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 B) (C D )

\ / \ /

**Bridge1**  **Bridge2**

\ /

**Bridge 3**

1. 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.
2. 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

1. 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.

1. **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)

1. **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 ) .

1. **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**

**A B C D**

**| | | |**

**| | | |**

**Bridge1 Bridge2 (ens4) (ens4) Bridge3 Bridge4**

**\ /**

**\ /**

**Bridge5**

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 to ping 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):

(A (B) (C D )

\ / \ /

**Bridge1(Routed mode)**  **Bridge2(Routed Mode)**

\ /

**Bridge 3**

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

**Is a tenant's traffic isolated from other tenants?**

The tenant’straffic 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 B C D**

**| | | |**

**| | | |**

**Bridge1 Bridge2 Bridge3 Bridge4**

**\ /**

**\ /**

**Bridge5**

(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

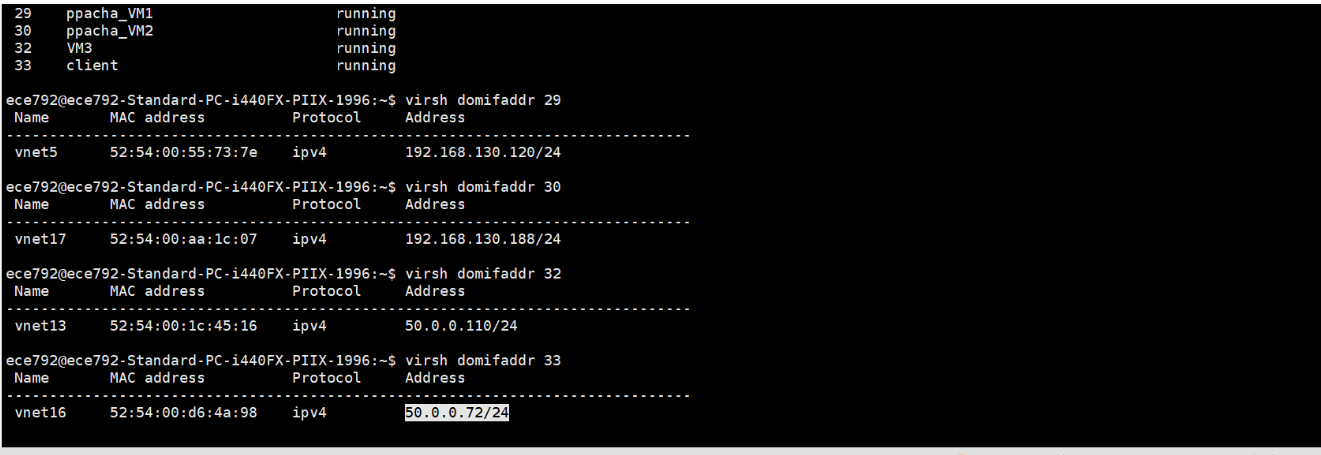
Router VM ----- VM3(In our topology )

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**

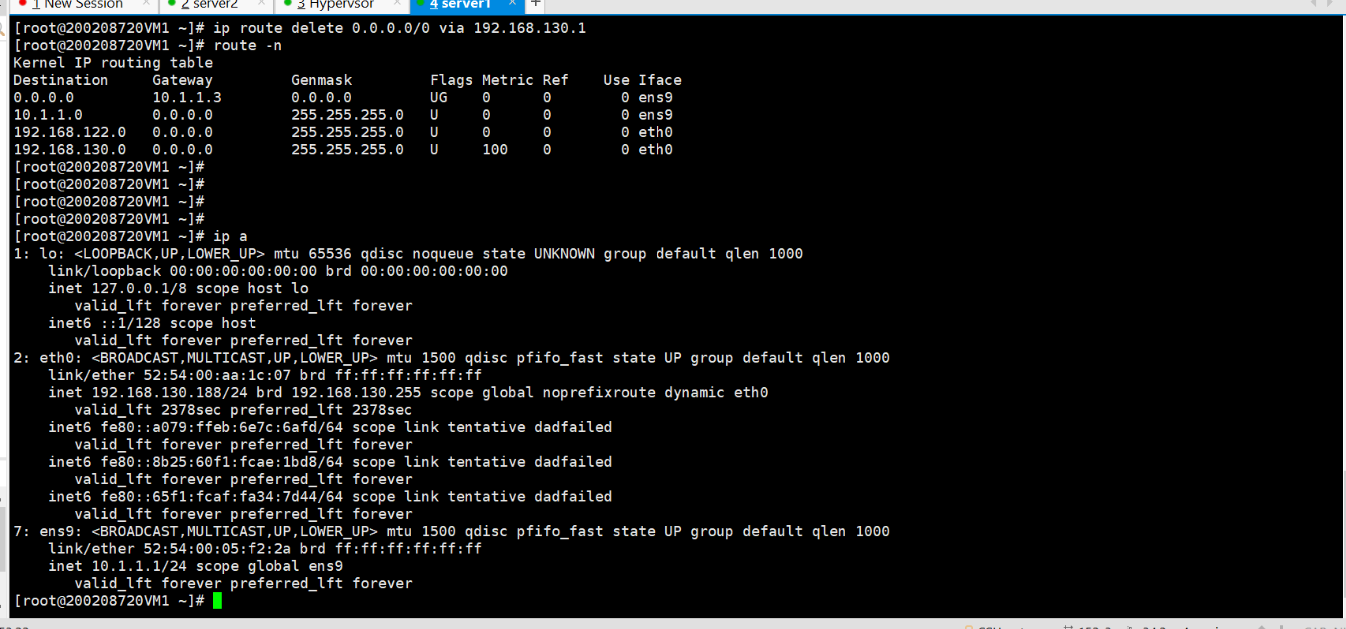
**The public network side of the Router VM is on 50.0.0.0/24 (ens3) subnet**

Here are the Ip addresses configured for the VMs

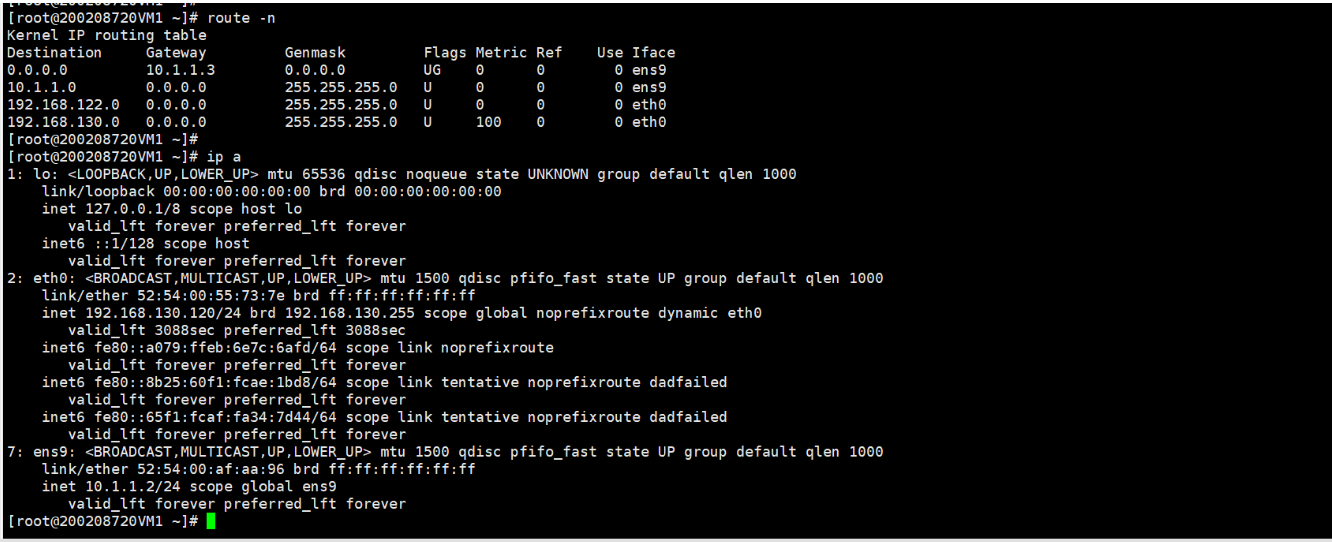


Forwarding table output of Each VMS:

Ppacha\_VM1(server 1): [ ip adresses & forwarding table output ]

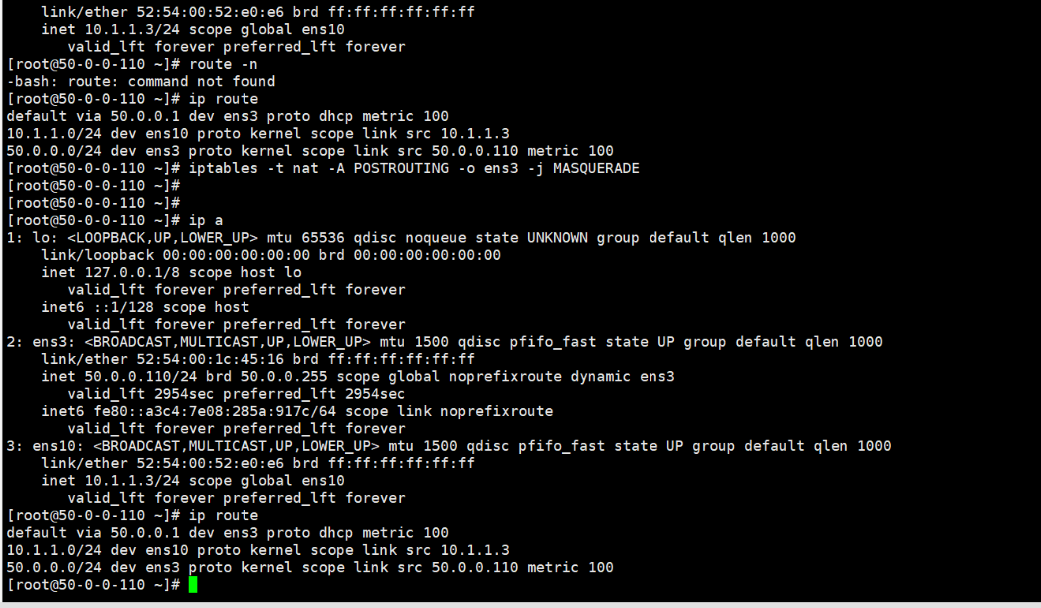


Ppacha\_VM2(server 2) : [ Ip address & forwarding table output ]



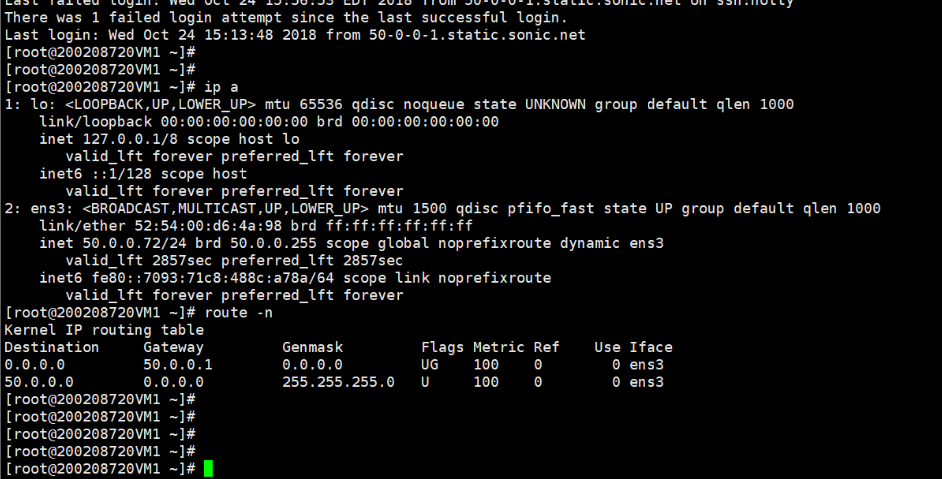
Router (VM3 in our topology)

Ip addresses and forwarding table:



Client(Client in our topology )

IP addresses of interfaces and forwarding table



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**

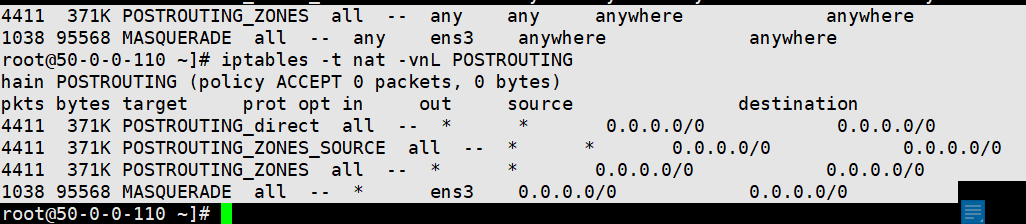
**Ens3 Ip address (Interface in the public network): 50.0.0.110**

