FIT9135 Data Communications

Assignment 2

Network Design and Bug Fixing

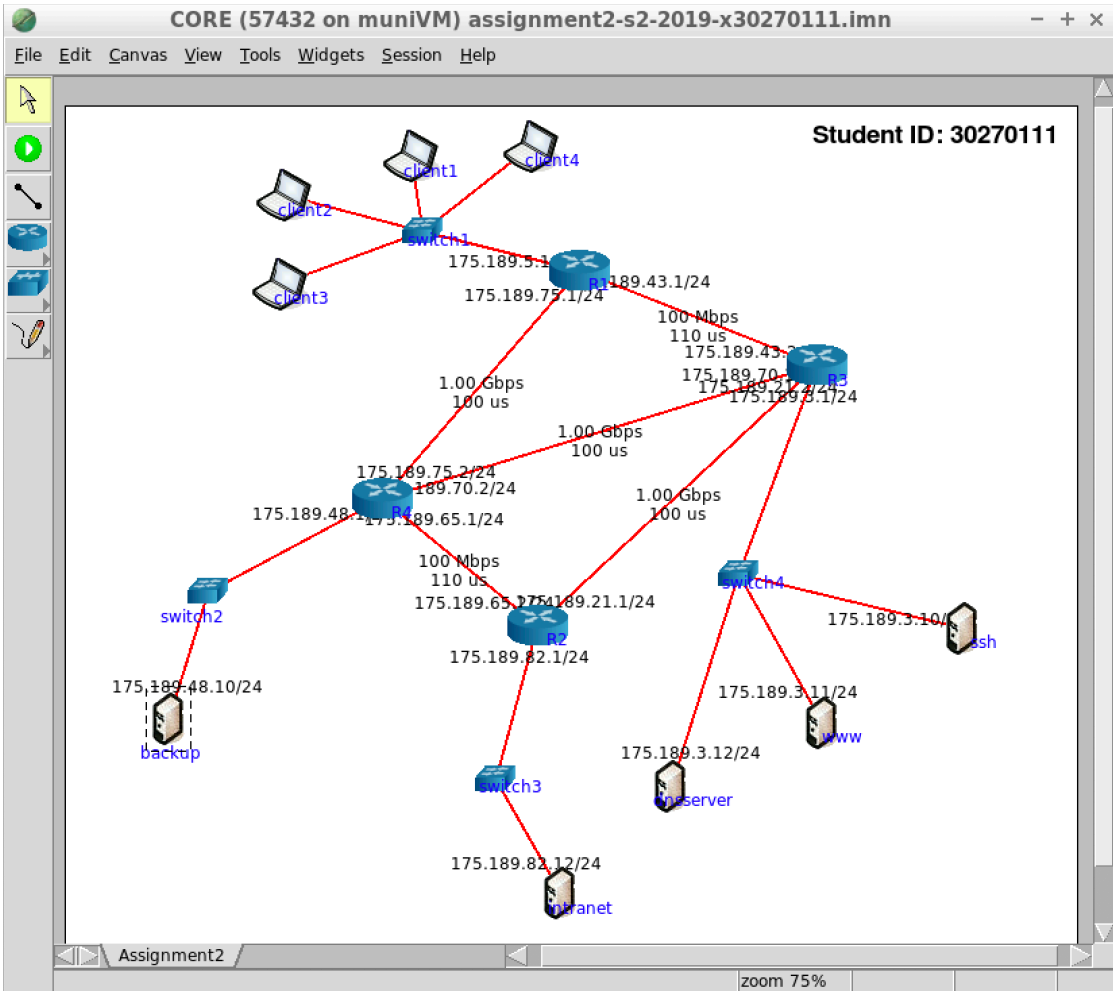
Tutor's name:
Sameela Suharshani Wijesundara
Faculty of Information Technology,
Monash University

Submitted by:
Farhad Ullah Rezwan
ID: 30270111
Submission date: May 27, 2019
Due date: May 27, 2019
FIT9135 Data Communications

Table of Contents

Task A: Setting up static routing tables

The given network for the fictious company currently has four subnets, the clients network (175.189.5.x) the www server network (175.189.3.x), the intranet server network (175.189.82.x) and the backup server network (175.189.48.x).



To make connection between clients, www server and intranet server, static routing table configuration is required for all the connecting routers- router 1 (R1), router 2 (R2), router 3(R3) and router 4(R4). I choose the optimal path considering the speed of the link and latency for setting up the static router configuration for the routers.

Choosing the best route considering link speed:

1. Clients network and www server network: Clients network which is connected to router R1 can communicate with the www server network, which is connected to router R3 by three routing options. If we consider the distance between R1 and the www server network, options are-

   Option 1. → one hop count via router R3 as routers R1 and R3 is directly connected,
   Option 2. → 2 hops via routers R4 and R3, and
   Option 3. → 3 hops via routers R4, R2 and R3.

If we consider the hop count, option 1 is the best route to connect R1 with the www server. However, the link between R1 and R3 has slow bandwidth of 100 Mbps and latency is 110 us or 110 microseconds which may cause bottleneck during huge amount of data transfers using this route. Again, for option 3, link that connects router R4 and R2 has same link speed and delay of 100Mbps and 110us respectively. On the other hand, Option 2 has best route considering the link speed and latency which is 1Gbps and 100us respectively throughout the links between its two hops. For this reason, I choose option 2 as the route between clients network and www server network.

2. Clients network and intranet server network: Considering the latency level and link speed, the best route to connect clients network (connected to router R1) and intranet server network (connected to router R2) is via routers R1 to R4, R4 to R3 and R3 to R2. All of these connections have higher bandwidth of 1Gbps and lower latency of 100us microseconds compared to alternative paths those have links with lower bandwidth of 1Mbps and higher latency of 110us.
3. Intranet server network and www server network: Considering the link speed latency and also the distance or hop count, the best route for connecting intranet server network (connected to R2) and www server network (connected to R3) is the direct link between routers R2 and R3. Here, the bandwidth for this link is 1Gbps and latency is 100us.

Setting up the configuration of static routing table:

For changing the static routing table for each router, it is required to make changes in the static route option which appear in the core simulator when a router is double clicked and then clicked in services.

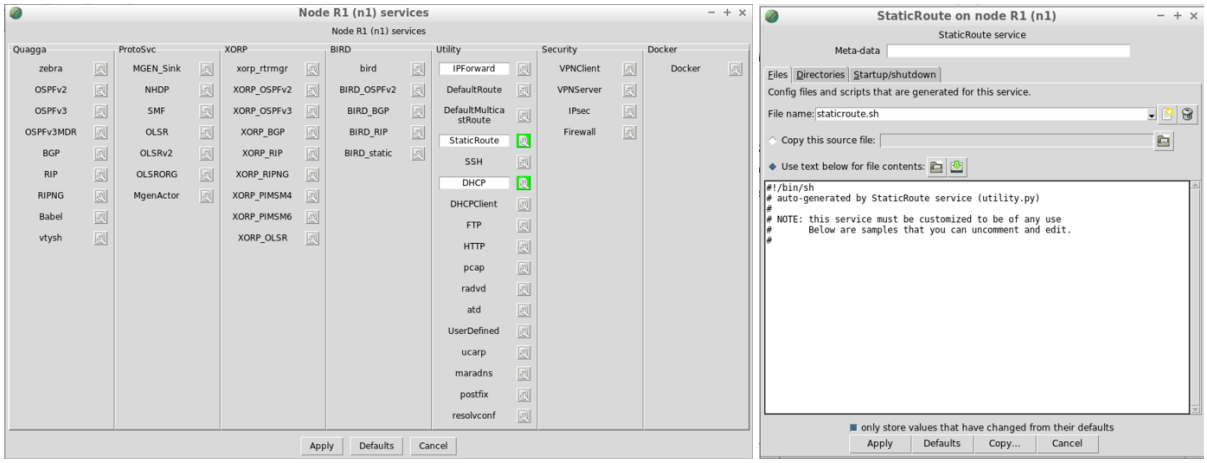
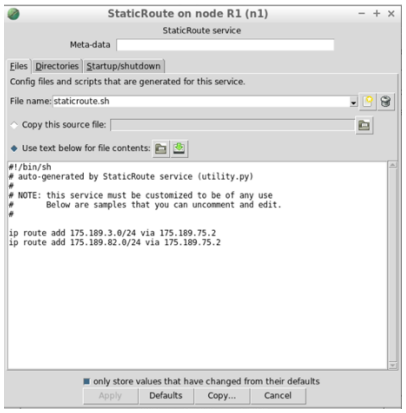


Figure: Configuring static routing table for R1

1. Configuring Routing table for router R1: Router R1, which is directly connected to the clients network, required to forward traffic for network 175.189.3.0/24 (www server network) and 175.189.82.0/24 (intranet server network) to router R4. To add new rules we can simply add following two lines in the shell script for Router R1 like this:



ip route add 175.189.3.0/24 via 175.189.75.2
ip route add 175.189.82.0/24 via 175.189.75.2

After writing the rules we can simply press apply so save the changes.

