Faculty of Engineering & Technology
Electrical & Computer Engineering Department

Computer Network

ENCS3320

Project 2 Report

Prepared by:

Nirmeen Al-Sheikh - 1200200 **Section:** 1

Mariam Hamad - 1200837 **Section:** 3

Leena Affouri - 1200335 **Section:** 1

Instructor: Dr. Abdalkarim Awad

Date: 4/7/2023

Aim of the project:

The goal of the project is to understand and apply the concepts of DHCP, DNS, and ICMP protocols in computer networks. It involves capturing and analyzing packets using Wireshark software, building a network topology with routers, switches, and PCs, configuring OSPF routing protocol, implementing DHCP for automatic IP address assignment, setting up a DNS server, and testing connectivity using ping and traceroute commands. The project aims to provide practical experience and knowledge in network protocols and their application in a network environment.

Part a: explain briefly the function of: DHCP, DNS, and ICMP.

- DHCP (Dynamic Host Configuration Protocol) is a service that dynamically assigns IP addresses to network devices. It ensures that each device connected to the network has a unique IP address. To assign an IP address to a client, four messages are exchanged between the client and the DHCP server (DHCP discover, DHCP offer, DHCP request, DHCP ACK). DHCP can return more than just the assigned IP address (such as the default gateway, the name and IP address of the DNS server, and the network mask).

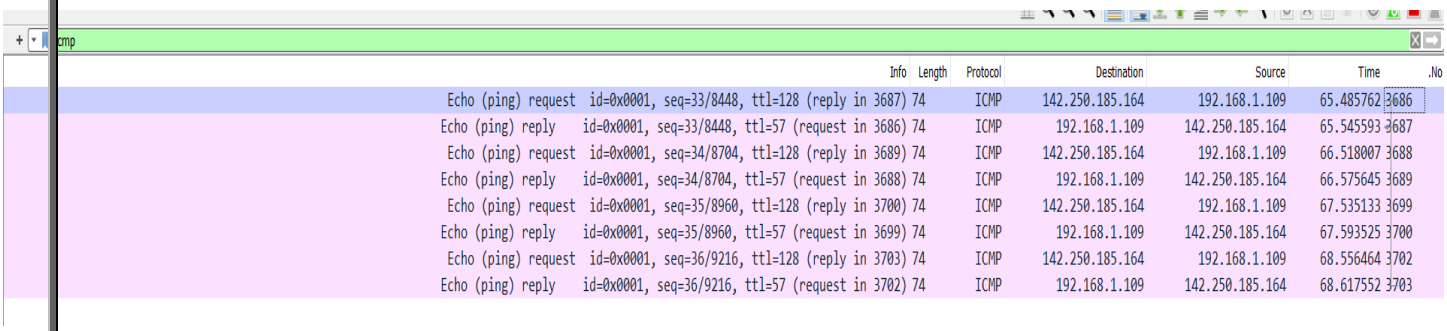
- DNS (Domain Name System) is mapping between names and IP addresses, allowing users to access websites and services using easy-to-remember domain names instead of complex IP addresses.

- ICMP (Internet Control Message Protocol) is a network protocol that detects faults while transmitting messages to a destination. It aids in the detection and reporting of network problems such as network congestion, inaccessible hosts, and network failures. ICMP packets are used for a variety of network-related activities, including ping queries to determine whether or not a host is accessible.

Part a: Using Wireshark software

ICMP packets

```
C:\Users\khaled>ping www.google.com

Pinging www.google.com [142.250.185.164] with 32 bytes of data:
Reply from 142.250.185.164: bytes=32 time=59ms TTL=57
Reply from 142.250.185.164: bytes=32 time=57ms TTL=57
Reply from 142.250.185.164: bytes=32 time=58ms TTL=57
Reply from 142.250.185.164: bytes=32 time=61ms TTL=57

Ping statistics for 142.250.185.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 57ms, Maximum = 61ms, Average = 58ms
```



