Question(1)

Please refer to Readme1_question1

Question(2)

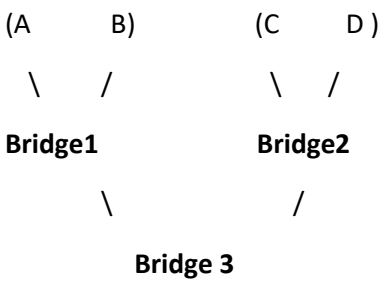
Please refer to Readme_question2

Question (3):

Design 1:

Assuming Virtual Machines A and B are in **Hypervisor1** & C and D are in other **Hypervisor2** Host

The topology looks like below



(a) The tenant traffic is not isolated as it is connected to a L2 bridge (broadcast to all of its interfaces) . The other tenants will also receive each other traffic as all are in same L2 domain.

(b) If two tenants A and B in the same hypervisor has the same IP address they wont be able to ping each other as ping to the same addresss would route to the local host interfaceand packet never goes out of VM.

A ---B communication fails (Which has the same Ip address)

Assume C pinging A the packet instead might reach B because both A and B has the same Ip address C might get mac address of B (Through arp request and reply) instead of A mac address C might send the packet to B instead of A .
So even the communication between C ----A or C----B might fail and the data path might not be as intended.
The only successful communication possible is between C and D

(c) Assuming A and C in the different Hypervisor has the same IP address
Assuming the Mac table entries are not populated in the VM.

B wants to ping A so the arp request will reach to both A and C and D. A and C replies back as arp request as they have same IP and it might happen that A arp entry in B might get replaced by C Mac address .So the packet From B will reach C which is intended to reach A

So the B---A data path might break similarly D ---C data path might break in the above manner . B---D data path will be successful (The ones that don't have the same IP)

A ----C communication won't happen at all as they have the same adress so it will result in the pinging the local host.

(d) if two tenants in the same hypervisor host use the same MAC address

Suppose A and B in the same Hypervisor has the same IP address
A wants to ping B ,the arp request for B's mac address will reach the L1 bridge and B replies back to the Arp request with an Mac address and also the destination mac address is also on the same interface, As switch wont forward back to the same interface the packet gets dropped.

So the communication A----B breaks(The VMs having the same Mac address).

Suppose C wants to communicate to A and pings A then the arp request will reach A and A will reply back to C and the **bridge1** has Mac entry for A .If incase D pings B and B respond back to the D request then the Mac entry in the switch will get replaced by B mac entry as it has replied back to D, as A and B has the same Mac address, Now C----A communication will break as the packet will get forwarded to B instead of A as the Mac table entry in switch got replaced by B mac address. B doesnt reply back to C as its IP is different from the A's IP and the packet will get dropped.

So C---- A or A---C or B ----D or D---B data path breaks.
Only C and D communication succeeds in this case (The ones that doesn't have the same Mac address and rest of the possibilities will break)

(e) if two tenants in a different hypervisor host use the same MAC address:

Suppose if A and C in the above topology have same MAC address **Mac_common**

If A Pings C, Bridge 3 will have a Mac entry for "Mac_common " with the interface connected with Bridge1 and when C replies back to the arp request of A the Mac entry for "Mac_common" will get replaced with interface connected with the bridge 2 and destination address of the packet is also on to the same interface as they have the same Mac so the switch will not forward packet on to the interface whose output is on to the input interface and so packet get dropped at bridge and so the data path between A and C fails.

A ---C communication fails (The ones having the same Mac)

If B wants to ping A the arp request will reach all of the virtual machines as A and C has the same mac address the Mac entry in the switch for “Mac_common ” entry might get replaced by the interface connected to C instead of interface connected to A and so the bridge 1 will forward the packet to C instead of A .As C IP address is different from A the packet will be dropped.

Similarly if B wants to C the packet might reach C as they have the same mac address and the packet will get dropped as C IP address is different from the A address

B ---A or B ---C or D---A or D ---C communication or data path breaks
B and D communication succeeds (The ones having the different Mac address) .

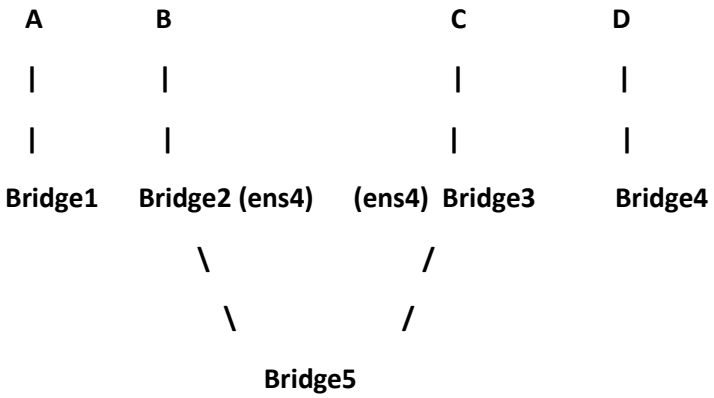
(f) VLAN based solution:

As VLAN will limit the broadcast domain so VLAN will act to provide isolation. This however becomes difficult for the admin to configure VLAN’s which may prove to be a drawback

DESIGN2:

Topology

A and B are in Hypervisor 1 and C and D are in Hypervisor 2



Bridge 1 is not connected to any interface .

Bridge 4 is not connected to any interface .

(a)

The disadvantages of this approach is Only B and C communicate and rest of communications breaks

The bottleneck will be the interfaces i,e the interfaces needed to connect between the local bridges and the bridge between the hypervisors

(b) **If two tenants in the same hypervisor host use the same IP address**

Assuming A and B has the same IP address in the hypervisor

As A and B communication breaks as there is interconnection between the **Bridge 1** and **Bridge 2**

B and C communication happens successfully via **bridge 5**

A and C communication doesn't happen as there isn't any data path between Bridge 1 and Bridge 3

(c) **if two tenants in a different hypervisor host use the same IP address**

Case1: If A and C has the same Ip address

Then the B ---C data path doesn't break as there is connectivity via Bridge2 ---Bridge 5----Bridge 3

A --- B and A---C data path breaks as there is no interconnectivity between the bridges

Bridge 1 and Bridge2 for (A ---B) and Bridge 1 and Bridge 3 for (A---C)

Case 2: If **B and C have the same Ip address :**

Then even the B ---C data path fails when B tries pinging C, as B Ip address is same as the C the packet doesn't reach out of B

A---C and A---B data path breaks as there is no connectivity between the bridges

(d) **if two tenants in the same hypervisor host use the same MAC address**

Suppose A and B has the same Mac address

B and C communication succeeds as these have different Mac address and different Ip address

So the communication happens via (B----Bridge2 ---Bridge 5----Bridge 3 ----C)

A and B communication fails as there is no connection between Bridge 1 and Bridge 2 so the data path breaks .Similarly A and C communication breaks as there is no inter connectivity **between Bridge 1 and Bridge 3**

(e) **if two tenants in a different hypervisor host use the same MAC address**

Case 1: If A and C has the same mac address:

This case the ping(data path doesn't break) between B and C as both have different Mac and and Ip

A---C and A---B communication breaks as there is no data path connection between the bridges1 and Bridge 2 and Bridge1 and Bridge 3

Case2: If B and C have the same mac Adress (Mac_common):

If B wants to ping C, B sends a arp request to bridge 5 and bridge will have an entry for (Mac_common) on the B side ones C replies back for the arp request the Mac entry for **Mac_common** will get updated to link on C side as the output port points out to the same port arrived the packet gets dropped so the data path breaks between B and C.

A—B and A—C data path breaks as there is no route between Bridge 1 and Bridge 2 and (bridge 1 and bridge 3)

(f).NO VLan isolation is needed as the tenant traffic is already isolated by having separate bridge for each tenant.

1. **Design 1 vs. Design 2:**

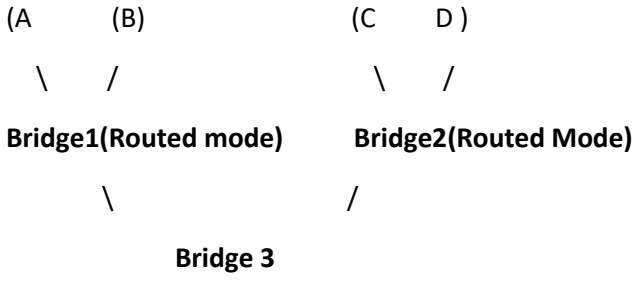
   Admin hat

   a) Design 1: Traffic Isolation is not provided. Since, VLAN's are used, it might be a problem for the admin to create and maintaining the VLAN's .
   b) Design 2: Isolation is provided. But number of ports will increase as the number of bridges increases, which may prove to be a problem to keep track of and configure.

Provider Hat

a) Design 1: As VLAN's are to be used, provider has to enable features of VLAN in order to provide isolation, because, this design does not isolate tenant's traffic from each other.
b) Design 2: Isolation is provided. So, additional feature of VLAN need not be provided by the provider hat as the tenant's traffic is automatically isolated.

Question (4):



Design 1: All VMs in the hypervisor are connected to the same bridge

Is a tenant's traffic isolated from other tenants?

The tenant's traffic will not be isolated as the tenant networks are on the same bridge(routed) mode and there will be routing established between the tenant's. Each tenant will be associated with a particular subnet

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

If A and B in the hypervisor has the same Ip address the A and B communication breaks

As A will self ping itself and packet won't reach out of A so the data path Breaks

A and C communication happens properly and via

A ---Bridge1 ----Bridge 3 ----Bridge 2 ----C

(c).If two tenants in a different hypervisor host use the same IP addres

If A and C has the same Ip address across different Hypervisors

Then A and B communication happens properly via data path

A---Bridge 1 -----B

A ---- C communication fails as A and C have the same Ip the packet will not Leave A(the ping packet will reach A via loopback)

(d). if two tenants in the same hypervisor host use the same MAC address

If and A and B have the same Mac address(Mac_common) in the same hypervisor

A wants to ping B, the arp request for B's mac address will reach the L1 bridge and B replies back to the Arp request with an Mac address and also the destination mac address is also on the same interface, As switch wont forward back to the same interface the packet gets dropped.

A ----C communication happens properly via data path

A --- bridge1 interface ---ens4(Hyp1) ----bridge 3 –(ens4)(Hyp2)----bridge 2 L3 interface---C

(e). **If two tenants in a different hypervisor host use the same MAC address.**

Suppose A and C have the same MAC address across the hypervisor

A –B communication happens properly as there are no conflicts between them via data path

First A send the packets to the default gateway A and gateway will forward it to the B(Based on the forwarding table in host which has the route to B)

A ----bridge 1 (L3 interface) ----B

A ---C communication also happens with out any issue

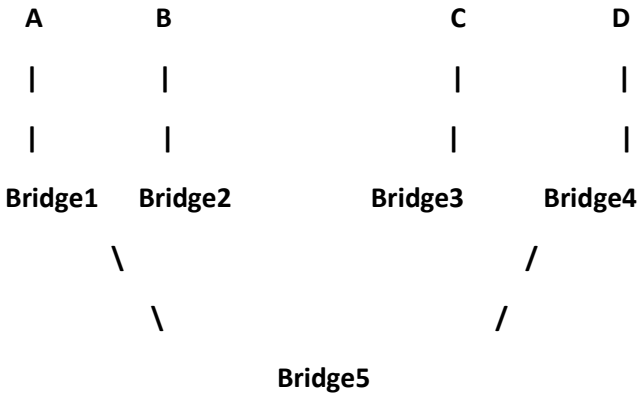
A ---Bridge1(L3 interface) ---- ens4 --bridge 3 –-----ens4 -----bridge 2 (L3 interface)----C

(f). Yes VLANs will provide the isolation .

DESIGN2:

Topology

A and B are in Hypervisor 1 and C and D are in Hypervisor 2



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

The disadvantage for the provider is that each tenant in the hypervisor should have their own bridgeThe no of bridges increases when tenants increases. So, memory overhead occurs, as each bridge connected to the tenant will have its own forwarding table. So, the number of interfaces via which the bridge connects to the hypervisor becomes the bottleneck.

(b). if two tenants in the same hypervisor host use the same IP address

If A and B have the same Ip address in the Hypervisor

If A wants to pings B A will ping itself and packet wont leave out of A and the data path breaks

A----B communication fails

Assume C pinging A the packet instead might reach B because both A and B has the same Ip address C.

Ones The packet reaches the ens 4 of Hypervisor 1it will send an arp saying who has the IP it might get switched between B and A .

So the data path between C and A breaks.

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

If A and C in the different hypervisor has the same Ip address

If packet A wants to ping C the packet wont reach out of Packet A it wil self ping itself

So the A----C communication breaks.

Suppose if B wants to ping A or C there will be two entries in the routing tables

So it depends upon the routing table.

