UCCN2243

Internetworking Principles and Practices

Assignment

Name	Student ID	Practical Group	Course
Wan Jia Xin	1806623	7	CS
Tai Jia Wei	1806718	7	CS
Lee Gui Hong	1806414	7	CS
Koh Wai Yang	1703761	7	IA

Contents

Question 1 (a)

We propose adding a Router and using ACL. In the proposed router, we implement trunking and Access List to control the flow of the network. The new router is shown as below in figure 1 and the network are configured accordingly.

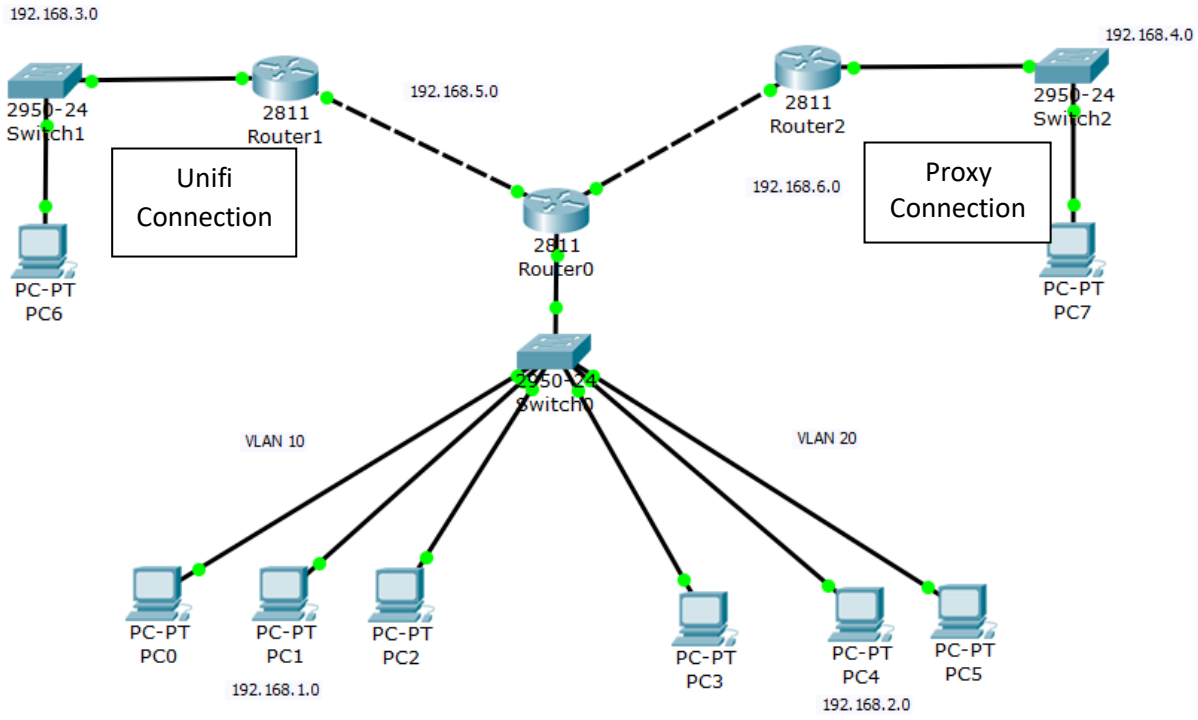

Figure 1

Question 1 (b)

Requirements 1: Section A PCs need a Unifi Connection while Section B PCs require a Proxy Connection

For the first requirement, we use the following command to set ACL as shown in Figure 2

Network A to UNIFI Network, but not Proxy Network

Router0(config)#access-list 100 permit icmp 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Router0(config)#int fa0/0.1

Router0(config)#ip access-group 100 in

Network B to Proxy Network, but not UNIFI Network

Router0(config)#access-list 101 permit icmp 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255

Router0(config)#int fa0/0.2

Router0(config)#ip access-group 101 in

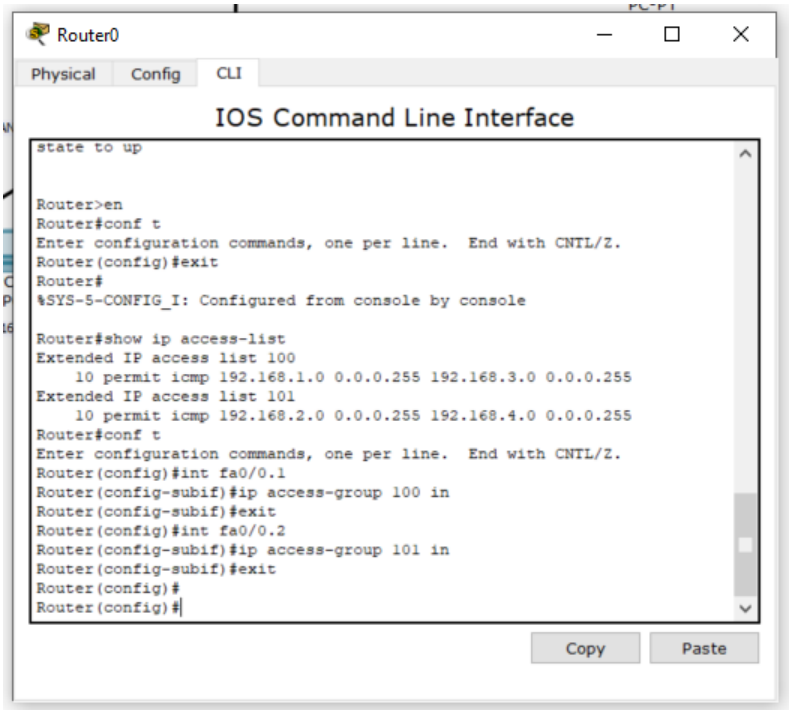

Figure 2

And as you can see in Figure 3, PC 3 is able to ping the Proxy Network, but cannot ping UNIFI Network.

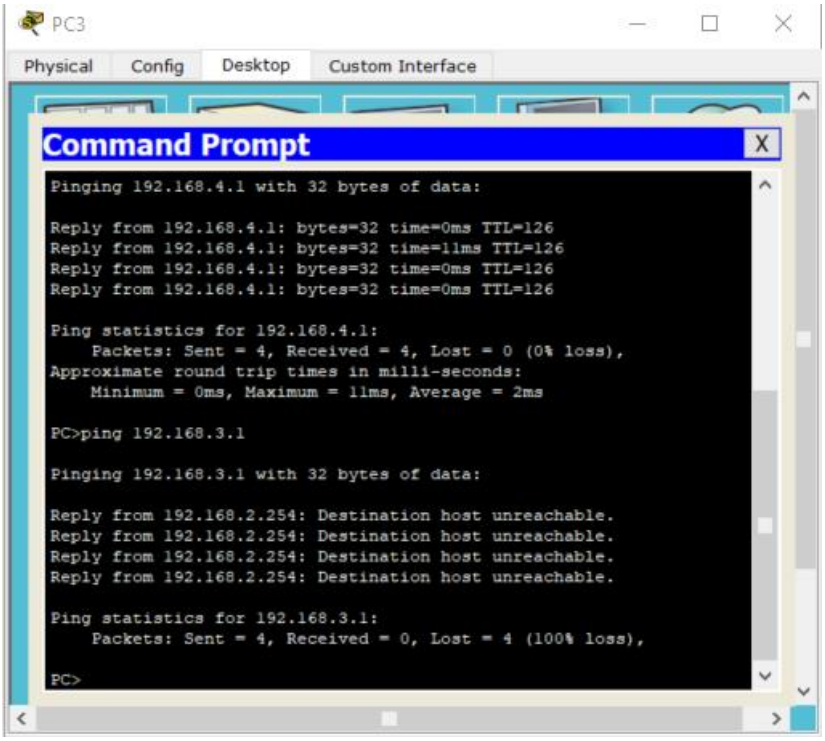

Figure 3

And in Figure 4, PC 0 is able to ping the UNIFI Network, but cannot ping Proxy Network.

