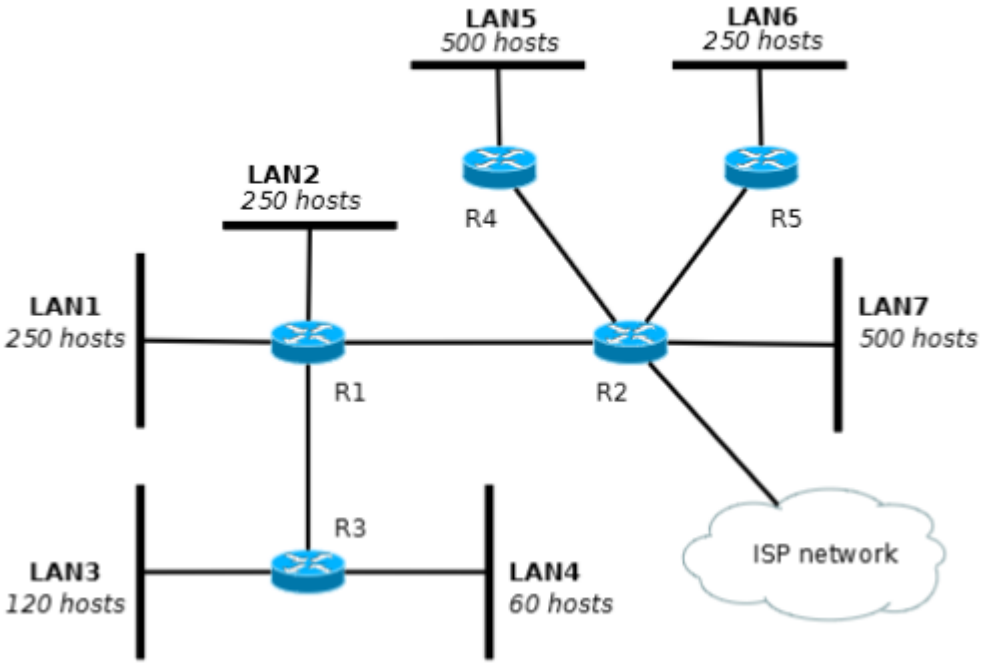
4.1 IP address Planning

Aim:

To define a IPv4 address

Network diagram:



Process:

Only one prefix 37.SN.40.0/21 is needed for the IP address planning here.

4.3 Static Routing Configuration

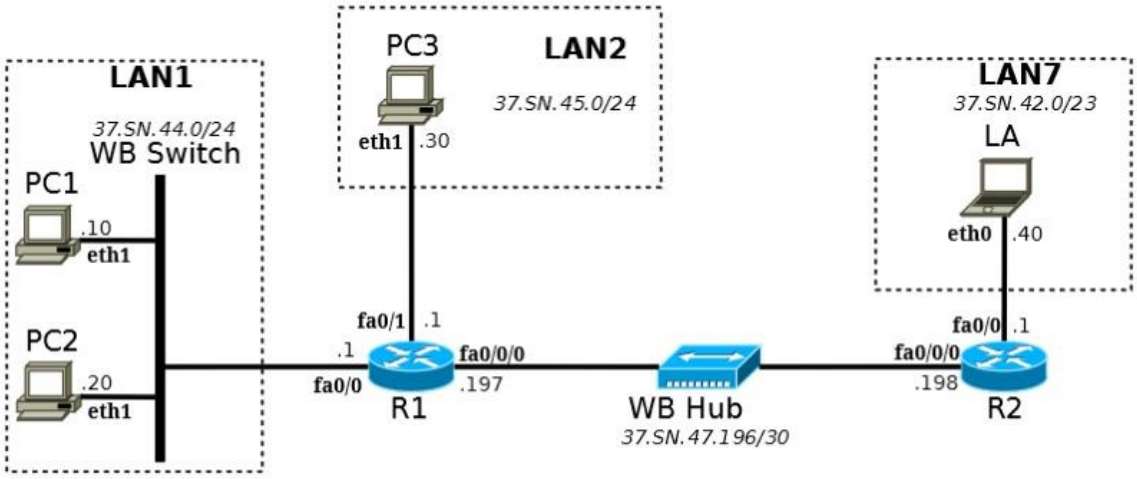
Aim:

To manually add static entries to routers' routing table.

Components Used:

Components	Quantities
PC	3
Laptop	1
Switch	1
Router	2
Hub	1

Network diagram:



Setup:

LAN1 has PC1 & PC2 connected via a switch. LAN7 has laptop. The two routers are interconnected to the Hub. PC3 is also connected to the hub. The interface fa0/1 of R1 is unplugged.

Process:

The default gateway is set and the eth0 interface is used for SLC to manage the router.

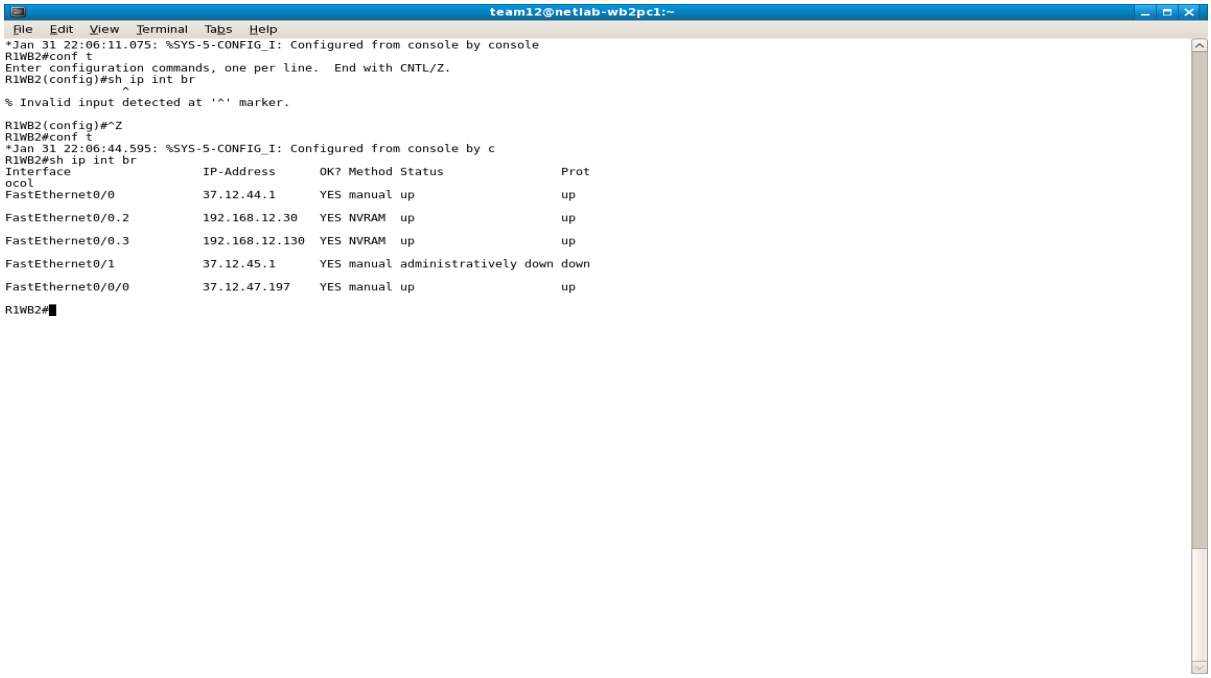


Fig 4.2.1 Router configuration using SLC

The routing table of each router is checked using **show ip route** command in privileged EXEC mode and the laptop tries pinging to PC1