A----D communication succeeds

B ---D communications happens without any problem as they don't have any conflicts

(d). **Two tenants in the same hypervisor host use the same MAC address.**

If A and B in the same hypervisor has the same mac address

A ---B communication happens as A send the packet to L3 interface of the bridge and L3 interface will intiate the arp and B replies back to the L3 interface and so the data path succeeds

If A ---C wants to communicate with each other and data path succeeds

B----C communication succeeds

Similarly A---D and B---D communication suceeds

The data path is

A ----L3 inetrface(bridge 1) ----ens4 ----bridge3 ----ens4 ---L3 ineterface (bridge 2) ----C

Every tenant to communication succeeds and nothing breaks here

(e) **Two tenants in the different hypervisor host use the same MAC address**

If A and C in the different hypervisor has the same mac address

Then A----B data path doesn't break

Data path for A----B is A ----(L3 interface of Bridge 1) -----B

Even the A----C communication succeeds

The data path for the A----C communication is

A ----L3 inetrface(bridge 1) ----ens4 ----bridge3 ----ens4 ---L3 ineterface (bridge 2) ----C

Every tenant to communication succeeds and nothing breaks here

(f). As there is already isolation provided by the individual bridges to each tenant There is no limitation for the VLAN

Design 1 vs Design 2

Admin Hat:

Design 1: Easier for the Management;

Design2: Difficult for the management

Design 3: Management will be complex because there are multiple bridges.

Provider Hat:

Design 1: Every packet has to go through single bridge

Design 2: There is requirement for multiple Forwarding Tables to be created. So, this will lead to resource bottleneck.

Design 3: Multiple Bridges will be created leading to resource bottle neck

Question 5:

Part (a):

The VMS used for connection are

Client VM ----- Client (VM) in our topology

Router VM ----- VM3(In our topology)

Server VMS ------ ppacha_VM1 (server 1) pppacha_VM2 (server 2)

The private network side of the Router VM is on the 10.1.1.0/24(ens10) subnet

The public network side of the Router VM is on 50.0.0.0/24 (ens3) subnet

Here are the Ip addresses configured for the VMs

```
 29    ppacha_VM1                     running
 30    ppacha_VM2                     running
 32    VM3                            running
 33    client                         running

ece792@ece792-Standard-PC-i440FX-PIIX-1996:~$ virsh domifaddr 29
 Name       MAC address          Protocol     Address
-------------------------------------------------------------------------------
 vnet5      52:54:00:55:73:7e    ipv4         192.168.130.120/24

ece792@ece792-Standard-PC-i440FX-PIIX-1996:~$ virsh domifaddr 30
 Name       MAC address          Protocol     Address
-------------------------------------------------------------------------------
 vnet17     52:54:00:aa:1c:07    ipv4         192.168.130.188/24

ece792@ece792-Standard-PC-i440FX-PIIX-1996:~$ virsh domifaddr 32
 Name       MAC address          Protocol     Address
-------------------------------------------------------------------------------
 vnet13     52:54:00:1c:45:16    ipv4         50.0.0.110/24

ece792@ece792-Standard-PC-i440FX-PIIX-1996:~$ virsh domifaddr 33
 Name       MAC address          Protocol     Address
-------------------------------------------------------------------------------
 vnet16     52:54:00:d6:4a:98    ipv4         50.0.0.72/24
```

Forwarding table output of Each VMS:

Ppacha_VM1(server 1): [ip adresses & forwarding table output]

```
[root@200208720VM1 ~]# ip route delete 0.0.0.0/0 via 192.168.130.1
[root@200208720VM1 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.1.1.3        0.0.0.0         UG    0      0        0 ens9
10.1.1.0        0.0.0.0         255.255.255.0   U     0      0        0 ens9
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.130.0   0.0.0.0         255.255.255.0   U     100    0        0 eth0
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
[root@200208720VM1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:aa:1c:07 brd ff:ff:ff:ff:ff:ff
    inet 192.168.130.188/24 brd 192.168.130.255 scope global noprefixroute dynamic eth0
       valid_lft 2378sec preferred_lft 2378sec
    inet6 fe80::a079:ffeb:6e7c:6afd/64 scope link tentative dadfailed
       valid_lft forever preferred_lft forever
    inet6 fe80::8b25:60f1:fcae:1bd8/64 scope link tentative dadfailed
       valid_lft forever preferred_lft forever
    inet6 fe80::65f1:fcaf:fa34:7d44/64 scope link tentative dadfailed
       valid_lft forever preferred_lft forever
7: ens9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:05:f2:2a brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.1/24 scope global ens9
       valid_lft forever preferred_lft forever
[root@200208720VM1 ~]#
```

Ppacha_VM2(server 2) : [Ip address & forwarding table output]

```
[root@200208720VM1 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.1.1.3        0.0.0.0         UG    0      0        0 ens9
10.1.1.0        0.0.0.0         255.255.255.0   U     0      0        0 ens9
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.130.0   0.0.0.0         255.255.255.0   U     100    0        0 eth0
[root@200208720VM1 ~]#
[root@200208720VM1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:55:73:7e brd ff:ff:ff:ff:ff:ff
    inet 192.168.130.120/24 brd 192.168.130.255 scope global noprefixroute dynamic eth0
       valid_lft 3088sec preferred_lft 3088sec
    inet6 fe80::a079:ffeb:6e7c:6afd/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::8b25:60f1:fcae:1bd8/64 scope link tentative noprefixroute dadfailed
       valid_lft forever preferred_lft forever
    inet6 fe80::65f1:fcaf:fa34:7d44/64 scope link tentative noprefixroute dadfailed
       valid_lft forever preferred_lft forever
7: ens9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:af:aa:96 brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.2/24 scope global ens9
       valid_lft forever preferred_lft forever
[root@200208720VM1 ~]#
```

Router (VM3 in our topology)

Ip addresses and forwarding table:

```
    link/ether 52:54:00:52:e0:e6 brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.3/24 scope global ens10
       valid_lft forever preferred_lft forever
[root@50-0-0-110 ~]# route -n
-bash: route: command not found
[root@50-0-0-110 ~]# ip route
default via 50.0.0.1 dev ens3 proto dhcp metric 100
10.1.1.0/24 dev ens10 proto kernel scope link src 10.1.1.3
50.0.0.0/24 dev ens3 proto kernel scope link src 50.0.0.110 metric 100
[root@50-0-0-110 ~]# iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE
[root@50-0-0-110 ~]#
[root@50-0-0-110 ~]#
[root@50-0-0-110 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:1c:45:16 brd ff:ff:ff:ff:ff:ff
    inet 50.0.0.110/24 brd 50.0.0.255 scope global noprefixroute dynamic ens3
       valid_lft 2954sec preferred_lft 2954sec
    inet6 fe80::a3c4:7e08:285a:917c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: ens10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:52:e0:e6 brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.3/24 scope global ens10
       valid_lft forever preferred_lft forever
[root@50-0-0-110 ~]# ip route
default via 50.0.0.1 dev ens3 proto dhcp metric 100
10.1.1.0/24 dev ens10 proto kernel scope link src 10.1.1.3
50.0.0.0/24 dev ens3 proto kernel scope link src 50.0.0.110 metric 100
[root@50-0-0-110 ~]#
```

Client(Client in our topology)

IP addresses of interfaces and forwarding table

```
There was 1 failed login attempt since the last successful login.
Last login: Wed Oct 24 15:13:48 2018 from 50-0-0-1.static.sonic.net
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
[root@200208720VM1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:d6:4a:98 brd ff:ff:ff:ff:ff:ff
    inet 50.0.0.72/24 brd 50.0.0.255 scope global noprefixroute dynamic ens3
       valid_lft 2857sec preferred_lft 2857sec
    inet6 fe80::7093:71c8:488c:a78a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@200208720VM1 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         50.0.0.1        0.0.0.0         UG    100    0        0 ens3
50.0.0.0        0.0.0.0         255.255.255.0   U     100    0        0 ens3
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
```

Part(b): **Configuring the NAT setting on RouterVM so that servers can ping the client**.

Server IP address (ens9 Interface): 10.1.1.2

Client IP address: 50.0.0.72

==========Router interfaces==========

Ens10 IP address (interface in private network): 10.1.1.3

Ens3 Ip address (Interface in the public network): 50.0.0.110

The router VM Ip tables are configured such that whenever the servers ping the client the source IP address of the packets traversing from servers are replaced by IP address of router interface so that the private IP of the servers won't get exposed to the client.

The Nat rules are applied after the POSTROUTING :

Using the command

`iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE  <<<< IP table rule`

```
4411  371K POSTROUTING_ZONES  all  --  any    any     anywhere             anywhere
1038 95568 MASQUERADE  all  --  any    ens3    anywhere             anywhere
root@50-0-0-110 ~]# iptables -t nat -vnL POSTROUTING
hain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination
4411  371K POSTROUTING_direct  all  --  *      *       0.0.0.0/0            0.0.0.0/0
4411  371K POSTROUTING_ZONES_SOURCE  all  --  *      *       0.0.0.0/0            0.0.0.0/0
4411  371K POSTROUTING_ZONES  all  --  *      *       0.0.0.0/0            0.0.0.0/0
1038 95568 MASQUERADE  all  --  *      ens3    0.0.0.0/0            0.0.0.0/0
root@50-0-0-110 ~]#
```

The Iptables rule at the Router side

After doing the NAT operation and configuring the default gateway as **50.0.0.1** The server is able to ping the client successfully

Performing the “Ping **50.0.0.72** “from server **10.1.1.2**

Here are the Packet captures at the Client side :

```
[root@200208720VM1 ~]# tcpdump -i any icmp -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
15:58:40.399817 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 44, length 64
15:58:40.399902 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 44, length 64
15:58:41.402602 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 45, length 64
15:58:41.402672 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 45, length 64
15:58:42.404712 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 46, length 64
15:58:42.404784 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 46, length 64
15:58:43.407335 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 47, length 64
15:58:43.407424 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 47, length 64
15:58:44.408668 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 48, length 64
15:58:44.408743 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 48, length 64
15:58:45.410056 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 49, length 64
15:58:45.410130 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 49, length 64
15:58:46.417024 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 50, length 64
15:58:46.417091 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 50, length 64
15:58:47.417365 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 51, length 64
15:58:47.417444 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 51, length 64
15:58:48.421733 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 52, length 64
15:58:48.421800 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 52, length 64
15:58:49.423441 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 53, length 64
15:58:49.423524 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 53, length 64
15:58:50.425452 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 54, length 64
15:58:50.425540 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 54, length 64
15:58:51.428081 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 55, length 64
15:58:51.428155 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 55, length 64
15:58:52.437867 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 8649, seq 56, length 64
15:58:52.437940 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 8649, seq 56, length 64
^C
```

Packet capture on the Server Side:

```
64 bytes from 50.0.0.72: icmp_seq=53 ttl=63 time=9.69 ms
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
16:01:52.194311 IP 10.1.1.2 > 50.0.0.72: ICMP echo request, id 8650, seq 54, length 64
16:01:52.203906 IP 50.0.0.72 > 10.1.1.2: ICMP echo reply, id 8650, seq 54, length 64
64 bytes from 50.0.0.72: icmp_seq=54 ttl=63 time=9.64 ms
16:01:53.196827 IP 10.1.1.2 > 50.0.0.72: ICMP echo request, id 8650, seq 55, length 64
64 bytes from 50.0.0.72: icmp_seq=55 ttl=63 time=8.70 ms
16:01:53.205470 IP 50.0.0.72 > 10.1.1.2: ICMP echo reply, id 8650, seq 55, length 64
16:01:54.198729 IP 10.1.1.2 > 50.0.0.72: ICMP echo request, id 8650, seq 56, length 64
16:01:54.212597 IP 50.0.0.72 > 10.1.1.2: ICMP echo reply, id 8650, seq 56, length 64
64 bytes from 50.0.0.72: icmp_seq=56 ttl=63 time=14.1 ms
16:01:55.200263 IP 10.1.1.2 > 50.0.0.72: ICMP echo request, id 8650, seq 57, length 64
16:01:55.215364 IP 50.0.0.72 > 10.1.1.2: ICMP echo reply, id 8650, seq 57, length 64
64 bytes from 50.0.0.72: icmp_seq=57 ttl=63 time=15.1 ms
16:01:56.202028 IP 10.1.1.2 > 50.0.0.72: ICMP echo request, id 8650, seq 58, length 64
64 bytes from 50.0.0.72: icmp_seq=58 ttl=63 time=10.0 ms
16:01:56.212068 IP 50.0.0.72 > 10.1.1.2: ICMP echo reply, id 8650, seq 58, length 64
16:01:57.204278 IP 10.1.1.2 > 50.0.0.72: ICMP echo request, id 8650, seq 59, length 64
16:01:57.214628 IP 50.0.0.72 > 10.1.1.2: ICMP echo reply, id 8650, seq 59, length 64
64 bytes from 50.0.0.72: icmp_seq=59 ttl=63 time=10.3 ms
16:01:58.206810 IP 10.1.1.2 > 50.0.0.72: ICMP echo request, id 8650, seq 60, length 64
16:01:58.217763 IP 50.0.0.72 > 10.1.1.2: ICMP echo reply, id 8650, seq 60, length 64
64 bytes from 50.0.0.72: icmp_seq=60 ttl=63 time=11.0 ms
16:01:59.208944 IP 10.1.1.2 > 50.0.0.72: ICMP echo request, id 8650, seq 61, length 64
64 bytes from 50.0.0.72: icmp_seq=61 ttl=63 time=10.3 ms
16:01:59.219200 IP 50.0.0.72 > 10.1.1.2: ICMP echo reply, id 8650, seq 61, length 64
16:02:00.210727 IP 10.1.1.2 > 50.0.0.72: ICMP echo request, id 8650, seq 62, length 64
16:02:00.223427 IP 50.0.0.72 > 10.1.1.2: ICMP echo reply, id 8650, seq 62, length 64
64 bytes from 50.0.0.72: icmp_seq=62 ttl=63 time=12.7 ms
16:02:01.212873 IP 10.1.1.2 > 50.0.0.72: ICMP echo request, id 8650, seq 63, length 64
64 bytes from 50.0.0.72: icmp_seq=63 ttl=63 time=10.8 ms
16:02:01.223650 IP 50.0.0.72 > 10.1.1.2: ICMP echo reply, id 8650, seq 63, length 64
16:02:02.214920 IP 10.1.1.2 > 50.0.0.72: ICMP echo request, id 8650, seq 64, length 64
```

