# Set up routing table enabling three networks contains computers to reach each other

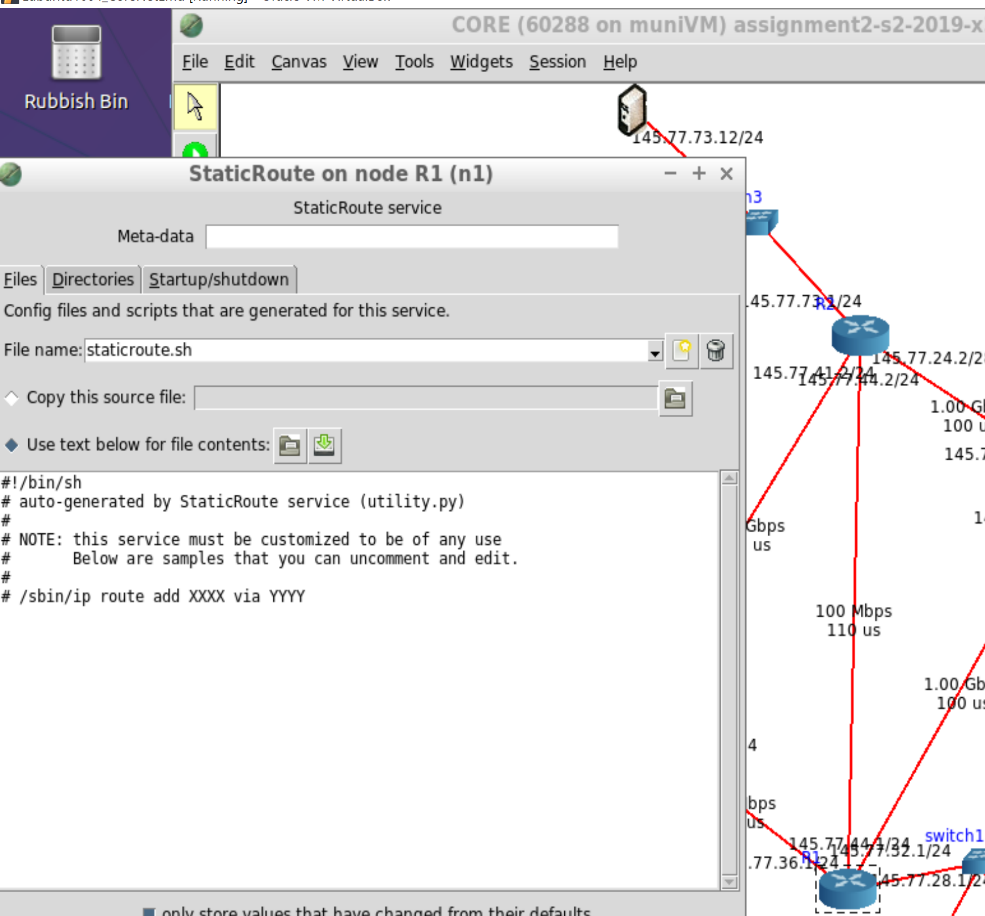
While browsing the static route table of the network, **the first error is observed** which is the routing table has not been set up. Hence neither of any ping command or lynx was successful.

Figure error 1, empty routing tables

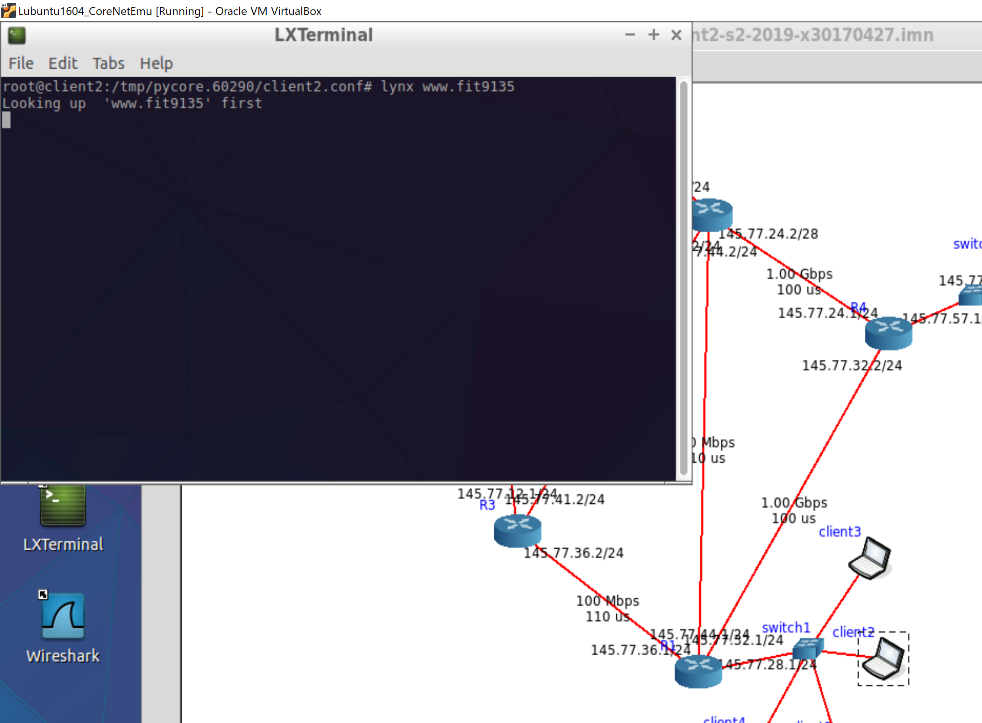


Figure unsuccessful lynx

This error is fixed by setting up the routing tables as follow

## Client reach www server

### Set up

* Enables static route service at **all routers**
* At R1 static route configuration file, use the command: ip add route 145.77.12.0/24 via 145.77.32.2
* At R4 static route configuration file, write the command: ip add route 145.77.12.0/24 via 145.77.24.2
* While setting the routing table of R2, **the second error is founded**, two interfaces connecting R3 and R2 has the same IP address 145.77.41.2.
* This error is fixed by changing the IP address of interface on R2 to 145.77.41.1.
* Then write the command

ip add route 145.77.12.0/24 via 145.77.41.2

Figure 3 error 2 two connecting interface has the same IP address

* This route is chosen because the connection has better link state between routers.

