Sexta Conferencia de Directores de Tecnología de Información, TICAL 2016
Gestión de las TICs para la Investigación y la Colaboración
Buenos Aires, 13 al 15 de septiembre de 2016

Deploying SDN experiments in Latin America: the ONOS and SDN-IP application use case at AmLight

Humberto Silva Galiza de Freitas[a], Marcos Felipe Schwarz[a], Jeronimo Aguiar Bezerra[b], Julio E. Ibarra[b]

[a] NEG AmLight, Rede Nacional de Ensino e Pesquisa (RNP), Av. Dr. Andre Tosello, 208, 13083-886 Campinas, São Paulo, Brazil
humberto.galiza@rnp.br, marcos.schwarz@rnp.br

[b] Center for Internet Augumented Research (CIARA), Florida International University (FIU), 11200 S.W. 8th Street Charles Perry (PC) Bldg - Suite 312, Miami, United States
jbezerra@fiu.edu , julio@fiu.edu

Abstract. AmLight boasts a geographical network and has been using with SDN/OpenFlow since the middle of 2014. Since the beginning, the network is capable of slicing, and this provided the ability to implement testbeds in parallel with the production network. This paper describes AmLight's experience on deploying a global experimentation Software-Defined network running on a dedicated slice. This network was deployed along with thirteen NRENs and universities around the globe. The main goals of this network were: a) to provide end-to-end provisioning of Layer 3 connectivity without using legacy routers; b) transform Autonomous Systems (AS) running OpenFlow into IP/BGP transit networks; c) provide a feasible migration strategy from legacy IP/BGP networks towards an SDN/OpenFlow approach.

Keywords: Software-Defined networking. ONOS. BGP.

1 Introduction

By the middle of 2014, AmLight became the first research and academic network bridging the Americas to deploy the SDN novel by using the OpenFlow protocol. As a consequence, the network programmability emerged as a new service offered to the academic community, and for the first time, U.S. and Latin American researchers could use AmLight's infrastructure to prototype their network-aware applications, using an approach called slicing.

With dedicated slices, researchers now have the possibility of implementing testbeds with real network devices, including all limitations. Their applications can be moved from a simulated environment to an at-scale, experimental environment, where they would face production challenges, such as CPU, memory, and bandwidth, as well as hardware and software limitations. Network testbeds can control how packets are forwarded on a per-hop basis, and if desired, packets could be manipulated along the forwarding path.

The AmLight's experience obtained both from the SDN/OpenFlow deployment process, and all hosted network testbeds has enabled AmLight engineers to help similar initiatives in Latin America. Currently, several collaboration projects are being supported, and in this paper some sucessfull use cases involving AmLight and Latin America RENs and Universities in the field of advanced networks will be detailed.

The rest of the paper is organized as follows: Section 2 describes the AmLight project, its network, and how the network programmability and slicing are being supported for network experimentation. Section 3 describes the ONOS and its SDN-IP application advantages when moving from IP/legacy towards an SDN approach. Section 4 presents the Global ONOS SDN-IP deployment and how the ONOS and its SDN-IP application were deployed at AmLight. Section 5 provides the final considerations and the next steps.

2 Description of AmLight

Americas Lightpaths (AmLight - NSF Award # for AmLight OCI-0963053) is a project of the U.S. National Science Foundation International Research Network Connections (IRNC) program to facilitate science research and education between the U.S. and the nations of Latin America. AmLight operates a number of international network 10G and 100G links connecting U.S. R&E networks to similar networks in Latin America.

The AmLight links are shared and operated collaboratively by Florida International University (FIU), the Academic Network of São Paulo (ANSP), and Rede Nacional de Ensino e Pesquisa (RNP). The AmLight network topology is represented in Figure 1.

Fig. 1. AmLight topology connecting Miami in the U.S., Fortaleza, Rio de Janeiro and São Paulo in Brazil, and Santiago in Chile. AmLight also operates circuits from Panama City to Miami in a collaboration with RedCLARA.

