ECE792-038 Homework Assignment #3
Virtualization Datapath, IPTABLES, Namespaces
Due Wednesday, October 31, 2018

Problem 1. ***(20 Points)***

Libvirt+python: Admin Dnana Hgnis is notorious for being forgetful; he made a mistake while configuring the hypervisor on a VM. The mistake involved duplicate mac and IP addresses. Write an application to do the following:

1. List all MAC addresses and IP addresses of the running VMs.
2. Resolve all IP and MAC conflicts.
3. Extend your application (summit it as application 2) to work for multiple hypervisors. You give the list of hypervisors as the input to your application and you should find the duplicate MAC and IP addresses of all running VMs.

Problem 2. ***(20 Points)***

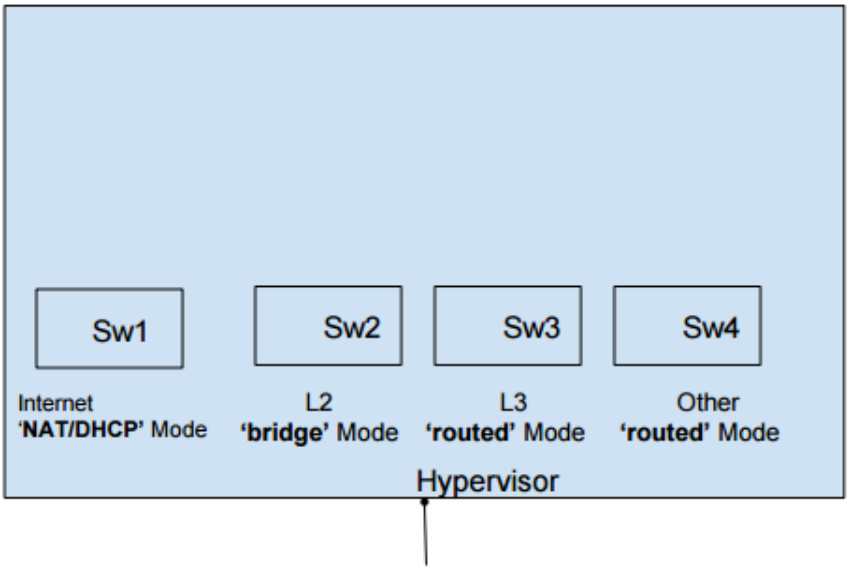

Figure 1: OVS network infrastructure

Ansible: Create ansible playbooks to do the following.

1. Playbook to create ovs network infra structure as shown in Figure 1.
2. Playbook to define network as internet (NAT/DHCP), l2 (bridge), l3 (routed), other (routed).
3. Playbook to create 2 VMs with 2 interfaces, 2 vcpu, 2 GB RAM, 12 GB disk space, and two applications, namely wireshark and iperf. VM1 should be connected to Internet and L2 Network. VM2 should be connected to Internet and L2 Network.
4. (BONUS) Playbook to create VMs where user gives topology as list. For example:

```
VM number    - List of interfaces
1          - {Internet, L2, L3}
2          - {Internet}
3          - {L2, L3}
```

Problem 3. ***(15 Points)*** **L2 Mode.**

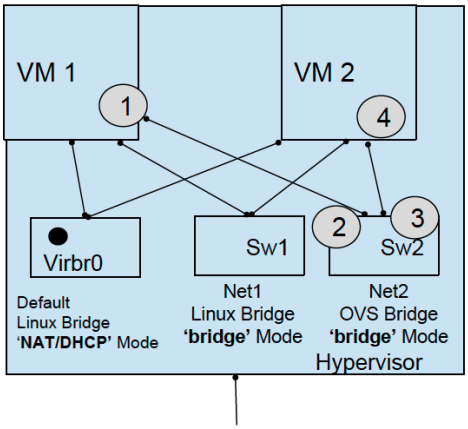

Figure 2: Data path shown as series of interfaces for Inter VM communication at L2 in the same host

Consider a system in which each hypervisor host has VMs from multiple tenants; each tenant has VMs in multiple hypervisor hosts. The tenant wants all his/her VMs to communicate over an L2 network - see Figure 2 and Figure 3. Two designs have been proposed:

- Design 1: All VMs from all tenants are connected to same bridge (in bridge mode).
- Design 2: Each tenant has its own bridge (in bridge mode).

Design an experiment to answer the following questions. Make reasonable assumptions, List down system limitation, if any; you need to collaborate with another team for experiments with multiple hypervisor hosts.

1. Design 1:
   (a) What are the disadvantages for tenants? Is a tenant's traffic isolated from other tenants?
   (b) What, if anything, breaks if two tenants in the same hypervisor host use the same IP address?