### Testing

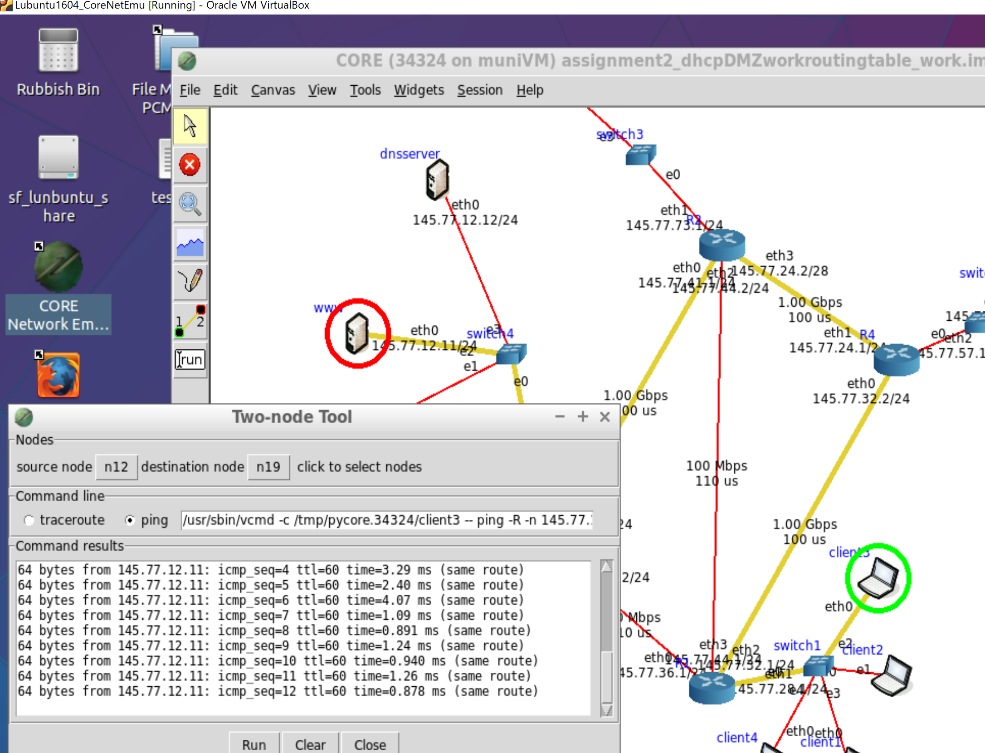


Figure 4 client ping www server

* Test by using the ping command from client to www server, the connection is successful.

## Client reach intranet

### Set up

Figure 5 error 3 SSH server wrong subnet address

* At R2 configuration file write command: ip add route 145.77.73.12 via 145.77.32.2
* At R4 configuration file write command: ip add route 145.77.73.12 via 145.77.24.2
* The **third error is founded here** as intranet and SSH server has the same subnet address of 145.77.73.0/24, while SSH server belongs to the subnet 145.77.12.0/24
* This error is fixed by changing the SSH server IP address to 145.77.12.10
* This route is chosen because the connection has better link state between routers.

### Testing

* Test by ping from client to intranet, the ping is successful

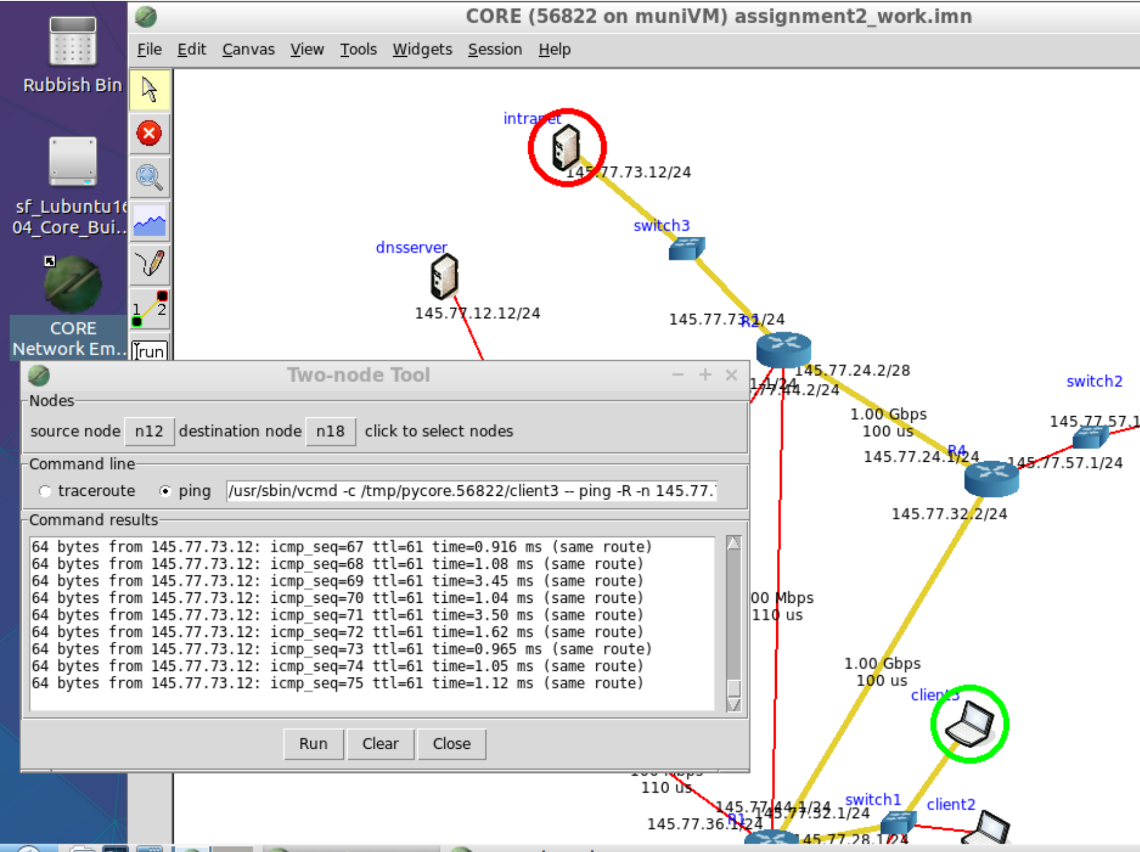


Figure 6 client ping intranet

## Intranet reach www server

### Set up

* As R2 already has the destination of www server in the routing table, no new command needed
* This route is chose because it has least hop also good link state

### Testing

* Test by ping from intranet to www server, which is successful.