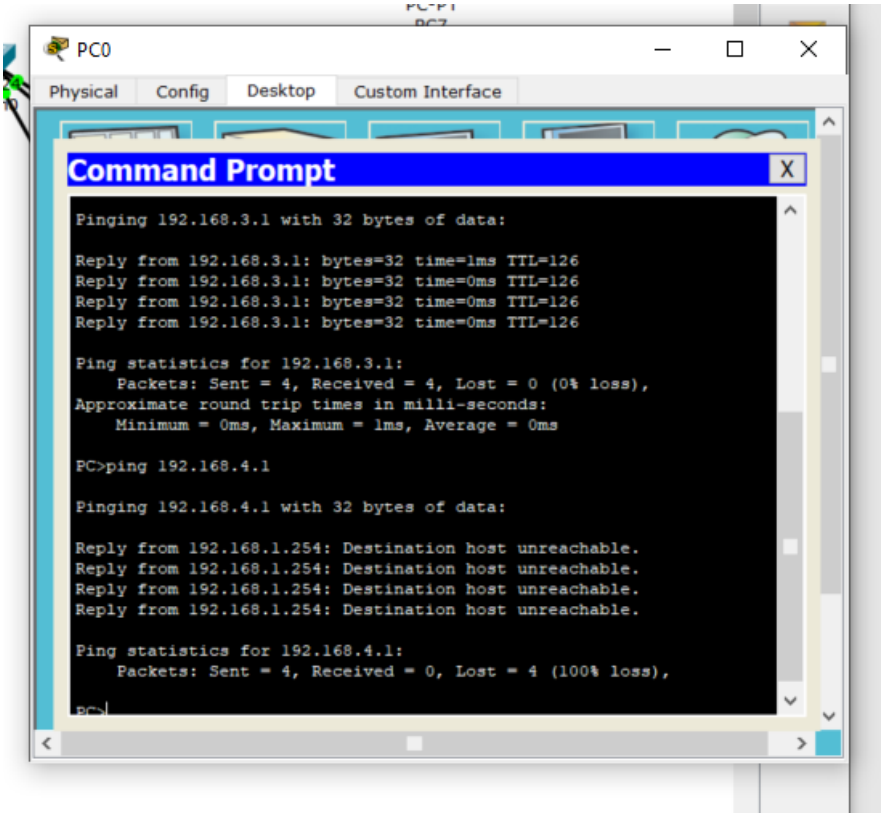

Figure 4

Requirements 2: Section A PCs need a Proxy Connection while Section B PCs require a Unifi Connection

To configure the second requirements, go to Router 1 and type the following commands, as shown in Figure 5:

Network A to Proxy Network, but not UNIFI Network

Router0(config)#access-list 102 permit icmp 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255

Router0(config)#int fa0/0.1

Router0(config)#ip access-group 102 in

Network B to UNIFI Network, but not Proxy Network

Router0(config)#access-list 103 permit icmp 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255

Router0(config)#int fa0/0.2

Router0(config)#ip access-group 103 in

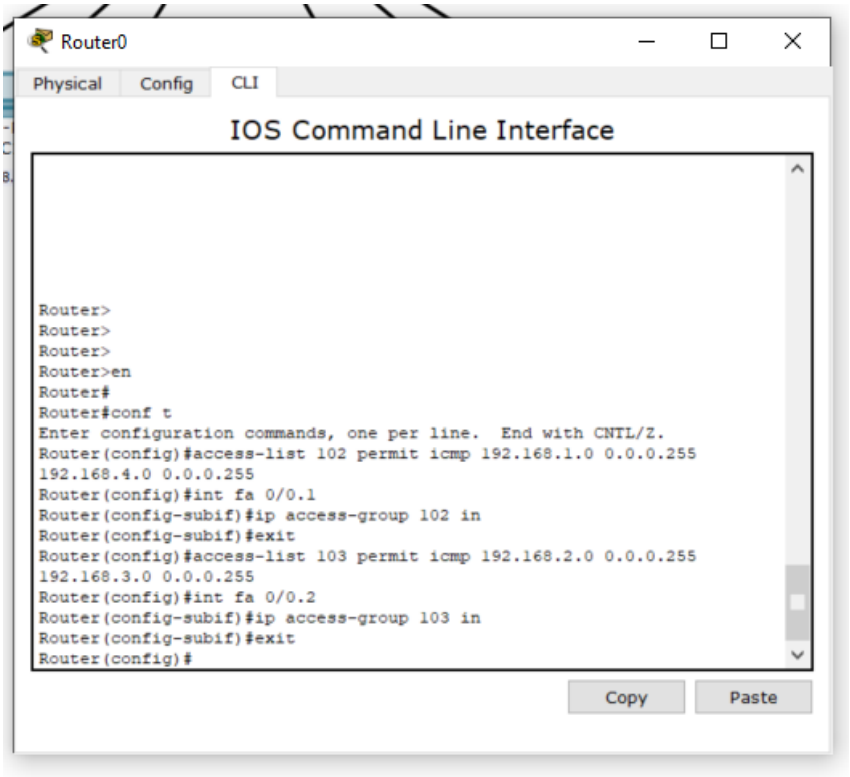

Figure 5

After configuring the router, we can see that PC 0 from Section A can ping the Proxy Network, but not the UNIFI Network (Figure 6). And PC 3 from Section B can ping the UNIFI Network but not the Proxy Network (Figure 7).

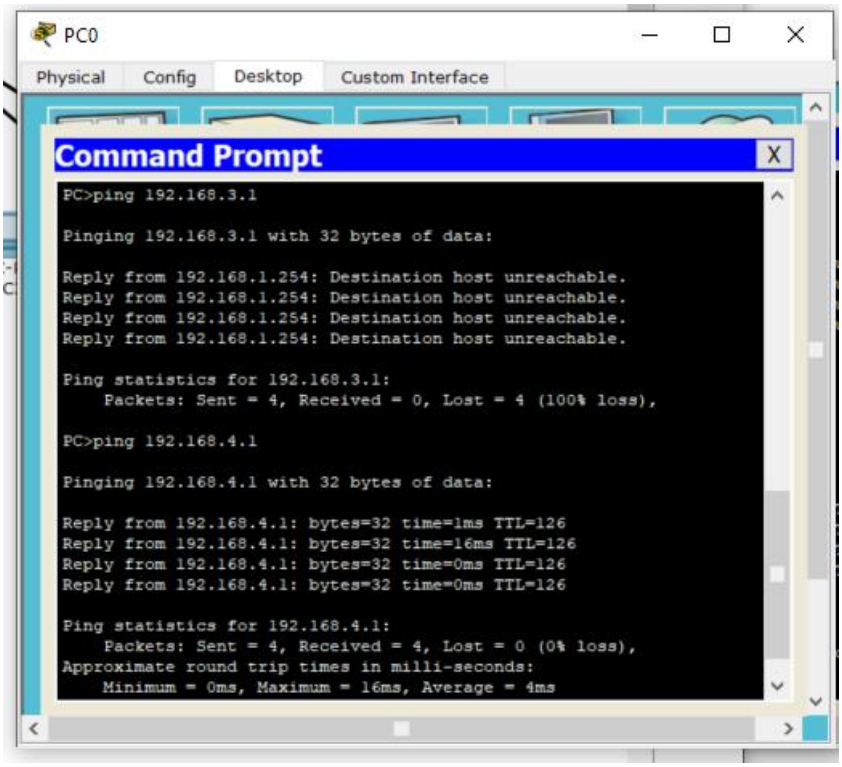

Figure 6

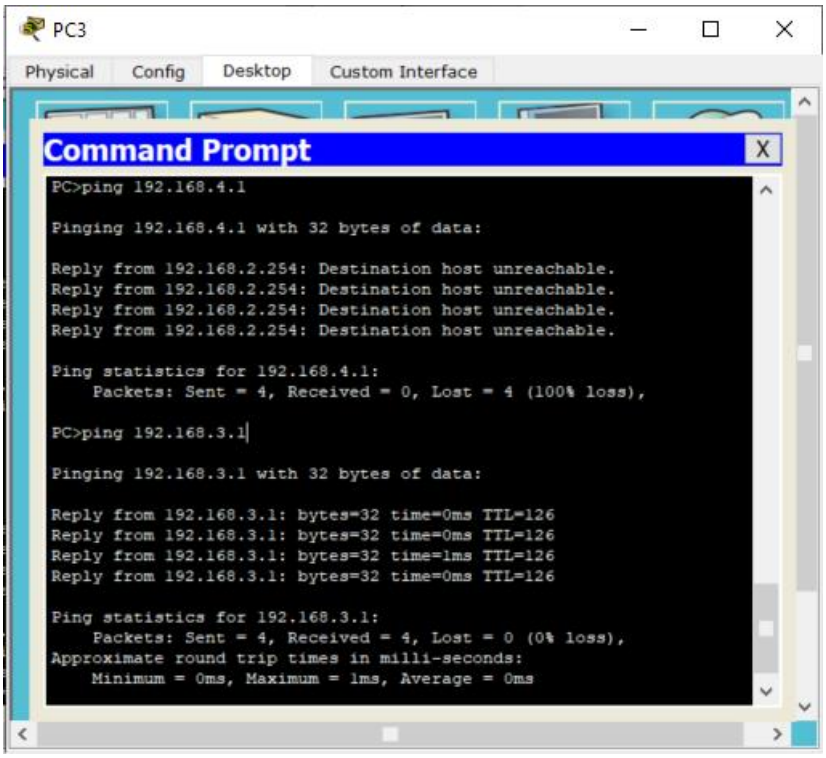

Figure 7

Requirements 3: Both Section A and Section B PCs require the Unifi Connection

To configure the second requirements, go to Router 1 and type the following commands, as shown in Figure 8:

Router0(config)#access-list 104 permit icmp 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Router0(config)#int fa0/0.1

Router0(config)#ip access-group 104 in

Router0(config)#access-list 105 permit icmp 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255

Router0(config)#int fa0/0.2

Router0(config)#ip access-group 105 in

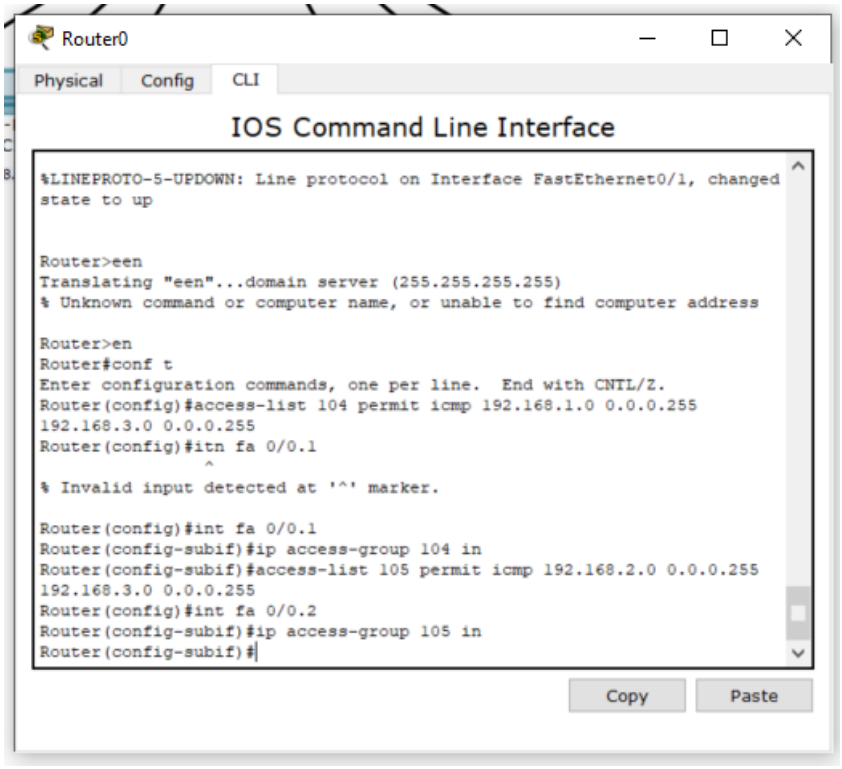

Figure 8

After configuring the router, we can see both PC 0 from Section A and PC 3 from Section B can ping the UNIFI Network but not the Proxy Network (Figure 9, 10).

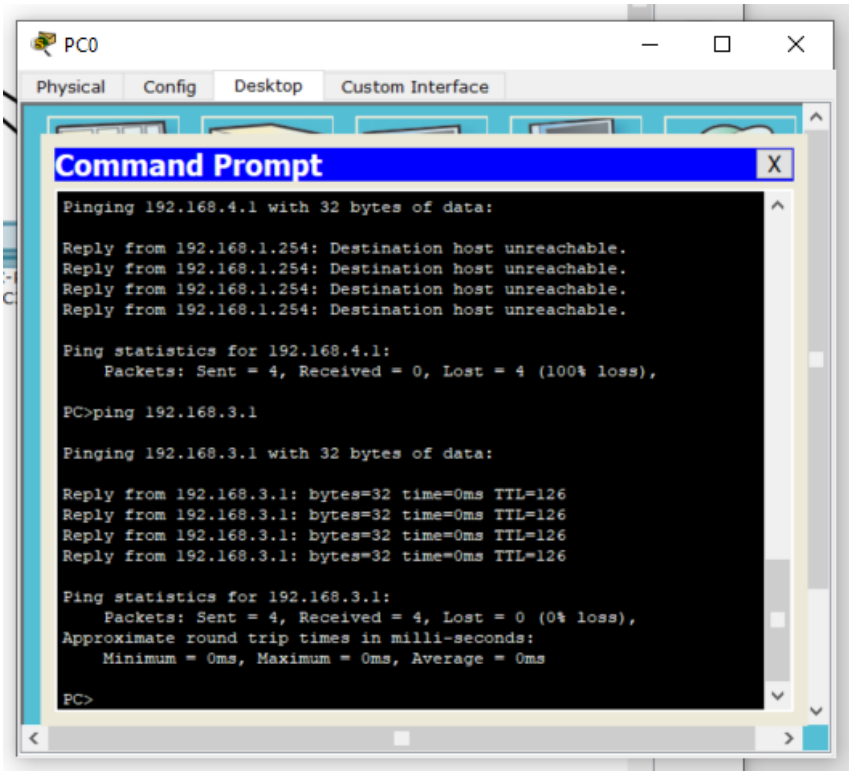

Figure 9

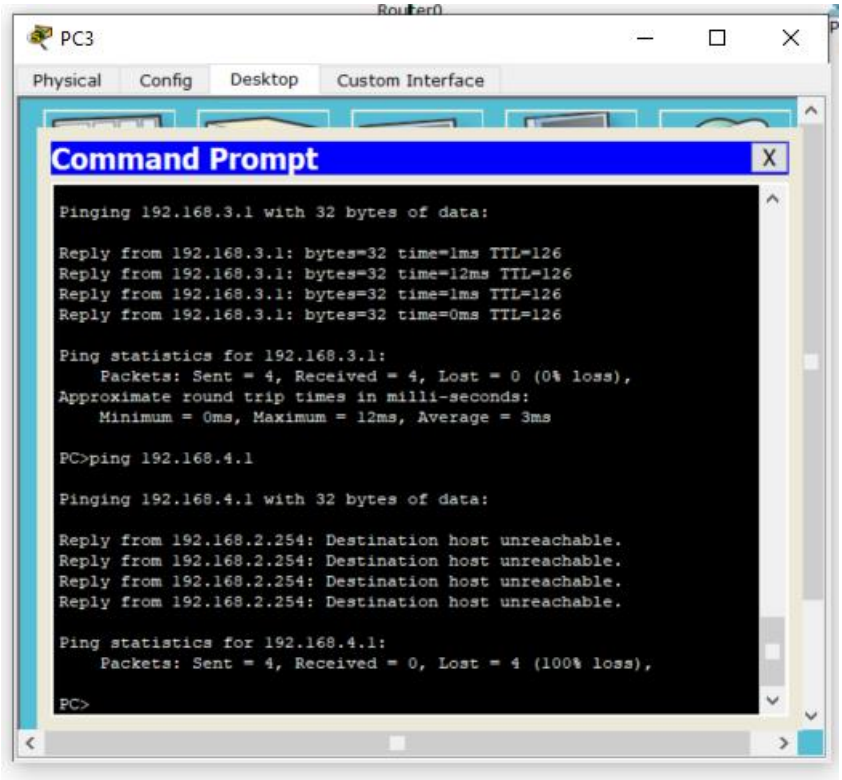

Figure 10

Requirements 4: Both Section A and Section B PCs require the Proxy Connection

To configure the second requirements, go to Router 1 and type the following commands, as shown in Figure 11:

Router0(config)#access-list 106 permit icmp 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255

Router0(config)#int fa0/0.1

Router0(config)#ip access-group 104 in

Router0(config)#access-list 107 permit icmp 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255