2. Configuring Routing table for router R2: Router R2, directly connected to the intranet server network, is required to forward traffic for network 175.189.5.0/24 (clients network) and 175.189.3.0/24 (www server network) to router R3. For router R2, rules that is added is:

ip route add 175.189.5.0/24 via 175.189.21.2
ip route add 175.189.3.0/24 via 175.189.21.2

3. Configuring Routing table for router R3: Router R3 is required to forward traffic for network 175.189.82.0/24 (intranet server network) and 175.189.5.0/24 (clients network) to router R2 and router R4 respectively. For router R3, rules that is added is:

ip route add 175.189.82.0/24 via 175.189.21.1
ip route add 175.189.5.0/24 via 175.189.70.2

4. Configuring Routing table for router R4: Router R4 is required to forward traffic for network 175.189.3.0/24 (www server network), 175.189.82.0/24 (intranet server network), and 175.189.5.0/24 (clients network) to router R3, router R3 and router R1 respectively. For router R4, rules that is added is:

ip route add 175.189.3.0/24 via 175.189.70.1
ip route add 175.189.82.0/24 via 175.189.70.1
ip route add 175.189.5.0/24 via 175.189.75.1

After editing the configurations, “ip route” command is used to check the routing tables for each routers in the shell terminal.

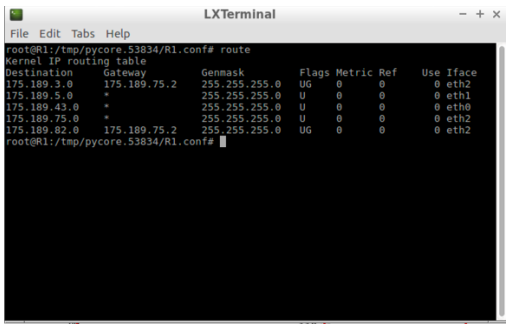


Figure: Router 1 routing table

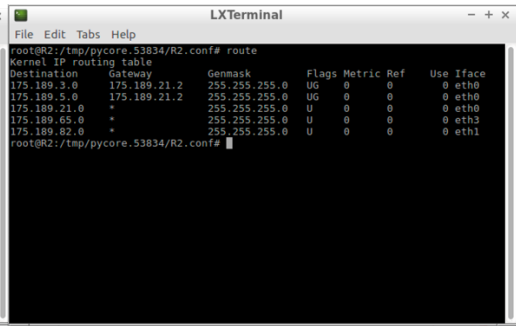


Figure: Router 2 routing table

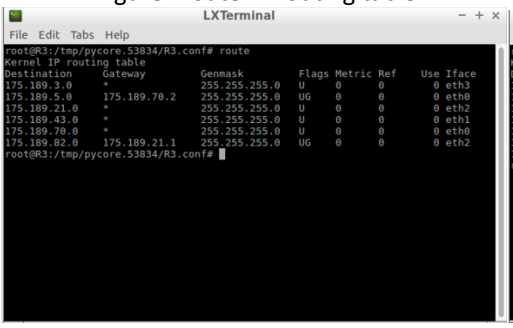


Figure: Router 3 routing table

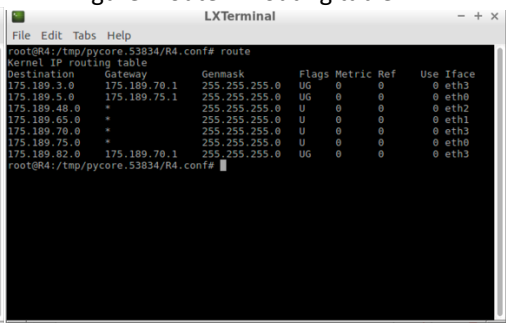


Figure: Router 4 routing table

NB: After configuring all the routing settings, the backup network is connected to route from all the other networks. This configuration is not documented here.

Task B: Finding errors in network configuration

The class B network that this company currently owns, has subnet mask of 24, which means the last one byte of IP address is meant to be used for host addresses. Currently this company has four gateway routers connecting subnets. One of the important tasks of router is to maintain connections of two or more subnets so that they have unique addresses on each subnet. The www, clients, intranet and backup server network have their own specific subnet addresses. Besides, the backbone networks (BN's), that connects these LANS should have a unique subnet too. While configuring for the static routing tables for the network I found three errors in the configuration of IP addresses and masks relating to these subnets. The following sections describes the errors in brief with adequate solutions.

Error 1: Different address for the same subnet:

The router 2 (R2) interface eth1 has IP address of 175.189.82.1/24 which connects the Intranet server through switch three, that is basically falls in the same subnet. However, the IP address of intranet server is assigned to different host address of 175.189.48.12/24 which create problem of different network addresses but in same subnet.

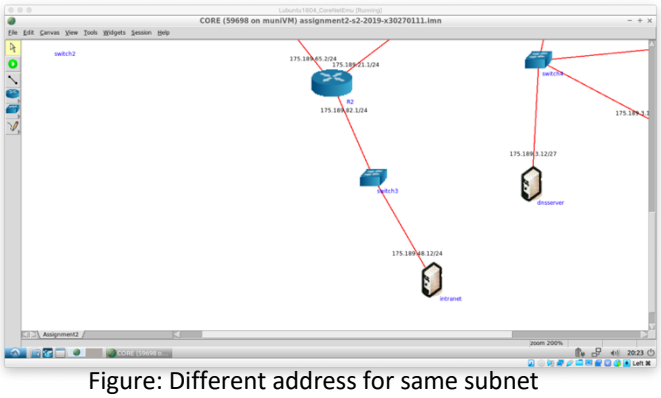


Figure: Different address for same subnet

To fix this problem we can simply change the IPv4 address of intranet host from 175.189.48.12/24 to 175.189.82.12/24 by double clicking the intranet. After completion, pressing Apply will save any changes.

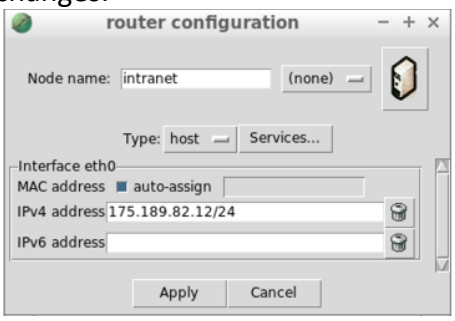


Figure: Changing the network address

For testing the fix, it was observed that lynx command for 175.189.3.11 worked correctly as expected.

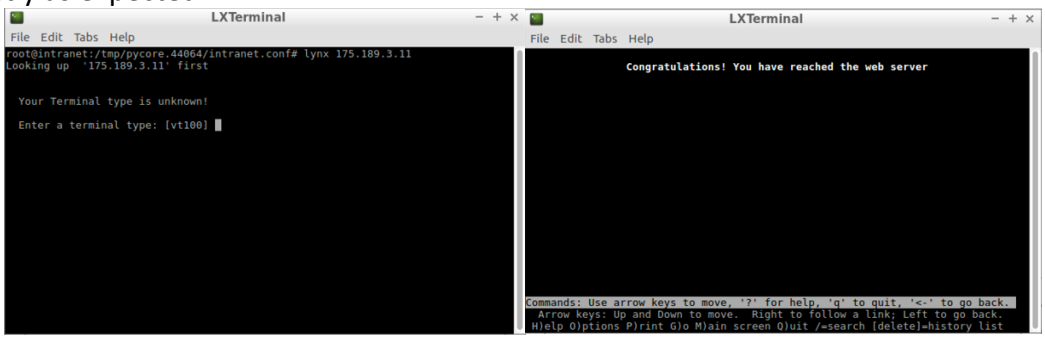
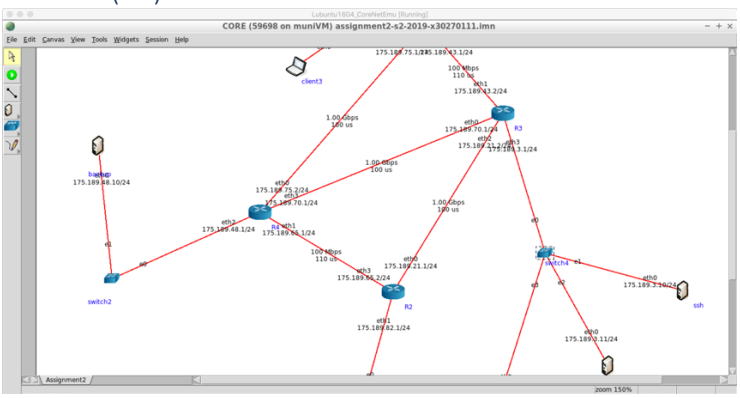


Figure: testing the fix

Error 2: Same interface address Router 3(R3) and Router 4(R4):

As we can see from the simulation screenshot that the interface eth3 of R4 and the interface eth0 of R1 has same IP address. This could cause routing table problem as we know that router choose its paths following the direction in routing tables. Same IP address for interfaces can confuse the both routers and other routers also. This might sometime cause loop in the network.



