

Software Defined Networks: The Future of Networking

Amanda Zeqiri¹, Endrit Sino², Genta Rexha³ and Igli Tafa⁴

¹Lecturer, Department of Applied Mathematics, FNSc, University of Tirana
Tirana, Albania
amanda.zeqiri@fshn.edu.al

²Lecturer, Department of Information Engineering, FIT, Polytechnic University of Tirana
Tirana, Albania
esino@hotmail.com

³Lecturer, Information Technology Department, University of Elbasan
Elbasan, Albania
gentarexha@yahoo.com

⁴Lecturer, Department of Information Engineering, FIT, Polytechnic University of Tirana
Tirana, Albania
itafaj@gmail.com

Abstract

Internet and mainly today's computer network environment, has seen a powerful evolution and success. But contradictory with this, engineers and architects, have concluded that as result of its ossification, internet is becoming more and more difficult to develop and move forward. Different vendors, with different technology, have emerged Internet in a situation in which we can deal with, only if a broad understanding and convergence is achieved between, the two main actors: R&D community and the investors. But what happened is that as the time flew, the academic researchers, found more and more less space to contribute and to share they ideas. All this has occurred during the past ten years, where the internet found his major development, from several factors. Among them I will discuss the most important and with the most significative contribution and also will introduce the Software-Defined Networks model. This model will be briefly analyzed in a position paper with his major strengths and weaknesses over the today model of Internet.

Keywords: *Software Defined Networks, remote networking, controllers, switches, security.*

1. Introduction

Introducing new features, protocols, algorithms or even basic ideas in what should be the next generation trend of Internet, has become more and more challenging due to several factors. Maybe the first one that comes to mind is the main investors, who paradoxically, may be

described as the main obstacle of the case. The more that academic researchers tries to give shape to new ideas, the more they face bureaucracy, or less friendly environment to test or evaluate them. Must say that not always stakeholders and important vendors have the fault; therefore may be some for researchers too. But the fact remains, that there is so much to do to prevent the Internet from 'ossifying'. During the years the Internet has proven to be error-prone and hard to maintain. These must be sufficient reasons for the investors to rely and support the new trends and solutions proposed from academic agenda, even if they might seem impossible or revolutionary. The limited flexibility maybe the first milestone to reach for the researchers. The more that the networks expands, the less flexible it becomes and also hard to evolve in terms of infrastructure and protocols or algorithms. In last few years, a new approach, maybe somewhat revolutionary, has taken a good amount of academic attraction and work hours. Software Defined Networks (SDN), is a very good challenging and promising subway to face the stand-still situation that Internet is facing in the past 10 years. This new network paradigm tries to mitigate the today's management framework that network administrators and operators use. Underlying in a clear and effective way, the control plane and the data plane, SDN intends to elevate the network

maintaining and developing task, to a whole new dimension.

Implementing and testing new protocols or algorithms in nowadays Internet, has become a very challenging mission. The academic agenda and scientific researchers, have initiated several approaches in terms of presenting and advertising this model to the biggest investors (e.g. Cisco, Juniper, IBM etc.). The Open Search Community is the marcher of the SDN paradigm. They have clarified the urgent issues that we should address immediately.

This paper intends to give a clear sight in the benefits of embracing SDN, as future networks paradigm and also identifying the first and maybe the most urgent aspects of SDN, that require the immediate attention of both, the academic researchers and infrastructure vendors. In section 2, I am going to depict the SDN way of managing and developing the network. Also key points in terms of weaknesses and strengths will be mentioned. In section 3, will be presented and shortly described the Open Flow protocol, distinguishing its ability to enable innovation and academic research, within a commercial architecture, without “disturbing” the customer care aspect of investors. I will continue to address the biggest challenges of SDN, in section 4, where also will be presented a future and a forthcoming field, where SDN paradigm, can be nicely placed. Like the last paragraph, the concluding remarks, will be lined up.

