Exercise for Lecture Software Defined Networking

Prof. Dr. David Hausheer
Julius Rückert, Leonhard Nobach

TECHNISCHE UNIVERSITÄT DARMSTADT

Winter Term 2015/16
Exercise No. 4
Published at: 24.11.2014
Submission exclusively via Moodle, Deadline: 08.12.2014
Contact: [rueckert|lnobach]@ps.tu-darmstadt.de
Web: http://www.ps.tu-darmstadt.de/teaching/ws1516/sdn/
Submission: https://moodle.tu-darmstadt.de/enrol/index.php?id=6349
– Example Solution –

Problem 4.1 - Network Virtualization and Slicing

a) Duties of an SDN Controller

Name three duties of a typical SDN controller and state at least two examples for each of them.

Solution:

A) Monitoring of the physical network, e.g. which switches exist and the states of their rules. Example states are the packet and byte counters for each flow rule in an OpenFlow switch.

B) Control: e.g., tunnel setup and the mapping between the virtual and physical topology.

C) Tell the switch what to do: e.g., create/modify/delete flow rules and define the matching and action field of the rules.

b) Network Virtualization with VLANs

Two datacenters D and E use VLANs for traffic isolation between their hosts. The datacenters are connected over a L3 connection, e.g. the Internet, and need to share their network segments.

I Propose a solution (without using SDN or VXLAN) for preserving the slices, even when communication is carried out over the L3 link.

Solution: The problem to address is that VLAN tags cannot be forwarded over public Layer 3 networks like the Internet without applying *encapsulation*. Encapsulation, also known as tunneling, adds an encapsulation and IP header before the Ethernet frame, so that the frame can be sent over Layer 3 networks. For this kind of solution, we require tunnel endpoints, which add and strip the encapsulation headers, and address themselves in the source and destination addresses of the outer IP packet.
Therefore, we set up two tunnel endpoints, each at the perimeter of the two datacenters. The tunnel endpoints have access to the public L3 network, as well as to the L2 network comprised of different VLANs. Possible encapsulation protocols (except VXLAN) are for example GRE

II On an example of two hosts A (in Datacenter D) and B (in Datacenter E), draw a communication diagram of a packet sent from A to B over a common network segment. This diagram should include every intermediate hop (except pure L2 switches and simple routers on the Internet).

Solution: In our diagram, the tunnel endpoints are `tepD` and `tepE`.

```
A --> tepD --> tepE --> B
```

III Draw the protocol stack (except Layer 1 and everything above the Transport Layer) of the packet into the diagram, between each two intermediate hops. Example: (Ethernet, IP, UDP)

Solution: In our diagram, the tunnel endpoints are `tepD` and `tepE`.

```
A -(Ethernet, VLAN, IP, UDP)-> tepD -(..., IP, GRE, Ethernet, VLAN, IP, UDP)-> tepE
-(Ethernet, VLAN, IP, UDP)-> B
```

IV Make yourself familiar with VXLAN and the VXLAN header. Name at least *two* advantages of VXLAN compared to your solution (Hint: Think about an intermediate NAT between the datacenters).

Solution:

- VXLAN allows for 16777215 different network slices, compared to VLANs only supporting 4096.
- As VXLAN makes use of UDP, it survives port translations, and thus allows to traverse NAT gateways. With GRE, this is not possible.

V Name at least *one* advantage of OpenFlow compared to (pure) VXLAN in the context of network slicing.

Solution:

- More flexible redirection of traffic (for example when "switching" between VNFs)
- Allows for new use cases like efficient multicast and NFV service chains.
- Significantly lower overhead on the data plane due to the possibility of using local labels, instead of encapsulation.

c) Energy saving

Imagine at least one scenario in which SDN can save energy.

Solution:

It can be more energy efficient to put the control plane processing on a single powerful processor instead of distributing these calculations amongst many switches.

Problem 4.2 - FortNOX

a) FortNOX Authentication

How does FortNOX guarantee that only certain users can add/modify/delete flow rules? Which steps are required to be performed by the FortNOX administrator in advance w.r.t. the authentication mechanism.

Solution:

The administrator has to take the public key of an asymmetric cryptographic key pair and make it available in FortNOX. The user which owns the corresponding private key can now send commands to FortNOX with an digital signature of these commands in addition.

b) FortNOX Rule Conflicts

How can FortNOX solve rule conflicts? Give an example.

Solution:

First, a human admin sets a flow rule which allows all traffic on port 80. Second, a security app decides to block all traffic on all ports. FortNOX prioritizes the flow rules w.r.t. their issuing source. A human admin has a higher priority than a security app. As a consequence, the security app's rule causes a conflict and is not applied since the existing rule from a human admin is already there.

Problem 4.3 - Case Study 4 - Home Router Virtualization

a) This task is a case study. You are supposed to demonstrate theoretical concepts defined in the lecture in an applied setting. Only the problem and its rough context is defined. The context may be extended, if necessary. You are intended to define processes and procedures to solve the problem. Your solution should be defined to an extent allowing a team of skilled staff to implement your solution, i.e., details may be omitted, if they do not have a large impact on your solution. The solution should be presented in a text-based form. Additional literature may be used.

Scenario and Setting:

MVA GmbH is the vendor of the well known BoxFritz home router series. The Software Defined Networking trend is a major threat to MVA's business model: most Internet Service Providers (ISPs) want to get rid of home routers, as the monetary expenses for the device and maintenance constitute the majority of costs per subscriber. MVA's management fears that ISPs will enter the home router market with cheap and "dumb" data planes controlled by an ISP owned controller.

In order to prevent a disadvantageous strategic position, the management decides to offensively anticipate the SDN trend.

As a first step, MVA equips the BoxFritz home router series with OpenFlow capabilities controlled by an MVA owned controller. Based on this setup, MVA wants to offer value added services to their customers.

MVA plans to start a field test offering the following service to private subscribers:

Over-the-Top (OTT) service providers like YouTube or Hulu often apply country barriers to traffic coming from foreign IPs due to legal issues. MVA wants technical means to identify requests to foreign blocked OTT services using a predefined list of domain names per country (e.g., http://www.hulu.com in Germany). Whenever a user in country A requests a blocked service in country B, the traffic should be redirected transparently to a proxy in country B to circumvent the barrier.

Create a system architecture to implement the service. Include a description of the involved components, the necessary communication between components and the necessary OpenFlow rules.