As an academic network, the AmLight network transports science applications using L2 and L3VPNs; IP and IPv6, including multidomain multicast applications. In parallel with the academic traffic, AmLight also transports non-academic IP and IPv6 traffic, including access to traditional websites, e-mails and multimedia applications. Most of the academic (science research) applications transported use large packets (over 8000 Bytes) with a few flows consuming an elevated amount of bandwidth. Non-academic applications usually use multiple low-bandwidth flows with small packets (up to 1500 Bytes). Both, academic and non-academic application profiles are critical for AmLight operations, requiring that monitoring and troubleshooting tools be installed and ready for any incident.

2.1 Network Programmability at AmLight

Network programmability (or *slicing*) allows multiple tenants to share the same physical infrastructure. A tenant can be a customer requiring an isolated network slice or an experimenter who wants to control and manage some specific traffic from a subset of endpoints.

With slices, a controller of one slice cannot interfere with other slices; for example, it cannot remove flow entries or overlap them. Network programmability was achieved at the AmLight network using Internet2's Flow Space Firewall (FSFW) - an OpenFlow proxy that controls what OpenFlow controllers can do to the OpenFlow devices.

FSFW makes possible a new service called "network slicing", "network virtualization" or just "*slicing*" with specific switch ports and VLAN ranges, allowing multiple controllers to manage one or more OpenFlow devices.

Different from other slicing tools, such as FlowVisor, FSFW does not try to change any OpenFlow message sent by the OpenFlow controller; it just accepts or rejects the message, sending an OpenFlow error to the controller in case of rejection.

To enable slicing, all OpenFlow devices must be configured to have the FSFW as its OpenFlow controller; a TCP session is then established from the device to the FSFW. Once this connection is established, FSFW checks which slices have the new connected OpenFlow device included in its configuration.

Acting as a proxy for multiple devices and controllers, FSFW has to handle all OFPT_ERROR messages. These messages are generated by OpenFlow devices and only use the transaction ID (XID) field associated with the request as an identification. The only way FSFW can associate the OFPT_ERROR received to a controller is by having control of all XIDs in use; in this case, FSFW generates XIDs and keeps a hash internally.

Below is an example of a slice configured on FSFW, using XML format:

```
<slice name="AmLight">
   <switch name="ampath1">
     <port name="eth1/8">
```

```
        <range start="50" end="1777"/>
        <range start="1800" end="1849"/>
      </port>
      <port name="eth2/1">
        <range start="50" end="1777"/>
        <range start="1800" end="1849"/>
      </port>
    </switch>
    <switch name="ampath2”>
      <port name="eth1/2”>
        <range start="50" end="1777"/>
        <range start="1800" end="1849"/>
        </port>
      <port name="eth2/3”>
        <range start="50" end="1777"/>
        <range start="1800" end="1849"/>
      </port>
    </switch>

    <controller ip_address="2.2.2.2"
      ssl="false" port="6633"/>
</slice>
```

In this XML code snippet, a slice named “AmLight” with two switches, “ampath1” and “ampath2”, are configured. Each switch has two ports and two VLAN ranges associated with each port. At the end of the slice configuration, an OpenFlow controller is specified, where the network administrator inserts an IP address, a TCP port and a SSL option.