Router0(config)#int fa0/0.2

Router0(config)#ip access-group 107 in

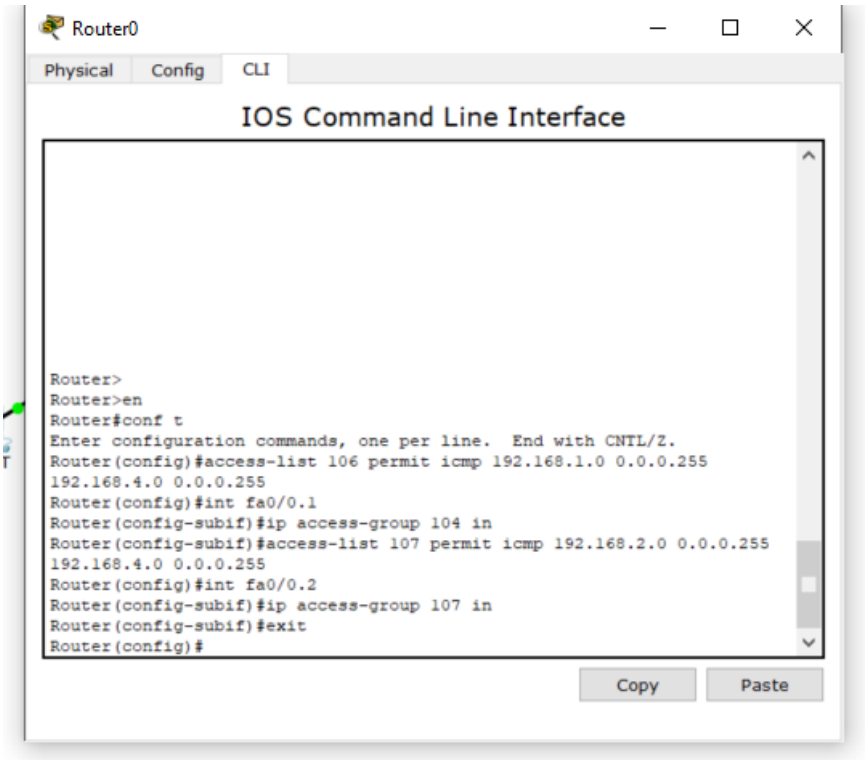

Figure 11

After configuring the router, we can see both PC 0 from Section A and PC 3 from Section B can ping the Proxy Network but not the UNIFI Network (Figure 12, 13).

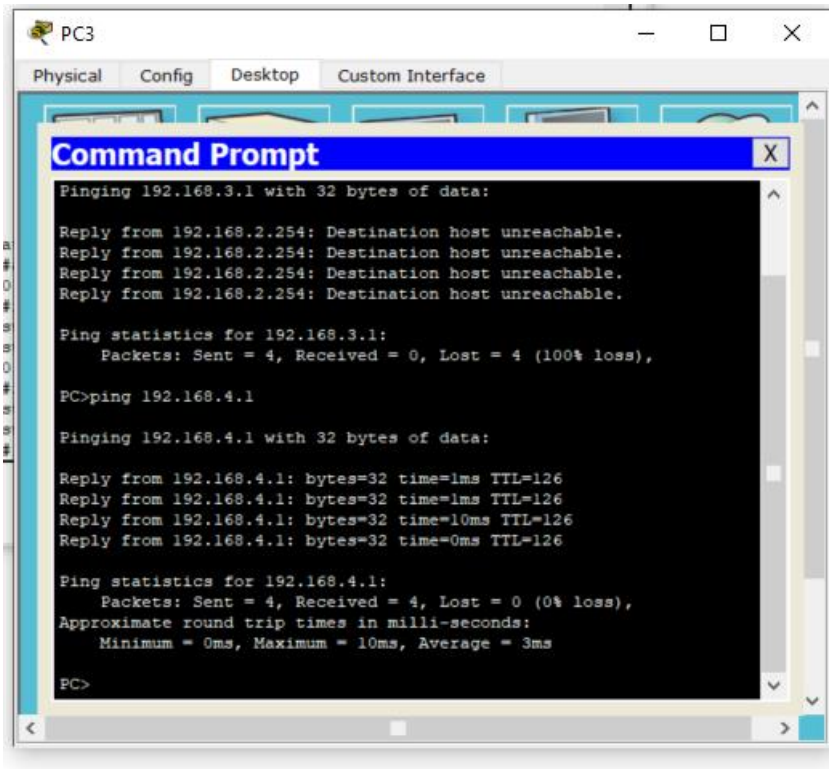

Figure 12

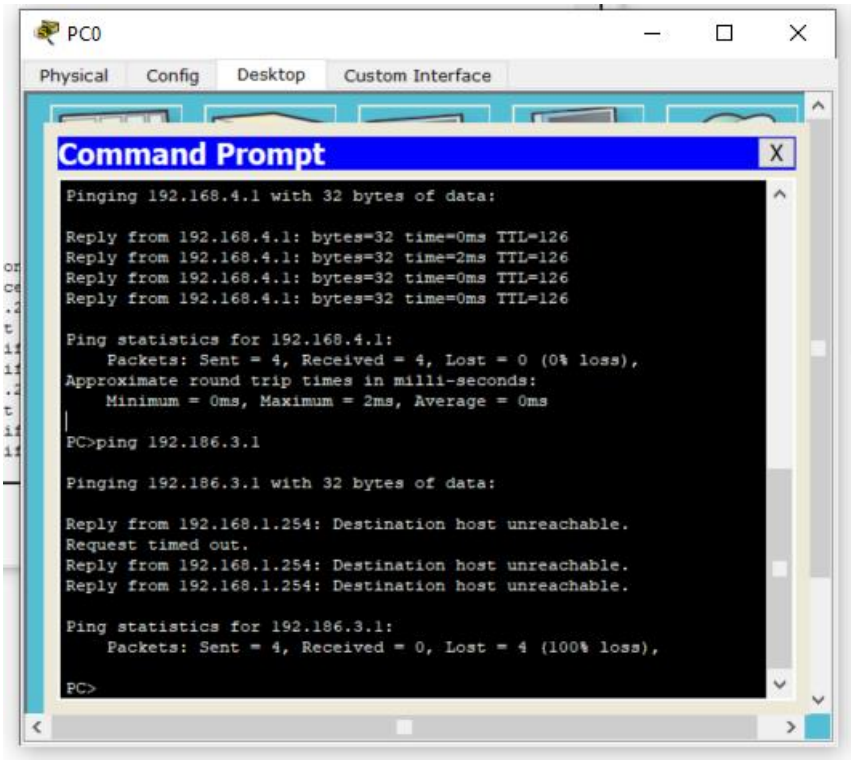

Figure 13

Question 1 (c)

The router that we choose to use in our proposed solution is Cisco Cisco2811vk9 2811 Router Voice Bundle. It is widely used commercially and the price is around RM2945.00. The reason why this router is so costly because it contains a few extra features like an increase in security and voice performance new embedded service options, and dramatically increased slot performance and density while maintaining support for most of the more than 90 existing modules that are available today. It also provides voice-over-IP (VoIP) and voice-over-Frame Relay (VoFR) transport to robust, centralized solutions. Below is a visual of the router:

Question 2 (a)

Topology (Figure 2.1)

