COMP416: Computer Networks

Project 3

Network Layer Analysis and Cisco Simulation Tool

Meryem Karakaş 69074

Part-1: Network Layer Analysis

1. What are table routes? Find the routing table using the 'ip' command. Examine the output and explain all the parameters of the routing tables.

Table routes are set of rules, they define how packets are routed within a network. They are used to determine where data packets will be directed while traveling over an IP network. Each routing table is stored in a router/switch and is used to determine the next hop for a packet.

```
mkarakas@DESKTOP-JLQSV8A:~$ ip route show
default via 172.23.208.1 dev eth0 proto kernel
172.23.208.0/20 dev eth0 proto kernel scope link src 172.23.209.127
mkarakas@DESKTOP-JLQSV8A:~$
```

Figure 1. The command to show the routing table

The output of 'ip route show' command shows the routing table for the network. The first line shows the default route for the network, which is the network address of the gateway router (172.23.208.1) and the device (eth0) through which the router is connected to the network.

The second line shows the network address (172.23.208.0/20) of the local network, the device (eth0) to which the network is connected, the protocol (kernel) used to communicate between the local network and the gateway router, and the source address (172.23.209.127) of the local network.

2. Explain the purpose and options used with the command: 'ip -br -c addr show'. Explain the results of this command elaborating on each field separately.

```
mkarakas@DESKTOP-JLQSV8A:~$ ip -br -c addr show
lo               UNKNOWN        127.0.0.1/8 ::1/128
bond0            DOWN
dummy0           DOWN
tunl0@NONE       DOWN
sit0@NONE        DOWN
eth0             UP             172.23.209.127/20 fe80::215:5dff:fe4b:c3b/64
mkarakas@DESKTOP-JLQSV8A:~$
```

Figure 2. Output of “ip -br -c addr show” command

The purpose of the command is to view the IP address configuration of a system. The '-br' option allows the output to be rendered in an easy-to-read format. The '-c' option is used to show the output in tabular form.

lo is the loopback interface. It is a virtual interface used for testing purposes and is always up. Its IP address is 127.0.0.1/8 and ::1/128.

bond0, dummy0, tunl0@NONE, and sit0@NONE are all down, meaning they have no active network connections.

eth0 is an ethernet interface that is up, meaning it has an active network connection. Its IP address is 172.23.209.127/20 and its IPv6 address is fe80::215:5dff:fe4b:c3b/64.

ICMP Analysis

3. Find the minimum TTL less than which the traceroute messages do not reach your particular URL destination.

```
mkarakas@DESKTOP-JLQSV8A:~$ traceroute -I ICMP www.yale.edu
traceroute to pantheon-systems.map.fastly.net (151.101.66.133), 64 hops max
  1   172.23.208.1  0.721ms  0.760ms  0.650ms
  2   172.16.104.2  4.346ms  1.678ms  1.605ms
  3   10.20.30.3  3.578ms  3.688ms  2.675ms
  4   212.175.32.141  3.505ms  3.922ms  2.625ms
  5   212.174.167.209  4.726ms  3.060ms  5.193ms
  6   212.156.121.72  3.791ms  3.212ms  2.909ms
  7   *  81.212.201.195  5.107ms  3.542ms
  8   212.156.120.178  4.375ms  3.977ms  3.884ms
  9   212.156.101.196  46.378ms  45.972ms  45.287ms
 10   213.198.83.221  52.171ms  47.738ms  56.963ms
 11   168.143.105.215  47.595ms  48.821ms  46.765ms
 12   151.101.66.133  46.979ms  47.576ms  47.410ms
mkarakas@DESKTOP-JLQSV8A:~$
```

Figure 3. The traceroute (with ICMP packets) for address www.yale.edu

```
mkarakas@DESKTOP-JLQSV8A:~$ ping -t 11 www.yale.edu
PING pantheon-systems.map.fastly.net (151.101.130.133) 56(84) bytes of data.
From ae-0.fastly.frnkge07.de.bb.gin.ntt.net (168.143.105.215) icmp_seq=1 Time to live exceeded
From ae-0.fastly.frnkge07.de.bb.gin.ntt.net (168.143.105.215) icmp_seq=2 Time to live exceeded
From ae-0.fastly.frnkge07.de.bb.gin.ntt.net (168.143.105.215) icmp_seq=3 Time to live exceeded
^C
--- pantheon-systems.map.fastly.net ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2003ms

mkarakas@DESKTOP-JLQSV8A:~$ ping -t 12 www.yale.edu
PING pantheon-systems.map.fastly.net (151.101.130.133) 56(84) bytes of data.
64 bytes from 151.101.130.133 (151.101.130.133): icmp_seq=1 ttl=50 time=47.2 ms
64 bytes from 151.101.130.133 (151.101.130.133): icmp_seq=2 ttl=50 time=45.8 ms
64 bytes from 151.101.130.133 (151.101.130.133): icmp_seq=3 ttl=50 time=45.7 ms
64 bytes from 151.101.130.133 (151.101.130.133): icmp_seq=4 ttl=50 time=45.6 ms
^C64 bytes from 151.101.130.133: icmp_seq=5 ttl=50 time=46.6 ms

--- pantheon-systems.map.fastly.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4220ms
rtt min/avg/max/mdev = 45.629/46.215/47.243/0.625 ms
```

Figure 4. Ping commands to find out minimum TTL value

I tried some TTL values by using '-t' flag and I found that the minimum TTL to reach the destination URL “www.yale.edu” is 12.