Info	Length	Protocol	Destination	Source	Time	.No
Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 3687)	74	ICMP	142.250.185.164	192.168.1.109	65.485762	3686
Echo (ping) reply id=0x0001, seq=33/8448, ttl=57 (request in 3686)	74	ICMP	192.168.1.109	142.250.185.164	65.545593	3687
Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 3689)	74	ICMP	142.250.185.164	192.168.1.109	66.518007	3688
Echo (ping) reply id=0x0001, seq=34/8704, ttl=57 (request in 3688)	74	ICMP	192.168.1.109	142.250.185.164	66.575645	3689
Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 3700)	74	ICMP	142.250.185.164	192.168.1.109	67.535133	3699
Echo (ping) reply id=0x0001, seq=35/8960, ttl=57 (request in 3699)	74	ICMP	192.168.1.109	142.250.185.164	67.593525	3700
Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 3703)	74	ICMP	142.250.185.164	192.168.1.109	68.556464	3702
Echo (ping) reply id=0x0001, seq=36/9216, ttl=57 (request in 3702)	74	ICMP	192.168.1.109	142.250.185.164	68.617552	3703

On command, they used the "ping" program to send ICMP (Internet Control Message Protocol) echo request packets to the domain "www.google.com." A host's reachability and responsiveness on an Internet Protocol (IP) network are tested using the ICMP echo request, a network diagnostic tool.
This is how the output is broken down: The user sends four ICMP echo request packets to the IP address 142.250.185.164, which is the host www.google.com.
Four ICMP echo reply packets are sent by the host at the IP address 142.250.185.164 as a sign that the echo requests were successfully received.
Each echo request packet has 32 bytes of data, according to the "bytes=32" portion of the response.
The round-trip time (RTT) for each response is provided in the "time" field in milliseconds. The RTT values in this instance have a range of 57 to 61 ms, with an average of 58 ms. these numbers show how long it took for the ICMP echo request packet to get to the target host and how long it took for the ICMP echo reply packet to go back to the source.

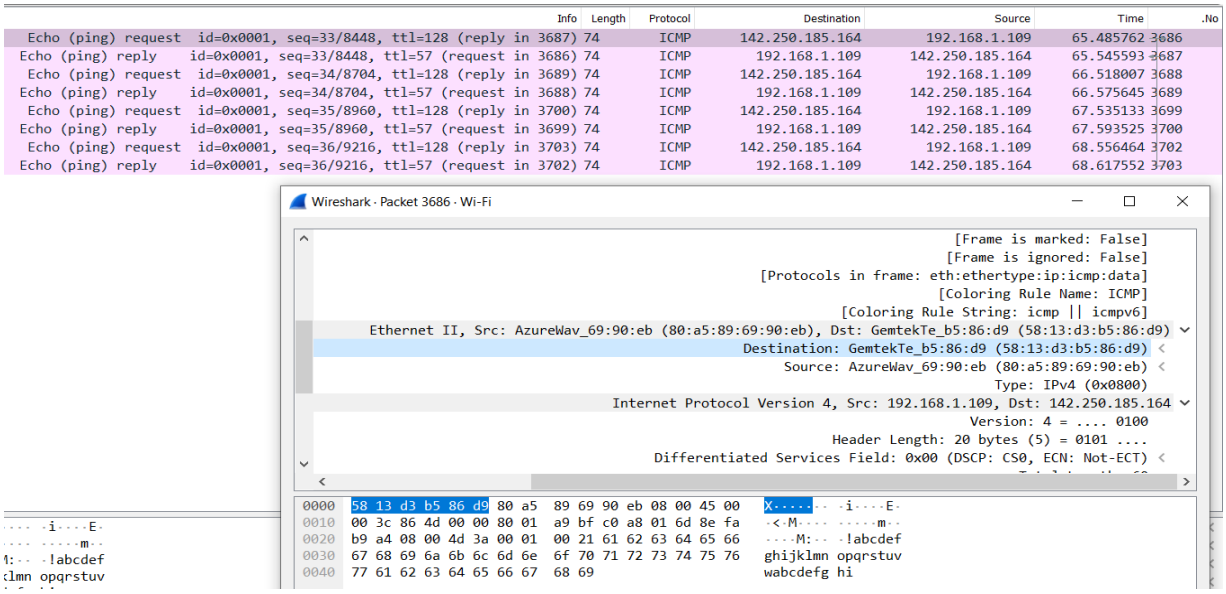
The "TTL" (Time To Live) value denotes how many network hops a packet may make before it becomes inactive. The TTL value in this instance is 57, meaning that the packet has 57 possible router transits before it expires.

The outcomes of the ping operation are compiled in the "Ping statistics" section. Four packets were transmitted, four packets were received, and there was no packet loss (0% loss), according to the statement.