2. Details and specifications

For nowadays applications and software, Internet has become the key stone of success. Now users, want to do more and more, and keep less megabytes in their “stackframes”. The need for network applications, gaming software or web services has increased epidemically. Thus, engineers have developed new technologies, like cloud computing or virtualization, to offer a wide range of applications and services, and in the same time, to achieve better resources usage and performance. This spectacular achievement, somehow, has pushed Internet in a challenging situation. As he seizes a considerable territory in the whole application and service oriented fields of networking, he sees himself more and more enable to change, evolve or even develop with bigger steps. The virtualization approach, have been a very good model and achievement for

everyone. Even though, the two different currents (“pursuits” and “pluralists”) see this property, in two different ways, I would give a slight advantage the second one. More and more the network and computing resources will consider the need of virtualization. This opinion of mine is also clearly evidenced from [6 , 10]. They commonly present a new way in how we should see the service offering and enabling, from the network point of view. They emphasize, that virtualization, should be more and more present in our project and management agenda.

When SDN was introduced for the first time, it aimed to enable a faster, productive and direct academic research in networks and to facilitate innovation. The need of that, was firstly recognized from the academic staff, but what happens now is that, the switch/router manufacturers themselves, have distinguished this urgent need, so a lack of cooperation is being prepared from both sides. In fig. 1 is depicted the main difference that SDN will introduce. From now on, the decision making in forwarding and routing will operate remotely, and switches will only derive in scan-match operations. The more that the researchers excavate in this field, the more they find that SDN can do so much more than that. More and more, SDN is being treated as a better way of network maintaining, or networking in general.

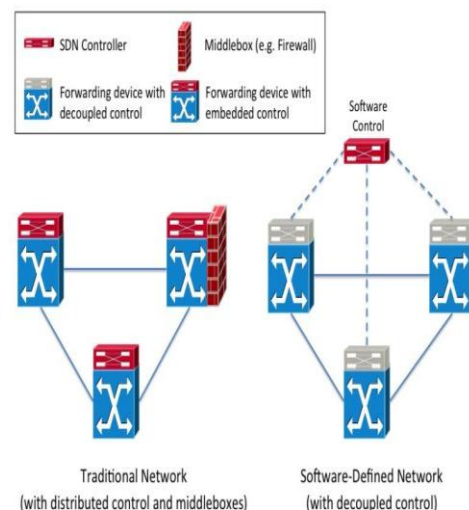


Fig. 1 The SDN model differences from the traditional IP network.

2.1 SDN model strengths

Besides the familiar environment that it creates, for the R&D community, it is eligible to mention that it is an beneficial approach for the investors too. They can increase the range of functionalities and services that they can offer to the customer. With the single router abstraction, they can follow a different approach from virtualization, and experience the “Platform as a service” model, which aims the better usage of every single computer and network resource of the platform. With this pattern, the network owner can differentiate his services and offer new ones. This, is described as a demanding solution for today's ISP, because now they can offer more, and as a result earn more in financial terms.

Another key point to mention is the decoupling between the control plane and data plane, which enables network administrators to perform normal IP routing through low cost hardware [6]. Through the virtualization of actual physical infrastructure, enables the decision-making process to take place in the VMs interconnections, first. But implementing SDN not only affects network administrators and operators work (now they will have an easier job to monitor, maintain and modify the network), software engineers also will be able to build platform independent and less complex architectures[12]. And all this due to the existence of VMs and their logical connections. Also the congestion detection and defending from various threats (e.g. DoS) now is more easy, because the administrators now have a much more easy statistic collecting task. The need to observe and control everything that passes through the network, implies the need of a model like SDN[11]. The granular control bench that comes as a product of it, affects thoroughly the performance and the complexity of the whole system. From the economical and financial point of view of enterprises, now the network maintaining and controlling is much more cheaper due to the “single interface” model (every switch/router configuration or update, now can be done remotely, so there is no need for the network operators to “touch” every thing with their hands) and maybe it will require less human resources, that often is the most expensive asset for companies. Not to mention that they now can use software, completely independent from the hardware they use.