Packet Capture on the Router VM in public network (ens3) :

```
16 packets received by filter
0 packets dropped by kernel
[root@50-0-0-110 ~]# tcpdump -i ens3 icmp -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
16:37:22.435314 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 10328, seq 1, length 64
16:37:22.441529 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 10328, seq 1, length 64
16:37:23.436951 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 10328, seq 2, length 64
16:37:23.443065 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 10328, seq 2, length 64
16:37:24.439145 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 10328, seq 3, length 64
16:37:24.443734 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 10328, seq 3, length 64
16:37:25.440914 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 10328, seq 4, length 64
16:37:25.449762 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 10328, seq 4, length 64
16:37:26.442885 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 10328, seq 5, length 64
16:37:26.447601 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 10328, seq 5, length 64
16:37:27.443915 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 10328, seq 6, length 64
16:37:27.449048 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 10328, seq 6, length 64
16:37:28.447938 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 10328, seq 7, length 64
16:37:28.453392 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 10328, seq 7, length 64
16:37:29.450734 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 10328, seq 8, length 64
16:37:29.453985 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 10328, seq 8, length 64
16:37:30.454219 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 10328, seq 9, length 64
16:37:30.459613 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 10328, seq 9, length 64
16:37:31.453538 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 10328, seq 10, length 64
16:37:31.459168 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 10328, seq 10, length 64
16:37:32.455924 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 10328, seq 11, length 64
16:37:32.465282 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 10328, seq 11, length 64
16:37:33.458687 IP 50.0.0.110 > 50.0.0.72: ICMP echo request, id 10328, seq 12, length 64
16:37:33.469305 IP 50.0.0.72 > 50.0.0.110: ICMP echo reply, id 10328, seq 12, length 64
^C
24 packets captured
24 packets received by filter
```

Packet Capture on the Server2 in private network (ens10) :

```
[root@50-0-0-110 ~]# tcpdump -i ens10 icmp -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens10, link-type EN10MB (Ethernet), capture size 262144 bytes
16:38:14.803407 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 1, length 64
16:38:14.810725 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 1, length 64
16:38:15.804798 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 2, length 64
16:38:15.814099 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 2, length 64
16:38:16.806888 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 3, length 64
16:38:16.812260 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 3, length 64
16:38:17.809199 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 4, length 64
16:38:17.813720 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 4, length 64
16:38:18.811195 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 5, length 64
16:38:18.815666 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 5, length 64
16:38:19.813739 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 6, length 64
16:38:19.819868 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 6, length 64
16:38:20.816272 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 7, length 64
16:38:20.820263 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 7, length 64
16:38:21.817998 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 8, length 64
16:38:21.825424 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 8, length 64
16:38:22.820367 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 9, length 64
16:38:22.825976 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 9, length 64
16:38:23.824213 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 10, length 64
16:38:23.830501 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 10, length 64
16:38:24.829570 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 11, length 64
16:38:24.835720 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 11, length 64
16:38:25.833291 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 12, length 64
16:38:25.837264 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 12, length 64
16:38:26.835558 IP 10.1.1.1 > 50.0.0.72: ICMP echo request, id 10329, seq 13, length 64
16:38:26.839724 IP 50.0.0.72 > 10.1.1.1: ICMP echo reply, id 10329, seq 13, length 64
^C
26 packets captured
26 packets received by filter
0 packets dropped by kernel
[root@50-0-0-110 ~]#
```

Part (c):

Configure the NAT/PAT proxy setting so that the client can ssh to Server 1 and Server 2

Using different port numbers to SSH TO THE SERVERS :

Server1 IP address (ens9 Interface): **10.1.1.1**

Server 2 Ip address (ens9 interface): 10.1.1.2

Client IP address: **50.0.0.72**

==========Router interfaces==========

Ens10 IP address(interface in private network): **10.1.1.3 (default gateway for 10.1.1.1 and 10.1.1.2)**

Ens3 Ip address (Interface in the public network): **50.0.0.110**

50.0.0.110 – (Routers public side IP:)

Ssh 50.0.0.110 -p 2000 (to SSH to server 1)

Ssh 50.0.0.110 -p 3000 (to ssh to server 2)

IP TABLES AT THE router side are

```
[root@50-0-0-110 ~]# iptables -t nat -vnL PREROUTING
Chain PREROUTING (policy ACCEPT 13 packets, 940 bytes)
 pkts bytes target     prot opt in     out     source               destination
   19  1140 DNAT       tcp  --  ens3   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3000 to:10.1.1.2:22
    6   360 DNAT       tcp  --  ens3   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:2000 to:10.1.1.1:22
 7773 2193K PREROUTING_direct  all  --  *      *       0.0.0.0/0            0.0.0.0/0
 7773 2193K PREROUTING_ZONES_SOURCE  all  --  *      *       0.0.0.0/0            0.0.0.0/0
 7773 2193K PREROUTING_ZONES  all  --  *      *       0.0.0.0/0            0.0.0.0/0
[root@50-0-0-110 ~]# iptables -t nat -vnL POSTROUTING
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    4   240 MASQUERADE  all  --  *      ens10   0.0.0.0/0            0.0.0.0/0
 6372  547K POSTROUTING_direct  all  --  *      *       0.0.0.0/0            0.0.0.0/0
 6372  547K POSTROUTING_ZONES_SOURCE  all  --  *      *       0.0.0.0/0            0.0.0.0/0
 6372  547K POSTROUTING_ZONES  all  --  *      *       0.0.0.0/0            0.0.0.0/0
 2993  271K MASQUERADE  all  --  *      ens3    0.0.0.0/0            0.0.0.0/0
[root@50-0-0-110 ~]# iptables -vnL FORWARD
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  274 32545 ACCEPT     all  --  *      *       50.0.0.0/24          0.0.0.0/0
 1106  111K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
 1406  104K FORWARD_direct  all  --  *      *       0.0.0.0/0            0.0.0.0/0
 1406  104K FORWARD_IN_ZONES_SOURCE  all  --  *      *       0.0.0.0/0            0.0.0.0/0
 1406  104K FORWARD_IN_ZONES  all  --  *      *       0.0.0.0/0            0.0.0.0/0
 1386  102K FORWARD_OUT_ZONES_SOURCE  all  --  *      *       0.0.0.0/0            0.0.0.0/0
 1386  102K FORWARD_OUT_ZONES  all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate INVALID
 1386  102K REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
[root@50-0-0-110 ~]#
```

These three rules have been applied in the iptables :

iptables -t nat -I PREROUTING --dport 2000 -i ens3 -j DNAT --to 10.1.1.1:22

iptables -t nat -I PREROUTING --dport 3000 -i ens3 -j DNAT --to 10.1.1.1:22

iptables -t nat -I POSTROUTING -o ens10 -j MASQUERADE

iptables -I 1 FORWARD -s 50.0.0.0/24 -j ACCEPT

When we use the ssh 50.0.0.110 -p 2000

To SSH to server1 (10.1.1.1)

```
    inet6 fe80::7093:71c8:488c:a78a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@client ~]# cat /etc/hostname
client
[root@client ~]# ssh 50.0.0.110 -p 2000
root@50.0.0.110's password:
Last login: Sat Oct 27 13:42:51 2018 from gateway
[root@server1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:af:aa:96 brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.1/24 scope global ens9
       valid_lft forever preferred_lft forever
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:55:73:7e brd ff:ff:ff:ff:ff:ff
    inet 192.168.130.120/24 brd 192.168.130.255 scope global noprefixroute dynamic eth0
       valid_lft 3295sec preferred_lft 3295sec
    inet6 fe80::a079:ffeb:6e7c:6afd/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::8b25:60f1:fcae:1bd8/64 scope link tentative noprefixroute dadfailed
       valid_lft forever preferred_lft forever
    inet6 fe80::65f1:fcaf:fa34:7d44/64 scope link tentative noprefixroute dadfailed
       valid_lft forever preferred_lft forever
[root@server1 ~]# cat /etc/hostname
server1
[root@server1 ~]#
```

Packet capture at the Server1 side :

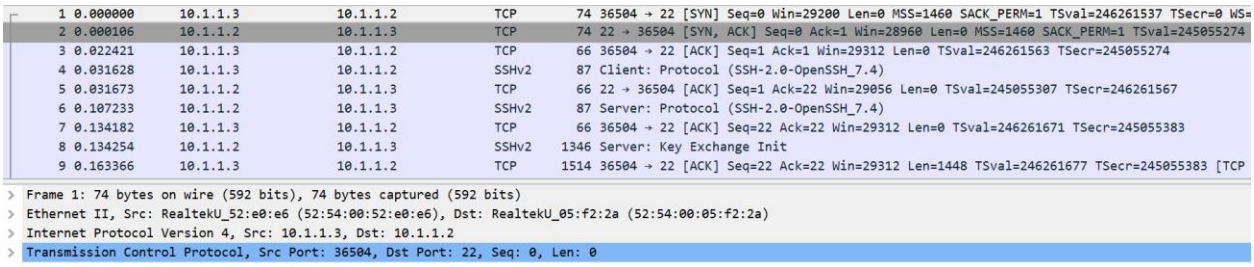
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.1.3	10.1.1.1	SSH	150	Client: Encrypted packet (len=84)
2	0.038056	10.1.1.1	10.1.1.3	TCP	66	22 → 49490 [ACK] Seq=1 Ack=85 Win=249 Len=0 TSval=244579291 TSecr=245340461
3	0.125324	10.1.1.1	10.1.1.3	SSH	94	Server: Encrypted packet (len=28)
4	0.137516	10.1.1.3	10.1.1.1	TCP	66	49490 → 22 [ACK] Seq=85 Ack=29 Win=271 Len=0 TSval=245340618 TSecr=244579378
5	0.147483	10.1.1.3	10.1.1.1	SSH	178	Client: Encrypted packet (len=112)
6	0.147509	10.1.1.1	10.1.1.3	TCP	66	22 → 49490 [ACK] Seq=29 Ack=197 Win=249 Len=0 TSval=244579400 TSecr=245340625
7	0.896163	10.1.1.1	10.1.1.3	SSH	566	Server: Encrypted packet (len=500)
8	0.944609	10.1.1.3	10.1.1.1	TCP	66	49490 → 22 [ACK] Seq=197 Ack=529 Win=291 Len=0 TSval=245341429 TSecr=244580149
9	0.944671	10.1.1.1	10.1.1.3	SSH	110	Server: Encrypted packet (len=44)

```
> Frame 1: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
> Ethernet II, Src: RealtekU_52:e0:e6 (52:54:00:52:e0:e6), Dst: RealtekU_af:aa:96 (52:54:00:af:aa:96)
> Internet Protocol Version 4, Src: 10.1.1.3, Dst: 10.1.1.1
> Transmission Control Protocol, Src Port: 49490, Dst Port: 22, Seq: 1, Ack: 1, Len: 84
> SSH Protocol
```

Doing SSH to ssh 50.0.0.72 -p 3000 should do ssh to 10.1.1.2:

```
Last login: Sat Oct 27 13:04:45 2018 from 50-0-0-1.static.sonic.net
[root@client ~]# ssh 50.0.0.110 -p 3000
The authenticity of host '[50.0.0.110]:3000 ([50.0.0.110]:3000)' can't be established.
ECDSA key fingerprint is SHA256:AZNcls2Huh2c9+xyV8tBquhdQb/kdq1501mexOcnowk.
ECDSA key fingerprint is MD5:10:2e:5c:21:57:28:a1:c2:22:43:c5:8d:8d:df:e2:93.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[50.0.0.110]:3000' (ECDSA) to the list of known hosts.
root@50.0.0.110's password:
Last login: Sat Oct 27 12:43:42 2018 from gateway
[root@server2 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:05:f2:2a brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.2/24 scope global ens9
       valid_lft forever preferred_lft forever
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:aa:1c:07 brd ff:ff:ff:ff:ff:ff
    inet 192.168.130.188/24 brd 192.168.130.255 scope global noprefixroute dynamic eth0
       valid_lft 3410sec preferred_lft 3410sec
    inet6 fe80::a079:ffeb:6e7c:6afd/64 scope link tentative dadfailed
       valid_lft forever preferred_lft forever
    inet6 fe80::8b25:60f1:fcae:1bd8/64 scope link tentative dadfailed
       valid_lft forever preferred_lft forever
    inet6 fe80::65f1:fcaf:fa34:7d44/64 scope link tentative dadfailed
       valid_lft forever preferred_lft forever
[root@server2 ~]# cat /etc/hostname
server2
[root@server2 ~]#
```