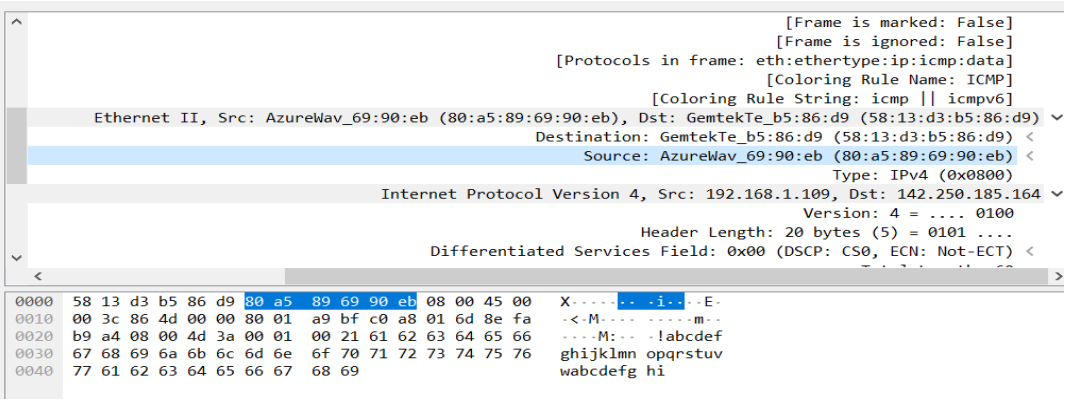
1- MAC addresses for the source and destination:

Source: 80:a5:89:69:90:eb AzureWav_69:90:eb
58:13:d3:b5:86:d9 is the destination: GemtekTe
The MAC addresses of the Ethernet frames are displayed in these fields. The network interface that sent the frame is represented by the "Source" MAC address, while the intended receiver is represented by the "Destination" MAC address.
Media Access Control address is referred to as a MAC address. It is a distinctive number that the maker of a network interface card (NIC) assigns to it. Both wired and wireless network interfaces are given MAC addresses.

MAC addresses have a 48-bit (6-byte) identification format. Six sets of two hexadecimal digits, often separated by colons or hyphens, are the most common way to represent it.



These is the source Mac address of request packet



These is the destination Mac address of request packet.

2- Addresses for the source and destination computers using Internet Protocol Version 4 (IPv4):

