May 31, 2018

LAYER 4 THROUGH LAYER 7 SERVICE CHAINING FOR VIRTUAL NETWORK FUNCTIONS IN CLOUD ENVIRONMENT

Balaji Sundararajan

Samar Sharma

Yegappan Lakshmanan

LAYER 4 THROUGH LAYER 7 SERVICE CHAINING FOR VIRTUAL NETWORK FUNCTIONS IN CLOUD ENVIRONMENT

AUTHORS:
Balaji Sundararajan
Samar Sharma
Yegappan Lakshmanan

ABSTRACT

Methods are described to perform service chaining on a physical switch for virtual services. First, the switch observes and classifies Local Area Network (LAN) traffic, and determines that it needs to apply a service chaining rule based on classification results. Second, the switch forwards the traffic to the first Virtual LAN (VLAN) in the input chain. When the frame is processed by the container / Virtual Machine (VM), it forwards the traffic on the egress VLAN, which is used as an input to the next element in the chain.

DETAILED DESCRIPTION

Creating a chain of Layer 4 (L4) through Layer 7 (L7) services/applications (e.g., firewall, Load Balancing (LB), etc.) for the case of containers or virtual services where the switching is to be performed by a physical switch has not been addressed. This is a very powerful use-case.

For a physical switch connected to multiple virtual services inside one physical server, the physical switch performs the service chaining of the virtual services. The techniques described herein address this problem domain, and specifically service chaining in a cloud environment on a physical switch when the services are virtual.

Consider a physical switch connected to servers, with each server running multiple containers with many Virtual Network Functions (VNFs), such as firewalls, Web application firewalls, Distributed Denial of Service (DDoS), etc.). For various types of traffic, these VNFs should be stitched together.

The trunk interface between the switch and servers carries many Virtual Local Area Networks (VLANs). First, the switch observes and classifies Local Area Network (LAN) traffic and determines that it needs to apply a service chaining rule based on classification results. Second, the switch forwards the traffic to the first VLAN in the input chain. When the frame is processed by the container / Virtual Machine (VM), it forwards the traffic on

the egress VLAN, which is used as an input to the next element in the chain. A service chain can be provided in this manner via Layer 2, physically, or in TRUNK MODE, where many containers/VMs of different flavors can intercept and process traffic in L2 mode. In essence, selective VLAN translation capability is provided, without routing or Layer 3 (L3) hopping, along with service chaining. This is not currently available in any service chaining solution.

When sending traffic from a first container in the chain to a second container in the chain, the physical switch modifies the VLAN, without modifying the Media Access Control (MAC) or Internet Protocol (IP) addresses of the packet. In traditional service chaining, the VNF or container identifies the packet destined thereto using the destination MAC address or destination IP address. By contrast, here the VNF or container identifies the packet destined thereto using VLAN.

If customers deploy VMs in hypervisors connected via Single Root Input/Output Virtualization (SRIOV), there is no way to switch VLANs, where the multiple VLANs traverse the same physical link. In order to provide the capability to offer L2 service chaining, these techniques enable tagging VLANs in the input chain and subsequent hops of network services that are in L2 mode (“bump in the wire”).

Figure 1 below illustrates an overview of an example system configured to implement the solution described herein.

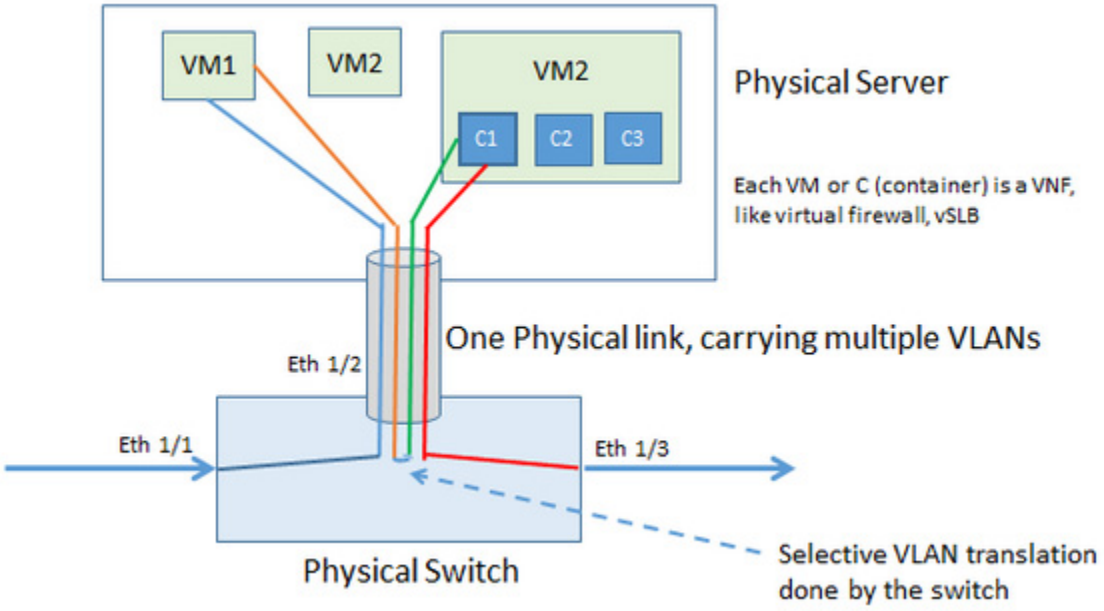

Figure 1

In summary, methods are described to perform service chaining on a physical switch for virtual services. First, the switch observes and classifies LAN traffic and determines that it needs to apply a service chaining rule based on classification results. Second, the switch forwards the traffic to the first VLAN in the input chain. When the frame is processed by the container/VM, it forwards the traffic on the egress VLAN, which is used as an input to the next element in the chain.