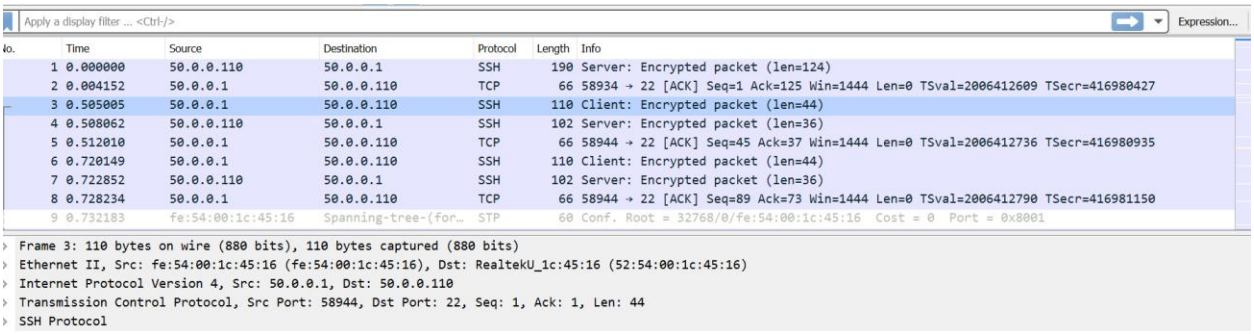
Packet capture at the server2 side :



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.1.3	10.1.1.2	TCP	74	36504 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=246261537 TSecr=0 WS=
2	0.000106	10.1.1.2	10.1.1.3	TCP	74	22 → 36504 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=245055274
3	0.022421	10.1.1.3	10.1.1.2	TCP	66	36504 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=246261563 TSecr=245055274
4	0.031628	10.1.1.3	10.1.1.2	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_7.4)
5	0.031673	10.1.1.2	10.1.1.3	TCP	66	22 → 36504 [ACK] Seq=1 Ack=22 Win=29056 Len=0 TSval=245055307 TSecr=246261567
6	0.107233	10.1.1.2	10.1.1.3	SSHv2	87	Server: Protocol (SSH-2.0-OpenSSH_7.4)
7	0.134182	10.1.1.3	10.1.1.2	TCP	66	36504 → 22 [ACK] Seq=22 Ack=22 Win=29312 Len=0 TSval=246261671 TSecr=245055383
8	0.134254	10.1.1.2	10.1.1.3	SSHv2	1346	Server: Key Exchange Init
9	0.163366	10.1.1.3	10.1.1.2	TCP	1514	36504 → 22 [ACK] Seq=22 Ack=22 Win=29312 Len=1448 TSval=246261677 TSecr=245055383 [TCP

```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: RealtekU_52:e0:e6 (52:54:00:52:e0:e6), Dst: RealtekU_05:f2:2a (52:54:00:05:f2:2a)
> Internet Protocol Version 4, Src: 10.1.1.3, Dst: 10.1.1.2
> Transmission Control Protocol, Src Port: 36504, Dst Port: 22, Seq: 0, Len: 0
```

Packet Capture at the router side :

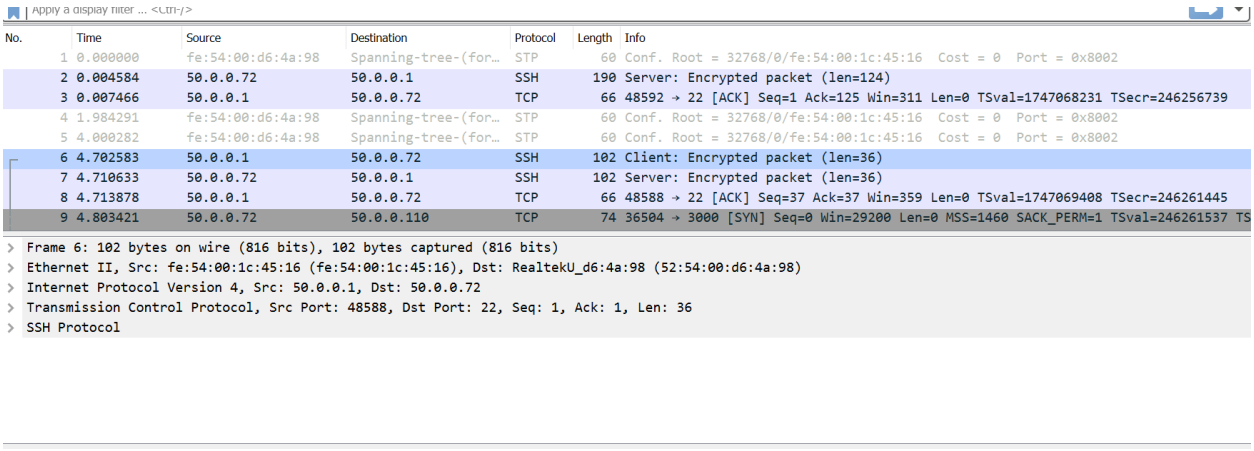


Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	50.0.0.110	50.0.0.1	SSH	190	Server: Encrypted packet (len=124)
2	0.004152	50.0.0.1	50.0.0.110	TCP	66	58934 → 22 [ACK] Seq=1 Ack=125 Win=1444 Len=0 TSval=2006412609 TSecr=416980427
3	0.505005	50.0.0.1	50.0.0.110	SSH	110	Client: Encrypted packet (len=44)
4	0.508062	50.0.0.110	50.0.0.1	SSH	102	Server: Encrypted packet (len=36)
5	0.512010	50.0.0.1	50.0.0.110	TCP	66	58944 → 22 [ACK] Seq=45 Ack=37 Win=1444 Len=0 TSval=2006412736 TSecr=416980935
6	0.720149	50.0.0.1	50.0.0.110	SSH	110	Client: Encrypted packet (len=44)
7	0.722852	50.0.0.110	50.0.0.1	SSH	102	Server: Encrypted packet (len=36)
8	0.728234	50.0.0.1	50.0.0.110	TCP	66	58944 → 22 [ACK] Seq=89 Ack=73 Win=1444 Len=0 TSval=2006412790 TSecr=416981150
9	0.732183	fe:54:00:1c:45:16	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/fe:54:00:1c:45:16 Cost = 0 Port = 0x8001

```
> Frame 3: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Ethernet II, Src: fe:54:00:1c:45:16 (fe:54:00:1c:45:16), Dst: RealtekU_1c:45:16 (52:54:00:1c:45:16)
> Internet Protocol Version 4, Src: 50.0.0.1, Dst: 50.0.0.110
> Transmission Control Protocol, Src Port: 58944, Dst Port: 22, Seq: 1, Ack: 1, Len: 44
> SSH Protocol
```

Packet capture at the client side :



Part (d):

Load defined:

Rsyslog Messages of the client to the Router which

/etc/rsylog.conf file

```
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
*.* @50.0.0.110

# ### end of the forwarding rule ###
```

Moving the syslog traffic to the Router VM (50.0.0.110)

(b) Load balancing at the Router Knob

As the rsyslog port is UDP port and transfer of data takes place on port number 514

Th following Ip table rules have been applied in the prerouting stage :

10.1.1.1 ----Server1 IP

10.1.1.2 ---- server2 IP

Rules applied for Load Balancing :

Rule 1:

iptables -t nat -D PREROUTING -p udp -s 50.0.0.0/24 --dport 514 -j DNAT --to-destination 10.1.1.1:514

Rule2:

iptables -t nat -D PREROUTING -p udp -s 50.0.0.0/24 --dport 514 -m state --state NEW -m statistic --mode nth --every 2 --packet 0 -j DNAT --to-destination 10.1.1.2:514

Ip tables on the Router VM:

```
[root@router ~]# iptables -t nat -vnL PREROUTING
Chain PREROUTING (policy ACCEPT 16 packets, 1184 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1   126 DNAT       udp  --  *      *       50.0.0.0/24          0.0.0.0/0           udp dpt:514 state NEW statistic mode nth every 2 to:10.1.1.2:51
4
    1   124 DNAT       udp  --  *      *       50.0.0.0/24          0.0.0.0/0           udp dpt:514 to:10.1.1.1:514
    0     0 DNAT       tcp  --  ens3   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3000 to:10.1.1.2:22
    0     0 DNAT       tcp  --  ens3   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:2000 to:10.1.1.1:22
   16  1184 PREROUTING_direct  all  --  *      *       0.0.0.0/0            0.0.0.0/0
   16  1184 PREROUTING_ZONES_SOURCE  all  --  *      *       0.0.0.0/0            0.0.0.0/0
   16  1184 PREROUTING_ZONES  all  --  *      *       0.0.0.0/0            0.0.0.0/0
[root@router ~]#
```

(c) Verification :

From the snapshot of Router Ip tables.

```
[root@router ~]# iptables -t nat -vnL PREROUTING
Chain PREROUTING (policy ACCEPT 537 packets, 45048 bytes)
 pkts bytes target     prot opt in     out     source               destination
   34  4016 DNAT       udp  --  *      *       50.0.0.0/24          0.0.0.0/0           udp dpt:514 state NEW statistic mode nth every 2 to:10.1.1.2:51
4
   34  4099 DNAT       udp  --  *      *       50.0.0.0/24          0.0.0.0/0           udp dpt:514 to:10.1.1.1:514
    0     0 DNAT       tcp  --  ens3   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3000 to:10.1.1.2:22
    0     0 DNAT       tcp  --  ens3   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:2000 to:10.1.1.1:22
  537 45048 PREROUTING_direct  all  --  *      *       0.0.0.0/0            0.0.0.0/0
  537 45048 PREROUTING_ZONES_SOURCE  all  --  *      *       0.0.0.0/0            0.0.0.0/0
  537 45048 PREROUTING_ZONES  all  --  *      *       0.0.0.0/0            0.0.0.0/0
[root@router ~]#
```

The packets are getting divided among the two servers

Out of 68 packets generated by syslog process from Client

34 are being sent to the Server 1 **10.1.1.1**

34 are being sent to the server 2 **10.1.1.2**

Problem(6):

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

L2 ISOLATION IN TENANT1

Here the VMS in the tenant 1

T1-VM1 –10.2.2.0/24 subnetwork

Default gateway for the T1-VM1 INETRFACE IS ns1 interface (veth_t1br0_ns1) –10.2.2.3

T2-VM1 - 10.3.3.0/24 subnetwork

Default gateway for the T1-VM2 INTERFACE is ns1 interface (veth_t1br1_ns1) -10.3.3.2

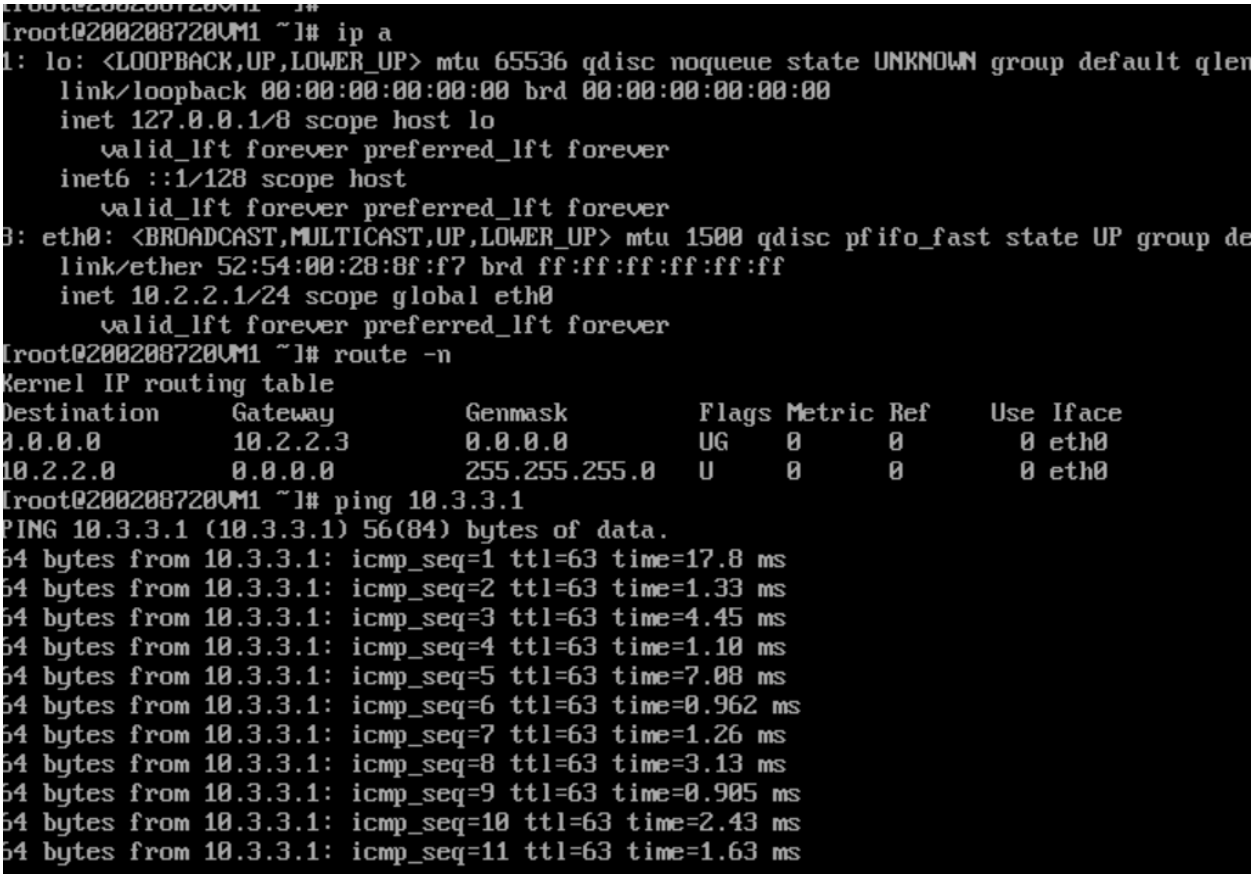
Interface config and route table of the NS1 :

```
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.2.2.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t1br0_ns1
10.3.3.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t1br1_ns1
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
109: veth_ns1_ns1@if108: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether ee:13:e3:c8:64:8f brd ff:ff:ff:ff:ff:ff link-netnsid 0
153: veth_t1br0_ns1@if154: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 9e:9e:b3:3c:3b:86 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.2.2.3/24 scope global veth_t1br0_ns1
       valid_lft forever preferred_lft forever
    inet6 fe80::9c9e:b3ff:fe3c:3b86/64 scope link
       valid_lft forever preferred_lft forever
155: veth_t1br1_ns1@if156: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether f6:32:29:42:5b:98 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.3.3.2/24 scope global veth_t1br1_ns1
       valid_lft forever preferred_lft forever
    inet6 fe80::f432:29ff:fe42:5b98/64 scope link
       valid_lft forever preferred_lft forever
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

The VMs in the same tenant are L2 isolated

As T1-VM1 is successfully able to ping T1-VM2

T1-VM1 (10.2.2.1) -----T1-VM2(10.3.3.1)



Packet Capture at T1-VM1(eth0) interface:

```
02:35:46.184759 IP 10.2.2.1 > 10.3.3.1: ICMP echo request, id 2644, seq 170, length 64
02:35:46.184843 IP 10.3.3.1 > 10.2.2.1: ICMP echo reply, id 2644, seq 170, length 64
02:35:47.186845 IP 10.2.2.1 > 10.3.3.1: ICMP echo request, id 2644, seq 171, length 64
02:35:47.186926 IP 10.3.3.1 > 10.2.2.1: ICMP echo reply, id 2644, seq 171, length 64
02:35:48.196241 IP 10.2.2.1 > 10.3.3.1: ICMP echo request, id 2644, seq 172, length 64
02:35:48.196303 IP 10.3.3.1 > 10.2.2.1: ICMP echo reply, id 2644, seq 172, length 64
02:35:49.197632 IP 10.2.2.1 > 10.3.3.1: ICMP echo request, id 2644, seq 173, length 64
02:35:49.197703 IP 10.3.3.1 > 10.2.2.1: ICMP echo reply, id 2644, seq 173, length 64
02:35:50.199919 IP 10.2.2.1 > 10.3.3.1: ICMP echo request, id 2644, seq 174, length 64
02:35:50.199996 IP 10.3.3.1 > 10.2.2.1: ICMP echo reply, id 2644, seq 174, length 64
02:35:51.201565 IP 10.2.2.1 > 10.3.3.1: ICMP echo request, id 2644, seq 175, length 64
02:35:51.201651 IP 10.3.3.1 > 10.2.2.1: ICMP echo reply, id 2644, seq 175, length 64
02:35:52.204595 IP 10.2.2.1 > 10.3.3.1: ICMP echo request, id 2644, seq 176, length 64
02:35:52.204661 IP 10.3.3.1 > 10.2.2.1: ICMP echo reply, id 2644, seq 176, length 64
02:35:53.206835 IP 10.2.2.1 > 10.3.3.1: ICMP echo request, id 2644, seq 177, length 64
02:35:53.206915 IP 10.3.3.1 > 10.2.2.1: ICMP echo reply, id 2644, seq 177, length 64
02:35:53.557532 IP 10.3.3.2 > 10.3.3.1: ICMP net 192.73.243.97 unreachable, length 84
02:35:54.207968 IP 10.2.2.1 > 10.3.3.1: ICMP echo request, id 2644, seq 178, length 64
02:35:54.208040 IP 10.3.3.1 > 10.2.2.1: ICMP echo reply, id 2644, seq 178, length 64
02:35:55.209747 IP 10.2.2.1 > 10.3.3.1: ICMP echo request, id 2644, seq 179, length 64
02:35:55.209815 IP 10.3.3.1 > 10.2.2.1: ICMP echo reply, id 2644, seq 179, length 64
02:35:56.211810 IP 10.2.2.1 > 10.3.3.1: ICMP echo request, id 2644, seq 180, length 64
02:35:56.211887 IP 10.3.3.1 > 10.2.2.1: ICMP echo reply, id 2644, seq 180, length 64
02:35:57.213505 IP 10.2.2.1 > 10.3.3.1: ICMP echo request, id 2644, seq 181, length 64
02:35:57.213578 IP 10.3.3.1 > 10.2.2.1: ICMP echo reply, id 2644, seq 181, length 64
```

Where as arping is not successful as they are not in the same L2 -domain

And it resulted in no packet capture

Arping -I eth0 10.3.3.1

```
10.2.2.3                 ether   9e:9e:b3:3c:3b:86   C
[root@200208720VM1 ~]# arping -I eth0 10.3.3.1
ARPING 10.3.3.1 from 10.2.2.1 eth0
```

a

Packet capture at the T1-VM2 SIDE (10.3.3.1):

```
[root@200208720VM1 ~]# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
02:42:18.108479 IP 200208720VM1.41397 > 192.111.144.114.ntp: NTPv4, Client, length 48
02:42:18.108832 IP gateway > 200208720VM1: ICMP net 192.111.144.114 unreachable, length 84
02:42:21.953966 IP 200208720VM1.46661 > 173.230.152.251.ntp: NTPv4, Client, length 48
02:42:21.956554 IP gateway > 200208720VM1: ICMP net 173.230.152.251 unreachable, length 84
02:42:23.115816 ARP, Request who-has gateway tell 200208720VM1, length 28
02:42:23.116100 ARP, Reply gateway is-at f6:32:29:42:5b:98 (oui Unknown), length 28
02:42:23.143237 ARP, Request who-has 200208720VM1 tell gateway, length 28
02:42:23.143263 ARP, Reply 200208720VM1 is-at 52:54:00:9d:91:be (oui Unknown), length 28
02:42:24.255461 IP 200208720VM1.42526 > 172.98.77.203.ntp: NTPv4, Client, length 48
02:42:24.255769 IP gateway > 200208720VM1: ICMP net 172.98.77.203 unreachable, length 84
```

No arp request from 10.2.2.1 reached 10.3.3.1

Arp table of the T1-VM1:

```
^C^C
--- 10.3.3.1 ping statistics ---
385 packets transmitted, 385 received, 0% packet loss, time 384949ms
rtt min/avg/max/mdev = 0.684/2.743/19.306/2.761 ms
[root@200208720VM1 ~]# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.2.2.3                 ether   9e:9e:b3:3c:3b:86   C                     eth0
[root@200208720VM1 ~]#
```

L2 ISOLATION in tenant2:

T2-VM1 –20.0.0.0/24 network

T2-VM2 --- 20.1.1.0/24 network

Interface config of the ns2 :

```
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# ip netns exec ns2 bash
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
111: veth_ns2_ns2@if110: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state LOWERLAYERDOWN group defaul
    link/ether de:26:b1:cc:15:48 brd ff:ff:ff:ff:ff:ff link-netnsid 0
164: veth_t2br0_ns2@if165: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 0e:92:14:2d:60:f0 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 20.0.0.2/24 scope global veth_t2br0_ns2
       valid_lft forever preferred_lft forever
    inet6 fe80::c92:14ff:fe2d:60f0/64 scope link
       valid_lft forever preferred_lft forever
166: veth_t2br1_ns2@if167: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether e6:f7:51:8c:e5:ba brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 20.1.1.2/24 scope global veth_t2br1_ns2
       valid_lft forever preferred_lft forever
    inet6 fe80::e4f7:51ff:fe8c:e5ba/64 scope link
       valid_lft forever preferred_lft forever
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
20.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t2br0_ns2
20.1.1.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t2br1_ns2
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

T2-VM1(20.0.0.1) ------ T2-VM2(20.1.1.1)

Packet capture on the T2-VM2

```
[root@200208720VM1 ~]# ^C
[root@200208720VM1 ~]# tcpdump -i eth0 icmp -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:35:11.156333 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 1, length 64
15:35:11.156535 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 1, length 64
15:35:12.171122 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 2, length 64
15:35:12.171204 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 2, length 64
15:35:13.173529 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 3, length 64
15:35:13.173602 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 3, length 64
15:35:14.176472 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 4, length 64
15:35:14.176544 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 4, length 64
15:35:15.177453 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 5, length 64
15:35:15.177524 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 5, length 64
15:35:16.179419 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 6, length 64
15:35:16.179491 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 6, length 64
15:35:17.184358 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 7, length 64
15:35:17.184442 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 7, length 64
15:35:18.184415 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 8, length 64
15:35:18.184487 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 8, length 64
15:35:19.185885 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 9, length 64
15:35:19.185983 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 9, length 64
15:35:20.189125 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 10, length 64
15:35:20.189211 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 10, length 64
15:35:21.189313 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 11, length 64
15:35:21.189399 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 11, length 64
15:35:22.192289 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 12, length 64
15:35:22.192377 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 12, length 64
15:35:23.194513 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 13, length 64
15:35:23.194584 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 13, length 64
15:35:24.202041 IP 20.0.0.1 > 20.1.1.1: ICMP echo request, id 4465, seq 14, length 64
15:35:24.202108 IP 20.1.1.1 > 20.0.0.1: ICMP echo reply, id 4465, seq 14, length 64
```

Arptable of the T2-VM1:

```
-bash: ARP: command not found
[root@200208720VM1 ~]#
[root@200208720VM1 ~]# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
20.0.0.2                 ether   0e:92:14:2d:60:f0   C                     eth0
[root@200208720VM1 ~]# arping -I eth0 10.2.2.1
ARPING 10.2.2.1 from 20.0.0.1 eth0
^CSent 27 probes (27 broadcast(s))
Received 0 response(s)
[root@200208720VM1 ~]#
```

Arp table of the T2-VM2:

```
[root@200208720VM1 ~]# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
20.1.1.2                 ether   e6:f7:51:8c:e5:ba   C                     eth0
[root@200208720VM1 ~]# arping -I eth0 20.0.0.1
ARPING 20.0.0.1 from 20.1.1.1 eth0
^CSent 14 probes (14 broadcast(s))
Received 0 response(s)
[root@200208720VM1 ~]#
```

No response has been captured in the arping -I eth0 command.

Part(b) :

Topology for the below case is

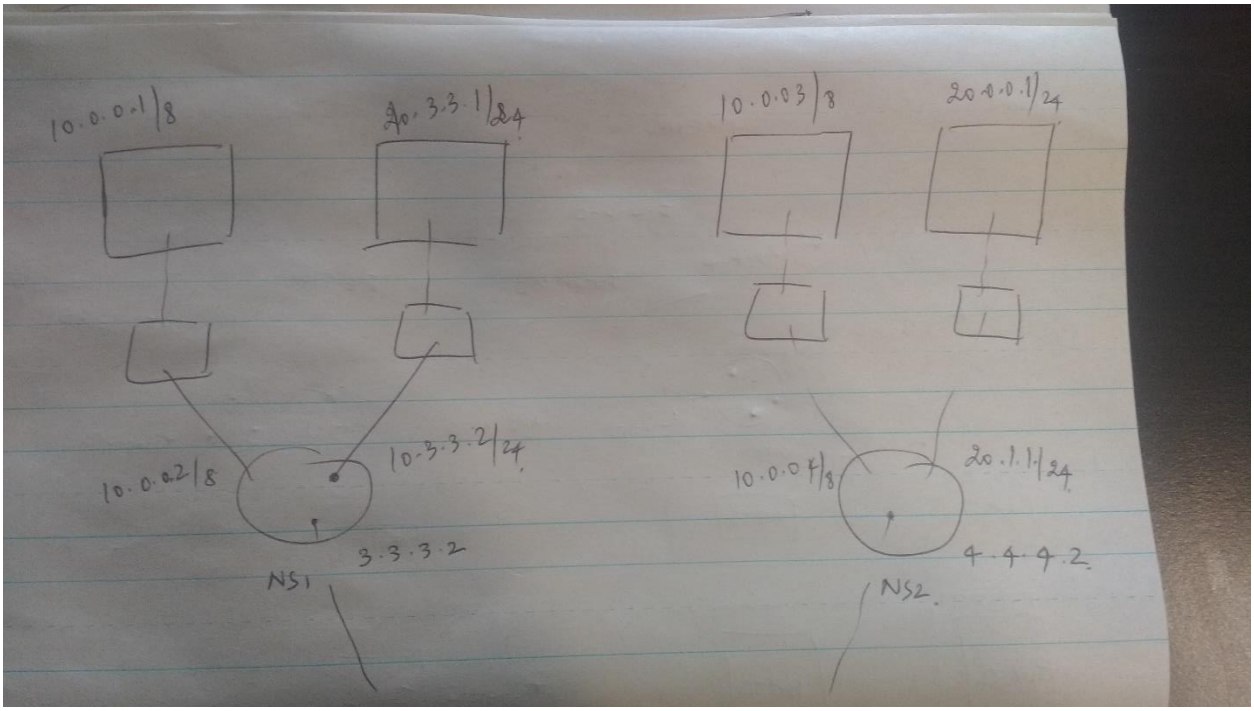
Blue tenants has these subnets (10.0.0.0/8) &(10.3.3.0/24)

Red tenants has these subnets (10.0.0.0/8) & (20.1.1.0/24)

NS1 & NS2 are connected to host via veth_pair (for Internet connectivity)