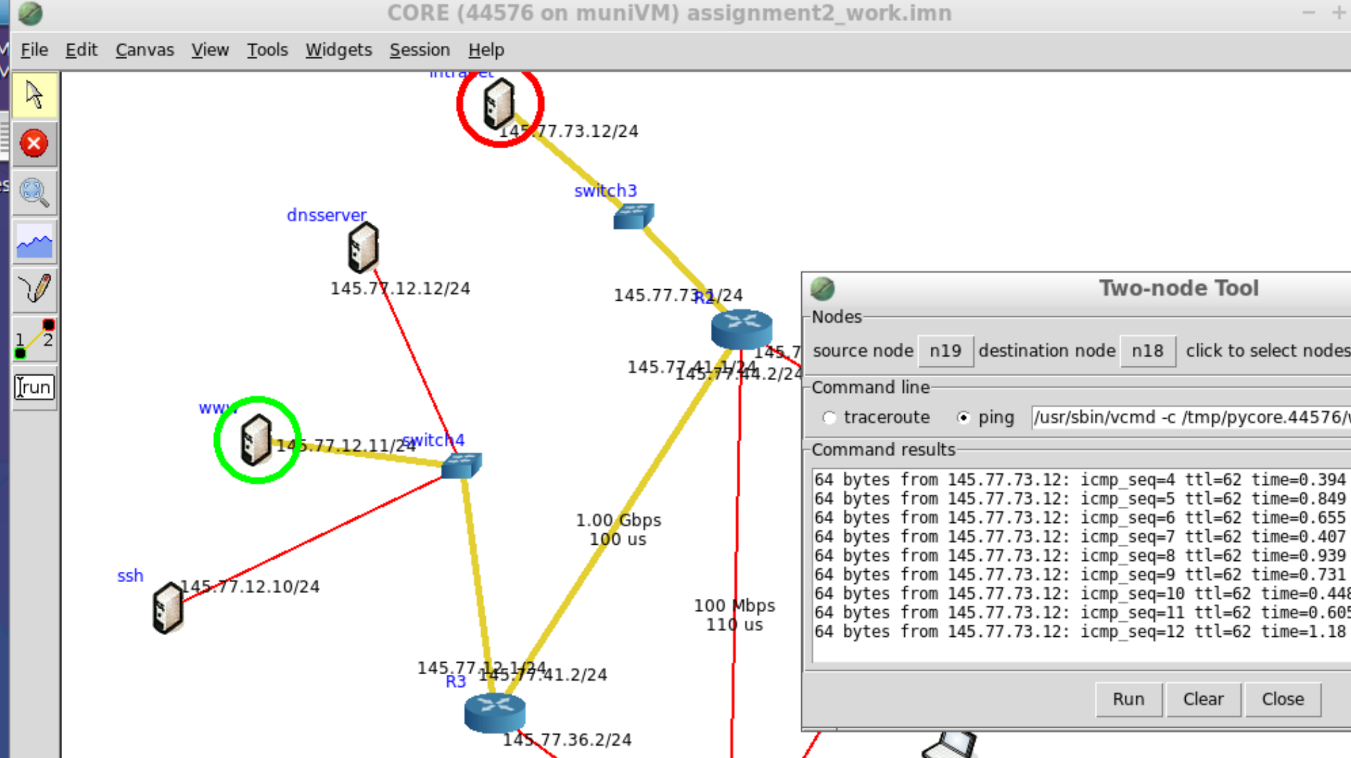


Figure 7 intranet ping www server

## Summary

The first error in configuration founded is the routing table has not been set up for any router. The routing table can be check on static route configuration file of each router. This is fixed by adding command line ip add route <destination ip address> via <the ip address of next router interface in the route>. For example, for client to reach intranet server, the routing table of client LAN router needed a line: “ ip add route 145.77.73.12 via 145.77.24.2”, 145.77.73.12 is the ip address of intranet server, and 145.77.24.2 is the interface IP address which is the next interface the packet need to go in the route. On the routing table R2 it needed to know that in order to reach client, the next interface IP address is 145.77.44.1, the ip add route command need to be added. Routing tables of each router is set up by this method, the routes are mentioned in the previous part of report. Whether the error is fixed can be test by ping command between 2 computers/servers. If they can reach each other via the chosen route, that indicates the routing table has successfully set up.

While setting up routing table, the interfaces connect router 2 and router 3 appears to have same IP address (145.77.41.2), this is an error as they are two different router interfaces. The error is fixed by change IP address of one of the interfaces to 145.77.41.1. This can be test by the ping command same as test the routing table.

The last error found is SSH server which is in the same subnet as www server has different subnet IP address. SSH server has the subnet address same as intranet server (145.77.73.0). Because this is not a VLAN, computers in the same subnet should have same subnet address. This error is fixed by changing the IP address of SSH server to 145.77.12.10/24.

