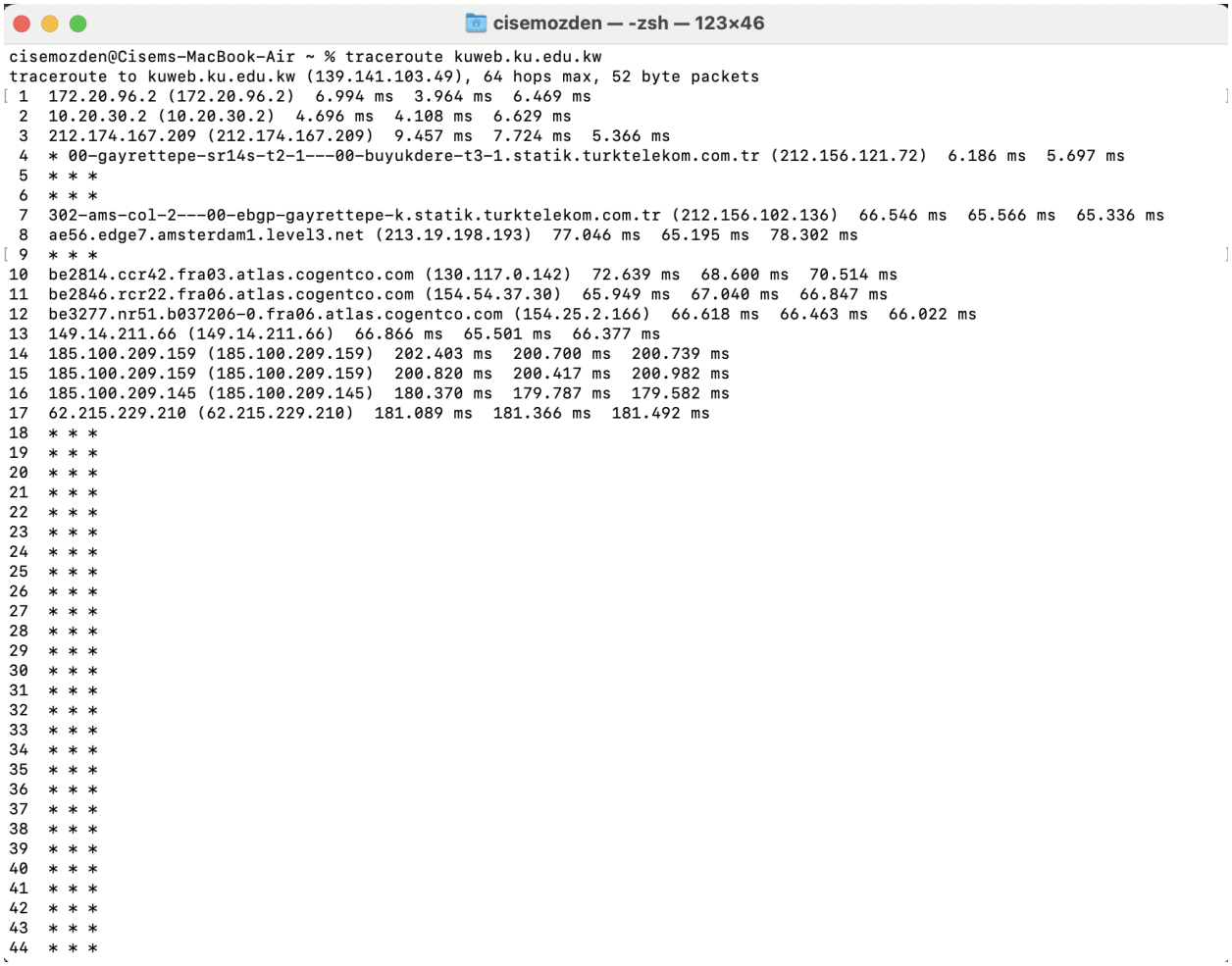
COMP416: Computer Networks
Project 3 Report
Network Layer Analysis and Simulations with Cisco Tracer

Çisem Özden, 69707

Part 1 Network Layer Analysis
Part 1.1: ICMP Analysis

1. *Find the minimum TTL less than which the traceroute messages do not reach your particular URL destination. Provide a screenshot satisfying your answer.*

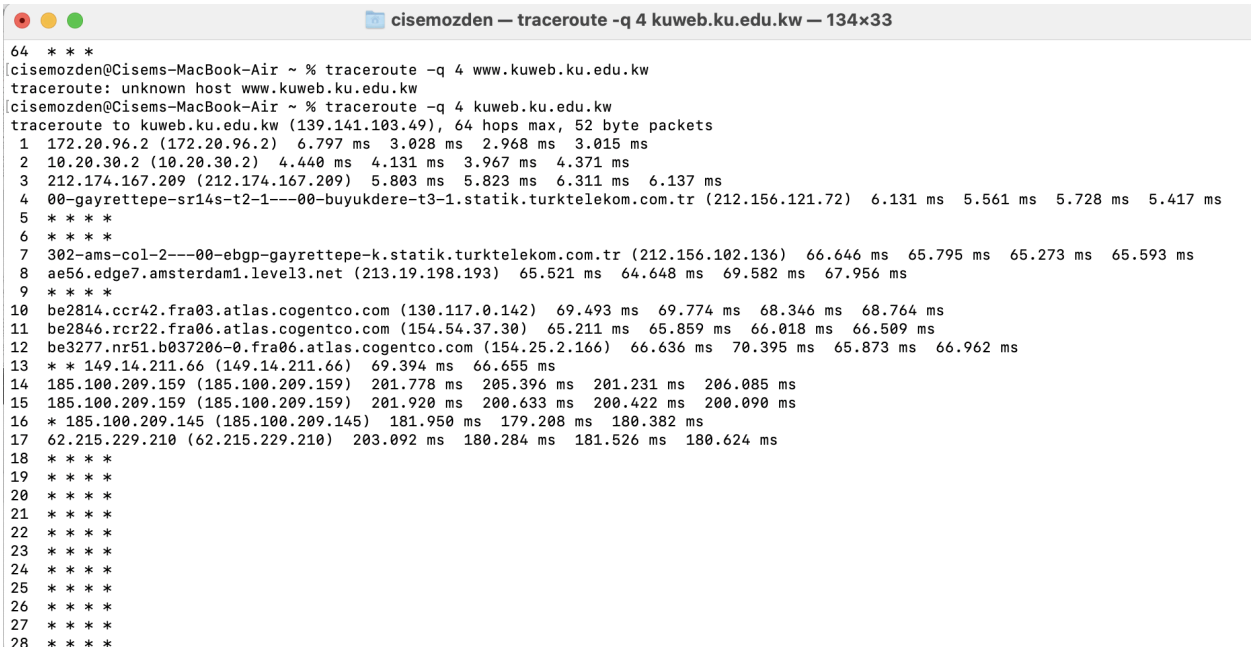
To find the minimum TTL less than which the traceroute messages do not reach my URL destination, we can look for the last TTL value where I receive a response. It is seen from the screenshot below that the last TTL with a response is at the 17th hop. After that, starting from 18th hop, we see only asterisks, indicating that the traceroute messages did not reach the destination. Therefore, the minimum TTL less than which the traceroute messages do not reach my URL destination is 18. (P.S. The asterisks continue till the 64th hop, then the traceroute completes.)