Veth_ns1_prov ---veth pair for NS1 for internet connectivity

Veth_ns2_prov ---veth pair for NS2 for internet connectivity



L3 isolation between two tenants:

Config & route table of T1-VM1(Blue Tenant):

```
[root@200208720VM1 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.0.2        0.0.0.0         UG    0      0        0 eth0
10.0.0.0        0.0.0.0         255.0.0.0       U     0      0        0 eth0
[root@200208720VM1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
    link/ether 52:54:00:28:8f:f7 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.1/8 scope global eth0
       valid_lft forever preferred_lft forever
[root@200208720VM1 ~]#
```

Config & route table of T2-VM1(Red Tenant)

```
[root@200208720VM1 ~]# ip route add default via 10.0.0.4
[root@200208720VM1 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.0.4        0.0.0.0         UG    0      0        0 eth0
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
[root@200208720VM1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
    link/ether 52:54:00:01:7a:99 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.3/24 scope global eth0
       valid_lft forever preferred_lft forever
[root@200208720VM1 ~]#
```

Forwarding Table of Ns1 & Ns2:

```
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         3.3.3.1         0.0.0.0         UG    0      0        0 veth_ns1_prov
3.3.3.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_ns1_prov
6.6.6.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_ns1_ns1
10.0.0.0        0.0.0.0         255.0.0.0       U     0      0        0 veth_t1br0_ns1
10.3.3.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t1br1_ns1
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

```
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         4.4.4.1         0.0.0.0         UG    0      0        0 veth_ns2_prov
4.4.4.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_ns2_prov
6.6.6.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_ns2_ns2
10.0.0.0        0.0.0.0         255.0.0.0       U     0      0        0 veth_t2br0_ns2
20.1.1.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t2br1_ns2
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

Forwarding table of Host hypervisor:

```
ece792@ece792-Standard-PC-i440FX-PIIX-1996:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.122.1   0.0.0.0         UG    100    0        0 ens3
0.0.0.0         192.168.123.1   0.0.0.0         UG    101    0        0 ens5
5.5.5.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_def_prov
50.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 public_net
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 vnet26
192.168.100.0   0.0.0.0         255.255.255.0   U     0      0        0 SW1
192.168.105.0   0.0.0.0         255.255.255.0   U     0      0        0 SW3
192.168.110.0   0.0.0.0         255.255.255.0   U     0      0        0 SW4
192.168.122.0   0.0.0.0         255.255.255.0   U     100    0        0 ens3
192.168.123.0   0.0.0.0         255.255.255.0   U     100    0        0 ens5
192.168.130.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
192.168.132.0   0.0.0.0         255.255.255.0   U     0      0        0 l3bridge
192.168.134.0   0.0.0.0         255.255.255.0   U     0      0        0 l3bridge_net2
192.168.150.0   0.0.0.0         255.255.255.0   U     0      0        0 ovs-bridge
200.0.0.0       202.0.0.1       255.255.255.0   UG    0      0        0 ens4
201.0.0.0       0.0.0.0         255.255.255.0   U     0      0        0 rdesign1
202.0.0.0       0.0.0.0         255.255.255.0   U     0      0        0 ens4
```

L3-isolation :

Blue tenant subnets T1-VM1 (10.0.0.0/8) & T1-VM2(10.3.3.0/24)

Red tenant subnets T2-VM2(10.0.0.0/8) & T2-VM1(20.1.1.0/24)

Suppose T1-VM1 (10.0.0.0/8) wants to communicate with T2-VM1(20.1.1.0/24) as the route in NS1 will point to the default gateway which is in host and host doesn't have any route for 20.0.0.0/24 in its forwarding table so the packet gets dropped at the host.

Similarly, if T2-VM1(20.0.0.1/24) wants to communicate with the T1-VM1(10.0.0.1/8) as the Forwarding table of NS2 points to the default gateway in host, As host doesn't have any route for 20.0.0.0/24 in its forwarding table and packet gets dropped at the host.

Trying to Ping 20.1.1.1 from 10.0.0.1

```
[root@200208720VM1 ~]# ping 20.1.1.1.
ping: 20.1.1.1.: Name or service not known
[root@200208720VM1 ~]# ping 20.1.1.1
PING 20.1.1.1 (20.1.1.1) 56(84) bytes of data.
From 128.109.18.109 icmp_seq=1 Destination Net Unreachable
From 128.109.18.109 icmp_seq=4 Destination Net Unreachable
From 128.109.18.109 icmp_seq=19 Destination Net Unreachable
From 128.109.18.109 icmp_seq=29 Destination Net Unreachable
From 128.109.18.109 icmp_seq=45 Destination Net Unreachable
```

Trying to ping 10.0.0.1 from 20.1.1.1

```
[root@200208720VM1 ~]# [497499.104851] [drm:qxl_send_monitors_c
[498955.549894] [drm:qxl_send_monitors_config [qxl]] *ERROR* hea

[root@200208720VM1 ~]# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
From 10.0.0.3 icmp_seq=1 Destination Host Unreachable
From 10.0.0.3 icmp_seq=2 Destination Host Unreachable
From 10.0.0.3 icmp_seq=3 Destination Host Unreachable
From 10.0.0.3 icmp_seq=4 Destination Host Unreachable
From 10.0.0.3 icmp_seq=5 Destination Host Unreachable
From 10.0.0.3 icmp_seq=6 Destination Host Unreachable
From 10.0.0.3 icmp_seq=7 Destination Host Unreachable
From 10.0.0.3 icmp_seq=8 Destination Host Unreachable
```

Only the Request has been observed but no replies has been captured at 10.0.0.1

```
52 packets captured
52 packets received by filter
0 packets dropped by kernel
[root@t1-vm1-bluetenant ~]# tcpdump -i eth0 icmp -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:47:19.029571 IP 10.0.0.1 > 20.1.1.1: ICMP echo request, id 5314, seq 714, length 64
14:47:20.029767 IP 10.0.0.1 > 20.1.1.1: ICMP echo request, id 5314, seq 715, length 64
14:47:21.030024 IP 10.0.0.1 > 20.1.1.1: ICMP echo request, id 5314, seq 716, length 64
14:47:22.031219 IP 10.0.0.1 > 20.1.1.1: ICMP echo request, id 5314, seq 717, length 64
14:47:23.031750 IP 10.0.0.1 > 20.1.1.1: ICMP echo request, id 5314, seq 718, length 64
14:47:24.031700 IP 10.0.0.1 > 20.1.1.1: ICMP echo request, id 5314, seq 719, length 64
14:47:25.031671 IP 10.0.0.1 > 20.1.1.1: ICMP echo request, id 5314, seq 720, length 64
14:47:26.031681 IP 10.0.0.1 > 20.1.1.1: ICMP echo request, id 5314, seq 721, length 64
^C
8 packets captured
```

Part(B) :

The tenants having the same subnets 10.0.0.8 should be able to reach to internet.

The tenants are (10.0.0.1) (T1-VM1) ----Blue tenant

(10.0.0.3)(T2-VM1) ---Red tenant

Ip tables of Ns1 & Ns2:

NS1 Iptable:

```
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -t nat -vnL
Chain PREROUTING (policy ACCEPT 13 packets, 996 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   13   996 MASQUERADE  all  --  *      veth_ns1_prov  10.0.0.0/8           0.0.0.0/0
   41  3116 MASQUERADE  all  --  *      veth_ns1_prov  10.3.3.0/24          0.0.0.0/0
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -vnL
Chain INPUT (policy ACCEPT 1631 packets, 203K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 222K packets, 19M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 2784 packets, 228K bytes)
 pkts bytes target     prot opt in     out     source               destination
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

NS2 IP table:

```
[sudo] password for ece792:
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# ip netns exec ns2 bash
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -t nat -vnL
Chain PREROUTING (policy ACCEPT 1096 packets, 83224 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 32 packets, 2136 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 12 packets, 768 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1116 84592 MASQUERADE  all  --  *      veth_ns2_prov  0.0.0.0/0            0.0.0.0/0
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -vnL
Chain INPUT (policy ACCEPT 145K packets, 46M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 28104 packets, 2358K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 58659 packets, 3114K bytes)
 pkts bytes target     prot opt in     out     source               destination
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

For the Internet connectivity applied the Masquerade rules otherwise when the packet return from the internet it wont be able to communicate to the Guest VM (10.0.0.1)(T1-VM1) or 10.0.0.3(T2-VM1)

Applying the rules at the NS1:

Iptables -t nat -I POSTROUTING -o veth_ns1_prov -j MASQUERADE

Applying the rules at the NS2:

Iptables -t nat -I POSTROUTING -o veth_ns2_prov -j MASQUERADE

Veth_ns1_prov ---Veth Pair connecting the Ns1 and the host

Veth_ns2_prov ---- veth_pair connecting the NS2 and host

Packet capture at Tenant blue tenant (10.0.0.1)(T1-VM1):

```
0 packets dropped by kernel
[root@t1-vm1-bluetenant ~]# tcpdump -i eth0 icmp -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:22:30.356739 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5337, seq 31, length 64
15:22:30.366086 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5337, seq 31, length 64
15:22:31.358434 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5337, seq 32, length 64
15:22:31.370282 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5337, seq 32, length 64
15:22:32.360641 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5337, seq 33, length 64
15:22:32.373785 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5337, seq 33, length 64
15:22:33.362661 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5337, seq 34, length 64
15:22:33.372901 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5337, seq 34, length 64
15:22:34.364252 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5337, seq 35, length 64
15:22:34.377138 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5337, seq 35, length 64
15:22:35.366781 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5337, seq 36, length 64
15:22:35.376006 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5337, seq 36, length 64
15:22:36.369700 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5337, seq 37, length 64
15:22:36.379037 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5337, seq 37, length 64
15:22:37.371242 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5337, seq 38, length 64
15:22:37.380890 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5337, seq 38, length 64
15:22:38.372683 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5337, seq 39, length 64
15:22:38.392958 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5337, seq 39, length 64
15:22:39.374776 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5337, seq 40, length 64
15:22:39.385778 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5337, seq 40, length 64
15:22:40.376480 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5337, seq 41, length 64
15:22:40.386326 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5337, seq 41, length 64
^C
```

Packet capture at Red tenant (T2-VM1)(10.0.0.3)

```
root@10.0.0.3's password:
Last login: Wed Oct 31 14:33:43 2018 from gateway
[root@t2-vm1-redtenant ~]# tcpdump -i eth0 icmp -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:28:29.560238 IP 10.0.0.3 > 8.8.8.8: ICMP echo request, id 7413, seq 11, length 64
15:28:29.569541 IP 8.8.8.8 > 10.0.0.3: ICMP echo reply, id 7413, seq 11, length 64
15:28:30.562532 IP 10.0.0.3 > 8.8.8.8: ICMP echo request, id 7413, seq 12, length 64
15:28:30.573045 IP 8.8.8.8 > 10.0.0.3: ICMP echo reply, id 7413, seq 12, length 64
15:28:31.563959 IP 10.0.0.3 > 8.8.8.8: ICMP echo request, id 7413, seq 13, length 64
15:28:31.573261 IP 8.8.8.8 > 10.0.0.3: ICMP echo reply, id 7413, seq 13, length 64
15:28:32.565987 IP 10.0.0.3 > 8.8.8.8: ICMP echo request, id 7413, seq 14, length 64
15:28:32.575175 IP 8.8.8.8 > 10.0.0.3: ICMP echo reply, id 7413, seq 14, length 64
15:28:33.568035 IP 10.0.0.3 > 8.8.8.8: ICMP echo request, id 7413, seq 15, length 64
15:28:33.579450 IP 8.8.8.8 > 10.0.0.3: ICMP echo reply, id 7413, seq 15, length 64
15:28:34.570069 IP 10.0.0.3 > 8.8.8.8: ICMP echo request, id 7413, seq 16, length 64
15:28:34.579297 IP 8.8.8.8 > 10.0.0.3: ICMP echo reply, id 7413, seq 16, length 64
15:28:35.572075 IP 10.0.0.3 > 8.8.8.8: ICMP echo request, id 7413, seq 17, length 64
15:28:35.583219 IP 8.8.8.8 > 10.0.0.3: ICMP echo reply, id 7413, seq 17, length 64
15:28:36.573823 IP 10.0.0.3 > 8.8.8.8: ICMP echo request, id 7413, seq 18, length 64
15:28:36.583194 IP 8.8.8.8 > 10.0.0.3: ICMP echo reply, id 7413, seq 18, length 64
15:28:37.575968 IP 10.0.0.3 > 8.8.8.8: ICMP echo request, id 7413, seq 19, length 64
15:28:37.586956 IP 8.8.8.8 > 10.0.0.3: ICMP echo reply, id 7413, seq 19, length 64
15:28:38.578166 IP 10.0.0.3 > 8.8.8.8: ICMP echo request, id 7413, seq 20, length 64
15:28:38.588718 IP 8.8.8.8 > 10.0.0.3: ICMP echo reply, id 7413, seq 20, length 64
^C
```

Part (c)