To solve this issue, we can assign new IP address for interface eth3 of R4, changing the value from 175.189.70.1/24 to 175.189.70.2/24 will solve this error.

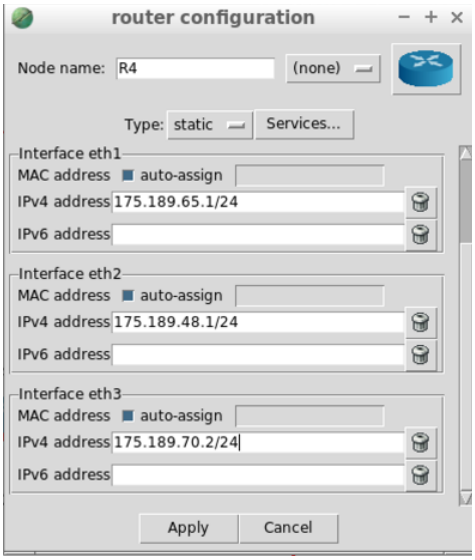


Figure: Changing the interface address of R4 (eth3)

For testing this correction, we can simply try to lynx www.fit9135 from router R4, and it worked fine.

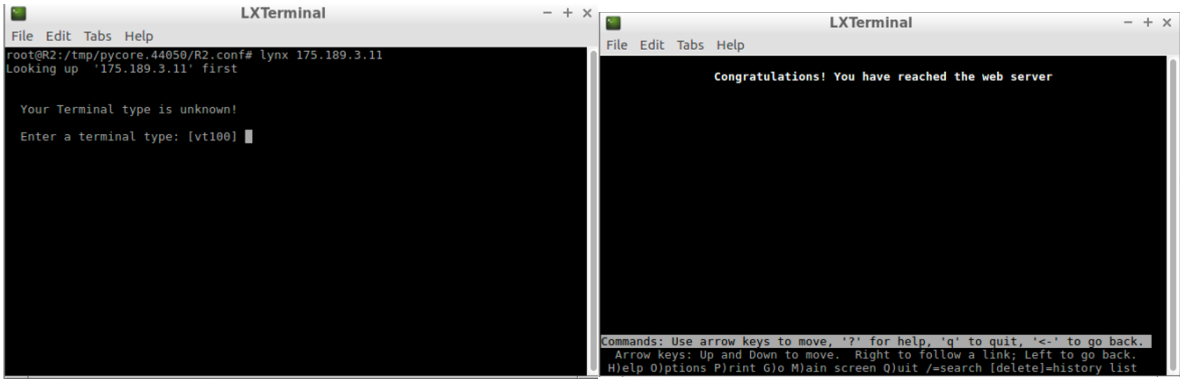


Figure: Testing the fix

Error 3: Incorrect subnet mask for dnsserver:

The dnsserver has wrong subnet mask of /27 which could cause the dnsserver to not get some broadcast packets from R3, beside it may cause static routing table problem as we know that we set a network address for every router while doing static routing table. Which means different netmask could isolate the dnsserver from incoming of packets from the outside devices that transfer for same network address.

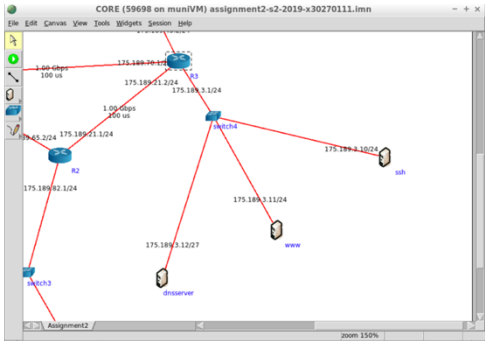


Figure: incorrect subnet mask for dnsserver

Changing the configuration setting of subnet mask from 175.189.2.12/27 to 175.189.2.12/24 for dnsserver fixed this problem.

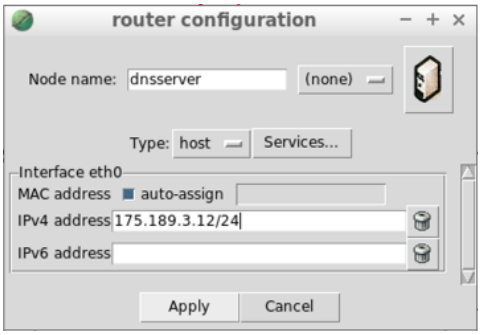


Figure: Changing subnet mask for dnsserver

For testing the fix, it was observed that lynx command for 175.189.3.11 worked correctly as expected from dnsserver.

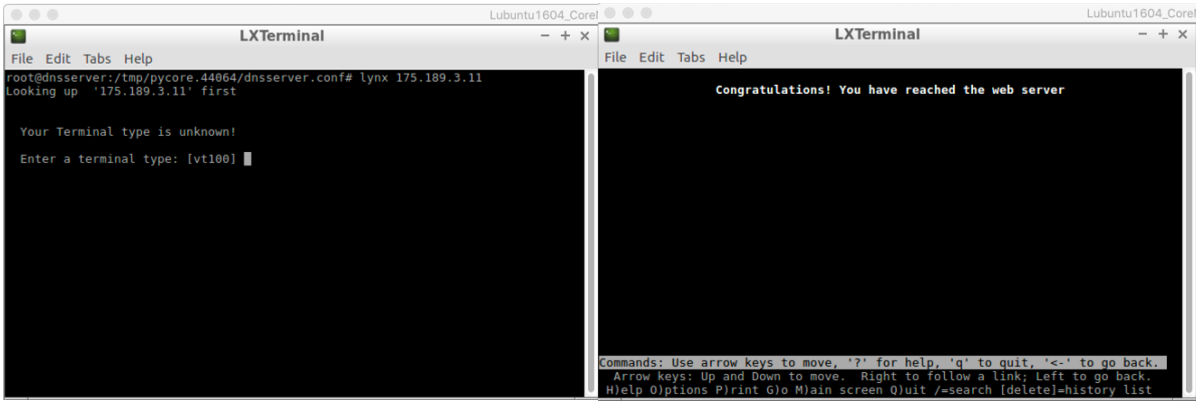


Figure: Testing the fix

Task C: Making R3 as default gateway router for R1, R2 and R4

C.1. Default route choice for R1:

For router R1 default route is chosen to R3 from its interface eth0, although its link speed is comparatively slow (i.e. 100Mbps). The prime reason for choosing this interface is, if I choose the default route to R3 via router R4 (using interface eth2), that already has incoming and outgoing traffic for internal clients for the company from the www server, intranet server, and backup server, can create bottlenecks. This change can be done just simply adding this command in DefaultRoute setting on R1:

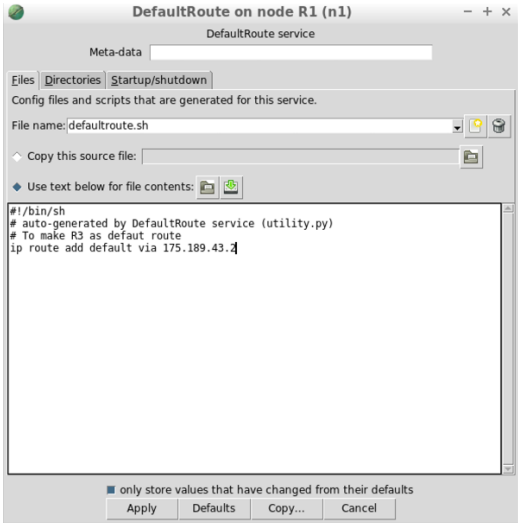
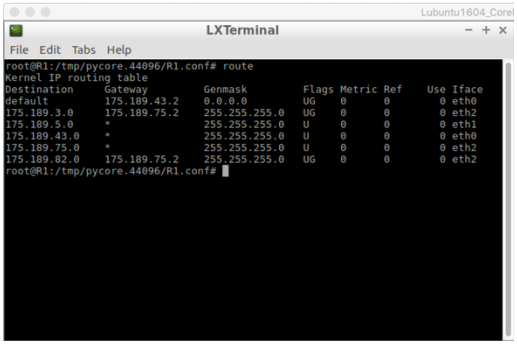


Figure: Changing default route for R1

Ip route add default via 175.189.43.2

Changes of default route setting on R1 can be seen by simply putting route command into the terminal R1.

Figure: Testing change default route for R1



C.2. Default route choice for R2:

For router R2 default route is chosen to R3 from its interface eth0. The command to put into the R2 Default route setting is:

Ip route add default via 175.189.21.2

Changes of default route setting on R2 can be seen by simply putting route command into the terminal R2.