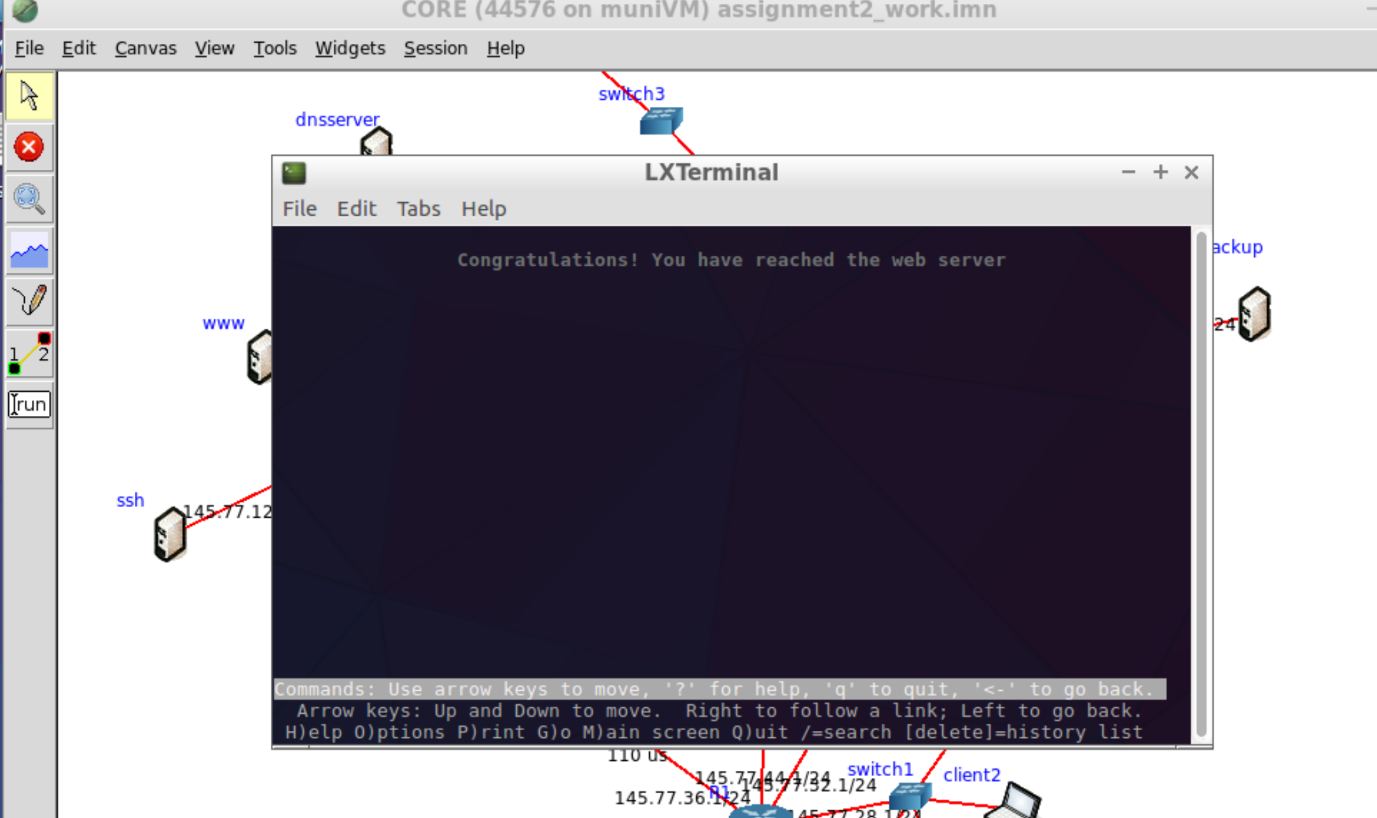


Figure 8 lyxn command appears to be successful

As shown in figure 6, the command lynx [www.fit9135](http://www.fit9135) appears to be successfully execute after all the errors are fixed.

# Make R3 the default router

## Set up

* The default route is set up by enabling default route service on each router first
* The command in the configuration file is: ip route add default <ip address of the next interface>
* At R1, the next hop of default route is R4, then at R4 the default route goes to R2, in the end goes into default router, which is R3 via interface 145.77.41.2

## Testing

* Testing is achieved by ping an IP address out of the network (8.8.8.8)
* We can see the ICMP packets reached 145.77.41.2

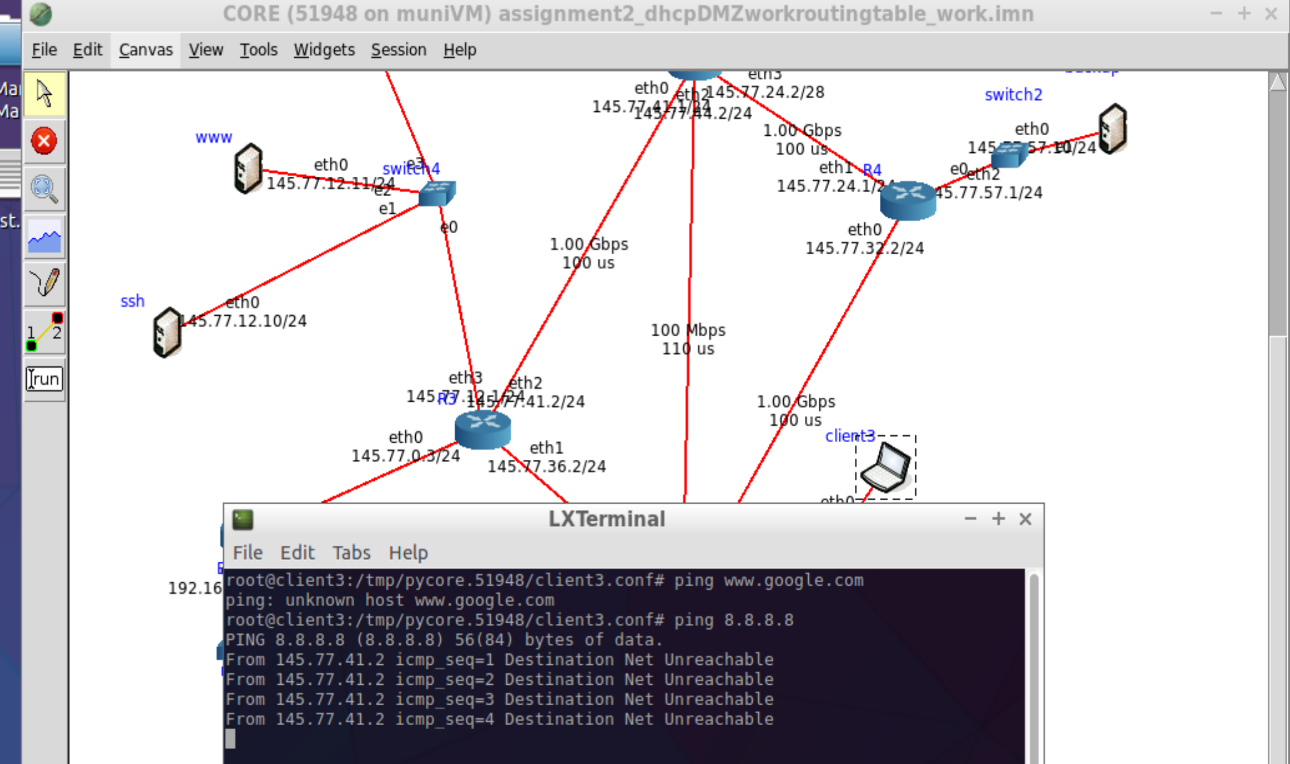
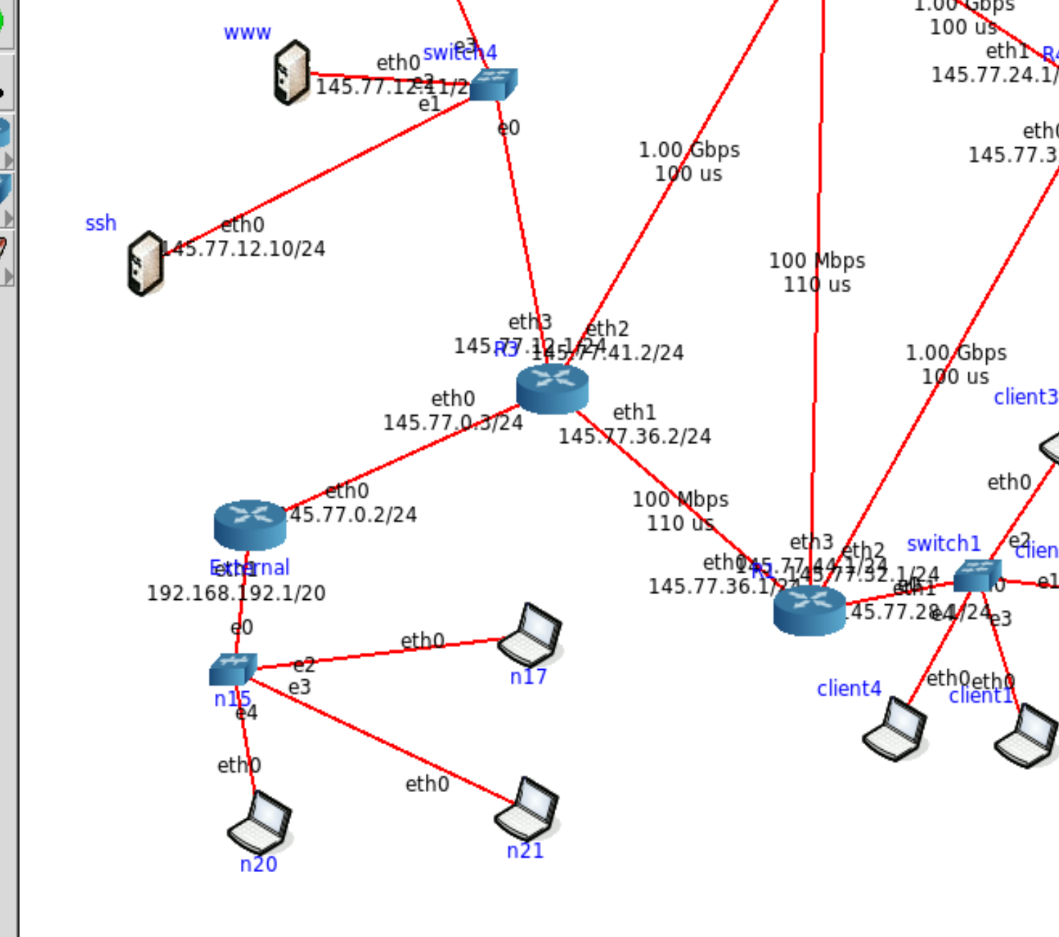