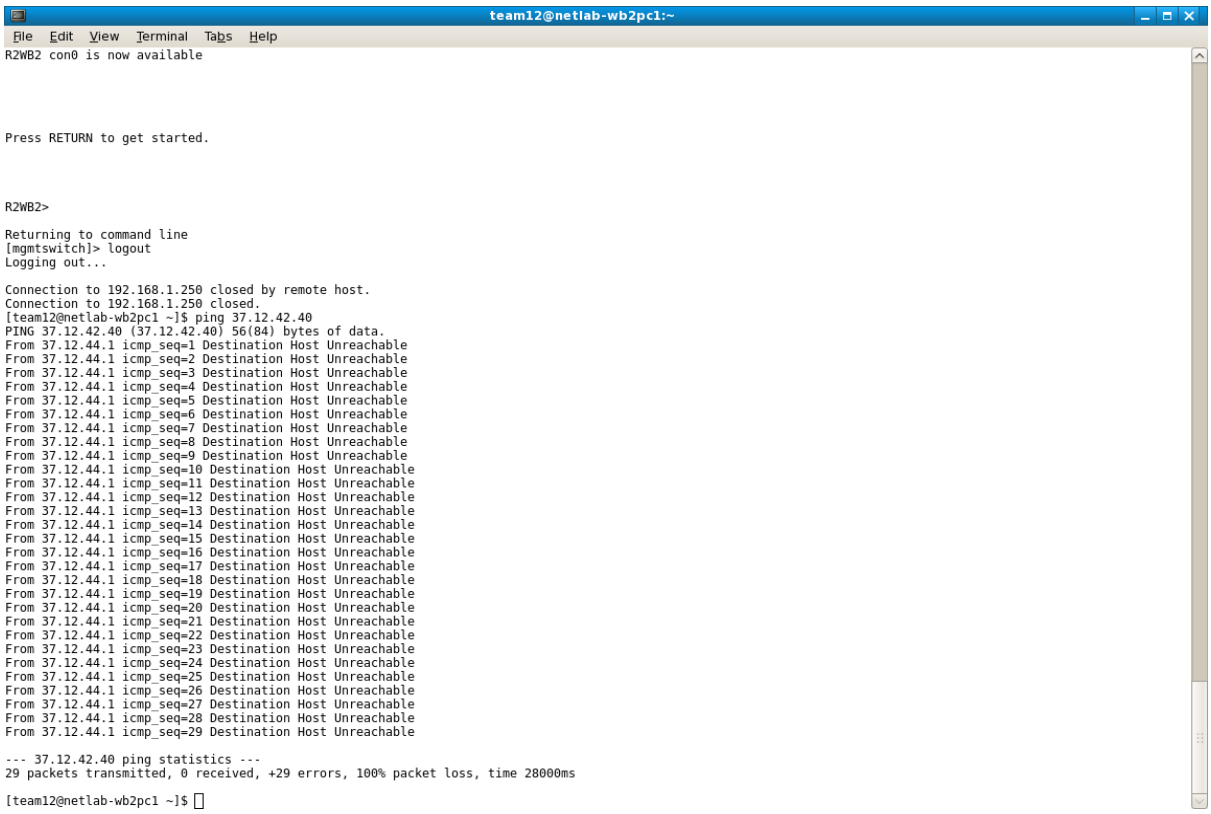


Fig 4.2.2 Failed ping from PC1 to laptop

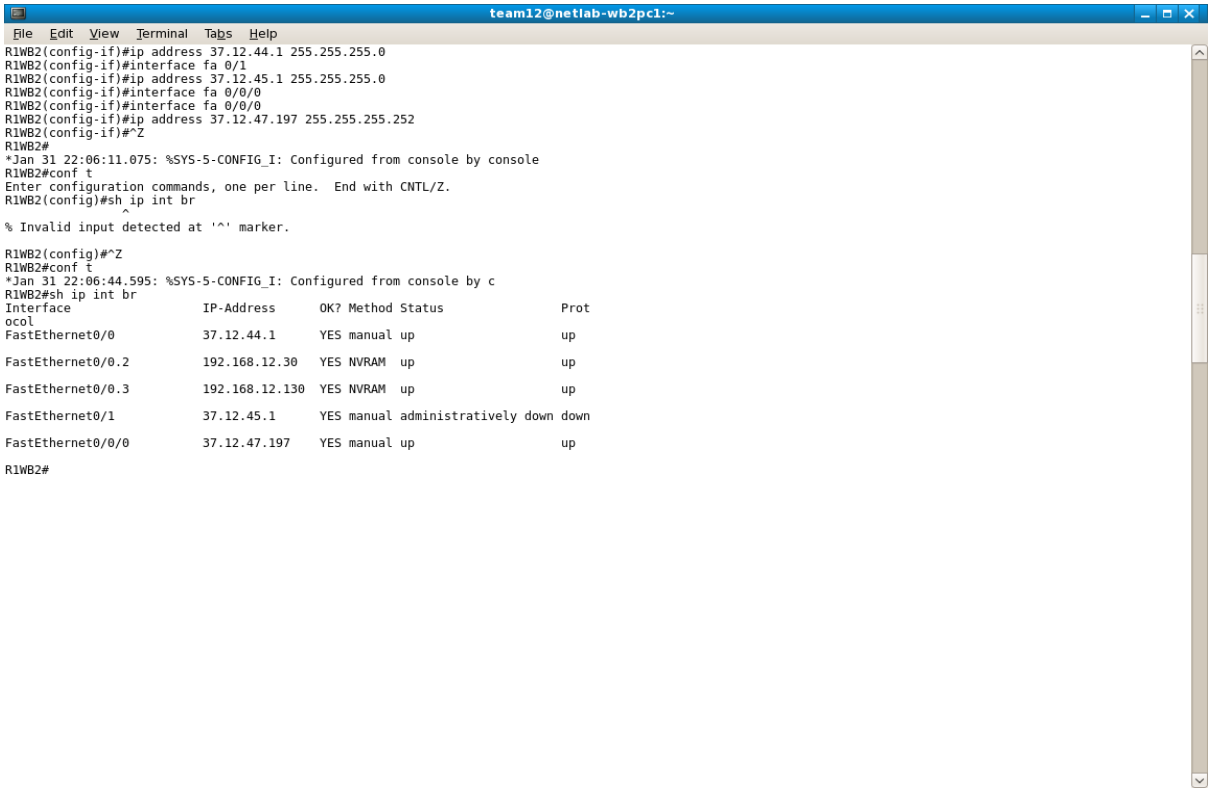


Fig 4.2.3 Directly connected route of R1

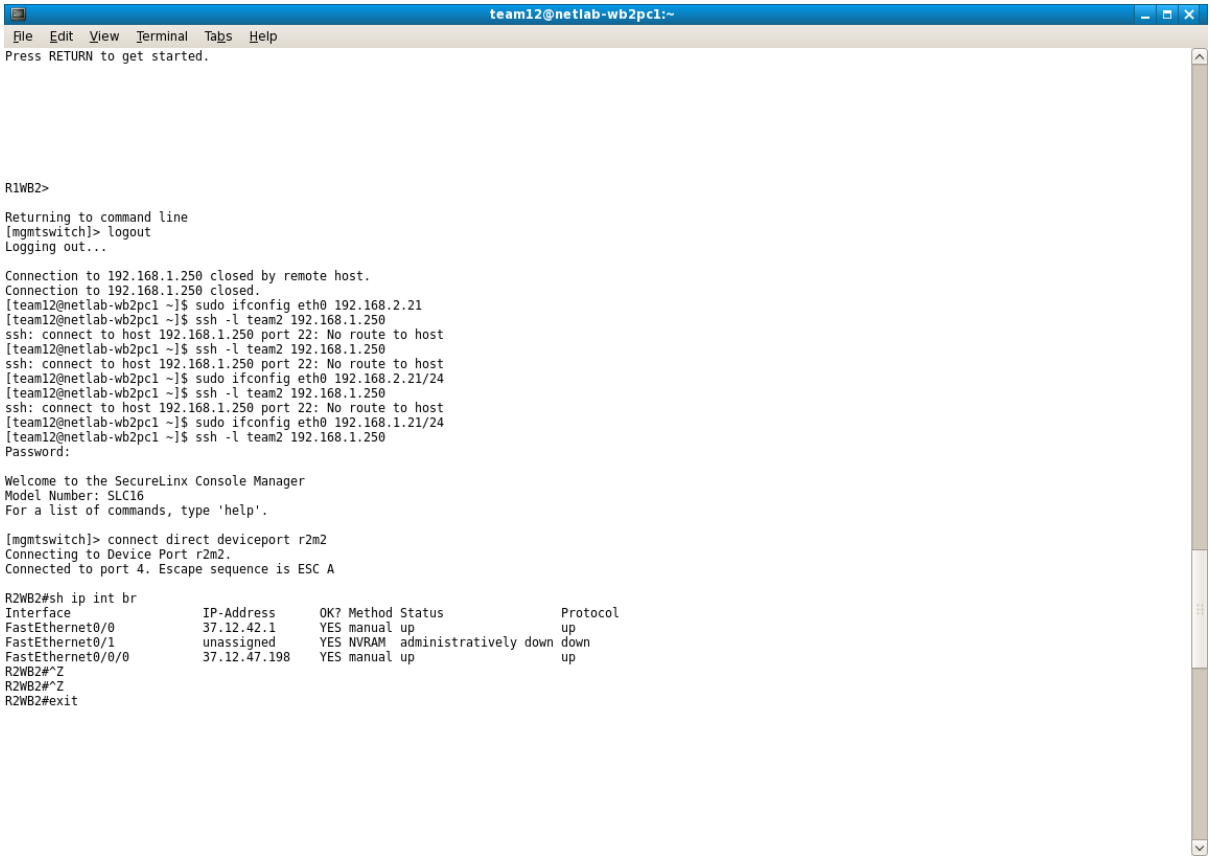


Fig 4.2.4 Directly connected route of R2

The above two figures show the directly connected routes of R1 and R2. Now, the static route is added by using the following command in global configuration mode