2.2 SDN model strengths

Even though, this model is presented with the best comments, still remains a lot of work to do ahead. The better and miraculous that this model might seem, the more difficult it gets to achieve all those things that we mentioned before. The better and miraculous that this model might seem, the more difficult it gets to achieve all those things that we mentioned before. As is illustrated from the diagram in fig. 2, the whole model is provided by three basic components,

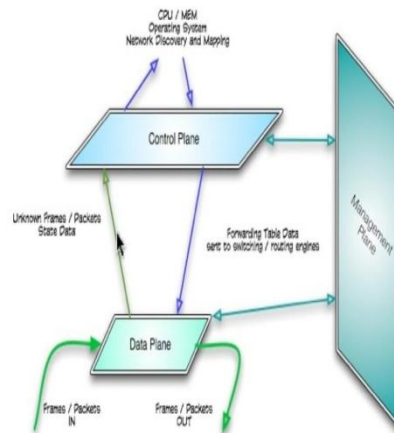


Fig. 2 The logical diagram of the main modules present in SDN model

the controllers (that represent the control plane), the switches or forwarding entities (that represent data plane, where the real payload data transaction takes place) and the management plane, which is somewhat a more abstract notion, that can be argued as a new level of monitoring nature or even a intermediate group of actors (operators, administrators etc.) that posses a different view of the system.

When this simple scheme faces the practical obstacles, we have a lot of “fun stuff”. We now will begin to think deeply every little detail and aspect of the model. Intuitively, we individualize the first single point of failure that comes to mind: the controllers. Is pretty clear that if someone possesses them, they probably will have in their hands the whole system[13]. So that this domain problem should have top priority, before projecting the whole distributed architecture. Another important issue related to

controllers, is the “how & where” to put the controllers problem[5]. This topic is more related with the performance and scalability aspects and considerations, but strictly should be consider with the first one. A solution for the first problem might be sharing the control between different control entities, but this neither guarantees the final solution. Now arises the problem of cooperation among them, which is a challenging task itself for the academics. As described in [5], the multiple controllers framework shows that there is light at the end of the tunnel. In addition, several approaches have been made in how to distribute the control logic, in the control plane. The two of them to be mentioned are Onix and Hyperflow, which propose to the sharing of control logic among multiple controllers, with hierarchy policies[3] implementation in addition. This increases significantly the system scalability but considerably decreases the whole system performance and latency.

After all this said above, the fact remains that we should stick to the idea of a single controller, but also here we will find several questions to answer. The first thing that comes to mind is the control-to-switch latency and frequency. This also rises the issue of security in the transactions between this two actors. Using the SSL encryption method may seem fair enough but still the man-in-the middle problem is not solved [1]. Not to mention here the case-sensitive of this aspect in wireless application of this model. In [1] are professionally enumerated different threat types (vectors), and as it is concluded just two of them represent new “kind” of threats, which means that this model has achieved to revolutionize the way that we see, manage and develop networks, without any big security drawback in principle. But the fact remains that this courageous approach has a lot of work to do regarding to security. Another principle to enumerate, is the “real-time” nature that controllers should have, before deployed into the system. As mention in section 2.1, this model would offer a better congestion control and intrusion detection and protection tools, but this directly increases the responsibility for the engineers. So they should think in a very scrupulously way, when comes to project the “brain” of the system. The controllers should be smart and fast enough to respond in real time to every possible scenario. After all, this is the whole cause of this model existence.

The applications security and integrity should be extremely good and well prepared. At the end of the day, they will be used by people who are ready to pay money for that service and for us, that has top priority. Another beautiful key point is the forensic nature of the system. For every threat presented or distinguished from our ID&PA system, we should provide the maximum of the necessary details and optimal amount of data. Finally, the last but not least important issue to address is the unpredictable nature of the networks. The traffic flows, the not constant quantity of data travelling through and maybe the not-common patterns that the system will face, should consume a significant of engineers attention.