Figure 9 default route reaches 145.77.41.2

# A new subnet with 3 client and DHCP server

* The subnet is set up accordingly



* DHCP service at external router is enabled, also DHCP client service on each client computer. Their configuration files are uncommented to enable the services

## Testing

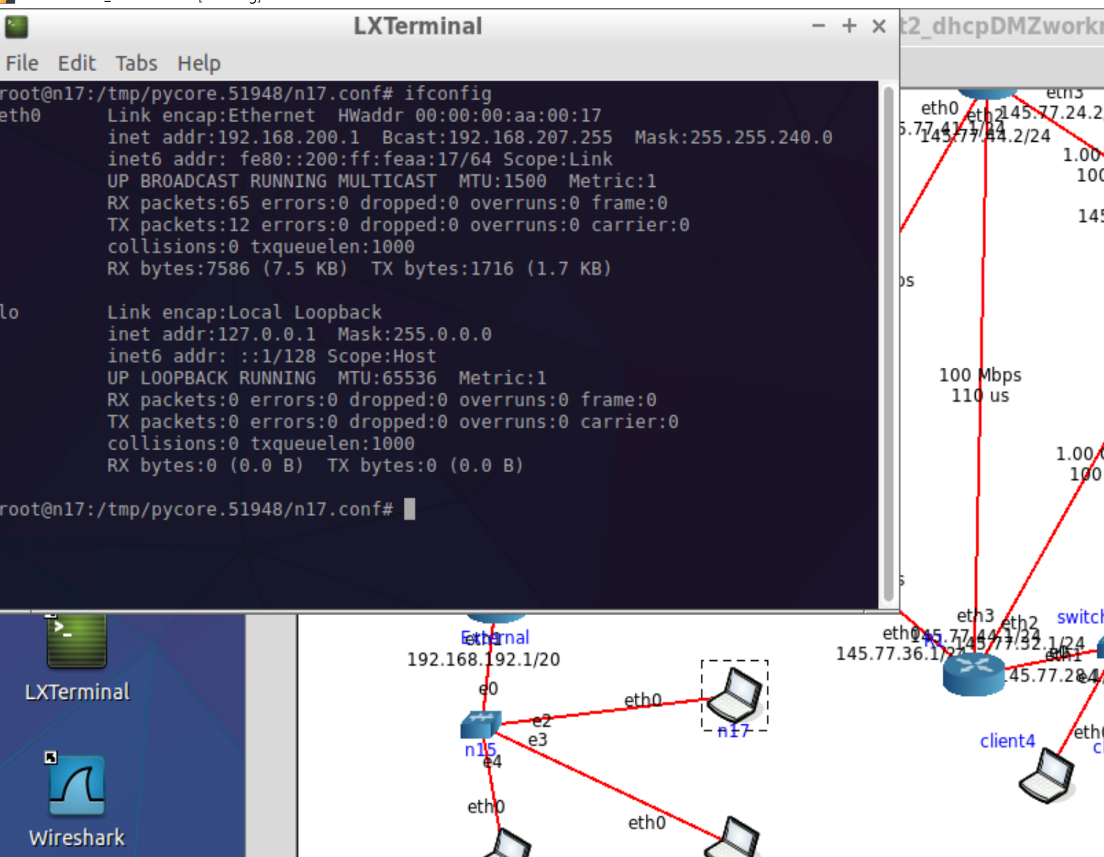


Figure 10 DHCP clients assigned IP address

The client computer successfully obtained an IP address.