ip route <destination network> <netmask> <next hop address>

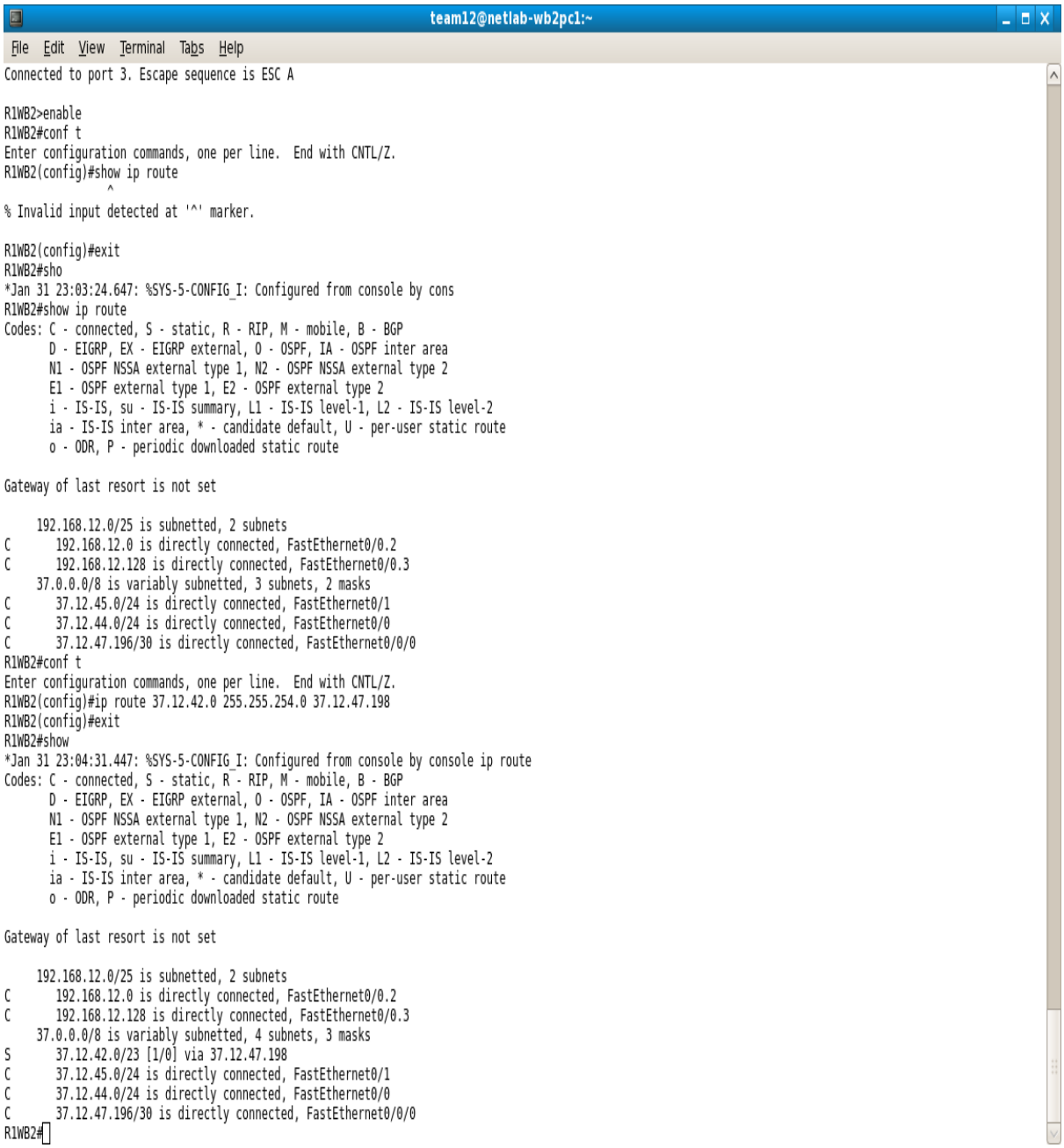


Fig 4.2.5 Static route configuration for R1

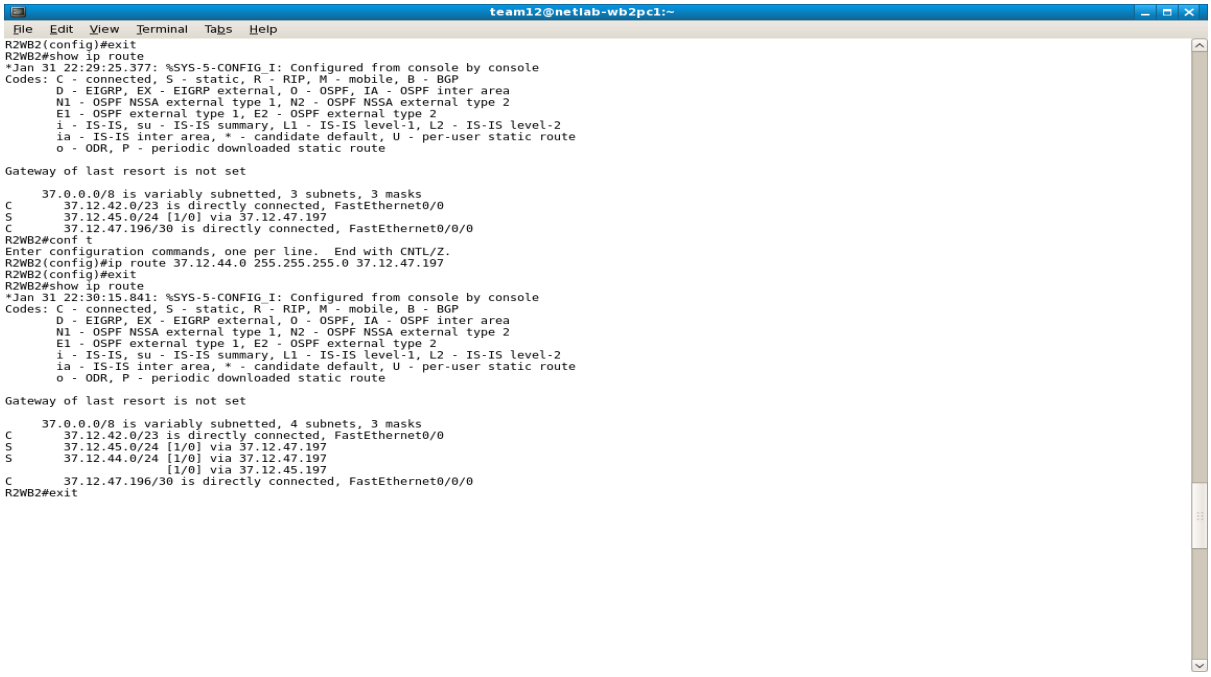


Fig 4.2.6 Static route configuration for R2

Now the **ping** command is used to verify the connectivity between LAN1 and LAN7. Then, **traceroute** is also used to study the path followed.