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**

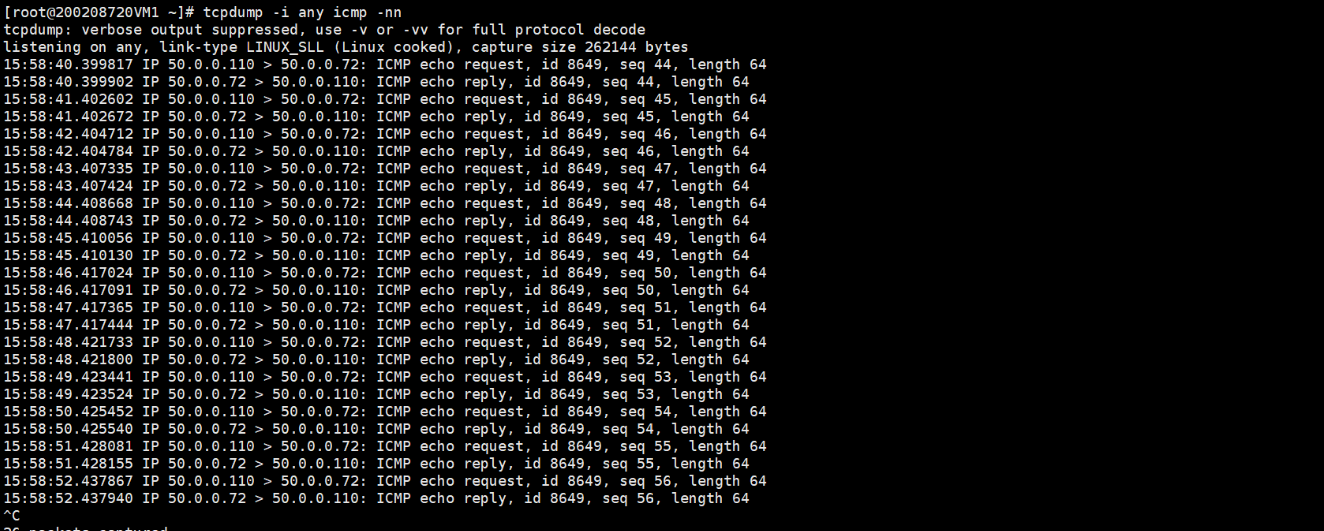


The Iptables rule at the Router side

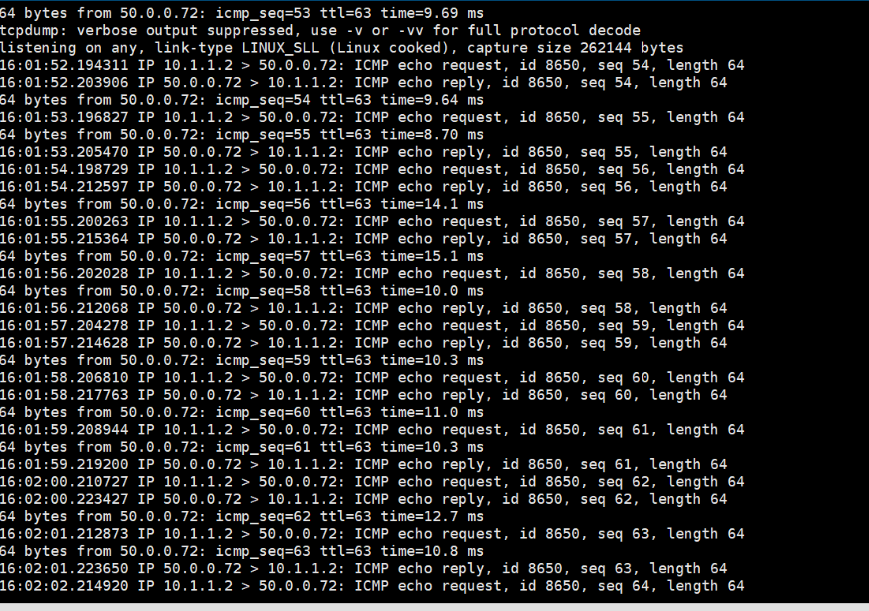
After doing the NAT operation and configuring the default gateway as **50.0.0.1** The server is able to ping the client successfully

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

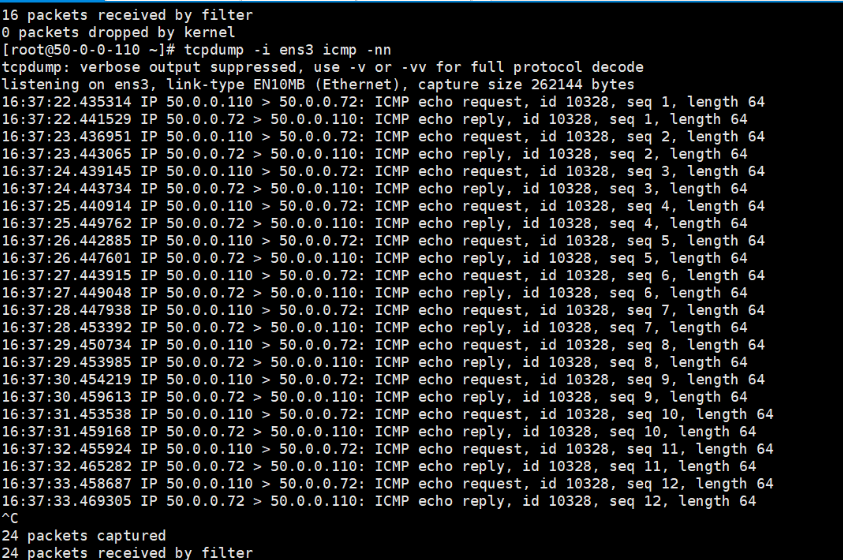
**Here are the Packet captures at the Client side :**



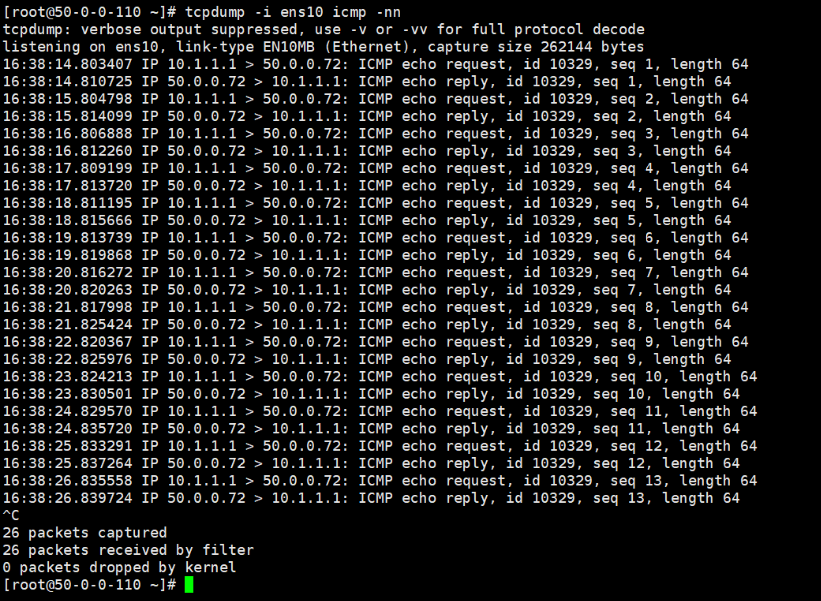
**Packet capture on the Server Side**:



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



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



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



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**

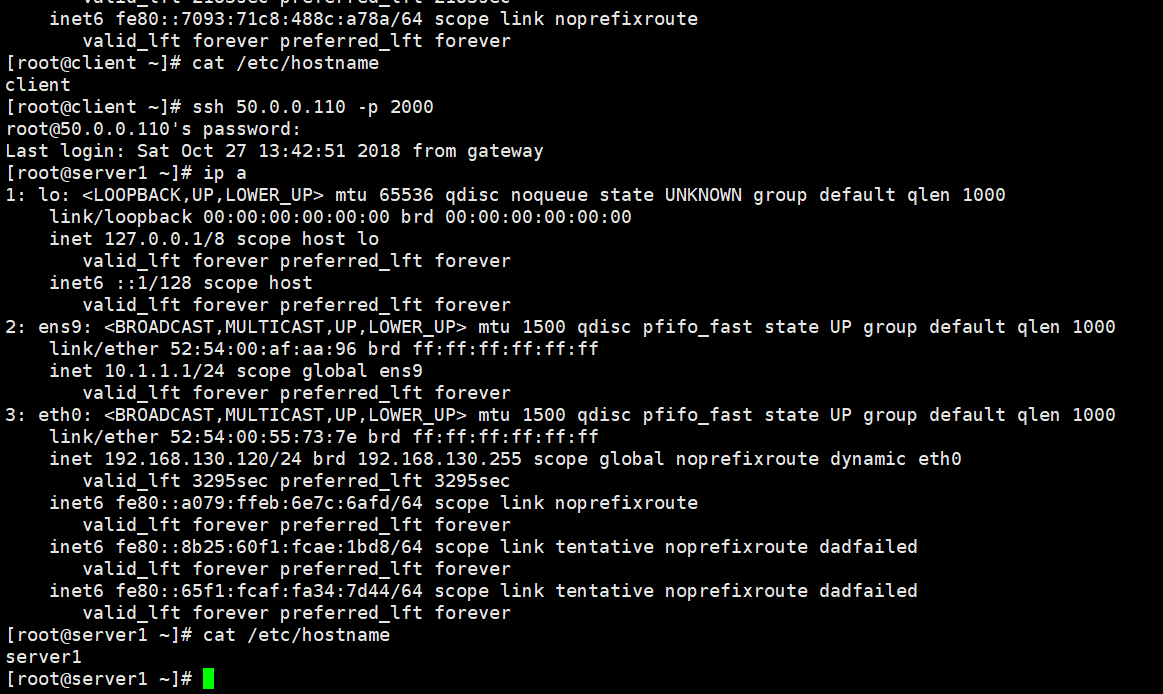
**iptables -t nat -I PREROUTING --dport 3000 -i ens3 -j DNAT --to 10.1.1.1:22**

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

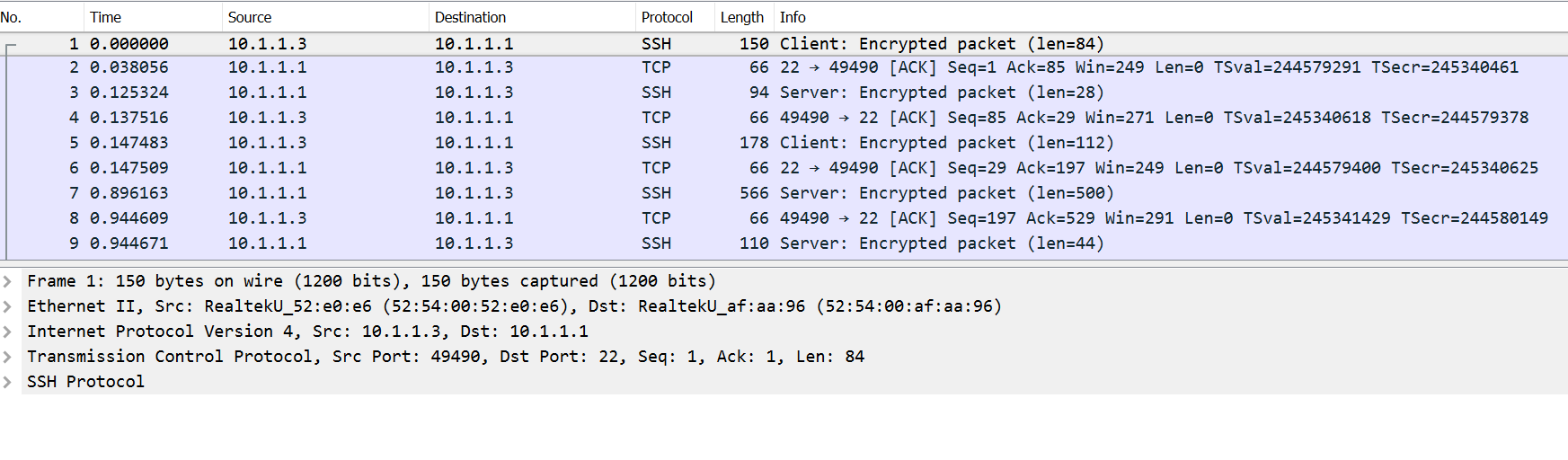
**iptables -I 1 FORWARD -s 50.0.0.0/24 -j ACCEPT**

When we use the ssh 50.0.0.110 -p 2000

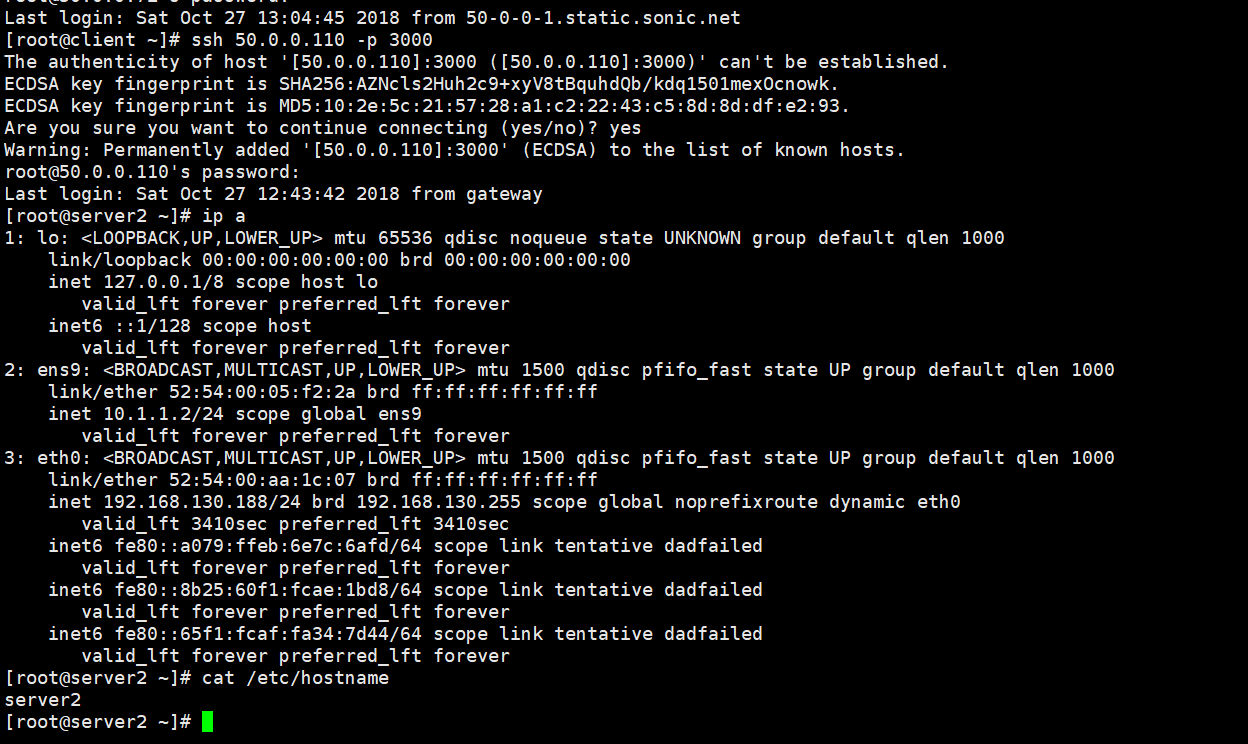
To SSH to server1 (10.1.1.1)