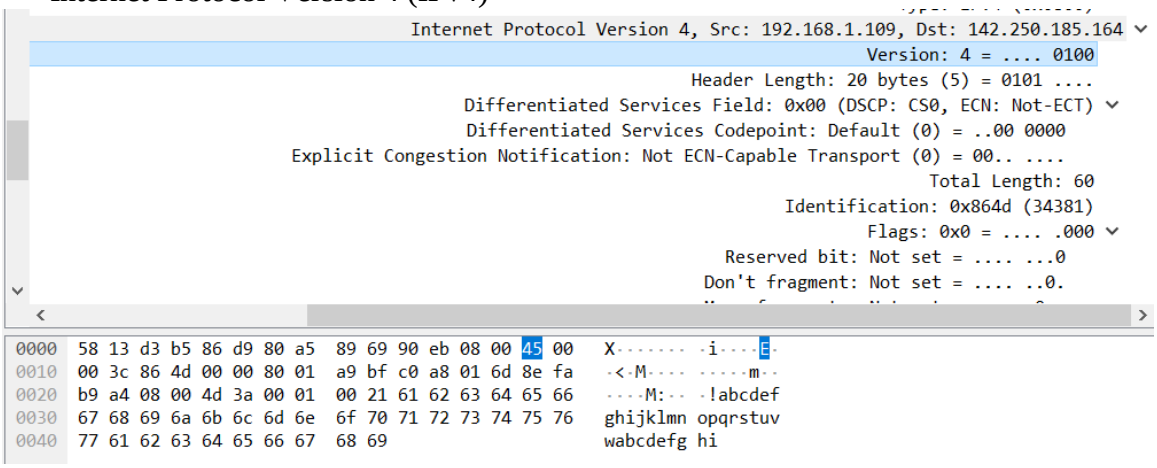
The source is 192.168.1.109

Location: 142.250.185.164

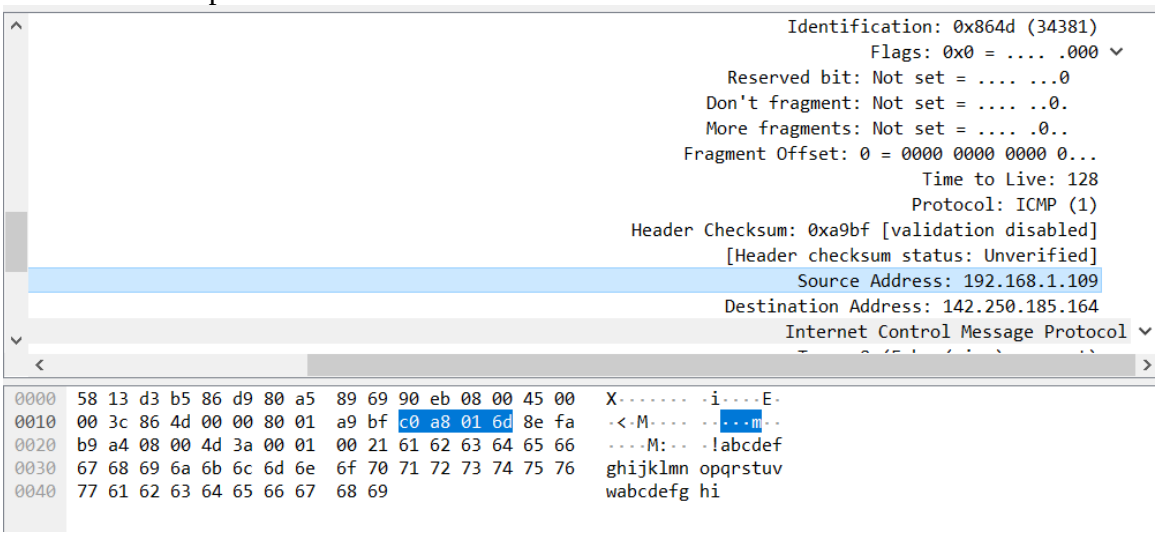
In network communication, the source IP address (192.168.1.109) indicates the IP address of the sender, whereas the destination IP address (142.250.185.164) represents the IP address of the intended receiver. The sender's device is identified by its source IP address (192.168.1.109), while the recipient device is identified by its destination IP address (142.250.185.164). These IP addresses are often shown in decimal format, also known as dotted-decimal notation, where each octet (8 bits) of the IP address is represented by a decimal number ranging from 0 to 255. This style is frequently used since it is simpler to use and easier for humans to read.

The images below show these IP addresses in hexadecimal format.

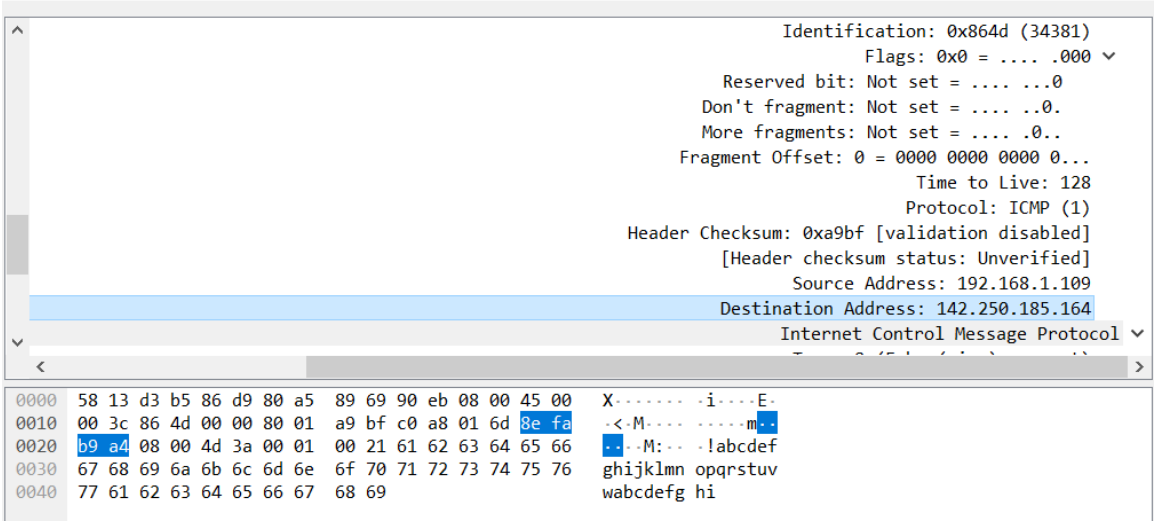
Internet Protocol Version 4 (IPv4)