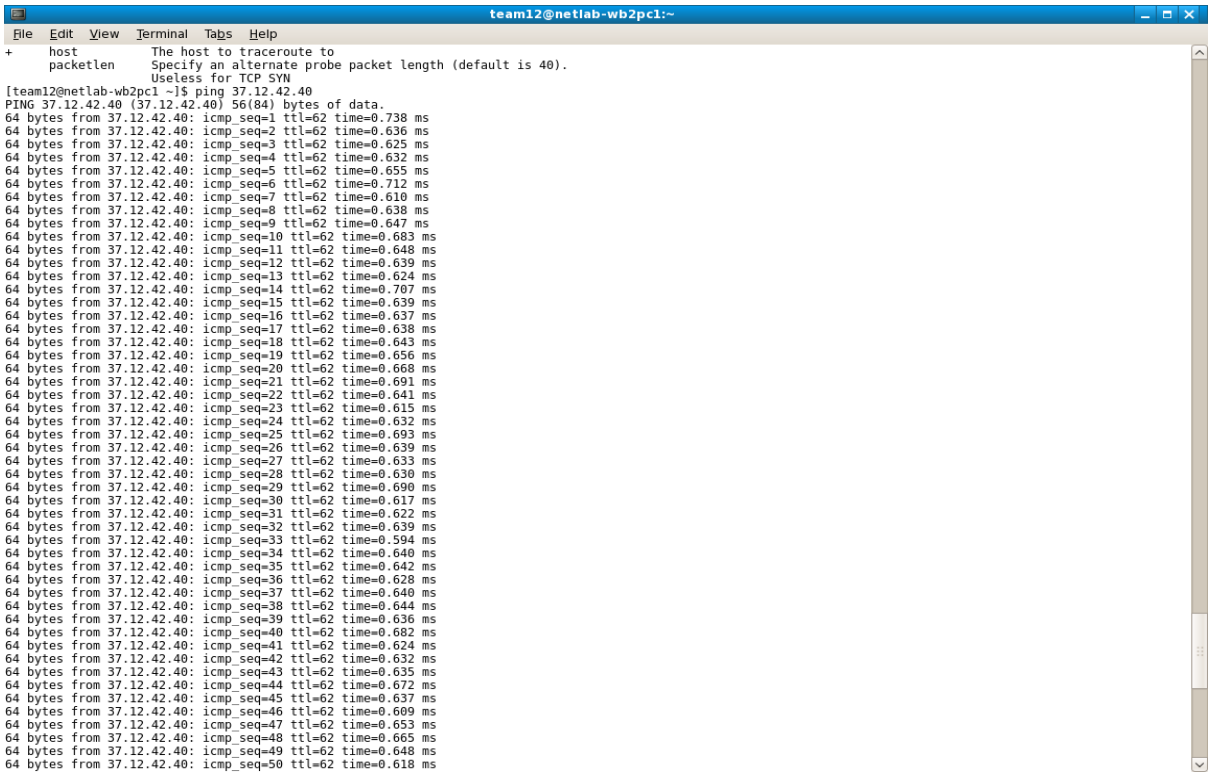


Fig 4.2.7 Successful ping from PC1 to laptop

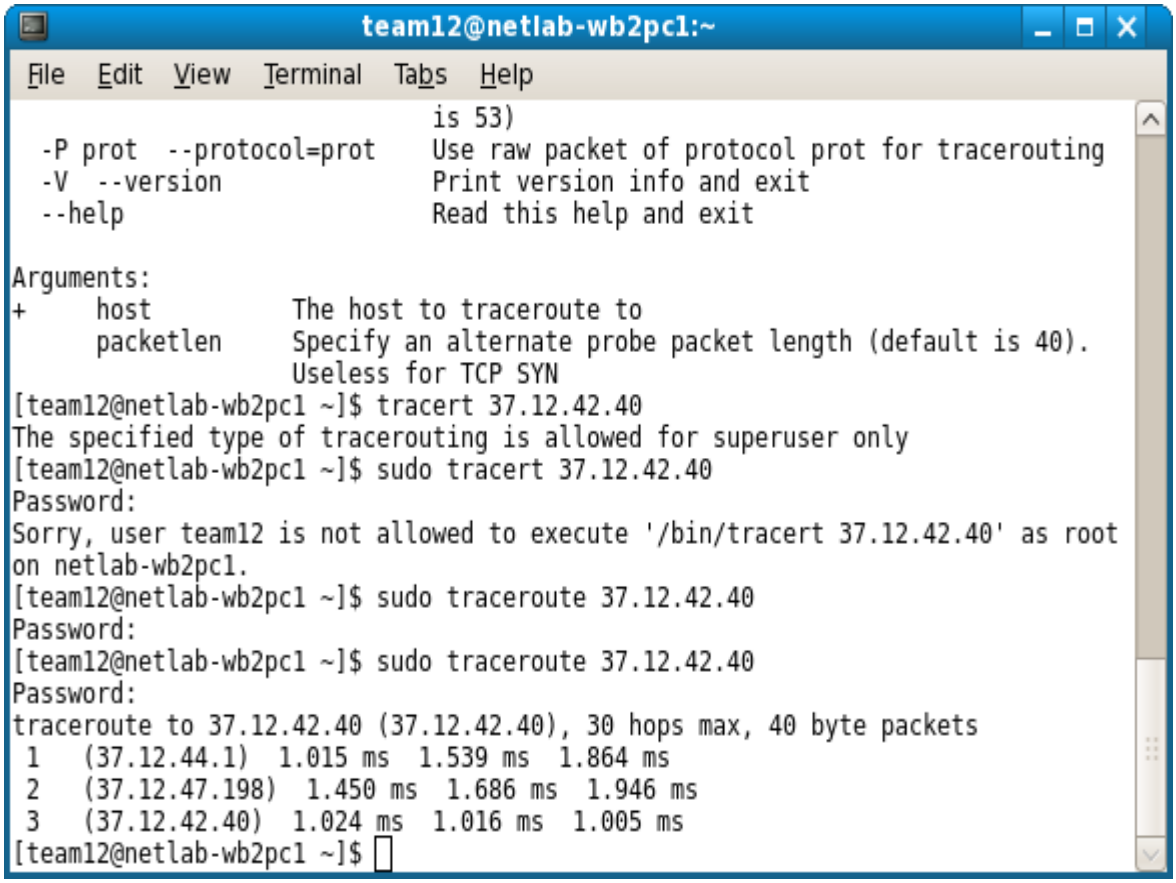


Fig 4.2.8 Traceroute

4.3 Configure DHCP server in Linux

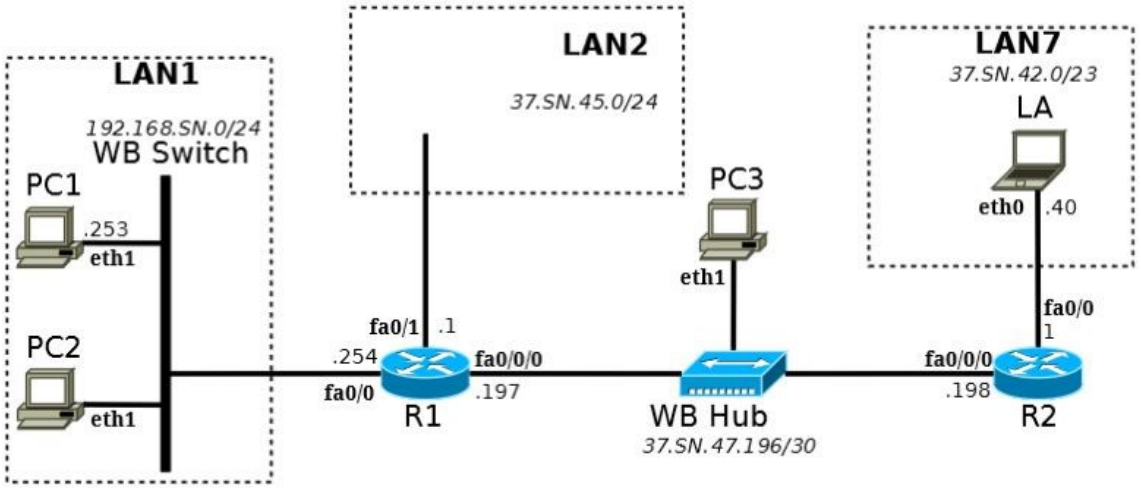
Aim:

To configure Linux machine as a DHCP server.

Components Used:

Components	Quantities
PC	3
Laptop	1
Switch	1
Router	2
Hub	1

Network diagram:



Setup:

LAN1 has PC1 & PC2 connected via a switch. LAN7 has laptop. The two routers are interconnected to the Hub. PC3 is also connected to the hub. The interface fa0/1 of R1 is unplugged.

Process:

The IP address of fa0/0 of R1 to **192.168.SN.254/24**. The DHCP server IP address is set to **192.168.SN.253/24.** In the Linux, dhcpd daemon is configured and the IP address in the range of 192.168.SN.1 to 192.168.SN.250 with netmask 255.255.255.0 is got.

The DHCP server on PC1 can be started using the command **sudo /etc/init.d/dhcpd start** and wireshark is ran on PC1 and laptop

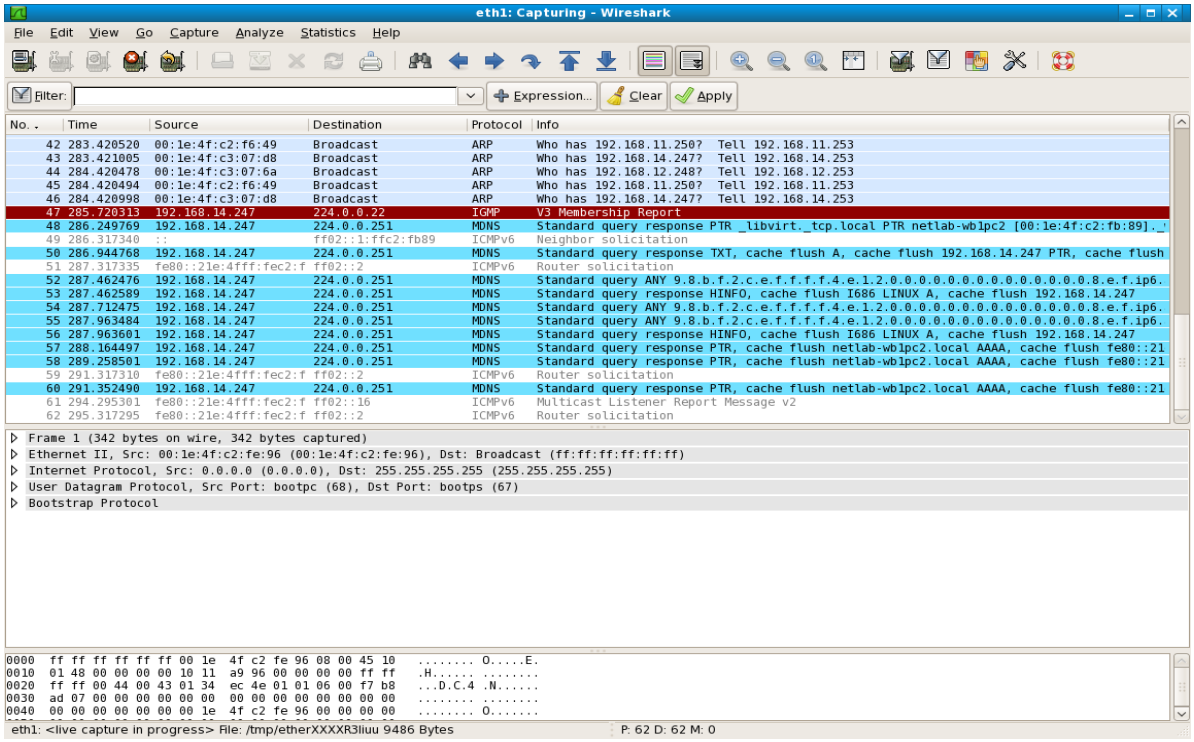


Fig 4.3.1 Wireshark in PC1

The DHCP client is ran on PC2 using the command **sudo dhclient eth1** and the output is observed. To stop the DHCP client, a DHCPRELEASE message must be sent using **sudo dhclient –r eth1**