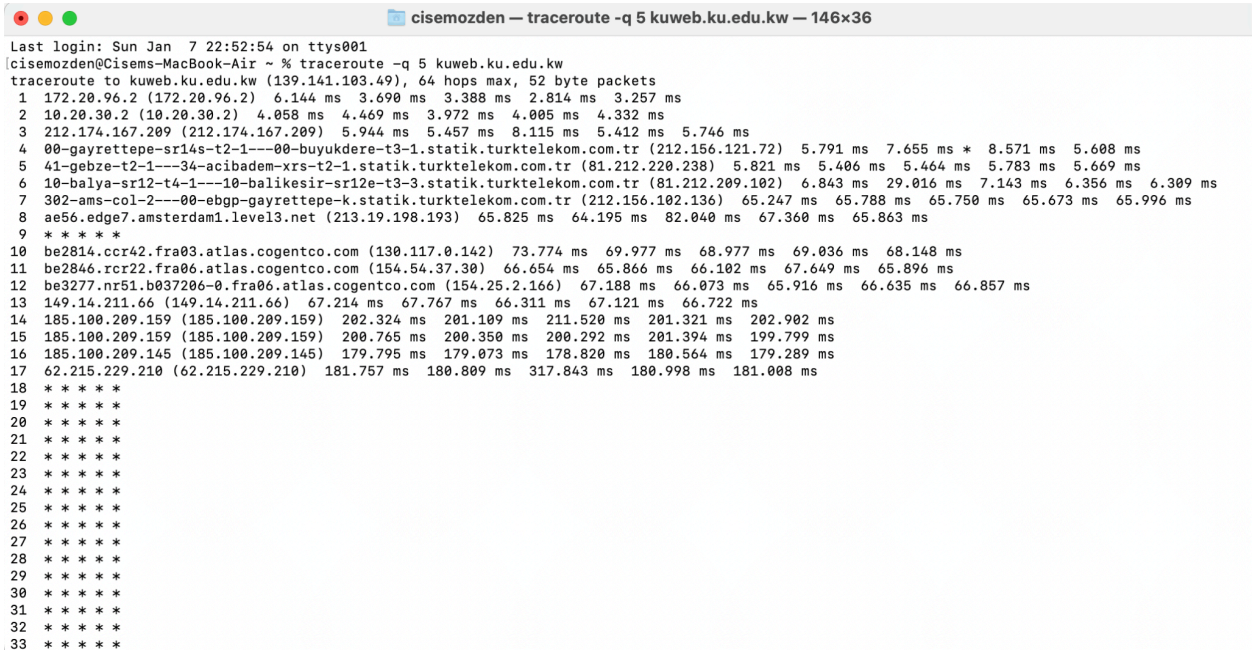
2. *What is the default number of probes used by the traceroute? Run multiple traceroutes, increasing the number of probes progressively. Explain your observation regarding the resolution of the route to your destination ip address.*

The default number of probes used by the traceroute is 3. To run the traceroute with increasing number of probes, the following command can be used: *traceroute -q 6 kuweb.ku.edu.kw* (any number can be used in the place of 6).

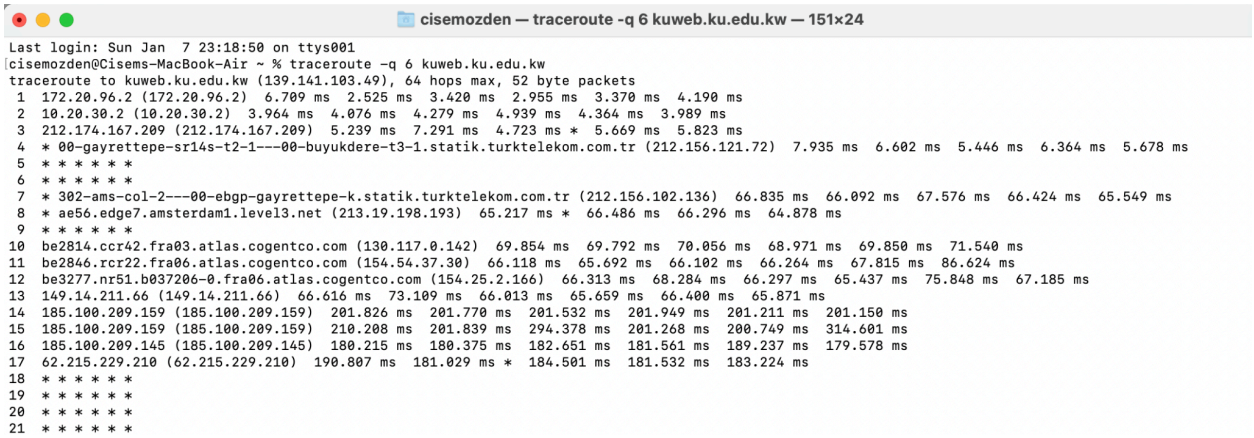
Result of using 4 probes: As seen from the below, in terms of resolution, there is not much difference compared to the default one (3 probes).



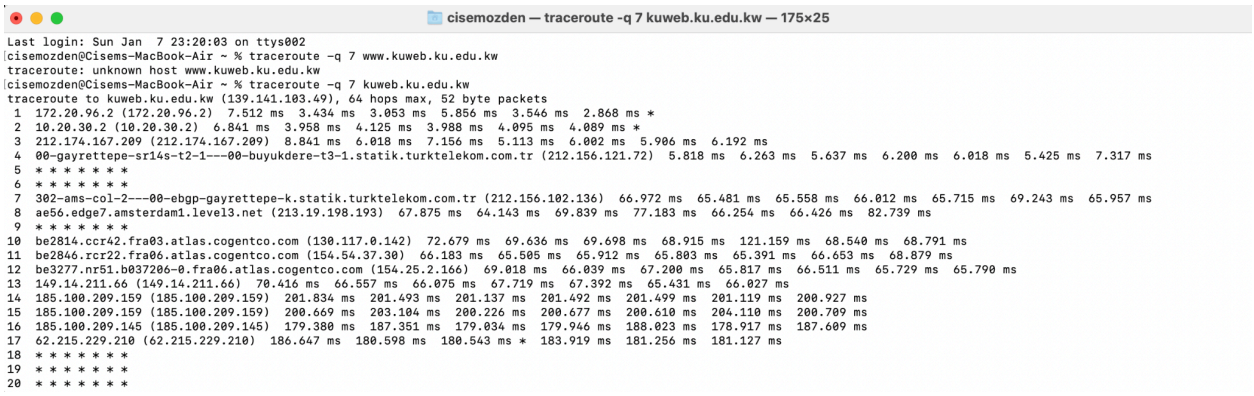
Result of using 5 probes: Looking at the result below, we can say that the resolution of the traceroute increased a bit. At hops 5 and 6, now, we are able to see some responses. Moreover, Except the 9th hop, there are no unstable conditions at all till the 18th hop compared to previous traceroutes.



Result of using 6 probes: With 6 probes, the responses seem to be less stable compared to previous traceroutes.



Result of using 7 probes: Using 7 probes doesn't seem to increase the resolution as well. The responses are similar to what was observed in the previous traceroutes.



Overall, I can say that the number of probes used in the traceroute may or may not change the resolution. It may provide more stable and reliable results as observed with 5 probes. Or, it may not affect it drastically as observed with other traceroutes.