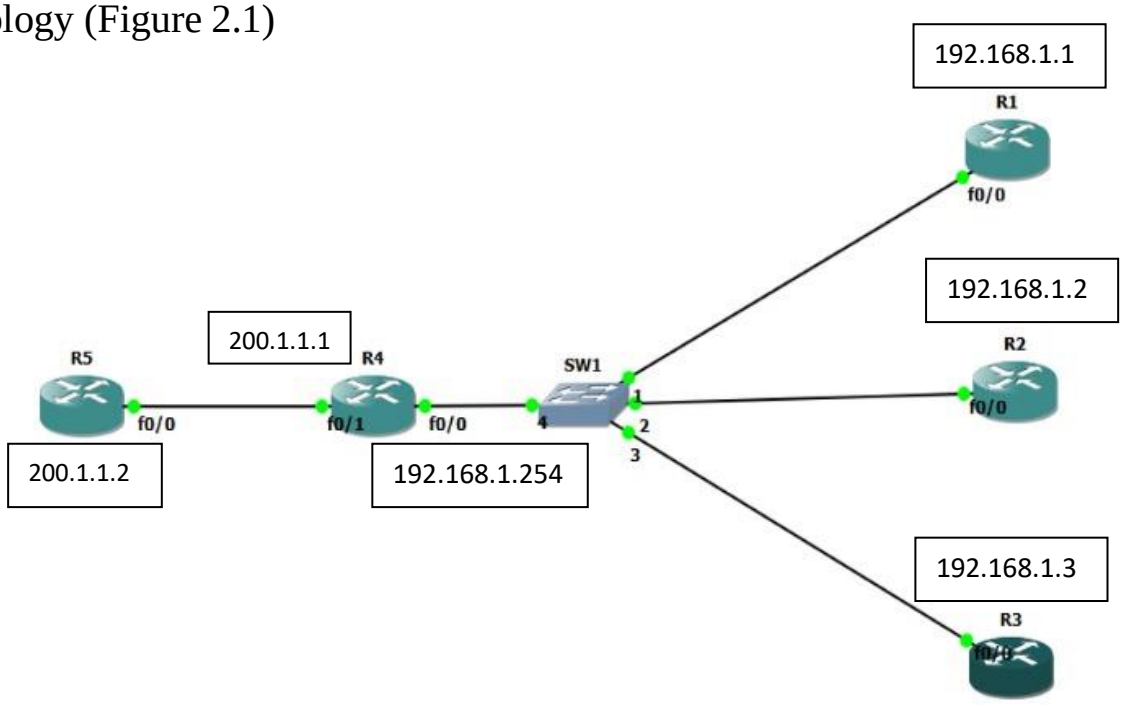

Figure 2.1

Question 2 (b)

Running Configurations of the Router

```
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.1.254
!
!
ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
```

```
!
!
interface FastEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.1.254
!
!
ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
```

```
!
!
interface FastEthernet0/0
 ip address 192.168.1.3 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.1.254
!
!
ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
```

Figure 1: Configuration of Router 1, Router 2, and Router 3

The figure above shows the ip address configuration of the three routers. Static route are also configured after the addresses has been set. Ip address of Router 1 is 192.168.1.1, Router 2 is 192.168.1.2, and Router 3 is 192.168.1.3 with the subnet mask of 255.255.255.0. The reason why default route is used because all the packet from these three Routers has to go through Router 4(192.168.1.254/24) in order to reach the outside network.

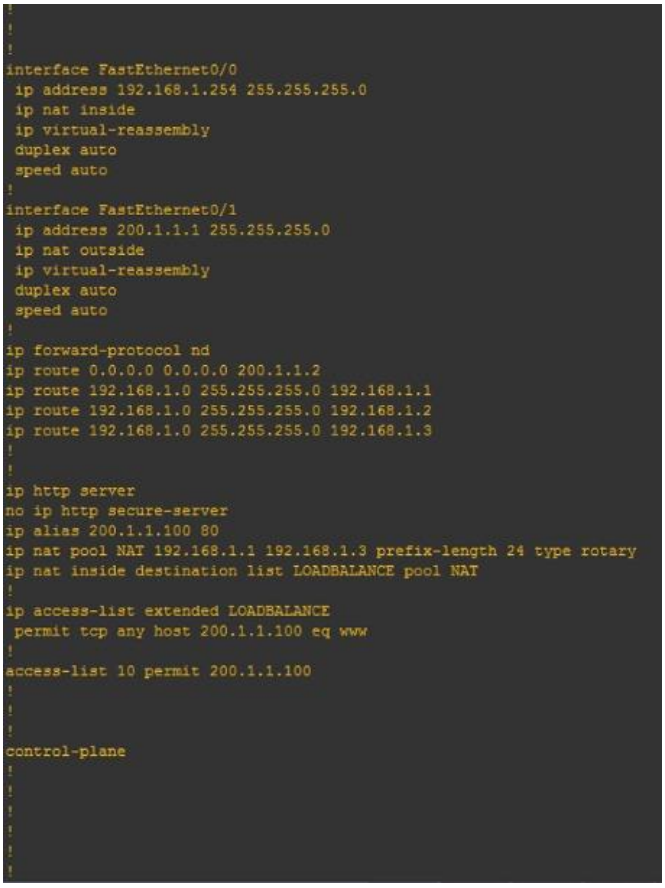

Figure 2: Router R4 configuration

Figure 2 shows the ip address configuration of Router 4. Static route are also configured after the addresses has been set. Ip address of Router 4 in interface fa0/0 is 192.168.1.254 with subnet mask of 255.255.255.0 and interface fa0/1 is 200.1.1.1 with subnet mask of 255.255.255.0. We configure interface fa0/0 as the inside network with the command "ip nat inside" and interface fa0/1 as the outside network with the command "ip nat outside". All the traffic that comes from Router 5 has to go through Router 4 in order to reach Router 1, Router 2 or Router 3 with the command "ip route 192.168.1.0 255.255.255.0 192.168.1.1" for Router 1, "ip route 192.168.1.0 255.255.255.0 192.168.1.1" for Router 2, and "ip route 192.168.1.0 255.255.255.0 192.168.1.3" for Router 3. The default route ("ip route 0.0.0.0 0.0.0.0 200.1.1.2") are used for packets that travel from the inside to the outside. First of all, we define a pool of address that contain the address of the router ("ip nat pool NAT 192.168.1.1 192.168.1.3 prefix-length 24 type rotary"). Next, we create an extended access-list named "LOADBALANCE" that permits the address of the router ("permit tcp any host 200.1.1.100 eq www "). Then, we enable a dynamic translation of inside destination addresses ("ip nat inside destination list LOADBALANCE pool NAT"). With this configuration the traffic from outside network will able to take turn to access the router of the inside network accordingly.

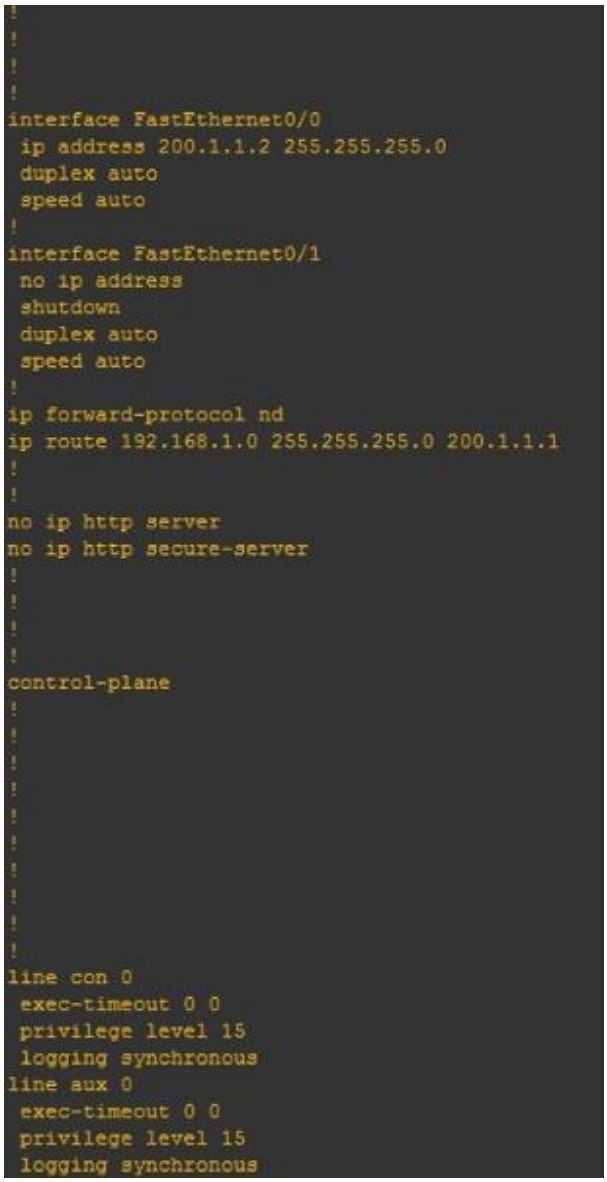

Figure 3: Router 5 configuration

The figure above shows the ip address configuration of Router 5. Static route are also configured after the addresses has been set. Ip address of of Router 5 is 200.1.1.2 with subnet mask 255.255.255.0. Traffic that go to subnet 192.168.1.0/24 has to go through Router 4(200.1.1.1) in order to reach.

