Mathematical Problems of Computer Science 58, 91–98, 2022.
doi: 10.51408/1963-0096

UDC 004.7

Network Management Automation Through Virtualization

Arusyak D. Manasyan

Institute for Informatics and Automation Problems of NAS RA
e-mail:armanasyan@iiap.sci.am

Abstract

The study aims to develop methods for automating network management by analyzing its virtual counterpart. The paper substantiates the relevance of this approach, identifies the advantages and disadvantages, highlights the existing problems, and suggests ways to solve them. As a result, the effectiveness of network virtualization was shown by the example of an experimental network.
Keywords: network, automation, virtualization, SDN (Software-Defined Network), OpenDaylight (Software), OpenFlow (Protocol).
Article info: Received 10 December 2021; received in revised form 8 July 2022; accepted 23 August 2022.

1. Introduction

The more devices are connected to the network, the more inconvenience there will be with the expenses of their utilization. And until the network system is automated, this problem will be constant. Organizations will spend a lot of money to buy powerful network devices, but network management will not become easier. That is why a study of network automation and virtualization was carried out, their current applications were discussed and solutions to existing problems were proposed.

As network traffic continues to grow, companies increasingly require large-scale network configurations. The move to cloud computing continues as enterprise customers and their applications rely more and more on network efficiency, so networks are expected to be highly reliable with minimal downtime. As the number of devices on the network increases, so does the need for uninterrupted, flexible, fast, and efficient communication between them. To do this, it is necessary to obtain a large number of network devices that will be of a high quality, and have great features, such as a large amount of memory, many interfaces, and powerful processors, and all this is associated with high costs, which is one of the main prerequisites for the emergence automation and virtualization concepts.

For service providers, automation is a key strategy to improve network agility and reliability while controlling operating and capital costs. Therefore, it is necessary to automate the work with network equipment. Automation of daily network tasks and functions, as well as automated monitoring of iterative processes, increases the availability of network services.

We can describe the current state of the networking industry as "critical". The market-dominant closed (proprietary) solutions are "boxes" for applications, and the interoperability of solutions from different vendors is best provided at the interface level. Networks are extremely complex, making them difficult to scale, manage, and trust. This slows down the further development of networks and programs running in them. Therefore, several solutions for network automation have been developed, and we talked about SDN in our research work. Software Defined Networking (SDN) introduces network virtualization capabilities, which makes it easier to build and manage network automation tasks. Using SDN, networks can be provisioned at the software layer, abstracting the underlying physical hardware. This takes automation to the next level and significantly accelerates network provisioning and configuration management. It also enables IT to attach network and security services to workloads using a policy-driven approach(see [1]). Today, network automation solutions allow us to perform a wide range of tasks, including network planning - design, including scenario planning - backup management, device testing - configuration testing, deployment of deployed physical devices - services, as well as virtual device deployment - provisioning devices, real-time network data collection systems related to applications, network topology, traffic, services, data analysis, including active artificial intelligence, machine learning analysis, to get an idea of the present and future, network behavior, check configuration compliance, to ensure all network devices and service requirements, software updates, including backing up software if necessary, fixing closed network issues, including troubleshooting, and complex, difficult-to-detect Troubleshooting activities, detailed analysis of reports, panels, alarms, warnings, compliance with security requirements, monitoring of the network and its services, service level to maintain customer satisfaction.

The purpose of this article is to show the benefits of network virtualization, present the tools necessary for this, and show its effectiveness as a result of the experimental application.

2.Analyses and Discussion

Network automation through SDN (see [2]) adds a number of capabilities to conventional automation paradigms, which optimize IT resources and require SDN as a networking architecture approach. It enables the control and management of networks using software applications. Through SDN networking, the behavior of the entire network and its devices is programmed in a centrally controlled manner through software applications using open APIs. SDN improves performance through network virtualization. In SDN[2] software-controlled applications or APIs work as a basis of complete network management that may be directing traffic on a network or communicating with underlying hardware infrastructure. So to put it simply, we can say that SDN can create virtual networks or control traditional networks with the help of software to improve security and reduce cost.

Traditional network refers to the old conventional way of networking, which uses fixed and dedicated hardware devices such as routers and switches to control network traffic. Inability to scale, as well as network security and performance are major concerns nowadays in the current growing business situation so SDN is taking control of traditional networks. The traditional network is static and based on hardware network appliances. Traditional network architecture was used by many companies until recent years but nowadays due to its drawbacks SDN has been developed and will be used more widely in the coming years(see [3]).

Table 1. Comparison of SDN to Traditional Network(see [3]).