The source ip address: 192.168.1.109

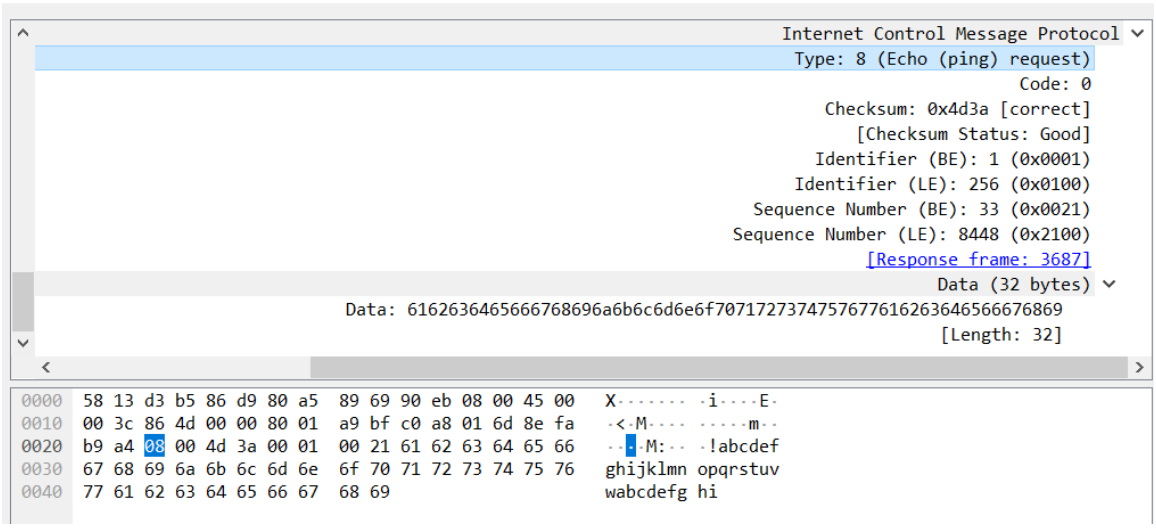


Destination ip address: 142.250.185.164



3- ICMP: Internet Control Message Protocol:

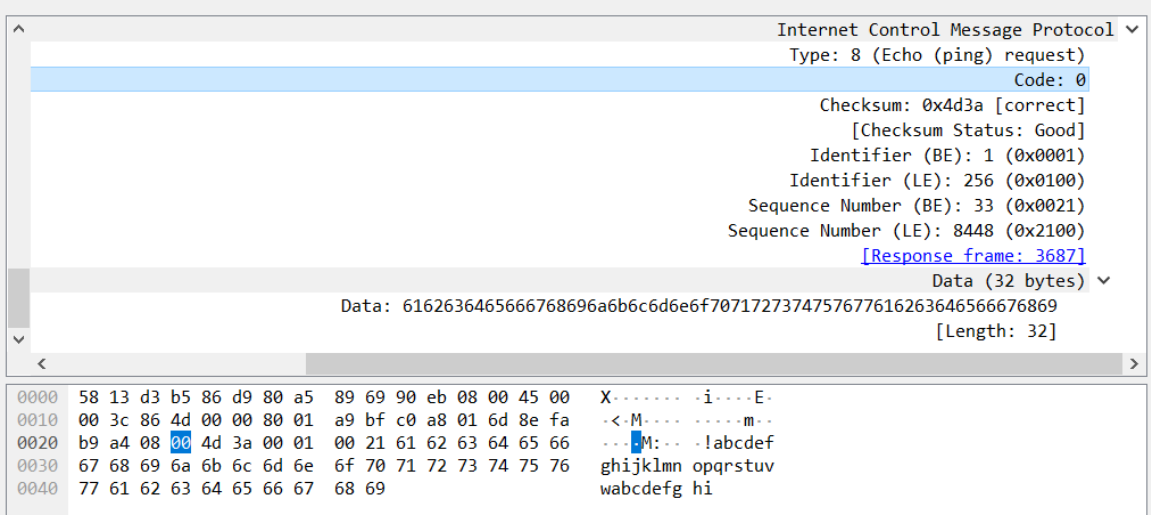
The Internet Protocol Suite includes the network protocol known as ICMP (Internet Control Message Protocol). Between network devices, it is mostly used to convey control and error messages. Type 8, which stands for an Echo (ping) request, is one of the frequently used ICMP message types. A network host's reachability and responsiveness are tested using echo request messages.