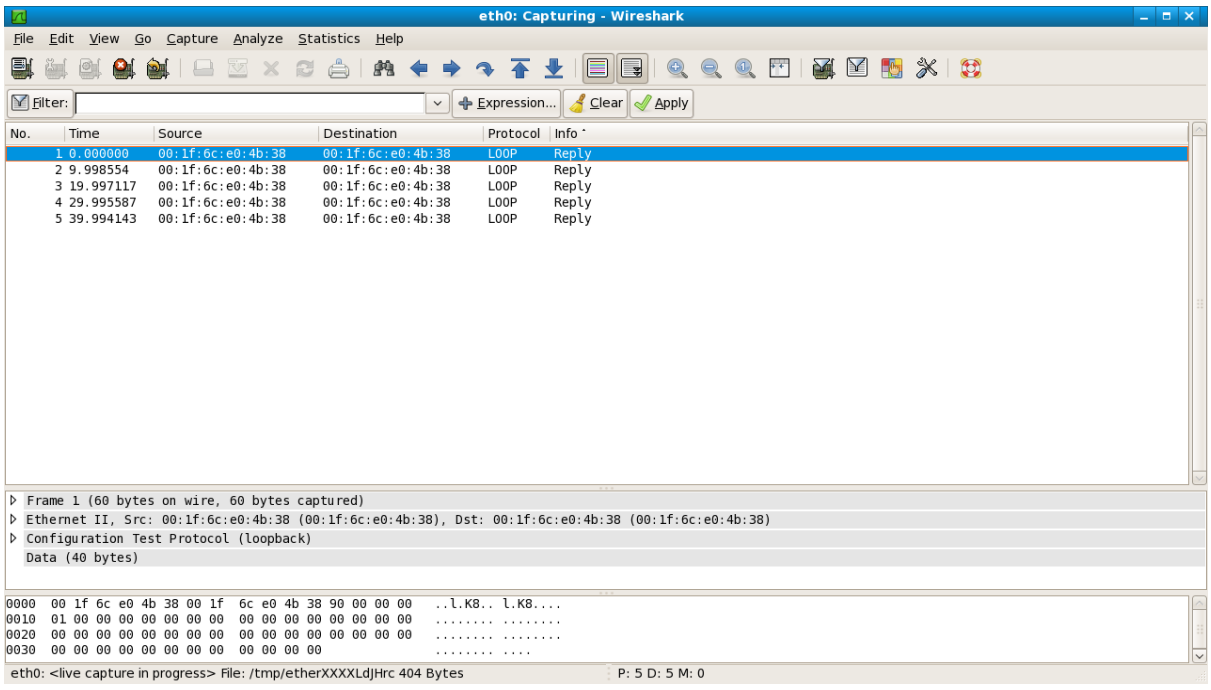


Fig 4.3.2 Wireshark in Laptop

The DHCP traffic captured by Wireshark and the configuration file is reported.

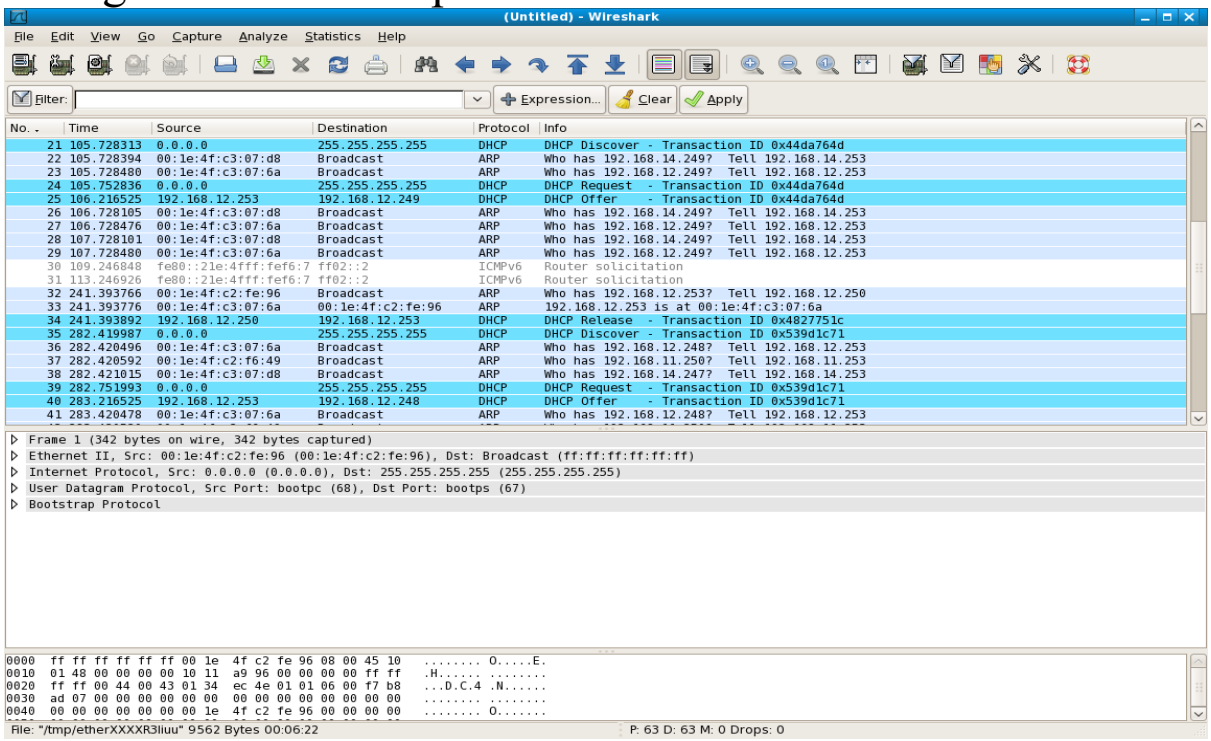


Fig 4.3.3 DHCP traffic in Laptop

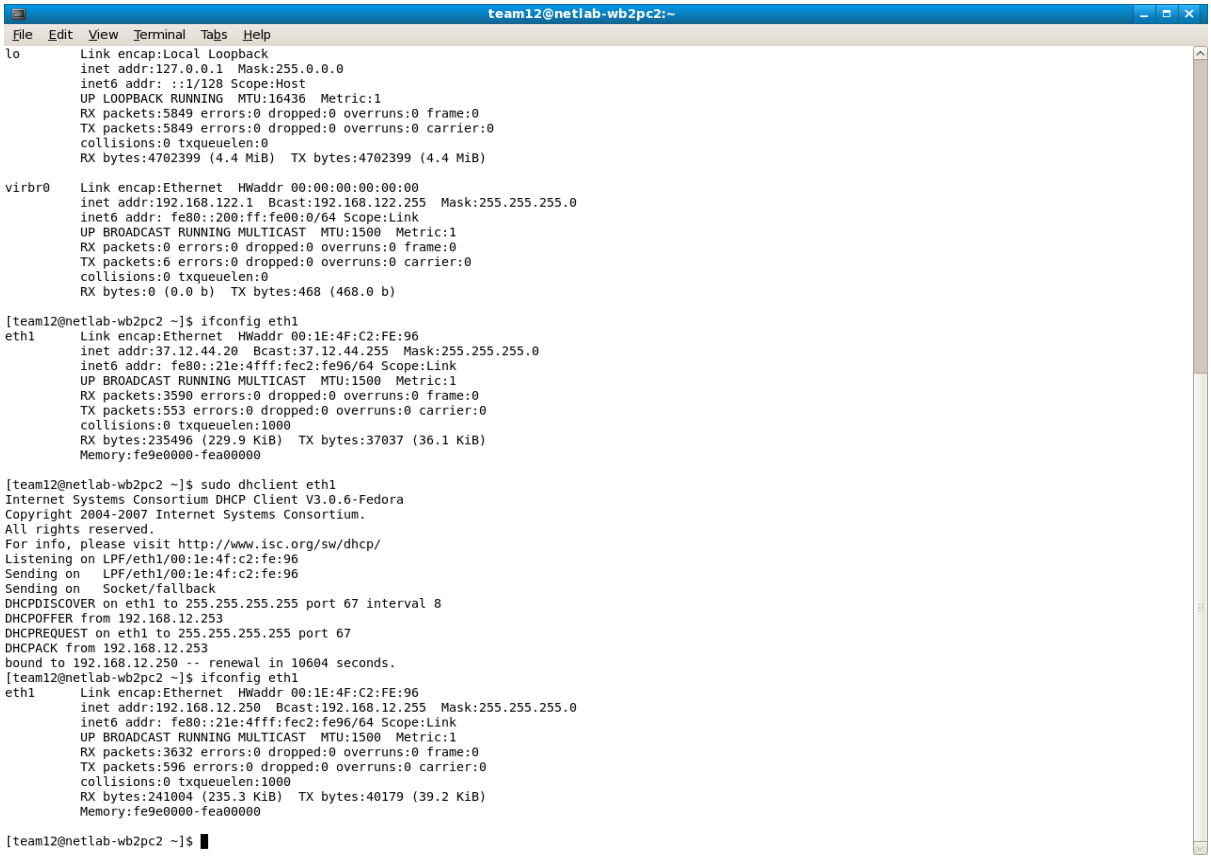


Fig 4.3.4 Configuration file

4.4 Configure NAT

4.4.1 Provide outbound connections

Aim:

To configure outbound NAT on R1 so that source IP address is changed one of the IP address in a predefined pool.