No	**SDN**	**Traditional Network**
1	Virtual networking approach.	Old conventional networking approach.
2	Centralized control.	Distributed control.
3	Programmable network.	This network is nonprogrammable.
4	Open interface.	Closed interface.
5	Data plane and control plane are decoupled by software.	Data plane and control plane are mounted on the same plane.
6	It supports automatic configuration so it takes less time.	It supports static/manual configuration so it takes more time.
7	It can prioritize and block specific network packets.	It leads all packets in the same way with no prioritization support.
8	It is easy to program as per need.	It is difficult to program again and replace the existing program as peruse.
9	The cost is low.	The cost is high.
10	Structural complexity is low.	Structural complexity is high.
11	Extensibility is high.	Extensibility is low.
12	It is easy to troubleshoot and report as it is centralized and controlled.	It is difficult to troubleshoot and report as it is distributed and controlled.
13	Its maintenance cost is lower than the traditional network.	Cost is higher than SDN.

As the SDN technology (see [4]) is based on an intelligent controller, it allows you to automatically redistribute traffic. It turned out that the device allows you to centrally change the settings of network equipment in branches, monitor the network status, load and quality of channels online, and solve problems. This ensures the transparency of data transmission networks and reduces the burden on IT professionals serving the network.

The study also showed that the SDN solution involves the automatic networking of private networks and the transmission of information through all available channels without losing the speed and quality of applications. For example, in the past, only expensive VPN channels were used to transmit audio or video without distortion. Now, thanks to SDN, we can only use the Internet and LTE as a backup(see [5]). In this way, customers can save on telecommunication bill payments and solve VPN reservation issues simply and cheaply. Unlike other virtualization technologies, the open-source SDN solution is more promising. SDN[2] already provides companies with many options to choose from OpenFlow, NETCONF, OVSDB, switches that support the API library, as well as enterprise software that utilizes these protocols. Like any other infrastructure, the SDN infrastructure is built on open standards. This open ecosystem accelerates network innovation. Although the traditional approach to building a network infrastructure still prevails due to the negative impact of mental inertia and crisis events, SDN already allows you to effectively solve problems in a virtual physical environment.

By automating the network, we get the following benefits and services: reduced problems, reduced costs, increased network flexibility, reduced network outages, increased number of strategic employees, advanced analysis, and network management capabilities.

3. Methods and Applications

The article methodology includes the study of epistemological issues, programs (OpenDaylight), protocols (OpenFlow) in the field of networks, using scientific literature, and research articles.

The research aim is to present an example of an automated network as a result of the analysis based on the studied materials. Below is the physical experimental network represented by the GNS3 simulator, which is fully operational, we will get the virtualized version of the following network, but the initial settings must be done one way or another.

This article provides a brief overview of virtual networks and network performance evidence. The physical network shown below is represented by a fully running GNS3 simulator. It contains hosts, routers (Mikrotik), and a virtual switch - OpenvSwitch.

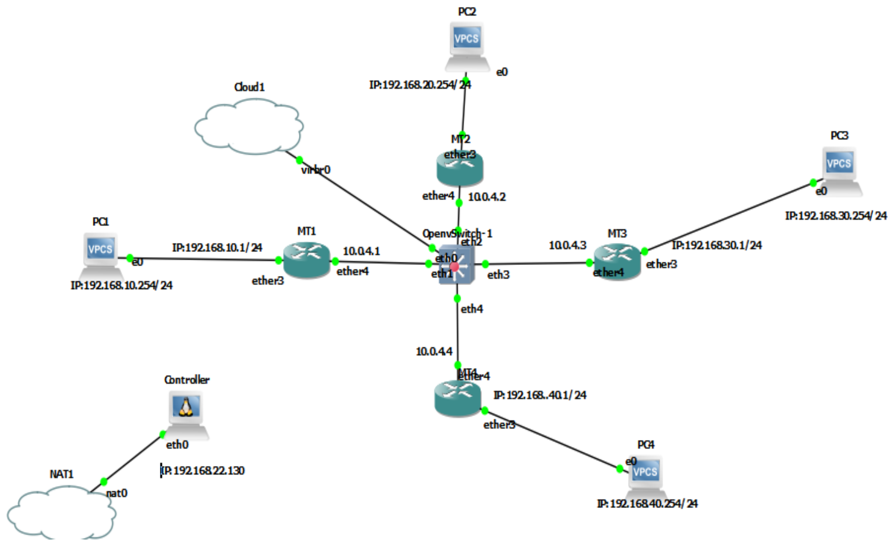

Fig . 1 . Network presented with GNS3 simulator.