Question 2 (c)

```
R4#show ip nat tr
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.1.1.100:80     192.168.1.1:80     200.1.1.2:37081    200.1.1.2:37081
R4#show ip nat tr
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.1.1.100:80     192.168.1.1:80     200.1.1.2:37081    200.1.1.2:37081
tcp 200.1.1.100:80     192.168.1.2:80     200.1.1.2:46618    200.1.1.2:46618
R4#show ip nat tr
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.1.1.100:80     192.168.1.1:80     200.1.1.2:37081    200.1.1.2:37081
tcp 200.1.1.100:80     192.168.1.2:80     200.1.1.2:46618    200.1.1.2:46618
tcp 200.1.1.100:80     192.168.1.3:80     200.1.1.2:59507    200.1.1.2:59507
R4#
```

Figure 4

The figure above show the NAT translation in Router 4.

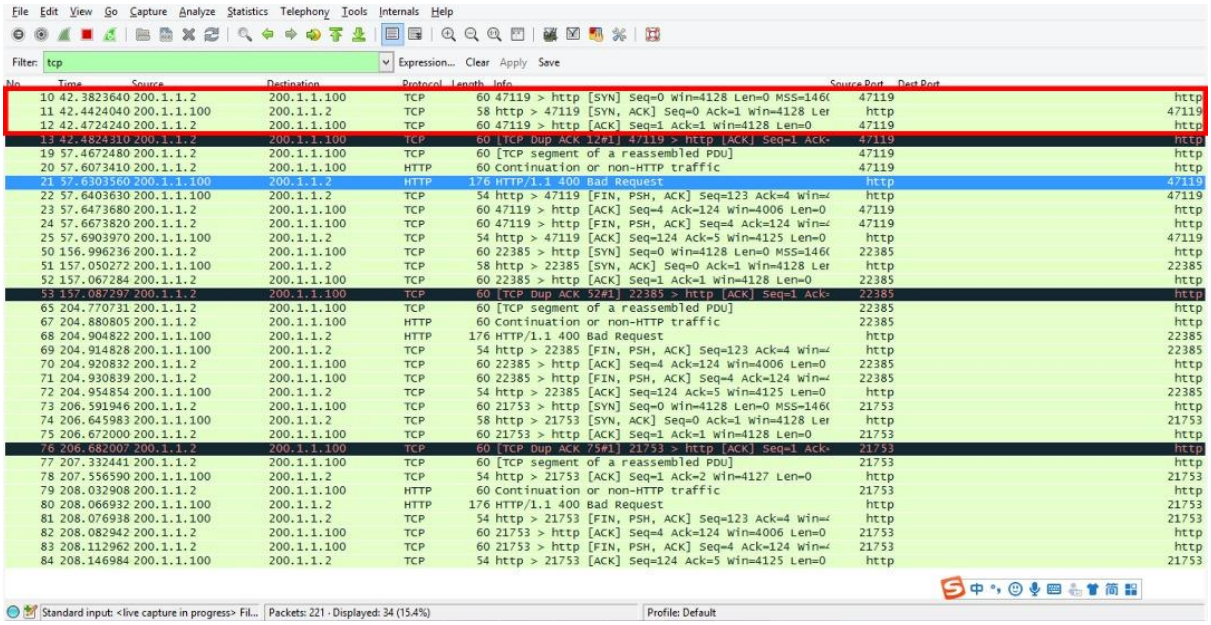

Figure 1 (capture at Router 5)

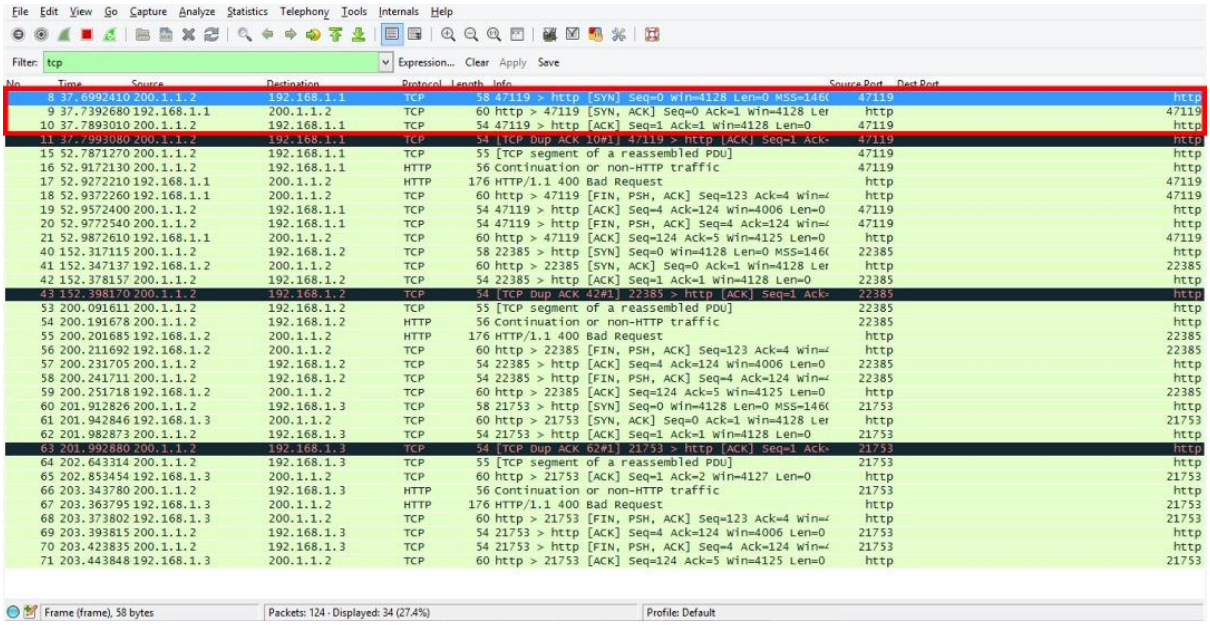

Figure 2 (capture at Router 4)

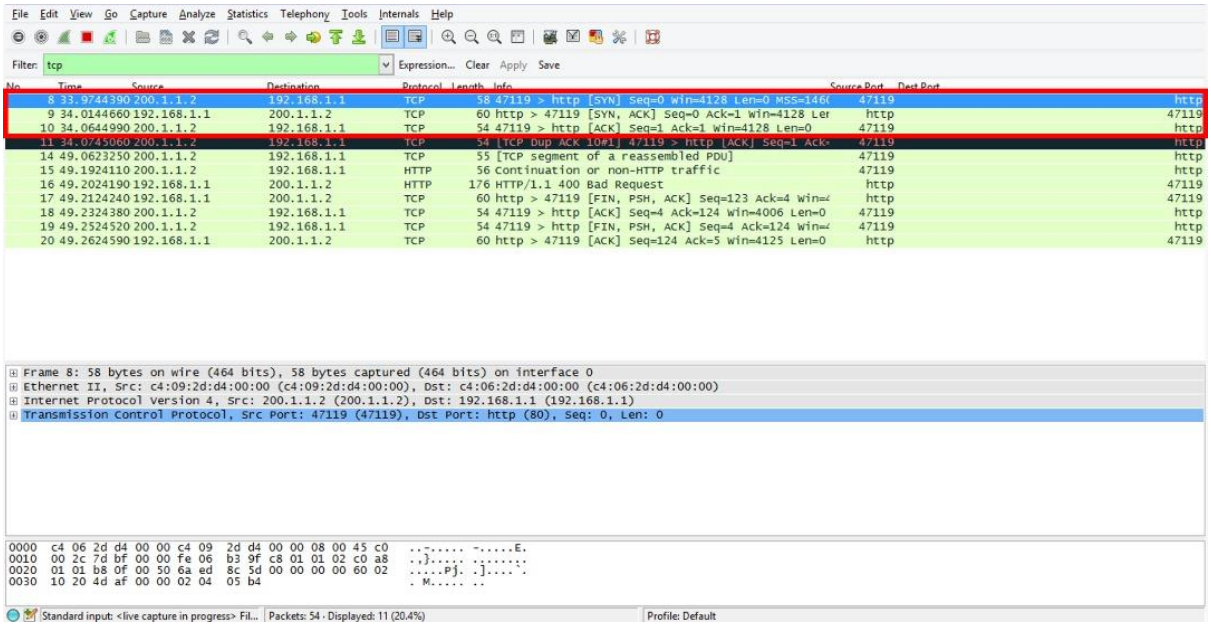

Figure 3 (capture at Router 1)

Figure 1, 2 and 3 shows that when telnet occur, Router 4 will redirect the packet to Router 1. Figure 1 show that when telnet 200.1.1.100, the packet will firstly travel to Router 4 and then it will be forwarded according to the NAT translation table based on Round Robin algorithm as shown in Figure 2 which in this case it will be forwarded to Router 1. Figure 3 shows that Router 1 receive the packet from the source address (200.1.1.2).