3. *What is a Routing Blackhole? Provide a scenario where Routing Blackholes may be used beneficially. No screenshot is expected.*

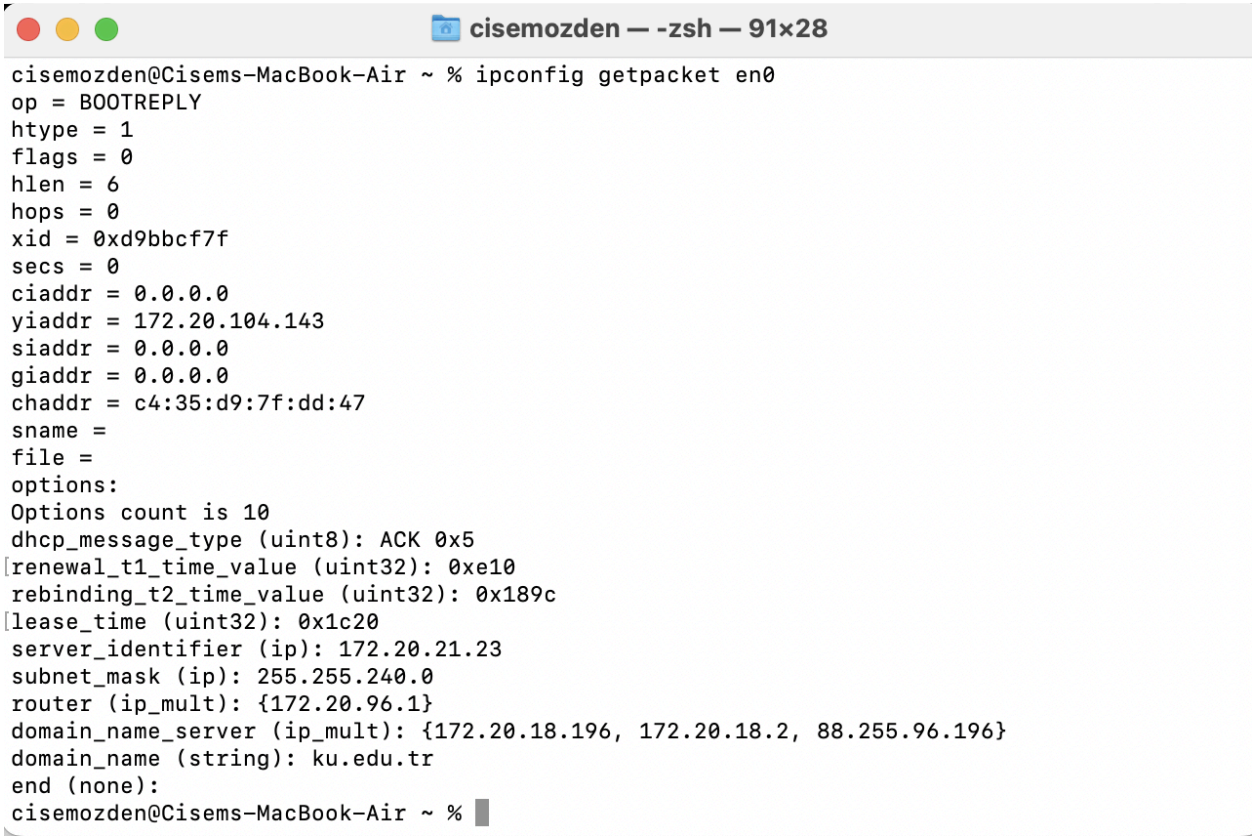
A routing blackhole refers to a network route that goes nowhere. Matching packets are dropped (ignored) rather than forwarded, resulting in loss of data. Routing blackholes can be useful against DDoS attacks. When a routing blackhole is implemented, if a DDoS attack is happening, then all the malicious traffic can be routed to the blackhole rather than the targeted IP address. In this way, DDoS attacks can be avoided.

Part 1.2: Network Interface Analysis

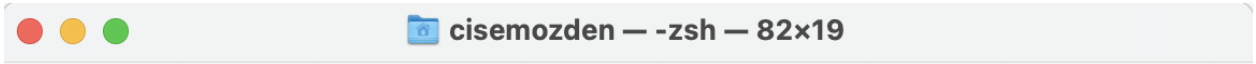
(P.S. Since the variations of *ipconfig* command is limited in Mac unlike Linux, I couldn't show the result for different objects in 2 of the commands. I am limited with en0 as interface_name because others don't give an output.)

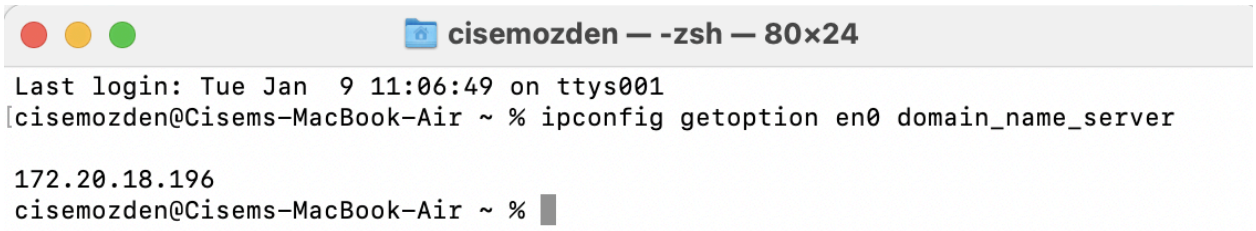
1. *Understand how to use the ip command and then execute three different variations (OBJECTs) of it while explaining their usefulness. Provide screenshots of each command executed. In each command, you are going to execute, use at least two OPTIONs you have not used before.*

ipconfig getpacket interface_name: It prints the DHCP/BOOTP packet that the client accepted from the DHCP/BOOTP server. This command is useful to check what the server provided, and whether the values are sensible. An example usage can be seen below.