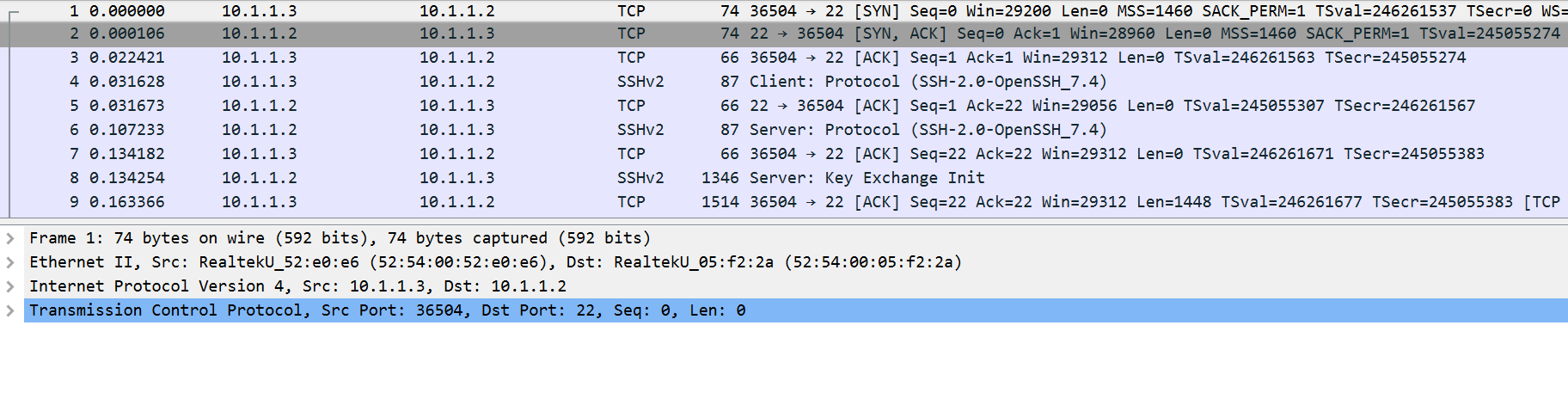
Packet capture at the Server1 side :



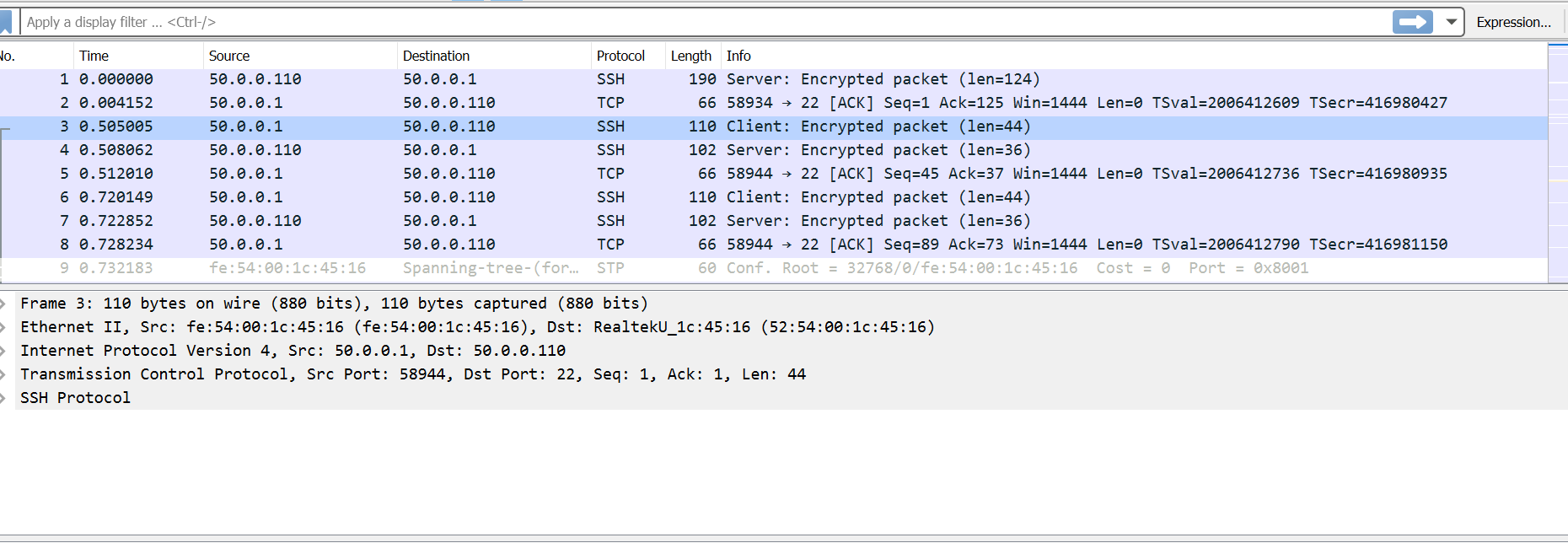
Doing SSH to ssh 50.0.0.72 -p 3000 should do ssh to 10.1.1.2:



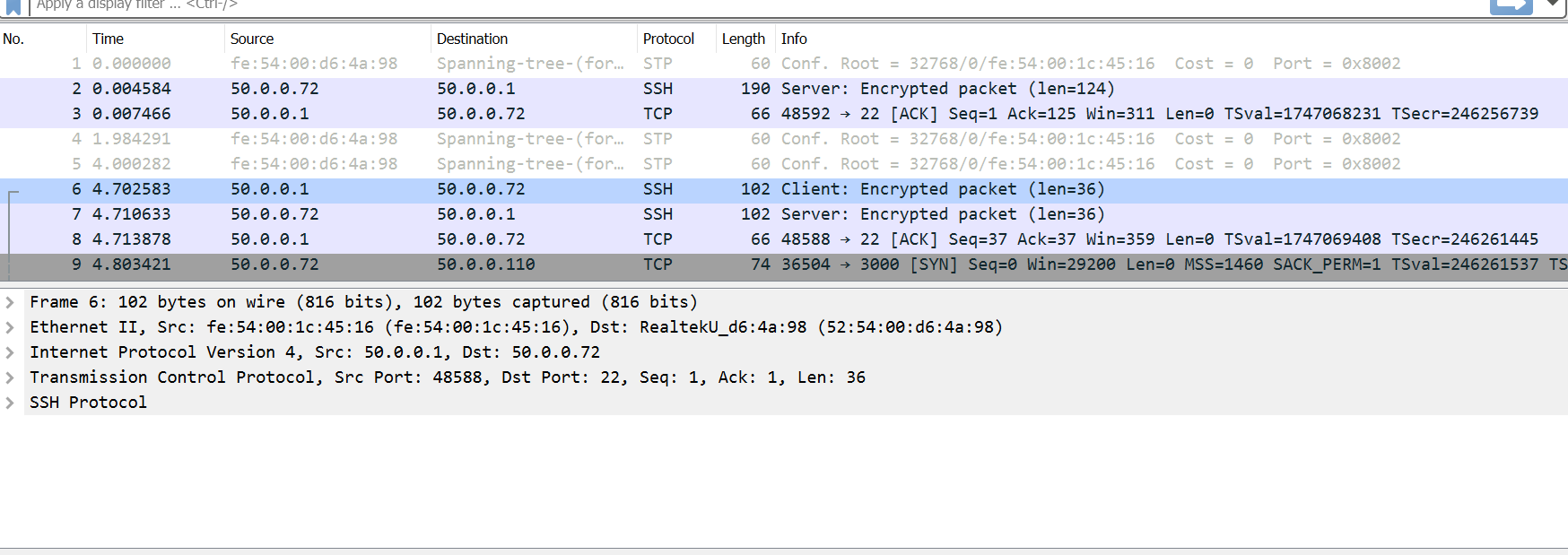
Packet capture at the server2 side :



Packet Capture at the router side :



Packet capture at the client side :

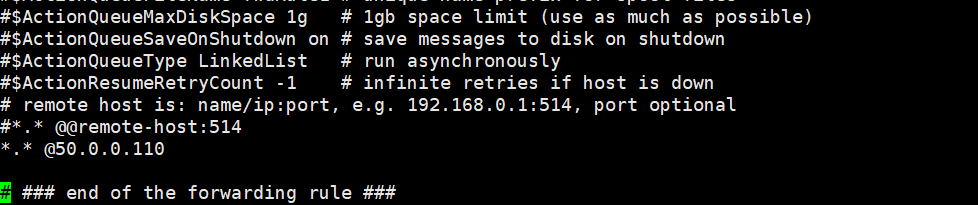


Part (d):

**Load defined:**

**Rsyslog Messages** of the client to the Router which

/etc/rsylog.conf file



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 :

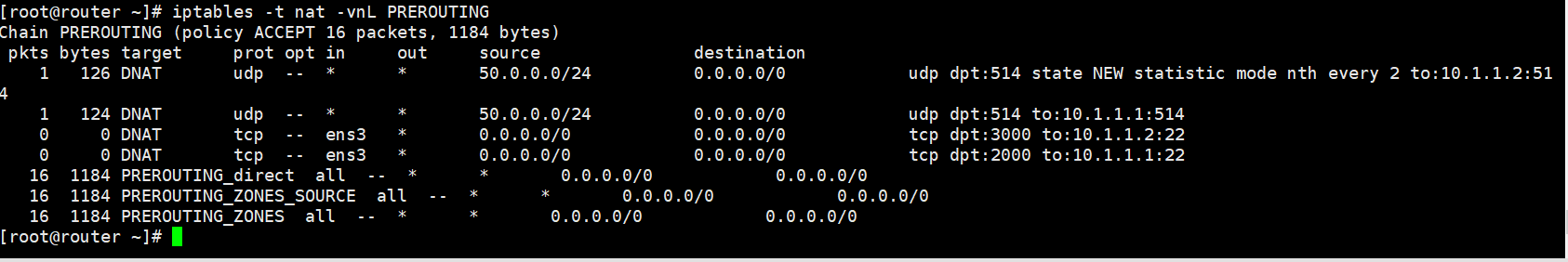
**Rule 1:**

**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:**

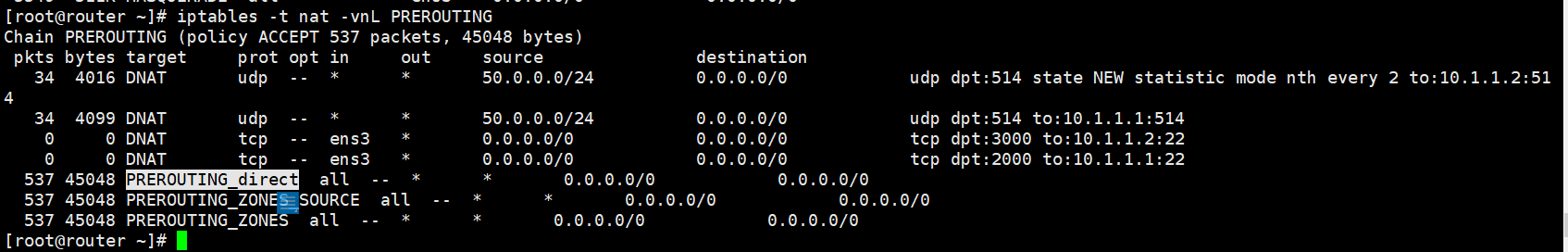
**iptables -t nat -D PREROUTING -p udp -s 50.0.0.0/24 --dport 514 -m state --state NEW -m statistic --mode nth --every 2 --packet 0 -j DNAT --to-destination 10.1.1.2:514**

**Ip tables on the Router VM:**

****

(c) Verification :

From the snapshot of Router Ip tables.