# DMZ set up

First the all the rules are flushed then default policies are added

iptables -F

iptables -P INPUT -j DROP

iptables -P OUTPUT -j DROP

iptables -P FORWARD -j DROP

## Any packets for the specific servers in the DMZ are accepted, including ICMPs

The firewall rules used are:

* iptables -A FORWARD -i eth0 -o eth3 -d 145.77.12.11 -p tcp --destination-port 80 -j ACCEPT
* iptables -A FORWARD -i eth0 -o eth3 -d 145.77.12.10 -p tcp --destination-port 22 -j ACCEPT
* iptables -A FORWARD -i eth3 -o eth0 -s 145.77.12.11 -p tcp --source-port 80 -j ACCEPT
* iptables -A FORWARD -i eth3 -o eth0 -s 145.77.12.10 -p tcp --source-port 22 -j ACCEPT
* iptables -A INPUT -p udp -d 145.77.12.12 --destination-port 53 -j ACCEPT
* iptables -A OUTPUT -p udp -s 145.77.12.12 --source-port 53 -j ACCEPT
* iptables -A FORWARD -i eth0 -o eth3 -d 145.77.12.11 -p icmp -j ACCEPT
* iptables -A FORWARD -i eth0 -o eth3 -d 145.77.12.10 -p icmp -j ACCEPT
* iptables -A FORWARD -i eth0 -o eth3 -d 145.77.12.12 -p icmp -j ACCEPT
* iptables -A FORWARD -i eth3 -o eth0 -s 145.77.12.11 -p icmp -j ACCEPT
* iptables -A FORWARD -i eth3 -o eth0 -s 145.77.12.10 -p icmp -j ACCEPT
* iptables -A FORWARD -i eth3 -o eth0 -s 145.77.12.12 -p icmp -j ACCEPT

### Testing

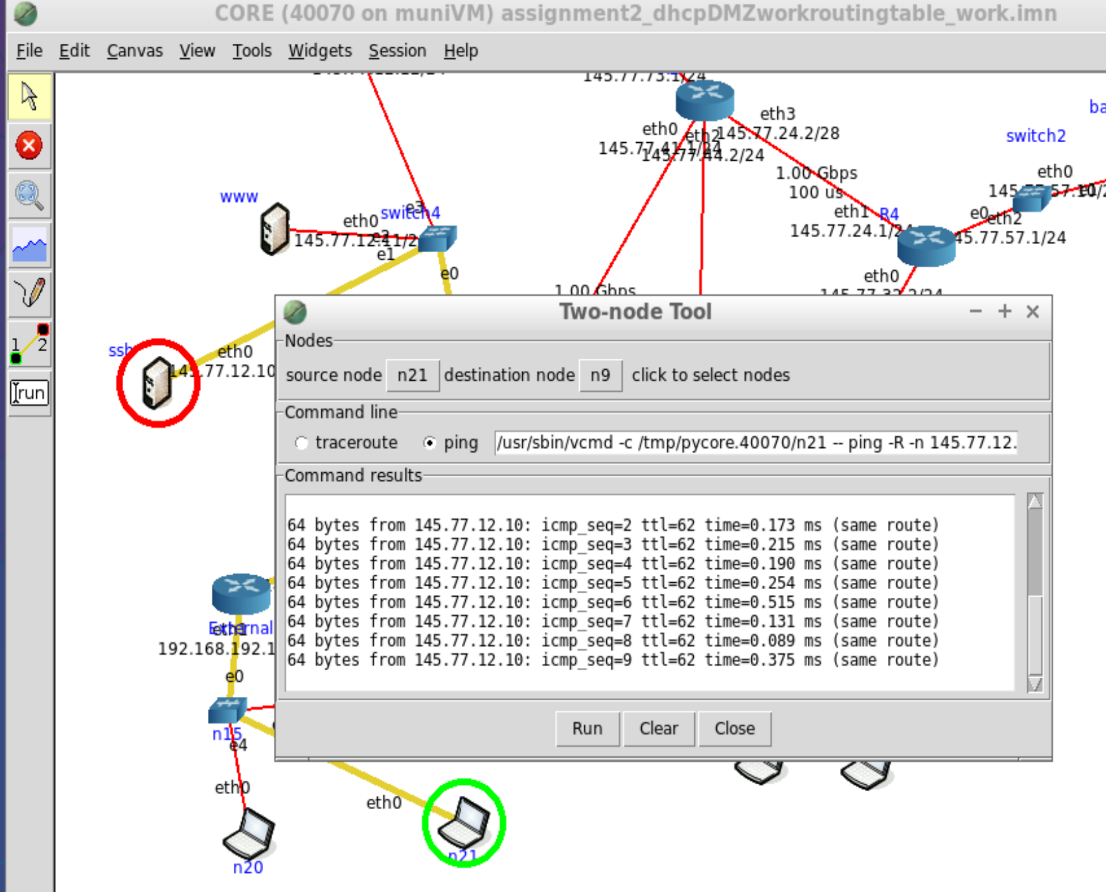


Figure 11 Outside client ping inside servers

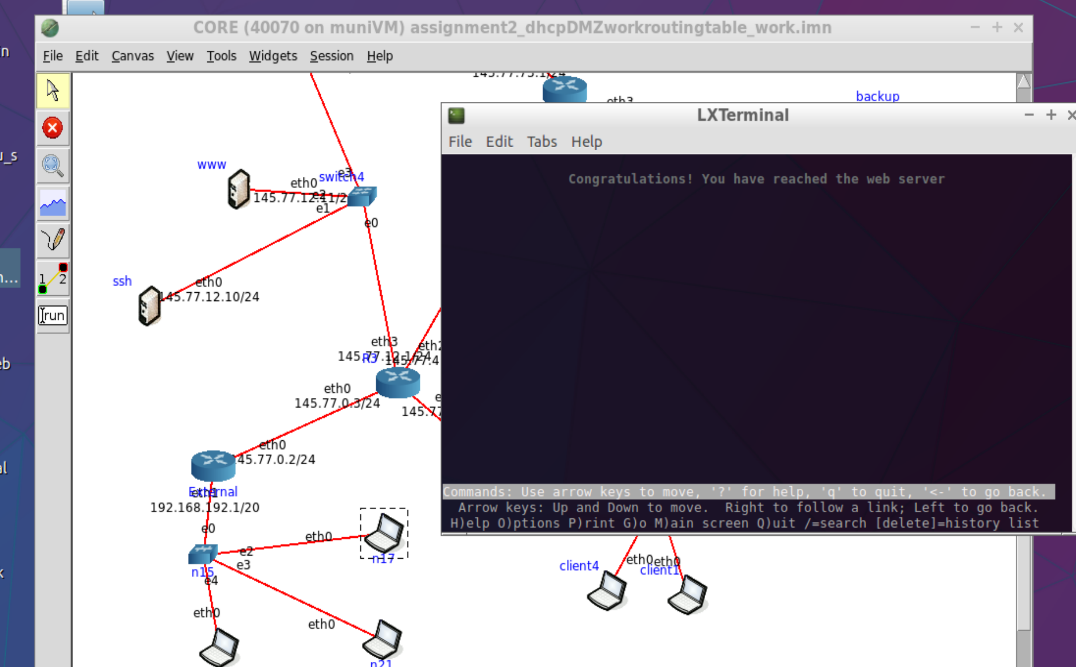


Figure 12 External client accessing www server

packets for the specific servers in the DMZ are accepted.