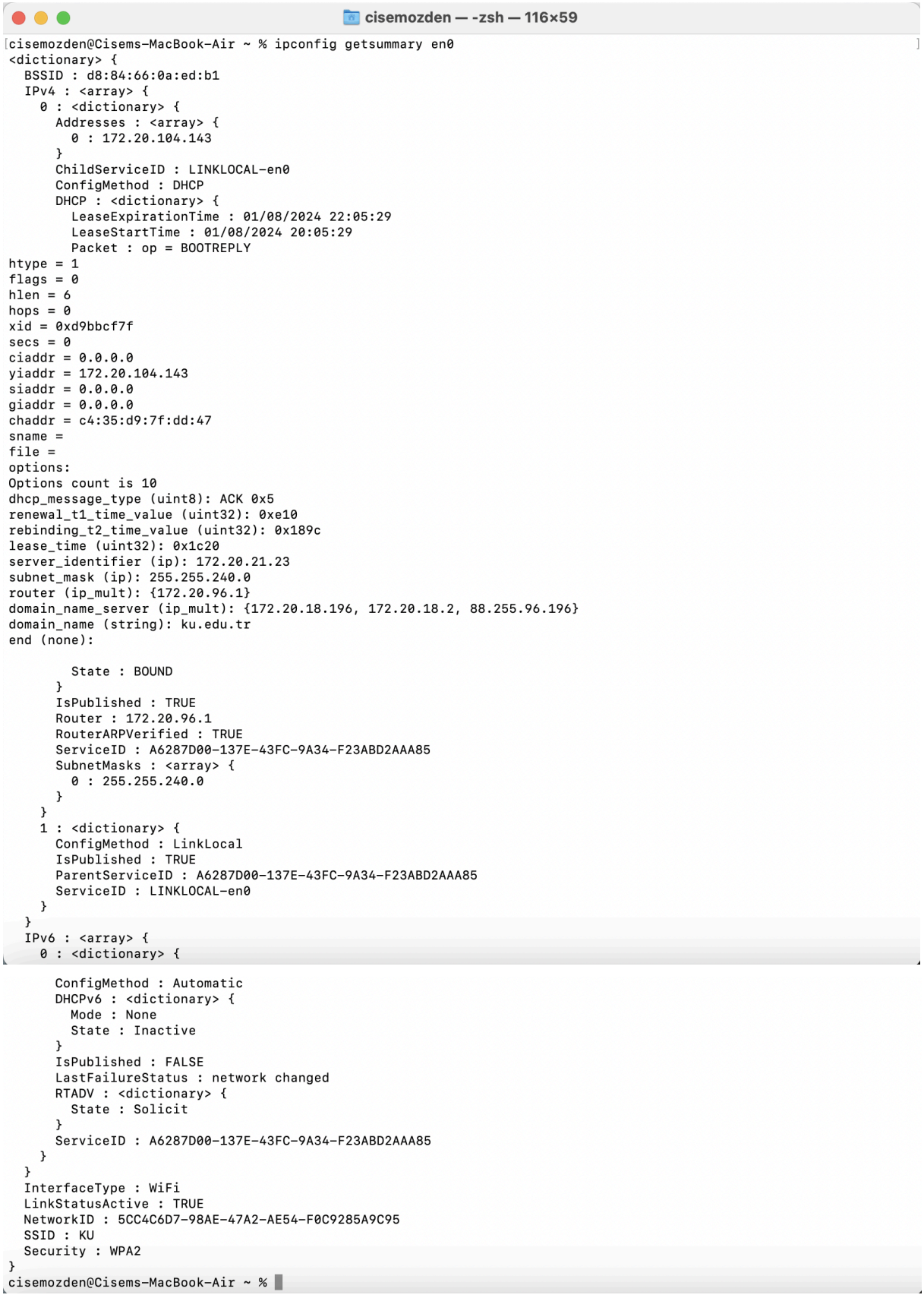


ipconfig getoption interface_name (option-name | option-code): It prints the BOOTP/DHCP option with the given name or option code integer value. If an option has multiple values, only the first value is printed. Example usages can be seen below.





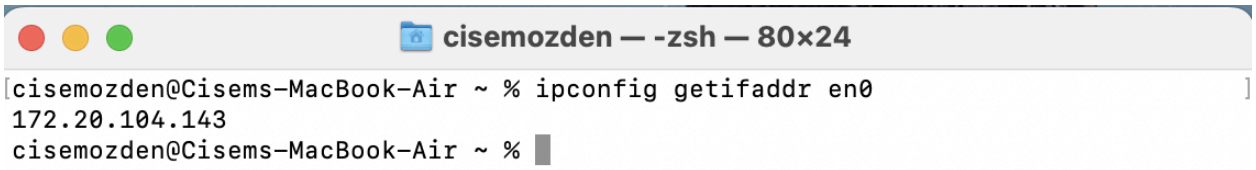
ipconfig getsummary interface_name: It prints the summary of the current IPConfiguration state over the specific interface. An example usage can be seen below.


cisemozden — -zsh — 116×59
cisemozden@Cisems-MacBook-Air ~ % ipconfig getsummary en0
<dictionary> {
BSSID : d8:84:66:0a:ed:b1
IPv4 : <array> {
0 : <dictionary> {
Addresses : <array> {
0 : 172.20.104.143
}
ChildServiceID : LINKLOCAL-en0
ConfigMethod : DHCP
DHCP : <dictionary> {
LeaseExpirationTime : 01/08/2024 22:05:29
LeaseStartTime : 01/08/2024 20:05:29
Packet : op = BOOTREPLY
htype = 1
flags = 0
hlen = 6
hops = 0
xid = 0xd9bbcf7f
secs = 0
ciaddr = 0.0.0.0
yiaddr = 172.20.104.143
siaddr = 0.0.0.0
giaddr = 0.0.0.0
chaddr = c4:35:d9:7f:dd:47
sname =
file =
options:
Options count is 10
dhcp_message_type (uint8): ACK 0x5
renewal_t1_time_value (uint32): 0xe10
rebinding_t2_time_value (uint32): 0x189c
lease_time (uint32): 0x1c20
server_identifier (ip): 172.20.21.23
subnet_mask (ip): 255.255.240.0
router (ip_mult): {172.20.96.1}
domain_name_server (ip_mult): {172.20.18.196, 172.20.18.2, 88.255.96.196}
domain_name (string): ku.edu.tr
end (none):
State : BOUND
}
IsPublished : TRUE
Router : 172.20.96.1
RouterARPVerified : TRUE
ServiceID : A6287D00-137E-43FC-9A34-F23ABD2AAA85
SubnetMasks : <array> {
0 : 255.255.240.0
}
}
1 : <dictionary> {
ConfigMethod : LinkLocal
IsPublished : TRUE
ParentServiceID : A6287D00-137E-43FC-9A34-F23ABD2AAA85
ServiceID : LINKLOCAL-en0
}
}
IPv6 : <array> {
0 : <dictionary> {
ConfigMethod : Automatic
DHCPv6 : <dictionary> {
Mode : None
State : Inactive
}
IsPublished : FALSE
LastFailureStatus : network changed
RTADV : <dictionary> {
State : Solicit
}
ServiceID : A6287D00-137E-43FC-9A34-F23ABD2AAA85
}
}
InterfaceType : WiFi
LinkStatusActive : TRUE
NetworkID : 5CC4C6D7-98AE-47A2-AE54-F0C9285A9C95
SSID : KU
Security : WPA2
}
cisemozden@Cisems-MacBook-Air ~ %

Part 2: Understanding IP and Subnetting

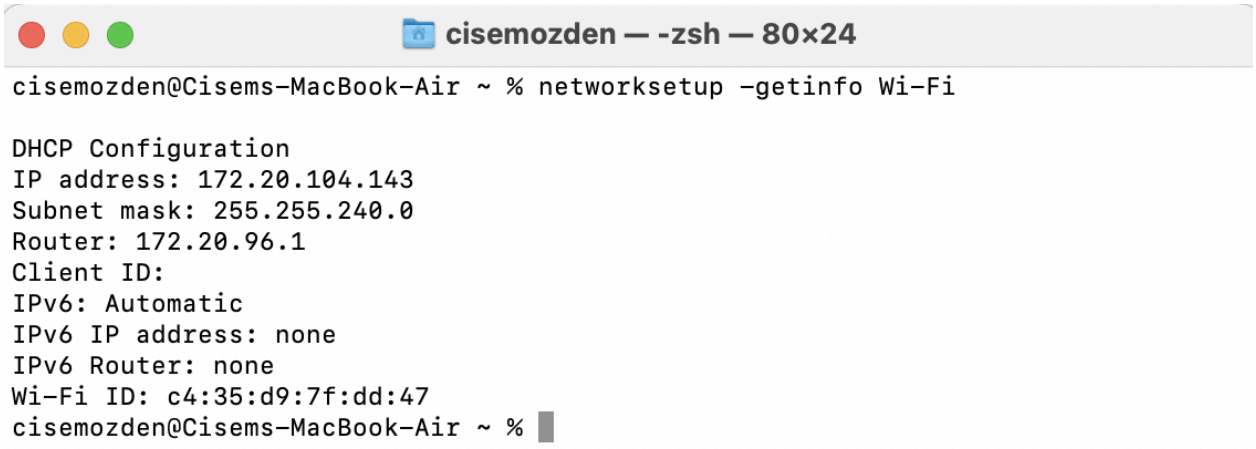
1. *Using the command line on your computer, what is the IP address of the network you are currently connected to (choose the one that has a default gateway)? Attach a screenshot of the used command showing the IP address as well as the whole interface information.*

The IP address of the network I am connected to is 172.20.104.143 as shown below. To get that information I used the *ipconfig getifaddr en0* command.



2. *What is the subnet mask of the network?*

To obtain the subnet mask information belonging to the ip address of the network I am connected to, *networksetup -getinfo Wi-Fi* command can be used as shown below. According to the output, the subnet mask of the network is 255.255.240.0.