Here are the settings of one of the devices, almost the same as the rest:

/routing OSPF instance

set [find default=yes] router-id=10.255.255.1

/IP address

add address=10.0.4.1/24 interface=ether4 network=10.0.4.0

add address=192.168.10.1/24 interface=ether3 network=192.168.10.0

/routing OSPF network

add area=backbone network=10.0.4.0/24

add area=backbone network=192.168.10.0/24

Here are the minimum settings that make the network complete.
For network virtualization, as mentioned at the beginning, we implemented an SDN solution. We have demonstrated the use of SDN with the OpenDaylight software, which is a software platform for SDN.

To work with our controller, to connect it to our physical network, we downloaded and activated the following components:

```
opendaylight-user@root>feature:install odl-restconf odl-l2switch-all odl-mdsal-apidocs
odl-dlux-all odl-openflowplugin-all
```

They provide a graphical user interface of OpenDaylight software, as well as the necessary tools and devices. After activating them, immediately after setting the appropriate settings in our physical OpenvSwitch network, we see a virtualized version of our network.
To establish a "controller" connection in our physical network, we have previously configured the OpenvSwitch OpenFlow device by giving it the IP address of the controller by typing the following command: **ovs-vsctl set-controller br0 tcp: 192.168.18.129:6633**, where 192.168.18.129 is the IP address of the controller and it can be different for different devices, 6633 is the connection port and the protocol that controls data transfer over TCP. Thanks to this, it was able to communicate with other devices.

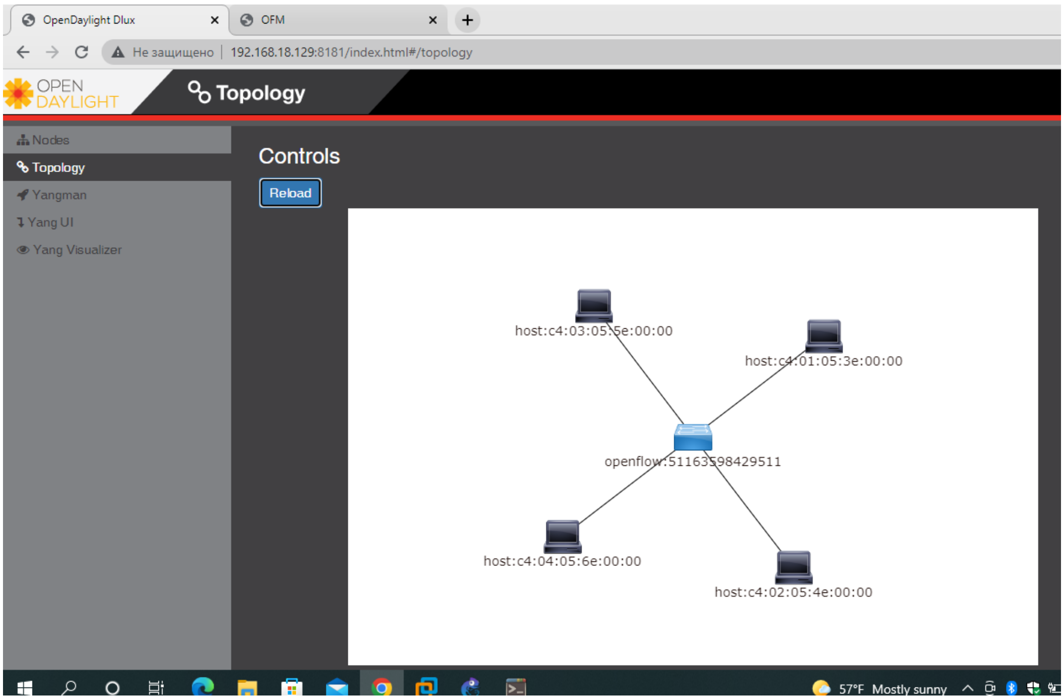

Fig. 2 . Example of a virtual network in OpenDaylight.

Fig. 2 shows a virtualized version of the physical network in OpenDaylight. The picture clearly shows all the devices in our network that are connected to the OpenFlow protocol support device, OpenvSwitch. It is thanks to the OpenFlow protocol that our SDN controller sees our entire physical network.

