Isolation of original (production) and mirrored traffics

Kazuhiro Suzuki and Soichi Shigeta
(Fujitsu Laboratories)

2015/11/16
Introduction

- The port mirroring capabilities are useful, but we also need to concern about performance impacts because the double number of packets must be transmitted.

- We guess that isolation between original (production) and mirrored traffics is required to manage QoS (or bandwidth) of each traffic. Especially, avoiding and controlling performance impacts for the original traffic.

- In our opinion, there are a few disadvantages in the current TaaS design.

- In this document, a design proposal to realize isolation is described.
Disadvantages of the current design

Assumptions:
- VMs A and B are running on different compute nodes (X and Y).
- VMs A and B communicate with each other.
- A Monitor VM is monitoring mirrored traffics.

Disadvantages:
1. A mirrored traffic double back to br_int. (in case of VM A is tapped)
2. A mirrored traffic flows the same VXLAN tunnel with original (production) traffic. (in case of VM B is tapped)
① To eliminate waste double back, connect a monitor VM to br_tap.
  - Flow entries in br_int and br_tap will be simplified.
  - Moreover, (we guess) “anti arp spoofing” can be enabled on br_int.

② To isolate original (production) and mirrored traffics from each other:
   step 1) Create another VXLAN tunnel (dynamically when it is needed) between br_taps.
   step 2) Add a flow entry to transfer mirrored packets to the tunnel.
Current Status

- We have implemented the proposed mechanism on our site.
  - version: kilo
shaping tomorrow with you