The UPV/EHU OpenFlow Enabled Facility

Jon Matias, Eduardo Jacob
University of the Basque Country
Alda. Urquijo s/n 48013 Bilbao (Spain)
+34 946017370
{jon.matias, eduardo.jacob}@ehu.es

ABSTRACT

This paper introduces the OpenFlow Enabled Facility deployed at the University of the Basque Country by the I2T research group. The EHU-OEF infrastructure is presented and security aspects are described. The IEEE 802.1X standard is used to authenticate and authorize the access to available services and resources.

Keywords

OpenFlow, NOX, IEEE 802.1X, Authentication and Authorization.

1. INTRODUCTION

This paper introduces some aspects of the OpenFlow Enabled Facility (OEF), which is currently under deployment at the campus of the University of the Basque Country (UPV/EHU). The EHU-OEF project has been proposed by the I2T research group from the same University. Since mid-2010, the I2T-OF division, composed by professors, researchers and students, is testing, developing and promoting the use of OpenFlow [1].

The EHU-OEF is the first campus-wide experience with OpenFlow at UPV/EHU. Prior to this, all the prototypes and developments related to OpenFlow have been tested at the I2T research laboratory. The idea behind this project is to broaden the experimentation in networking, while assuring the transport of production traffic. Once OpenFlow is deployed, the Software Defined Networking paradigm can be applied.

The University of the Basque Country employs over 7.000 persons throughout 31 faculties and schools geographically distributed in three campuses with over 50.000 undergraduate and postgraduate students. Traditionally, at the UPV/EHU there are only a few roles that could be assigned to an end-user (e.g. student, researcher, lecturer, or administrative). This means that once a role is assigned, a set of resources are available. The resources are different depending on the selected role. However, as networking researchers who take part in different platforms and experiments (sometimes with specific connections to outside partners), there is an increasing necessity to address the setup and management of experiments. Nowadays, this could take long time (days or even weeks) and a lot of e-mails and phone calls to get the final configuration working. The worst thing is that at the end, there are some limitations that cannot be overcome, for instance, the ability to run multiple roles or testing new protocols.

The rest of the paper is organized as follows. First, the OpenFlow Enabled Facility infrastructure is introduced in section 2. Then, security aspects, mainly authentication and authorization issues, regarding the OEF are analyzed in section 3. Finally, section 4 presents some conclusions.

2. OPENFLOW ENABLED FACILITY

In this section, the EHU-OEF infrastructure is described more in detail. The infrastructure is still under deployment, but a first functional setup has been released. The current deployment is shown in Figure 1. The resources available at I2T to build the facility are seven NEC switches (IP8800/S3640 OpenFlow enabled) [2], two NetFPGAs and four WiFi APs (Pantou).

Both professor offices and practice labs are connected by the OpenFlow infrastructure to the I2T research lab. At this first stage, only one node of each type has been involved, but the idea is to have more in the future. The I2T research lab is well connected to the UPV/EHU production network and directly to both the Spanish NREN (RedIRIS) and the Basque NREN (i2basque). The facility has a 10Gbps core, with a 10Gbps connection to the RedIRIS PoP. Due to the fact that the NEC IP8800 only has two 10Gbps interfaces, 1Gbps links have been used to connect the rest nodes. The users (professors, researchers and students) are also connected at 1Gbps.

At OEF, both production and experimental traffic share the same physical infrastructure. Afterwards, each of these traffic flows are identified and forwarded to the appropriate output.

In order to control the OEF, the NOX controller [3] has been configured. New modules have been developed for NOX to get the desired behavior. The controller is located at the I2T research laboratory, directly connected to one of the NEC switches. The OpenFlow control traffic has been configured as inband, which means that the same physical links used for transmitting data are used to transport the OpenFlow protocol packets from the NOX to the switches. By doing this inband communication, no extra connectivity is needed to transport the control plane. All the NEC switches have configured the VLAN 100 for that purpose.

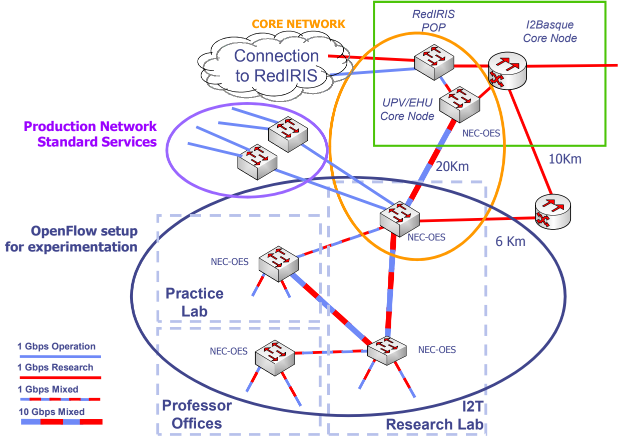

Figure 1. UPV/EHU OpenFlow Enabled Facility.

3. AUTHENTICATION & AUTHORIZATION

Due to the quite extensive area currently covered by the OEF, the security is a fundamental concern. Although, the infrastructure is mainly based on wired connections, the same users need to access the network services at different locations (lab, classroom, office) and the same physical ports can be used by different users with different roles. This dynamic scenario needs to be securely controlled. Prior to the OEF deployment, the access to the I2T research network was controlled by IEEE 802.1X and a RADIUS server connected to the I2T LDAP. Therefore, instead of deploying an OpenFlow integrated solution (such as Ethane [4]), we decided to reuse the preexisting security infrastructure.