4. What is the default number of probes used by the traceroute? Run multiple traceroutes, increasing the number of probes progressively. Explain your observation regarding the resolution of the route to your destination ip address.

```
mkarakas@DESKTOP-JLQSV8A:~$ traceroute -I ICMP -q 4 www.yale.edu
traceroute to pantheon-systems.map.fastly.net (151.101.66.133), 64 hops max
  1   172.23.208.1  0.335ms  0.444ms  0.400ms  0.279ms
  2   172.16.104.2  6.565ms  2.030ms  1.732ms  1.623ms
  3   10.20.30.3  3.302ms  2.736ms  2.698ms  2.967ms
  4   212.175.32.141  3.998ms  2.652ms  4.462ms  2.752ms
  5   212.174.167.209  4.248ms  2.903ms  3.036ms  3.154ms
  6   212.156.121.72  4.130ms  4.426ms  3.337ms  3.438ms
  7   *  *  *  *
  8   *  212.156.120.178  5.899ms  7.857ms  4.080ms
  9   212.156.101.196  46.223ms  49.720ms  45.205ms  45.254ms
 10   213.198.83.221  49.397ms  47.285ms  46.830ms  46.242ms
 11   168.143.105.215  47.834ms  46.872ms  46.250ms  46.492ms
 12   151.101.66.133  47.223ms  47.280ms  51.065ms  47.569ms
mkarakas@DESKTOP-JLQSV8A:~$ traceroute -I ICMP -q 5 www.yale.edu
traceroute to pantheon-systems.map.fastly.net (151.101.130.133), 64 hops max
  1   172.23.208.1  0.554ms  0.654ms  1.184ms  2.570ms  0.822ms
  2   172.16.104.2  4.219ms  2.005ms  1.775ms  1.801ms  4.061ms
  3   10.20.30.3  3.984ms  2.644ms  2.529ms  5.451ms  2.533ms
  4   212.175.32.141  2.743ms  2.856ms  2.718ms  2.630ms  3.232ms
  5   212.174.167.209  4.744ms  4.105ms  9.030ms  3.549ms  6.193ms
  6   212.156.121.72  3.546ms  3.153ms  2.902ms  4.134ms  3.249ms
  7   *  *  *  *  *
  8   212.156.120.178  4.962ms  3.550ms  3.973ms  4.199ms  3.594ms
  9   212.156.101.196  45.356ms  45.354ms  45.046ms  45.178ms  44.887ms
 10   213.198.83.221  54.909ms  52.855ms  47.045ms  46.648ms  52.653ms
 11   168.143.105.215  50.533ms  51.764ms  50.273ms  50.501ms  50.199ms
 12   151.101.130.133  46.031ms  48.592ms  45.454ms  45.743ms  45.587ms
mkarakas@DESKTOP-JLQSV8A:~$
```

Figure 5. Running traceroute with different number of probes

Every route in the path probed 3 times with traceroute command by default. Increasing the number of probes while running traceroute will improve the resolution of the route by providing more data points to work with. A higher number of probes will give a more detailed view of the route, allowing for better analysis of the connection and its performance. This can help identify any potential bottlenecks or points of failure in the network.

5. What is a Routing Blackhole? Provide a scenario where Routing Blackholes may be used beneficially.

Routing blackhole is a network security method based on discarding all packets that meet certain criteria. This technique is used to prevent the spread of malicious traffic, such as malware or spam. Routing blackholes can help secure the network. When a computer on the network is infected with malware, a routing blackhole can be used to prevent the malware from accessing other computers on the network.

Part-2: Simulations with Cisco Packet Tracer

6. *Attach a screenshot of the designed network with a label beside each port indicating its IP address.*

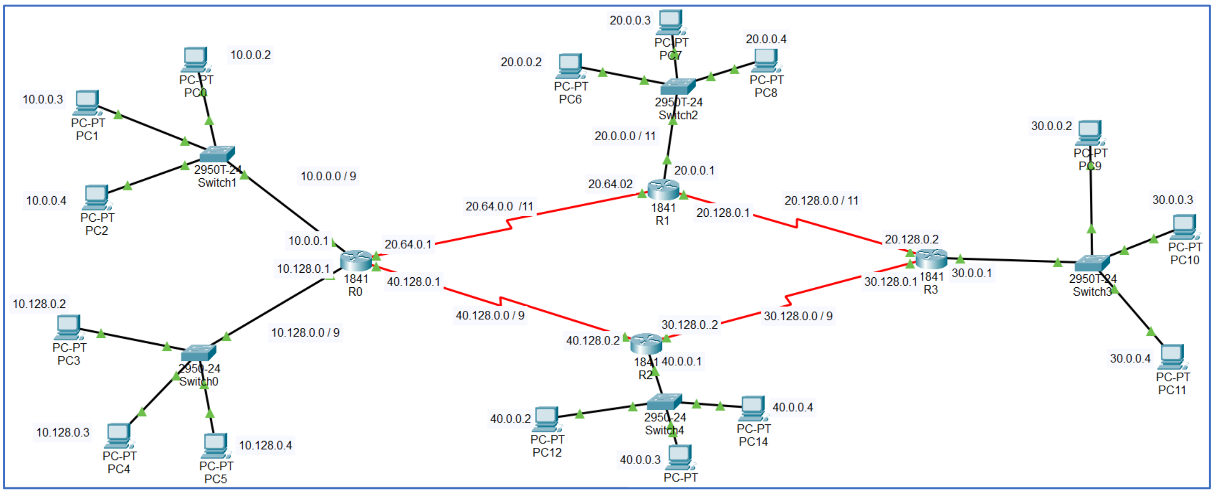

Figure 6. My network design with Cisco Packet Tracer

7. In step E of the network simulation process, you probably configured the routers using the Graphical User Interface. However, in real life, command lines are used. Make a table having

two columns. The first column is the process, and the second one is the command. You can notice the commands written automatically when selecting an option in the GUI.