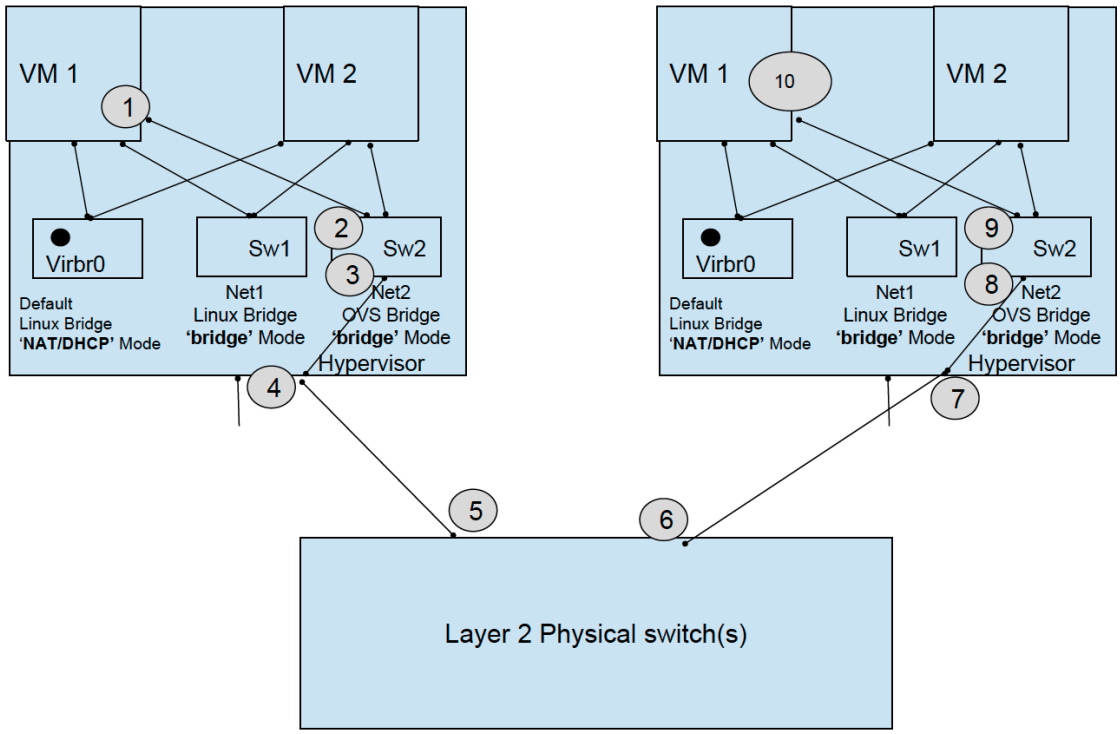

Figure 3: Data path shown as series of interfaces for Inter VM communication at L2 in different host

(c) What, if anything, breaks if two tenants in a different hypervisor host use the same IP address?

(d) What, if anything, breaks if two tenants in the same hypervisor host use the same MAC address?

(e) What, if anything, breaks if two tenants in a different hypervisor host use the same MAC address?

(f) What about a VLAN based solution? Will it work to provide isolation? What are the limitations of this solution? No need to perform experiments for this question.

2. Design 2:

(a) What are the disadvantages for the provider? Which resource in the hypervisor hosts will be a bottleneck?

(b) What, if anything, breaks if two tenants in the same hypervisor host use the same IP address?

(c) What, if anything, breaks if two tenants in a different hypervisor host use the same IP address?

(d) What, if anything, breaks if two tenants in the same hypervisor host use the same MAC address?

(e) What, if anything, breaks if two tenants in a different hypervisor host use the same MAC address?

(f) Do we need VLANs in the hypervisor bridge or do VLANs in Physical L2 network suffice? No need to perform experiments for this question.

3. Design 1 vs. Design 2:

(a) Admin Hat: List trade-offs with Design 1 and Design 2.

(b) Provider hat (hypervisor host's configuration point of view): List trade-offs with Design 1 and Design 2.

Problem 4. ***(15 Points)*** **L3 Mode** Consider a system in which each hypervisor host has VMs from