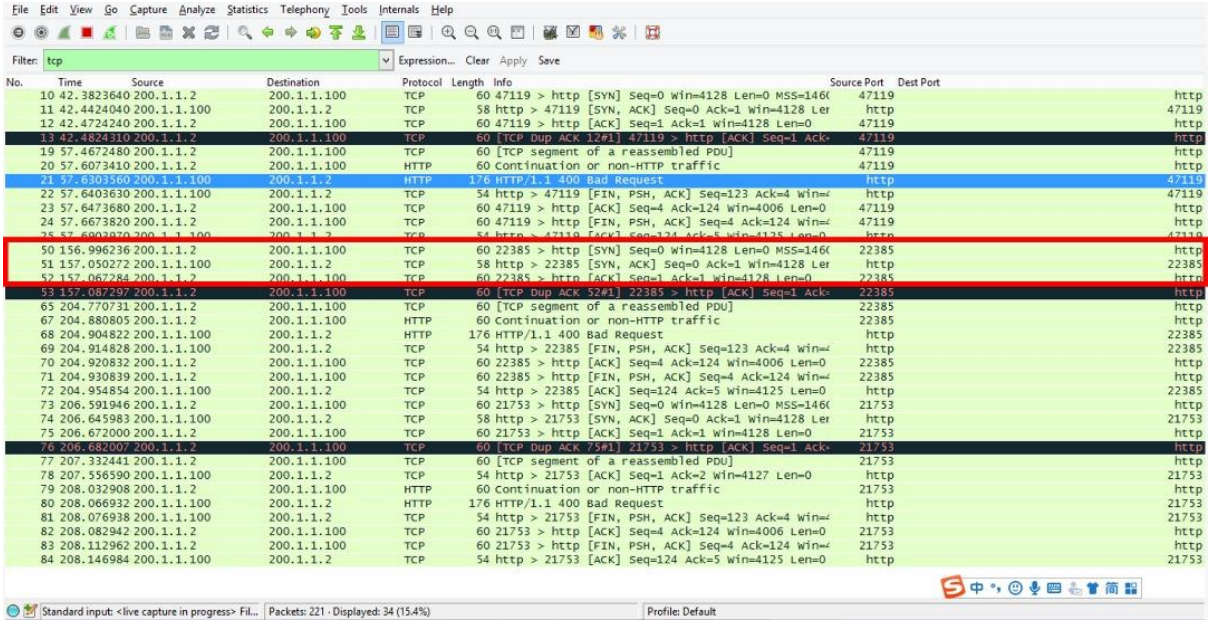

Figure 4 (capture at Router 5)

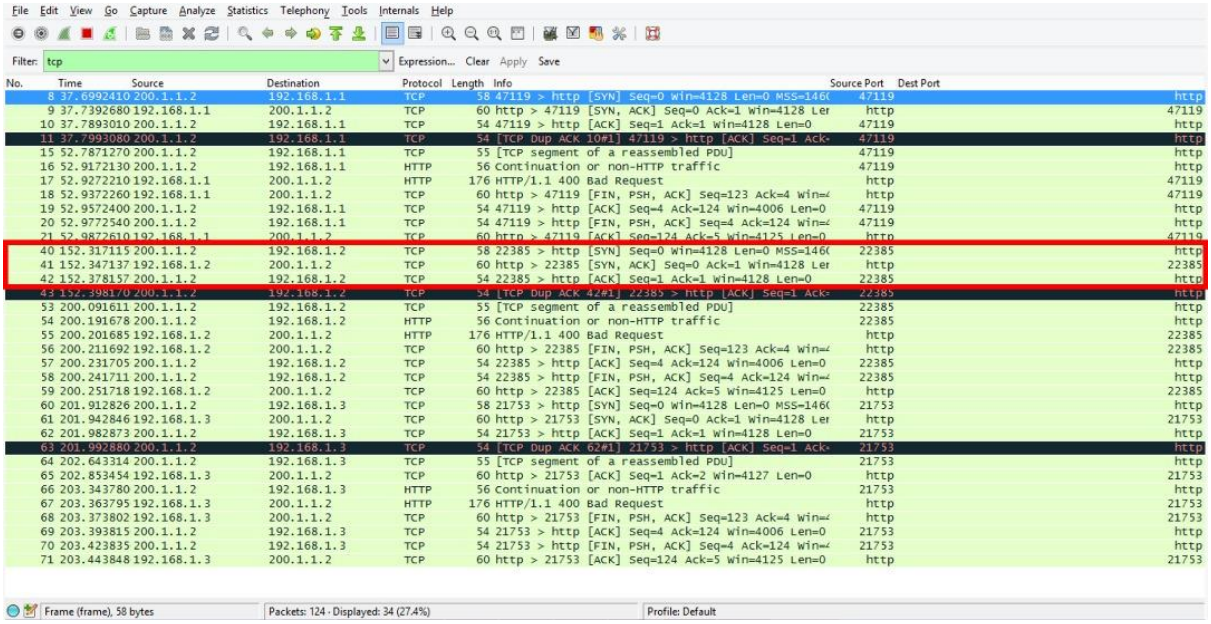

Figure 5 (capture at Router 4)

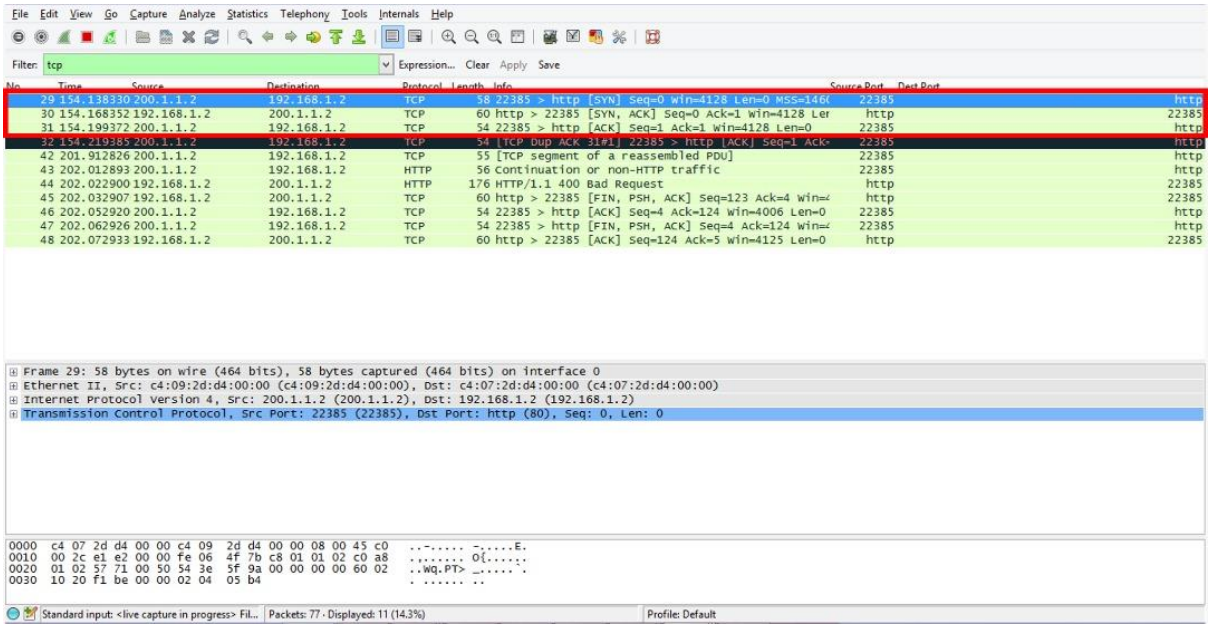

Figure 6 (capture at Router 2)

Figure 4, 5 and 6 shows that when telnet occur, Router 4 will redirect the packet to Router 2. Figure 4 show that when telnet 200.1.1.100, the packet will firstly travel to Router 4 and then it will be forwarded according to the NAT translation table based on Round Robin algorithm as shown in Figure 5 which in this case it will be forwarded to Router 2. Figure 6 shows that Router 2 receive the packet from the source address (200.1.1.2).