I will give configuration commands for one PC and one Router, configuration for others are similar. Although the addresses and masks for other routers and PCs vary, I will not write them all, as the procedure is approximately the same.

Router 0:

Process	Command
IP address configuration for FastEthernet0/0 interface	ip address 10.0.0.1 255.128.0.0
Enabling the port	no shut
IP address configuration for FastEthernet0/1 interface	ip address 10.128.0.1 255.128.0.0
IP address configuration for Serial0/0/1 interface	ip address 20.64.0.1 255.224.0.0
IP address configuration for Serial0/1/1 interface	ip address 40.128.0.1 255.128.0.0
Static routing to reach network 20.0.0.0	ip route 20.0.0.0 255.224.0.0 20.64.0.2
Static routing to reach network 30.0.0.0	ip route 30.0.0.0 255.128.0.0 40.128.0.2
Static routing to reach network 40.0.0.0	ip route 30.0.0.0 255.128.0.0 40.128.0.2

PC 0:

Process	Command
IP address configuration for this PC	ip address 10.0.0.2 255.128.0.0
Default gateway configuration	ip default-gateway 10.0.0.1

8. What are the different types of cables that have been used? Why is it a must to connect two distant routers with a serial cable?

The most common types of cables used in networking are copper, fiber optic, twisted pair, coaxial, and serial cables. I used Copper Straight-Through cable when making the switch-PC and switch-router connections.

Connecting two remote routers with a serial cable is a must because a serial cable is the most reliable and secure way to connect two remote routers. It allows a direct point-to-point connection, providing a secure, reliable and high-speed connection between two routers.

9. Explain, with the help of screenshots, the process of adding the serial ports to one of the routers.

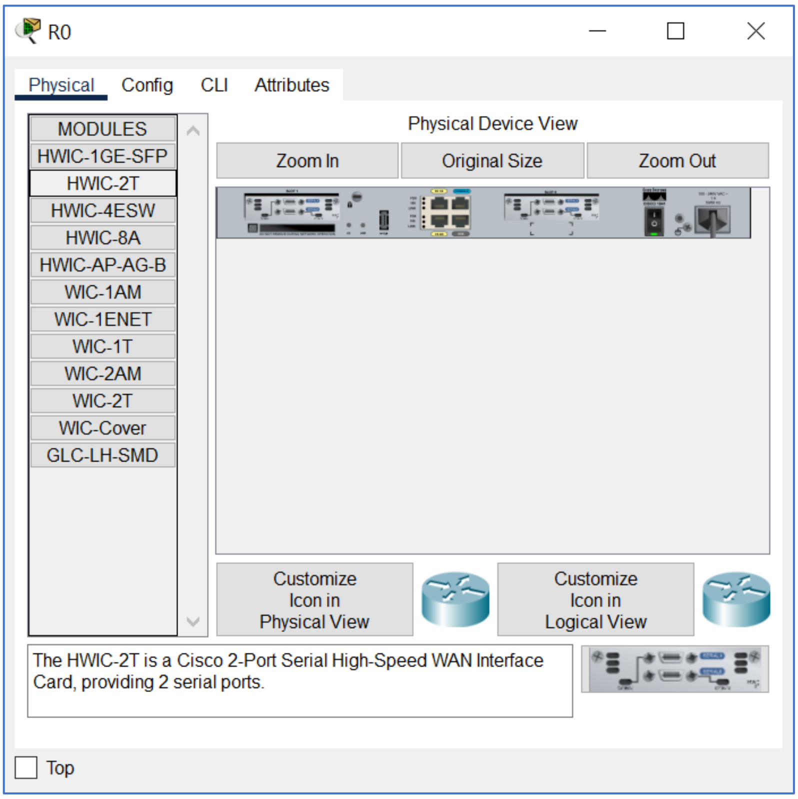

Figure 7. Physical view of Router 0 after inserting HWIC-2T cards

First of all, I added 2 HWIC-2T Interface Cards, which provides 2 serial ports, to each router. Then I opened the command line interface (CLI). I used the “configure terminal” command to enter global configuration mode. I entered the serial interface name to access the serial port configuration. I entered the “ip address” command to assign the IP address for the serial port. After, enter the “no shutdown” command to enable the interface. Lastly, I saved the configuration by entering the “copy running-config startup-config” command.

