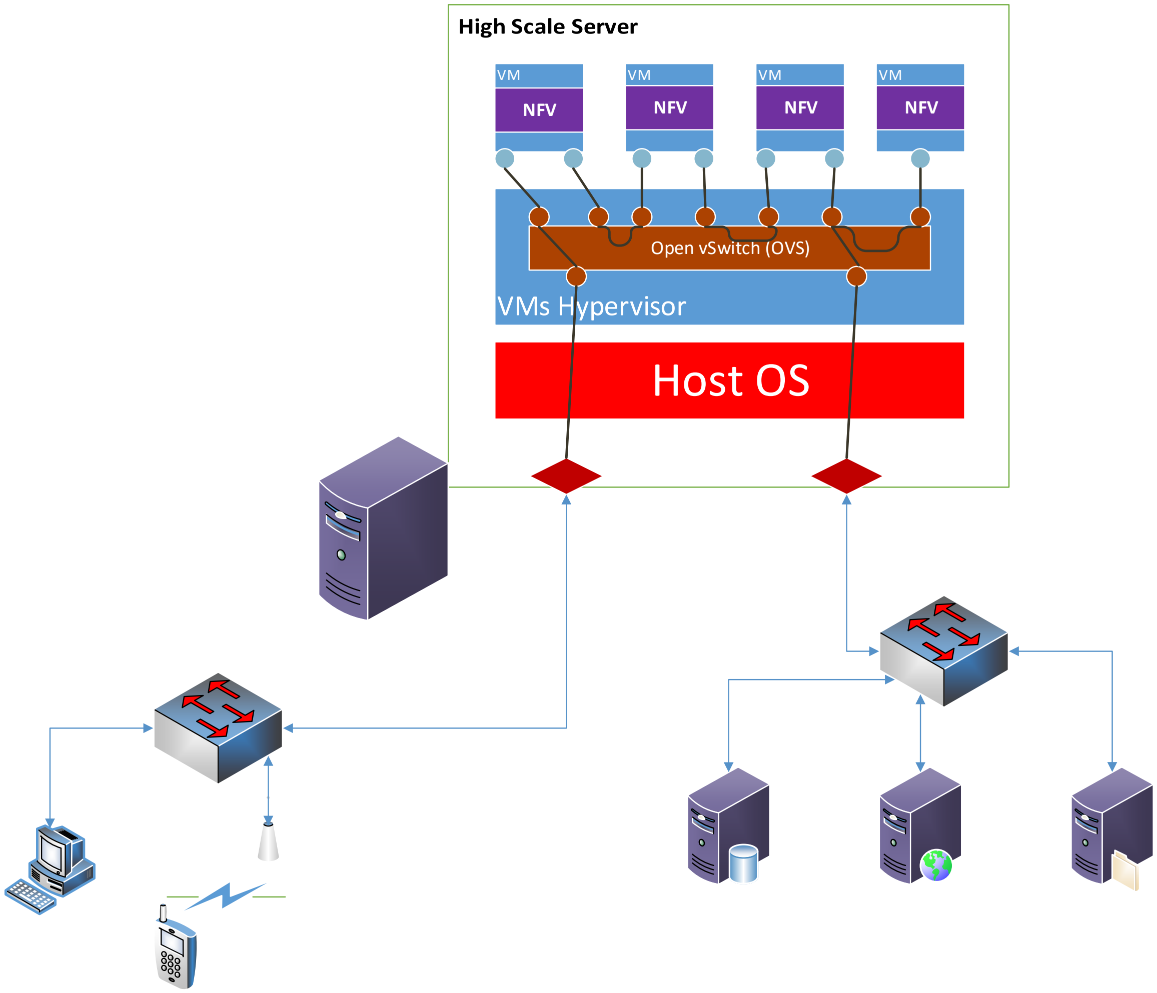
# Distributed Denial of Service (DDoS) attack detection in a virtualized network

## Abstract:

Today's Carrier Ethernet architecture is undergoing the biggest transformation since the beginning of the internet. Video, mobile and cloud usage is driving huge growth in traffic while the constantly changing traffic patterns requires ability to introduce new services quickly. This led the creation of Networking Function Virtualization (NFV), which defines the specifications for Virtualized Network Function (VNF).

VNF is a software implementation of a network function such as routing or firewall. Each such VNF runs in a virtual machine (VM). The VMs are created in a compute blade or in a high scale server – unusually called the host device. The VMs are located on top of the host's Hypervisor that uses Open Virtual Switch (OVS) to switch the data traffic to/from each VM/NFV and also to chain the traffic between them.

Distributed Denial of Service (DDoS) attack embedded in the data traffic can cause performance degradation to the OVS, NFVs as well as to the servers behind. A good sign for DDoS attack is an increasing or high rate of active data flows in each time slot – compared to normal or pre-defined number of flows threshold. In order to detect such case – it is required to have ability to estimate on-line the total number of flows per VM/NFV. The number of flows estimation can be done by analyzing sampled stream per VM/NFV.

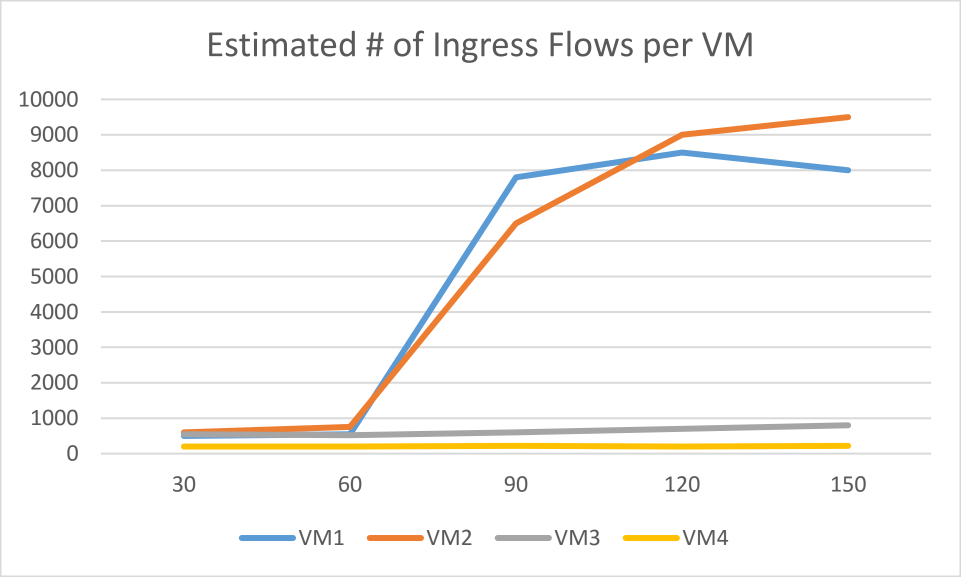

High Scale Server
VM
NFV
VM
NFV
VM
NFV
VM
NFV
Open vSwitch (OVS)
VMs Hypervisor
Host OS

## Goals:

Implement real-time DDoS attack detection per VM by analyzing sample of the Ingress and Egress stream on each VM. The implementation requires per VM Ingress/Egress number of flows estimation in each time slot (For example: in 30 seconds) by classifying the sampled packet's 5-Tuple fields -using HyperLogLog algorithm according to ***Cardinality Estimation Meets Good-Turing*** article (Algorithm 1).

Use a host device to simulate the attackers by opening a high rate of flows (TCP, UDP) using DDoS tools or by injecting real captured traffic with DDoS attacks in it.

Example of expected output:



## Requirements:

Internet Networking Course

## Guided by:

Telco Systems
A BATM Company