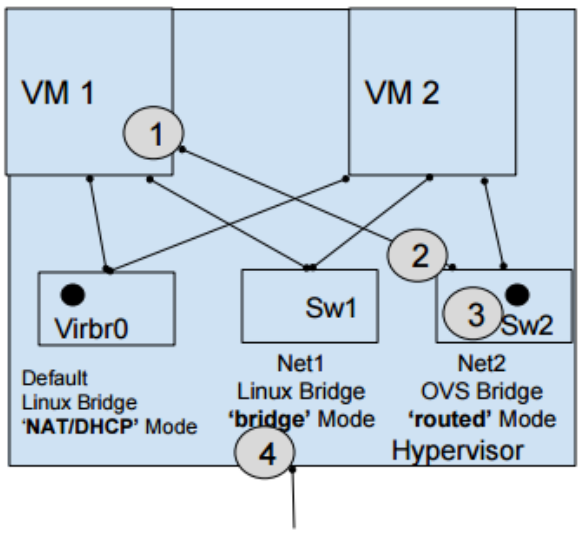

Figure 4: Data path shown as series of interfaces for VM communicated to internet using hypervisor Host as a router

multiple tenants; each tenant has VMs in multiple hypervisor hosts. The tenant wants all his/her VMs to communicate over an L3 network - see Figure 4. Two designs have been proposed:

- Design 1: All VMs in the hypervisor are connected to the same bridge (in routed mode).

- Design 2: Each tenant in the hypervisor has its own bridge (in routed mode).
- Design 3: Each VM in the hypervisor has its own bridge (in routed mode).

Design an experiment to answer the following questions.

1. Design 1:
   (a) What are the disadvantages for tenants? Is a tenant's traffic isolated from other tenants?
   (b) What, if anything, breaks if two tenants in the same hypervisor host use the same IP address?
   (c) What, if anything, breaks if two tenants in a different hypervisor host use the same IP address?
   (d) What, if anything, breaks if two tenants in the same hypervisor host use the same MAC address?
   (e) What, if anything, breaks if two tenants in a different hypervisor host use the same MAC address?
   (f) What about a VLAN based solution for providing L3 connectivity to each VM? Will it work? What are the limitations of this solution?
2. Design 2:
   (a) What are the disadvantages for the provider? Which resource in the hypervisor hosts will be a bottleneck?
   (b) What, if anything, breaks if two tenants in the same hypervisor host use the same IP address?
   (c) What, if anything, breaks if two tenants in a different hypervisor host use the same IP address?
   (d) What, if anything, breaks if two tenants in the same hypervisor host use the same MAC address?
   (e) What, if anything, breaks if two tenants in a different hypervisor host use the same MAC address?
   (f) Does a VLAN based solution in this design overcome any limitations of the VLAN based solution used in design 1?
3. Design 1 vs. Design 2:
   (a) Admin Hat: List trade-offs with Design 1, Design 2, and Design 3.
   (b) Provider hat (hypervisor host's configuration point of view): List trade-offs with Design 1, Design 2, and Design 2.
   (c) What are the missing pieces to have complete network isolation (IP, MAC, L2/L3 FT) between tenants in the hypervisor network?

Problem 5. ***(35 Points)***

IPTable, NAT/PAT: Consider the scenario shown in Figure 5. The customer has a client and two server applications in respective VMs. The client is in a public network while the servers are inside a private one. The hosts in the private network can not access hosts in any public network without the **NAT operation at RouterVM** (it's a restriction imposed by the admin).

Do the following tasks:

1. Set the topology as given in Figure 5. List IP/subnet plan for each L3 interfaces and provide Forwarding Tablel output for each VM.
2. Configure the NAT setting on RouterVM so that servers can ping the client. Verify via appropriate wireshark captures.

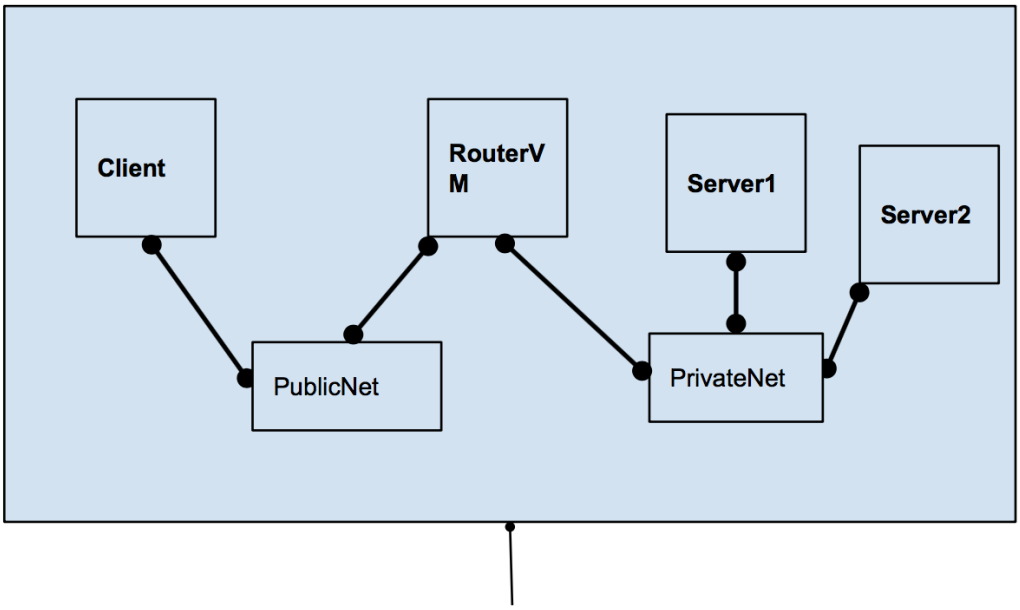

Figure 5: A NAT Problem.