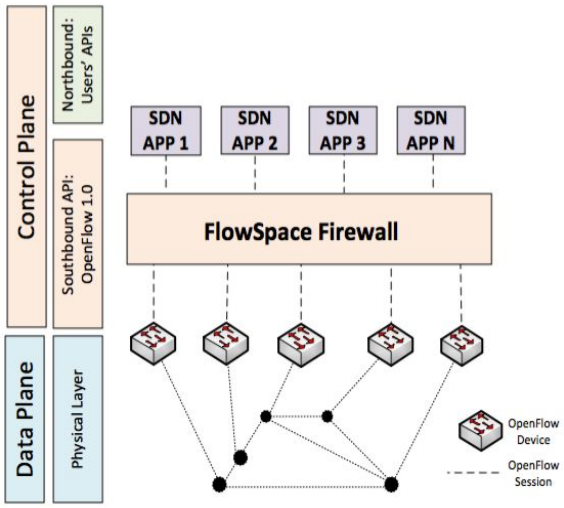

Fig. 2. AmLight SDN stack after deploying OpenFlow 1.0, FlowSpace Firewall and SDN applications. The dashed line between devices and the Flow Space Firewall and, between Flow Space Firewall and SDN applications (represented by purple boxes) represent the OpenFlow sessions established. In this configuration in the SDN stack, FSFW acts as a proxy between the

physical layer (represented by OpenFlow devices and links) and the control layer, represented by SDN applications.

To describe how AmLight supports network virtualization, we refer to Figure 2: the FSFW manages what each SDN application can do to OpenFlow devices. It is important to observe that, from the perspective of the data plane, all flows are handled in the same way. OpenFlow devices are not aware of multiple controllers, and all flow entries are inserted in the same table, as part of the same data plane. In this case, because SDN applications can send OpenFlow messages to the OpenFlow devices (assuming they were allowed by the FSFW), the OpenFlow agent inside each device is responsible for interpreting those messages and reacting in the proper way (sending an error, installing the flow, sending a reply, etc.).

In the upcoming sections, we will describe the ONOS and its SDN-IP, and how the presented AmLight slicing capability allowed the network experimentation.

3 The ONOS and SDN-IP application

Open Networking Operating System (ONOS) is a free, Open Source, carrier-grade SDN Operating System designed for Service Providers. ONOS has been architected based on three key principles: Scalability, High Availability, and performance. Moreover, it provides well-defined Northbound and Southbound abstractions and software modularity. ONOS ecosystem comprises of ON.Lab [3] and organizations that are funding and contributing to the ONOS initiative. AmLight is one of the ONOS Project official collaborators since the middle of 2015.

SDN-IP is an ONOS application able to transform a Software-Defined network in an IP transit network, thus, a) connecting the SDN domain to legacy networks using BGP; b) allowing multiple Administrative Domains to communicate through the SDN network.

From ONOS perspective, SDN-IP is just an application that specifies their network control desires in a policy-based form, or *ONOS Application Intent Request*, and uses its services to install and update the appropriate forwarding state in the SDN data plane.

SDN-IP provides a concrete migration solution to SDN. Operators can introduce new SDN capabilities along the existing legacy infrastructure, allowing the two technologies to coexist, while accelerating SDN adoption [4].