The expected behavior is described as follows. When a new user (student, internal/external researcher, professor) wants to get access to the OEF network, an identifier and requested service should be provided. In this context, the service is the final reason of connectivity (e.g. access to Internet, access to experiment A, or access to private I2T resources). In the end, the service can be identified by a set of flows (OpenFlow rules). Depending on the requested service and the result of the authentication and authorization process, the OEF is configured (on demand) to permit or deny the access from the user to the service. A similar behavior is proposed at RFC 4675 [5] by dynamically assigning the VLAN ID.

To get all this working, three main issues need to be solved:

- The interaction of legacy protocols with OpenFlow.
- OpenFlow configuration depending on the authentication and authorization process.
- A control framework to isolate traffic between experiments and production network.

Regarding the first issue, the legacy protocol should be analyzed in detail and univocally defined as OpenFlow flows. In this case, the protocol is the EAPoL and this traffic is completely identified by its ethertype (0x888E) and multicast address (01:80:C2:00:00:03). Therefore, all the EAPoL traffic exchange between the user and the authenticator (IEEE 802.1X terminology) can be defined as flows. This step is identified with (1) “AAA control” at Figure 2.

The process is as follows. A new packet with ethertype 0x888E is sent from the user’s MAC address to the multicast address. Since there is no previously defined rule to handle this traffic, the packet is encapsulated and redirected to the NOX controller. The NOX identifies the ethertype as AAA traffic and checks the multicast address. Then, the learning process takes place and registers the physical port associated with the user’s MAC address. The authenticator is supposed to be an internal process from the switch, but this is not an option when dealing with an OF switch. Consequently, the authenticator is running on an external machine at the I2T research lab, and all the traffic should be redirected to it. At the edge node, enabling the EAPoL exchange means two rules, which can be easily defined:

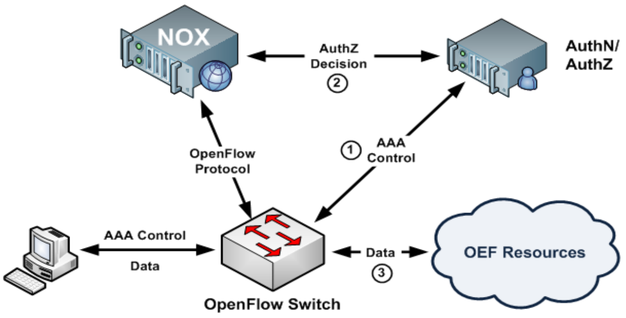

Figure 2. Authentication and Authorization in the OEF.

DstAddr: 01:80:C2:00:00:03, SrcAddr: UserMACAddr, Ethtype: 0x888E, InPort: Learned_Port => Action: Authenticator_Port

DstAddr: UserMACAddr, SrcAddr: 01:80:C2:00:00:03, Ethtype: 0x888E, InPort: Authenticator_Port => Action: Learned_Port

Regarding the second issue, a new communication channel with the NOX controller is needed. Opposite to previously described mechanism of sending packets from the OF switch to the NOX, in this case an asynchronous channel from an external entity (the AuthZ server) is required. For that purpose, a web service based on REST is enabled at the NOX controller. This step is identified with (2) “AuthZ decision” at Figure 2. Therefore, a new REST client is implemented and launched once the AuthZ generates a profile describing the service. For optimization reasons, the profile is transmitted to the NOX in JSON format. Once the JSON profile gets into the controller, it is parsed to obtain the needed parameters to activate the new access from the user to the service.

In the simplest case, the user requests a new service to get access to Internet: step (3) “Data” at Figure 2. The service can be identified at flow level as IP traffic from the client’s MAC address to the gateway’s MAC address, and vice versa:

DstAddr: Gateway_Address, SrcAddr: UserMACAddr, Ethtype: 0x0800, InPort: Learned_Port => Action: Gateway_Port

DstAddr: UserMACAddr, SrcAddr: Gateway_Address, Ethtype: 0x0800, InPort: Gateway_Port => Action: Learned_Port

Regarding the last issue (for future work), the control framework is expected to be based on FlowVisor [6], which creates network slices. In addition, this will enable the possibility of experiments running their own controller.

4. CONCLUSIONS

The paper has presented the current status of the EHU-OEF infrastructure. Afterwards, the secure procedure to request a network service has been described, which is based on IEEE 802.1X. Instead of developing an authenticator or an EAPoL proxy at NOX, the EAPoL traffic has been identified and forwarded to an external machine running a Linux-based authenticator, improving the provisioning performance.

5. ACKNOWLEDGMENTS

This work has been partially funded by the Spanish MICINN project A3RAM-NG (TIN2010-21719-C02-01).

6. REFERENCES

[1] N. McKeown, et. al., “OpenFlow: Enabling Innovation in Campus Networks”, ACM SIGCOMM 2008.

[2] NEC IP8800, http://www.nec.co.jp/ip88n/ip8800_s3630

[3] N. Gude, et. al. “NOX: Towards an Operating System for Networks”, ACM SIGCOMM 2008.

[4] M. Casado, et. al., “Ethane: Taking Control of the Enterprise”, ACM SIGCOMM 2007

[5] RFC 4675, RADIUS Attributes for Virtual LAN and Priority Support, http://www.ietf.org/rfc/rfc4675.txt

[6] R. Sherwood, “Flowvisor: A network virtualization layer”.