INVESTIGATING THE BENEFITS OF THE SDN APPROACH TO IT DEPARTMENTS IN COMPARISON TO THE TRADITIONAL APPROACH

Kemal YAMAN

SEPTEMBER 2022

ÇANKAYA UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

DEPARTMENT OF COMPUTER ENGINEERING

MASTER THESIS IN

INFORMATION TECHNOLOGIES

INVESTIGATING THE BENEFITS OF THE SDN APPROACH TO IT DEPARTMENTS IN COMPARISON TO THE TRADITIONAL APPROACH

Kemal YAMAN

SEPTEMBER 2022

ABSTRACT

INVESTIGATING THE BENEFITS OF THE SDN APPROACH TO IT DEPARTMENTS IN COMPARISON TO THE TRADITIONAL APPROACH

YAMAN, KEMAL

Master of Science in Information Technologies

Supervisor: Assoc. Prof. Dr. Özgür Tolga PUSATLI

September 2022, 69 pages

The aim of this thesis is to compare the traditional hardware-defined network approach and the software-defined network (SDN) approach in terms of their effects on the IT departments of companies in addition to investigating the benefits of an SDN. With the increase in the usage of the SDN in the sector, the benefits of an SDN and the organizational changes it may cause have been studied. Considering the increasing data capacities and high-volume network connections, it can be said that a new network approach is needed. The effects and benefits of an SDN on an IT department is a problem that needs to be investigated. With this study, organizational changes for IT departments, automation of work and processes, rationalization of business procedures, and redesign of business processes are examined. The contribution of the SDN approach to innovation, savings, network performance, monitoring and management, defining and providing services, the insurance of the security of networks, the situation in terms of open-source software development, and the effects on existing oligopolistic vendors and small vendors have been investigated.

It can be said that the adoption rate of the SDN approach in the sector is quite low. Resistance to organizational change caused by SDN, uncertainties that may occur in network management, and security concerns are some of the reasons for this low rate of uptake. In this thesis, the comparisons between the traditional approach and SDN, as well as the benefits of SDN have been investigated and answers to these

concerns have been found. With this study, it has been concluded that an SDN accelerates innovation, provides less expensive networks, increases performance and offers easy-to-manage, secure networks. It has been observed that the solutions offered by small-scale vendors, together with the development of software capabilities and standard network tools, can be presented as an alternative in the industry. According to these results, the adoption of the SDN approach in the sector may accelerate.

This study makes examinations in terms of enterprise companies, but not in terms of Internet service providers or telecommunication operators. As a result of these explanations, the research question of this study, “What are the benefits of an SDN approach to an IT department compared with traditional approach?” can be answered as the SDN approach compared to the traditional approach makes it possible to establish networks with savings, faster initial setup, and more secure and enhanced software capabilities.

Keywords: Software Defined Network, Traditional Network, Network and Security Procedure, Business Process Design.

ÖZ

GELENEKSEL YAKLAŞIMLA KARŞILAŞTIRILDIĞINDA, YTA YAKLAŞIMININ BT DEPARTMANLARINA YARARLARININ ARAŞTIRILMASI

YAMAN, Kemal
Bilgi Teknolojileri Yüksek Lisans

Danışman: Doç. Dr. Özgür Tolga PUSATLI
Eylül 2022, 69 sayfa

Bu tezin amacı donanım tanımlı geleneksel ağ yaklaşımı ile YTA (yazılım tanımlı ağ) yaklaşımının, şirketlerin BT departmanlarına etkileri açısından kıyaslanması ve YTA'nın faydalarının araştırılmasıdır. Sektörde YTA kullanımının yaygınlaşması ile beraber, YTA'nın faydaları ve neden olabileceği organizasyonel değişiklikler üzerinde çalışılmıştır. Artan veri kapasiteleri ve yüksek hacimli bağlantı yoğunluğu göz önünde bulundurulduğunda yeni bir ağ yaklaşımına ihtiyaç olduğu söylenebilir. Yeni ağ yaklaşımlarından biri olan YTA'nın, BT birimlerine getirdiği faydalar ve BT birimleri açısından etkilerinin neler olduğu araştırılması gereken bir problemdir. Bu çalışma ile BT birimleri için, organizasyonel değişiklikler; iş ve işlemlerin otomatikleştirilmesi, iş prosedürlerinin yenilenmesi ve rasyonelleştirilmesi, iş süreçlerinin yeniden tasarlanmas incelenmiştir. SDN yaklaşımının; inovasyon, tasarruf, ağ performansı, ağın izlenmes ve yönetimi, servislerin tanımlanması ve sunumu, ağların güvenliğinin sağlanmasındaki durumu, açık kaynak yazılım geliştirme açısından durumu ile mevcut oligapol üreticilere etkisi ile küçük üreticilere katkıları araştırılmıştır.

Sektörde YTA yaklaşımının benimsenme hızının bir hayli yavaş olduğu söylenebilir. Bu yavaşlığın nedenleri arasında, YTA'nın neden olacağı organizasyonel

değişikliğe direnç, ağ yönetiminde meydana gelebilecek belirsizlikler ve güvenlik endişeleri gösterilebilir. Bu tezde ile geleneksel yaklaşım ile YTA arasındaki karşılaştırmalar ve YTA'nın faydaları araştırılmış ve söz konusu endişelere cevaplar aranmıştır. Bu çalışma ile YTA'nın, inovasyonu hızlandırdığı, daha az maliyetli ağlar kurulmasını sağladığı, performansı artırıp kolay yönetilebilen, güvenli ağlar sunduğu sonucuna ulaşılmıştır. Yazılım kabiliyetlerinin gelişmesi ve standart ağ yönetim araçları ile beraber küçük ölçekli üreticilerin sunduğu çözümlerin de sektörün tanınan üreticilerinin çözümlerine alternatif olabileceği görülmüştür. Ulaşılan bu sonuçlara göre YTA yaklaşımının sektörde benimsenmesi hızlanabilir.

Bu çalışma, kurumsal şirketler açısından incelenmiş olup İnternet servis sağlayıcısı ya da telekomünikasyon opratörleri açısından incelenmemiştir. Tüm bu açıklamaların sonucu olarak bu çalışmanın araştırma sorusu olan "Geleneksel yaklaşımla kıyaslandığında YTA yaklaşımının getireceği faydalar nelerdir?" şu şekilde cevaplanabilir: YTA yaklaşımı, geleneksel yaklaşıma kıyasla, mali tasarruf sağlayan, ilk kurulumu daha hızlı servisler sunan, daha güvenli, yazılım kabiliyetleri artırılmış ağlar kurabilmeyi mümkün kılar.

Anahtar Kelimeler: Yazılım Tanımlı Ağ, Geleneksel Ağ, Ağ ve Güvenlik Prosedürleri, İş Süreçlerinin Tasarımı

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my parents for their support and sacrifice for me. Your memories would ever shine in my mind.

Special thanks to my supervisor Assoc. Prof. Dr. Özgür Tolga PUSATLI for the excellent guidance and providing me with an excellent atmosphere to conduct this research. My special gratitude also goes to the rest of the thesis committee Prof. Dr. Murat KOYUNCU and Prof. Dr. Hakan MARAŞ for the encouragement and insightful comments.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ACL	: Access Control List
API	: Application Programming Interface
CAPEX	: Capital Expenditure
CCNA	: Cisco Certification Network Associate
DCN	: Data Center Network
DEVOPS	: Development and Operations
FHRP	: First Hop Redundancy Protocol
IoT	: Internet of Things
IPTV	: Interet Protocol Television
IT	: Information Technologies
LAN	: Local Area Network
M2M	: Machine to Machine
MIB	: Management Information Base
NETCONF	: Network Configuration Protocol
ONF	: Open Network Foundation
OPEX	: Operational Expenditure
OSPF	: Open Shortest Path First Protocol
QoS	: Quality of Services
RFC	: Request for Comment
RIP	: Routing Information Protocol
SDN	: Software Defined Network
SD-WAN	: Software Defined Wide Area Network
SNMP	: Simple Network Management Protocol
STP	: Spanning Tree Protocol
UML	: Unified Modeling Language

VXLAN : Virtual Extensible Locol Area Network

WAN : Wide Area Network

XML : Extensible Markup Language

1. INTRODUCTION

The widespread use of connected devices in enterprises along with smart phones, the introduction of live broadcasts over the Internet, and the digitization of financial and commercial transactions have significantly increased the amount of data on the Internet. The expectation of high quality video broadcasts and the increase in the number of social media subscribers bring additional burden in terms of capacity in network environments. On the other hand, the need for reliable and secure data transmission is also increasing. According to Juniper Networks, data traffic is expected to increase 9.6 times by 2025, connecting more than 30 billion devices between 2020 and 2022 and close to 80 billion by 2025 [1]. Therefore, there is a need for improvement in network infrastructures necessary for the transmission and presentation of data in high volumes and at high speeds brought about by the exponential growth in information technologies. The most popular and accepted approach by industry and academia in order to meet this need is the software-defined network (SDN) approach. An SDN is a network approach that is not hardware-defined as its basic definition, but attempts to meet any requirements in software-defined terms. To date, the SDN as a concept does not have a standard definition. It is defined according to the approaches of network vendors and a number of the network communities. However, improved agility, security and performance is promised with the software defined approach by vendors [2]In this study, the benefits of the SDN approach as a solution to the ossified structure of traditional networks are discussed. Although the adoption of SDN as an alternative solution is discussed in the sector, it can be said that the rate of spread of SDNs is low. There are a number of reasons for the slow progress of the transition to software-defined networks, which are recommended to meet the network needs of these developing information technologies. Some of these reasons are due to companies' IT policies, organizational structures and security concerns. It is a problem that needs to be studied in terms of how this paradigm shift, which accompanies software-defined networks in network

infrastructures, and in terms of how it can cause changes in companies' IT departments.

With this study, the benefits of the SDN approach to IT departments in enterprise companies were investigated by comparing the approach with the traditional network approach. When the studies in the literature are examined, it can be observed that there is a paucity of studies on how IT departments in enterprise companies are exposed to organizational changes to adopt the SDN approach.

As a contribution to the studies in the literature, this study focuses on the benefits of SDNs compared to the traditional approach. Along with the adoption of the SDN approach, research has been carried out on the changes that may occur in an IT department and how such changes can be beneficial in the long term.

In this study, only enterprise companies have been given focus. Internet service providers or telecommunication operators were not included in the study. In the scope of these explanations, the research question of this study is "What are the benefits of the SDN approach to an IT department compared with a traditional approach?"

This thesis is organized as follows: Chapter 2 reviews a number of important definitions and comparisons pertaining to networking approaches. In Chapter 3, organizational changes with the SDN approach and business process redesign are studied. Finally, the thesis is concluded in Chapter 4.

2. BACKGROUND AND LITERATURE REVIEW

2.1. BACKGROUND

2.1.1. Traditional Network Approach

In this work, we attribute the traditional network approach to all networks that were used before the SDN approach. The traditional approach is based on hardware-defined networking. In the traditional approach, each network node has three planes, namely a control plane, a data (forwarding) plane, and a management plane [3]. The control plane is responsible for controlling routing protocols, how the data is forwarded, and which rules apply to the data. The data plane is responsible for deciding which frame or packet passes through which interface. The management plane is responsible for device management. Moreover, traditional networks fully depend on human interaction, which in turn lead inevitably to occurrences of misconfigurations. The traditional approach is therefore not efficient for configuration, optimization or troubleshooting [4].

Data growth is enhanced with digital transformations. Therefore, managing computer networks with a traditional, static, approach means configuring and adapting all devices manually by administrators on the infrastructure. When a network infrastructure needs to be enlarged or when it is on a large network infrastructure, the administrator has to control the devices all the time because traditional networks are based on protocols that are configured by humans [3].

2.1.2. SDN Approach

The Software Defined Network is a new network approach to provide communication of services and applications. With an SDN, the control and data planes are decoupled. This separation ensures centralized management and operation of the network domain. The functions of the control plane, which performs load balancing, routing and access control, are provided by software on the controller [5]. While the functions of the control plane are performed by an external controller, the functions of the data plane can be provided by dummy switches. According to the Internet Research

Task Force, this separation ensures faster innovation on both the data plane and control plane [6]. The SDN approach has three parts: Overlay, Underlay and Controller. In the underlay, such traditional networks, switches and routers are located differently from the traditional approach: the devices do not have control plane capabilities. The controller is a server that has all control plane capabilities and is the brain of the infrastructure. Controller and underlay devices communicate with OpenFlow, which is a widely accepted communication framework developed at Stanford University [6]. Overlay is the software part that manages network traffic. Since our subject requires going into more technical details of SDNs, we consider this much explanation sufficient for now.

The SDN is a new approach to solve ossified network issues. According to Vodafone, the SDN is the long-awaited solution to complex and expensive network problems. As the opposite of the traditional network, the SDN frees up manual configuration of network devices.