OpenFlow is a protocol for managing data processing, which is transmitted over the network through routers and switches using SDN technology. Fast packet forwarding (data forwarding) on a classic router or switch and high-level routing decisions (control operations) are made on the same device. The OpenFlow switch separates these two functions. Data redirection is performed by the switch itself, while routing decisions are entrusted to a separate controller, usually a standard server.
After clicking on the network topology, Yang automatically shows us the CONFREST API URL it uses to get this information:

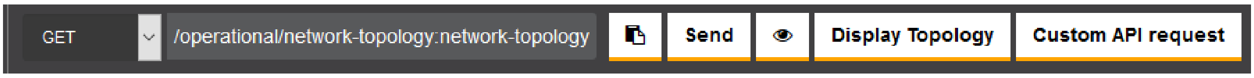

Fig. 3. CONFREST API URL

By clicking the send button(Fig.3), we can see the topology of our operational network.

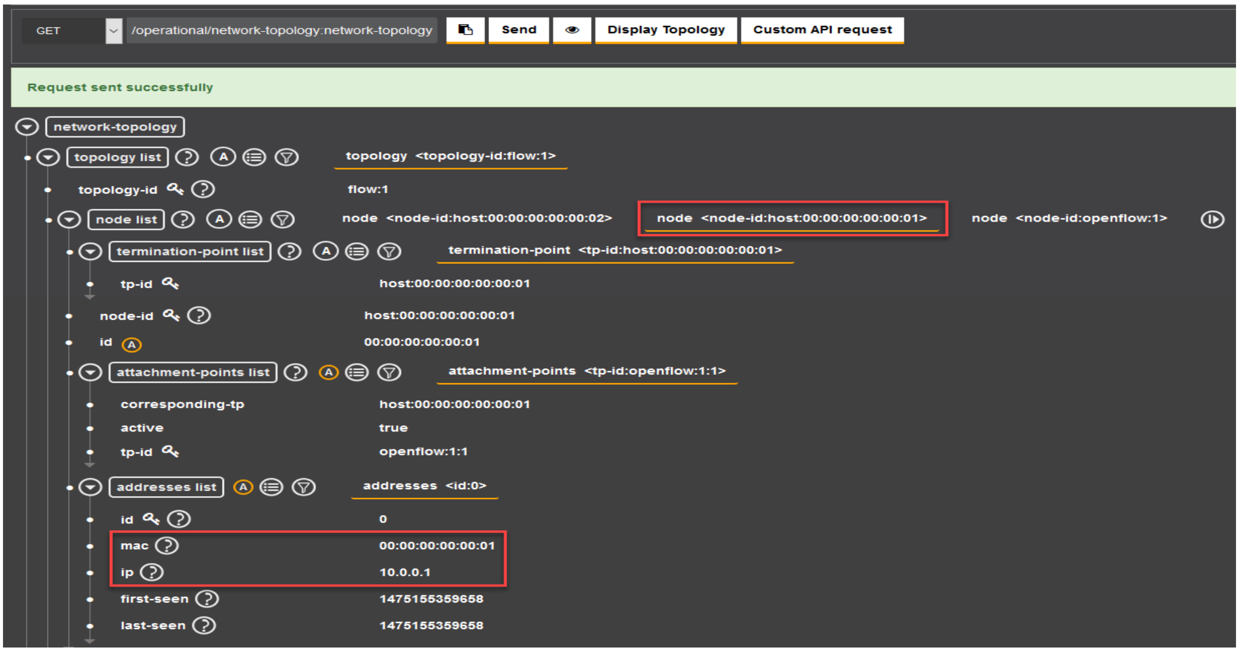

Fig. 4. Operating network topology.

In Fig. 4, we can see information about our current topology, including the MAC (Media Access Control) and IP addresses of our hosts. So, you do not need to enter the device to see them every time, but you can see them from one control panel of SDN.

When we send network traffic, all the information about it is mentioned in the flow tables of the SDN: how many packages were sent to us, how many arrived, how many dropped on the way, and what errors we encountered. And all that information we can see in the nodes of Fig.5.