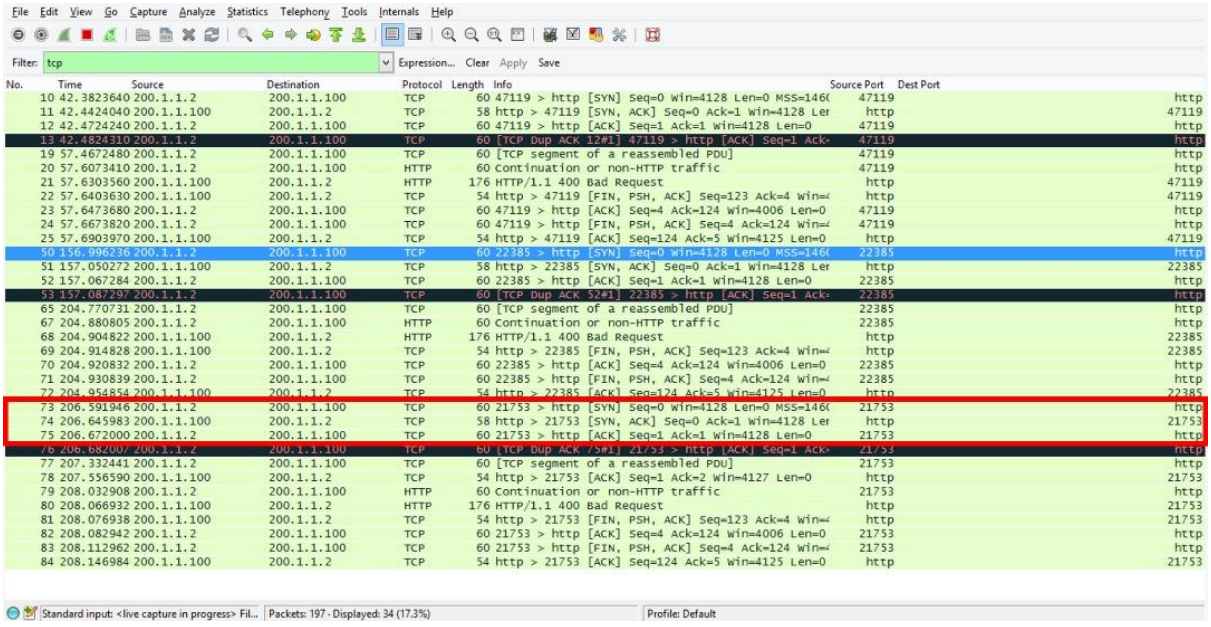

Figure 7 (capture at Router 5)

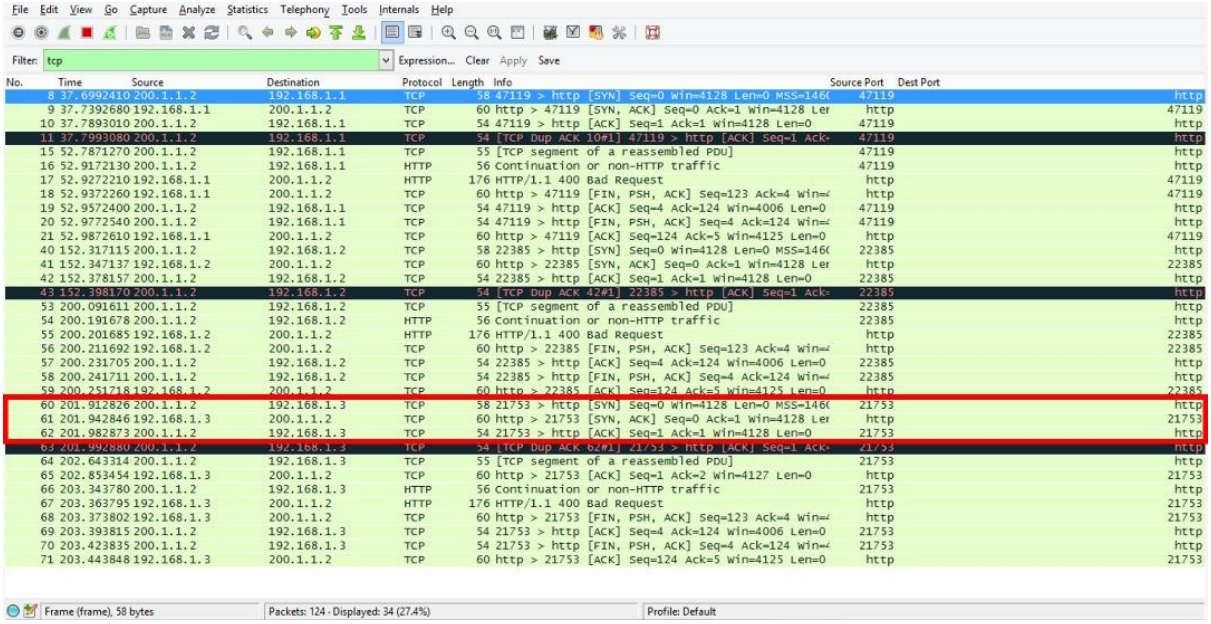

Figure 8 (capture at Router 4)

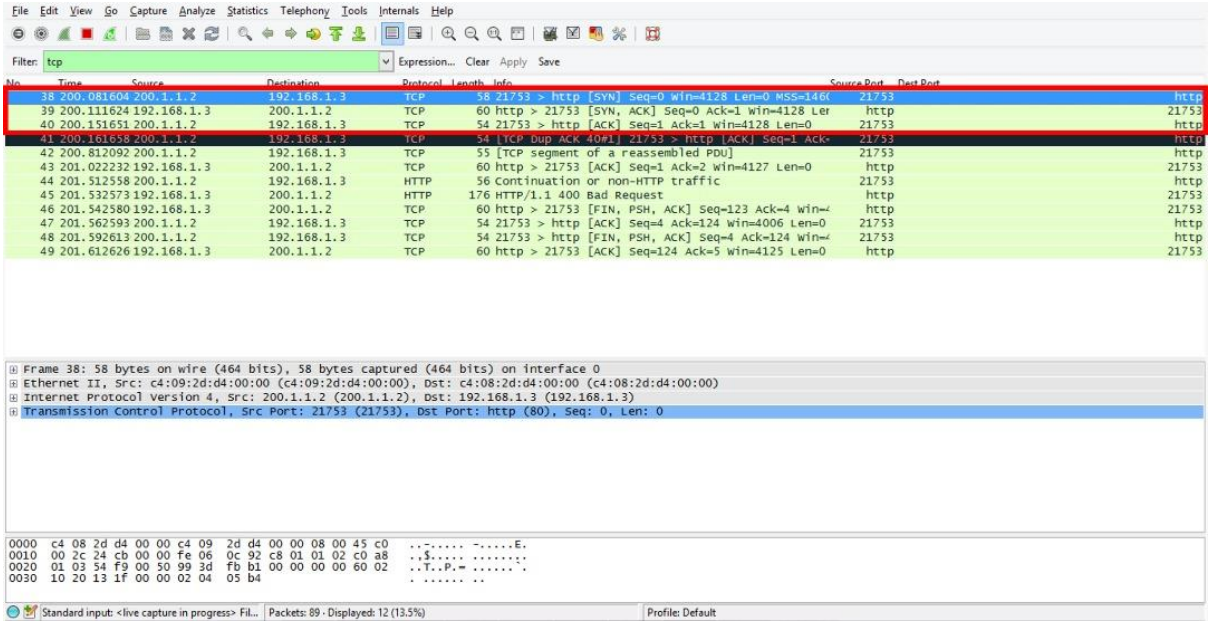

Figure 9 (capture at Router 3)

Figure 7, 8 and 9 shows that when telnet occur, Router 4 will redirect the packet to Router 3. Figure 7 show that when telnet 200.1.1.100, the packet will firstly travel to Router 4 and then it will be forwarded according to the NAT translation table based on Round Robin algorithm as shown in Figure 8 which in this case it will be forwarded to Router 3. Figure 9 shows that Router 3 receive the packet from the source address (200.1.1.2).