Topology for this scenario looks likes below

The T1-VM1 ----- 10.0.0.0/24 subnet

T1-VM2 ----------10.1.1.0/24 subnet

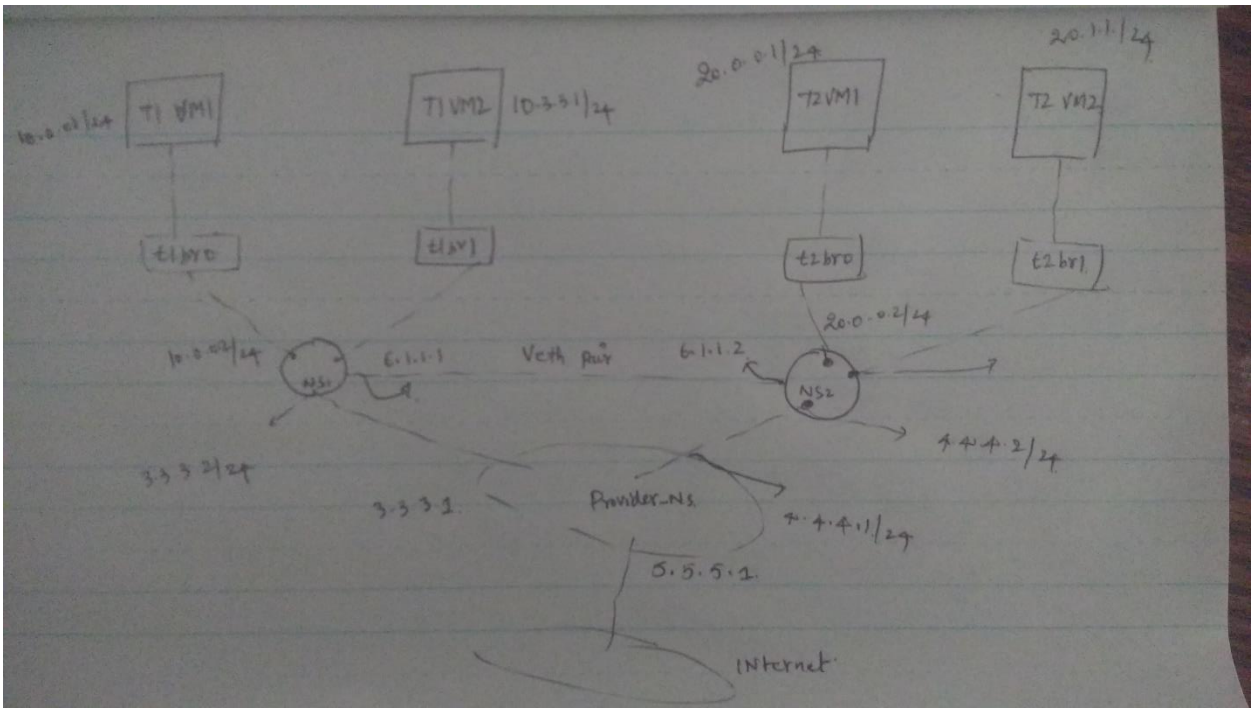
T2-VM1 ----------20.0.0.0/24 subnet

T2 -VM2 ----------20.1.1.0/24 subnet

Ns1 and Provider Ns are connected via 3.3.3.0/24 subnet

NS2 and Provider NS are connected via 4.4.4.0/24 Subnet

Ns1 and Ns2 are connected via Veth pair in the subnet 6.1.1.0/24 subnet



All the interface configs of all the namespaces and VMs

Provieder_namespace config:

```
       valid_lft forever preferred_lft forever
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         5.5.5.2         0.0.0.0         UG    0      0        0 veth_prov_def
3.3.3.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_prov_ns1
4.4.4.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_prov_ns2
5.5.5.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_prov_def
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
188: veth_prov_ns1@if189: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 3e:37:c9:ad:28:e9 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet 3.3.3.1/24 scope global veth_prov_ns1
       valid_lft forever preferred_lft forever
    inet6 fe80::3c37:c9ff:fead:28e9/64 scope link
       valid_lft forever preferred_lft forever
190: veth_prov_ns2@if191: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 2e:a3:05:d1:3d:65 brd ff:ff:ff:ff:ff:ff link-netnsid 2
    inet 4.4.4.1/24 scope global veth_prov_ns2
       valid_lft forever preferred_lft forever
    inet6 fe80::2ca3:5ff:fed1:3d65/64 scope link
       valid_lft forever preferred_lft forever
195: veth_prov_def@if194: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 4a:c8:2f:0e:e5:ed brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 5.5.5.1/24 scope global veth_prov_def
       valid_lft forever preferred_lft forever
    inet6 fe80::48c8:2fff:fe0e:e5ed/64 scope link
       valid_lft forever preferred_lft forever
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

Rename

Ns1 interface config & forwarding table :

```
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
153: veth_t1br0_ns1@if154: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 9e:9e:b3:3c:3b:86 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.0.2/24 scope global veth_t1br0_ns1
       valid_lft forever preferred_lft forever
    inet6 fe80::9c9e:b3ff:fe3c:3b86/64 scope link
       valid_lft forever preferred_lft forever
155: veth_t1br1_ns1@if156: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether f6:32:29:42:5b:98 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.3.3.2/24 scope global veth_t1br1_ns1
       valid_lft forever preferred_lft forever
    inet6 fe80::f432:29ff:fe42:5b98/64 scope link
       valid_lft forever preferred_lft forever
189: veth_ns1_prov@if188: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 4e:53:63:e0:3d:01 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet 3.3.3.2/24 scope global veth_ns1_prov
       valid_lft forever preferred_lft forever
    inet6 fe80::4c53:63ff:fee0:3d01/64 scope link
       valid_lft forever preferred_lft forever
197: veth_ns1_ns1@if196: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether fa:aa:f4:8d:27:a4 brd ff:ff:ff:ff:ff:ff link-netnsid 2
    inet 6.6.6.1/24 scope global veth_ns1_ns1
       valid_lft forever preferred_lft forever
    inet6 fe80::f8aa:f4ff:fe8d:27a4/64 scope link
       valid_lft forever preferred_lft forever
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

Ns1 Route table :

```
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         3.3.3.1         0.0.0.0         UG    0      0        0 veth_ns1_prov
3.3.3.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_ns1_prov
6.6.6.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_ns1_ns1
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t1br0_ns1
10.3.3.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t1br1_ns1
20.0.0.0        6.6.6.2         255.255.255.0   UG    0      0        0 veth_ns1_ns1
20.1.1.0        6.6.6.2         255.255.255.0   UG    0      0        0 veth_ns1_ns1
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

NAME SPACE 2 config & forwarding table :

```
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
164: veth_t2br0_ns2@if165: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 0e:92:14:2d:60:f0 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 20.0.0.2/24 scope global veth_t2br0_ns2
       valid_lft forever preferred_lft forever
    inet6 fe80::c92:14ff:fe2d:60f0/64 scope link
       valid_lft forever preferred_lft forever
166: veth_t2br1_ns2@if167: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether e6:f7:51:8c:e5:ba brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 20.1.1.2/24 scope global veth_t2br1_ns2
       valid_lft forever preferred_lft forever
    inet6 fe80::e4f7:51ff:fe8c:e5ba/64 scope link
       valid_lft forever preferred_lft forever
191: veth_ns2_prov@if190: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 1a:f2:27:28:a5:8e brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet 4.4.4.2/24 scope global veth_ns2_prov
       valid_lft forever preferred_lft forever
    inet6 fe80::18f2:27ff:fe28:a58e/64 scope link
       valid_lft forever preferred_lft forever
196: veth_ns2_ns2@if197: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether ca:c8:3f:b2:6b:2a brd ff:ff:ff:ff:ff:ff link-netnsid 2
    inet 6.6.6.2/24 scope global veth_ns2_ns2
       valid_lft forever preferred_lft forever
    inet6 fe80::c8c8:3fff:feb2:6b2a/64 scope link
       valid_lft forever preferred_lft forever
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

NS2 Forwarding table :

```
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         4.4.4.1         0.0.0.0         UG    0      0        0 veth_ns2_prov
4.4.4.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_ns2_prov
6.6.6.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_ns2_ns2
10.0.0.0        6.6.6.1         255.255.255.0   UG    0      0        0 veth_ns2_ns2
10.3.3.0        6.6.6.1         255.255.255.0   UG    0      0        0 veth_ns2_ns2
20.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t2br0_ns2
20.1.1.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t2br1_ns2
```

Forwarding table & interface config of one of the Blue tenant(T1-VM1) (10.0.0.1)

```
[root@200208720VM1 ~]#
[root@200208720VM1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
    link/ether 52:54:00:28:8f:f7 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.1/24 scope global eth0
       valid_lft forever preferred_lft forever
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
[root@200208720VM1 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.0.2        0.0.0.0         UG    0      0        0 eth0
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
[root@200208720VM1 ~]#
```

Forwarding table and Ip address of one Red tenant(T2-VM1) (20.0.0.1)

```
Object "aip" is unknown, try "ip help".
[root@200208720VM1 ~]# ^C
[root@200208720VM1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
    link/ether 52:54:00:01:7a:99 brd ff:ff:ff:ff:ff:ff
    inet 20.0.0.1/24 scope global eth0
       valid_lft forever preferred_lft forever
[root@200208720VM1 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         20.0.0.2        0.0.0.0         UG    0      0        0 eth0
20.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
[root@200208720VM1 ~]#
```

IP tables of the Namesapces :

Iptables of the NS 1:

```
iptables: command not found
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -t nat -vnL POSTROUTING
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   18  1368 MASQUERADE  all  --  *      veth_ns1_prov  10.3.3.0/24          0.0.0.0/0
   37  2868 MASQUERADE  all  --  *      veth_ns1_prov  10.0.0.0/24          0.0.0.0/0
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -vnL
Chain INPUT (policy ACCEPT 1468 packets, 185K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 222K packets, 19M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 2492 packets, 206K bytes)
 pkts bytes target     prot opt in     out     source               destination
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

Ip tables of the NS 2:

```
       valid_lft forever preferred_lft forever
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -t nat -vnL POSTROUTING
Chain POSTROUTING (policy ACCEPT 6 packets, 408 bytes)
 pkts bytes target     prot opt in     out     source               destination
  722 54800 MASQUERADE  all  --  *      veth_ns2_prov  0.0.0.0/0            0.0.0.0/0
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -vnL
Chain INPUT (policy ACCEPT 19 packets, 3653 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 1082 packets, 86154 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 26 packets, 3665 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

Iptables of Provider namespace:

```
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -vnL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 2986 packets, 230K bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    60 REJECT     tcp  --  *      *       4.4.4.0/24           0.0.0.0/0           tcp dpt:22 reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT 1 packets, 88 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -t nat -POSTROUTING
iptables v1.6.0: -P requires a chain and a policy
Try `iptables -h' or 'iptables --help' for more information.
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -t nat -vnL POSTROUTING
Chain POSTROUTING (policy ACCEPT 3 packets, 180 bytes)
 pkts bytes target     prot opt in     out     source               destination
  702 53368 MASQUERADE  all  --  *      veth_prov_def  4.4.4.0/24          0.0.0.0/0
  785 59732 MASQUERADE  all  --  *      veth_prov_def  3.3.3.0/24          0.0.0.0/0
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

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

Checking for the Blue tenants(10.0.0.1) ICMP traffic

As by default the forwarding policy is allow for all packets

No rule has been applied at **provider_ns** to allow the ICMP traffic

ICMP packet is successfully reaching the internet :

Packet capture at the Blue tenant (10.0.0.1)

```
--- 8.8.8.8 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15044ms
rtt min/avg/max/mdev = 9.204/10.536/20.525/2.660 ms
[root@200208720VM1 ~]# tcpdump - i eth0 icmp -nn
tcpdump: syntax error
[root@200208720VM1 ~]# tcpdump -i eth0 icmp -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:40:22.273226 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5075, seq 1, length 64
11:40:22.284310 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5075, seq 1, length 64
11:40:23.275528 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5075, seq 2, length 64
11:40:23.285270 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5075, seq 2, length 64
11:40:24.277499 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5075, seq 3, length 64
11:40:24.286840 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5075, seq 3, length 64
11:40:25.279871 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5075, seq 4, length 64
11:40:25.290101 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5075, seq 4, length 64
11:40:26.281736 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5075, seq 5, length 64
11:40:26.291833 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5075, seq 5, length 64
11:40:27.284194 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5075, seq 6, length 64
11:40:27.293507 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5075, seq 6, length 64
11:40:28.286706 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5075, seq 7, length 64
11:40:28.296041 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5075, seq 7, length 64
11:40:29.288577 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5075, seq 8, length 64
11:40:29.298552 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5075, seq 8, length 64
11:40:30.290479 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5075, seq 9, length 64
11:40:30.299846 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5075, seq 9, length 64
11:40:31.292986 IP 10.0.0.1 > 8.8.8.8: ICMP echo request, id 5075, seq 10, length 64
11:40:31.304111 IP 8.8.8.8 > 10.0.0.1: ICMP echo reply, id 5075, seq 10, length 64
```

Packet capture at the Provider name space (Allowing the ICMP traffic for the Blue tenant)

Packets will be Masqeraded with the Ip of namespace 1 interface (3.3.3.2) while going out of NS1