Since the SDN approach is a software-defined concept, open source and general adoption are important during the development stages. Separation of the control and data planes, virtualization of network functions, and especially the controller features where the SDN will be managed are three important stages of development. As can be seen in Figure 1, the OpenFlow idea, which aims to manage traffic with a single protocol for the entire underlay, which is an important stage of the SDN approach, was introduced in 2008 [7].

In 2010, ONIX offered a support controller with an information base for applications [8]. ONIX was the first platform to be the control plane of a distributed network. It provides API for all system control planes [8]. The Open Network Operation System (ONOS) is an open source SDN controller that introduced open-source controller applications to provide a network topology database in 2014 [9]. In the history of the SDN, the emergence and proposition of OpenFlow, ONIX and ONOS respectively, and their widespread acceptance in the industry have led to the rapid spread of SDNs.

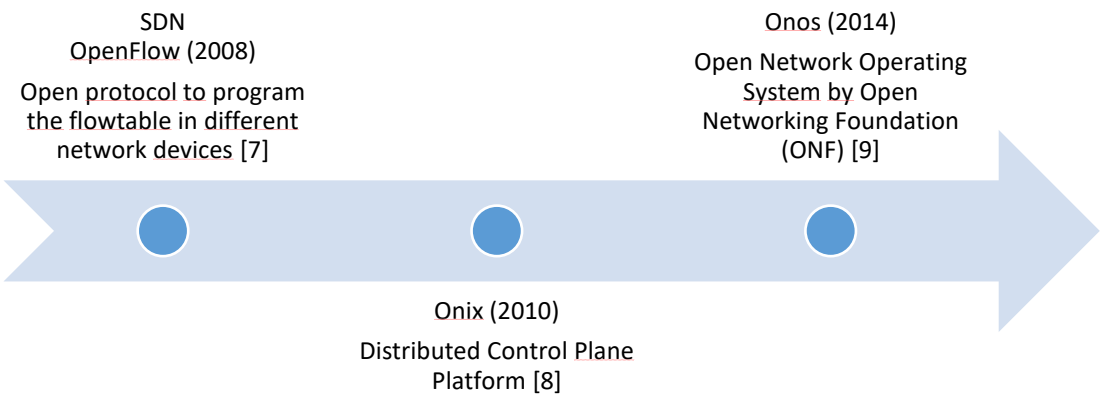

Figure 1: History of SDNs

2.1.3. Capital and Operational Expenditures

Capital expenditures (CAPEX) are the cost calculations of the initial infrastructure materials expenditures, such as switchers and routers (including software licenses), local cabling, etc. [10]. Operational expenditures (OPEX) are the cost calculations of operational needs, such as power consumption, maintenance and reparations [10].

In this study, there will be some comparisons of piece and cost of ownership of network devices, which includes software license costs, routers, switches, firewalls and other middle boxes on the SDN and traditional networks involving CAPEX. Energy consumption, leased lines and maintenance are the part of the OPEX cost.

CAPEX savings means reducing the number and variety of equipment used and OPEX savings means reducing energy consumption and reducing maintenance and operating costs.

2.1.4. System Development and Organizational Changes

In this study, we compare the traditional approach with the SDN approach in terms of ensuring automation of increasing efficiency and replacing manual tasks. The SDN approach changes the rationalization of procedures regarding standard operating procedures. Moreover, the SDN approach analyzes, simplifies and redesigns business processes, such as combining steps and functions and eliminating repetition of infrastructural devices and workflows. Such radical changes are discussed as a redesign or paradigm shift in the business, as discussed in [11].

The SDN approach requires a fundamental change in network management. While the traditional approach is based on hardware, the SDN approach is based on software. Because of this fundamental difference in approach, the SDN is called a new paradigm in the literature [12-16].

2.2. LITERATURE REVIEW

2.2.1. Comparison of the SDN Approach with the Traditional Network Approach

It is uncertain whether the future needs of IT can be met with the traditional network approach. In order to overcome this uncertainty, serious studies have been carried out both in academia and in the sector. Cheaper, safer and easier-to-apply approaches should be adapted to the current approaches in order for the benefits of the studies to be deemed sufficient and for the new approaches to be adopted.

In our study, we focus on some of the main benefits of the SDN approach, which is our subject here; however, we will not delve into too many technical details. Furthermore, the software-defined network seems to bring many engineering technical benefits in comparison to traditional networks. Some of these include platform scalability [17], performance management [18], and virtualization [19]. On the other hand, cost management, configuration management and provisioning management are priority issues for our section about benefits.

Although many of the technical benefits have been studied, it does not seem logical for companies to adopt a new approach that has not yet been fully standardized. Nevertheless, the main reasons that may cause companies to take the SDN approach will be the issues related to financial and service quality.

New technologies brought about by digitalization require much faster networks. On the other hand, in order to ensure competition, the need for lower cost infrastructures is increasing. In addition to all these factors, reducing human impact by machine learning and central control are becoming increasingly important for network infrastructures. With growing Internet traffic and geographical independence, data dependent data centers force a change of approach of managing networks. Compared with traditional networks, an SDN provides more automated tools, which lowers the probability of misconfiguration and ensures predictable scaling of infrastructure. Centralized control and management of networking provides more manageable

distributed and load balanced traffic. Thus, application performance is expected to improve. As discussed in Section 2.1.3, decreasing middle boxes and centralizing management and control makes for more secure infrastructure and reduces expenses, including CAPEX and OPEX spending [20].

2.2.1.1. Cost Comparison

Local area networking (LAN), data center networking (DCN) and wide area networking (WAN) have different types of infrastructure and ranges. LAN is the type of network that belongs to the relevant organization for the communication of host, client or servers in several buildings close to each other. DCN is the type of network in which the communication of servers, storage and other IT devices in a data center are provided. WAN, on the other hand, is the network that companies provide over the lines they lease from a service provider to access their remote offices or external stakeholders.

LANs have wired and wireless network access with many network devices that are connected each other with short cabling. Therefore, only the initial setup cost is important, including the setup of devices (switches, access points, access controllers, routers, etc.) and cabling.

In legacy WAN, leasing a line is an Opex cost issue for enterprises. On the other hand, changing the current infrastructure is difficult and vendor dependent. Therefore, architecture is resistant and rigid. On an SDN, open networks are independent of vendor specification and SD-WANs (software defined wide area networks) ensure path detection. Therefore, SD-WANs provide cost saving and greater flexibility [21].

As a synthesis of LAN and WAN, the initial setup costs, security and leases of lines become important costs issues for DCN. These costs increase especially in the communication of multiple data centers, which are required for new generation redundant data centers.

Especially for an initial setup in traditional networks, one single device has its control, management and data (forwarding) plane together on itself. This situation forces network nodes to have strong hardware to operate the control, management and data planes together. Therefore, traditional, hardware-based devices are expensive. On the other hand, the SDN control plane is not a burden for network nodes. On an SDN

structure, network devices have only the data plane. The control plane is separated from the network devices and is given to a central controller [22]. This means it is less expensive to own the devices. Additionally, in the traditional approach, because of the control plane of each device, all necessary protocols need to be configured on each device.

In the traditional approach, each device must have its own control and data planes. Devices with both a control plane and a data plane are called black boxes, and most of the devices in the traditional approach are black boxes. Black boxes are expensive. In the traditional approach, the infrastructure cost is high because of the expensive black boxes needed when implementing a network infrastructure. The SDN approach solves these situations with separate control and data planes. An SDN does not need black boxes, which have both control and data planes on the device [23]. An SDN offers centralized control on a controller and data plane switches without the control plane on its own. Thus, in contrast to the traditional approach, in the SDN approach the cost of switch ownership is lower with the dummy boxes.

In addition, some of the advantages of SDNs pertaining to load balancing [24], delay reduction [25], and decreasing the number of devices ensure lower energy consumption. An SDN provides software based load balancing. Since network devices distribute and balance loads according to the decision of the controller, the devices do not take responsibility for the load balancing management on themselves, thereby consuming less energy. Similarly, managing the routing and traffic control with a controller ensures a reduction in total system delays as well as power savings.

2.2.1.2. Provisioning Comparison

Considering full automation and effortless management as the two of the main objectives of future networks, there are many routers, switches and middleboxes in traditional networks. Therefore, managing future networks taking a traditional approach is more difficult. With the growth of data and IT infrastructure, configuring devices, attempting to calculate forwarding packets and frames by protocols and managing advertisement or update packets to maintain networks persistence is more difficult than before [21].

In traditional networks, deployment is difficult to manage. For instance, routing of packets with static routes is easy on a small network. However for larger intra area

networks distance vector routing protocols (i.e., RIP, ERGRP) or link state routing protocols have to be preferred. For these dynamic routing protocols, network administrators need to configure each device carefully and without any failure. Complications become more difficult to manage considering OSI Layers 2 and 3. Additionally, in wide area networks, campus networks or data centers, each Layer 2 switching protocol, such as STP, LLDP, etc., or Layer 3 routing protocols and FHRP protocols, are needed for robust configuration. For example, to configure the spanning tree protocol (STP), an administrator needs to decide on the STP mode, STP device priority or port type (i.e., designated, block or root) for each device separately. With SDN, it is possible to reduce the effect of spanning tree [26]. Also with SDNs, using the virtual extensible locol area network (VXLAN) feature provides solutions to Layer 2 issues by carrying them over to Layer 3. This reduces the effect of the spanning tree or other Layer 2 problems.

On the other hand, an SDN provides route selection with lower packet losses [27] and dynamic changes in the weight of the links to select stable connections [28].

With an SDN, such load balancing, intrusion detections and firewall systems can be virtualized. Virtualization provides faster provisioning than physical devices. Configuring hardware can take weeks in traditional networks; however, on an SDN, this process occurs in minutes. Creating a cloud network environment is already innovatively faster. The programmability of a network provides rapid use and provisioning of networks. Therefore, with an SDN, an administrator can easily ensure the migration of applications to hybrid IT i.e. cloud and on-premises together [29]. Examples include [30].

Companies with an available cloud platform can have fast commissioned network nodes with a software-define network.

Management and visibility with this agility become possible proactively. However, manual administrations of traditional networks cannot ensure this agility [29].

Furthermore, the SDN approach has centralized management of ensuring operational efficiency for service chains which is needed by the running applications on the network [29]. An SDN provides faster provisioning on some of the network

applications, access control lists (ACL) [31], load balancing, QoS, congestion detection, reliability, node and link disjoint routing [32].

In addition, an SDN provides, with the agility of an SDN structure, efficient local caching and auto scaling to the end user by reducing the number of necessary network administrators [33] [34].

2.2.2. Automation of IT with an SDN

An SDN provides many benefits in terms of automation for network infrastructure with applications as argued in [35]. In traditional networks, switches and routers decide to forward traffic when a packet arrives. With an SDN, even switches and routers forward the destinations, but SDN controllers decide on the path, and programmable interfaces automate routers and switches in the environment [29]. This centralized approach increases the ability to automate.

Information Technologies, IoT, AI, NFV and other technologies are becoming more widespread. Reducing human intervention in these technologies is important to reduce the number of errors. For this reason, it is not easy to meet the requirements of these technologies taking the traditional approach where administrative influence is high [36].

As mentioned in Section 2.1.2, the control plane and data plane are decoupled in the SDN approach. The control plane's responsibilities are met by the central controller, resulting in less connection time [37]. Thus, automation is easier with efficient and fast connectivity.

In the SDN approach, the controller is a single point of many factors, including failure, management, decider of forwarding, etc. Therefore, planning, provisioning and configuring communications from controllers makes the administrator more focused on it. Controllers need to be reliable, redundant and more secure appliances. With these conditions, an SDN provides automation and orchestration for network services with reduced complexity [29].

On the other hand, the evolution of SDNs is slow. Virtualized datacenters and services need more automation and more rapid deployment. To solve the need of orchestration, administrators can use a number of open source tools, but the interoperability issue still needs to be solved. The interoperability problem can be solved using OpenFlow protocols [38].

Although they were initially slow to support OpenFlow, major manufacturers such as Cisco [39], Juniper [40] and Arista [41] have produced products that can work with OpenFlow. Additionally OpenFlow is supported by many other vendors' productions [42].

The evolution of OpenFlow with a high rate of adoption is important for the automation of networks. Therefore, since the first version of OpenFlow 1.0 published in 2009, there have been many new improvements in subsequent versions. As the time of writing the 1.6 version is available to Open Network Foundation (ONF) members [43].

As a trend of the Internet of Things and the Industry 4.0 revolution, automation of networking has become more important. An SDN provides programmable and flexible architecture to achieve automated networking. An SDN provides innovative implementation, especially in traffic engineering or security policies, and reconfigurations of network devices [44].

An SDN also provides low latency and less floating activity to decrease the number of duplicated packets [44]. Fewer duplicated packets that ensure fewer retransmissions are a benefit that strengthens an SDN's hand in providing fast communication.

