International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195289

# Centralized Management and Control of Network Devices

**I. Govindharaj*, S. Mohanraj, P. Motheesh, R. Rajaguru**
Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, Tamil Nadu, India

## ABSTRACT
Computer networking is plays vital role in everyday business opportunity, network administrator and engineers has responsibility to keep network infrastructure of organization 24/7. The more up time of network the more business operates smoothly, network downtime may cause several problems in business, imagine what would happen if network of stock exchange is goes down for one are two minutes it would cause loss of million dollars. Management of network infrastructure and networking devices is quite daunting task for network engineers. In this paper we described the methods and technologies used for management and controlling of network devices. Network infrastructure management is big task for any organization. Complexity of network device management is based on the size and design of network. In recent time new technologies are emerging in management of network infrastructure like software defined networking we reviewed SDN pros and cons.
**Keywords :** Software defined networking, Management, Routing, Open flow protocol.

## I. INTRODUCTION

Management of network resources and data flow is become more complex in today's network. Companies invest big sum of amount in network infrastructure management, some of networking industries provide lot of services for network management. In order to manage network devices and infrastructure services network engineers and administrator have to possess lot of skill set, a company may use network devices like router, switch, firewall from different manufactures which means it has various network operating system depends on vendor of network device vendor, so the engineer Software Defined Networking (SDN) is a new approach in networking Technology, designed to create high level abstractions on top of which hardware and software infrastructure can be built to support new cloud computing applications. SDN is also referred to as programmable network, since it isolates control plane from data plane and provides an independent and centralized unit to control the network. Central control over the network provides lot of benefits.

Network automation is the process of automating the configuration, management, testing, deployment, and operations of physical and virtual devices within a network. Every day network tasks and functions are performed automatically. Using a combination of hardware and software based solutions, large organizations, service providers, and enterprises can implement network automation to control and manage repetitive processes and improve network service availability.

## II. PURPOSE OF TASK

The purpose of this task is to identify various technologies used in networks for management and dataflow control and analyse advantages and disadvantages and other issues in network infrastructure. New technologies are being introduced in computer networks. These

technologies need to be researched and testing for consistency and efficiency of its operation.

These technologies may benefit a lot to business but these benefits must be analysed in various business tiers respective to cost, interoperability, portability and efficiency. Small scale industries find difficulties to moving into new technologies because of cost and portability.

## III. ISSUES IN NETWORK MANAGEMENT

There are several complexities and issues in management of network devices. If you want to change the operating status of network, you have to configure each device in network. In order to configure device like router, switch and other network devices you have to configure them via CLI or telnet or SSH. The following are common challenges

1. Utilization of resources
2. Network management
3. Error management
4. Traffic management

Resource utilization is one of the commonly known issues in network management, to achieve maximum throughput resources have to be utilized in efficient way.

Error management is another factor of network management. Network administrators have to analyse logs on daily basis to identify those errors and implement solutions based on error. This task is one of the difficult task for network administrators.

Management of traffic is one of the daunting task of network management, complexity of traffic is based on design and size of network. Traffic management includes classification of traffic, type of service, prioritizing traffic based on type of data.

Adding new programs or adding new policies require administrator configuring numerous individual devices which will require administrator to have working knowledge of device operating system (OS) and configuration methods. In some case single network may have different vendor products, that makes administrator need to have knowledge of various vendor products. As your network scales, it became more and more inflexible as more and more devices have to be configured for every change.

As mentioned above to access into device we need to use CLI – command line interface or SNMP or other access methods and configure control plane in order to influence new behaviour in forwarding plane.