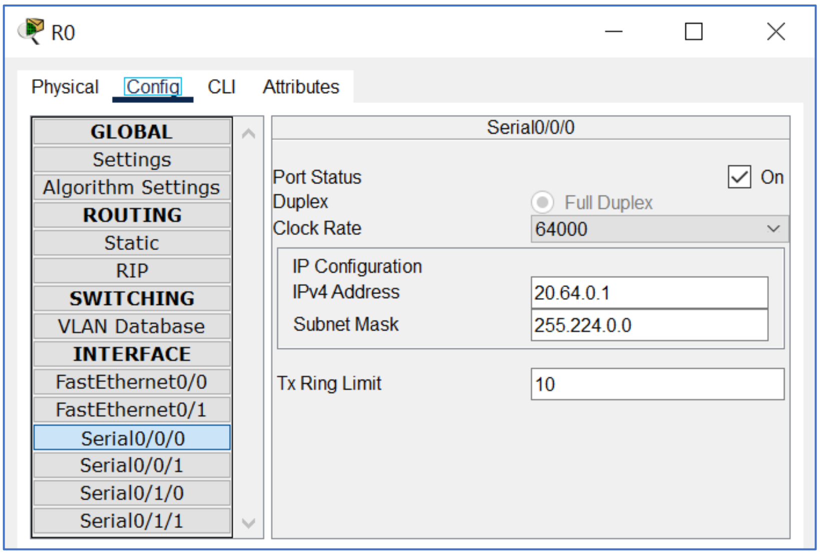

Figure 8. One of the serial port configuration of Router 0

10. For each network, how many subnetworks should be used? Include the calculations in your report.

The number of required subnets is determined by the size of the network, the number of devices that need to be connected, and the security requirements of the network. You can find below how I divided the addresses 10.0.0.0, 20.0.0.0, 30.0.0.0, 40.0.0.0 given to us into subnets according to my network topology and my calculation details:

Since the 10.0.0.0/8 address is a private address and can only be a local address, I allocated this address to 2 subnets for 2 different laboratories in Location 1. I placed 3 PCs in each of the 2 subnets, so I divided the address into 2 subnets so that they can have an equal number of devices. As a result, the address of one of the subnetworks became 10.0.0.0/9, while the other became 10.128.0.0/9.

Since the number of devices connected to the networks is not very large, I did not perform a detailed address allocation process. I simply split the networks into subnets. I divided the 20.0.0.0/8 address into 3 subnetworks. One of the networks represents the network between router 0 and router 1, the other represents the network between router 1 and router 3, and the third represents the network where laboratory 3 is located. The corresponding network addresses are 20.64.0.0/11, 20.128.0.0/11 and 20.0.0.0/11.

I split 30.0.0.0/8 into 2 subnets. One of the networks represents the network where laboratory 4 is located, and the other represents the network between router 2 and router 3. The corresponding network addresses are 30.0.0.0/9 and 30.128.0.0/9.

Finally, I also split the address of 40.0.0.0/8 into 2 subnets. One of the networks represents the network where lab 5 is located, and the other represents the network between router 0 and router 2. The corresponding network addresses are 40.0.0.0/9 and 40.128.0.0/9.

11. For each laboratory, what is the network ID, the maximum number of devices we can connect, the gateway IP, and the broadcast IP addresses?

Note: For networks with a Network ID of X.X.X/9, we have 23 (32-9) bits that we can use for the host. For networks with a Network ID of X.X.X/11, we have 21 (32-11) bits that we can use for the host. I took this into account when finding the maximum number of hosts in the calculations. I also subtracted 2 from each result because one of the addresses is the subnet ID (the first address) and the other is the broadcast address (the last address).

Laboratory 1:

Network ID:	10.0.0.0/9
The max. # devices we can connect:	$2^{23} - 2$
The gateway IP:	10.0.0.1
The broadcast IP:	10.127.255.255

Laboratory 2:

Network ID:	10.128.0.0/9
The max. # devices we can connect:	$2^{23} - 2$
The gateway IP:	10.128.0.1
The broadcast IP:	10.255.255.255

Laboratory 3:

Network ID:	20.0.0.0/11
The max. # devices we can connect:	$2^{21} - 2$
The gateway IP:	20.0.0.1
The broadcast IP:	20.31.255.255

Laboratory 4:

Network ID:	30.0.0.0/9
The max. # devices we can connect:	$2^{23} - 2$
The gateway IP:	30.0.0.1
The broadcast IP:	30.127.255.255

Laboratory 5:

Network ID:	40.0.0.0/9
The max. # devices we can connect:	2^{23} - 2
The gateway IP:	40.0.0.1
The broadcast IP:	40.127.255.255

12. You can display the routing table using the command line at each router. Search for the command that displays the routing table and attach a screenshot for the routing table at each router.

The command is: *"sh ip route"*

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/9 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, FastEthernet0/0
C       10.128.0.0 is directly connected, FastEthernet0/1
     20.0.0.0/11 is subnetted, 2 subnets
S       20.0.0.0 [1/0] via 20.64.0.2
C       20.64.0.0 is directly connected, Serial0/0/0
     30.0.0.0/9 is subnetted, 1 subnets
S       30.0.0.0 [1/0] via 40.128.0.2
     40.0.0.0/9 is subnetted, 2 subnets
S       40.0.0.0 [1/0] via 40.128.0.2
C       40.128.0.0 is directly connected, Serial0/1/1
```

Figure 9. The routing table of Router 0