```
root@ece792-Standard-PC-i440FX-PIIX-1996:~# tcpdump -i veth_prov_ns1 icmp -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on veth_prov_ns1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C11:40:34.326262 IP 3.3.3.2 > 8.8.8.8: ICMP echo request, id 5075, seq 13, length 64
11:40:34.335212 IP 8.8.8.8 > 3.3.3.2: ICMP echo reply, id 5075, seq 13, length 64
11:40:35.328682 IP 3.3.3.2 > 8.8.8.8: ICMP echo request, id 5075, seq 14, length 64
11:40:35.337562 IP 8.8.8.8 > 3.3.3.2: ICMP echo reply, id 5075, seq 14, length 64
11:40:36.330031 IP 3.3.3.2 > 8.8.8.8: ICMP echo request, id 5075, seq 15, length 64
11:40:36.338969 IP 8.8.8.8 > 3.3.3.2: ICMP echo reply, id 5075, seq 15, length 64
11:40:37.331842 IP 3.3.3.2 > 8.8.8.8: ICMP echo request, id 5075, seq 16, length 64
11:40:37.342722 IP 8.8.8.8 > 3.3.3.2: ICMP echo reply, id 5075, seq 16, length 64
11:40:38.333794 IP 3.3.3.2 > 8.8.8.8: ICMP echo request, id 5075, seq 17, length 64
11:40:38.342692 IP 8.8.8.8 > 3.3.3.2: ICMP echo reply, id 5075, seq 17, length 64
11:40:39.335804 IP 3.3.3.2 > 8.8.8.8: ICMP echo request, id 5075, seq 18, length 64
11:40:39.344718 IP 8.8.8.8 > 3.3.3.2: ICMP echo reply, id 5075, seq 18, length 64
11:40:40.337887 IP 3.3.3.2 > 8.8.8.8: ICMP echo request, id 5075, seq 19, length 64
11:40:40.346734 IP 8.8.8.8 > 3.3.3.2: ICMP echo reply, id 5075, seq 19, length 64
11:40:41.340194 IP 3.3.3.2 > 8.8.8.8: ICMP echo request, id 5075, seq 20, length 64
11:40:41.353395 IP 8.8.8.8 > 3.3.3.2: ICMP echo reply, id 5075, seq 20, length 64
11:40:42.341979 IP 3.3.3.2 > 8.8.8.8: ICMP echo request, id 5075, seq 21, length 64
11:40:42.350904 IP 8.8.8.8 > 3.3.3.2: ICMP echo reply, id 5075, seq 21, length 64
11:40:43.343832 IP 3.3.3.2 > 8.8.8.8: ICMP echo request, id 5075, seq 22, length 64
11:40:43.352788 IP 8.8.8.8 > 3.3.3.2: ICMP echo reply, id 5075, seq 22, length 64
11:40:44.345988 IP 3.3.3.2 > 8.8.8.8: ICMP echo request, id 5075, seq 23, length 64
11:40:44.354938 IP 8.8.8.8 > 3.3.3.2: ICMP echo reply, id 5075, seq 23, length 64
11:40:45.347843 IP 3.3.3.2 > 8.8.8.8: ICMP echo request, id 5075, seq 24, length 64
11:40:45.356716 IP 8.8.8.8 > 3.3.3.2: ICMP echo reply, id 5075, seq 24, length 64

24 packets captured
24 packets received by filter
```

ICMP traffic test for the RED tenant VM (20.0.0.1)

```
               [ -Z user ] [ expression ]
[root@200208720VM1 ~]# tcpdump -i eth0 icmp -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:37:43.463453 IP 20.0.0.1 > 8.8.8.8: ICMP echo request, id 7101, seq 1, length 64
12:37:43.483985 IP 8.8.8.8 > 20.0.0.1: ICMP echo reply, id 7101, seq 1, length 64
12:37:44.465104 IP 20.0.0.1 > 8.8.8.8: ICMP echo request, id 7101, seq 2, length 64
12:37:44.475322 IP 8.8.8.8 > 20.0.0.1: ICMP echo reply, id 7101, seq 2, length 64
12:37:45.467034 IP 20.0.0.1 > 8.8.8.8: ICMP echo request, id 7101, seq 3, length 64
12:37:45.476450 IP 8.8.8.8 > 20.0.0.1: ICMP echo reply, id 7101, seq 3, length 64
12:37:46.468352 IP 20.0.0.1 > 8.8.8.8: ICMP echo request, id 7101, seq 4, length 64
12:37:46.477714 IP 8.8.8.8 > 20.0.0.1: ICMP echo reply, id 7101, seq 4, length 64
12:37:47.469983 IP 20.0.0.1 > 8.8.8.8: ICMP echo request, id 7101, seq 5, length 64
12:37:47.480814 IP 8.8.8.8 > 20.0.0.1: ICMP echo reply, id 7101, seq 5, length 64
12:37:48.471335 IP 20.0.0.1 > 8.8.8.8: ICMP echo request, id 7101, seq 6, length 64
12:37:48.480981 IP 8.8.8.8 > 20.0.0.1: ICMP echo reply, id 7101, seq 6, length 64
12:37:49.473934 IP 20.0.0.1 > 8.8.8.8: ICMP echo request, id 7101, seq 7, length 64
12:37:49.483200 IP 8.8.8.8 > 20.0.0.1: ICMP echo reply, id 7101, seq 7, length 64
12:37:50.475894 IP 20.0.0.1 > 8.8.8.8: ICMP echo request, id 7101, seq 8, length 64
12:37:50.485300 IP 8.8.8.8 > 20.0.0.1: ICMP echo reply, id 7101, seq 8, length 64
12:37:51.477910 IP 20.0.0.1 > 8.8.8.8: ICMP echo request, id 7101, seq 9, length 64
12:37:51.487053 IP 8.8.8.8 > 20.0.0.1: ICMP echo reply, id 7101, seq 9, length 64
12:37:52.480092 IP 20.0.0.1 > 8.8.8.8: ICMP echo request, id 7101, seq 10, length 64
12:37:52.489675 IP 8.8.8.8 > 20.0.0.1: ICMP echo reply, id 7101, seq 10, length 64
12:37:53.481565 IP 20.0.0.1 > 8.8.8.8: ICMP echo request, id 7101, seq 11, length 64
12:37:53.491721 IP 8.8.8.8 > 20.0.0.1: ICMP echo reply, id 7101, seq 11, length 64
^C
22 packets captured
```

Packet capture at the Provider_ns interface

Packets will be be Masqeraded with the Ip of NS2 inetrface (4.4.4.2) while going out of NS2

```
listening on veth_prov_ns2, link-type EN10MB (Ethernet), capture size 262144 bytes
^C12:37:43.466835 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 1, length 64
12:37:43.479769 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 1, length 64
12:37:44.466565 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 2, length 64
12:37:44.476411 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 2, length 64
12:37:45.468498 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 3, length 64
12:37:45.477507 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 3, length 64
12:37:46.469800 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 4, length 64
12:37:46.478765 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 4, length 64
12:37:47.471420 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 5, length 64
12:37:47.480298 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 5, length 64
12:37:48.472777 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 6, length 64
12:37:48.481709 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 6, length 64
12:37:49.475380 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 7, length 64
12:37:49.484260 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 7, length 64
12:37:50.477343 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 8, length 64
12:37:50.486259 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 8, length 64
12:37:51.479332 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 9, length 64
12:37:51.488137 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 9, length 64
12:37:52.481870 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 10, length 64
12:37:52.490763 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 10, length 64
12:37:53.483041 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 11, length 64
12:37:53.492719 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 11, length 64
12:37:54.485926 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 12, length 64
12:37:54.494865 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 12, length 64
12:37:55.487654 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 13, length 64
12:37:55.496541 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 13, length 64
12:37:56.490676 IP 4.4.4.2 > 8.8.8.8: ICMP echo request, id 7101, seq 14, length 64
12:37:56.499623 IP 8.8.8.8 > 4.4.4.2: ICMP echo reply, id 7101, seq 14, length 64

28 packets captured
```

Blocking the SSh traffic for the red tenants (20.0.0.1 & 20.1.1.1)

```
--- 8.8.8.8 ping statistics ---
267 packets transmitted, 266 received, 0% packet loss, time 266648ms
rtt min/avg/max/mdev = 8.953/10.066/28.134/1.929 ms
[root@200208720VM1 ~]# ^C
[root@200208720VM1 ~]# ^C
[root@200208720VM1 ~]# ^C
[root@200208720VM1 ~]# ssh 8.8.8.8
ssh: connect to host 8.8.8.8 port 22: Connection refused
[root@200208720VM1 ~]# ssh 8.8.8.8
ssh: connect to host 8.8.8.8 port 22: Connection refused
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
```

SSh traffic being blocked at the provider namespace

With the command

Iptables -I FORWARDING -s 4.4.4.2 –dport 22 -j REJECT <<<<<<<<<<<<<<<<<<<<<<<<<

Because all the traffic from NS2 is being Masqueraded with NS2 outgoing interface (4.4.4.2)

Ip table rule at the provder_ns

```
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -vnL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 2986 packets, 230K bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    60 REJECT     tcp  --  *      *       4.4.4.0/24           0.0.0.0/0           tcp dpt:22 reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT 1 packets, 88 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -t nat -POSTROUTING
iptables v1.6.0: -P requires a chain and a policy
Try `iptables -h' or 'iptables --help' for more information.
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# iptables -t nat -vnL POSTROUTING
Chain POSTROUTING (policy ACCEPT 3 packets, 180 bytes)
 pkts bytes target     prot opt in     out     source               destination
  702 53368 MASQUERADE  all  --  *      veth_prov_def  4.4.4.0/24           0.0.0.0/0
  785 59732 MASQUERADE  all  --  *      veth_prov_def  3.3.3.0/24           0.0.0.0/0
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

While allowing the ssh traffic for the Blue tenants(10.0.0.1) & 10.3.3.1

We are not getting connection refused message here.

```
[root@200208720VM1 ~]# [491414.511983] [drm:qxl_send_monitors_config
[493219.141413] [drm:qxl_send_monitors_config [qxl]] *ERROR* head 4 w

[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
[root@200208720VM1 ~]#
[root@200208720VM1 ~]# ssh 8.8.8.8
```

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

My provider network is provider_ns (Namesapce) and Veth_pair between the ns1 and ns2

Provider_ns to have the connectivity for the internet

And the veth_pair is to allow the communication between the two namesapces (NS1 & NS2)

In order to allow the ssh traffic between the two VMS

Veth_ns1_ns1(6.1.1.1) and veth_ns2_ns2(6.1.1.2) has been used between the vms:

Blue tenant VMs subnets ---------- (10.0.0.0/24) & (10.3.3.0/24) subnets

Red Tenants VMS subnets ----------(20.0.0.0/24) & (20.1.1.0/24) subnets

The routes for the 20.0.0.0/24) & (20.1.1.0/24) are added in NS1 via 6.6.6.2(Veth_pair) other interface (6.6.6.2)

When blue tenant(10.0.0.1) wants to communicate with the red tenants(20.0.0.1) the traffic will be follow this data path

10.0.0.1 ----t1br0 bridge ---ns1 ---Veth-pair ---ns2---- t2br0 ----20.0.0.1

Routing table of NS1 :

```
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         3.3.3.1         0.0.0.0         UG    0      0        0 veth_ns1_prov
3.3.3.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_ns1_prov
6.6.6.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_ns1_ns1
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t1br0_ns1
10.3.3.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t1br1_ns1
20.0.0.0        6.6.6.2         255.255.255.0   UG    0      0        0 veth_ns1_ns1
20.1.1.0        6.6.6.2         255.255.255.0   UG    0      0        0 veth_ns1_ns1
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

Route table of Ns2 :

The routes for the (10.0.0.0/24) & (10.3.3.0/24) are added in NS2 via 6.6.6.1(Veth_pair) other interface

When red tenant(20.0.0.1) wants to communicate with the blue tenant(10.0.0.1), The traffic will be follow this data path

20.0.0.1 ----t2br0 bridge ---ns2 ---veth-pair ---ns1---- t1br0 ----10.0.0.1

```
Cannot open network namespace "bash": No such file or directory
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# ip netns exec ns2 bash
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# ip aroute -n
Object "aroute" is unknown, try "ip help".
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         4.4.4.1         0.0.0.0         UG    0      0        0 veth_ns2_prov
4.4.4.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_ns2_prov
6.6.6.0         0.0.0.0         255.255.255.0   U     0      0        0 veth_ns2_ns2
10.0.0.0        6.6.6.1         255.255.255.0   UG    0      0        0 veth_ns2_ns2
10.3.3.0        6.6.6.1         255.255.255.0   UG    0      0        0 veth_ns2_ns2
20.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t2br0_ns2
20.1.1.0        0.0.0.0         255.255.255.0   U     0      0        0 veth_t2br1_ns2
root@ece792-Standard-PC-i440FX-PIIX-1996:/home/ece792#
```

Able to ssh from the blue Tenant(10.0.0.1) (t1-vm1) --- 20.0.0.1(t2-vm1)

From T1-VM1-blue tenant

```
[root@200208720VM1 ~]# cat /etc/hostname
t1-vm1-bluetenant
[root@200208720VM1 ~]# ssh root@20.0.0.1
The authenticity of host '20.0.0.1 (20.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:AZNcls2Huh2c9+xyV8tBquhdQb/kdq1501mexOcno
wk.
ECDSA key fingerprint is MD5:10:2e:5c:21:57:28:a1:c2:22:43:c5:8d:8d:df:e2
:93.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '20.0.0.1' (ECDSA) to the list of known hosts.
root@20.0.0.1's password:
Last login: Wed Oct 31 13:16:59 2018 from gateway
[root@t2-vm1-redtenant ~]# cat /etc/hostname
t2-vm1-redtenant
[root@t2-vm1-redtenant ~]#
```

Capture of ssh from 20.0.0.1 to 10.0.0.1(red tenant to Blue tenant)