Mitigating the Risks of Supporting Multiple Control Planes in a Production SDN Network: A Use Case

Jeronimo Bezerra[1], Julio Ibarra[1], Marcos Schwarz[2], Humberto Freitas[2], Heidi Morgan[3]

[1]Florida International University – Miami, FL – USA

[2]Rede Nacional de Ensino e Pesquisa – Campinas, SP – Brazil

[3]University of Southern California – Los Angeles, CA – USA

{jbezerra, julio}@fiu.edu, {marcos.schwarz, humberto.galiza}@rnp.br, hlmorgan@isi.edu

Abstract. *The SDN paradigm enables network operators to host multiple control planes in parallel, being an approach to support multiple network services. Supporting multiple control planes over production networks exposes the production environment to potential risks and increases operational complexity. To understand and mitigate these risks, we implemented procedures and tools that resulted in a more reliable network. This paper describes our experience and findings with the support of multiple control planes in a wide-area production network.*

1. Introduction

Hosting multiple control planes enables SDN networks to offer specialized network services. However, supporting multiple control planes in a production SDN network involves potential risks and increases the complexity of operation and troubleshooting processes. Risks result from code instability in the OpenFlow agents, and the complexity of operation and troubleshooting is a consequence of extra protection layers and procedures required to handle the software instability.

With the vast adoption of OpenFlow [McKeown et al. 2008], network operators are being exposed to some operational gaps, such as the lack of specialized OpenFlow troubleshooting tools. AmLight has hosted multiple SDN control planes in parallel with production applications since 2014 [Ibarra et al. 2015] using the Flow Space Firewall (FSFW)[1], an OpenFlow proxy developed to support multiple control planes operating in parallel in an OpenFlow network. During this period, unexpected network outages were seen. Aiming to handle these operational OpenFlow gaps and increase the network's resilience, some procedures and tools were created.

In the first year after the OpenFlow activation, AmLight's production network was involved in nearly twenty network outages due to OpenFlow agents' crashes. In these situations, troubleshooting has proved to be difficult. In each event, OpenFlow switches and SDN applications' event logs and packet inspection were used. Nevertheless, unfortunately, the tools did not provide enough information, making it impossible to understand the event completely.

[1] "FSFW: Flow Space Firewall": http://globalnoc.iu.edu/sdn/fsfw.html

This paper's contribution is to describe the AmLight experience when hosting multiple control planes alongside with production applications and present some innovations developed to handle these operational gaps introduced with the OpenFlow deployment.

2. Innovations Developed to Minimize Risks on SDN Networks

Three main innovations were created to help to minimize the risks of supporting multiple SDN control planes: (1) an evaluation methodology, (2) an OpenFlow packet dissector (the OpenFlow Sniffer) and (3) an OpenFlow packet filter (the Testbed Sanitizer). These innovations are described in the next sections.

2.1. The Evaluation Methodology

Before hosting any new control plane, an evaluation methodology is performed. The evaluation methodology focuses on identifying OpenFlow messages that could affect the network resilience. The validation process identifies the OpenFlow messages used by the new control plane software using the OpenFlow Sniffer and validates these messages against the ones supported by the production OpenFlow switches. Then, the application is hosted in a testing environment with physical devices and, in case no impact is observed, a production slice is created for it.

2.2. The OpenFlow Sniffer

The OpenFlow Sniffer [Bezerra et al. 2016] is a tool developed with the focus on troubleshooting OpenFlow environments hosting multiple control planes. The OpenFlow Sniffer was developed to handle OpenFlow proxies, allowing network operators to associate a controller with an OpenFlow switch. The proxy support is especially useful in cases of asynchronous OpenFlow messages because only one type of OpenFlow message carries the *datapath-id* of the OpenFlow switch. Currently, the OpenFlow Sniffer is the only production tool available with such support, and it operates passively to lower the risks to the SDN controller's environment.

2.3. Testbed Sanitizer

Testbed Sanitizer is a tool created to facilitate the troubleshooting procedure and, at the same time, reduce exposure to risks. Its primary purpose is to filter all undesired OpenFlow messages per network device's line card and software version.

Filtering all undesired OpenFlow messages requires a catalog of all line cards and software versions in use. The OFTest[2] tool, a framework and test suite to validate compliance with the OpenFlow specification, was employed to create this catalog. After running OFTest's tests against every switch's line card, the output is parsed and exported to an XML file.

The Testbed Sanitizer works intercepting OFPT_FLOW_MOD messages received from all OpenFlow control planes and validating these messages against the catalog created with the OFTest. Only the OpenFlow messages added to the catalog are forwarded to the switches. Others are rejected with an OFP_ERROR message, thus, protecting the switches from unsupported OpenFlow messages.

[2] OFTest, Available: http://www.projectfloodlight.org/oftest/

3. AmLight Innovations Initiatives Evaluated

During the last two years, a few different SDN control planes were hosted at AmLight in parallel with production control planes. This section describes our experience with two of them: (1) the ONOS/SDN-IP application and (2) the FIBRE testbed.