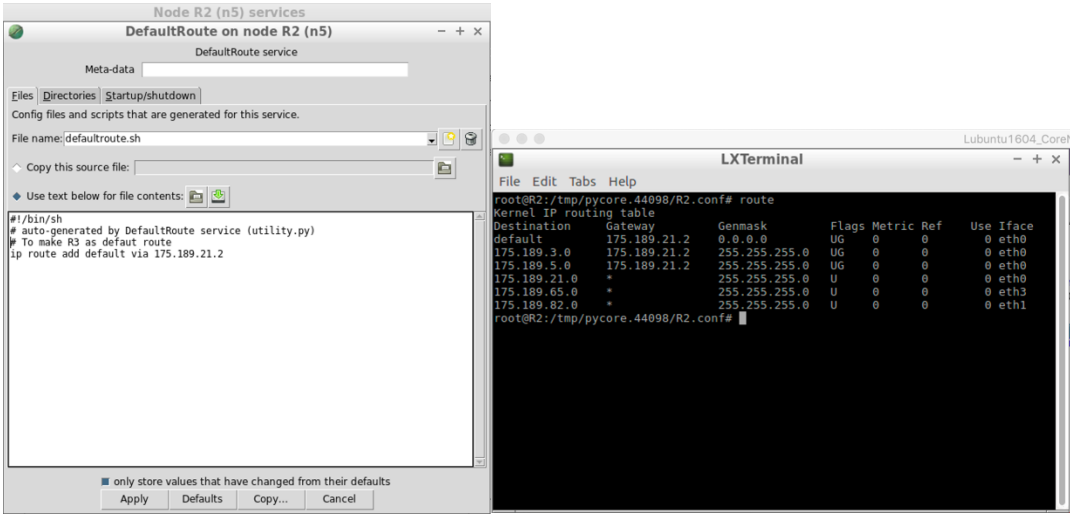


Figure: Changing default route for R2, and testing the change

C.3. Default route choice for R4:

For router R4 default route is chosen to R3 from its interface eth3. The command to put into the R4 default route setting is:

Ip route add default via 175.189.70.1

Changes of default route setting on R4 can be seen by simply putting route command into the terminal R4.

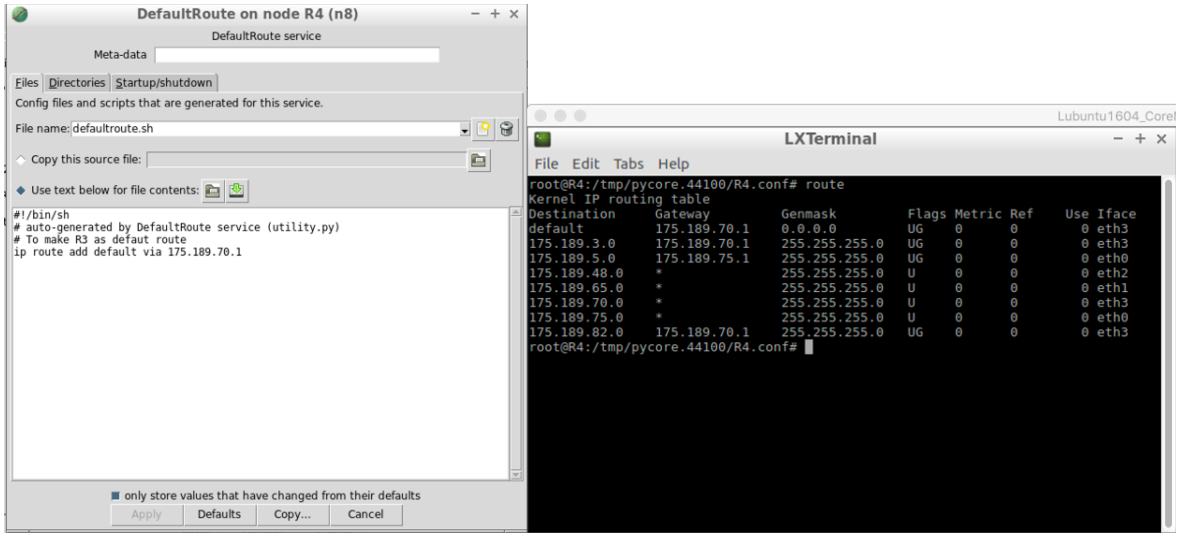


Figure: Changing default route for R4, and testing the change

Task D: Adding a new subnet

A new subnet is added with three client computers named exclient1, exclient2, and exclient3. The network address for this whole subnet is 192.168.192.0/20. The router is named as external and configured with DHCP settings. And the clients is configured with DHCPClient settings. The configuration steps of these two settings is described below:

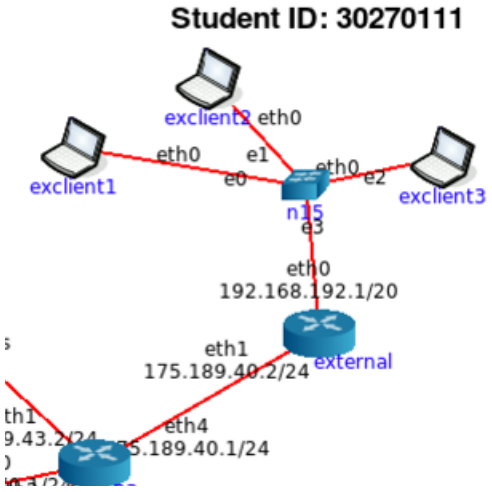


Figure: new subnet

Step 1: Set up external router as DHCP server:

In order to set up the DHCP in external router, DHCP, settings in services has to be configured. The subnet mask which this new network is 20, or 255.255.255.240.0, so the ip address range for host addresses for this new network starts from 192.168.192.1 and ends

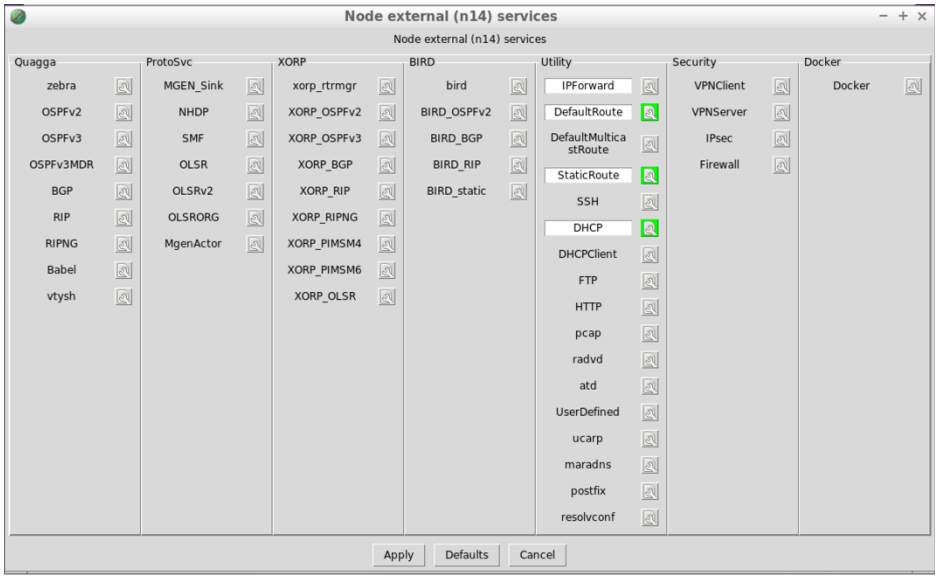
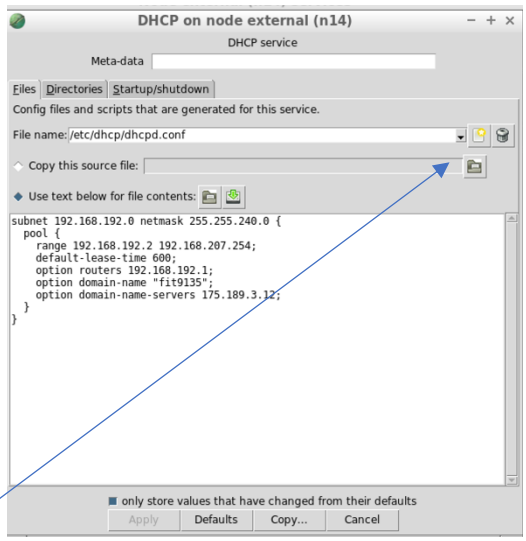


Figure: DHCP service under unility for external server

at 192.168.207.254. the default lease time for each host address is set to 600 and other DNS setting like the name and the server address 175.189.3.12 has been set up. The whole shell script is drafted up here.