4- The ICMP (Internet Control Message Protocol) code:

Code: 0

In this field, the ICMP message code is specified. The value 0 here denotes an ordinary Echo request message.

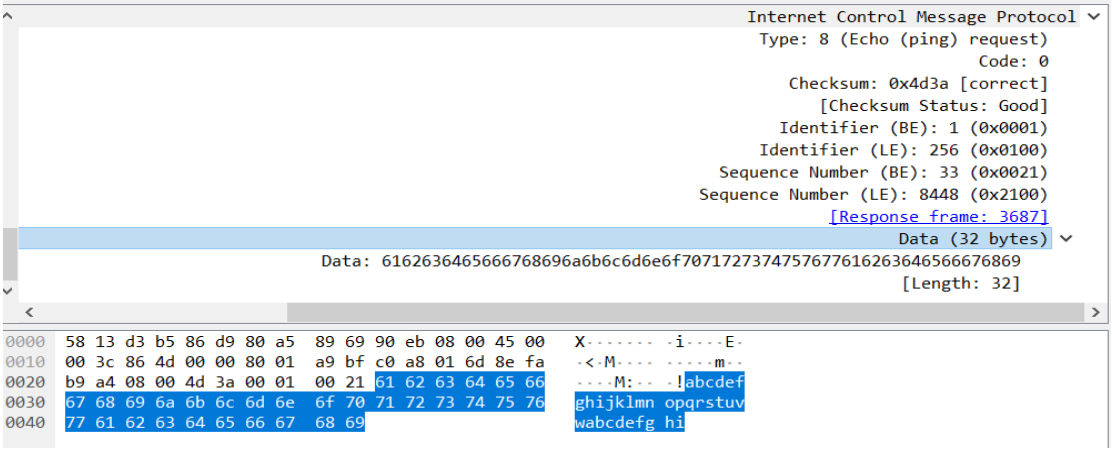


5- ICMP (Internet Control Message Protocol) Data:

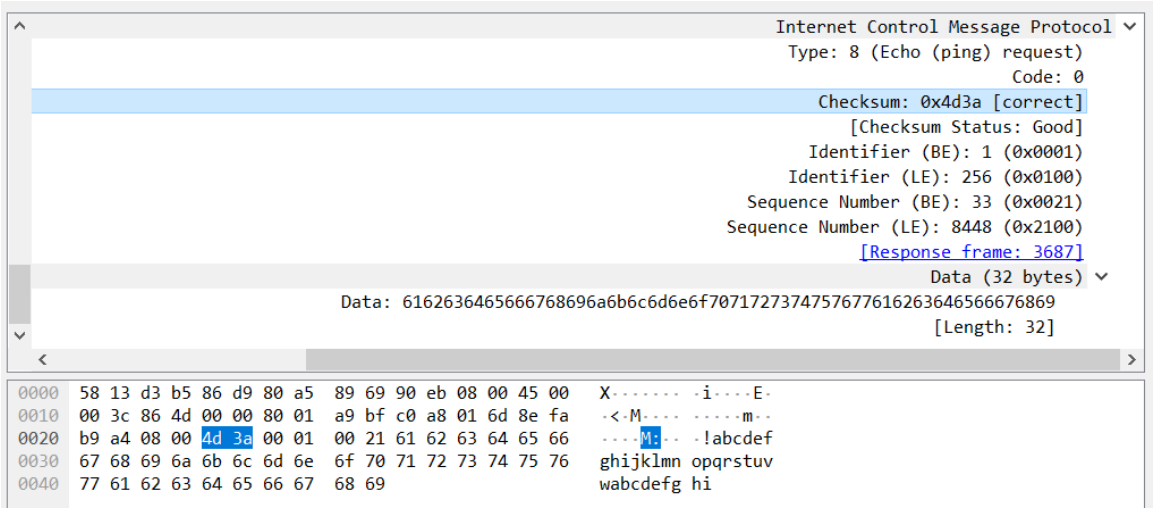
"Data Length" refers to the total amount of ICMP data in the ICMP message. Additional details related to the kind of ICMP message being transmitted are contained in the ICMP data part. The ICMP data, for instance, comprises a payload of arbitrary data needed to identify the request and its response in the case of an Echo Request (ping) message. The amount of payload or additional information that can be included in an ICMP message depends on the length of the ICMP data.