3.1. Using ONOS as a use case

Open Network Operating System[3] (ONOS) is an open source OpenFlow controller developed with the focus on Internet Service Providers. ONOS has an application to handle BGP feeds, IP and IPv6 forwarding, called SDN-IP.

During the ONOS SDN-IP's evaluation process, AmLight engineers were not aware of the lack of support for MAC rewriting in one of AmLight's OpenFlow switches. Consequently, OpenFlow error messages were sent back and, as the FSFW proxy sits between the controller and OpenFlow switches, the process of locating the OpenFlow switch generating the error message was quite complex.

With the OpenFlow Sniffer's proxy support, different from any other traditional sniffer available, determining the OpenFlow switch without the MAC rewriting support became possible to be done in near real time. Similar troubleshooting methodology was utilized to identify modules that did not support matches based on TCP ports. With the OpenFlow Sniffer, all possible matches and actions used by ONOS/SDN-IP were mapped during the evaluation methodology process.

3.2. Using FIBRE as a use case

The FIBRE [Sallent 2012] federated research testbed has a set of wireless and OpenFlow devices available for experimentation. An overlay network (FIBREnet) interconnects all the facilities and enables wide-area OpenFlow experiments. FlowVisor [Sherwood et al. 2009] is being used as an SDN hypervisor to enable researchers to create network slices.

During FIBRE's evaluation process, the following challenges were found: (1) FlowVisor expected to fully control the OpenFlow switches, not a slice; (2) Use of untagged VLAN is hardcoded into FlowVisor but at AmLight, untagged VLAN was reserved for internal use; (3) FIBRE assumes that any OpenFlow controller can be used by the user but AmLight requires that all controllers needs to be validated through the evaluation methodology; (4) All OpenFlow features are provided to the FIBRE user. But, at AmLight, only risk-free features are allowed.

The challenges detected during the evaluation process forced AmLight to try a new approach: a new security layer was created to filter these unsupported OpenFlow messages. The Testbed Sanitizer was then created and was described in Section 2.3.

6. Findings

Most of the issues threatening network availability were stateful, not stateless. Stateful issues occur as a result of multiple messages, or a sequence of messages in a particular context. Even with the evaluation methodology in place, stateful issues may pass undetected. As a proof of concept, the Testbed Sanitizer has proved to be an interesting

[3] Open Network Operating System, Available: http://onosproject.org

approach to handling unsupported OpenFlow messages. However, it may require a significant development effort to address stateful issues. As a lesson learned, it became evident that we should work with the network device's vendor to improve its OpenFlow agent instead of investing in external security filters. Any extra layer of protection, in the end, also increases the operational complexity and should be avoided.

Additionally, the application of the evaluation methodology when starting a new control plane proved to be fundamental. Throughout the evaluation process, AmLight engineers could understand how the application worked and then be prepared for future troubleshooting processes. Even though the evaluation process is very useful, it is very time-consuming and needs to be automated for future evaluations.

Before having the Testbed Sanitizer and the OpenFlow Sniffer, troubleshooting activities used to last up to 30 hours, and, during the process, outages compromised the production network. With the innovations in place, all OpenFlow messages are traced effectively, and non-compliant OpenFlow messages are discarded in real-time. The number of outages that resulted from these stateless non-compliant OpenFlow messages dropped substantially: from 15 network outages to 0 in the first year.

7. Conclusions

Hosting multiple control planes in parallel has proven to be complex, but possible, manageable and beneficial to network operators. It requires a deep understanding of how network devices and protocols work, how to debug issues, and how to avoid impacts to the network resilience. Troubleshooting tools and OpenFlow agents still need to evolve to protect against a single experimental application compromising the overall availability of a production environment. The Evaluation Methodology, the OpenFlow Sniffer, and the Testbed Sanitizer have considerably reduced the potential risks of supporting parallel control planes at AmLight.

References

Bezerra, J., Galiza, H., Ibarra, J., & Schwarz, M. (2016) "AmLight's OpenFlow Sniffer dissected: Troubleshooting production networks". In Anais do WPEIF 2016 Workshop de Pesquisa Experimental da Internet do Futuro (p. 33). (to appear in proceedings).

Ibarra, J., Bezerra, J., Morgan, H., Lopez, L., Cox, D., Stanton, M., Machado, I. & Grizendi, E. (2015). "Benefits brought by the use of OpenFlow/SDN on the AmLight intercontinental research and education network". In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM) (pp. 942-947). IEEE.

McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Turner, J. (2008). OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38(2), 69-74.

Sallent, S., Abelém, A., Machado, I., Bergesio, L., Fdida, S., Rezende, J., Tassiulas, L. (2012). FIBRE project: Brazil and Europe unite forces and testbeds for the Internet of the future. In International Conference on Testbeds and Research Infrastructures (pp. 372-372). Springer Berlin Heidelberg.

Sherwood, R., Gibb, G., Yap, K. K., Appenzeller, G., Casado, M., McKeown, N., & Parulkar, G. (2009). Flowvisor: A network virtualization layer. OpenFlow Switch Consortium, Tech. Rep, 1-13.