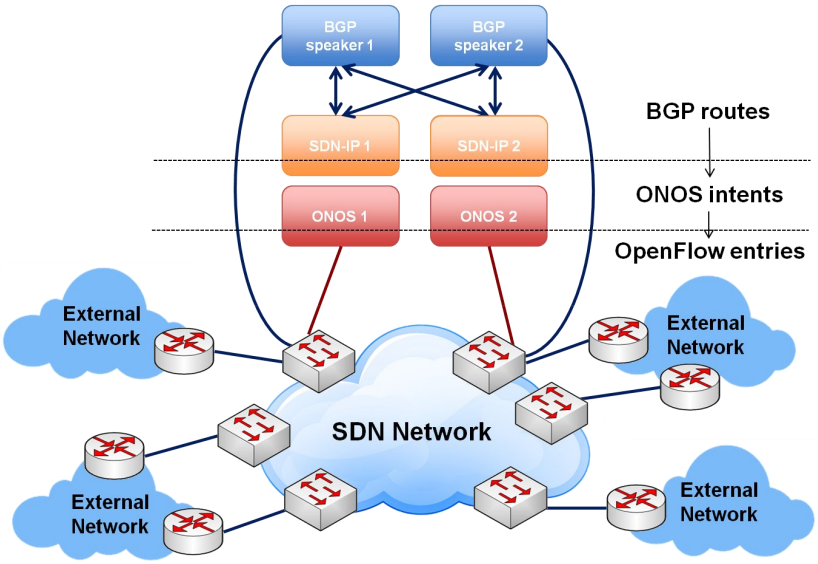

Fig. 3. ONOS SDN-IP application architecture: external networks using legacy IP/BGP peer with ONOS BGP speakers. The best route for each destination is selected by the SDN-IP application according to the iBGP rules, and finally translated into an ONOS Application Intent Request. Then, ONOS translates the Intents into OpenFlow entries and installs the entries into the SDN switches. Those rules are used to forward the IP traffic between the interconnected IP networks.

4 Global ONOS SDN-IP deployment

The Global ONOS SDN-IP deployment testbed has been first deployed in mid-2015 and expanded in 2016 connecting thirteen RENs and Research Institutions spanning five continents as depicted in Figure 4.

Fig. 4. Global ONOS SDN-IP deployment interconnecting RENs and universities from five continents.

Besides AmLight, GEÁNT and Internet2, the current testbed facility interconnects ten additional Research and Education Networks (RENs) from different countries: Academic Network of Sao Paulo in Brazil (ANSP), Australian Academic Network (AARNet), Brazilian National Research and Education Network (RNP), Caribbean Knowledge and Learning Network (CKLN), Commonwealth Scientific and Industrial Research Organisation (CSIRO), Italian Research & Education Network (GARR), Korea Research Environment Open NETwork (KREONET), Latin American Cooperation of Advanced Networks (RedCLARA), Red Universitaria Nacional in Chile (REUNA), and the National Chiao Tung University (NCTU) from Taiwan.

The following motivations have been considered at the time AmLight decided to join the SDN Global Deployment: (1) create a global SDN network; (2) provide L2 and L3 connectivity without legacy equipment in the network core; (3) bring network innovation exploiting new applications developed internally at AmLight.

From the ONOS community perspective, a deployment such that experiment would demonstrate that ONOS could work in real networks, and its high performance, high availability and scalability features meet all the highest requirements from network operators. Furthermore, having a real world use case would provide fundamental feedback from production, which is translated into requirements, thus improving the software development cycle by an agile deployment model.

The global deployment participants got interconnected by using AmLight (from the U.S to Latin America), PacificWave (from the U.S to Asia and Oceania), and ES.Net (from the U.S to Europe) international links. Layer 3 reachability between the external domains was fulfilled by using the traditional IP/BGP peering.

Also, it is worth mentioning that as the network had the purpose to be a platform for innovation, both CSIRO/AARNet and GEÁNT have developed and employed their SDN/IP application to bridge the legacy IP/BGP and the SDN worlds. This accomplishment highlights how easy it is to dock a new software piece into ONOS and then make it interoperable with existing applications.

4.1 ONOS SDN-IP testbed at AmLight

Initially, to set up the ONOS SDN-IP application experiment at AmLight, engineers had to pay attention to specific OpenFlow features support in the switches, such as mac-address rewriting (OpenFlow 1.0 optional action *SET_DL_DST*), required by the SDN-IP application. After finishing the validation process on the environment, a dedicated network slice was created to provide isolation to this application.