3. *What is the network (subnet) address that you are connected to?*

To calculate the network address, the following steps are pursued: first write the binary representation of the subnet mask, then write the binary representation of the IP address. Finally, performing a bitwise AND operation between them gives us the network address. The binary representation of the subnet mask is the following: 11111111.11111111.11110000.00000000. The binary representation of the IP address is 10101100.00010100.01101000.10001111. Performing AND operation between them gives us the network address: 10101100.00010100.01100000.00000000 which is equivalent to 172.20.96.0.

4. *What is the broadcast address?*

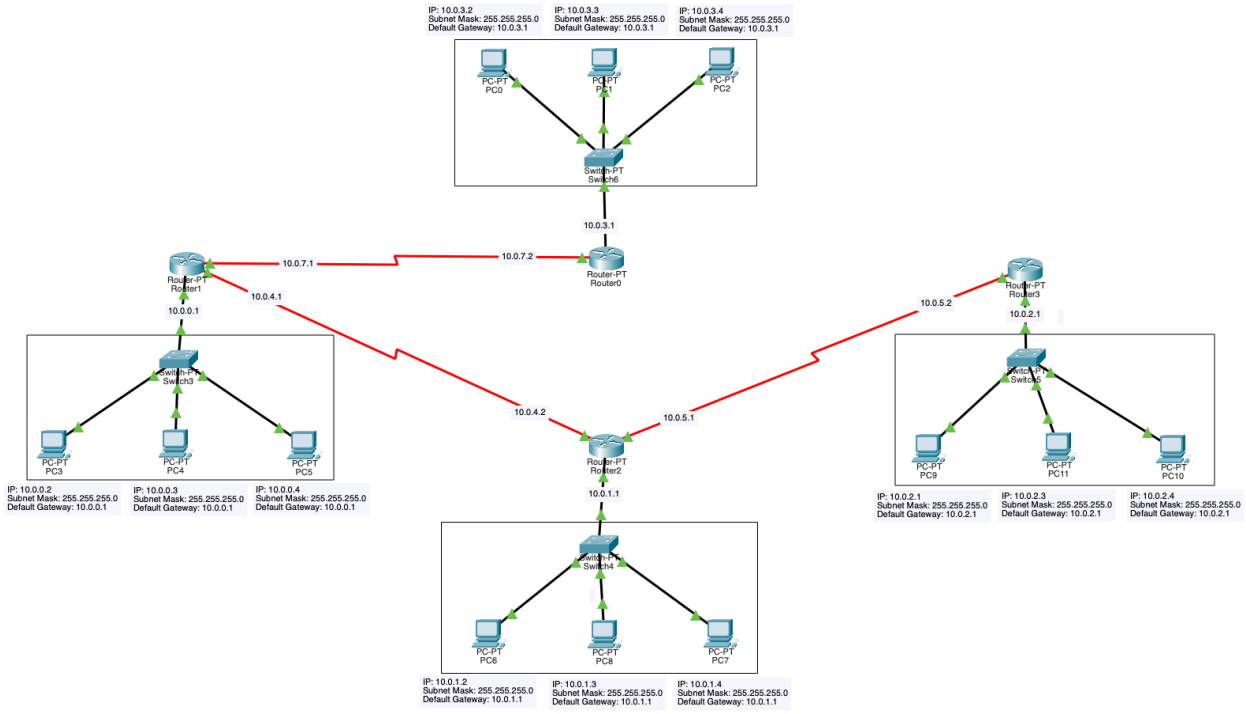
To calculate the broadcast address the following steps are pursued: first write the binary representation of the subnet mask, then calculate the wildcard mask by taking the inverse of the subnet mask. Finally, perform the bitwise OR operation between the wildcard mask and the binary representation of the network address. The binary representation of the subnet mask is the following: 11111111.11111111.11110000.00000000. Then, the Wildcard mask is 00000000.00000000.00001111.11111111. The binary representation of the network address (172.20.96.0) is 10101100.00010100.01100000.00000000. Performing OR operation between them gives us the broadcast address: 10101100.00010100.01101111.11111111 which is equivalent to 172.20.111.255.

5. *Calculate and write down the maximum number of devices that can connect to the identified network. Provide explanations.*

The binary representation of the subnet mask 255.255.240.0 is the following: 11111111.11111111.11110000.00000000. The number of 1s in the representation is 20, and the number of 0s is 12. Total number of hosts can be calculated as follows: 2^12=4096. However, the number of usable hosts is 4096-2=4094 since the first possible address of the subnet is the network address and the last possible address is the broadcast address.

Part 3: Simulations with Cisco Packet Tracer

1. *Attach a screenshot of the designed network with a label beside each port indicating its IP address, subnet mask, and gateway (if exists).*



I didn't write the subnet mask for all the ports so as not to make it too crowded. But it is the same for the serial and fast ethernet ports, as well. Subnet mask is 255.255.255.0 for all the ports.

2. *Which IP address you have selected from Options I, II, and III, and why?*

I chose Option 2. Although we are allowed to place 3 devices per subnet in the topology, the subnets should be configured so that they can accommodate 30, 20, 15, and 25 devices. Moreover, the topology should be scalable enough to add more branches and more devices in the future. When the calculations are made for all the options, the maximum number of hosts for Option 1, Option 2, and Option 3 are found as 256(2^8), 65536(2^16), and 4096(2^12), respectively. Considering the requirements, it is best to choose Option 2 since it can accommodate the most IP addresses.

3. *How many branches does your network architecture support? What is the maximum number of devices that could be connected in each branch? Provide explanations. Include the calculations in your report (images of handwritten calculations are acceptable).*

I chose the IP address as 10.0.0.0/16. With this IP, my network can accommodate a maximum of 65536 IP addresses - 65534 of them are usable. Furthermore, I chose the mask for each subnet as 255.255.255.0. Thanks to this configuration, my network can accommodate 256 subnets, each of which can support 254(2^8-2) IP addresses. However, in my network topology, I used 3 serial connections to connect 4 branches. For these connections, distinct subnets are used as well. Therefore, for my network to support n branches, n-1 serial connections would be needed, meaning 2n-1 subnets would be used in total. Since this network architecture allows a maximum of 256 subnets, the maximum number of branches my network architecture can support is 128, each of which can support 254 devices at most. The supporting calculations, and the table can be also seen below.

Chosen IP address: 10.0.0.0/16

Maximum number of hosts => 32-16=16. $2^{16}-2 = 65534$

Chosen subnet mask: 255.255.255.0

Information on subnets:

Subnet Number	Host IP Range	Usable Host IP Range	# Usable Hosts
1	10.0.0.0 - 10.0.0.255	10.0.0.1-10.0.0.254	254
2	10.0.1.0-10.0.1.255	10.0.1.1-10.0.1.254	254
3	10.0.2.0-10.0.2.255	10.0.2.1-10.0.2.254	254
⋮	⋮	⋮	⋮
256	10.0.255.0-10.0.255.255	10.0.255.1-10.0.255.254	254

n branches + (n-1) subnets for connecting routers => 2n-1

$2n-1 \leq 256$.

$2n \leq 257$

$n \leq 128.5$ → $\boxed{n=128}$ at most.