## IV. STUDY OF SOFTWARE DEFINED NETWORKING

Designing and managing networks systems become a very challenging task because of the high level of complexity involved in network design. The tight coupling between a network's data and control plane gets a rise various challenges to management and evolution of network. Network engineers need to be manually transform their high level companies network policies into low-level configuration commands of particular device, process which for complex networks can be highly challenging and error prone. Adding new functionality to the existing network system, like intrusion detection systems(IDS) ,load balancers and other systems usually requires tampering with the network's infrastructure and has a direct impact on its logic because of change, while deploying new protocols could be a quite slow process and it may demanding years of study and testing to ensure its working and interoperability among the implementations provided by various system vendors.

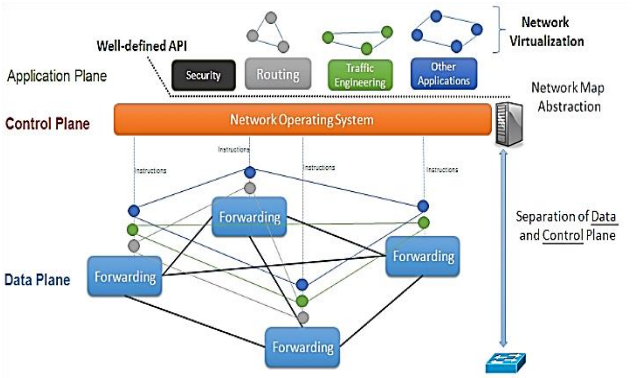


Fig. 1. Software defined network approach

The peak of network programmability has been evolved in past years as a means to change this situation by promoting new technologies in network management and the deployment of network services through programmability of the underlying network entities using some of the open network application programming interface(API). This takes us to new reliable and flexible computer network able to operate according to the user's needs in a direct analogy to how programming languages are being used to reprogram computer systems in order to perform a tasks without the need for continuous change of the existing hardware platform. Programmable network is a relatively new era of a network programmability which changes the way that networks are designed and managed by introducing an abstraction that decouples the control from the data plane, as illustrated in Figure 1. In this method a control program, referred as the central SDN controller, has an entire view of the whole network and is responsible for the making decisions over its functions, while the hardware is simply responsible for delivery packets into their destination as per the controller's instructions, typically a set of packet-handling rules.

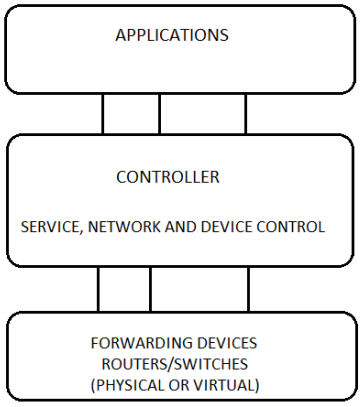


Fig. 2. SDN Approach

Programmable network architecture is quite remarkably flexible it could operate with various types of switches and at different layers of protocol. Controller of SDN and switches can be implemented for Ethernet switches, Internet routers, transport switching, or application layer switching and routing. Software defined networks relies on the common functionality found on networking devices, which essentially involve forwarding packets based on some form of flow definition. There is another important protocol that used by controller of to interact with device that is protocol called openFlow.

## V. SDN CONTROLLDRS

As already plotted above, one of the core ideas of the software defined network philosophy is the existence of a network operating system placed between the application layer and the network infrastructure. This network operating system is responsible for managing and coordinating the resources of the whole network and for revealing an abstract unified view of all components to the applications executed on top of it. This idea is analogous to the one followed in a computer system, where the os of network devices lies between user space and the hardware and is responsible for managing the hardware resources and providing common services for programs for user. Similarly, network engineers,

administrators and developers are now given with a homogeneous environment easier to program and configure much like a typical computer program developer would.

The logically centralized control and the generalized network abstraction it offers make the SDN model applicable to a wider range of applications and heterogeneous network technologies compared to the conventional networking paradigm. For instance, consider a heterogeneous environment composed of a fixed and a wireless network comprised of a large number of related network devices (routers, switches, wireless access points, middle boxes, etc.). In the traditional networking architecture, each networking device would require individual low-level configuration by the network engineer in order to operate properly as per requirements. Moreover, since each and every device in network targets a different networking technology, it would have its own specific configuration and management requirements, meaning that extra effort would be required by the administrators to make the whole network operate as required. On the other side, with the logically centralized control of software defined network, the administrator would not have to worry about low level details. Instead, the network management would be performed by defining a proper high level policy, leaving the network operating system responsible for communicating with and configuring the operation of network devices.