3. Configure the NAT/PAT proxy setting so that the client can ssh to Server 1 and Server 2. Verify via appropriate wireshark captures. (Hint: Client has the knowledge of the public IP of RouterVM only. So it will use the public IP of RouterVM to SSH into servers.)
4. Use RouterVM to do NAT-based server load balancing for the traffic coming from the client to the two servers.
   (a) Define load precisely.
   (b) Configure the balancing knob at the RouterVM.
   (c) Verify that the load balancing mechanism is working.

Problem 6. ***(35 Points)***

Namespaces: Consider the topology shown in Figure 6. We have two tenants in the server, Red and Blue. Each tenant has two subnets, allocated to VM1 and VM2 respectively. Within a tenant, we need L2 isolation of the two subnets. Moreover, we need both L2 as well as L3 isolation among the tenants. To get this complete isolation of address spaces, each tenant has their own network namespaces (labeled NS1 and NS2 in the figure). L3 isolation means that both tenant can have same IP subnets for their VMs and still be able to reach outside network (a host like google.com). Provider network figure is a flexible box (can have one or more interfaces/devices), make necessory configuration for the Provider network block.

Use appropriate wireshark captures (you have to take multiple in some cases) and the forwarding table snapshots to answer the following questions:

1. Demonstrate the L2 isolation between two subnets of the same tenant. (Hint: Broadcast should be restricted and VMs can have same MAC addresses)
2. Demonstrate the L3 isolation between two tenants.

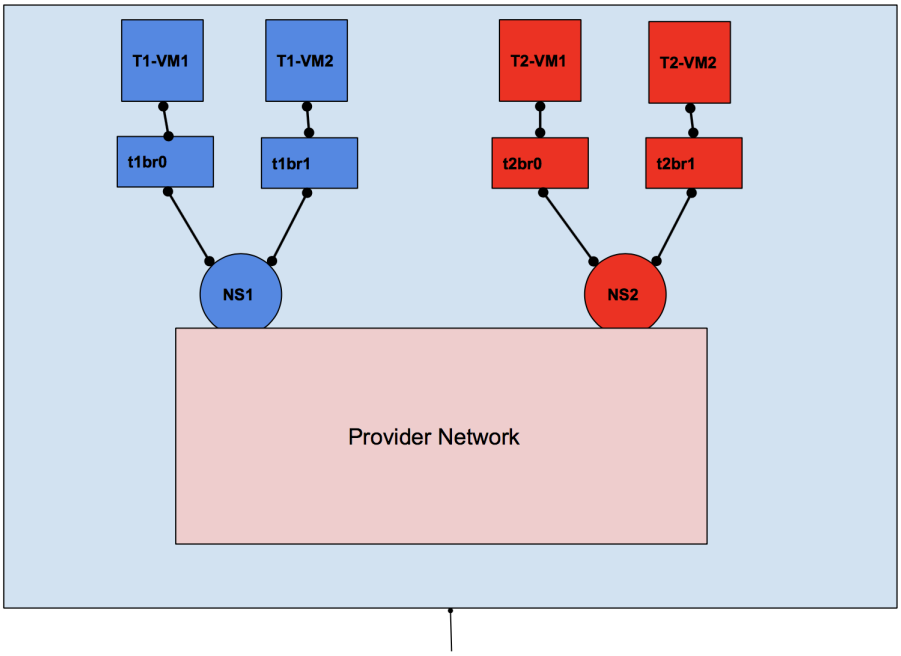

Figure 6: Network Namespace Problem

- VMs of tenant 1 should not be able to ping to tenant 2 VMs whether they have same or different IP subnets.
- In another experiment, both tenants use one subnet that is common (e.g., 10.0.0.0/8) and one that is different. The hosts in the common subnet for tenant red and tenant blue should be able to ping the internet.

3. *Forwarding table and IP tables in Host hypervisor.* In this experiment, make sure not to use the hypervisor host's default forwarding table/IP tables. Configure a new network namespaces (call it provider_ns) in the hypervisor. Implement and verify the following policies in the provider network namespace.

   (a) Internet policy. Allow ICMP traffic for both tenants. Allow SSH traffic for only the blue tenant.

   (b) Local L3 policy. Allow red tenant and blue tenant to ssh each other's VM, provided the subnets are different.