4. *While configuring your network, you probably configured the routers using the Graphical User Interface. However, in real life, a command line is probably 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.*

Router 1:

Process	***Command***
Selecting and configuring FastEthernet0/0 with ip address 10.0.0.1 and subnet mask 255.255.255.0	*interface FastEthernet0/0* *ip address 10.0.0.1 255.255.255.0*
Selecting and configuring Serial2/0	*interface Serial2/0* *ip address 10.0.7.1 255.255.255.0*
Selecting and configuring Serial3/0	*interface Serial3/0* *ip address 10.0.4.1 255.255.255.0*
Static routing for network 10.0.1.0	*ip route 10.0.1.0 255.255.255.0 10.0.4.2*
Static routing for network 10.0.2.0	*ip route 10.0.2.0 255.255.255.0 10.0.4.2*
Static routing for network 10.0.5.0	*ip route 10.0.5.0 255.255.255.0 10.0.4.2*
Static routing for network 10.0.3.0	*ip route 10.0.3.0 255.255.255.0 10.0.7.2*

Router 2:

Process	***Command***
Selecting and configuring FastEthernet0/0 with ip address 10.0.1.1 and subnet mask 255.255.255.0	*interface FastEthernet0/0* *ip address 10.0.1.1 255.255.255.0*
Selecting and configuring Serial2/0	*interface Serial2/0* *ip address 10.0.4.2 255.255.255.0*
Selecting and configuring Serial3/0	*interface Serial3/0* *ip address 10.0.5.1 255.255.255.0*
Static routing for network 10.0.0.0	*ip route 10.0.0.0 255.255.255.0 10.0.4.1*
Static routing for network 10.0.2.0	*ip route 10.0.2.0 255.255.255.0 10.0.5.2*
Static routing for network 10.0.3.0	*ip route 10.0.3.0 255.255.255.0 10.0.4.1*
Static routing for network 10.0.7.0	*ip route 10.0.7.0 255.255.255.0 10.0.4.1*

Router 3:

Process	***Command***
Selecting and configuring FastEthernet0/0 with ip address 10.0.2.1 and subnet mask 255.255.255.0	*interface FastEthernet0/0* *ip address 10.0.2.1 255.255.255.0*
Selecting and configuring Serial3/0	*interface Serial3/0* *ip address 10.0.5.2 255.255.255.0*
Static routing for network 10.0.1.0	*ip route 10.0.1.0 255.255.255.0 10.0.5.1*
Static routing for network 10.0.0.0	*ip route 10.0.0.0 255.255.255.0 10.0.5.1*
Static routing for network 10.0.4.0	*ip route 10.0.4.0 255.255.255.0 10.0.5.1*
Static routing for network 10.0.3.0	*ip route 10.0.3.0 255.255.255.0 10.0.5.1*
Static routing for network 10.0.7.0	*ip route 10.0.7.0 255.255.255.0 10.0.5.1*

Router 0:

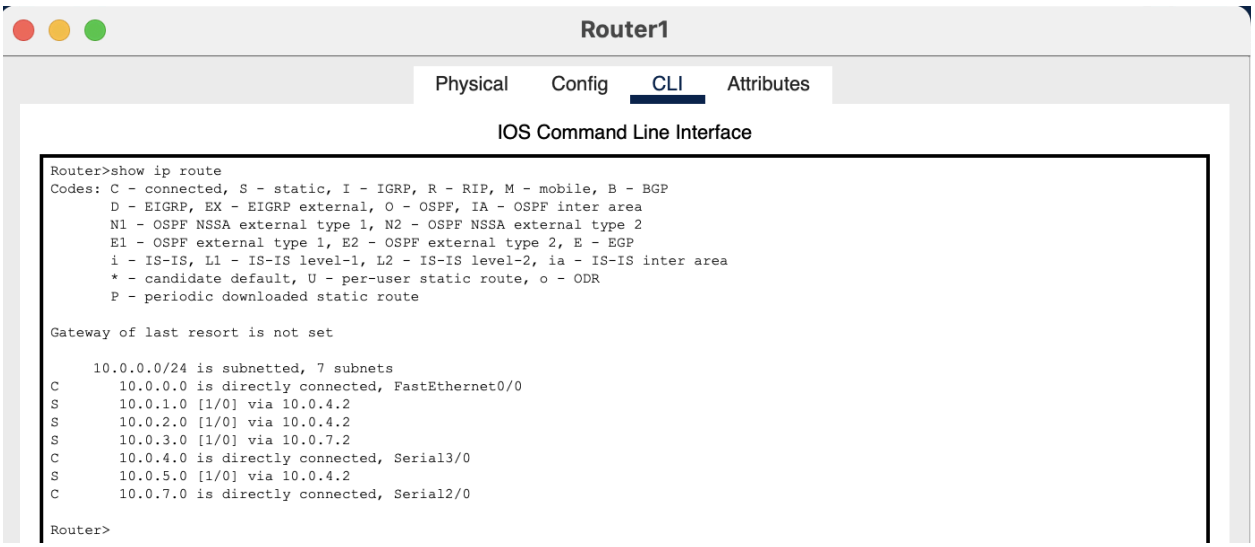
Process	***Command***
Selecting and configuring FastEthernet0/0 with ip address 10.0.3.1 and subnet mask 255.255.255.0	*interface FastEthernet0/0* *ip address 10.0.3.1 255.255.255.0*
Selecting and configuring Serial2/0	*interface Serial2/0* *ip address 10.0.7.2 255.255.255.0*
Static routing for network 10.0.0.0	*ip route 10.0.0.0 255.255.255.0 10.0.7.1*

Static routing for network 10.0.1.0	*ip route 10.0.1.0 255.255.255.0 10.0.7.1*
Static routing for network 10.0.2.0	*ip route 10.0.2.0 255.255.255.0 10.0.7.1*
Static routing for network 10.0.4.0	*ip route 10.0.4.0 255.255.255.0 10.0.7.1*
Static routing for network 10.0.5.0	*ip route 10.0.5.0 255.255.255.0 10.0.7.1*

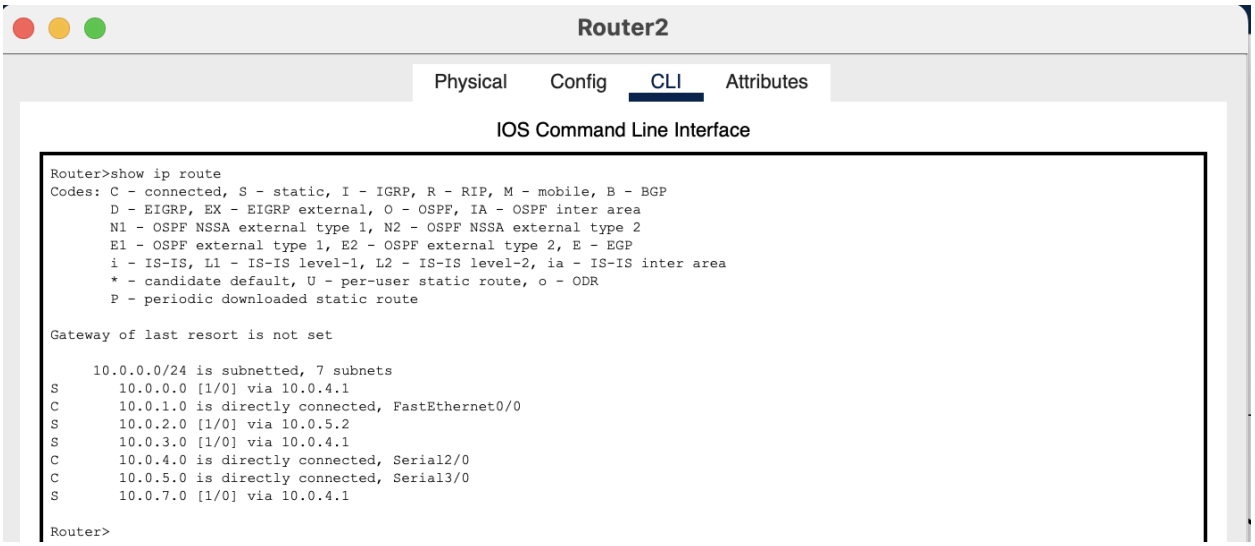
5. *You can display the routing table using the command line at each router. Search for the command that displays the routing table and attach a screenshot for the routing table at each router.*

To display the routing table, *show ip route* command can be used in the CLI of the selected router. There is only one router in my network topology and the following figure shows the corresponding routing table.