Having discussed the general concepts behind the controller of SDN, the following subsections take a closer look at specific design decisions and implementation choices made at this core component that can prove to be critical for the overall efficiency, performance and scalability of the network.

## VI. OPENFLOW PROTOCOL

Following the SDN principle of decoupling the control and data planes, open Flow provides a standardized way of managing traffic in switches and of exchanging information between the switches and the controller, as Figure 2 illustrates. The Open Flow switch is composed of two logical components. The first component contains one or more flow tables responsible for maintaining the information required by the switch in order to forward packets. The second component is an OpenFlow client, which is essentially a simple API allowing the communication of the switch with the controller. The flow tables consist of flow entries, each of which defines a set of rules determining how the packets belonging to that particular flow will be managed by the switch (i.e., how they will be processed and forwarded). Each entry in the flow table has three fields: (i) a packet header defining the flow, (ii) an action determining how the packet should be processed, and (iii) statistics, which keep track of information like the number of packets and bytes of each flow and the time since a packet of the flow was last forwarded. Once a packet arrives at the OpenFlow switch, its header is examined, and the packet is matched to the flow that has the most similar packet header field. If a matching flow is found, the action defined in the action field is performed. These actions include the forwarding of the packet to a particular port in order to be routed through the network, the forwarding of the packet in order to be examined by the controller, or the rejection of the packet. If the packet cannot be matched to any flow, it is treated according to the action defined in a table-miss flow entry.

The exchange of information between the switch and the controller happens by sending messages through a secure channel in a standardized way defined by the OpenFlow protocol. This way, the controller can manipulate the flows found in the flow table of the switch (i.e., add, update, or delete a flow entry) either

proactively or reactively as discussed in the basic controller principles. Since the controller is able to communicate with the switch using the OpenFlow protocol, there is no longer a need for network operators to interact directly with the switch.
Main challenges in SDN include:

- Security threats
- Attack on control plane
- Attack on vulnerabilities on switches
- Attack on controllers
- Attack on administrative stations
- Lack of trusted sources.

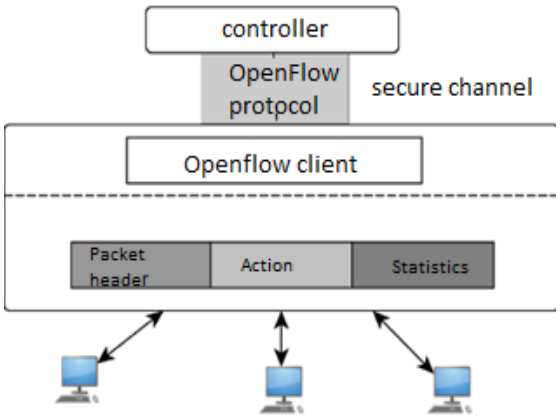


Fig. 3. Openflow with controller

## VII. CHALLENGES IN SDN

Main challenges in SDN include:

- Security threats
- Attack on control plane
- Attack on vulnerabilities on switches
- Attack on controllers
- Attack on administrative stations
- Lack of trusted sources.

They can be reduced to some extent by redundancy (of devices and applications), same application to run on different controllers, self-correction and healing mechanisms and dynamic device association to another controller in case of a failure.

## VIII. PROPOSED SYSTEM

Our system is web based application for network management. Unlike SDN we are not decoupling control plane from data plane, each node in a network can independently work and make decisions based on individual configuration of control plane.

