Enterprise SDN has three key features:

1. The first is Application related provisioning. When personnel are transferred within a company. An administrator has to gather information such as user section, device information and working hours from separate databases under a legacy network, and then assign and configure the information manually one by one.
2. The second feature is security control by venerability countermeasure. After devices are granted through the provisioning feature, the devices will deal with various information and that will include personal and confidential information.
3. The third feature is behavioral detection. Most of the time, security control itself has to check vulnerability which is not enough as a protection. Because the users network access behaviour can face a threat of virus infection which could lead to an IT incident.

# III. ADVANTAGES AND DRAWBACKS OF SDN MODEL

## advantages

1. SDN doesn’t require expensive high end switches and can run on inexpensive hardware or switches. It doesn’t have a lot of processing lead because of in expensive high end switches. It helps to lower the organization operating cost
2. control.
3. SDN can filter the packets as they enter in the network says that all the switches now act like a firewall. This helps to control all the malicious activities and as well as secure the data.

## drawbacks

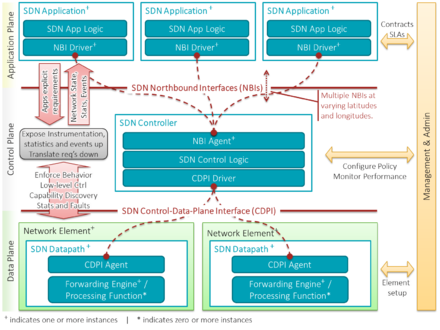
1. SDN has a drawback of scalability performance issue. It’s tough for a single controller to produce all the connection requests and forwarding decision. This is managed by replicating the controller but then this controller must be synchronized which brings more challenges that can be achieved. However, this is difficult. Basically, this controllers need to be synced and synchronization can be real challenge for the network administrator.
2. The second drawback is technology change. Any change is scary. SDN is a new technology that requires training and buying a new software and hardware for the network.
3. The another drawback is central point of failure. If central controller gets hacked then the whole network is hacked or if something goes wrong with this controller or the replicated few controller and the network is in trouble.

# V. SDN VS. TRADITIONAL NETWORK

## INFRASTRUCTURE

In traditional networking, the switch doesn’t have programmability. The rules cannot be changed dynamically as per our wish.

In Software Defined Networking, the switch is connected to a controller, which controls the actions of the switch. The controller can be programmed dynamically to control the switch, thus giving programmability to the switch.



# VI. CONCLUSION

SDN increases flexibility, visibility and efficiency while reducing complexity and costs. SDN are more dynamic networks, easy to manage, quicker to react and more efficient at delivering services with or without elastic bands. In this paper we have discussed SDN Architecture.

Different Enterprise networks architectures. This also provides applications of SDN like virtualization and advantages and disadvantages of SDN.

# REFERENCES

[1] "The future of network virtualization and SDN controllers", Oct. 2016, [online] Available: <https://www.temperednetworks.com/sites/default/files/pdf> s/fe atured\_content/2016-SDN-NVReport\_Tempered\_Networks.pdf.

[2] S. K. N. Rao, SDN and its use-case–NV and NFV, Oct. 2014, [online]

Available: http://www.nectechnologies.in/en\_TI/pdf/NTI\_whitepaper\_SDN\_NFV.pdf.

[3] Software-defined networking: The new norm for networks, Oct. 2012, [online]

Available:

https://www.opennetworking.org/images/stories/downloads/sdnresources/white-papers/wp-sdn-newnorm.pdf.

[4] J. Vestin, A. Kassler, J. Akerberg, "Resilient software defined networking for industrial control networks", 2015 10th International Conference on Information Communications and Signal Processing (ICICS), pp. 1-5, 2015.

[5] D. Levin, A. Wundsam et al., "Logically centralized?: state distribution trade-offs in software defined networks", Proc. ACM HotSDN12, pp. 1-6, 2012.