```
     10.0.0.0/9 is subnetted, 2 subnets
S       10.0.0.0 [1/0] via 20.64.0.1
S       10.128.0.0 [1/0] via 20.64.0.1
     20.0.0.0/11 is subnetted, 3 subnets
C       20.0.0.0 is directly connected, FastEthernet0/0
C       20.64.0.0 is directly connected, Serial0/0/0
C       20.128.0.0 is directly connected, Serial0/1/0
     30.0.0.0/9 is subnetted, 1 subnets
S       30.0.0.0 [1/0] via 20.128.0.2
     40.0.0.0/9 is subnetted, 1 subnets
S       40.0.0.0 [1/0] via 20.128.0.2
```

Figure 10. The routing table of Router 1

```
     10.0.0.0/9 is subnetted, 2 subnets
S       10.0.0.0 [1/0] via 40.128.0.1
S       10.128.0.0 [1/0] via 40.128.0.1
     20.0.0.0/11 is subnetted, 1 subnets
S       20.0.0.0 [1/0] via 30.128.0.1
     30.0.0.0/9 is subnetted, 2 subnets
S       30.0.0.0 [1/0] via 30.128.0.1
C       30.128.0.0 is directly connected, Serial0/0/1
     40.0.0.0/9 is subnetted, 2 subnets
C       40.0.0.0 is directly connected, FastEthernet0/0
C       40.128.0.0 is directly connected, Serial0/1/1
```

Figure 11. The routing table of Router 2