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**

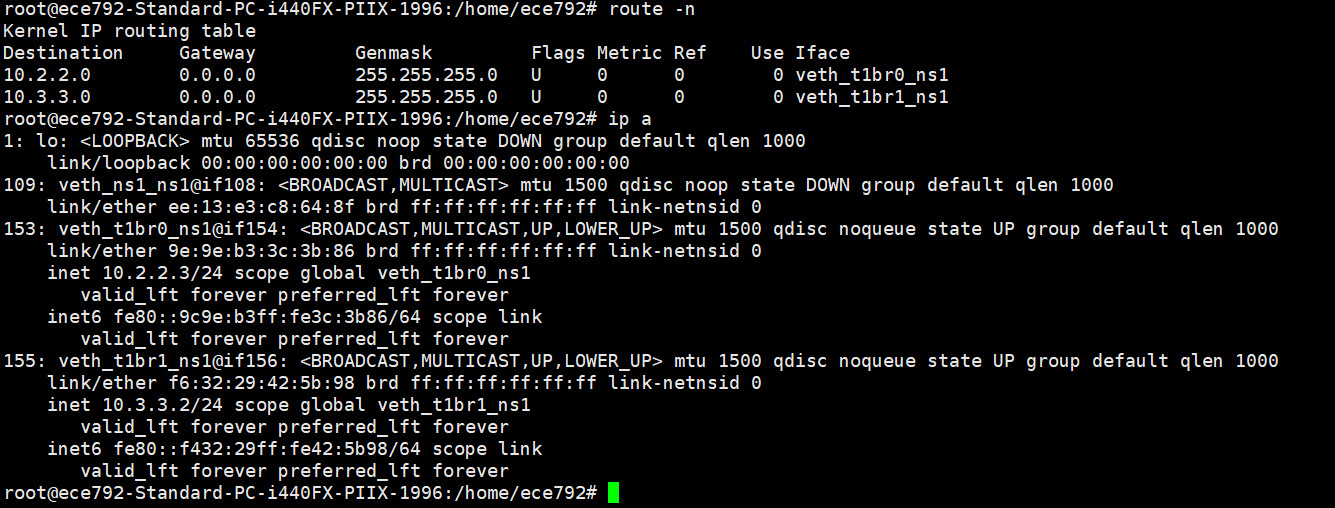
**T1-VM1 –10.2.2.0/24 subnetwork**

**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**

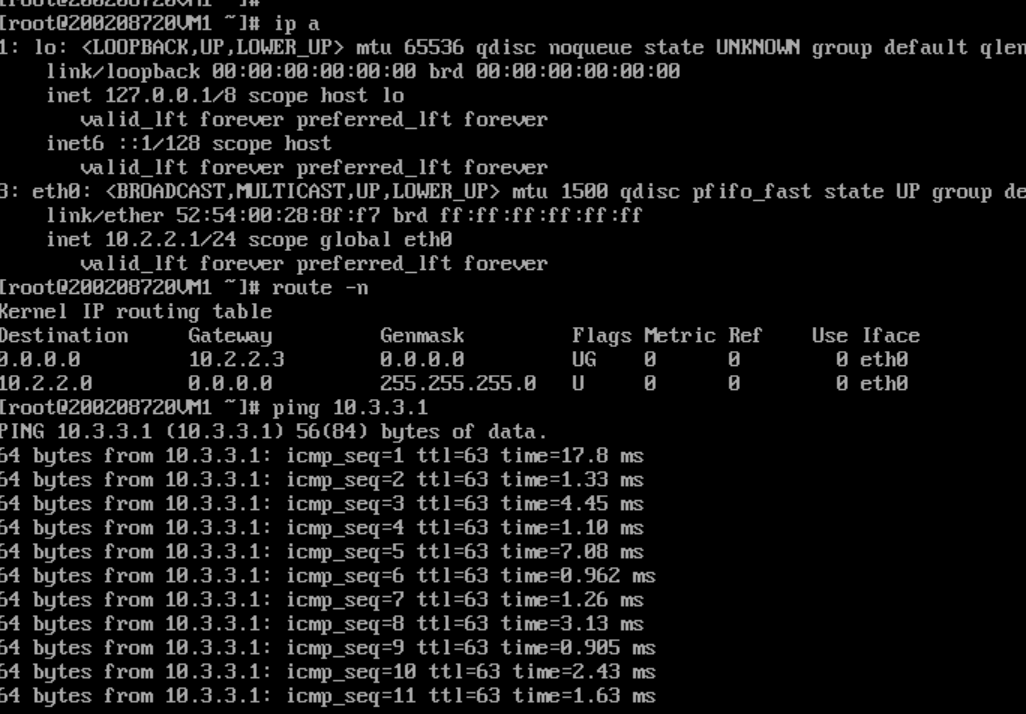
**Interface config and route table of the NS1 :**

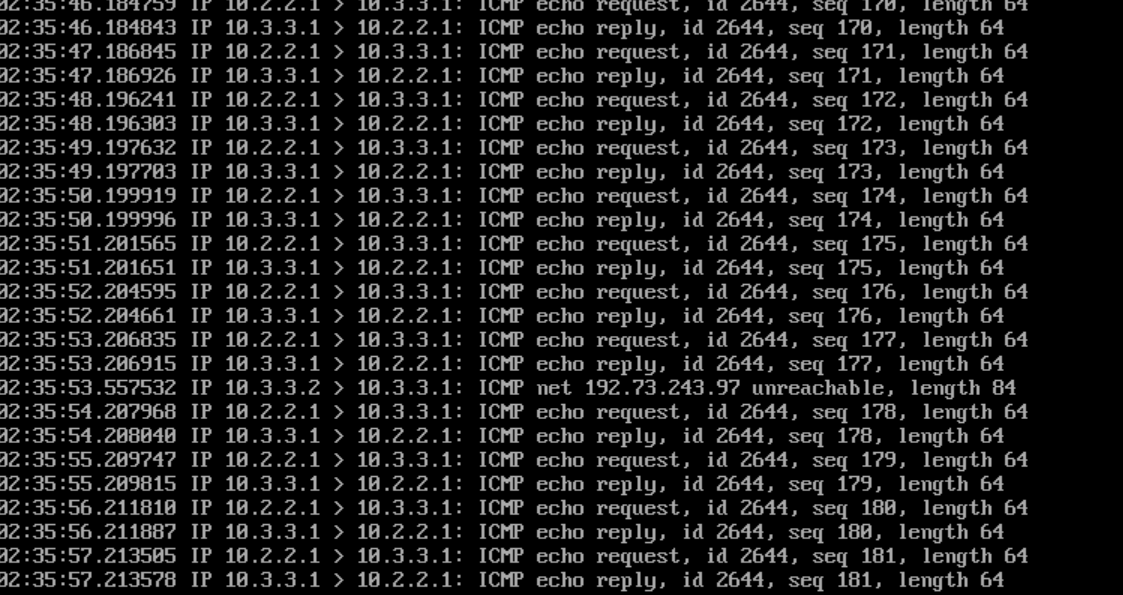
****

**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)

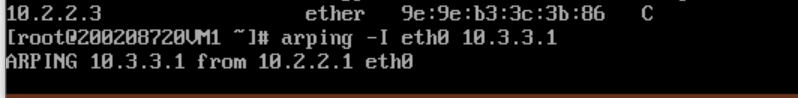


Packet Capture at T1-VM1(eth0) interface:

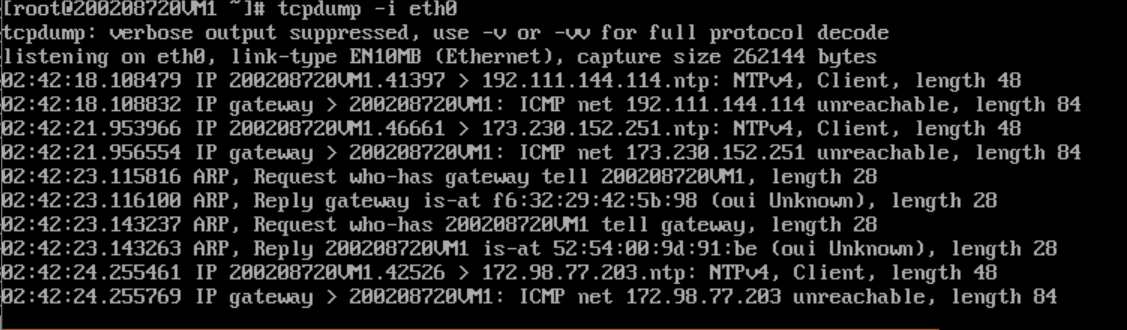
Where as arping is not successful as they are not in the same L2 -domain

And it resulted in no packet capture

Arping -I eth0 10.3.3.1

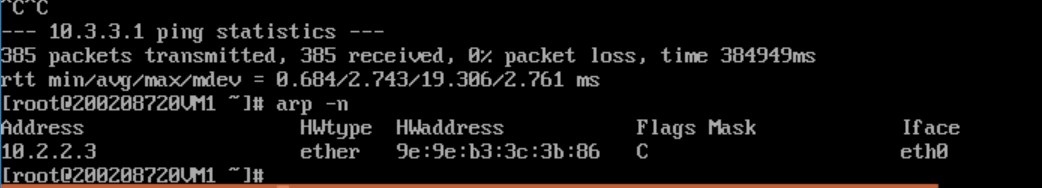
a

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



No arp request from 10.2.2.1 reached 10.3.3.1

Arp table of the T1-VM1:

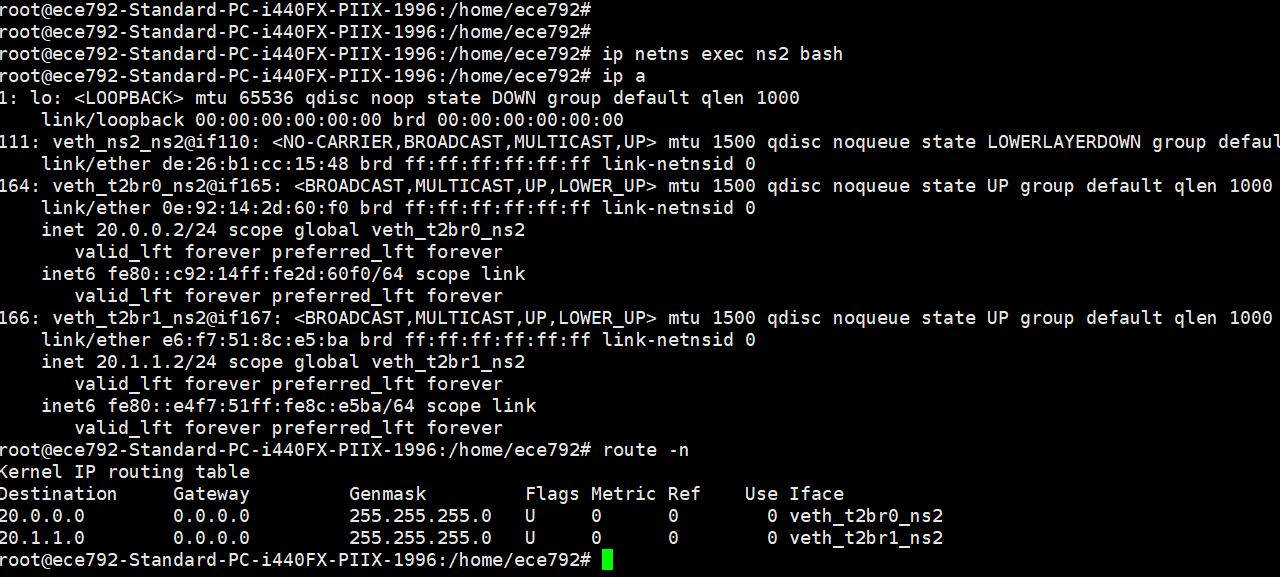


**L2 ISOLATION in tenant2:**

**T2-VM1 –20.0.0.0/24 network**

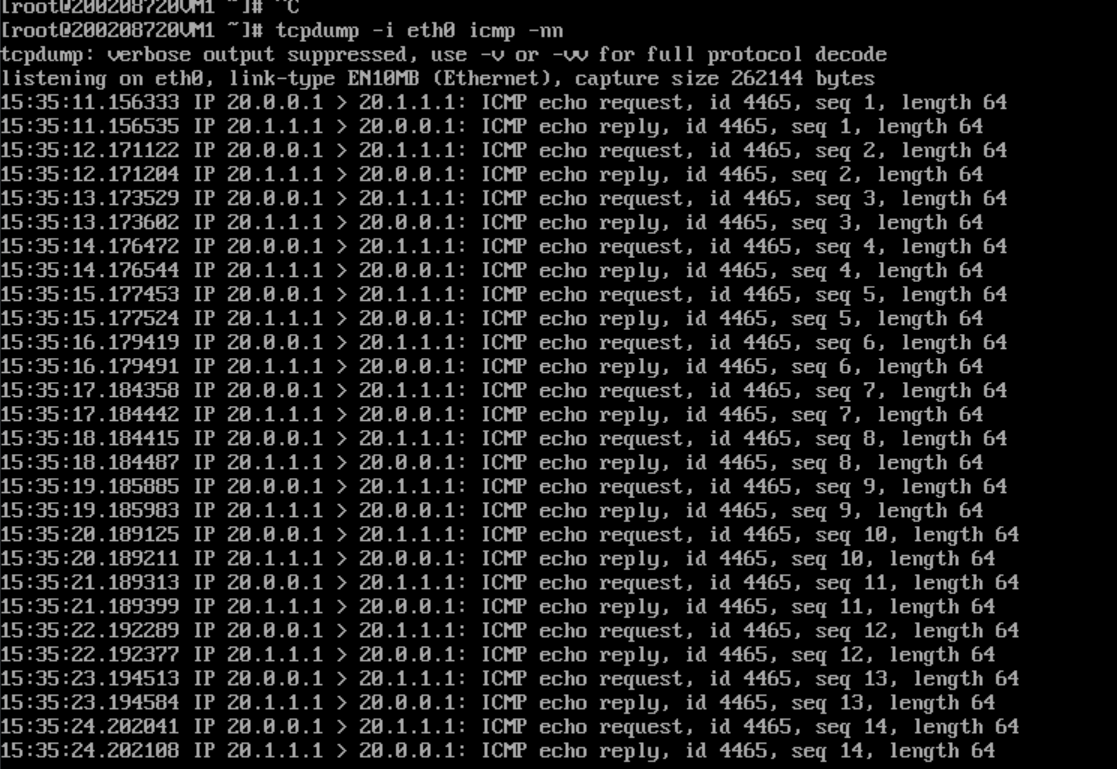
**T2-VM2 --- 20.1.1.0/24 network**

**Interface config of the ns2 :**

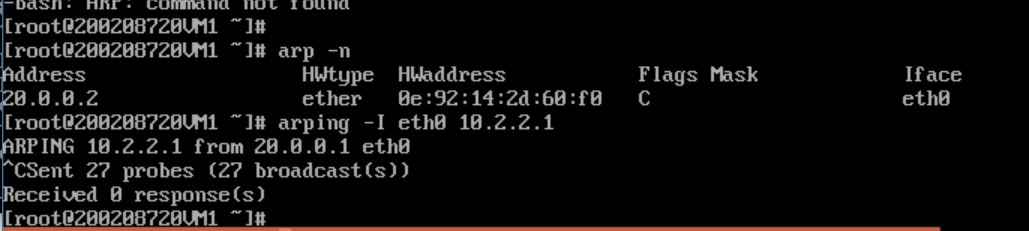
****

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

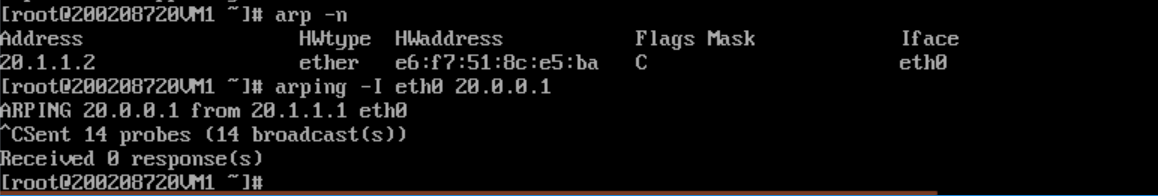
**Packet capture on the T2-VM2**



**Arptable of the T2-VM1:**



**Arp table of the T2-VM2:**



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**

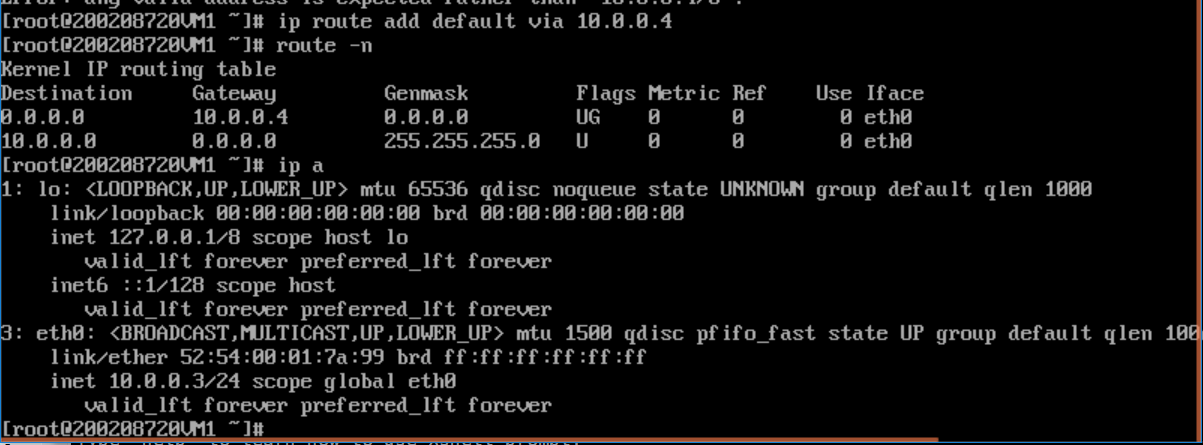
**Veth\_ns2\_prov ---veth pair for NS2 for internet connectivity**

****

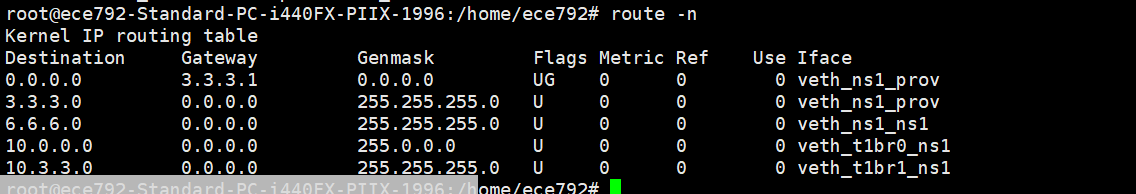
**L3 isolation between two tenants:**

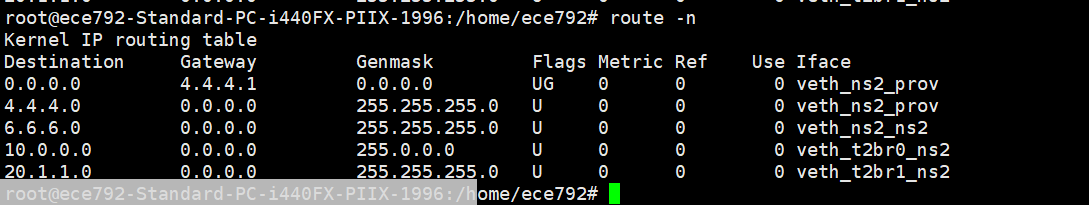
**Config & route table of T1-VM1(Blue Tenant ):**

****

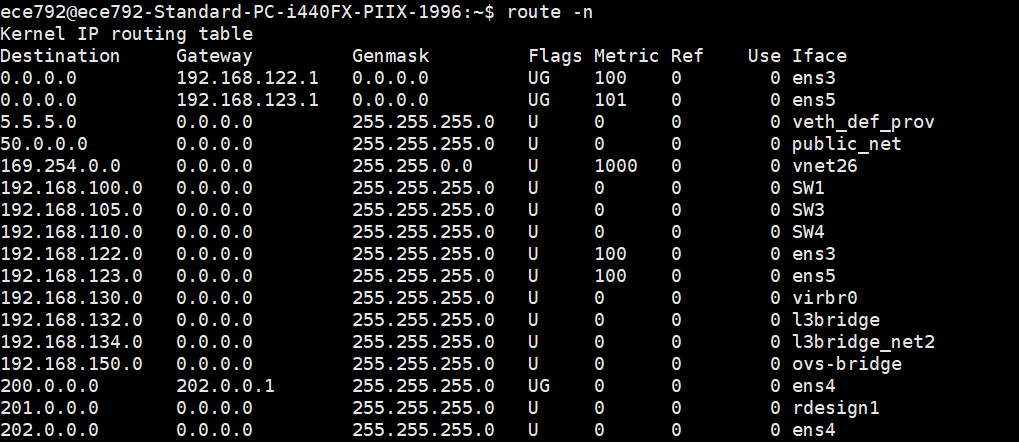
**Config & route table of T2-VM1(Red Tenant)**

**Forwarding Table of Ns1 & Ns2:**

****

****

**Forwarding table of Host hypervisor:**

****

**L3-isolation :**

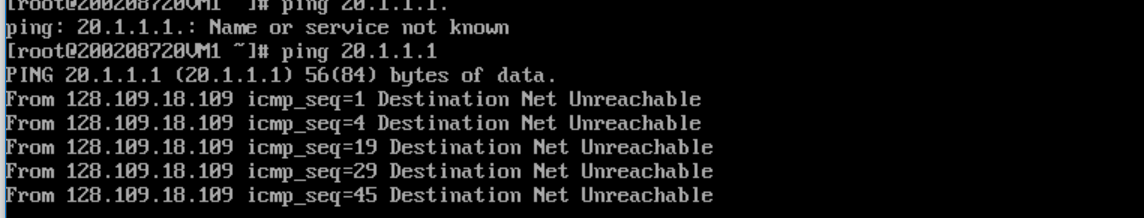
Blue tenant subnets T1-VM1 (10.0.0.0/8) & T1-VM2(10.3.3.0/24)

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

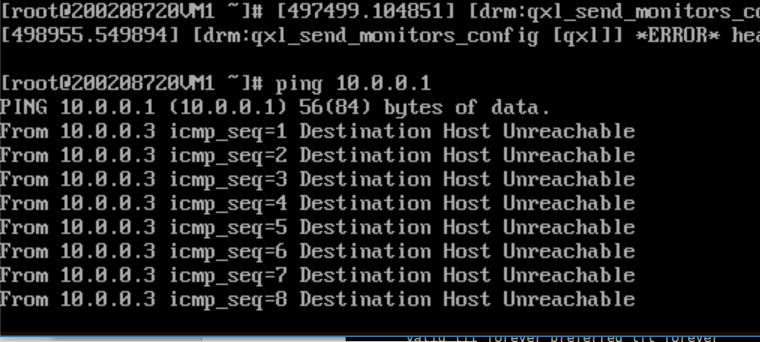
Suppose T1-VM1 (10.0.0.0/8) wants to communicate with T2-VM1(20.1.1.0/24) as the route in NS1 will point to the default gateway which is in host and host doesn’t have any route for 20.0.0.0/24 in its forwarding table so the packet gets dropped at the host.

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.

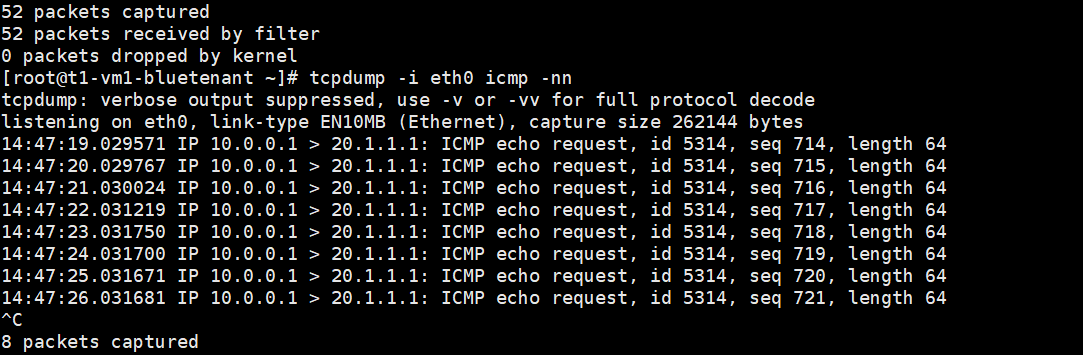
Trying to Ping 20.1.1.1 from 10.0.0.1



Trying to ping 10.0.0.1 from 20.1.1.1



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



**Part(B) :**

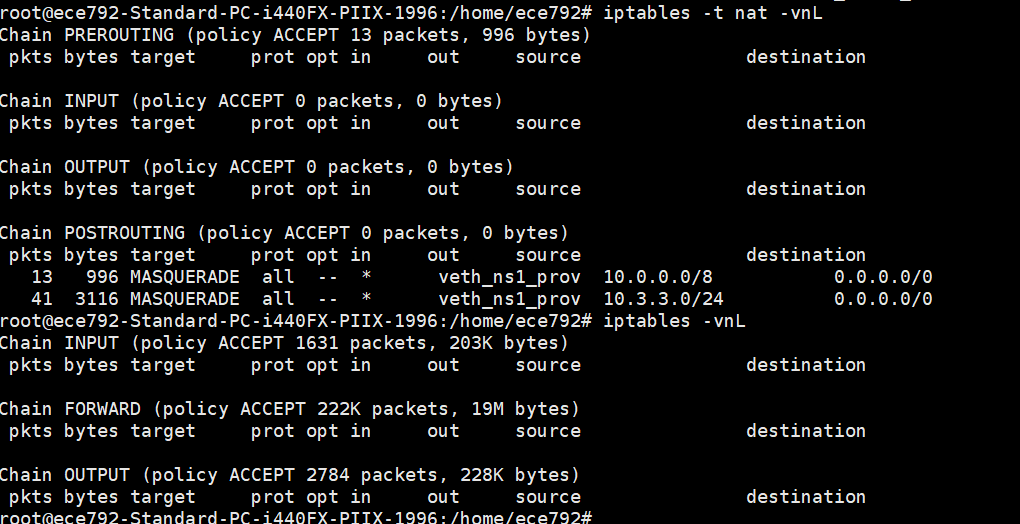
**The tenants having the same subnets 10.0.0.8 should be able to reach to internet**.

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

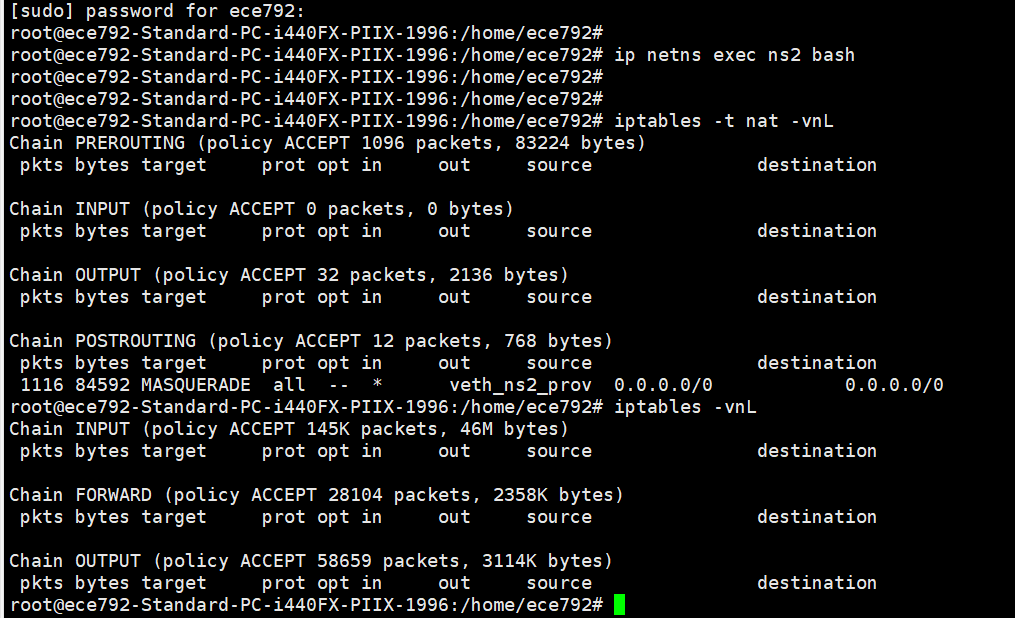
(10.0.0.3)(T2-VM1) ---Red tenant

Ip tables of Ns1 & Ns2:

**NS1 Iptable:**



NS2 IP table:



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**

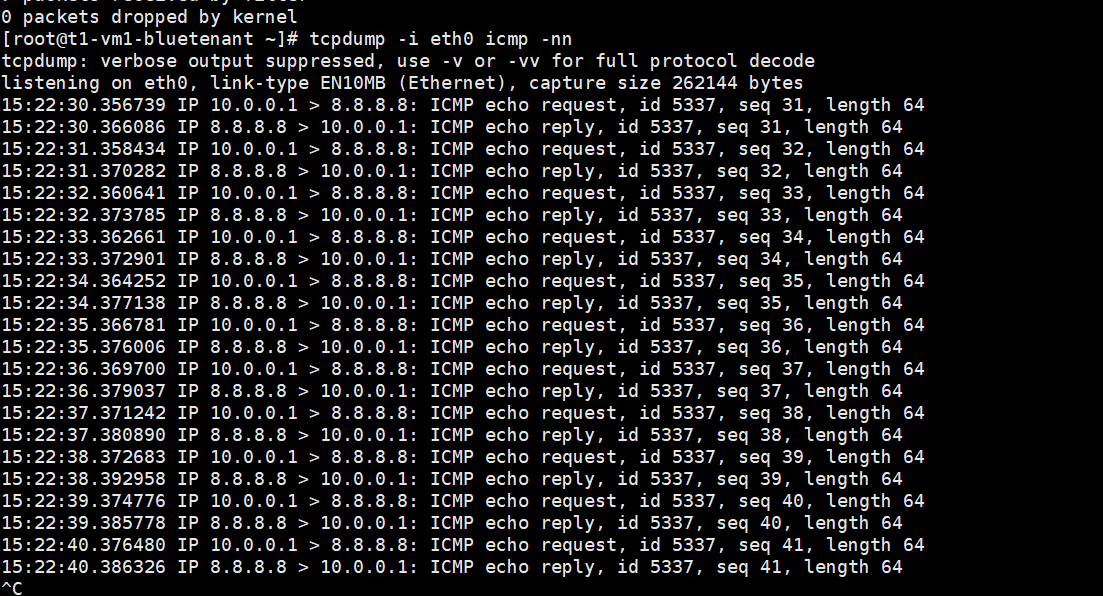
**Applying the rules at the NS2:**

**Iptables -t nat -I POSTROUTING -o veth\_ns2\_prov -j MASQUERADE**

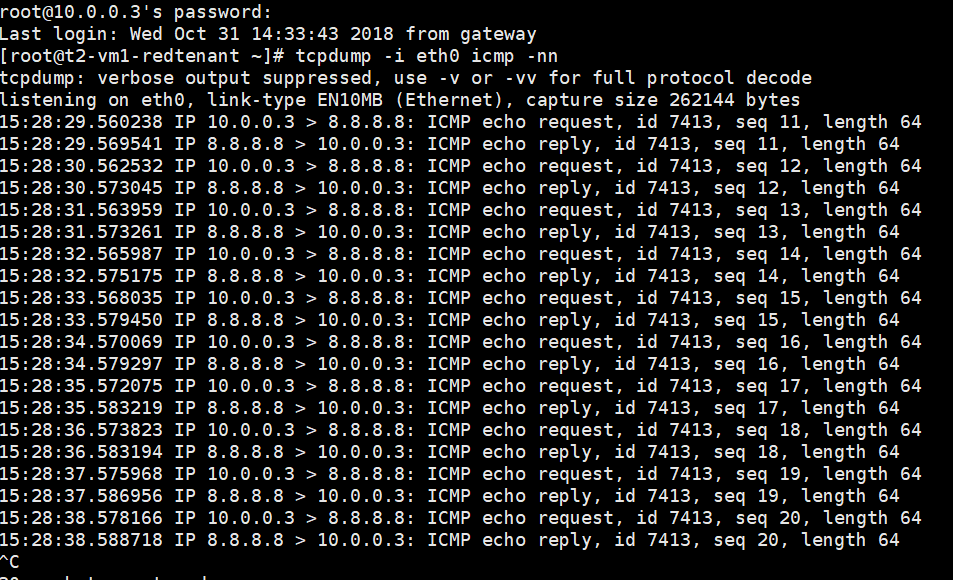
**Veth\_ns1\_prov ---Veth Pair connecting the Ns1 and the host**

**Veth\_ns2\_prov ---- veth\_pair connecting the NS2 and host**

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



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



**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**

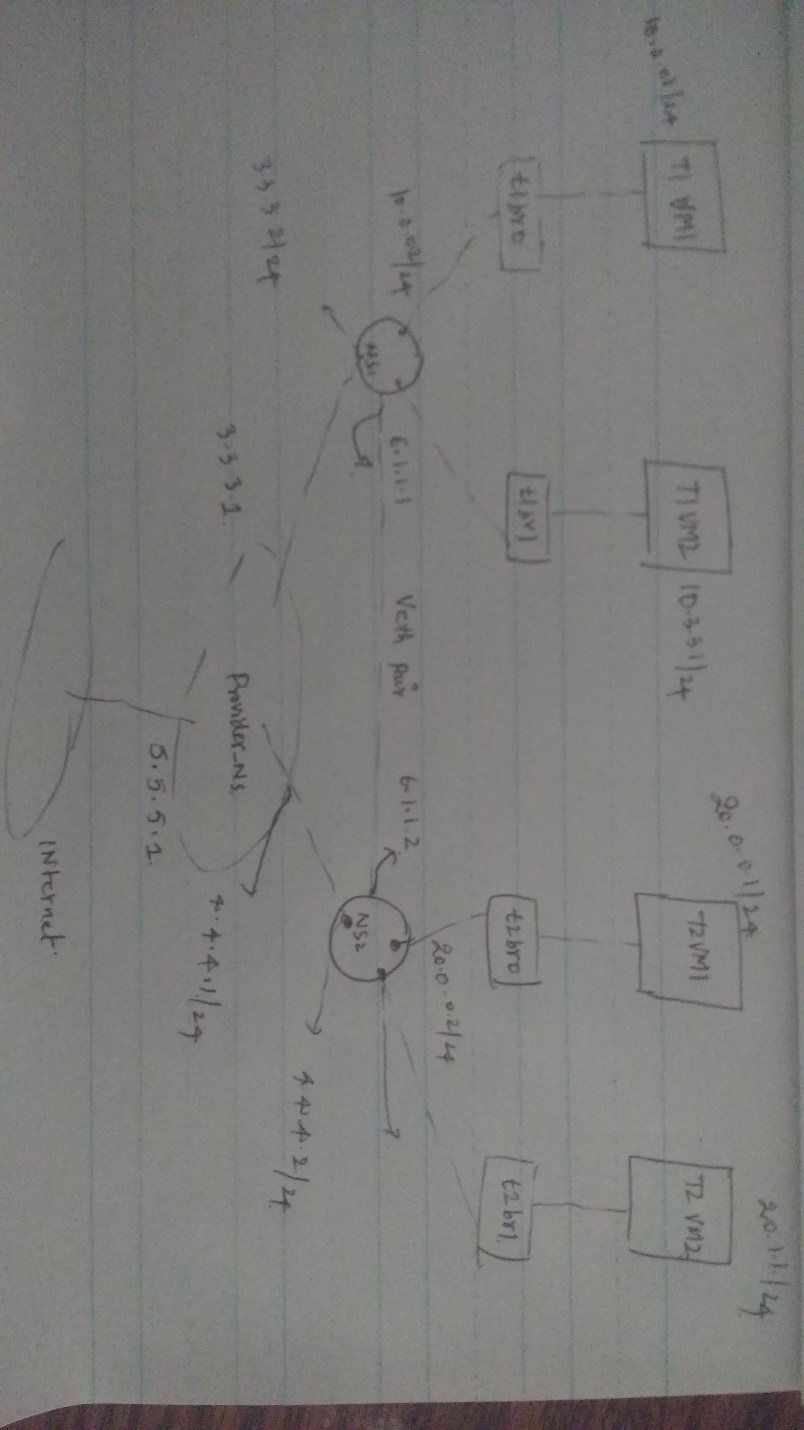
**T2-VM1 ------------20.0.0.0/24 subnet**

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

**Ns1 and Provider Ns are connected via 3.3.3.0/24 subnet**

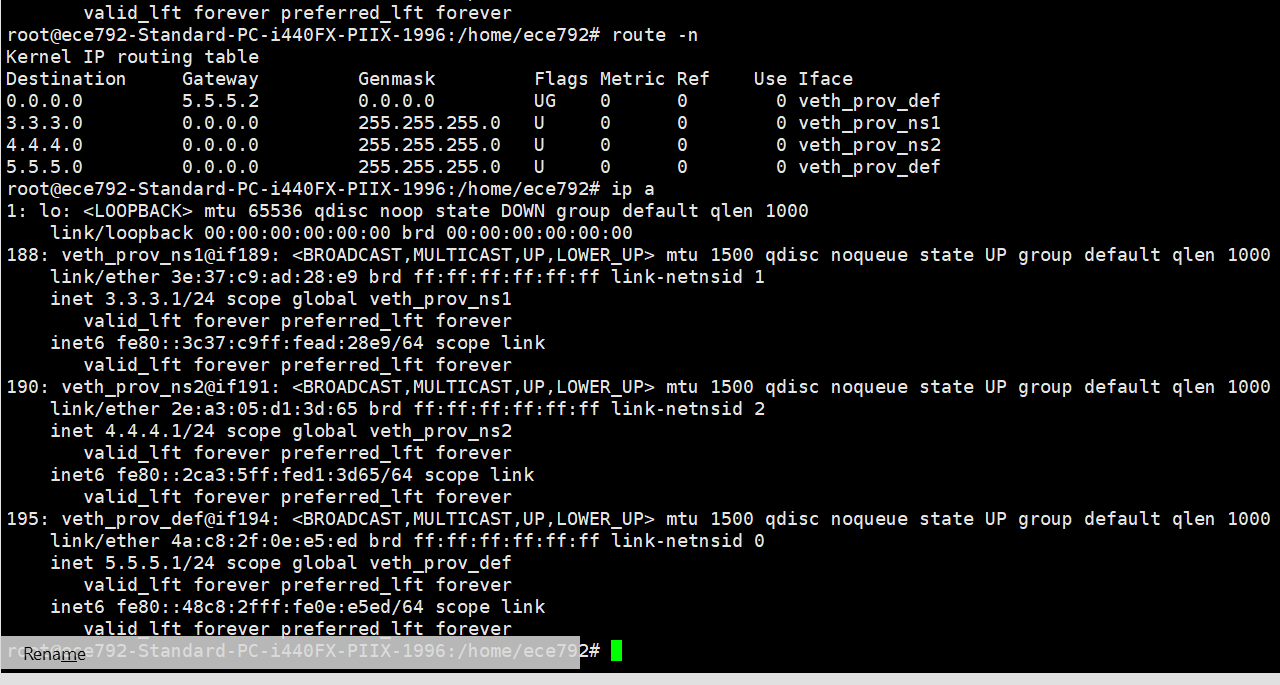
**NS2 and Provider NS are connected via 4.4.4.0/24 Subnet**