2.2.2.1. SDN Automation of Security

The SDN approach uses a central controller or a cluster of controllers. Thus, the central control point where all traffic is managed can be a direct target for attackers. Although in the SDN approach, infrastructure does not seem reliable due to the singularization of the control plane, new research [45] shows that the SDN is also as reliable as traditional networks if fast failure detection and recovery can be provided. The attacks to which networks are exposed are diversifying and increasing. Proactive measures and the ability to make quick decisions at the time of attack are important for strengthening the defenses of networks. Therefore, the importance of automation is increasing in terms of securing networks against threats.

Threats have become increasingly more sophisticated year by year. The World Economic Forum reported that cyberattacks are the second greatest risk to economies [46]. According to the Cisco Cybersecurity Report Series 2020 [47], many

companies have to take interest in 5,000 daily alerts; however, the numbers of cybersecurity staff are insufficient to answer the incoming alerts and threats [47].

According to Gartner, security automation is one of the top security and risk management trends [48]. An SDN enables a security manager to have centrally managed and automated platforms for network security. Automation in the security of a network can decrease the need for skilled engineers and provide fast responses to threats.

Machine learning, deep learning, model-based attack detection with online adaptation, reinforcement learning for threat mitigation, adversarial learning, moving target defense, network function virtualization, cyber deception, network slicing, and blockchain-assisted activities provide more computational events with an SDN [49].

An increase in data volume in addition to complex threats necessitates a rapid defense and response for networks. New network paradigms, such as 5/6G, IoT, cloud computing, cause complexity and larger networks; therefore, security for these new large networks should be automated [49]. From this point of view, we think it would be useful to expand the subject specifically to IoT (Section 2.2.2.2).

Although SDN offers new security features, due to its architecture, the central controller, which controls and manages infrastructure, makes a platform for a single point of attack for hackers, which is argued as one of the reasons that market growth has slowed [22].

2.2.2.2. Fast Transmission with IoT Devices

One of the other benefits of an SDN is fast computing and the consolidation of multiple IoT sensors that collect any necessary data on a single piece of infrastructure. For instance, an experience in Jalisco State in Mexico with an application, users are able to make payments without waiting due to density through implementations of IoT sensors in a software defined environment [27]. As mentioned previously, the SDN ensures less effort for communication and transmission. Therefore, an SDN is a better approach to IoT environments that have large transmission packets.

IoT devices are generally low-cost devices with less featured hardware. Therefore, adding more functions is subject to consider energy consumption. An SDN brings more software based functions to such devices. For instance, supporting low-

cost IoT devices with firewall features is possible with the SDN approach [50], thereby ensuring more security for the infrastructure with conserving energy.

On the other hand, in an SDN, the controller takes over the control plane responsibilities of each individual device in the traditional approach. However, SDN controllers are higher capacity devices compared to IoT devices. Thus, an SDN controller has more features than each single IoT devices' control plane to control intrusions and facilitate the detection and prevention of intrusions. [51].

2.2.3. Changes in Network Procedures with an SDN

In traditional networks, based on hardware, IT and network units work separately. An SDN facilitates greater collaboration between these units. On traditional hardware based infrastructure, capability depends on hardware. Vendor-centric configuration styles force staff to develop expertise in the configurations of particular hardware. Even though protocols have international standards, the configuration commands are not standard. With the evolution of virtualization technology, many vendors have begun to change their approach in the market and take an interest in other functionalities, which is expressed as a paradigm change. The main opportunity for these vendors is that their usual business pertains to virtualization, including firms such as Citrix and VMware.

A network has more concern for the needs of applications in terms of security, malware, intrusion detection or load balancing with an SDN. A network administrator has an interest in IT infrastructure units and application units and it is important to understand business priorities [29]. Therefore, having a strong software-defined environment is strongly dependent on powerful network infrastructure. Data volume and the number of cloud server applications are increasing. Therefore, networks are expected to have larger and more reliable capacities. Software as a service or drive applications cause problems for network administrators if there is insufficient bandwidth. Because of the increasing use of cloud services , delay and jitter have become important factors to consider. IP telephone, video broadcasting and live streaming applications force networks to become delay sensitive. Moreover, the number of applications being deployed via the cloud i.e. software as a service is increasing [52]. Enterprise companies are migrating their resources to the cloud. Hybrid IT (cloud and on-demand hosting of servers) is a transition stage. Cloud-base

applications give flexibility to companies. An example can be seen in the Volkswagen IT transformation experience, in what seems to be a customer experience problem at first was in fact determined as the inability of employees to adapt to this transformation, which is related to the lack of IT infrastructure [53]. Volkswagen had kept some of its services in the cloud environment; however customer complaints emerged during the adaptation period of its employees, who could not become accustomed to this situation. In fact, the problem consisted of accessing cloud-defined client applications, slow networking or the long time for employees to adapt. As mentioned previously, new generation technologies, such as the cloud, need a strong network infrastructure. The situation at Volkswagen exemplifies how an organization's network affects all its services. Implementation of applications from the cloud forces highly available, redundant, fast and flexible networks.

New business processes bring improved cost savings, performance and security to customers and companies. However, to implement this benefit, network infrastructure needs to be strong, especially in terms of bandwidth, delay and jitter related to delay-sensitive applications, availability, etc.

Serving from the cloud requires more network resources than on-promise environments. IT, software, infrastructure, and each "as-a-service" approach depend on stronger networks. The power of a network is about revenue, productivity, and experience for staff, partners and customers.

Another issue with procedures is the implementation of the infrastructure. Achievement of needs of scalability is difficult on vertical traditional networks. An SDN provides horizontal growth, which scales better. In contrast to the three-layer infrastructure (core, aggregation and access) of traditional enterprise networks, an SDN has two layers on the underlay infrastructure as spine and leaf devices. This reduces the number of hops and increases the capability of connections. Due to the structure of an SDN, horizontally implemented nodes can communicate with each other without additional routers because only an SDN controller in a virtualized environment is required [54].

2.2.3.1. Changes in Security Procedures with an SDN

A network administrator should have higher availability rates, secure networks for the next generation of malware and threats, and delivered content. One of the areas

where software-defined networks are used is the cloud. For instance, Google Cloud [55], Microsoft Azure [56] and AWS (Amazon Web Services) [57] use software defined networks on their respective clouds.

Cloud platforms are being developed to provide faster and secure access to data from anywhere at any time. A number of standards and procedures has become necessary for the secure use of the cloud. As an example of using secure cloud systems, the Presidency of the Republic of Turkey published the Presidential Information and Communication Security Measures Circular No: 2019/12.

The third article of the circular says *"Data belonging to public institutions and organizations will not be stored in cloud storage services, except for the institutions' own private systems or domestic service providers under the control of the institution."* [58].

Pursuant to this regulation, some domestic service providers deploy their own cloud systems.

Using software defined networks and environments is regulated governmentally for public organizations. Furthermore in July 2020, the Digital Transformation Office of the Presidency published the "Information and Communication Security Directory," which regulates cloud IT security pursuant to Article 4.3.

Additionally, enterprise companies need to change their own directories to adapt to software defined environments independently of regulations. Hence, network procedures are expected to change in a software defined environment.

2.2.3.2. Changing Functional Base Hardware Asset Management and Ownership Procedures

Decreasing the number of middlebox devices and the execution of their missions by the SDN controller are other issues on which to focus. In the traditional approach, hardware has a function. Routers, switches, firewalls, IPS/IDS, DBF, etc. have specific functionalities. Thus, most enterprises use functional base organizations in order to divide responsibilities according to asset. For instance, firewall security administrators, end point security administrators, WAN administrators, LAN administrators, datacenter network administrators, servers and storage, operating system administrators, developers, etc. exist in function base IT departments. Each

administrator operates their own hardware or appliances. Such functional base companies need to adapt their organizational chart to virtual and software defined environments. Beyond the SDN and virtual environment, many functions are bundled into one hardware cluster. For example, VMware NSX and ESX products provide switching, routing, firewall, load balancing, automation, URL filtering, malware detection, APIs and DevOps on a single cluster of hardware independently [59]. Alternatively, F5 NGINX, Cisco ACI and many other vendors' products also exist.

A different entity for each function in the traditional approach and the management method of these assets have to be changed with softwere define environment. The impact of a single physical asset on multiple functions and multiple units will require a change in asset management.

ISO 27001 Information Security Management Article A.8.1.2 pertains to the ownership of assets. The presentation of multiple functions in a single physical asset will also affect the approach to this international standard. In the traditional approach, with the thought that each device performs a function, the unit responsible for that function would be directly responsible for the related entity. Since an asset can meet more than one function in an SDN and it is used by more than one unit, it becomes necessary to work on the unit which will be responsible for the relevant asset.

2.2.3.2.1. Virtual Asset Management Example: Firewall on Every Host

Traditional network firewalls rely on physical devices. Therefore, firewall security is perimeter security. Moreover, with SDN virtual structure, a firewall can be placed on each node of the virtual environment as a granular structure. With this virtualization, the distribution of firewalls on all appliances and each host makes the networks ensure measurement and management of vulnerabilities.

In the traditional approach, firewalls are placed as a boundary between the Internet and Intranet domains, with the latter being remarked as a trusted zone. Therefore, attackers who are inside can easily attack the network. However, with an SDN, distributed firewalls can be placed wherever they can be easily placed [60].

2.2.4. Changes in the IT Market in relation to SDNs

2.2.4.1. Vendors' Approach to the SDN

Traditionally on networks, if a vendor were to be implemented on an enterprise, the vendor becomes the dominant vendor for the company. Having the maximum efficiency on structure and network devices, administrators would want to use network management protocols such as the simple network management protocol (SNMP) and only a single vendor's platforms. It is possible to handle multivendor device situations with SNMP but it is not as easy as expected. It is necessary for there to be MIB (Management Information Base) folders which can be integrated. Every vendor's network devices have different configuration styles. Furthermore, a number of vendors also have different configuration styles on different devices [60]. It is difficult to construct a standard in the networking market. For instance, RFC 1131, which was published in 1989, was the first version of OSPF. The second version, RFC 1247, was built in 1991. Then, several RFCs were published. Finally, OSPF version 2 was standardized in 1998 with RFC 2328. OSPF version 3, which was for IPv6, was standardized in 2008 with RFC 5329 [61] [62].

Hardware based network management is becoming more difficult due to the lack of standardization of some protocols and due to the fact that manufacturers offer their own protocols with minor improvements added on some protocols. other reasons include the difficulties of running multiple manufacturers' devices on the same infrastructure. The elimination of all these dilemmas is inevitable. Vendors who are aware of this situation have finally started to support OpenFlow. As mentioned previously, OpenFlow is a popular underlay protocol used for software-defined non-vendor-centric network traffic management.

2.2.4.2. Changing the Networking Training and Certification Concept

One of the perspectives affecting the views of producers in the market towards the SDN approach has begun to be observed in education systems. One of the largest networking vendors, Cisco, is also one of the largest networking training system academies. For the market, certification of Cisco is widespread for employees.

The change in Cisco's education system is also an indicator of how learning requirements in an SDN's IT departments have changed.

Before 2020, the largest vendors' training and certification paths did not include software development skills. The Cisco Certification Path prior to February 2020 is shown in Figure 2.

Figure 2: Cisco Career Certification Path before 2020 [63]

Before February 2020, Cisco had different career paths for each unit, including wireless, security, routing and switching, collaboration, data center, cloud and service provider. For each unit, Cisco had career levels, such as associate, professional and expert. As indicated, there had not been any educational issue regarding software development.

However, after February 2020, the Cisco Certification Path changed considerably (Figure 3).

Figure 3: Cisco Career Certification Path after February 2020 [64]

After February 2020, the major change to the career path diagram concerns development networking.

This development is relative software-defined networking. A second major change concerns the associate level. Before February 2020, the number of associate levels of different exams was eight; however, all these exams were gathered into one main exam called CCNA.

These changes, the collecting of all units associate levels of one exam, indicate that having associate knowledge is important for IT departments. Even being a professional or an expert is still differentiated from expertise, and having an inclusive perspective is still important for junior staff of an IT department, which depends on a Cisco career and certification path. Additionally, development for a networker involves being on this path.

As an administrator, every software defined network engineer is required to know about scripting, coding and APIs. The DevNet path may help networkers with this issue. With the same content of Cisco DevNet, Juniper Networks, another large networking vendor comparable to Cisco, announced the Juniper Networks Certified Associate, Automation and DevOps certification program in June 2020 [65]. The training and certification paths are almost the same as Cisco's. Both the Devnet and JNCIA-Devops comprise fundamental knowledge of development and automation. With this basic knowledge, engineers have the fundamental information for automation, development and integration programming.

2.3. ACTORS IN NETWORKS

It is necessary to mention the employees described in the study and the jobs for which they are responsible.

2.3.1. Network Administrator

Network administrators are the people who decide on the network architecture and network products to be used, and install and operate related network products. In order not to go into detail from a technical point of view, the network administrator, which we generally specify as the manager of these responsibilities, is the authority of the aforementioned responsibilities. It is the responsibility of the network administrator to define the network access of a server installed in the data center and to provide Internet or Intranet access. The management of a campus network, the management of a WAN network, the management of the leased circuits obtained from a service provider are also the responsibility of the network administrator. In the industry, especially in large structures, people who manage firewalls and switches/routers are separated according to one approach. It is seen that firewalls and other security products are managed by network administrators in some other approaches, especially in small or medium-sized structures. For this reason, we specifically have to mention the security administrators in our work, where some technical details are inevitably explained.