Shell scripting in external DHCP server:

```
subnet 192.168.192.0 netmask 255.255.240.0 {
pool {
  range 192.168.192.2 192.168.207.254;
  default-lease-time 600;
  option routers 192.168.192.1;
  option domain-name "fit9135";
  option domain-name-servers 175.189.3.12;
 }
}
```



The new config file is also added in the DHCP setting. The path is

var/lib/dhcp/dhcpd.leases

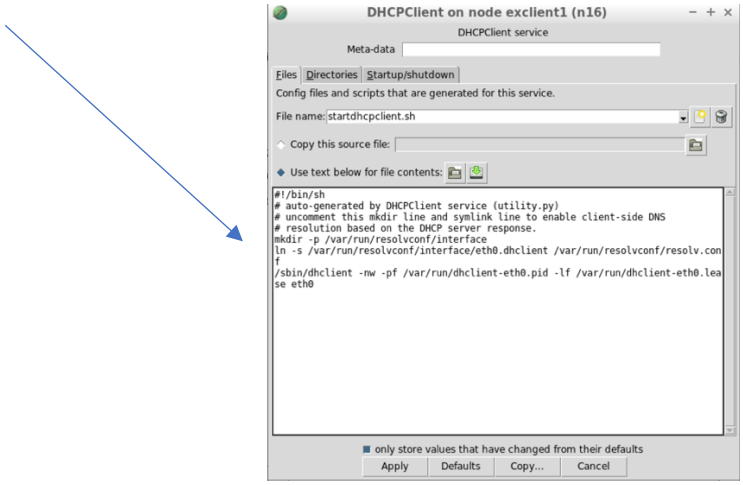
Step 2: Set up clients as DHCP clients:

In order to set up exclient1, exclient2 and exclient3, DHCPClient settings has to be configured in all the nodes. The command is drafted here:

Shell script in DHCP clients:

```
#!/bin/sh
# auto-generated by DHCPClient service (utility.py)
# uncomment this mkdir line and symlink line to enable client-side DNS
# resolution based on the DHCP server response.
mkdir -p /var/run/resolvconf/interface
ln -s /var/run/resolvconf/interface/eth0.dhclient /var/run/resolvconf/resolv.conf
/sbin/dhclient -nw -pf /var/run/dhclient-eth0.pid -lf /var/run/dhclient-eth0.lease
eth0
```

```
mkdir -p /var/run/resolvconf/interface
ln -s /var/run/resolvconf/interface/eth0.dhclient /var/run/resolvconf/resolv.conf
/sbin/dhclient -nw -pf /var/run/dhclient-eth0.pid -lf /var/run/dhclient-eth0.lease
eth0
```



Step 3: Set up interface addresses for external router and R3

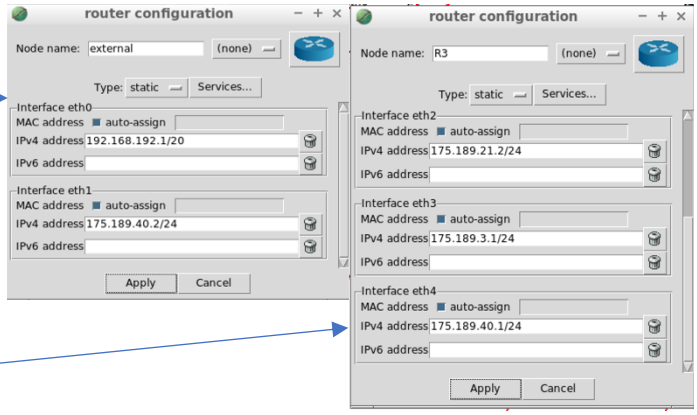
After implementing DHCP server and DHCP client rules, the interface addresses of external and router R3 is added as such. For the BN, new network address 175.189.40.0/24 is implemented in external router's eth1 and router R3's eth4 interfaces. For the external router, the first host address is used as the interface address of the router.

external router:

eth0: 192.168.192.1/20
eth1: 175.189.40.2/24

R3

eth4: 175.189.40.1/24



Step 4: Set the default route for external router to router R3

Finally, the default route of external router is set using ip route add command in the DefaultRoute service setting of external router.

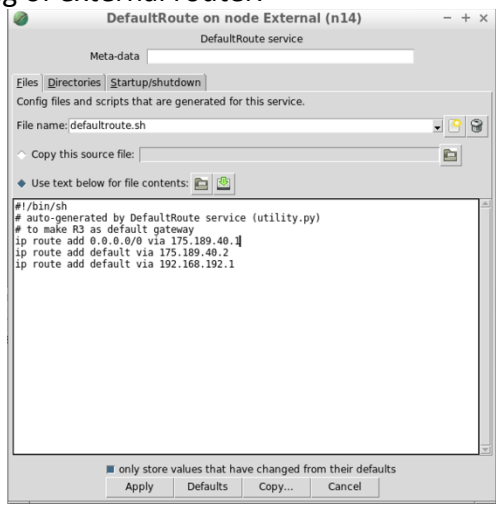


Figure: Setting up default route for external to R3

Testing External router as DHCP server:

After implementing all these steps, we can check the ipconfig information of clients to make sure that the external router is working as a DHCP server, by hovering the pointer over each external client in Core.

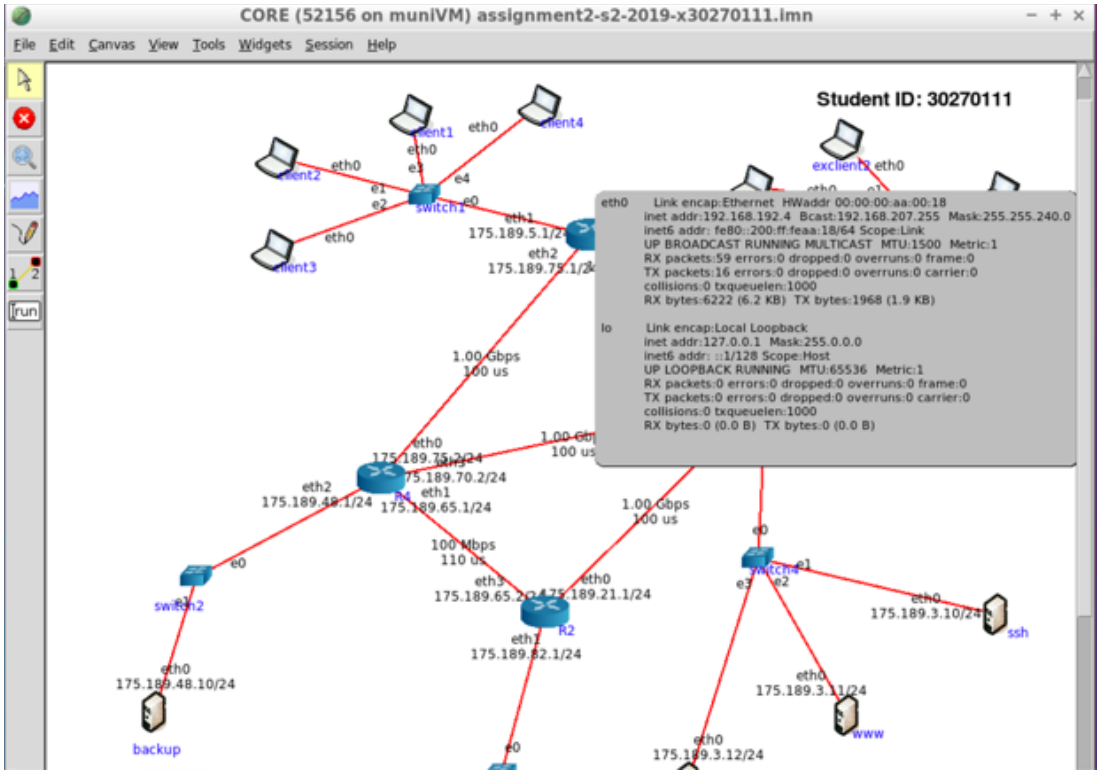


Figure: DHCP server is working as expected

Task E: Implementing Demilitarised Zone (DMZ)

Part A: Any packets for the specific servers in the DMZ are accepted

There are four types of packets that can be transferred within DMZ, internal company and outside external clients. These are: HTTP packets, SSH packets, DNS packets, and ICMP packets. Before setting up the rules, firewall setting is turned on and default commands in the firewall setting is added, which means the firewall will blocks all type of packets now.