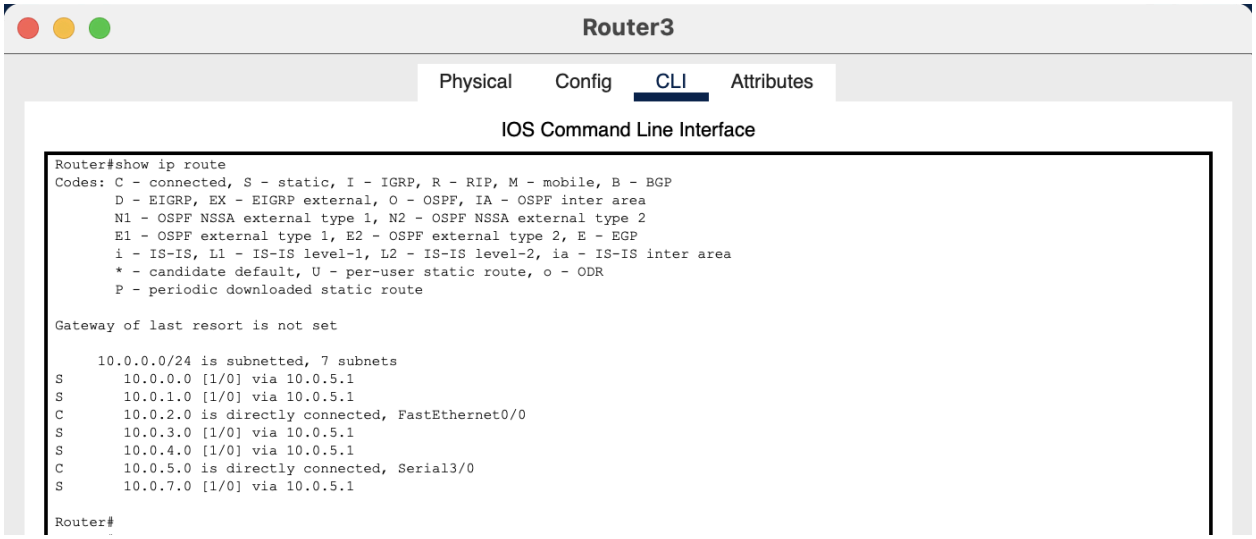
Routing table of Router 1:



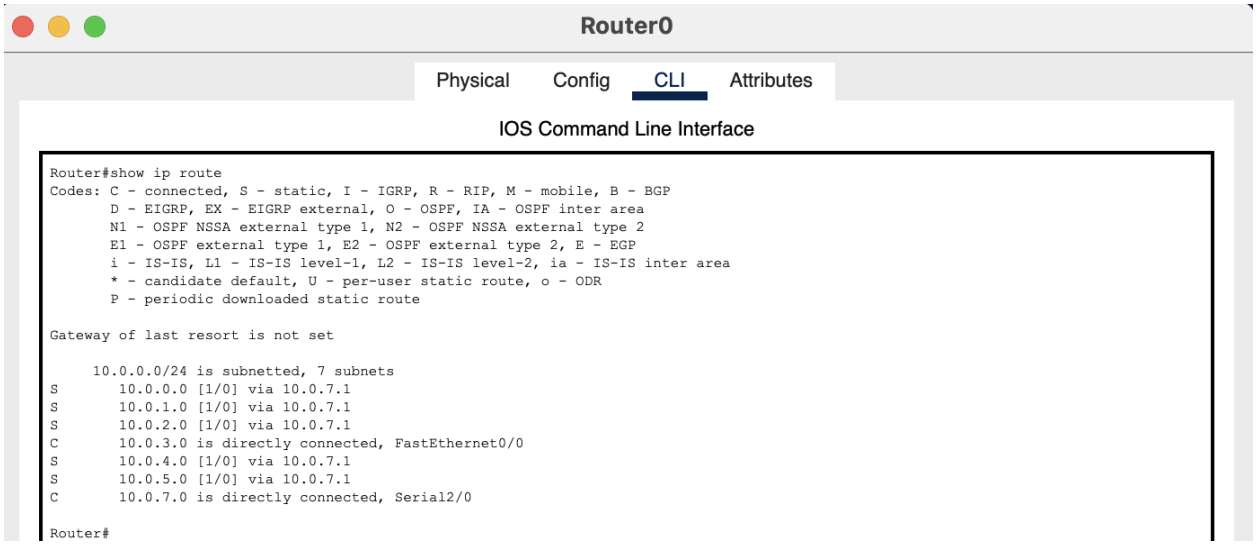
Routing table of Router 2:



Routing table of Router 3:



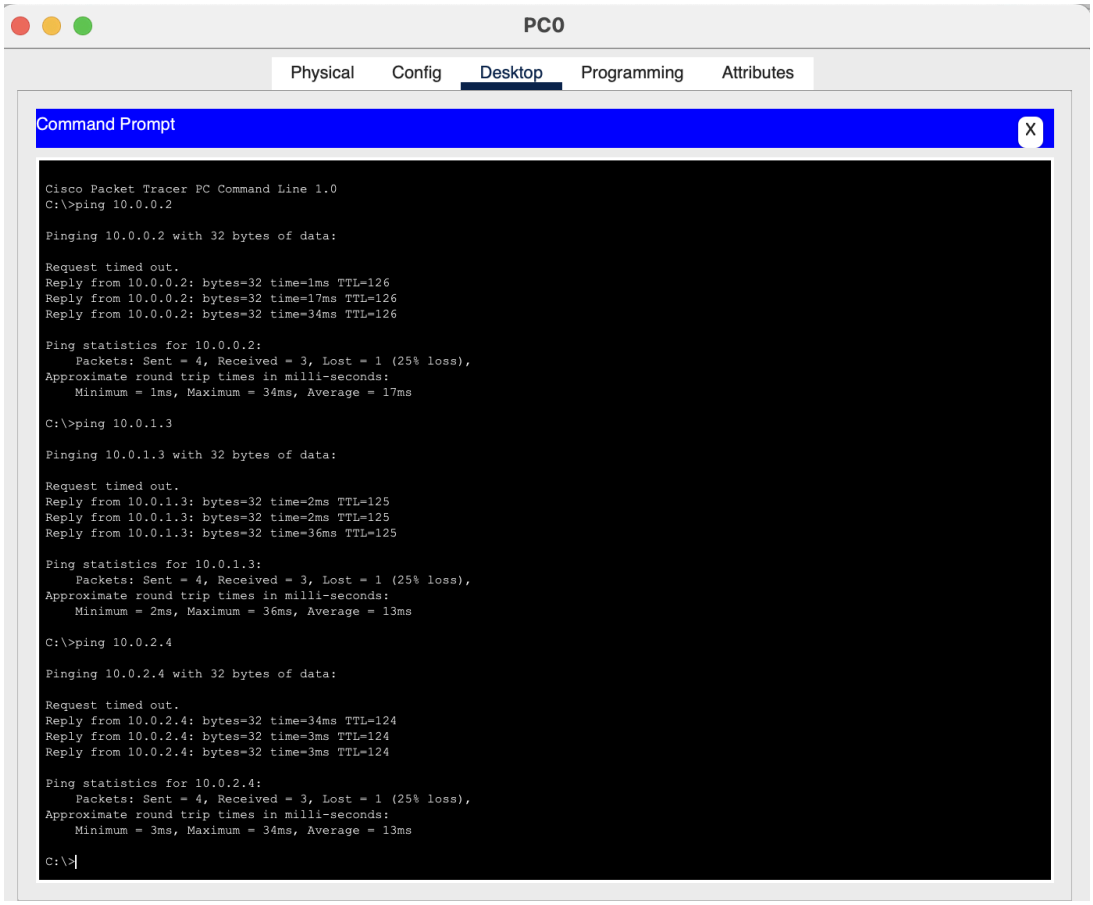
Routing table of Router 0:



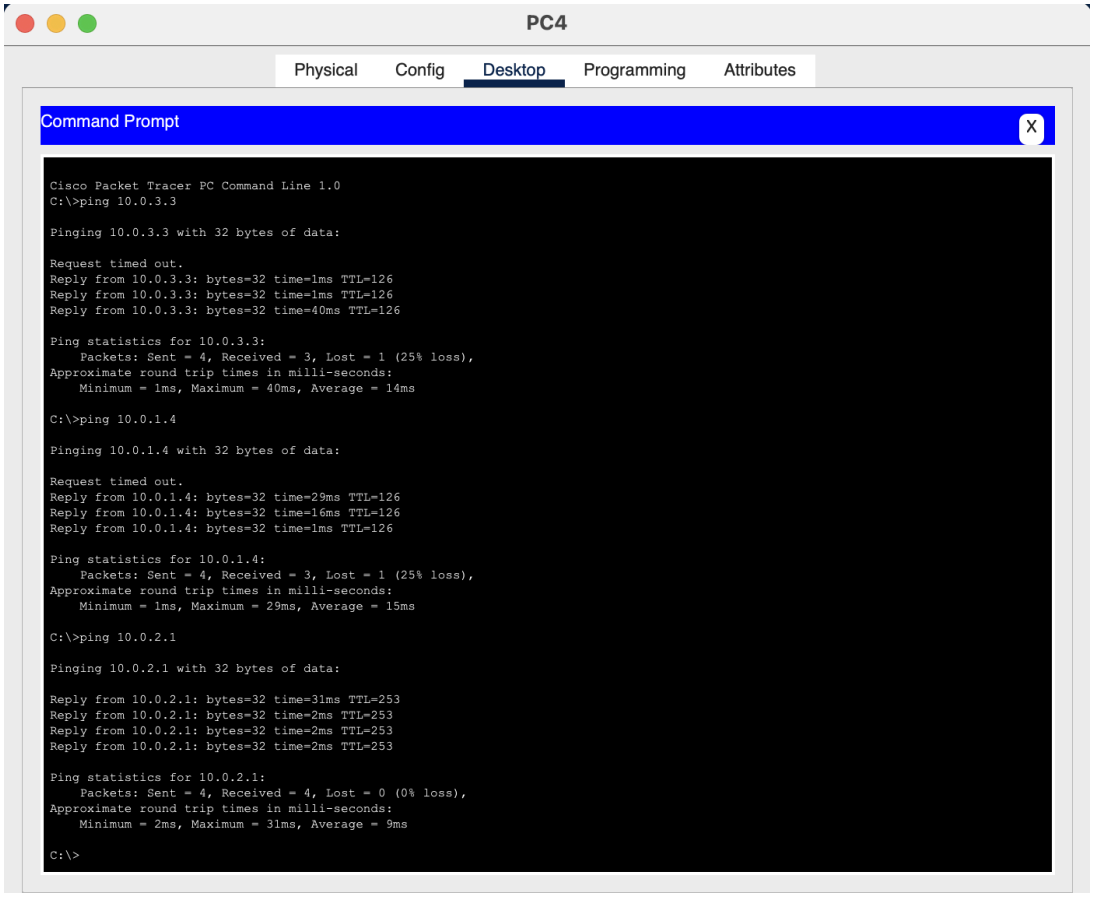
6. *Your network should be working, it means any two devices can communicate. Attach screenshots of using the ping command to test connectivity between a device from each branch with a device from other branches.*

From the screenshots below, communication between a device from each branch with a device from all other branches can be seen.

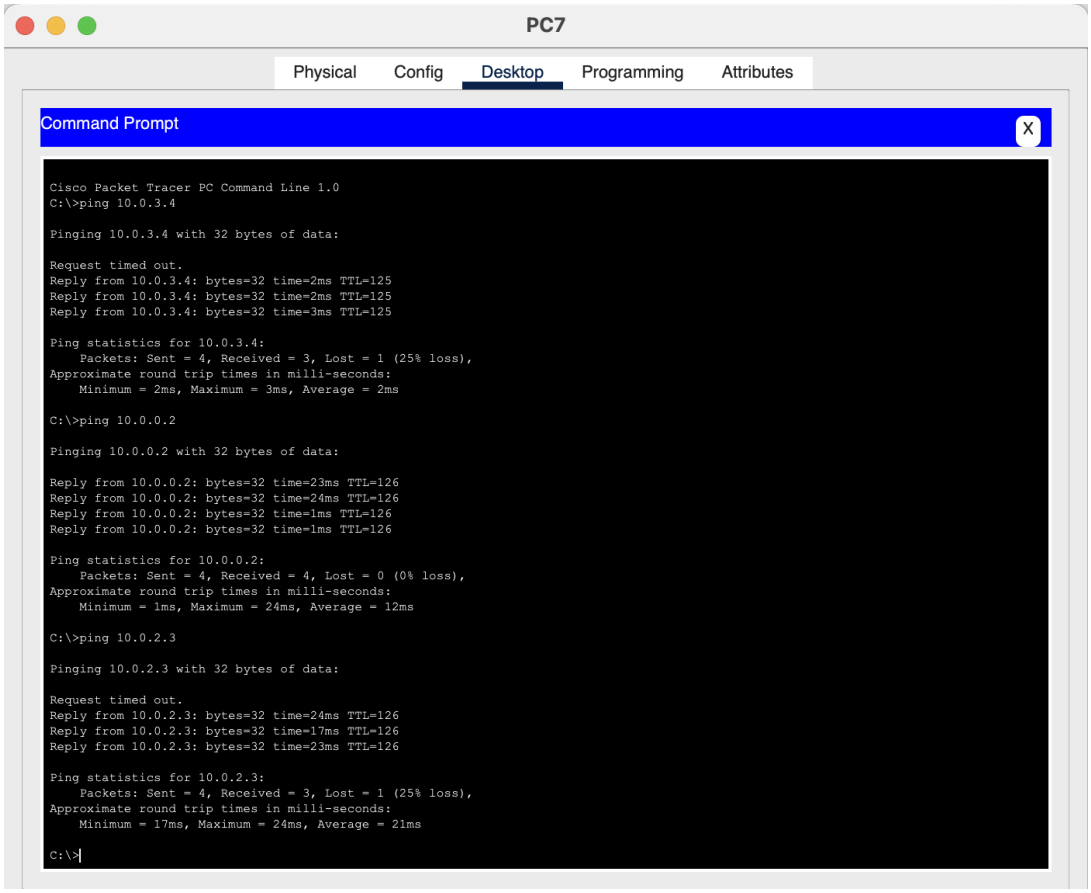
Ping from PC0 (belonging to subnet 10.0.3.0):



Ping from PC4 (belonging to subnet 10.0.0.0):



Ping from PC7 (belonging to subnet 10.0.1.0):



Ping from PC9 (belonging to subnet 10.0.2.0):