```
     10.0.0.0/9 is subnetted, 2 subnets
S       10.0.0.0 [1/0] via 20.128.0.1
S       10.128.0.0 [1/0] via 20.128.0.1
     20.0.0.0/11 is subnetted, 2 subnets
S       20.0.0.0 [1/0] via 20.128.0.1
C       20.128.0.0 is directly connected, Serial0/1/0
     30.0.0.0/9 is subnetted, 2 subnets
C       30.0.0.0 is directly connected, FastEthernet0/0
C       30.128.0.0 is directly connected, Serial0/0/1
     40.0.0.0/9 is subnetted, 1 subnets
S       40.0.0.0 [1/0] via 30.128.0.2
```

Figure 12. The routing table of Router 3

13. Your network should be working, it means any two devices can communicate. Use the ping command to test connectivity between a pc from each network with a pc from other laboratories.

I checked the connections using the ping command for each network. All devices can connect with each other. I've included the outputs below for the links that I think are important:

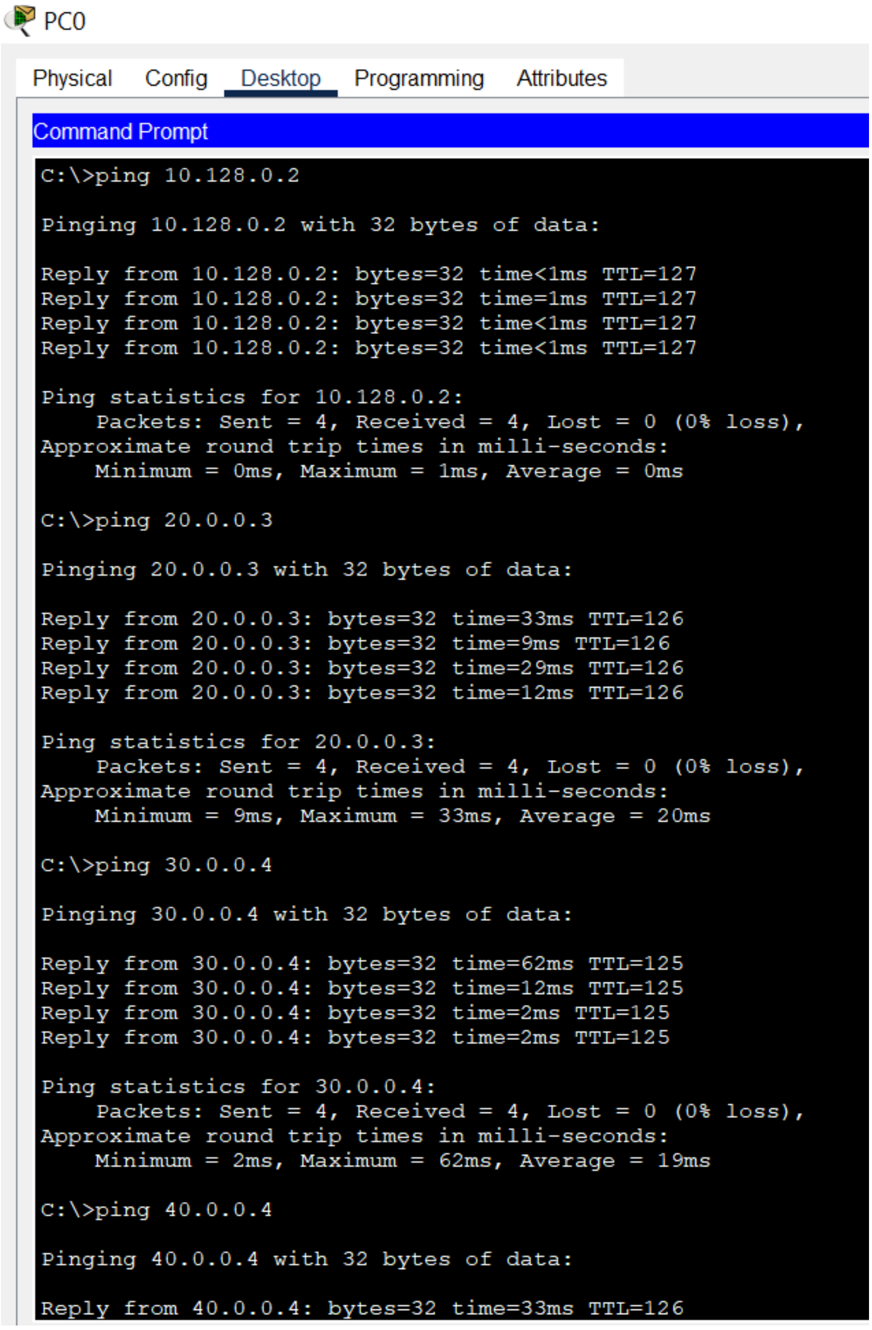

Figure 13. Some part of succesfull pings from PC 0 to the devices in other networks