Process:

Ping from PC2 to laptop is tried and an error message is got. The following commands are executed,

access-list 1 permit 192.168.SN.0 0.0.0.255
ip nat pool myPool 37.SN.44.1 37.SN.44.1 prefix-length 24

The above commands are executed in global configuration mode. Then its switched to interface configuration mode and the commands below are done.

interface fa0/0
ip nat inside
interface fa0/0/0
ip nat outside

Then its again changed to global configuration mode and NAT is enabled.

exit
ip nat inside source list 1 pool myPool overload

Laptop is pinged from PC2 and the traffic is captured using Wireshark on both PC2 and PC3.

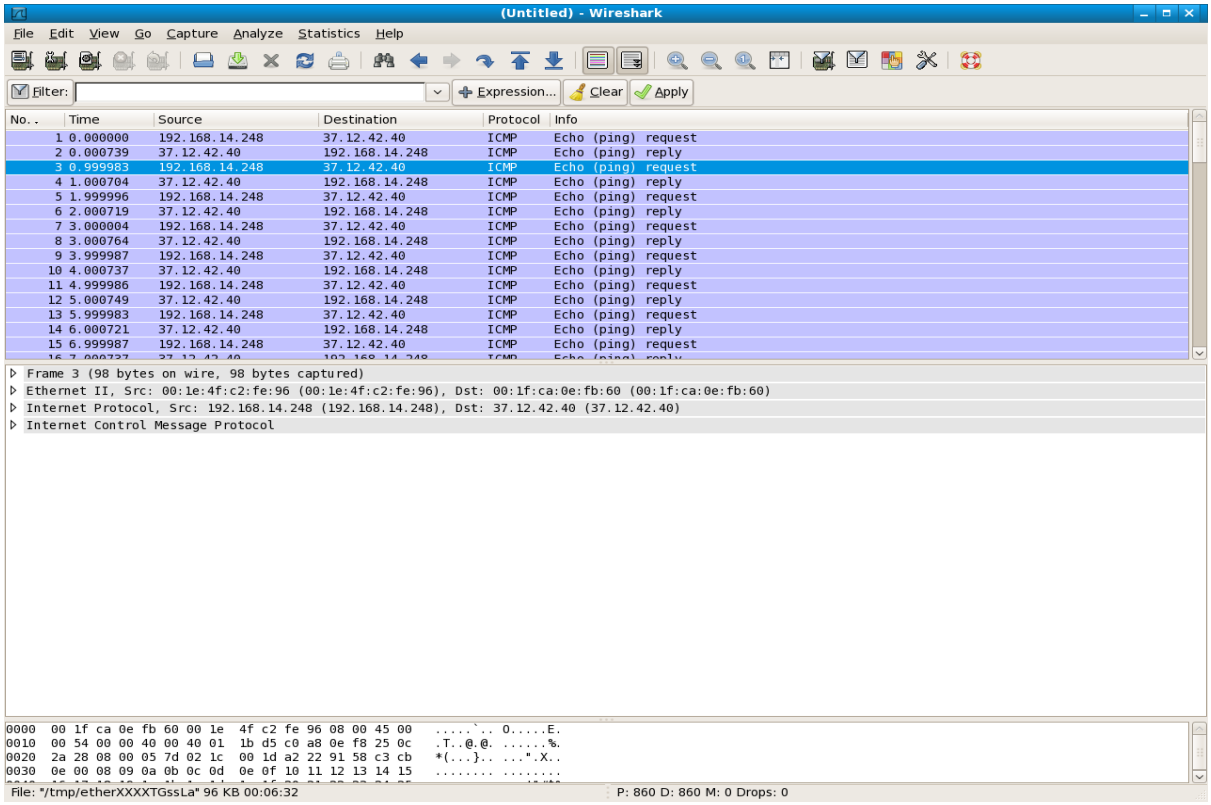


Fig 4.4.1.1 Wireshark traffic captured in PC2

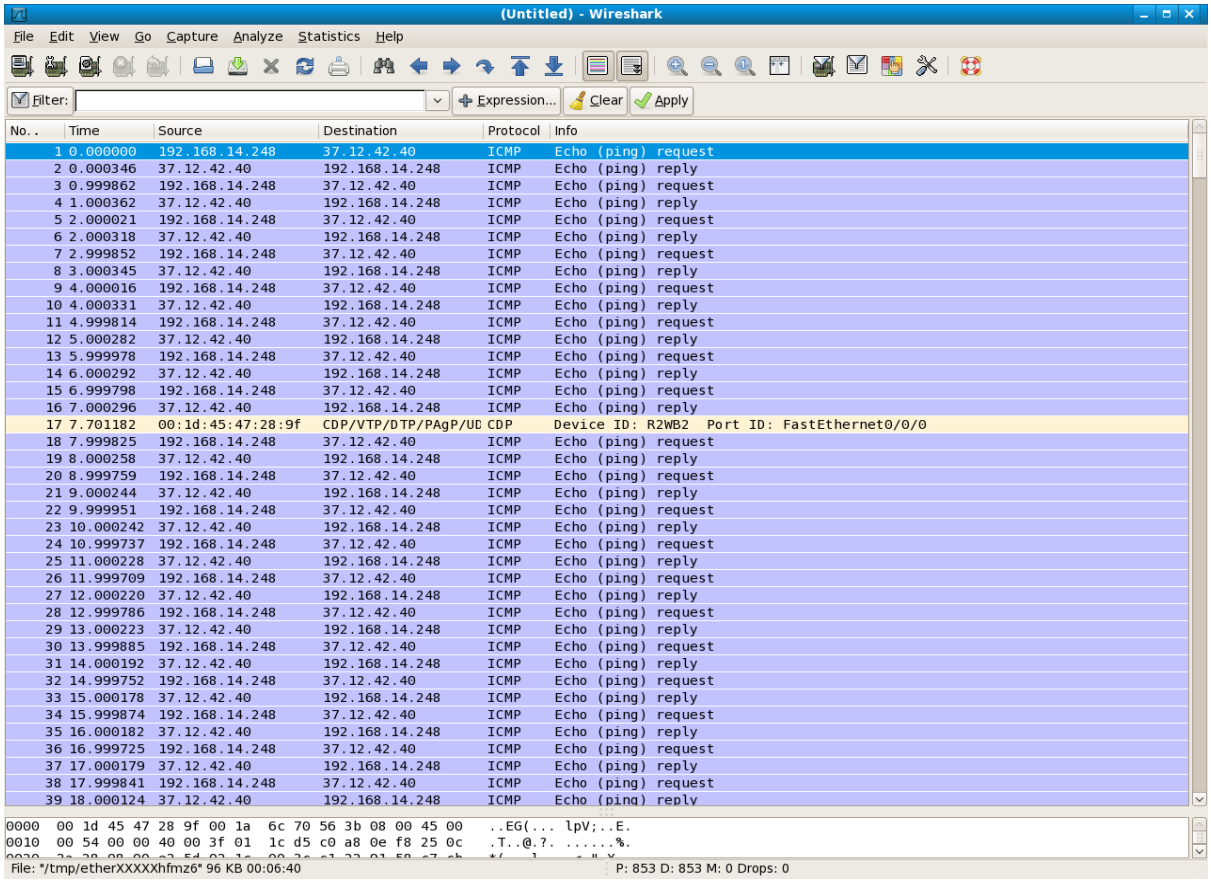


Fig 4.4.1.2 Wireshark traffic captured in PC3

In the privileged EXEC mode, the current status of the NAT table is checked using **show ip nat translations [verbose]** and the entire content of the current NAT table is cleared using **clear ip nat translation ***

4.4.2 Provide inbound NAT

Aim:

To configure port forwarding

Process:

The webserver is started on PC1 using the command **sudo /etc/init.d/httpd start** and from PC2 webpage with IP address **http://192.168.SN.253** is opened