3. Open Flow Switch Design

Even though was firstly proposed to work as a effective tool in enabling the innovation and research background of the networks, the manufacturers have in creased the number of the commercial switches that support OF protocol (HP, Juniper, Bigswitch, Quanta etc.)[4]. Actively lobbying and undermining the issue of the ossified Internet, has finally rewarded somehow the researchers. Even though there remains plenty of work and cooperation to do. The presence in some of the main architectures, kind of simplifies the work to do. Now finally, it is possible and eligible to test and experiment with real traffic. Of course this needs a sort of cooperation and coordination with the network administrators, but it may not be considered as an obstacle.

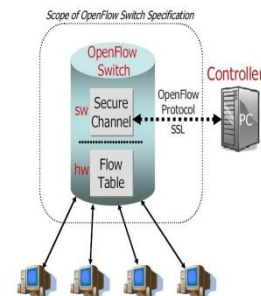


Fig. 3 The basic entities related with the Open Flow Switch design

Another good point to be mention is that vendors, do not have to expose themselves in terms of inner details of their architectures that they provide. For them, a very good perspective lays ahead. With this model of networking, they will have more possibilities to differentiate their products and services. They might become infrastructure and service providers in the same time[6, 9, 10]. The diversity offered in this model, enables *anyone* to perform individual approaches related to this aspect.

Referring of Open Flow switches, reminds us how they could be implemented and the problems related to them. Depicted in figure 3, the OF switch basically embodies the whole principle of SDN model: one controller on top and one switch on the “field”. Not described explicitly, the OF protocol is present in both planes, control and data plane. The work in developing and implementing this protocol has shown that this phase of the OF switch engineering stage, has critical impact in overall system performance[2]. This sensitive process shows that different approaches in implementing, should be followed under well-designed strategies. For instance, the way that different stakeholders(i.e. HP vs. Monaco and Quanta) choose to manage the flow table of the switch, impacts directly the performance introduced by the OF switch.

4. Challenges and future work

As the SDN increases its popularity, many questions expect short-term answers and solutions. The most of them are all security related, looking that always is a critical point in computer networks[13]. Reliability, scalability and performance considerations should also be present for further attention and research. Implementing OF protocol in more and more switches, looks like a more demanding task for now. Nevertheless, this is something that affected from time factor too. Virtualization was shortly discussed in section 2, but still remains an attractive point of referring. The Router as a service perspective seems very promising in terms of resource usage and performance[6]. Also “postponing” the decision-making phase in the virtual network (i.e. performing routing policies in the VMs first), lists more and more options.

Dealing with multiple controllers may not seem such a bad idea. The flexibility and scalability performed from this model, may seem very tempting for the developers and network owners. Security aspect of this model, significantly tries to balance this problems. The more controllers we have, the more we will be able to survive deadly attacks or to achieve disponibility. On the other hand, more controllers means more possible targets to attack. Here is a very beautiful trade-off made by most of the engineers: building a wider platform with more functionality and services or developing a smaller but consistent system. Granularity in terms of control and network monitoring is a promising and rewarding detail that always should drag the most of our attention, when we tend to deploy a SDN platform. Implementing the SDN as whole, knows only some symbolic achievements. Only 3 ways in how to deploy and implement a SDN model, are known[12]. The switch-based and overlay model are analogue to each-other. The real challenge that lays ahead, is the interaction between and the product the comes out from mixing those two. This may seem totally challenging and somehow impossible, but always promises the biggest reward. SDN model, in its first step had also a big “enemy”: its cost. This is a little bit justified from the fact of its new arrival and deployment, but the trend is clear: as the time passes the cost of every single SDN model component will decrease like every other brand and computer-related product that we have experienced. Another factor in decreasing overall costs of SDNs, will be the evolution of virtualization more and more, which enables the investors to better use their resources, offer more and as result, win more money. This key-stone will also enable better network monitoring and maintaining attributes, like Intrusion Detection & Protection, IP routing etc.