## Any packets from inside the company network are accepted

The fire wall rules used are:

* iptables -A INPUT -i eth1 -p all -j ACCEPT
* iptables -A INPUT -i eth2 -p all -j ACCEPT
* iptables -A INPUT -i eth3 -p all -j ACCEPT
* iptables -A OUTPUT -o eth1 -p all -j ACCEPT
* iptables -A OUTPUT -o eth2 -p all -j ACCEPT
* iptables -A OUTPUT -o eth3 -p all -j ACCEPT

### Testing

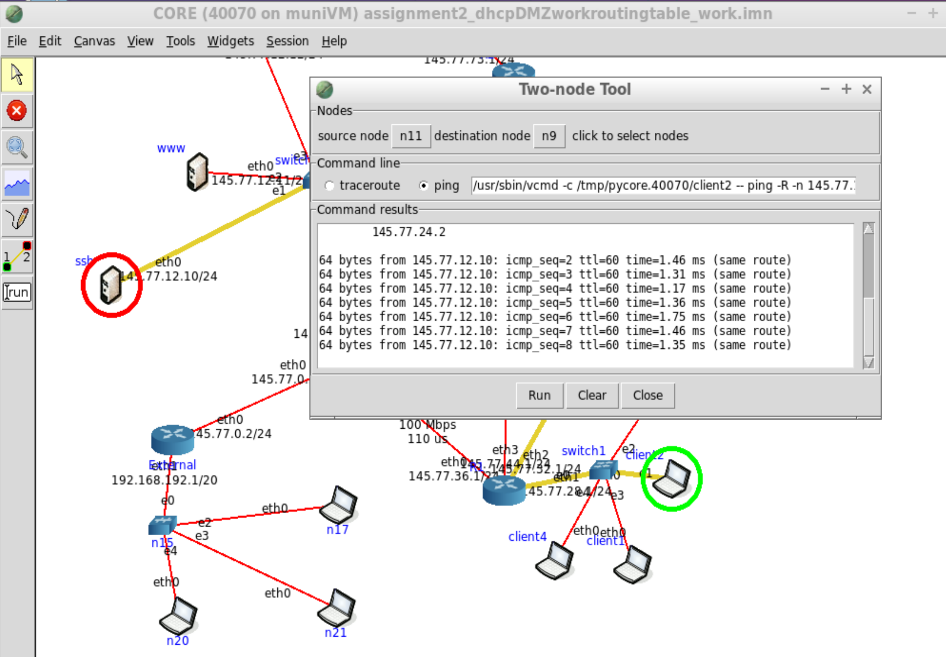


Figure 12 internal client ping SSH server

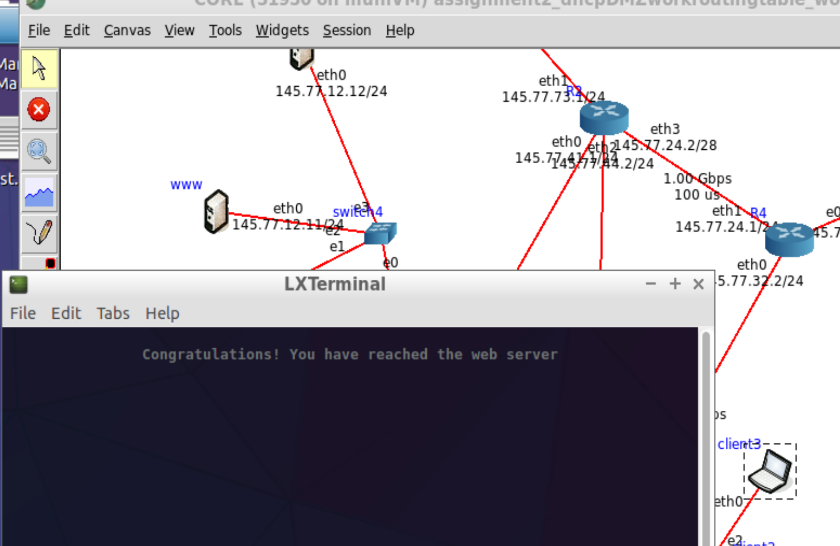


Figure 13 internal client lynx www server

Packets from inside the company are successfully accepted

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

The firewall rules used are:

* iptables -A INPUT -p all -m state --state RELATED, ESTABLISHED -j ACCEPT
* iptables -A OUTPUT -p all -m state --state RELATED, ESTABLISHED -j ACCEPT

## Any SSH packets from the **ssh** server into the company network are accepted

The firewall rule used is:

* iptables -A OUTPUT -o eth1 -p tcp --destination-port 22 -j ACCPECT

### Testing

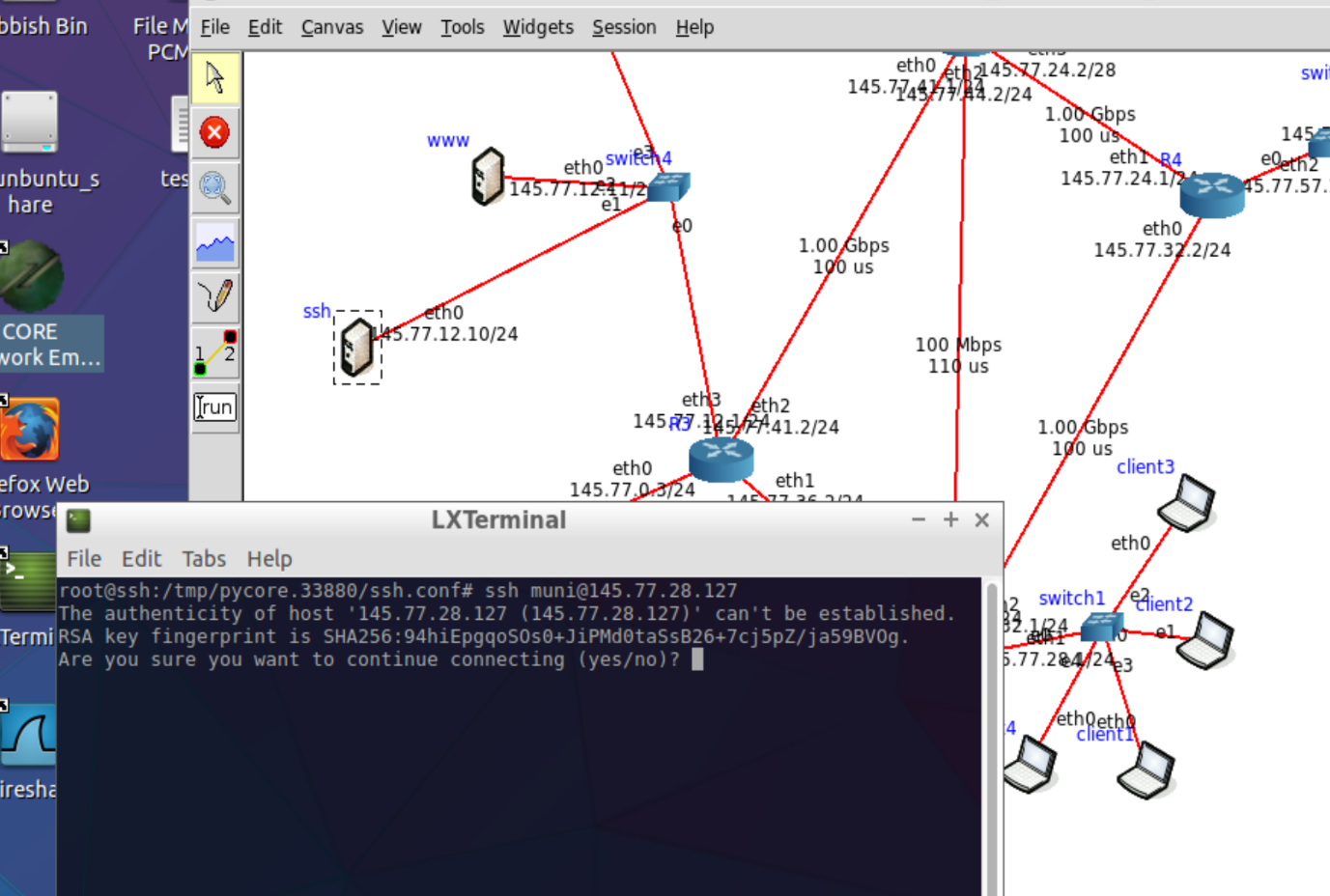


Figure 14 ssh sending ssh packet to inside client computer

## Any other packets are blocked

Firewall rules used:

* iptables -A INPUT -j DROP
* iptables -A OUTPUT -j DROP
* iptables -A FORWARDPUT -j DROP

### Testing

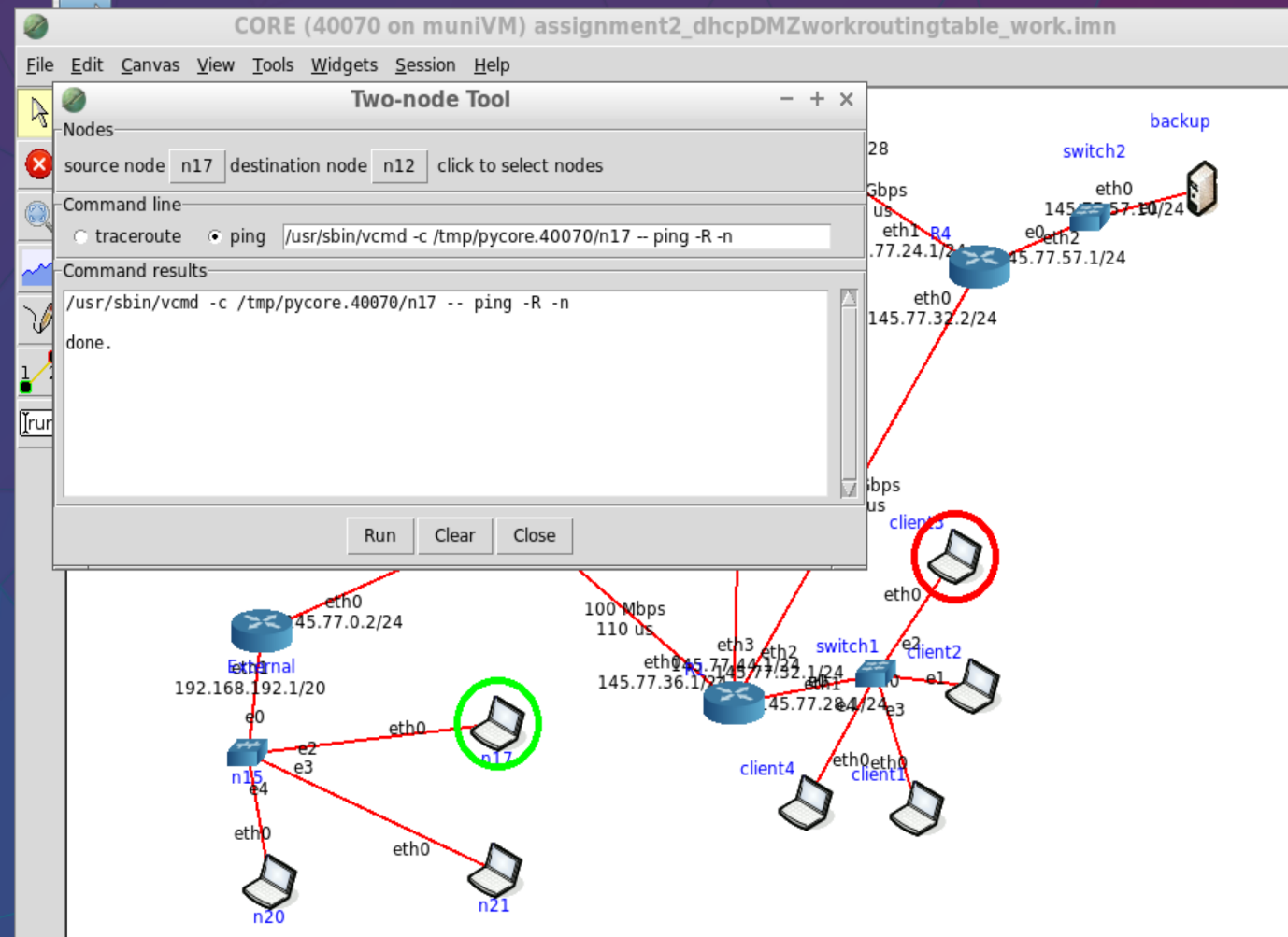


Figure 15 ICMP packet from external client to internal client is not allowed