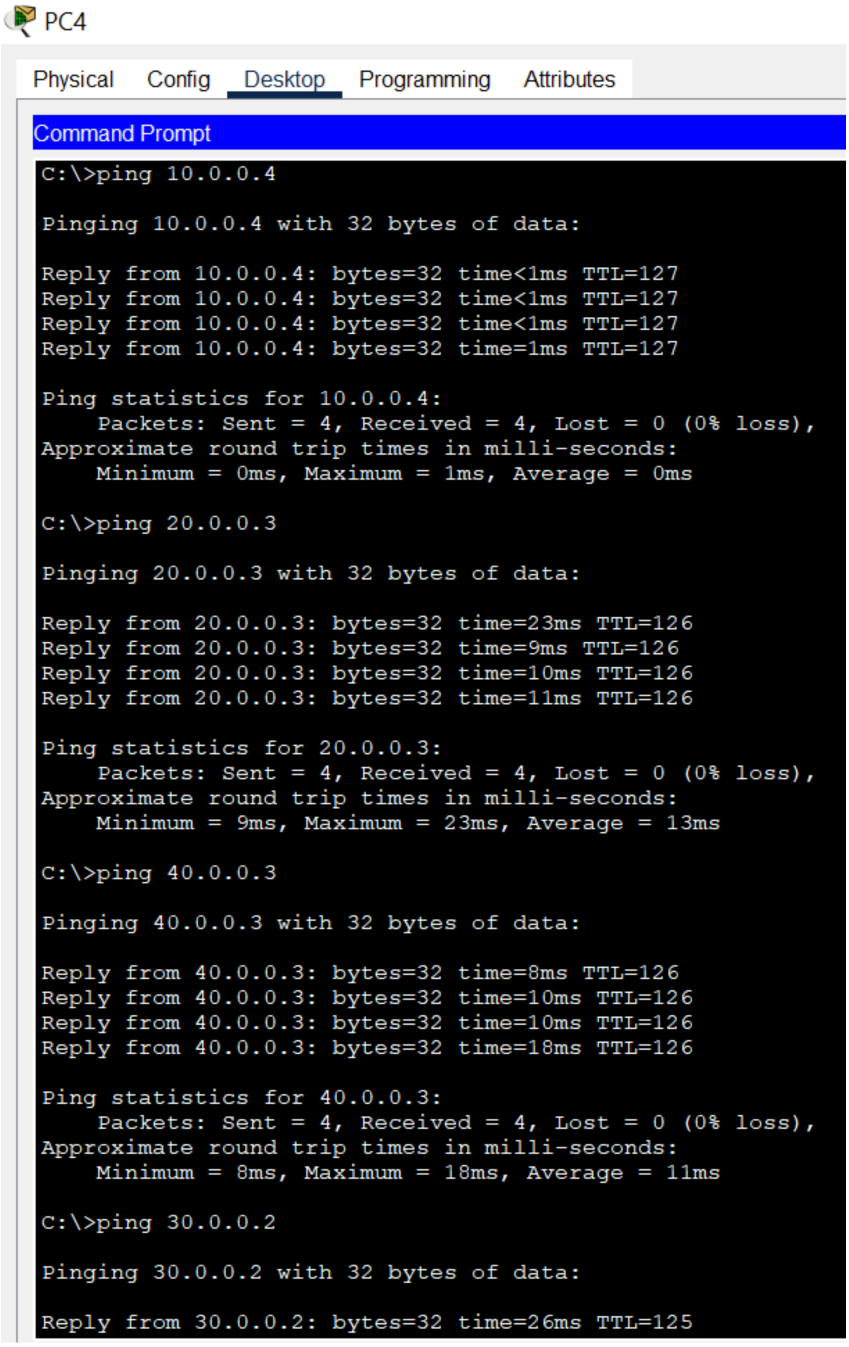

Figure 14. Some part of succesfull pings from PC 4 to the devices in other networks

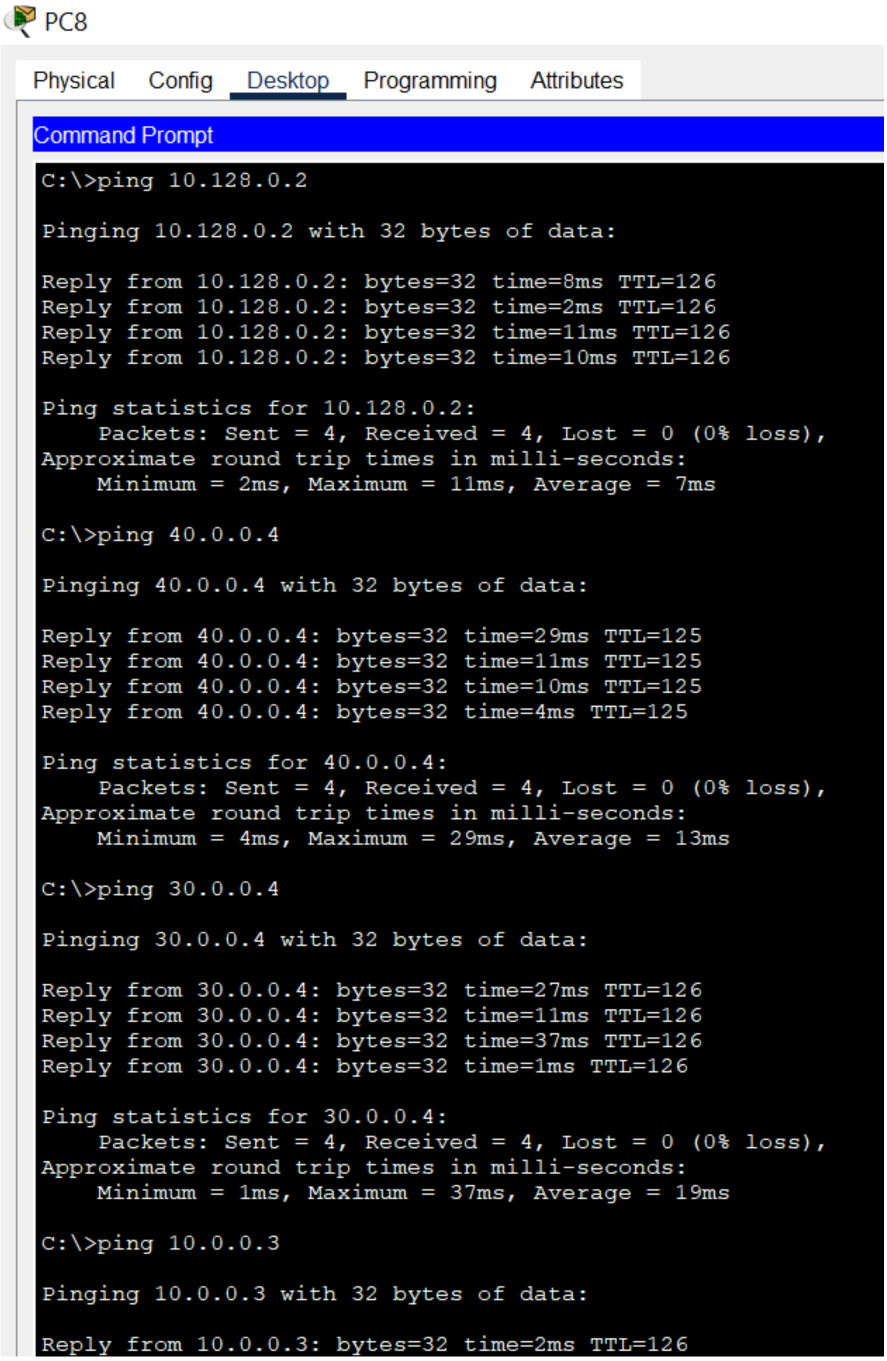

Figure 15. Some part of succesfull pings from PC 8 to the devices in other networks

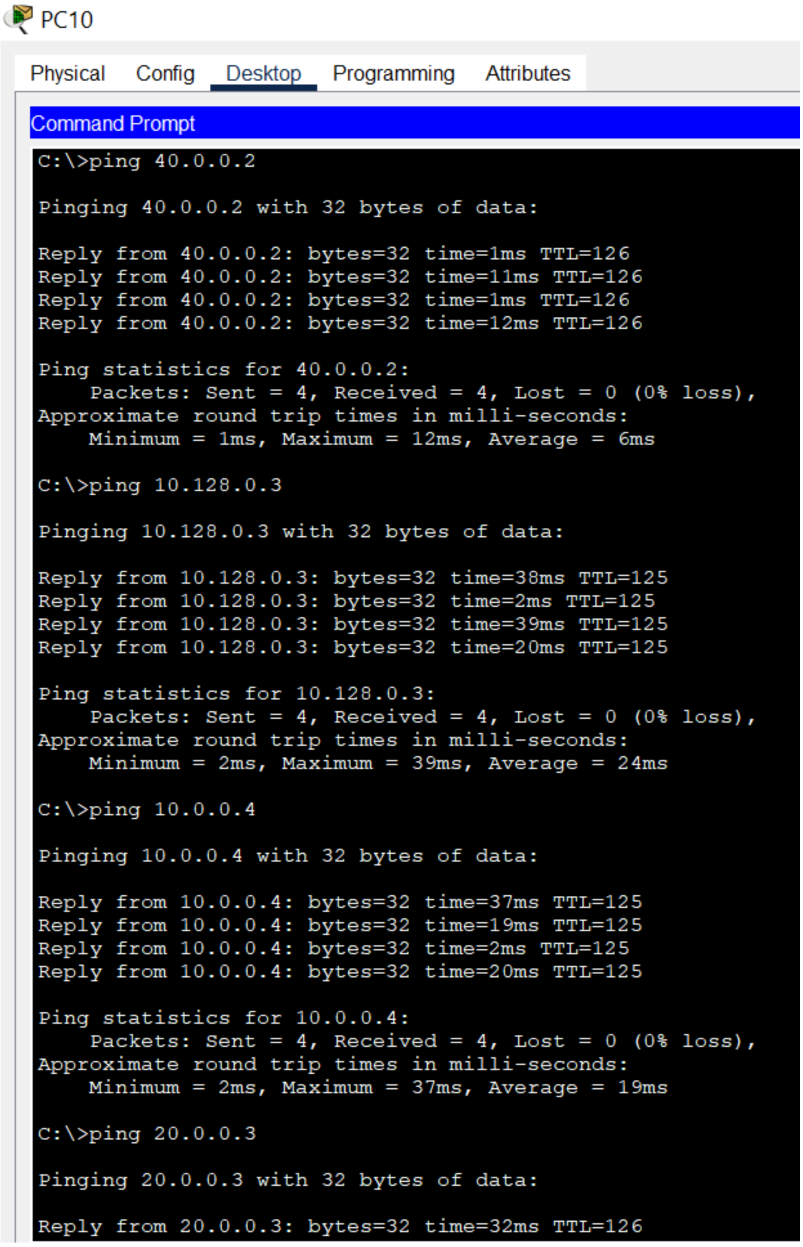

Figure 16. Some part of succesfull pings from PC 10 to the devices in other networks

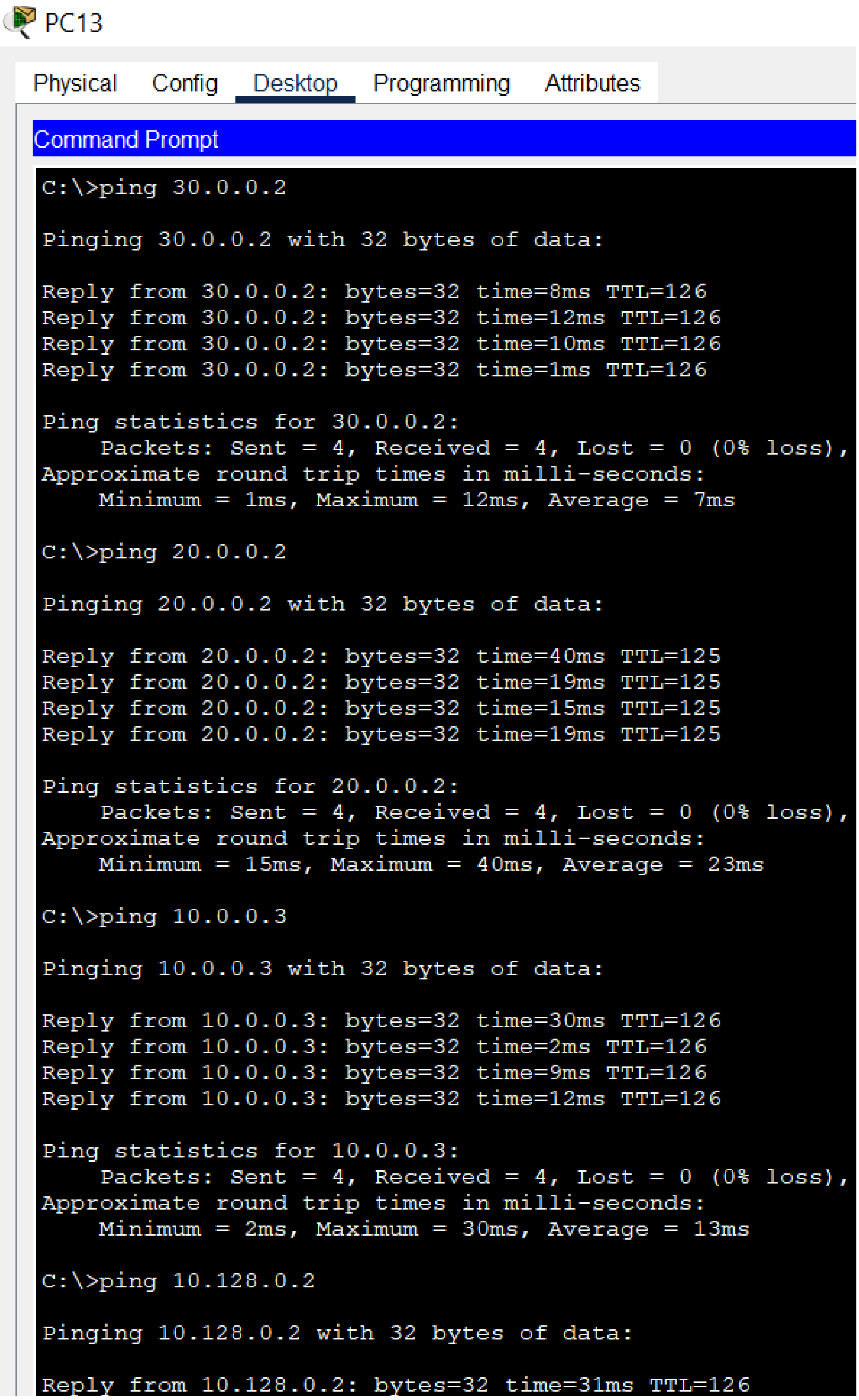

Figure 17. Some part of succesfull pings from PC 13 to the devices in other networks