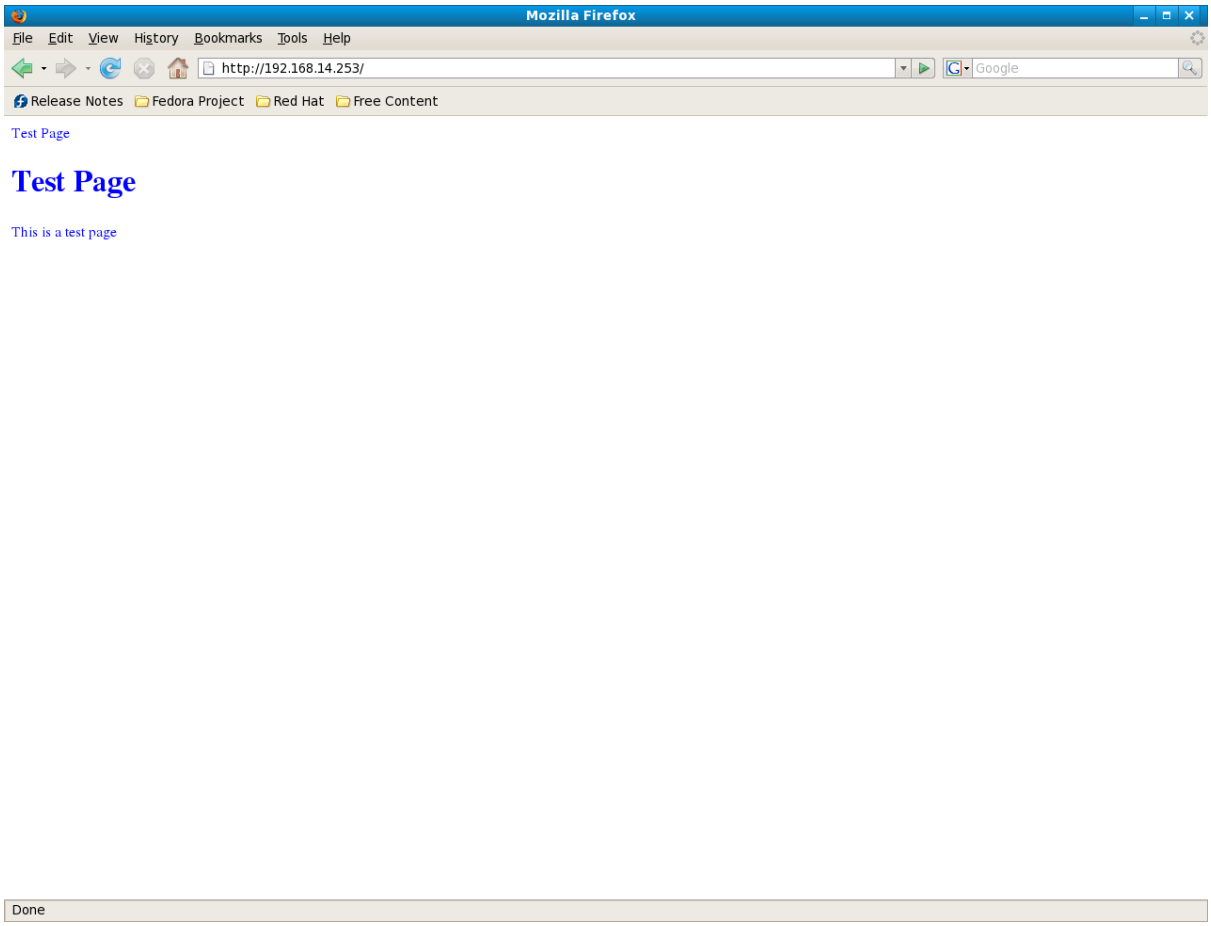


Fig 4.4.2.1 Webpage in PC2

But the webpage cannot be opened from Laptop since there is no way for using service hosted on internal server PC1. This problem is solved using port forwarding as below

ip nat inside source static tcp 192.168.SN.253 80 37.SN.45.1 8080

Now the webpage hosted on PC1 can be opened in Laptop using the url **http://37.SN.45.1:8080**