2.3.2. Security Administrator

The security administrator is responsible for ensuring the security of the end users in the campus network and the security of the servers running in the data center. Vulnerability scanning, threat intelligence assessment, penetration tests, hacking and defense, and log management are deep security issues the technical details of which we do not intend to delve as they are not within the scope of our study. Since the related topics are within the scope of cyber security and pertain to endpoint security, it may be designated as the next study topic. The security admin is the person who gives access permissions and manages the firewalls in traditional networks throughout our study.

As stated in Section 2.2.3.2, since two same features can be applied on two different devices, such as access list management in routers and rule sets in firewalls, we also hold network administrators responsible for these works in order not to delve too much into the technical details.

2.3.3. System Administrator

The system administrator is the staff member who makes the initial setup of a virtual or physical server and storage systems, operating system setups, antivirus and similar basic agent setups, and follows system updates. The system administrator provides the hardware and virtualization environments, makes the initial setup, manages the resources in the virtualization environment, and provides the server or storage environment to the developer.

2.3.4. Developer

In our context, a developer or software developer who uses the IT infrastructure develops and executes a program on server systems or a database on a storage system. The developer determines the infrastructure needed for the applications to run, requests the server or storage from the system administrator, and informs the network administrator which IPs or databases the applications need to access.

In order not to go into the depth of technical details and because their role is not important in our study, terms such as system analyst, database administrator, solution architect were omitted and they were defined as ‘developer.’

In this section, the basic definitions of traditional networking and SDN approaches are discussed. The status of the relevant approaches in the literature in terms of cost, implementation, network management and network security procedures were examined. Possible asset management approach changes were discussed with SDNs.

The impact of the software-defined network on the IT industry, vendors’ approaches to the SDN, and changes in the training and certification systems offered to experts were examined.

Based on this information in the literature, we will examine the impact of the SDN approach on the organizational structure of the IT departments of companies in the next section.

3. ORGANIZATIONAL CHANGE WITH THE SDN APPROACH

The SDN approach is taking firm steps forward to becoming a widespread network technology for both academia and industry. According to Cisco's 2020 Global Networking Trends report, by 2020, SDNs were used in data centers (64%), WANs (58%), and access networks (40%) [66]. The SDN helps IT departments to handle centralized, simplified and agile infrastructures [67]. The SDN infrastructure with a general and simple definition has three main elements: a controller, and southbound and northbound APIs. The controller is the core element of the infrastructure that is used to make the network centralized and automated, and to manage the policy enforcement for network environments. Southbound APIs manage the communication to underlay network devices with the controller and northbound APIs manage the applications that ensure any transactions expected from the network [68].

An SDN provides an easy operation to increase simplicity by decoupling the control and forwarding planes. Furthermore, an SDN can eliminate administrators' manual configurations and provide programmable networks. SDNs also provide open applications and service deployment with an adopted large community, namely the Open Network Foundation (ONF). These benefits ensure centralization and fast provisioning, and easy monitoring and automation of applications both for the cloud and on-premises environments.

The SDN uses software-based implementations. Vendor-independent and virtualized network nodes have fewer hardware requirements in an SDN. Thus, needs can be met with relatively cheaper and fewer devices. Moreover, while the periodic equipment and maintenance costs are less expensive, the number of administrators and amount of equipment needed is also reduced. According to Gregory Hess, Network Manager of Montana State University, SDNs provide low operational investment with minimal staff [69]

The increase in the provision of IT services over cloud computing places a serious burden on networks. It is a serious challenge for traditional networks to provide faster, more stable and higher quality data in cloud services. According to Juniper

Networks, the increasing number of cloud user organizations and the increasing number of cloud based applications will cause bottlenecks. Traditional networks are not easy to be used with the cloud. Therefore, the SDN is a solution for cloud-based applications with the benefits of simplified operations, increased business agility, and accelerated service delivery [70].

Although SDNs seem to promise a good present and a good future for networking, it cannot be said that it has made progress as rapidly as expected because it has not yet been comprehensively standardized. However, the increasing use of the cloud and the necessity of companies to reduce their IT infrastructure costs make essential demands on SDNs. There are no common solutions other than the SDN for problems such as the capacitive network infrastructure required by the cloud and the low-cost requirement. Although not yet standardized, the SDN seems to be the strongest possibility to meet such needs.

In the network industry, how long it takes for solutions and protocols to standardize is explained in the second chapter with the example of OSPF. With this, the SDN has strong community support. ONF, and of course OpenFlow, have received a strong reception. Finally, in addition to small manufacturers, large companies in the market, such as Cisco, Juniper, and Arista, have also started to support OpenFlow. All these cases show that SDN is one of the most powerful solutions to meet the expectations of the network industry.

3.1. FEWER HARDWARE REQUIREMENTS AND FAST PROVISIONING

An SDN provides consolidated network features on less hardware. In traditional networks, Layer 2, 3 and 4 features are especially met by some network devices, while the features of Layers 4 and 7 are met by a number of other network devices. An example of this case can be seen in Figure 4.

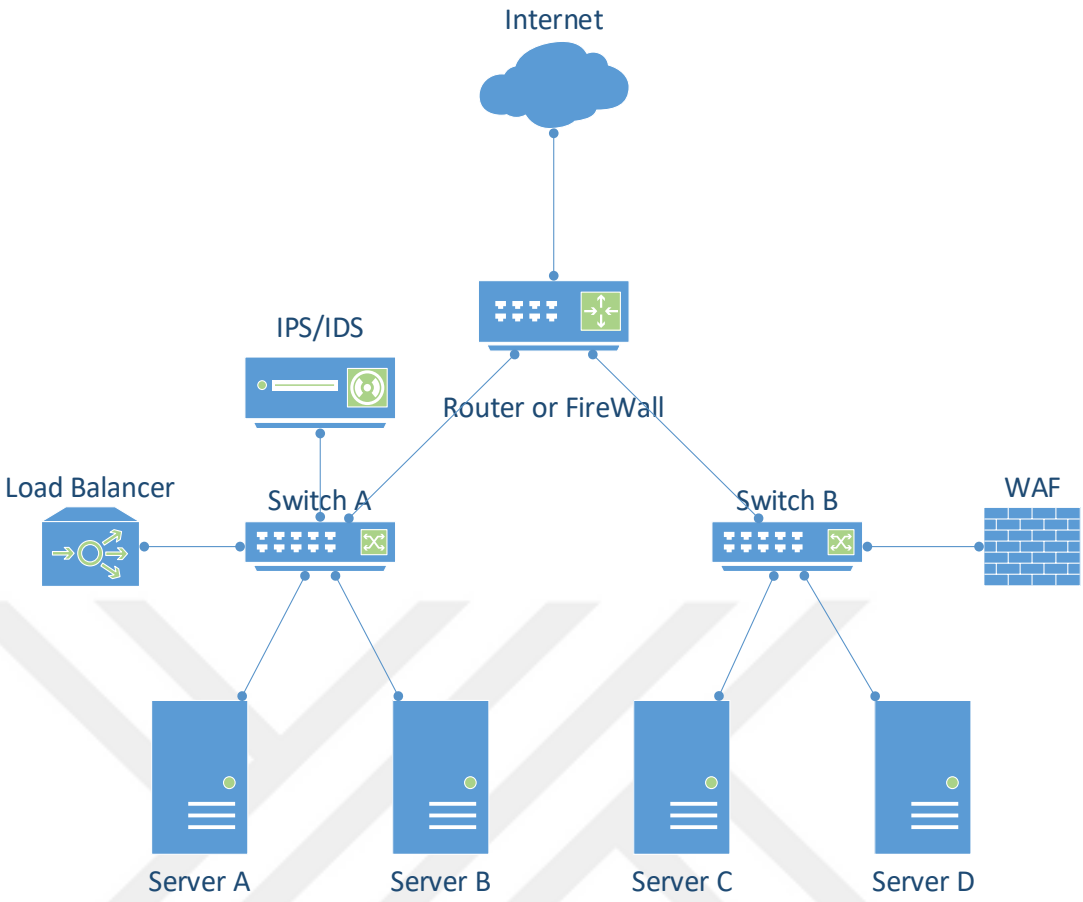

Figure 4: Simple traditional network infrastructure

In an SDN, on the other hand, it is possible to offer multiple features in a single piece of physical hardware as a contribution of virtualization.

Figure 5: Simple SDN infrastructure

The SDN is an approach that uses the possibilities of virtualization. With a physical server, it is possible to have and manage a basic network that is connected to the Internet. On a physical server, there should be more than a virtual server, a switch to obtain Layer 2 communication, a router to connect to the IP Layer, a firewall to control traffic, IPS/IDS (Intrusion Prevention and Detection System), WAF (Web Application Firewall), etc.

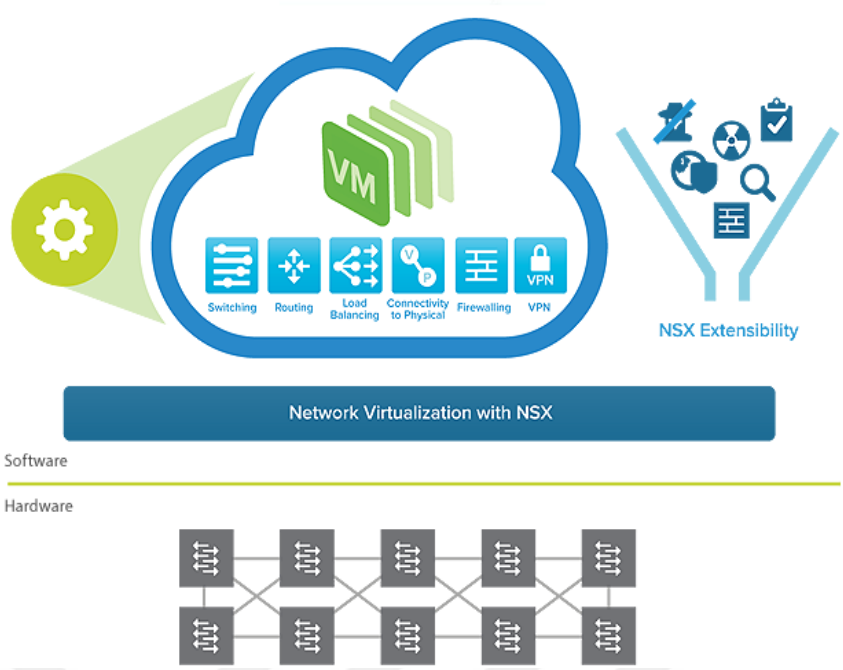

Figure 6: A VMware virtualized server with all networking features [71]

As can be seen in Figure 6, software-defined manufacturers provide physical device savings by virtualizing many main and middlebox products. In this way, in addition to physical device savings, physical space, energy, etc., savings are achieved. Furthermore, ease of network management and easy scaling become possible.

Another benefit of an SDN is that in much larger structures, fast end-to-end provisioning is possible thanks to the integration between servers and network devices. Network vendors and server virtualization vendors provide integration with a relationship. Examples of such relationships include Cisco and Red Hat [72], Arista and Microsoft [73], etc., achieving a fast provisioning of a software defined environment. With integrations such as these, the VLAN-VXLAN definition on which a server's IP will depend, switch VLAN-VXLAN configuration and firewall access permissions become possible with a single configuration set in the SDN approach.

3.2. AUTOMATION WITH OPENFLOW AND NETCONF

OpenFlow is a standard communication protocol that is used between an SDN controller and network devices. OpenFlow is used in configuring the network infrastructure devices of the SDN controller. OpenFlow has a continuous and stable history of updating and renewal. The fact that major vendors accept the existence of

OpenFlow and support it on their devices shows that the future of automation in the network will be with OpenFlow.

As OpenFlow, Network Configuration Protocol (NETCONF) is a standard (RFC 6241) to configure automated network operations [74].