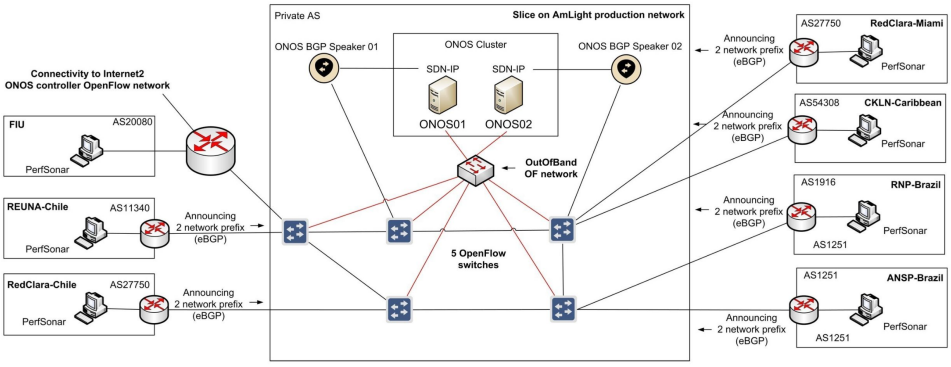

Fig. 5. ONOS SDN-IP deployment at AmLight: The bigger square represents the architectural diagram of ONOS SDN-IP deployment at AmLight network, combining five OpenFlow switches, controlled by an ONOS cluster that is composed of two controller instances and running SDN-IP. Two special purpose routers, also knows as the BGP speakers, peer with the external routers provided by RENs and, at the same time, connect to the SDN-IP instances. They are considered special purpose routers due to this dual-capability.

Additionally, AmLight connected with International RENs, by bringing up a general purpose router, and legacy IP/BGP setup to have to peer with each of them. After receiving the routes, AmLight re-advertised them to the ONOS BGP Speakers, and by iBGP these routes were learned by all RENs, thus delivering end-to-end connectivity between all connectors.

Furthermore, all participants installed a perfSonar [5] server on their sites and assigned to it an IP address from the pool of prefixes advertised in the testbed. By having these servers, it was possible to generate one-way delay measurements among the participants, and further, the results were presented to them through a web portal.

To summarize, the solution deployed was able to provision end-to-end Layer-3 connectivity without using legacy routers in the network core, transforming ASes running OpenFlow into IP (BGP) transit networks. Consequently, it can be recognized as an available migration strategy from legacy IP/BGP networks towards an SDN/OpenFlow approach.

5 Final Considerations

Joining the *Global SDN deployment powered by ONOS* provided excellent visibility and experience to AmLight's network. Its network virtualization capability has proved to be a valuable asset for testing new solutions using real network hardware and in a large scale.

The ONOS SDN-IP application deployment at AmLight validated that it is a nondisruptive solution that could be easily used as a migration path from legacy IP/BGP networks towards an SDN approach, in a reasonable period without requiring an immediate upgrade of networking devices.

As a future work, there are plans to attract more RENs and universities to join the testbed from Q2 2016. Also, with the imminent AmLight migration to OpenFlow 1.3, new ONOS features such as Multi-table pipeline support, QoS and IPv6 should be tested on a large scale using the testbed in place. Furthermore, the new ONOS Virtual Private Lan Service (VPLS) application is planned to be tested and validated in mid-2016 using a similar approach.

Acknowledgments

The authors would like to thank ON.Lab team (www.onlab.us), in special Luca Prete, for all the support provided for this experimentation.

References

1. Ibarra, J., Bezerra, J., Morgan, H., Fernandez Lopez, L., Stanton, M., Machado, I., Grizendi, E., and Cox, D. A. (2015). Benefits brought by the use of openflow/sdn on the amlight intercontinental research and education network. In *Integrated Network Man- agement (IM), 2015 IFIP/IEEE International Symposium on*, pages 942–947. IEEE.
2. Internet2 (2016). Internet2 - research and education network. *Online website: http://www.internet2.edu*.
3. ONOS (2016a). Onos project. *Online website: http://www.onosproject.org*.
4. ONOS (2016b). Sdn-ip application - onos project. *Online website: https://wiki.onosproject.org/display/ONOS/SDN-IP+Architecture*.
5. ESNet, GEÁNT, Indiana, U., and Internet2(2016).Perfsonar - performance service oriented network monitoring architecture. online website: http://perfsonar.net.