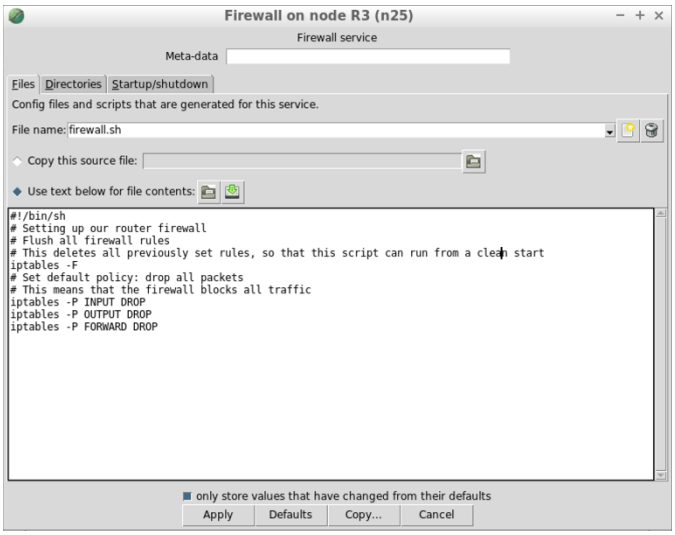


Figure: Default firewall setting on R3

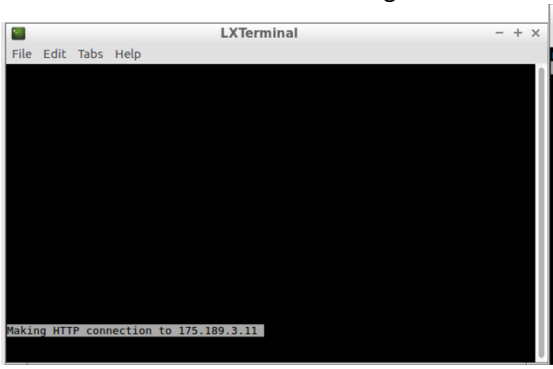


Figure: HTTP packet blocked

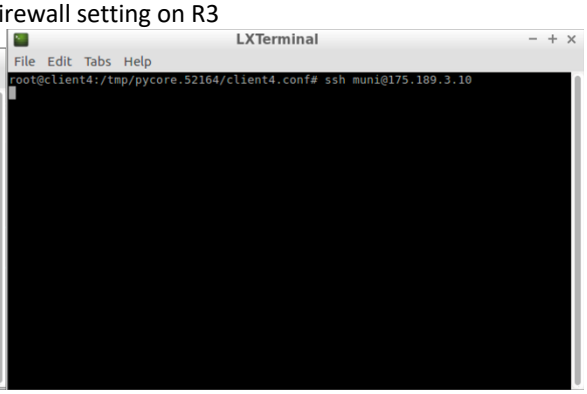


Figure: SSH packet blocked

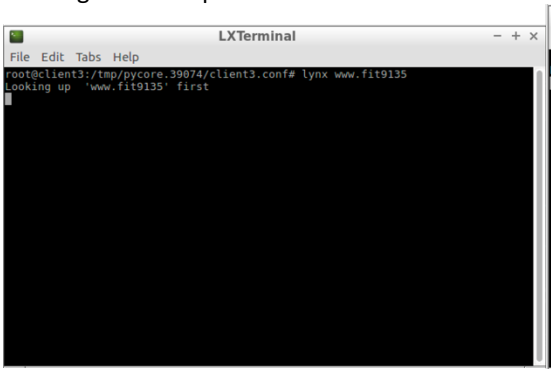


Figure: DNS packet blocked

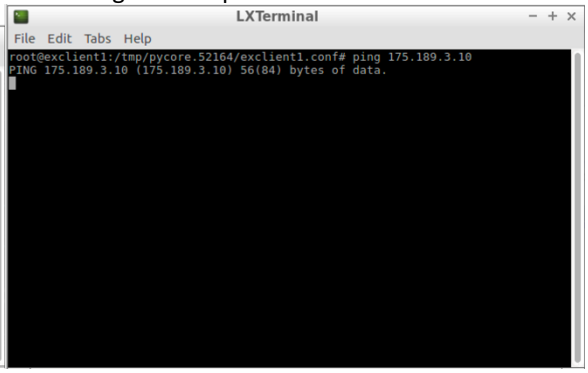


Figure: ICMP packet blocked

When the default setting of firewall is set, any packets cannot communicate using the router R3. When we start implementing rules one by one for different type of packets,

the packets will successfully transfer through the firewall router R3. All the configuration settings and rules of these packets for the firewall in R3 router is described below with adequate test results for the internal and external clients.

A.1 : Any packets for the specific servers in the DMZ are accepted (HTTP)

To implement this rule, these lines in the firewall setting of R3 is added.

```
iptables -A FORWARD -o eth3 -d 175.189.3.11 -p tcp --destination-port 80 -j ACCEPT
iptables -A FORWARD -i eth3 -s 175.189.3.11 -p tcp --source-port 80 -j ACCEPT
```

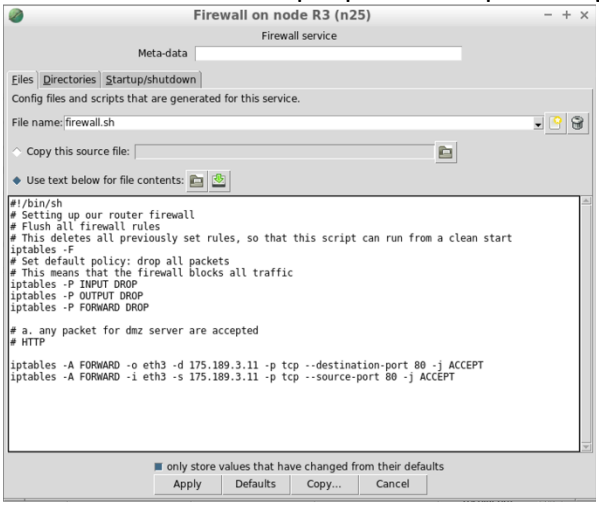


Figure: Setting HTTP firewall rule for R3

Results:

Command used to check result- lynx 175.189.3.11

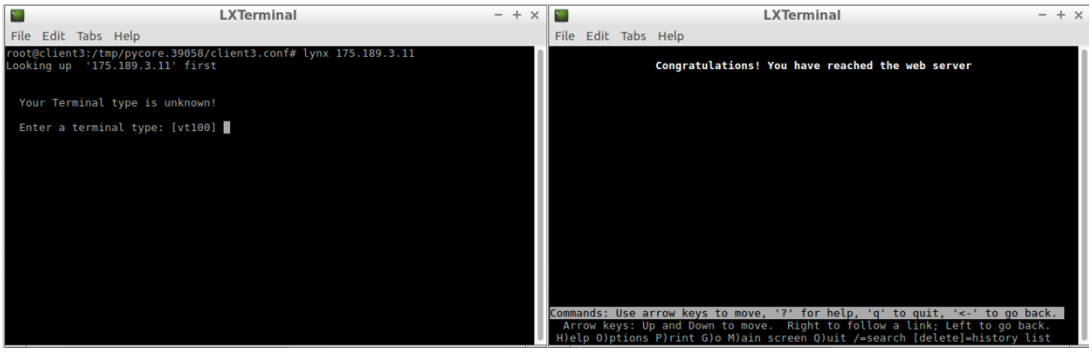


Figure: HTTP packet test from clients network (client3)

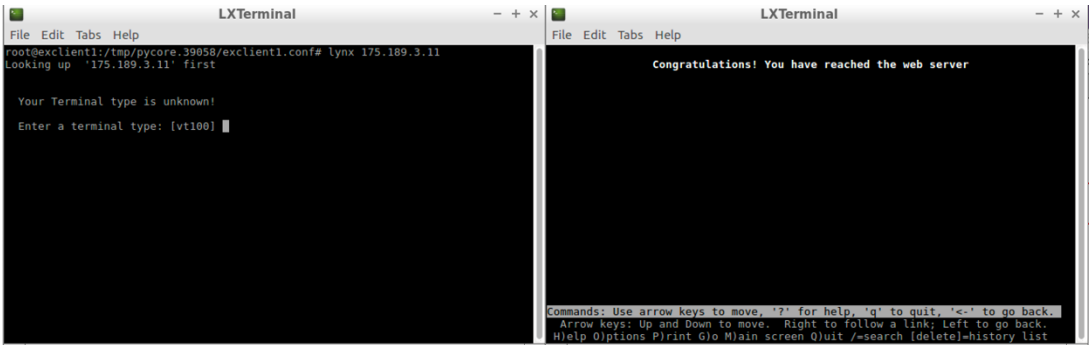


Figure: HTTP packet test from external network (exclient1)

A.2 : Any packets for the specific servers in the DMZ are accepted (SSH)

To implement this rule, these lines in the firewall setting of R3 is added.