Using the same set of configuration commands and development is one of the greatest problems for traditional networks. For instance, configuring a feature on different vendors' devices is not the same. An example of a configuration of CDP on a Cisco switch CLI is indicated below:

```
switch()# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# lldp enable
switch(config-if)# end
```

Obtaining the same configuration with NETCONF in XML data format is:

```
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:NETCONF:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:configure_"
xmlns:m="http://www.cisco.com/nxos:6.2.2.:_exec"
xmlns:m1="http://www.cisco.com/nxos:6.2.2.:configure__if-eth-base"
message-id="1">
      <nf:edit-config>
            <nf:target>
                  <nf:running/>
</nf:target>
      <nf:config>
            <m:configure>
                  <m:terminal>
                        <interface>
                              <__XML__PARAM__interface>
                                    <__XML__value>Ethernet2/1</__XML__
                              value>
                                    <m1:lldp>
                                          <m1:enable/>
                                    </m1:lldp>
                              </__XML__PARAM__interface>
                        </interface>
                        </m:terminal>
                  </m:configure>
            </nf:config>
            </nf:edit-config>
            </nf:rpc>
      ]]>]]> [75]
```

For another example of the show command:

```
cli configuration of showing the status of an interface:
switch()# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if) # do show interface ethernet 2/1
switch(config-if) # end
```

The NETCONF XML data model of showing the status of an interface:

```
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:NETCONF:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:configure_"
xmlns:m=http://www.cisco.com/nxos:6.2.2.:_exec" message-id="1">
      <nf:edit-config>
            <nf:target>
                  <nf:running/>
            </nf:target>
      <nf:config>
            <m:configure>
                  <m:terminal>
                  <interface>
                        <__XML__PARAM__interface>
                              <__XML__value>Ethernet2/1</__XML__
                        value>
                        </__XML__PARAM__interface>
                  </interface>
                  </m:terminal>
            </m:configure>
            </nf:config>
      </nf:edit-config>
</nf:rpc>
]]>]]> [75]
```

Another CLI part comparison of Cisco and Arista Networks configuration is shown below:

Cisco configuration [75]:

```
switch()# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# lldp enable
switch(config-if)# end [75]
```

Arista Configuration [76]:

```
switch()# config
switch(config)# interface ethernet 2/1
switch(config-if-Et4/1)# lldp receive
switch(config-if-Et4/1)#exit
```

As can be seen in the examples above, CLI commands differ among vendors. It is possible to obtain the same configuration for all NETCONF supported vendors with NETCONF.

3.3. NETWORK SECURITY PROCEDURE ON THE SDN APPROACH

Although security in an SDN is considered to be flawed due to the presence of the central controller, an SDN brings with it many network security benefits, as mentioned in Chapter 2. One of the most important security features that comes with an SDN is a virtual firewall for each server. In traditional networks, a firewall is a main-order device and usually at the top of the topology. Therefore, there are no security policies on the frame layer, Layer 2. For instance, servers on the same VLAN can communicate without any firewall audit. This issue is illustrated in the diagram in Figure 7.

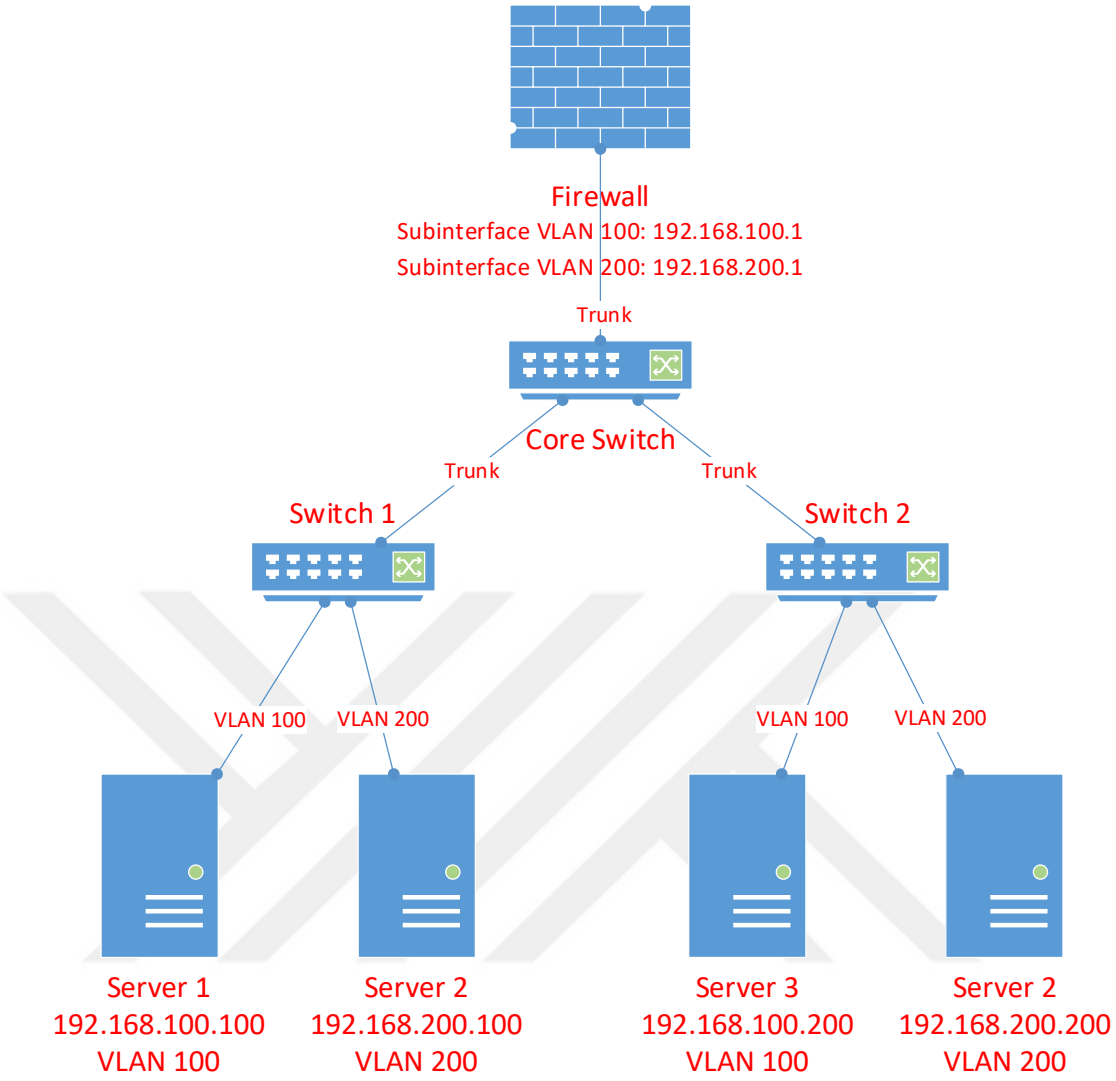

Figure 7: General firewall placement in traditional networks

In the diagram, servers 1 and 2 are connected to Switch 1, and servers 3 and 4 are connected to Switch 2. Although servers 1 and 3 are connected to different switches, they are on the same VLAN, just as servers 2 and 4. Servers 1 and 3 communicate with each other via the core switch without any audit of the firewall. However, servers 1 and 2, which are connected to the same switch, have to communicate with each other via the firewall. Therefore, servers that are on different VLANs are controlled by the firewall.

Any vulnerability in a server that is not under firewall control is also a problem for other servers in the same IP domain (same VLAN). In our diagram, any malware on Server 1 is also a threat to Server 3. To solve this problem, it is possible to install

virtual firewalls next to each host in the SDN with the contribution of virtualization (Figure 8).

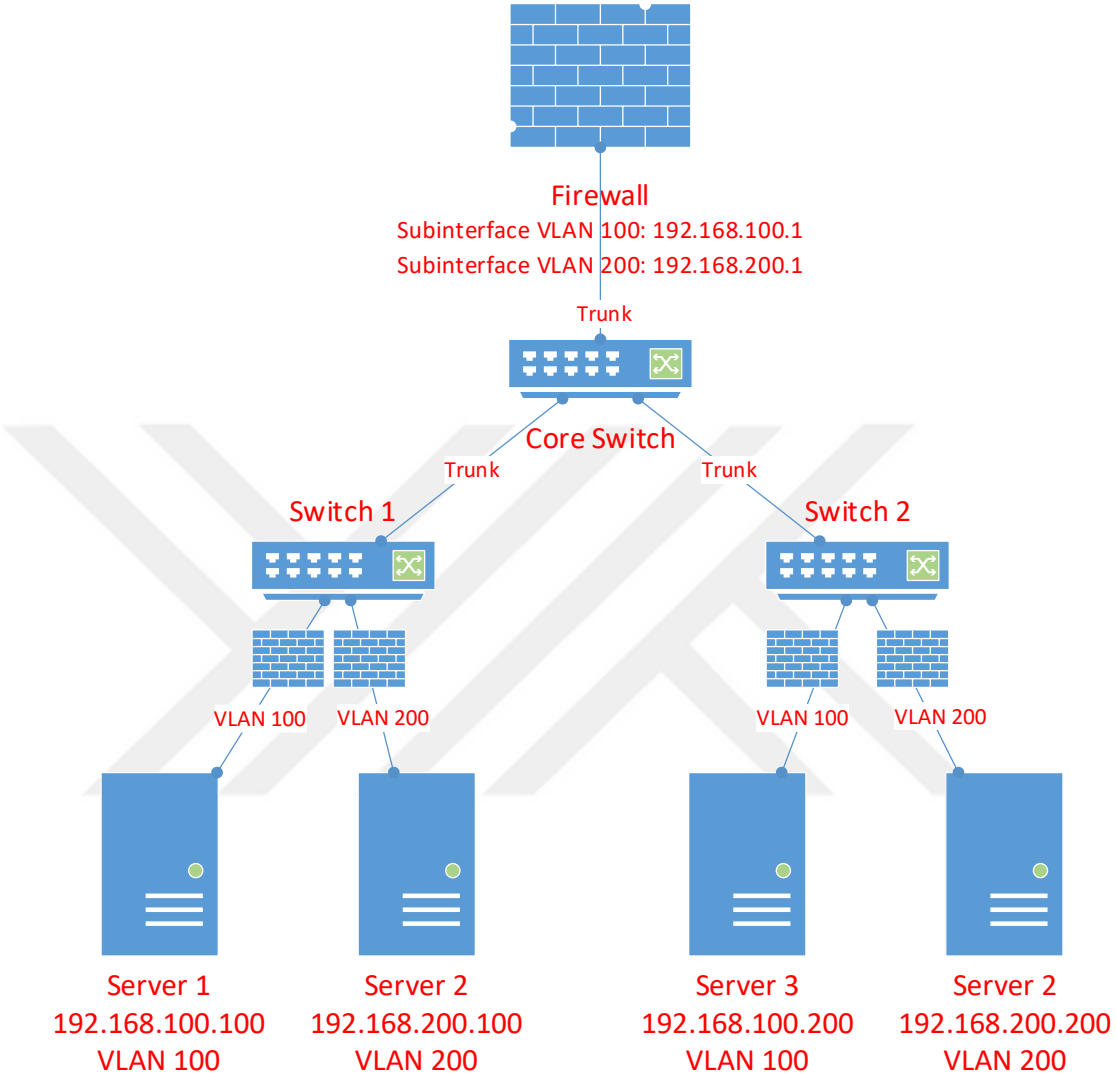

Figure 8: Firewall placement in a virtualized environment

It is possible to have a virtual firewall for each server in a virtualized environment. As previously mentioned, in the SDN approach, with the help of integration of vendors and the capabilities of virtualization, servers become more secure.

On the other hand, in brief, the SDN approach uses VXLAN as VLAN to tunnel Layer 2 connections over a Layer 3 network [77]. Therefore, each connection from the server to the switch to which it is attached is Layer 2, and the remainder of the

connection is Layer 3 and it becomes possible to audit the communication in the same IP domain.

3.4. IMPACT OF NEW PLAYERS ADOPTING AN SDN ON NETWORK PROCEDURES

SDNs affect networking from the first purchase to operating and service delivery. There have been companies that have dominated the network market for many years. SDNs may cause the share of small companies to increase in the market. This is possible with software development on dummy hardware.

In traditional networks, it had been necessary and habitual to meet with one of the few large network manufacturers, to purchase their products at high prices, and to stay in contact with these manufacturers throughout the entire service period.

With SDNs, the determination of the need, preparation of the specification, pre-purchase acceptance tests, initial installation, commissioning, support in cases of failure, replacement of defective equipment, product license renewals and all other similar processes have changed. Now, companies can meet their needs at far more affordable prices by purchasing white boxes and by providing as many features as they need through software.

Since the requirements and software are provided by a third-party company for externally supplied hardware, acceptance test procedures may also change. The tests on the acceptance of the network infrastructure obtained through software developments made white boxes more important for the health of the entire system. For this reason, the network services being provided to customers with the relevant network infrastructure are directly dependent on the outputs obtained from these tests because the supply of hardware and software from different companies increases the importance of first acceptance tests in terms of software hardware compatibility. The capacity of the network infrastructure is important in the sector where the need for capacity is increasing and “as a service” cloud services are becoming widespread. Therefore, it may be necessary to make more detailed calculations on the SLAs determined with customers.

The Volkswagen example mentioned in Chapter 2 showed that in cloud technologies, which are increasingly used, meeting network SLAs has become a crucial issue for companies that affect the core business. According to the CFO of

AT&T's John Stephens, SDNs are expected to save customer service cycle times, and improve service turn up [78]. The delay and packet loss amounts provided by an SDN are of great importance in meeting the needs in cloud technologies. The widespread use of SDN by major cloud service providers is also an indication of this.