Centralized management server is used for configuration and managing each and every resource on network. Only management of network is centralized control of network remain in individual nodes. In our solution automation of network is part of the framework, by using this automation module we can automate regular tasks that performed in network, this will reduce lot of overhead of network management. Tasks like backing up configuration, routine check of logs and etc. Fig. 4 is architecture of our system.

Advantages of our application:

- Centralized management
- Distributed control
- Automation of tasks
- Notification of events
- Ease of management

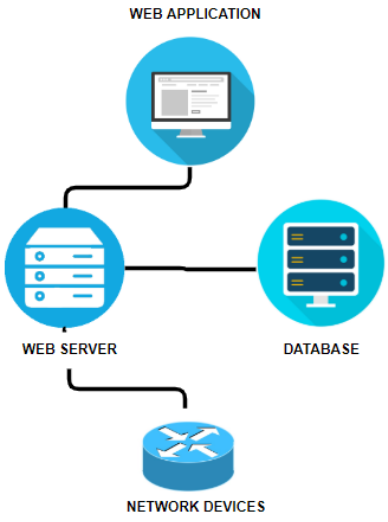


Fig. 4. Network management application architecture

This application contains four primary modules illustrated in fig 4.1. It is developed by layered approach so that makes made isolation of components which makes ease of management and error isolation.

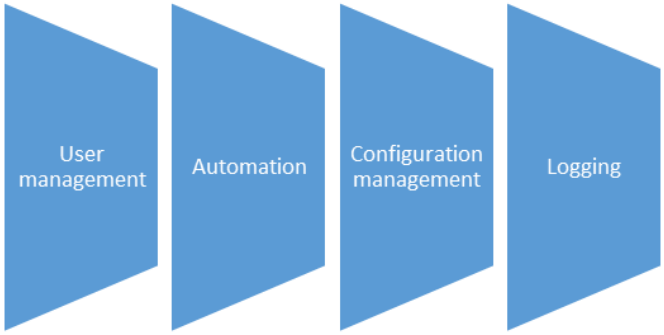


Fig. 4.1. Modules of network manager

### A. User Management

User management module deals with all kind of actions related to users, such as Adding user to application, user privilege, forgot password, reset password. Only super user can add other admin users, random password generator generate password while creation of user and send those credentials over email.

### B. Automation

Automation module is major part of this application. Tasks that are repeatedly performed by network administrators are automated and specified tasks are performed based on the respective time configured by user. Task includes configuration backup, log analysis, performance analysis.

### C. Configuration Management

This module manage operations related to all network device configurations. All device configurations are stored in server, operations are checking integrity of configurations, revert back consistent configuration file to device.

### D. Logging

Logging module create log file for each and every event in application and network devices. It can be used for if there is any inconsistency in management application and network devices.

## IX. CONCLUSION

In this paper we mentioned various technologies used in computer networks and researched issues in network management and control, also discussed about emerging networking solution software defined networking and openflow protocol its advantages and disadvantages. We also proposed our solution for management for network devices.

## X. REFERENCES

[1] Mahmudov salimjon olimjonovich, “Software defined networking,” (2016).

[2] R Dhaya, Suganth maharaj, Sowmya J, R Kanthavel,“SDN view point from IP networks pros and cons exploration of thoughts”, (2017).

[3] Open networking Foundation Software-Defined Networking (2012).The New Norm for Networks.

[4] OpenFlow-enabled SDN and Network Functions Virtualization (2014). Open networking Foundation.

[5] Hegr, T., Bohac, L., Uhlir, V., Chlumsky, P. (2013). OpenFlow Deployment and Concept Analysis. Advances in Electrical and Electronic Engineering, 11

**Cite this article as :** I. Govindharaj, S. Mohanraj, P. Motheesh, R. Rajaguru, "Centralized Management and Control of Network Devices", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 319-324, March-April 2019.
Available at doi : https://doi.org/10.32628/CSEIT195289
Journal URL : http://ijsrcseit.com/CSEIT195289