The maximum payload size specified by the underlying network protocol, such as IPv4 or IPv6, places restrictions on ICMP data. For instance, in IPv4 an ICMP message can only have a maximum payload size of 65,535 bytes, minus the size of the IP and ICMP headers.

In the figure bellow the length of data= 32
6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 9
The payload data of the ICMP packet is contained in this field. The data is a string of hexadecimal characters in the given capture. The ASCII representation of the letters "abcdefghijklmnopqrstuvwxyz" is used in this instance as the payload. The data consists of 32 bytes.

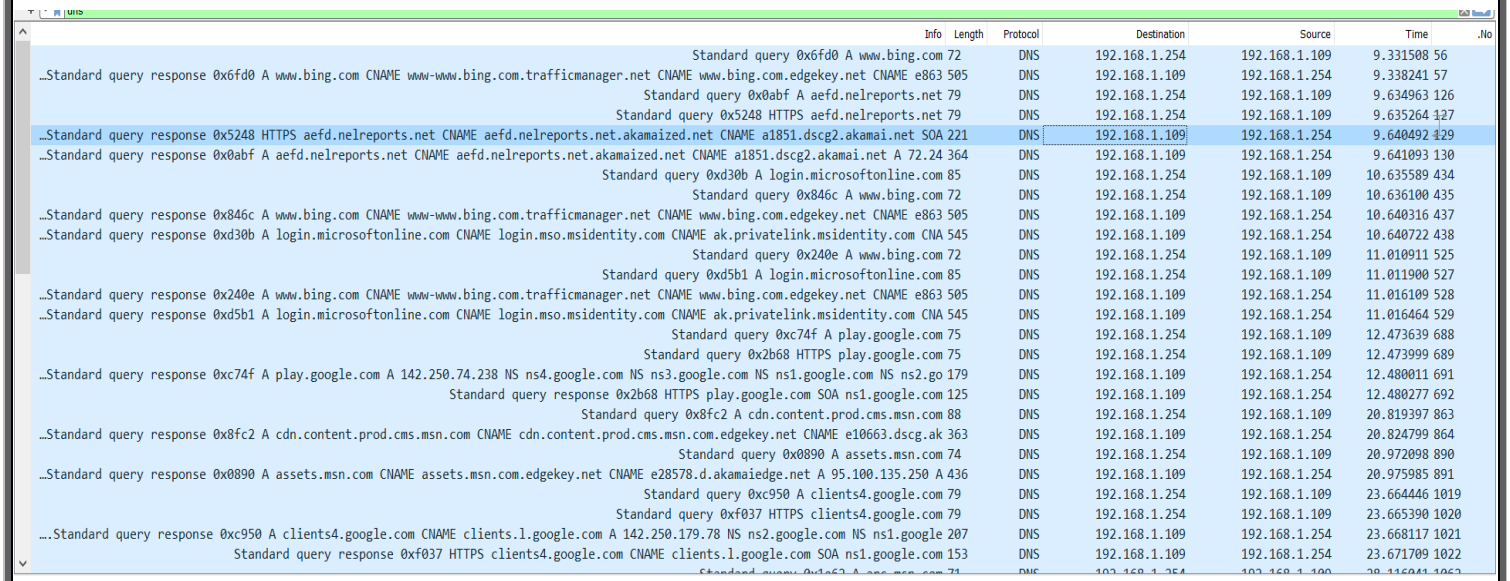


6- The checksum field in the packet capture supplied provides the computed value used for error detection and integrity testing of the ICMP packet. The checksum is used to guarantee the integrity of the packet during transmission and is computed over the ICMP header and contents. The received packet contains a valid and matching checksum since the checksum value in this instance is "0x4d3a," and it is marked as "[correct]