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

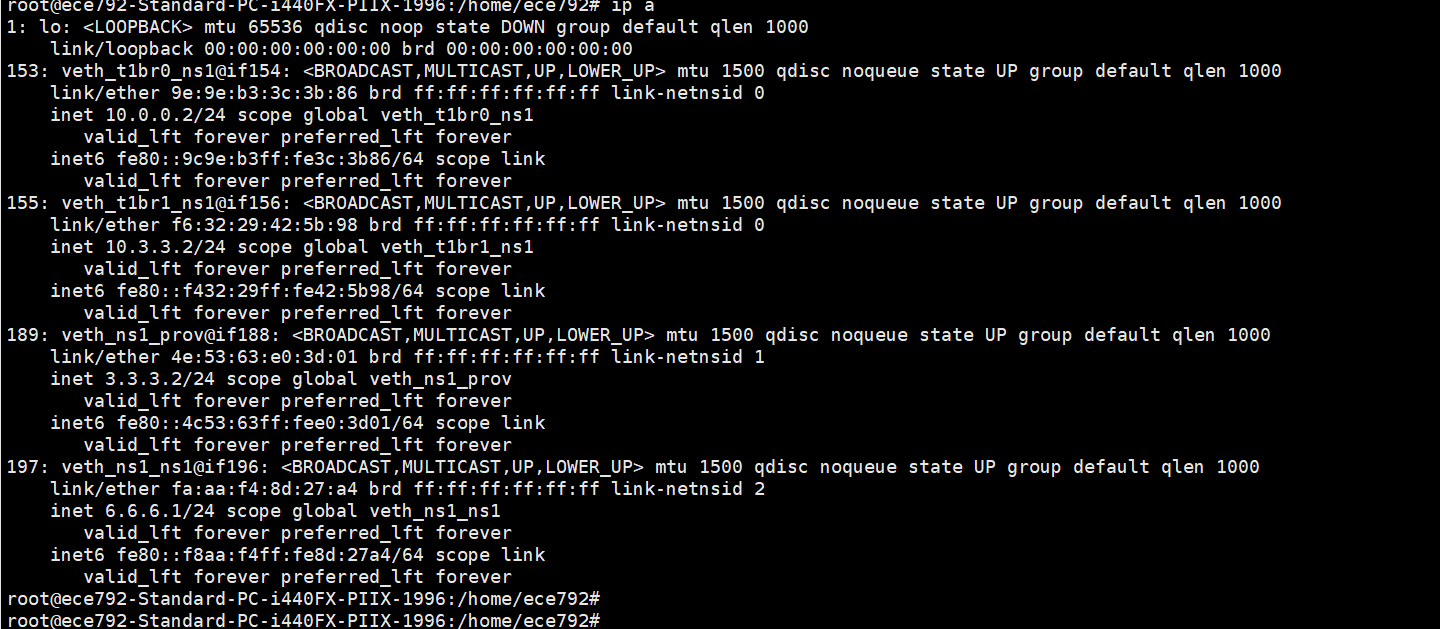
****

**All the interface configs of all the namespaces and VMs**

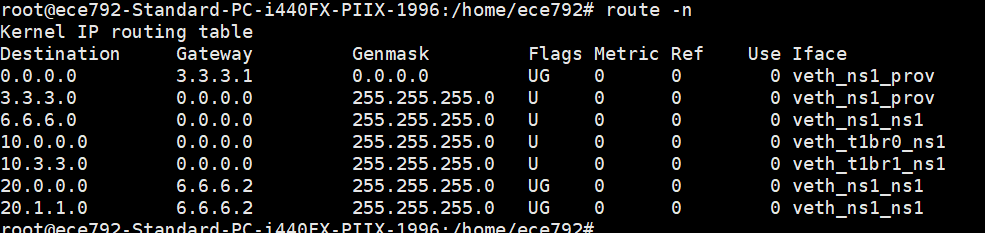
**Provieder\_namespace config:**

****

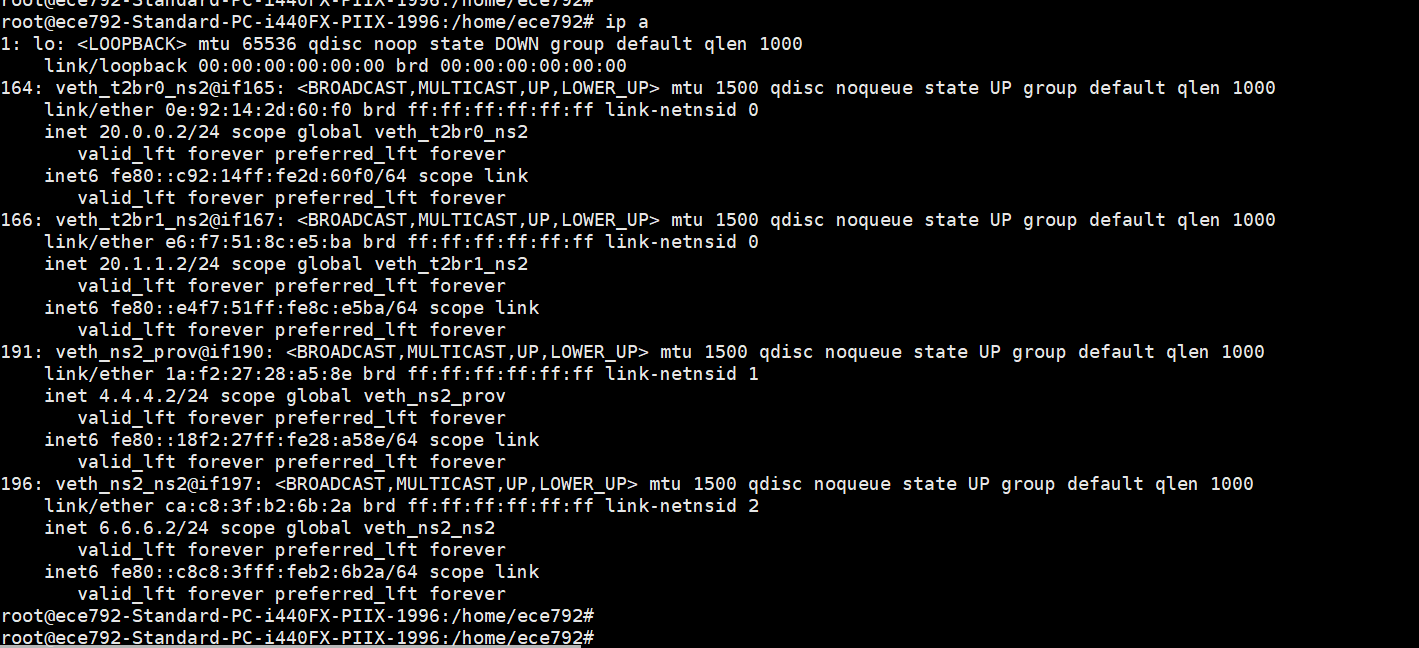
**Ns1 interface config & forwarding table :**

****

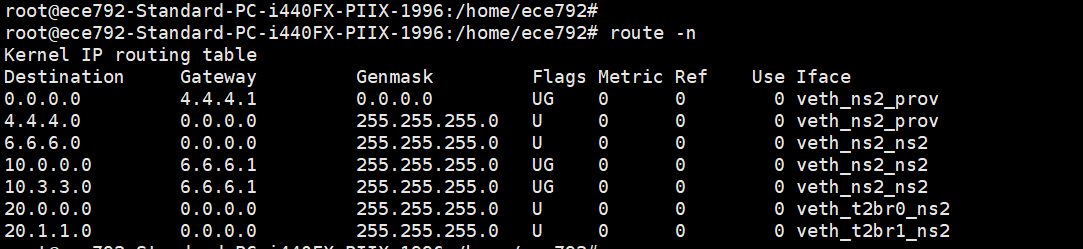
**Ns1 Route table :**

****

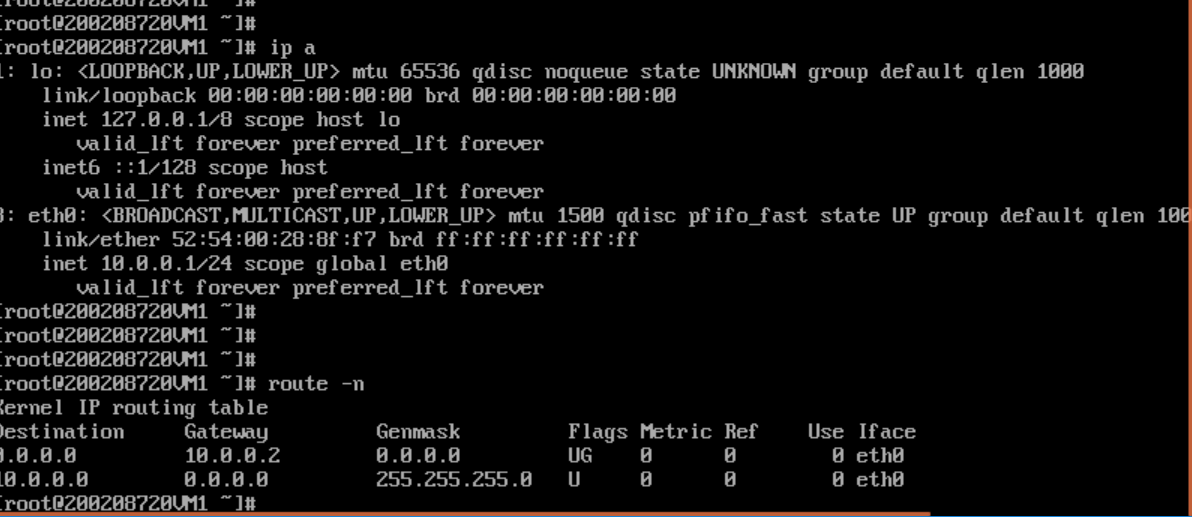
**NAME SPACE 2 config & forwarding table :**

****

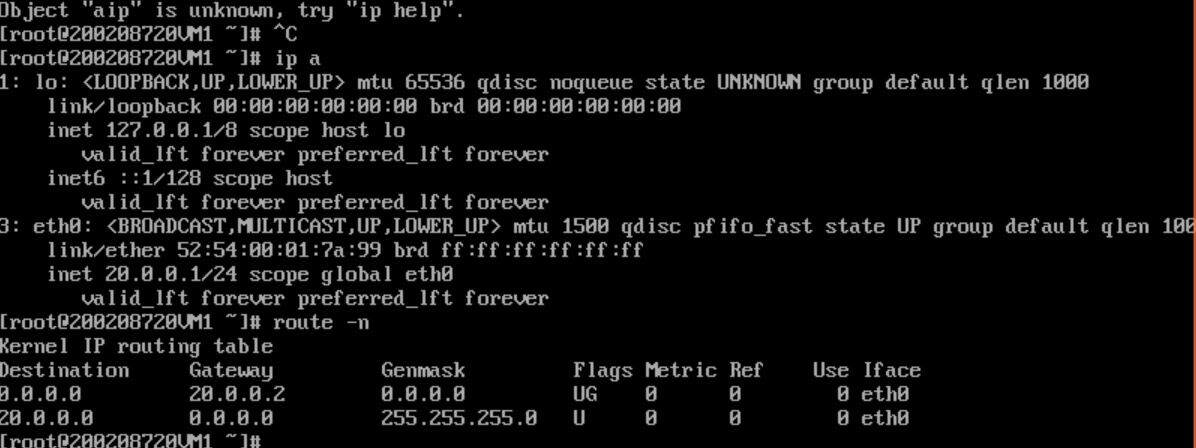
**NS2 Forwarding table :**

****

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

****

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

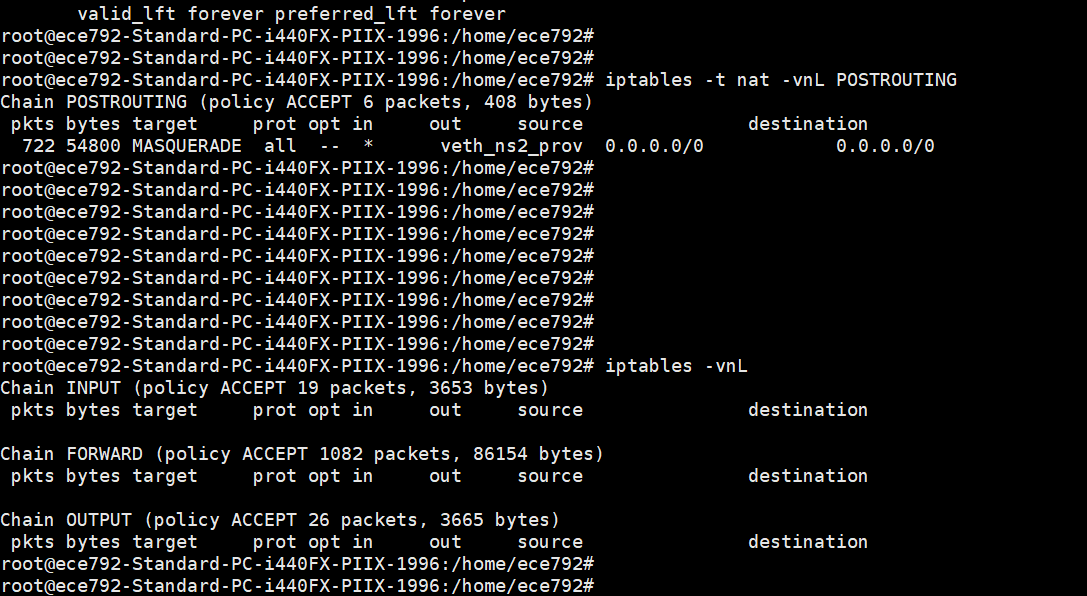
****

**IP tables of the Namesapces :**

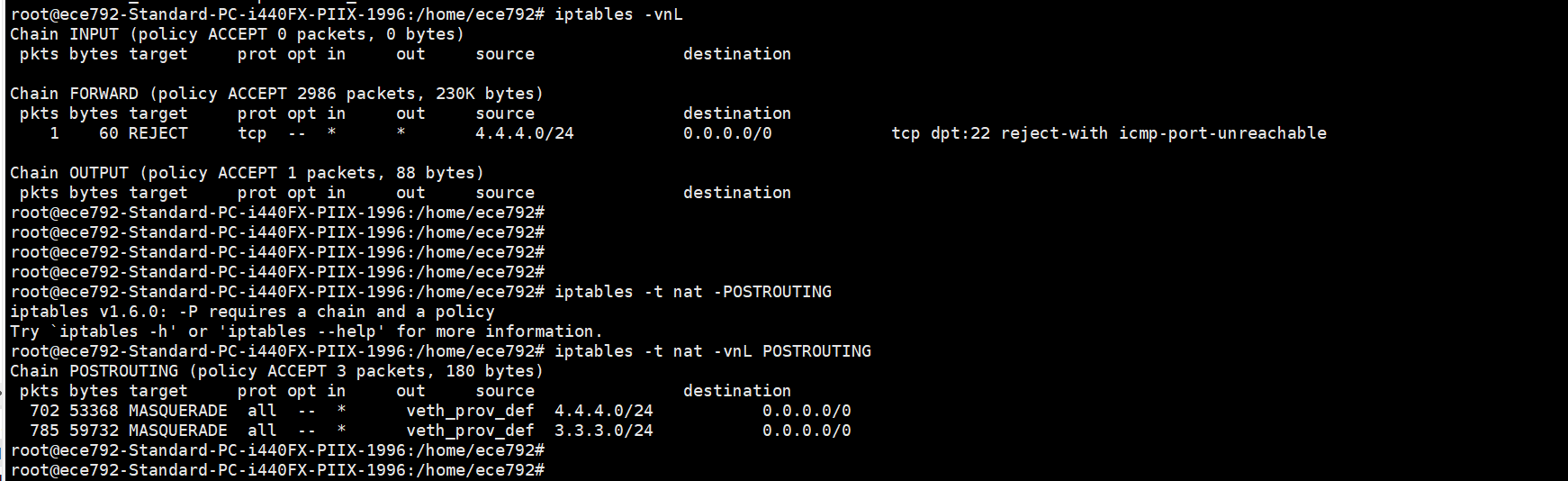
**Iptables of the NS 1:**

****

**Ip tables of the NS 2:**

****

**Iptables of Provider namespace:**

****

1. **Internet policy. Allow ICMP traffic for both tenants. Allow SSH traffic for only the blue tenant.**