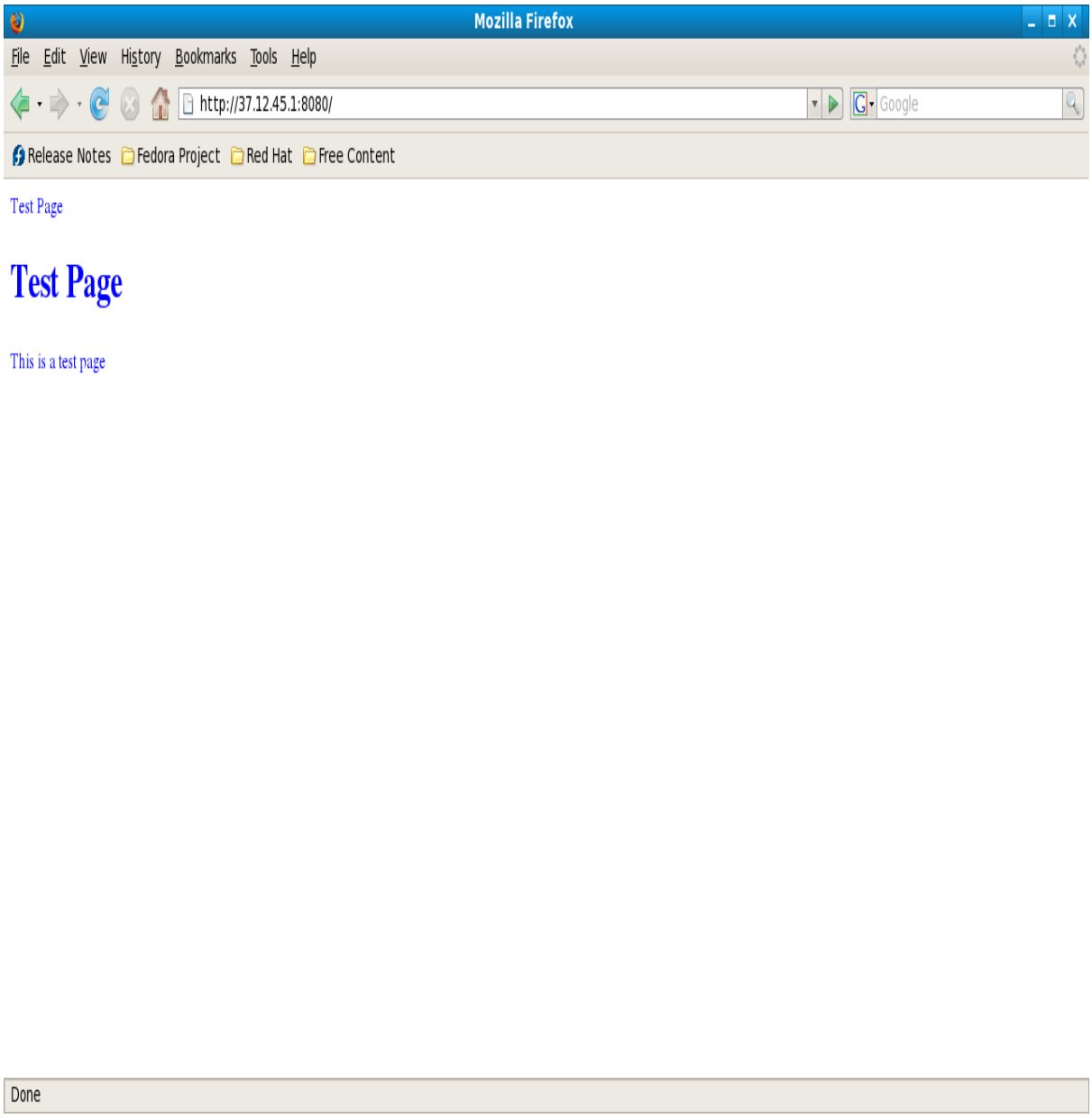


Fig 4.4.2.2 Webpage opened in Laptop

Then the status of NAT table on R1 is reported

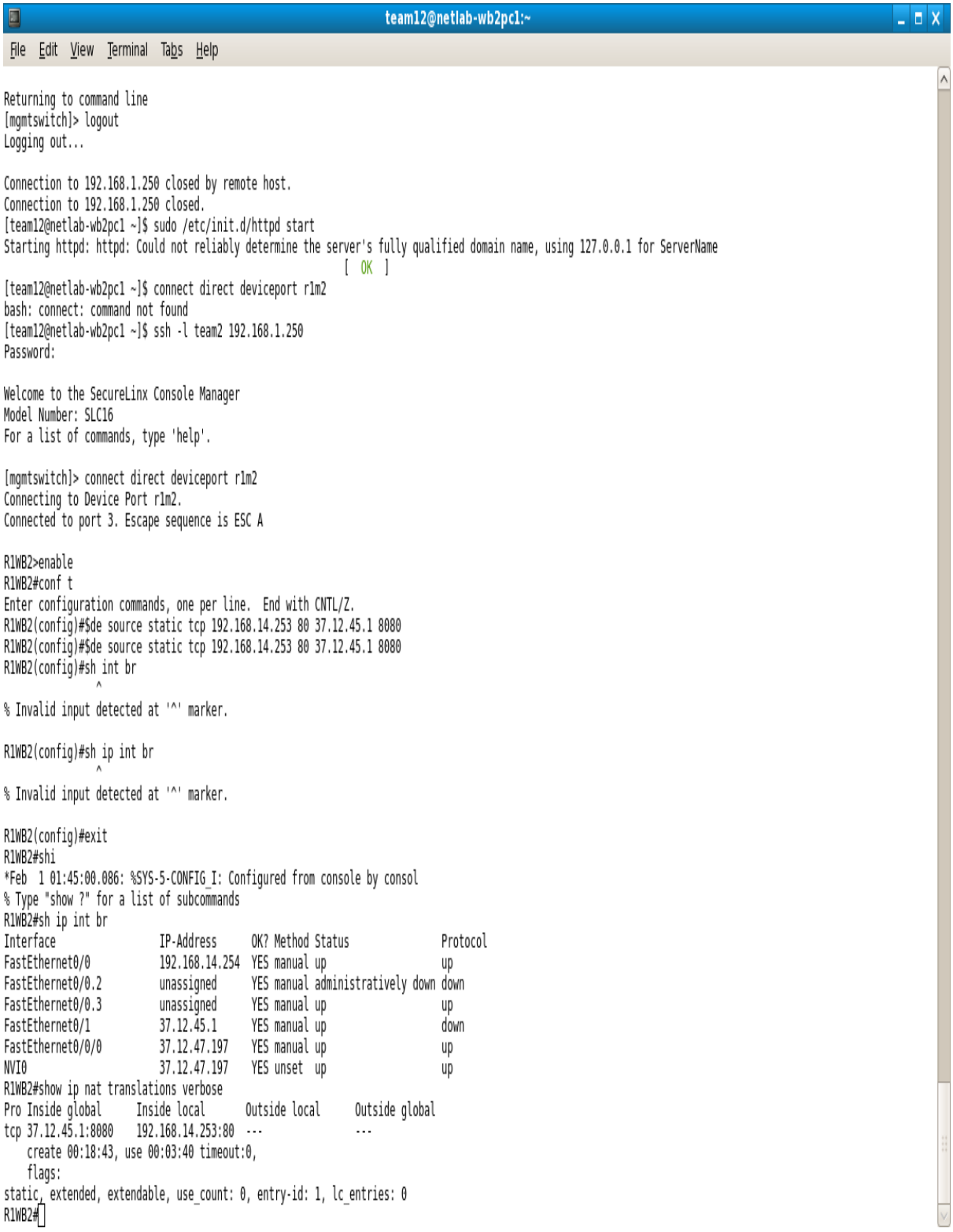


Fig 4.4.2.3 R1 NAT table status

The output of **show run** which is validated in privileged EXEC mode is done for both the routers.

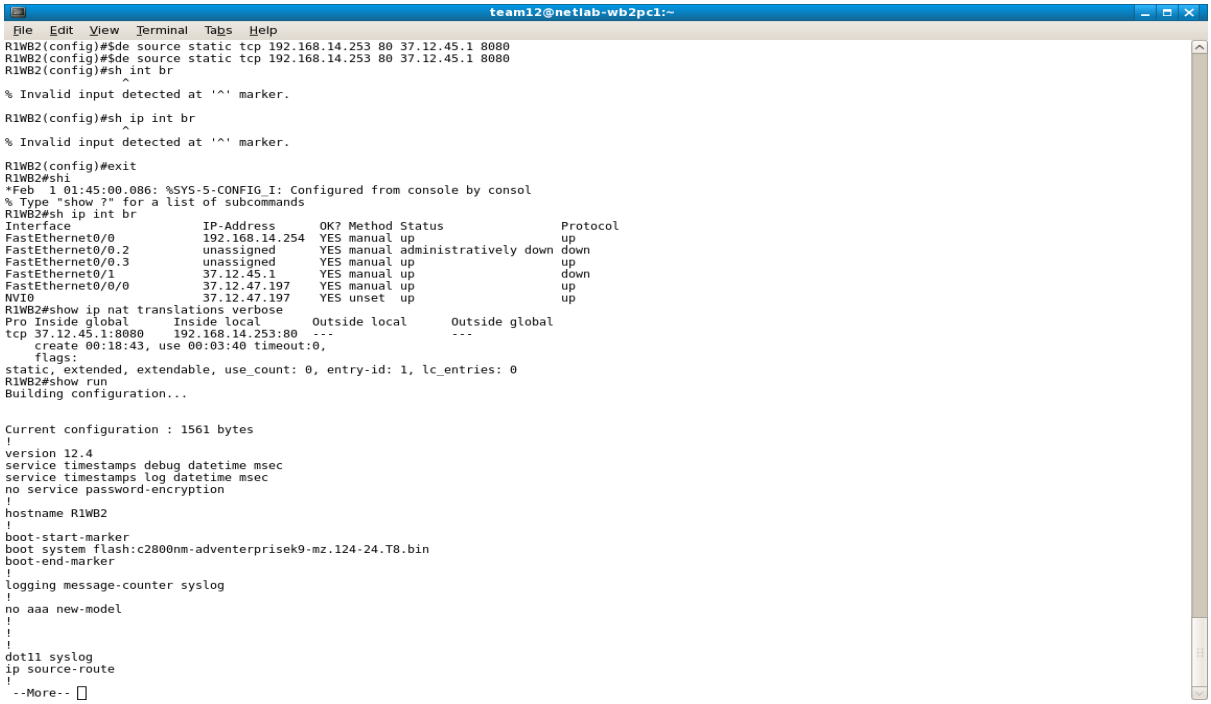


Fig 4.4.2.4 Output of show run in R1

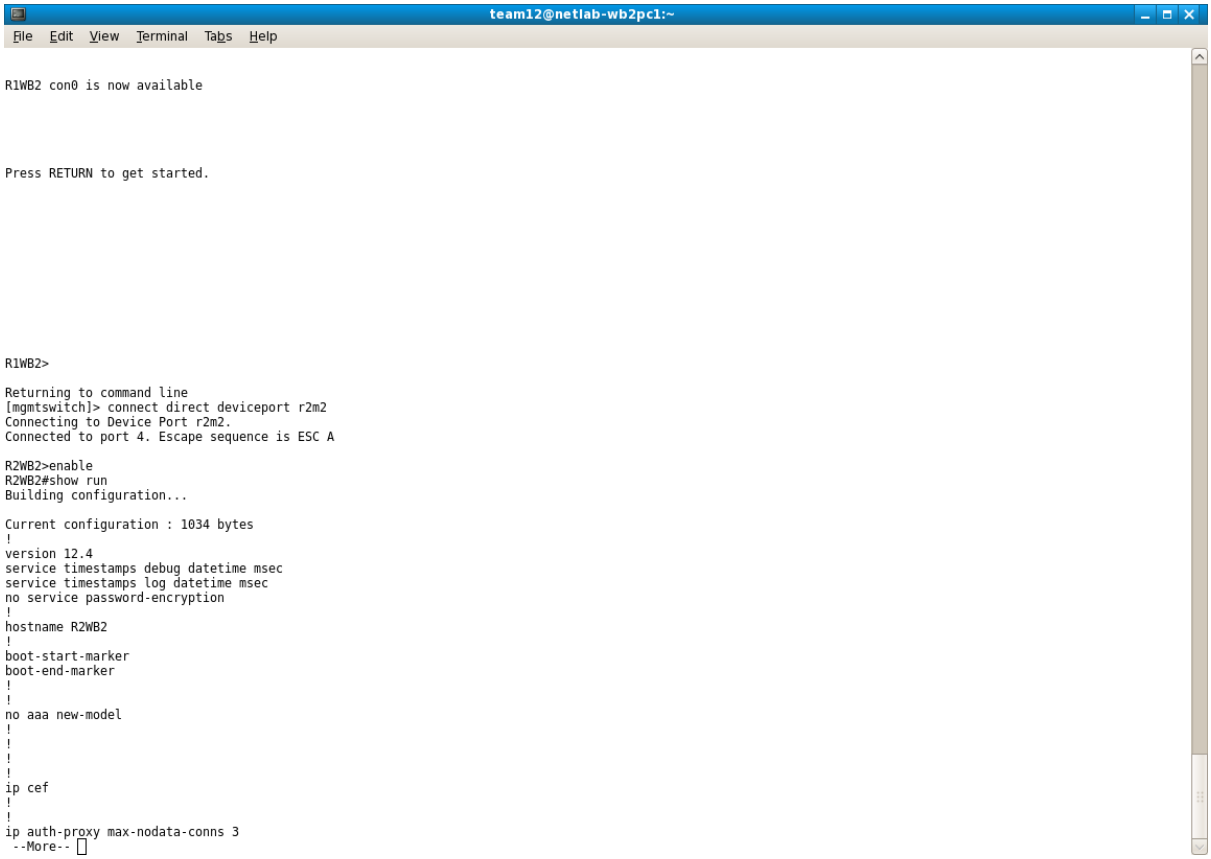


Fig 4.4.2.5 Output of show run in R2