Implying the switching vs. routing discussion in SDN, results very interesting from the perspective. Inter-domain routing protocols, are extremely reliable and fast protocols, but the principle should be simple: outside the world (between different ISPs) the switching will be faster and more economic to perform. It leaves the routing operation to be preferable only when we reach the local networks (MAN, WAN or LAN)[14]. This approach would be very productive if would have been followed strictly and given the appropriate amount of attention in

engineering agenda. I think that SDNs, offer a plenty of attractive benefits for ISPs, to hold on. Even though the plenty of security considerations, this model offers a very good QoS management tool, routing policies and plenty of other 'stuff'. The ISPs management routine, is imposed from the ossifying trend of the Internet. To be more precise, heart of the internet which are ISPs, suffer immense consequences regard with the inability of the network to develop, emerge, embrace new technologies or even experiment the old ones.

5. Conclusions

While the whole Internet struggles to find its rescue boat from this non-promising situation, I think that the key is the dialogue and collaborating seminars between investors and academic researchers. The last have given so much to the science as a whole, and now expect just a little bit of more "space" to test, evaluate, or experiment their ideas and works. Introduced approximately six years ago, the SDN paradigm, has known, a huge popularity in different professional spheres. The commercial manufacturers on the other hand, have finally concluded the first step, they have embedded OF protocol in their architectures. Also a collaborative spirit should be felt, even from important actors as ISPs themselves too. Not occasionally, in the entire paper, they are mention more often than any other actor. I see them in the front line of acting and collaborating because its clear and well-explained that they will be the biggest beneficiaries. They could revolutionaries the way they manage their networks, how they offer services or even how they defend themselves from random attacks. The research community on the other hand should continue to provide constant assistance on this new technology, with an increasing popularity from day to day. The opportunities are made to be cached, so this situation, should have students, academics and professionals as its main contributors.

References

[1] Diego Kreutz, Fernando M. V. Ramos, Paulo Verissimo: "Towards Secure and Dependable Software-Defined Networks"

- [2] Danny Yuxing Huang, Kenneth Yocum, and Alex C. Snoeren : "High-Fidelity Switch Models for Software-Defined Network Emulation"
- [3] Andrew D. Ferguson, Arjun Guha, Chen Liang : "Hierarchical Policies for Software Defined Networks"
- [4] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, Scott Shenker : "OpenFlow: Enabling Innovation in Campus Networks"
- [5] Md. Faizul Bari, Arup Raton Roy, Shihabur Rahman Chowdhury, Qi Zhang, Mohamed Faten Zhani, Reaz Ahmed, and Raouf Boutaba, David R. Cheriton School of Computer Science, University of Waterloo: "Dynamic Controller Provisioning in Software Defined Networks"
- [6] Marcelo R. Nascimento, Christian E. Rothenberg, Marcos R. Salvador, Carlos N. Corrêa, Sidney C. de Lucena, Maurício F. Magalhães : "Virtual Routers as a Service: The RouteFlow Approach Leveraging Software-Defined Networks"
- [7] Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turlitti : "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks"
- [8] Jonathan S. Turner, David E. Taylor: "Diversifying the Internet"
- [9] Eric Keller, Jennifer Rexford: "The "Platform as a Service" Model for Networking"
- [10] Tom Anderson, Larry Peterson, Scott Shenker, Jonathan Turner : "Overcoming the Internet Impasse through Virtualization"
- [11] Natasha Gude, Teemu Koponen, Justin Pettit, Ben Pfaff, Martín Casado, Nick McKeown, Scott Shenker : "NOX: Towards an Operating System for Networks"
- [12] Manal Algarni, Vinayak Nair, David Martin, Sayali Shirgaonkar : "Software-Defined Networking Overview and Implementation"
- [13] S. Sorensen. Security implications of software-dened networks. 2012. url: <http://goo.gl/BiXH2>.
- [14] James McCauley, Aurojit Panda, Martin Casado, Teemu Koponen, Scott Shenker: "Extending SDN to Large-Scale Networks"