Modifications in the business processes is not uncommon, and the improvements in the network technologies give rise to such changes. It is important to ensure adaptation to these procedural changes in terms of network technologies, such as SDNs.

3.5. CHANGES TO BUSINESS PROCESS DESIGNS WITH SDNs

Implementing an SDN in an IT infrastructure requires a holistic change for each IT asset and process. For instance, having more than one main function with a virtual cluster changes the asset management approach. This combination causes merging, or units to work closely according to business requirements.

In traditional networks, since each device responsible for their function works independently from other devices, skills were also defined on the basis of functions. Today and in the future, the presentation of functions over combined products, as well as the increase in the weight of the software, shows that function-based job definitions are gradually decreasing. As mentioned previously, network administrators learn data formats such as XML, JSON, YAML, define objects in software programs, and perform function and inheritance operations. This situation has also affected the training and certification systems of companies, as mentioned in Chapter 2, and as exemplified by Cisco Devnet and Juniper JNCIA-DevOps. In the past, there were only function-defined certification paths, such as network, security, data center, and WIFI. Lately, software capabilities and expertise have been added to the relevant certification and training systems. It can also be seen in the training processes of the Cisco and Juniper networks mentioned in Chapter 2 that not only topics, such as enterprise network, security, WIFI, and datacenter, but also certification paths covering software issues are defined for network administrators, such as Devnet and JNCIA-DevOps.

In IT departments that commonly work with function definitions, software developers, system administrators, network administrators and security administrators are defined separately from each other. However, with technologies such as the SDN, teams that listen to each other's needs and provide integrations that work more closely

than in the traditional approach, even if they are defined separately in the organizational charts.

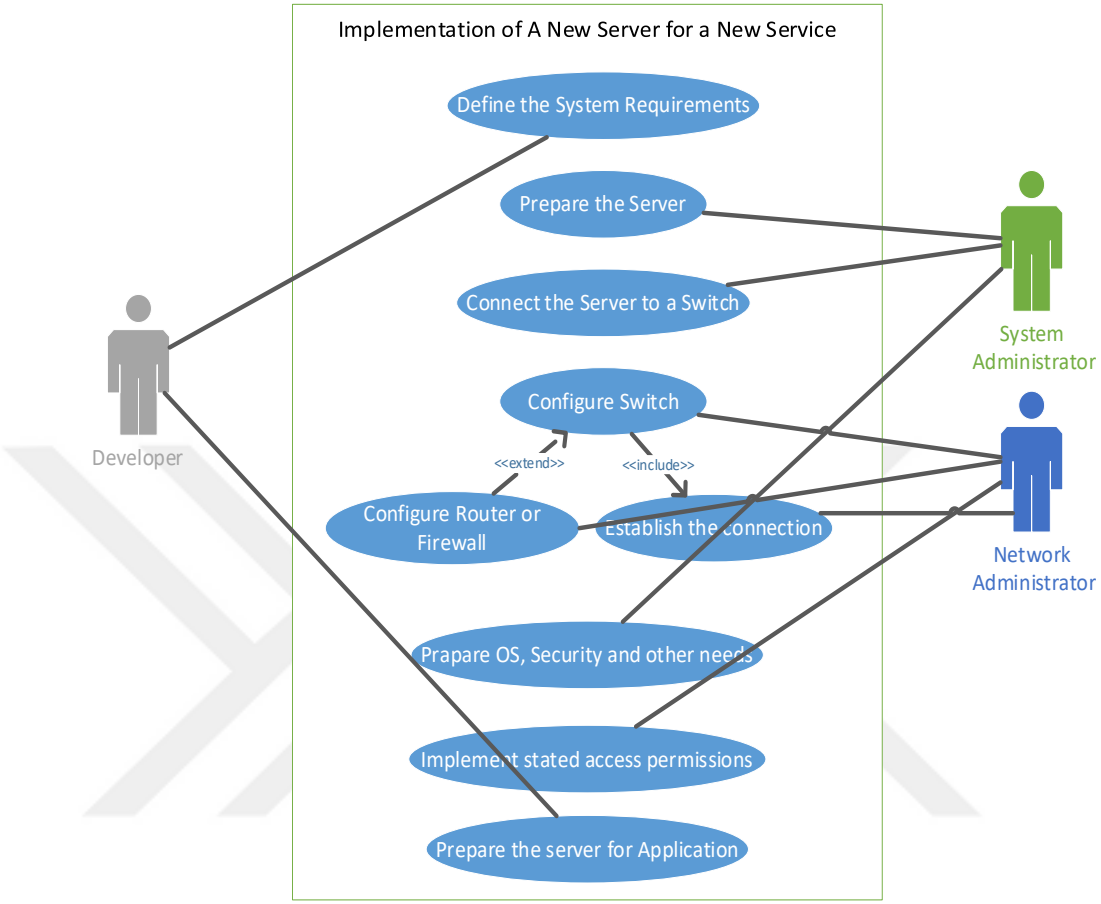

Figure 9: UML diagram of an implementation of a new server with the traditional approach

In the diagram in Figure 9, the duties of different units during the commissioning of a server or database are defined. It can be seen that commissioning a server involves quite a few independent tasks in traditional networks. However, with an SDN, the workflow becomes much simpler with the integration of the network and system vendors mentioned in Section 3.1 or with products that can handle all system and network requirements directly through their own appliances by virtualization, such as VMware or F5.

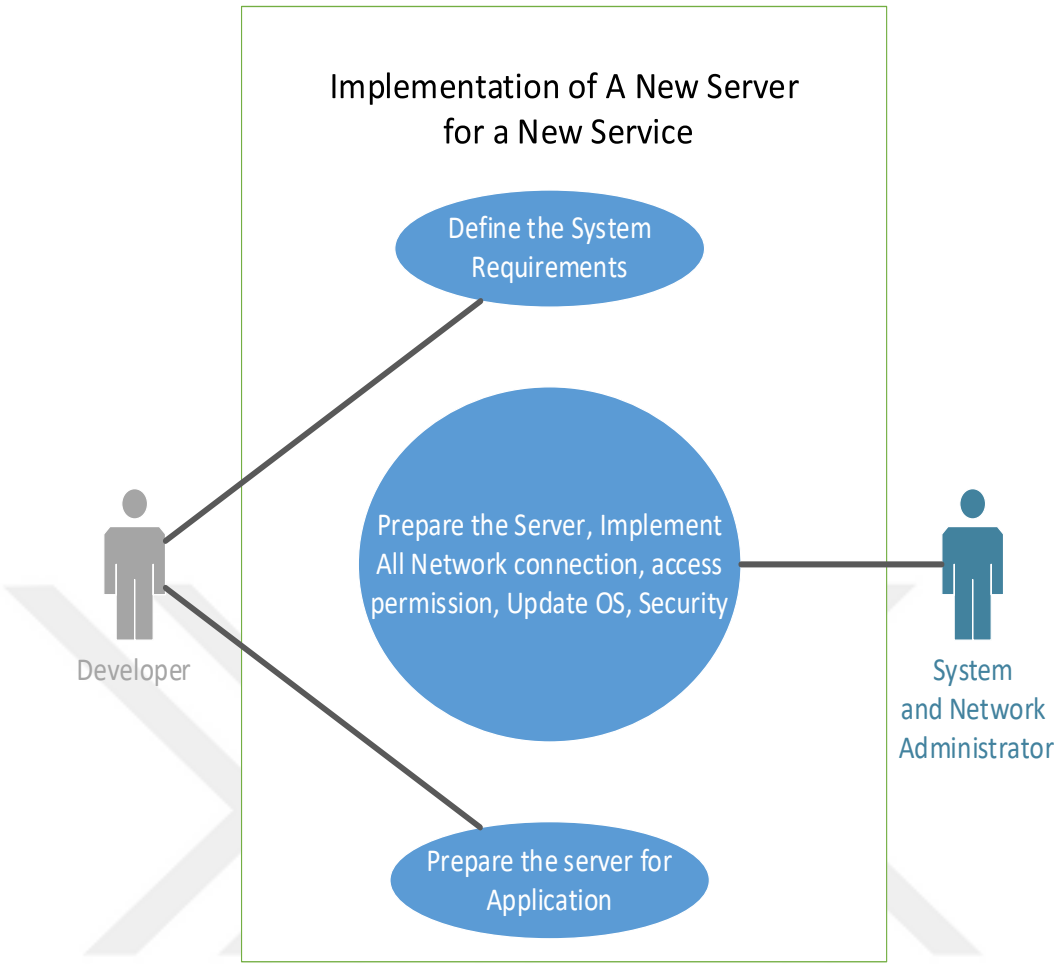

Figure 10: UML diagram of an implementation of a new server with the SDN approach

It can be seen in Figure 10 that it does not seem possible for future network solutions to establish traditional function-independent or product-independent units. It is becoming increasingly important to speed up and streamline the workflow and shorten the time to deploy a service. Therefore, companies that establish new networks would focus on the ability to perform multiple functions with as less hardware as possible. Moreover, as a result of this situation, the staff responsible for the operation of these products would be expected to perform multiple functions. As mentioned previously, this situation is reflected in educational paths. As different functions can be offered in a single product or in integrated products, the job descriptions of network specialists approach each other, and as a result, networkers who understand the system or system administrators who understand the network, etc. become desirable in the market.

3.6 BENEFITS OF SDNs

In this chapter, we studied some of the benefits of an SDN, which enables some organizational changes with an SDN. Some of these include obtaining what is needed with less hardware, fast first provisioning, automation with OpenFlow and standard configuration processes with NETCONF. Another benefit of an SDN includes how organizational change is related to software capabilities that eliminate the need to work with vendors that dominate the sector and increase the market share of small-scale vendors. On the other hand, it can be said that an SDN changes some of the business process designs as exemplified in figures 9 and 10, showing the provisioning of a new server for services.

In addition to the benefits mentioned, the list of studies in the literature cited in the thesis on some key issues in the comparison of SDNs and traditional approaches are listed in Table 1.

Table 1: References about the benefits of an SDN in the study

Benefits of SDN	**References**
Boosting Innovation	[6], [7], [8], [9], [17], [18], [19], [21], [28], [29], [35], [50]
OPEX and CAPEX savings	[20], [21], [23], [54]
Better performance, easy to **manage**	[17], [18], [19], [27], [28], [31], [32], [33], [34]
Fast provisioning for new servers	[27], [29], [37], [44], [72], [73]
New requirements by HR	[39], [40], [42], [64], [65]
More secure networks	[31], [32], [45], [49], [50], [60], [77]
Non-vendor centric infrastructure	[22], [23], [39], [40], [41], [43]
As an alternative: small scale vendors	[20], [21], [23], [26], [29], [42], [43]

Considering the comparisons and benefits, which emerged as a result of the literature review and examination of the situations of some major vendors, the next chapter presents the findings and limitations as a conclusion of the study.

4. CONCLUSION

4.1. FINDINGS

Decoupling of control and data planes accelerated innovation in network technologies.

In an SDN, data and control planes are separated. Separating the planes facilitates the partition of a business. In this manner, innovation in network technologies, such as traffic engineering, and security and configuration management, accelerates. The fact that hardware can be easily supplied as white box and that the software is not dependent on hardware vendors in the development of the software becomes one of the reasons for this acceleration. (Sections 2.1.2, 2.2.1 and 2.2.2)

It is less expensive to set up a new network with a Software Defined Network.

Networks, by having dummy hardware, only require that software be developed on top of it, and the purchase of many licenses is not needed in the procurement of a device. This means that it is cheaper for network administrators to set up a new network. With an SDN, as a result of separating the control and data layers in devices, supplying only devices with the data layer and fulfilling the needs in the control layer with a central controller ensures that products are supplied more cheaply. In traditional networks, devices are much more expensive due to the coexistence of the control and data planes. One of the reasons for this high cost is the license fees of the protocols running on the control plane. Blackbox devices, where all the features are licensed without selecting the licenses the company actually needs, are both expensive and available only from quasi-monopolistic vendors. (Sections 2.1.3, 2.2.1, 2.2.3 and 3.1)

With the decrease in the number of middleboxes and integration with other devices in the IT environment, the performance of the network increases and it becomes easier to monitor and manage.

As a result of the decoupling of data and control planes, the use of middleboxes has decreased due to the increase in integration with network management, virtualization and other product groups, such as servers or storage, provided through the controller. Furthermore, reducing the number of devices in the environment and providing the functions of multiple devices through a single device also provides energy, space and capital savings. Fewer devices also means easier network and asset management, less risk, a lower probability of devices being attacked and a less complex network. It becomes easier to manage networks that have basic and essential devices. Fewer devices will also reduce hop count. Therefore, delay and jitter are also reduced. Another issue related to asset management is that maintenance and license control of fewer devices, control of physical requirements, and change management processes become easier. As a result, meeting the tasks of middleboxes with fewer products in an SDN will provide administrative convenience, savings and less complexity. (Sections 2.2.1, 2.2.3 and 3.1)

Adding a new service to the network has become easier and safer. This increases the speed of service management that concerns the customer.