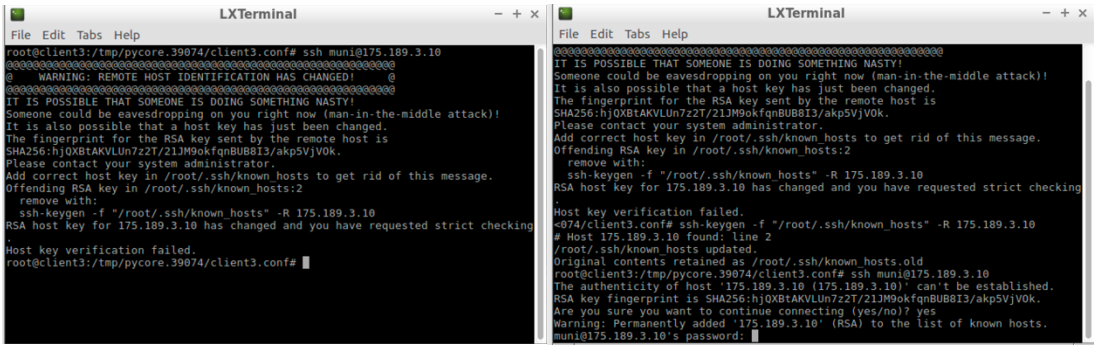
```
iptables -A FORWARD -o eth3 -d 175.189.3.10 -p tcp --destination-port 22 -j ACCEPT
iptables -A FORWARD -i eth3 -s 175.189.3.10 -p tcp --source-port 22 -j ACCEPT
```

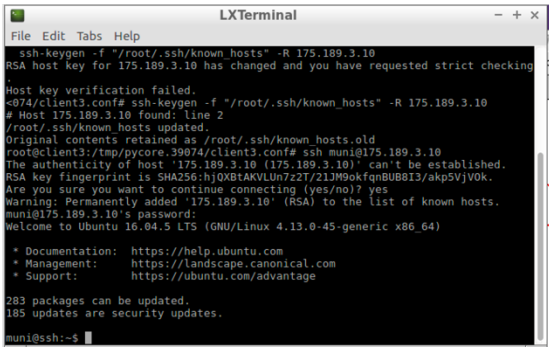
Results:

Command used to check result- shh muni@175.189.3.10

To solve man-in-the-middle attack error-

```
ssh-keygen -f "/root/.ssh/known_hosts" -R 175.189.3.10
```





Figures: SSH packet test from clients network (client3)

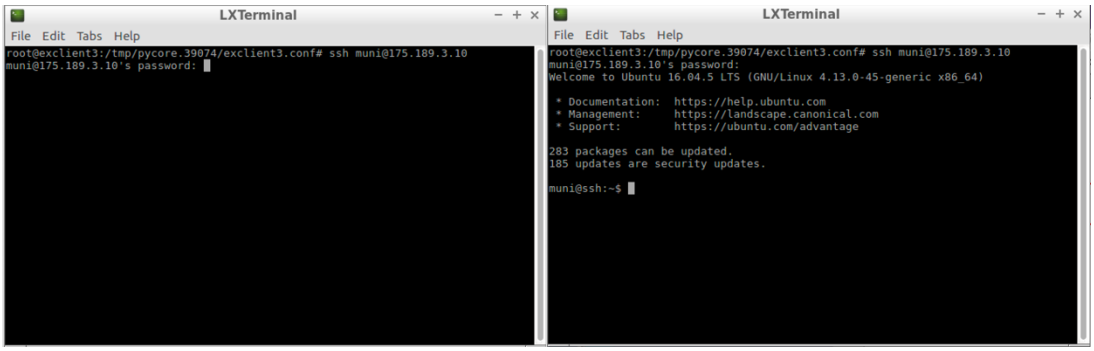


Figure: SSH packet test from external network (exclient3)

A.3 : Any packets for the specific servers in the DMZ are accepted (DNS)

To implement this rule, these lines in the firewall setting of R3 is added.

```
iptables -A FORWARD -o eth3 -d 175.189.3.12 -p udp --destination-port 53 -j ACCEPT
iptables -A FORWARD -i eth3 -s 175.189.3.12 -p udp --source-port 53 -j ACCEPT
```

Results:

Command used to check result- lynx www.fit9135

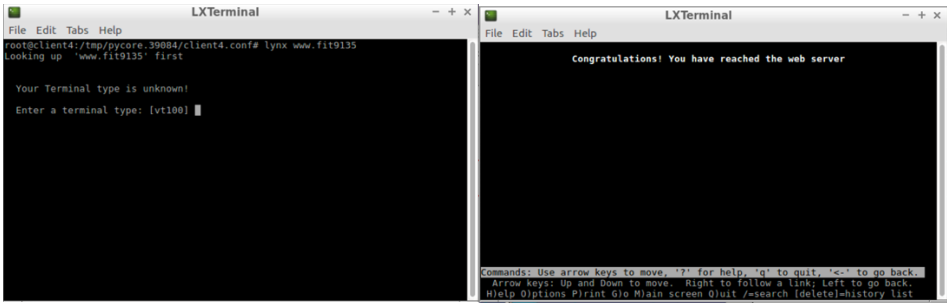


Figure: DNS packet test from clients network (client4)

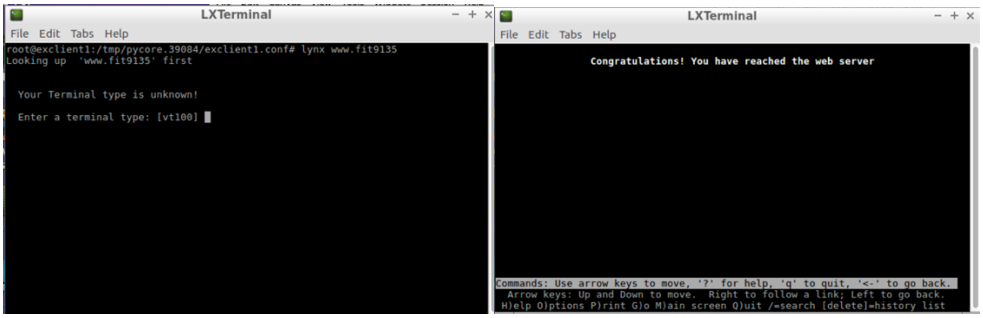


Figure: DNS packet test from external network (exclient1)

A.4 : Any packets for the specific servers in the DMZ are accepted (ICMP)

To implement this rule, these lines in the firewall setting of R3 is added.

```
iptables -A FORWARD -o eth3 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -i eth3 -p icmp --icmp-type 0 -j ACCEPT
```

Results:

Command used to check result- ping 175.189.3.10

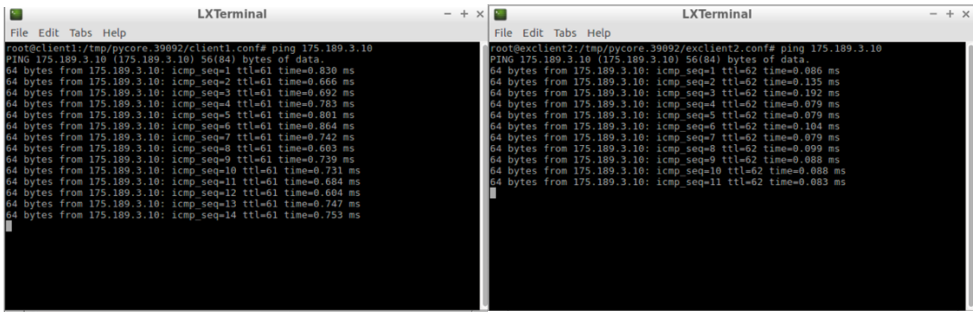


Figure: ICMP packet test from clients network (client1), and ICMP packet test from external network (exclient2)

Part B: Any packets from inside the company network are accepted.

To implement this rule, these lines in the firewall setting of R3 is added.

```
iptables -A FORWARD -i eth0 -j ACCEPT
iptables -A FORWARD -i eth1 -j ACCEPT
iptables -A FORWARD -i eth2 -j ACCEPT
iptables -A FORWARD -i eth3 -j ACCEPT
```

Result:

Command used to check result- lynx 175.189.3.11

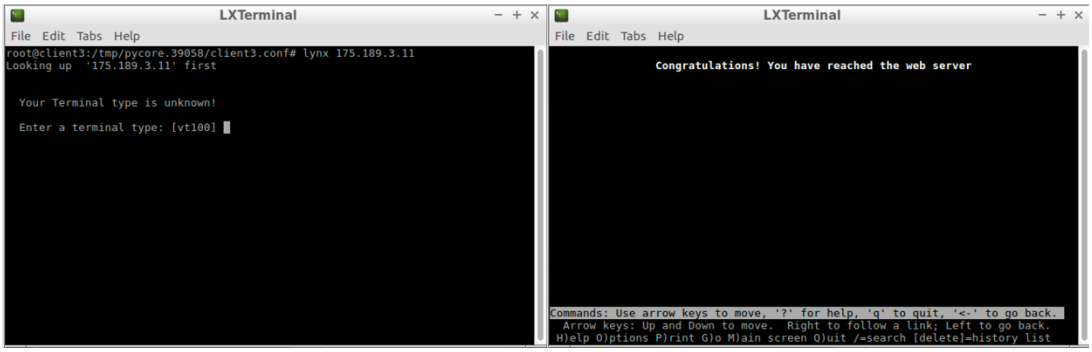


Figure: HTTP packet test from inside the company network (client3)

Part C: Any packets relating to connections that were established from inside the company network are accepted.