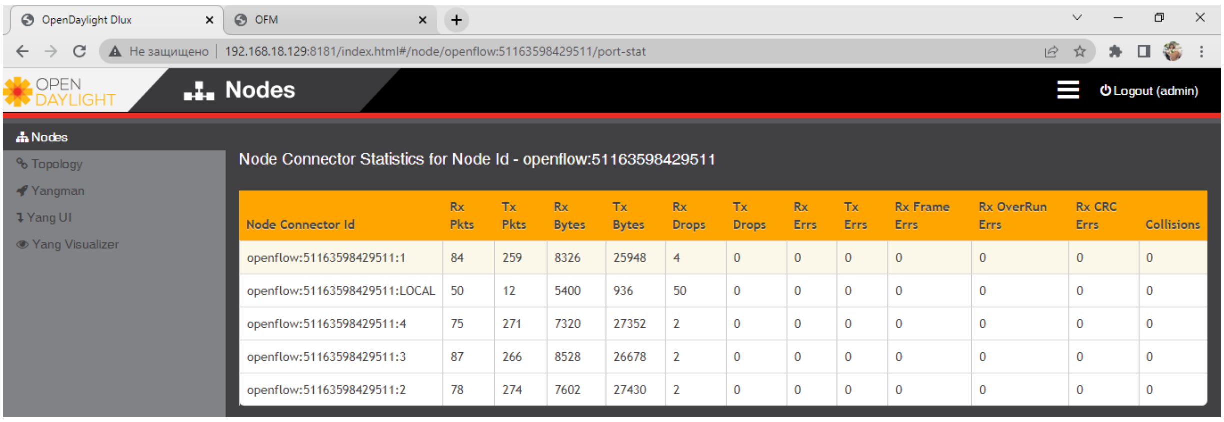

Fig.5. Node connector statistics.

5. Conclusion

This paper proposes a solution for network optimization. As a result of the research, we concluded that automation improves the speed of IT operations in response to analytical change. The ability to monitor operations, just as needed, provides greater visual control of the network, and transparency of processes within it. Network automation improves work efficiency, reduces human error, increases access to network services, and provides better customer service. Research has shown that the SDN solution includes the automatic integration of private networks, and the transmission of information over all available channels, without loss of application speed and quality. As a result of the study, it became clear that network automation can be implemented regardless of its type, which facilitates its transition. Network virtualization is a more all-encompassing version of virtualization that makes it possible to convert physical network hardware into software that can easily be transitioned to different domains as needed, increasing flexibility and scalability for the network. I came to the conclusion that its use on the network will be of great benefit to network administrators.

References

[1] How Can Network Automation Be Improved With SDN. [Online]. Available: https://www.acadiatech.com/blog/how-can-network-automation-improve-with-sdn/

[1] W. Braun and M. Menth, "Software-defined networking using OpenFlow: Protocols applications and architectural design choices", *Future Internet*, vol. 6, no. 2, pp. 302-336, 2014, [Online]. Available: http://www.mdpi.com/1999-5903/6/2/302

[2] S. Jena. Difference between Software Defined Network and Traditional Network. [Online]. Available: https://www.geeksforgeeks.org/difference-between-software-defined-network-and-traditional-network/

[3] J. Doherty, SDN and NFV Simplified: A Visual Guide to Understanding Software Defined Networks and Network Function Virtualization, Addison-Wesley Professional, March 2016.

[4] Software-Defined SD-WAN Technologies. [Online]. Available: https://tadviser.com/index.php/Article:SD-WAN_%28Software_Defined%29_Software-Defined_WAN

Ցանցի ղեկավարման ավտոմատացում վիրտուալացման միջոցով

Արուսյակ Դ. Մանասյան

ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտ
e-mail:armanasyan@iiap.sci.am

Ամփոփում

Հետազոտության նպատակն էր մշակել ցանցի ղեկավարման ավտոմատացման մեթոդներ՝ վերլուծելով դրանց վիրտուալ անալոգը: Աշխատանքում հիմնավորվում է այս մոտեցման արդիականությունը, վեր են հանվում առավելություններն ու թերությունները, ընդգծվում են առկա խնդիրները և առաջարկվում են դրանց լուծման ուղիներ: Արդյունքում ներկայացվել է ցանցերի վիրտուալացման արդյունավետությունը՝ փորձնական ցանցի օրինակով:

Բանալի բառեր՝ ցանց, ավտոմատացում, վիրտուալացում, SDN (Ծրագրակողմնորոշված ցանց), OpenDaylight (Ծրագրային ապահովում), OpenFlow (Արձանագրություն):

Автоматизация управления сетью за счет виртуализации

Арусяк Д. Манасян

Институт проблем информатики и автоматизации НАН РА
e-mail:armanasyan@iiap.sci.am

Аннотация

Цель исследования заключалась в разработке методов автоматизации управления сетью путем анализа ее виртуального аналога. В работе обосновывается актуальность такого подхода, выявляются преимущества и недостатки, подчеркиваются существующие проблемы и предлагаются пути их решения. В результате была показана эффективность виртуализации сети на примере пилотной сети.

Ключевые слова: сеть, автоматизация, виртуализация, SDN (Программно-определяемая сеть), OpenDaylight (Программное обеспечение), OpenFlow (Протокол).