Integration with virtualization products offers an easier provisioning opportunity. The network configuration of a virtual server can be easily performed by a virtual hosting tool that is compatible with, and able to communicate with, the network product in the environment. With virtualization becoming increasingly important for the protection of resources, this integration of an SDN in a shorter time offers a safer, more automated, and less human intervention in the initial setup. In this way, customer service times are also expected to decrease. (Sections 2.2.1.2, 2.2.2 and 3.1)

An SDN increases the level of knowledge of administrators in relation to areas of expertise.

Corresponding integration makes network and system administrators communicate more closely. Moreover, a system administrator can do some of the limited first implementation work of the network administrator and vice versa. This makes it possible to maintain a business with fewer employees. Another important result is that to facilitate the transition to an SDN, vendors have added trainings of configuring software defined networks into their training and certification programs. Vendors' new training models show that network managers must adapt to software

developments for their career development. This allows administrators to be informed about any related field of specialization and to understand each other's needs and expectations more easily. This promises companies to meet multiple functions with fewer administrators. (Sections 2.2.4.2 and 3.5)

An SDN enables more secure networks

Another important point is that because of the Layer 3 structure of SDN, it is possible to use a security product for each server. While the transition from Layer 2 to Layer 3 in traditional networks is possible in aggregation switches or directly in core switches, tunneling with the VXLAN protocol used by an SDN reduces Layer 2 traffic in the environment. Thus, direct traffic passes to Layer 3 in the edge switch to which the server is connected. In summary, an SDN supports more a secure environment; however, the probability of single points of failure keeps this argument open to discussion. (Sections 2.2.1, 2.2.2, 2.2.3 and 3.3)

SDN enables software development capabilities and reduces the necessity of vendor-defined configuration.

An SDN reduces manual configuration, allows programming and offers a rich coding opportunity with the advantage of using open source software libraries. By meeting software needs completely in the northbound, environments where software developers can easily find what they need are provided. This also reduces the need for the demanding protocol knowledge required to become a network administrator. Knowing how a protocol works in traditional networks, knowledge of configuring the relevant device of the relevant vendor, which is essential, ceases to be important with an SDN. An SDN encourages common configuration scripts in several languages for all vendors in a specific data format. Device configurations are made with standard data models. This means that approximately the same configuration language is used for all vendors. (Sections 2.2.1 and 3.5)

An SDN offers new opportunities to small-scale vendors by reducing the dominance of large vendors that dominate the market.

The use of SDNs is increasing with the standardization of OpenFlow in traffic monitoring, NETCONF in device configuration, and the adoption of the relevant standards by the major vendors that dominate the industry. Thus, an SDN increases the market share for small and medium-sized hardware vendors.

4.2. LIMITATIONS

This thesis was limited by a number of factors. The study was prepared with the information in the literature and a number of the vendors' white papers and datasheets although some switch configurations had been tested to be exemplary. Similarly, no fieldwork was conducted with local or global experts who had experienced the subject.

The transitional stages of redesigning an existing network with the SDN approach and how this transition would affect a company's administration were not discussed.

While the study focused on general enterprise companies, the effect of company and network size was not investigated in the study.

The impact of the SDN approach on ISP and network carrier companies was not considered. In this study, IT jobs outsourced by the service procurement method were not studied since studies have already been made on companies that directly loaded their IT processes.

In this study, no evaluations were made in terms of international standards such as ITIL, COBIT, CMMI, SPACE or ISO/EC 27001.

Additionally, IT management, administrative, management financial management, project management, etc. processes were not evaluated from an integrated perspective.

Major vendors, such as Cisco Networks, Juniper Networks, Arista Networks, and Huawei Networks, were the subject. However, no evaluation was made for the products of niche vendors.

4.3. FUTURE WORKS

Although we witness the rapid adoption of the SDN approach in the industry, it would be useful to examine the approaches and findings in this study in the transition stages and processes after the decision is made to adopt the SDN approach in a company operating in a traditional network.

The results of the SDN approach in more than one company should be evaluated with field studies.

The capabilities that manufacturers claim about their products in datasheets and whitepapers should be tested in a lab environment.

In the future work of this study, the effects of the SDN approach on new technological paradigms, such as artificial intelligence and the Internet of Things, should be studied.

4.4. CONCLUSION

In this study, the effect of the SDN approach on a company's IT infrastructure and processes is examined. The main focus is the IT structure of enterprise companies whose main business is not a telecommunication or Internet service provider. Network structures of large operators whose main business is network service provision and network infrastructures of enterprise companies are very different from each other. In general, three different network structures that an enterprise company will have are emphasized. These are LAN, WAN and Datacenter.

In this thesis, studies are made on the literature on basic network architecture and infrastructure, savings, human resources, network security and management.

The engineering differences between the traditional network approach and the SDN approach have shown that the influence of hardware, the hardware manufacturer, and the use of function-defined devices has decreased. In addition, in the SDN approach, the sector's encouraging effect was observed in increasing the basic server management and software knowledge levels of network administrators. For this reason, it can be said that such units are encouraged to work more closely with each other due to the integrations and associations brought about by the SDN approach. Moreover, opportunities arise for the network administrator and the system administrator to learn and perform some of each other's work.

With the SDN approach, companies have become able to meet their customers' needs faster and more securely. With the opportunities brought by virtualization and a software-defined environment, initial provisioning is accelerated, hop count is decreased and it becomes possible to establish more seamless networks in terms of delay and packet loss.

Another effect of the SDN paradigm in the industry is the decrease in the effect of the vendor-centric approach and the increase in the opportunities of niche vendors. In the SDN approach, where it is possible to eliminate the obligation of owning all of the basic licenses, companies are only required to pay for the licenses they use, and

even save on the installation and operation of network infrastructure due to reduced dependency on large vendors.

As a conclusion of all these studies, we believe we have answered our research question: “What are the benefits of the SDN approach to an IT department compared with a traditional approach?”

Finally, considering the limitations and discussions, it was observed in our study that the SDN approach offers remarkable organizational changes and benefits in network management.

REFERENCES

1. Salazar-Chacón Gustavo D. and. Reinoso García Andy R (2021), "Segment-Routing Analysis: Proof-of-Concept Emulation in IPv4 and IPv6 Service Provider Infrastructures", *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, pp. 1-7, doi: 10.1109/IEMTRONICS52119.2021.9422559.

2. Salazar-Chacón Gustavo D. (2022), "Hybrid Networking SDN and SD-WAN: Traditional Network Architectures and Software-Defined Networks Interoperability in digitization era", *Journal of Computer Science and Technology*, Volume 22, Number 1, pp. 93-97, doi:10.24215/16666038.22.e07

3. Awais Muhammad, Asif Muhammad, Ahmad Maaz Bin, Mahmood Toqeer and Munir Sundus (2021), "Comparative Analysis of Traditional and Software Defined Networks", *2021 Mohammad Ali Jinnah University International Conference on Computing (MAJICC)*, 2021, pp. 1-6, doi: 10.1109/MAJICC53071.2021.9526236.

4. "SDN vs Traditional Networking: Which Leads the Way?" http://www.chinacablesbuy.com/sdn-vs-traditional-networking-which-leads-the-way.html (Access Date: 02.02.2022)

5. Bhardwaj Ayush, Zhou Zhenyu and Benson Theophilus A. (2021), "A Comprehensive Study of Bugs in Software Defined Networks", *51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2021, pp. 101-115, doi: 10.1109/DSN48987.2021.00026.

6. S. Denazis, J. Hadi Salim, D. Meyer, D, and O. Koufopavlou (2015), "Software-Defined Networking (SDN): Layers and Architecture Terminology", RFC 7426, DOI 10.17487/RFC742

7. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner (2008), "OpenFlow: Enabling innovation in campus networks" *ACM SIGCOMM Computer Communications Review*.

8. T. Koponen, M. Casado, N. Gude, J. Stribling, L. Poutievski, M. Zhu, R. Ramanathan, Y. Iwata, H. Inoue, T. Hama, and S. Shenker. (2010), "ONIX: A distributed control platform for large-scale production networks." *In OSDI*, volume 10, pages 1–6,

9. U. Krishnaswamy, P. Berde, J. Hart, M. Kobayashi, P. Radoslavov, T. Lindberg, R. Sverdlov, S. Zhang, W. Snow, G. Parulkar (2013), *"ONOS: Open Network Operating System An Experimental Open-Source Distributed SDN OS"*. http://tinyurl.com/pjs9eyw

10. Reyes Ronald Romero, Sultana Shabnam, Pai Vishwanath Vijayakumar and Bauschert Thomas (2019), "Analysis and Evaluation of CAPEX and OPEX in Intra-Data Centre Network Architectures", 2019 *IEEE Latin-American Conference on Communications (LATINCOM),* pp. 1-6, doi: 10.1109/LATINCOM48065.2019.8937881.

11. Laudon Kenneth C, Laudon Jane P. (2020), *Management Information Systems: Managing the Digital Firm* 16th ed, Pearson Education, ch 13.

12. A.A. Shah et al. (2020), "A Real-time Simulation Framework for Complex and Large-scale Optical Transport Networks based on the SDN Paradigm", *2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT),* pp. 1-4, doi: 10.1109/DS-RT50469.2020.9213701.

13. F. Benamrane, M. Ali, D.K. Luong, Y.-F. Hu, J.-P. Li and K. Abdo, (2019), "Bandwidth Management in Avionic Networks based on SDN Paradigm and ML Techniques", *2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC),* pp. 1-9, doi: 10.1109/DASC43569.2019.9081746.

14. Pawel Parol and Michał Pawlowski (2013), "Towards networks of the future: SDN paradigm introduction to PON networking for business applications", *2013 Federated Conference on Computer Science and Information Systems,* pp. 829-836.

15. Dumba Braulio, Mekky Hesham, Jain Sourabh, Sun Guobao, Zhang and Zhi-Li (2016), "A Virtual Id Routing Protocol for Future Dynamics Networks and Its Implementation Using the SDN Paradigm", Journal of Network & Systems Management, 24(3):578-606. doi:10.1007/s10922-016-9373-0

16. Xiaogang Tu, Xin Li, Jiangang Zhou and Shanzhi Chen (2014), "Splicing MPLS and OpenFlow Tunnels Based on SDN Paradigm", *2014 IEEE International Conference on Cloud Engineering*, pp. 489-493, doi: 10.1109/IC2E.2014.20.

17. Yang Gyeongsik, Yu Bong-yeol, Jeong Wontae and Yoo Chuck (2018), "FlowVirt: Flow rule virtualization for dynamic scalability of programmable network virtualization", *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pp. 350-358.

18. G. Yang Gyeongsik, Yoo Yeonho, Kang Minkoo, Jin Heesang and Yoo Chuck (2021), "Bandwidth isolation guarantee for SDN virtual networks", *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, pp. 1-10.

19. A. Al-Shabibi, M. De Leenheer, M. Gerola, A. Koshibe, G. Parulkar, E. Salvadori et al. (2014), "OpenVirteX: Make your virtual SDNs programmable", *Proceedings of the third workshop on Hot topics in software defined networking*, pp. 25-30, 2014.

20. Ehtesham Habeeb (2022), "Why do Businesses Need to be Prepared for SDN Transition?". https://www.extnoc.com/blog/businesses-prepare-for-sdn-transition/ (Access Date: 20.05.2022)

21. R. Perez, A. Zabala and A. Banchs (2021), "Alviu: An Intent-Based SD-WAN Orchestrator of Network Slices for Enterprise Networks", *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, pp. 211-215, doi: 10.1109/NetSoft51509.2021.9492534.

22. Maleh Yassine, Qasmaoui Youssef El Gholami Khalid, Sadqi Yassine and Mounir Soufyane (2022), "A comprehensive survey on SDN security: threats, mitigations, and future directions", *Journal of Reliable Intelligent Environments*, pp.1-39, doi: https://doi.org/10.1007/s40860-022-00171-8

23. Elkhatib Yehia, Coulson Geoff and Tyson Gareth (2017), "Charting an intent driven network*", 2017 13th International Conference on Network and Service Management (CNSM),* pp. 1-5, doi: 10.23919/CNSM.2017.8255981.

24. Zhao Yong, Wang Xingwei, He Qiang, He, C. Zhang and Huang Min (2021), "PLOFR: An Online Flow Route Framework for Power Saving and Load Balance in SDN", *in IEEE Systems Journal*, vol. 15, no. 1, pp. 526-537, M doi: 10.1109/JSYST.2020.3010971.

25. Alnoman Ali and Anpalagan Alagan (2019), "A SDN-Assisted Energy Saving Scheme for Cooperative Edge Computing Networks", *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9013409.

26. Collymore Wayne (2019), "A Preemptive Hybrid Approach to Minimum Spanning Tree Restoration in Large Mesh SDN Networks," *2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 82-89, doi: 10.1109/FiCloudW.2019.00028.