To implement this rule, these lines in the firewall setting of R3 is added.

```
iptables -A FORWARD -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -o eth2 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Result 1:

Command used to check result- lynx www.fit9135

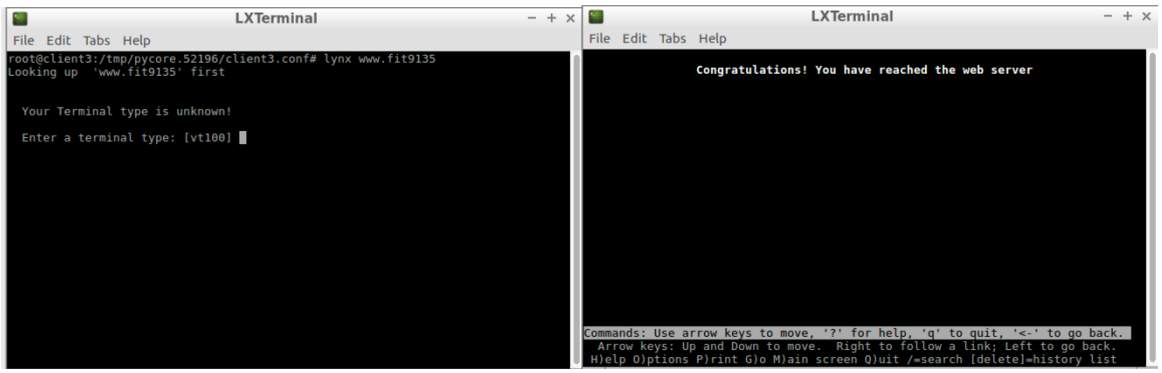


Figure: DNS packet test from clients network (client4)

Results 2:

After completing Part B and Part C external to clients network will have no ping.

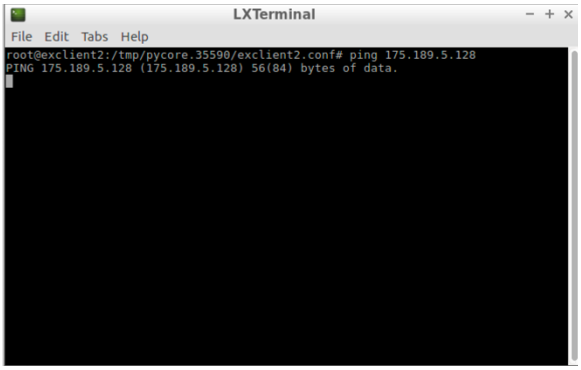


Figure: external to clients network will have no ping

After completing Part B and Part C clients network to DMZ will have ping

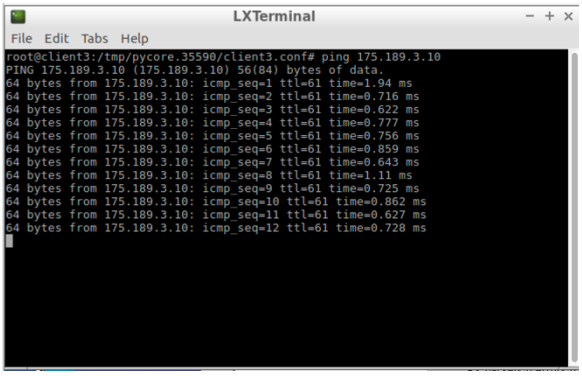


Figure: clients network to DMZ will have ping

Part D: Any SSH packets from the ssh server into the company network are accepted.

To implement this rule, these lines in the firewall setting of R3 is added.

```
iptables -A FORWARD -i eth3 -o eth1 -s 175.189.3.10 -p tcp --destination-port 22 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth3 -d 175.189.3.10 -p tcp --source-port 22 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth3 -o eth2 -s 175.189.3.10 -p tcp --destination-port 22 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth2 -o eth3 -d 175.189.3.10 -p tcp --source-port 22 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth3 -o eth0 -s 175.189.3.10 -p tcp --destination-port 22 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth0 -o eth3 -d 175.189.3.10 -p tcp --source-port 22 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

Result:

Command used to check result- ssh muni@175.189.3.10

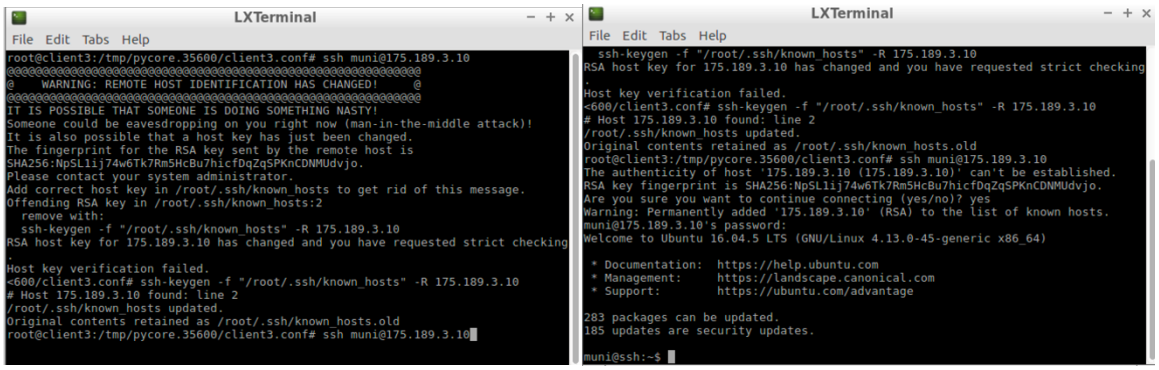


Figure: SSH packet test from clients network (client3)

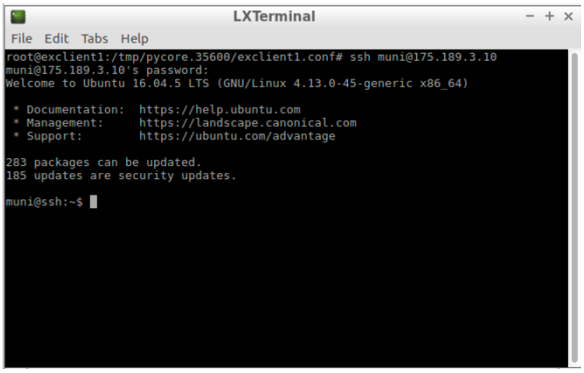


Figure: SSH packet test from external network (exclient1)

Part E: Any other packets are blocked.

Example E.1 : From external clients to intranet (web server) will not work

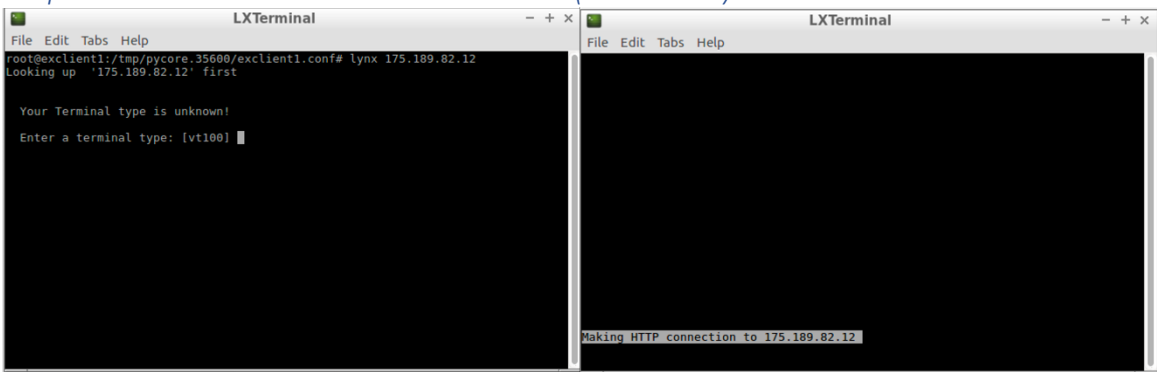


Figure: External clients (i.e. exclient1) can not access intranet server network's content

Example E.2 : Ping From external clients to local clients network will not work

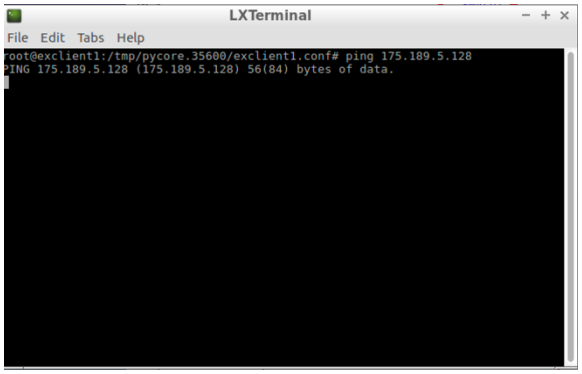


Figure: External clients (i.e. exclient1) can not ping company clients network