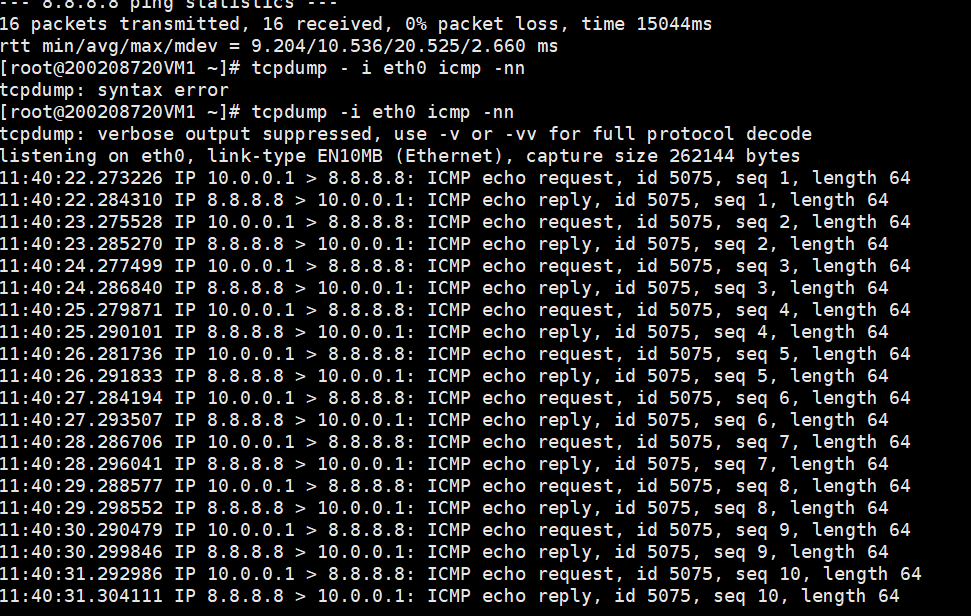
**Checking for the Blue tenants(10.0.0.1) ICMP traffic**

As by default the forwarding policy is allow for all packets

No rule has been applied at **provider\_ns** to allow the ICMP traffic

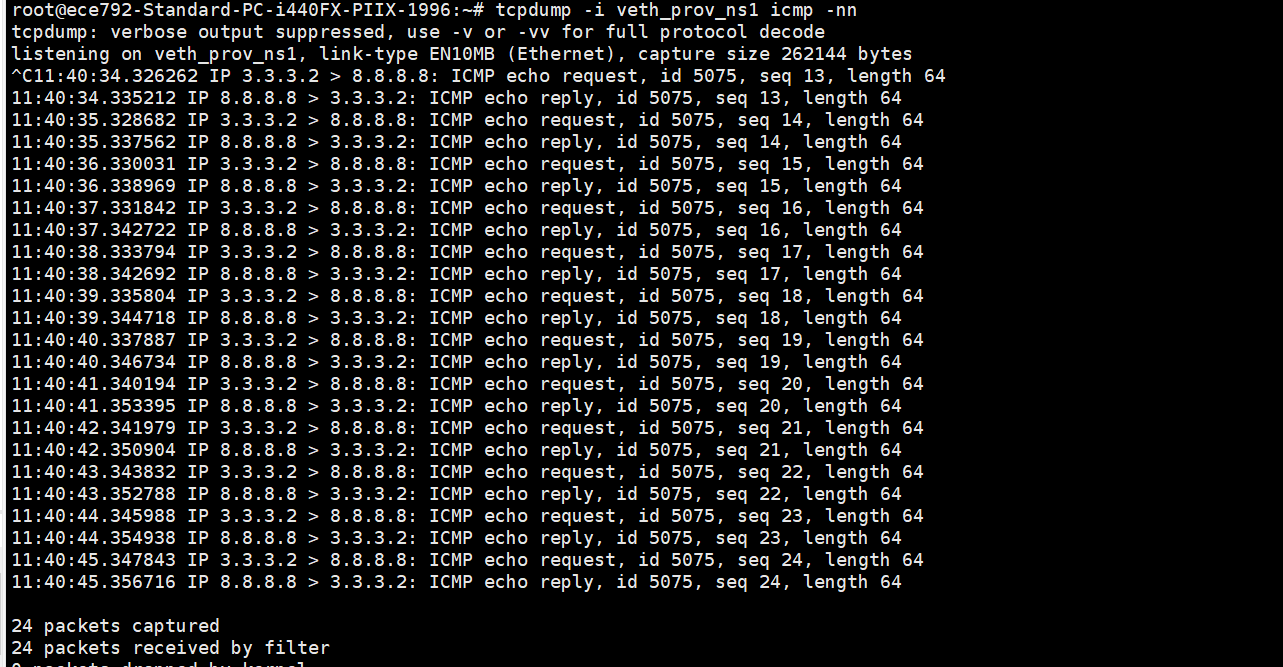
**ICMP packet is successfully reaching the internet :**

**Packet capture at the Blue tenant (10.0.0.1)**

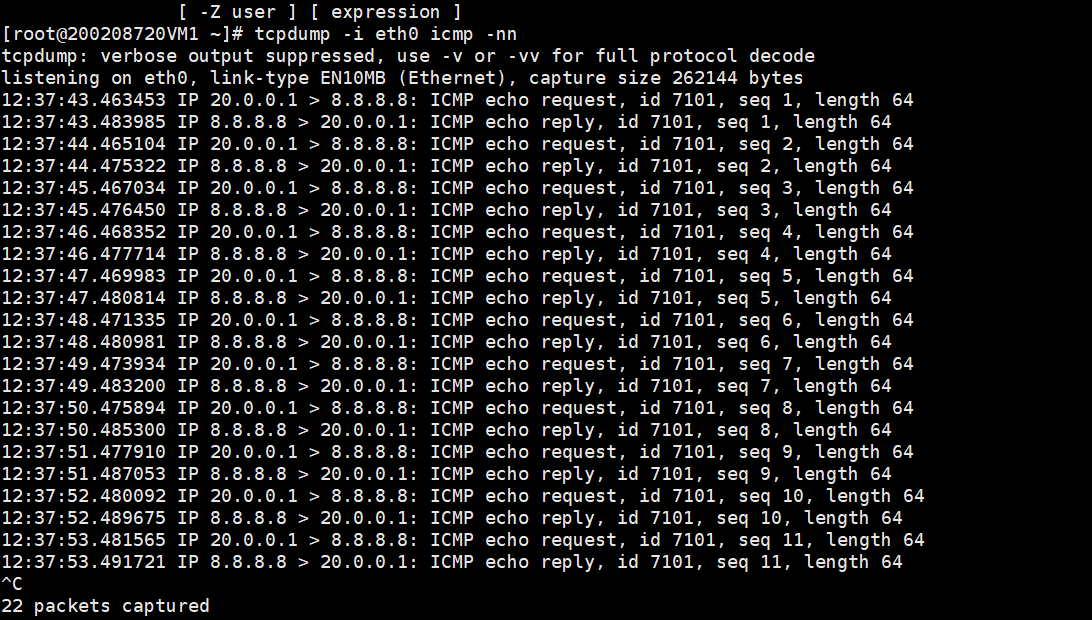
****

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**



**ICMP traffic test for the RED tenant VM (20.0.0.1)**

****

**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**

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

****

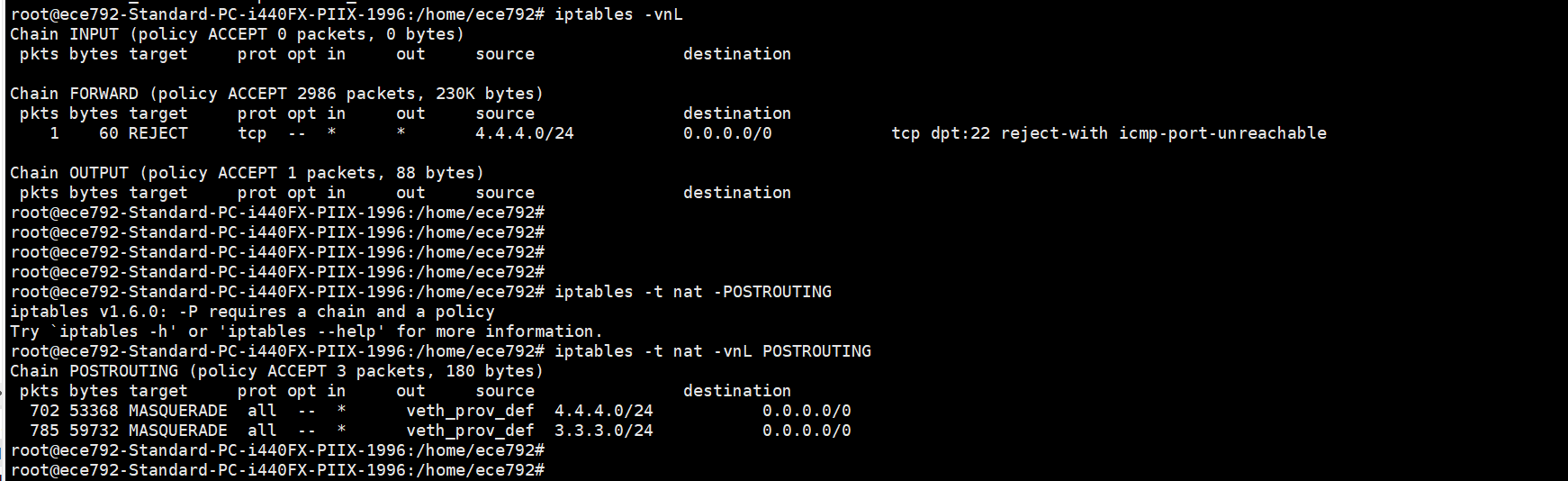
**SSh traffic being blocked at the provider namespace**

**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



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.



(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

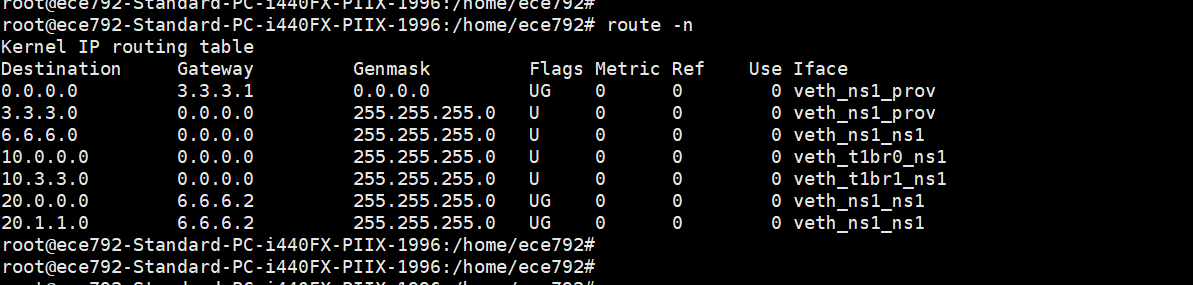
Red Tenants VMS subnets --------------(20.0.0.0/24) & (20.1.1.0/24 ) subnets

**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 :

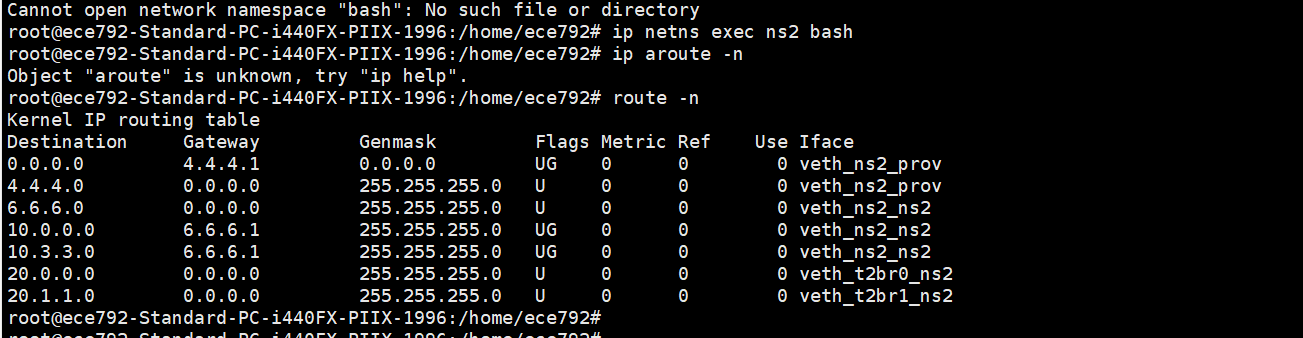


**Route table of Ns2** :

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

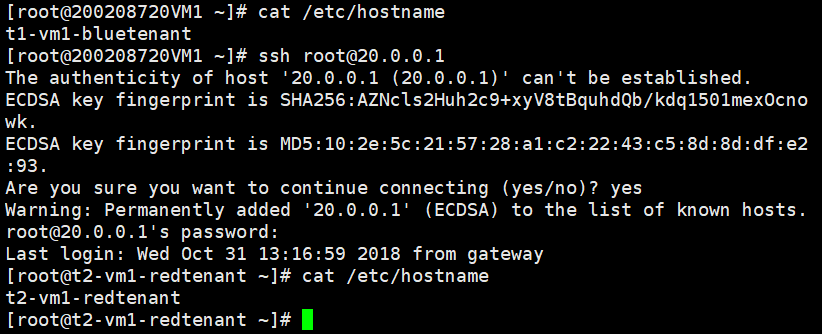
**When red tenant(20.0.0.1) wants to communicate with the blue tenant(10.0.0.1), The traffic will be follow this data path**

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



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

From T1-VM1-blue tenant



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