27. Cedillo-Elias E. Julieta, Larios Victor M, Orizaga-Trejo J. Antonio, Lomas-Moreno Carlos E., Ramirez J. Raul Beltran and Maciel Rocio (2019) "A Cloud Platform for Smart Government Services, using SDN networks: the case of study at Jalisco State in Mexico", *2019 IEEE International Smart Cities Conference (ISC2)*, pp. 372-377, doi: 10.1109/ISC246665.2019.9071680.

28. Akyildiz Hasan Anil, Hokelek Ibrahim, Ileri Mervan, Saygun Ece and Cirpan Hakan Ali (2017), "Joint server and route selection in SDN networks", *2017 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 1-5, doi: 10.1109/BlackSeaCom.2017.8277663.

29. IBM Global Technology Services, "Software Defined Networking in the new business frontier", https://www.ibm.com/downloads/cas/RWJLRAWE (Access Date:14.01.2022).

30. Burke Pat (2021), "How SDN Supports a More Agile Business", *CIO Insight*, https://www.cioinsight.com/infrastructure/how-sdn-supports-a-more-agile-business/ (Access Date:18.03.2022)

31. Mauricio Leopoldo A. F., Rubinstein Marcelo G., Duarte Otto Carlos M. B. (2018) "ACLFLOW: An NFV/SDN Security Framework for Provisioning and Managing Access Control Lists," *2018 9th International Conference on the Network of the Future (NOF)*, pp. 44-51, doi: 10.1109/NOF.2018.8598136.

32. C. Bharanidharan, I. Gandhi and R.D. Devapriya (2021), "An Enhanced Framework for Traffic Load Balancing and QoS Provisioning in SDN", *Wireless Personal Communication 121*, 3451–3472, https://doi.org/10.1007/s11277-021-08886-2

33. Miguel Pineda Jacob, Valdez Julian Troy, and Tan Wilson M. (2019), "Leveraging SDN and NFV for Provisioning Quality Network Infrastructure for Filipino Public Schools", *2019 IEEE R10 Humanitarian Technology Conference (R10-HTC)(47129)*, pp. 104-109, doi: 10.1109/R10-HTC47129.2019.9042444.

34. Tantayakul Kuljaree, Dhaou Riadh and Paillassa Beatrice (2017), "Mobility management with caching policy over SDN architecture", *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pp. 1-7, doi: 10.1109/NFV-SDN.2017.8169830.

35. Mark Mitchiner Mitch and Prasad Reema (2014), "Software-Defined Networking and Network Programmability: Use Cases for Defense and Intelligence Communities", https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/software_defined_networking.pdf (Access Date: 05.01.2022)

36. Ehtesham Habeeb (2022), "Why do Businesses Need to be Prepared for SDN Transition?", https://www.extnoc.com/blog/businesses-prepare-for-sdn-transition/ (Access Date: 21.01.2022)

37. Zaballa Eder Ollora, Franco David, Jacob Eduardo, Higuero Marivi and Berger Michael Stubert (2021) "Automation of Modular and Programmable Control and Data Plane SDN Networks," *2021 17th International Conference on Network and Service Management (CNSM)*, pp. 375-379, doi: 10.23919/CNSM52442.2021.9615508.)

38. S. Al-Rubaye and J. Aulin (2017) "Grid Modernization Enabled by SDN Controllers: Leveraging Interoperability for Accessing Unlicensed Band", in IEEE Wireless Communications, vol. 24, no. 5, pp. 60-67, doi: 10.1109/MWC.2017.1700089.)

39. Openflow, Cisco Whitepaper https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960xr/software/15_2_7_e/configuration_guide/b_1527e_consolidated_2960xr_cg/openflow.pdf (Access Date: 02.02.2022)

40. Openflow, Juniper Networks Whitepaper https://www.juniper.net/documentation/us/en/software/junos/sdn-openflow/topics/concept/junos-sdn-openflow-supported-platforms.html (Access Date: 02.02.2022):

41. Arista Networks, OpenFlow, Arista Networks User Manuel, https://www.arista.com/en/um-eos/eos-openflow#:~:text=OpenFlow%20is%20supported%20on%20both,ingress%20port%20is%20silently%20dropped (Access Date: 02.02.2022)

42. ONF OpenFlow Conformant: Certified Product List, ONF, https://opennetworking.org/product-registry/ (Access Date: 29.03.2022)

43. K. Nikoloval, I Atanasov and E. Pencheval (2018), "Software Defined Networks And OpenFlow: A Survey", *18 th International Multidisciplinary Scientific GeoConference SGEM*, Sofia, Vol. 18, Iss. 6.3, doi:10.5593/sgem2018/6.3/S27.090, https://www.proquest.com/openview/dc259c7090d861587dff410fead4c380/1?pq-origsite=gscholar&cbl=1536338 (Access Date:15.01.2022)

44. Schneider Ben, Zoitl Alois, Wenger Monika and Blech, Jan Olaf. (2017), "Evaluating software-defined networking for deterministic communication in distributed industrial automation systems", *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1-8, doi: 10.1109/ETFA.2017.8247594.

45. Y. Al Mtawa, A. Haque and H. Lutfiyya (2021), "Migrating From Legacy to Software Defined Networks: A Network Reliability Perspective", in *IEEE Transactions on Reliability*, vol. 70, no. 4, pp. 1525-1541, doi: 10.1109/TR.2021.3066526.

46. Richard Smith-Bingham (2019), "This is What CEOs Around The World See As The Biggest Risks to Business", https://www.weforum.org/agenda/2019/10/risks-to-doing-business-2019-developing-developed/ (Access Date: 20.05.2022)

47. "Securing What's Now and What's Next 20 Cybersecurity Considerations for 2020" *Cisco Cybersecurity Report Series 2020,* https://securitydelta.nl/media/com_hsd/report/278/document/2020-ciso-benchmark-cybersecurity-series-feb-2020.pdf (Access Date: 23.02.2022)

48. Rimol Meghan (2022), "Gartner Identifies Top Security and Risk Management Trends for 2022" https://www.gartner.com/document/3981492?ref=solrAll&refval=287935324 (Access Date: 04.03.2022)

49. Yungaicela-Naula Noe M., Vargas-Rosales Cesar, Pérez-Díaz Jesús Arturo and Zareei Mahdi (2022), "Towards security automation in Software Defined Networks", Computer Communications, Volume 183, Pages 64-82, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2021.11.014.

50. Chiliquinga Santiago, Manzano Santiago, Cordova Patricio, Garcia Marcelo V. (2020), "An Approach of Low-cost Software-Defined Network (SDN) Based Internet of Things", *2020 International Conference of Digital Transformation and Innovation Technology (Incodtrin)*, pp. 70-74, doi: 10.1109/Incodtrin51881.2020.00025.

51. Zaheer Amer, Asghar Muhammad Zeeshan and Qayyum Amir (2021), "Intrusion Detection and Mitigation Framework for SDN Controlled IoTs Network", *2021 IEEE 18th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET),* pp. 147-151, doi: 10.1109/HONET53078.2021.9615458.

52. Elfaki Abdelrahman Osman and Bassfar Zaid (2022), "Configuration of Business Process Workflow in Software as a Service: Validation of Constraint Dependency relationships", *2022 2nd International Conference on Computing and Information Technology (ICCIT),* pp. 359-362, doi: 10.1109/ICCIT52419.2022.9711622.

53. Williams David (2020), "Driving Transformative Experiences with Software-Defined Networks", https://www.telstra.com.au/business-enterprise/news-research/case-studies/driving-transformative-experiences-with-sdn (Access Date: 05.02.2022)

54. IBM Academy of Technology Red Hat OpenShift solution design guidance, *"All network communication is managed by the SDN, so no extra routes are needed on your virtual networks to achieve pod to pod communication."* https://www.ibm.com/cloud/architecture/articles/ibmaot-redhat-openshift/02-solutions-guide-networking-openshift-sdn (Access Date: 03.05.2022)

55. Google, *"Design your network infrastructure"*, Available (04.05.2022): https://cloud.google.com/architecture/framework/system-design/networking

56. Microsoft, Software Defined Networking (SDN) in Azure Stack HCI and Windows Server, 2022, https://docs.microsoft.com/en-us/azure-stack/hci/concepts/software-defined-networking (Access Date: 05.05.2022):

57. Shackleford Dave, and Khasnis Sagar (2022), "How to Implement a Software-Defined Network Security Fabric in AWS", *Webinar Series,* https://pages.awscloud.com/awsmp-ss-sec-Fortinet-SoftwareDefinedSec.html?ref_=awsmp_sol_sec_wb_impsftsecfab (Access Date: 04.05.2022)

58. Bilgi ve İletişim Güvenliği Tedbirleri (2019), "*2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi",* https://cbddo.gov.tr/bgrehber/2019-12-sayili-bilgi-guvenligi-tedbirleri-cumhurbaskanligi-genelgesi/ (Access Date: 15.03.2022)

59. VMware NSX Datasheet, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-datasheet.pdf (Access Date: 23.04.2022)

60. Kaur Karamjeet, Kumar Krishan, Singh Japinder and Singh Ghumman Navtej (2015) "Programmable firewall using Software Defined Networking", *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom),* pp. 2125-2129.

61. Moy John (2008), OSPF Version 2. https://datatracker.ietf.org/doc/html/rfc2328 (Access Date: 22.05.2022)

62. McKeown Nick, Anderson Tom, Balakrishnan Hari, Parulkar Guru, Peterson Larry, Rexford Jennifer, Shenker Scott and Turner Jonatan (2008), "OpenFlow: Enabling Innovation in Campus Networks", *ACM SIGCOMM Computer Communication Review,* Volume 38, Number 2, pp. 69-74.

63. Career Certification Pathways from Cisco (2018), https://honim.typepad.com/biasc/2018/02/career-certification-pathways.html (Access Date: 22.12.2021)

64. Career Certification Pathways from Cisco (2020), https://www.cisco.com/c/dam/en_us/training-events/certifications/career-path.pdf (Access Date: 22.12.2021)

65. Juniper Networks, "2020 Certification and Training News". https://www.juniper.net/us/en/training/news-2020.html (Access Date: 13.04.2022)

66. Cisco Networks (2020), "2020 Global Networking Trends Report". https://www.cisco.com/c/dam/m/en_us/solutions/enterprise-networks/networking-report/files/GLBL-ENG_NB-06_0_NA_RPT_PDF_MOFU-no-NetworkingTrendsReport-NB_rpten018612_5.pdf (Access Date: 04.03.2022)

67. Gilad Jonatan (2020), "SDN is Growing Up – It's called IBN". https://blogs.cisco.com/networking/sdn-is-growing-up-its-called-ibn (Access Date: 05.06.2022)

68. Cisco Networks, "Software-Defined Networking Provision, manage, and program networks more rapidly". https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html#~what-is-sdn (Acces Date: 03.02.2022)

69. Cisco Networks, "Leading Research University Expands Research Networking Capabilities for an Enhanced User Experience". https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/OCA/Assets/Education/Montana_State_University_Case_Study.pdf (Access Date: 04.05.2022)

70. Juniper Networks, "AGILITY WITHOUT COMPROMISE WITH JUNIPER SDN" https://www.juniper.net/content/dam/www/assets/solution-briefs/us/en/agility-without-compromise-with-juniper-sdn.pdf (Access Date: 02.05.2022)

71. TechRepublic Staff, "VMware NSX: A cheat sheet", https://www.techrepublic.com/article/vmware-nsx-the-smart-persons-guide/ (Access Date: 03.05.2022)

72. Lage Juan (2018), "Running RHV integrated with Cisco ACI", *Red Had Summit*,https://www.redhat.com/files/summit/session-assets/2018/Running-Red-Hat-Virtualization-integrated-with-Cisco-ACI-SDN-Distribution.pdf (Access Date: 22.04.2022)

73. Arista Networks, "Arista Introduces Network Applications with VMwareand Microsoft". https://s21.q4cdn.com/861911615/files/doc_news/Arista-Introduces-Network-Applications-with-VMware-and-Microsoft.pdf (Access Date: 23.04.2022)

74. Cisco Networks, "Data Model". https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-5/configuration_guide/prog/b_165_prog_9500_cg/data_models.pdf (Access Date: 03.05.2022)

75. Cisco Networks, "Converting CLI Commands to Network Configuration Format". https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/system-management/config/cisco_nexus7000_system-management_config_guide_8x/converting_cli_commands_to_network_configuration_format.pdf (Access Date: 04.05.2022)

76. Arista Networks, "EOS 4.28.1F User Manual". https://www.arista.com/en/um-eos/eos-link-layer-discovery-protocol#xx1149474 (Access Date: 04.05.2022):

77. Juniper Networks, "What is VXLAN?". https://www.juniper.net/us/en/research-topics/what-is-vxlan.html, (Access Date: 06.05.2022)

78. Buckley Sean (2014), "AT&T's Stephens: SDN will Save Customer Service Cycle Times, Improve Service Turn Up". https://www.fiercetelecom.com/telecom/at-t-s-stephens-sdn-will-save-customer-service-cycle-times-improve-service-turn-up (Access Date: 03.04.2022)