DNS

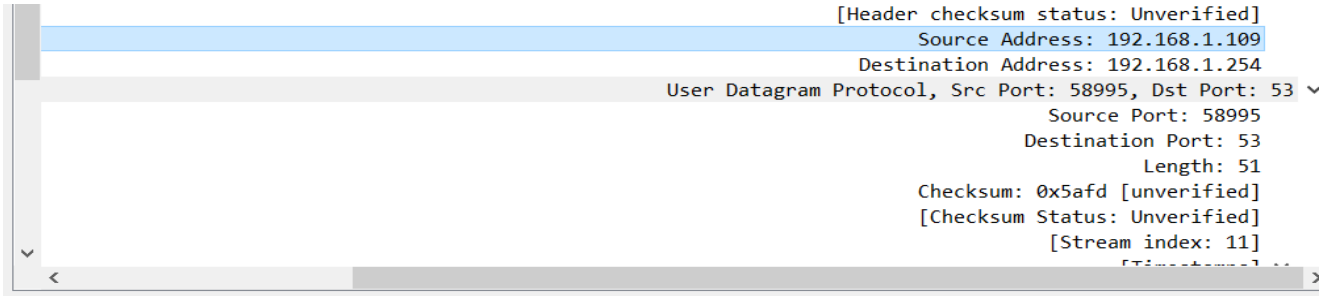
A protocol called DNS (Domain Name System) is used to convert domain names into IP addresses. Devices can search up and resolve domain names because to its distributed database functionality. For network communication, DNS converts a domain name entered by a user into an IP address.



Info	Length	Protocol	Destination	Source	Time	.No
Standard query 0x6fd0 A www.bing.com	72	DNS	192.168.1.254	192.168.1.109	9.331508	56
…Standard query response 0x6fd0 A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e863	505	DNS	192.168.1.109	192.168.1.254	9.338241	57
Standard query 0x0abf A aefd.nelreports.net	79	DNS	192.168.1.254	192.168.1.109	9.634963	126
Standard query 0x5248 HTTPS aefd.nelreports.net	79	DNS	192.168.1.254	192.168.1.109	9.635264	127
…Standard query response 0x5248 HTTPS aefd.nelreports.net CNAME aefd.nelreports.net.akamaized.net CNAME a1851.dscg2.akamai.net SOA	221	DNS	192.168.1.109	192.168.1.254	9.640492	129
…Standard query response 0x0abf A aefd.nelreports.net CNAME aefd.nelreports.net.akamaized.net CNAME a1851.dscg2.akamai.net A 72.24	364	DNS	192.168.1.109	192.168.1.254	9.641093	130
Standard query 0xd30b A login.microsoftonline.com	85	DNS	192.168.1.254	192.168.1.109	10.635589	434
Standard query 0x846c A www.bing.com	72	DNS	192.168.1.254	192.168.1.109	10.636100	435
…Standard query response 0x846c A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e863	505	DNS	192.168.1.109	192.168.1.254	10.640316	437
…Standard query response 0xd30b A login.microsoftonline.com CNAME login.mso.msidentity.com CNAME ak.privatelink.msidentity.com CNA	545	DNS	192.168.1.109	192.168.1.254	10.640722	438
Standard query 0x240e A www.bing.com	72	DNS	192.168.1.254	192.168.1.109	11.010911	525
Standard query 0xd5b1 A login.microsoftonline.com	85	DNS	192.168.1.254	192.168.1.109	11.011900	527
…Standard query response 0x240e A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e863	505	DNS	192.168.1.109	192.168.1.254	11.016109	528
…Standard query response 0xd5b1 A login.microsoftonline.com CNAME login.mso.msidentity.com CNAME ak.privatelink.msidentity.com CNA	545	DNS	192.168.1.109	192.168.1.254	11.016464	529
Standard query 0xc74f A play.google.com	75	DNS	192.168.1.254	192.168.1.109	12.473639	688
Standard query 0x2b68 HTTPS play.google.com	75	DNS	192.168.1.254	192.168.1.109	12.473999	689
…Standard query response 0xc74f A play.google.com A 142.250.74.238 NS ns4.google.com NS ns3.google.com NS ns1.google.com NS ns2.go	179	DNS	192.168.1.109	192.168.1.254	12.480011	691
Standard query response 0x2b68 HTTPS play.google.com SOA ns1.google.com	125	DNS	192.168.1.109	192.168.1.254	12.480277	692
Standard query 0x8fc2 A cdn.content.prod.cms.msn.com	88	DNS	192.168.1.254	192.168.1.109	20.819397	863
…Standard query response 0x8fc2 A cdn.content.prod.cms.msn.com CNAME cdn.content.prod.cms.msn.com.edgekey.net CNAME e10663.dscg.ak	363	DNS	192.168.1.109	192.168.1.254	20.824799	864
Standard query 0x0890 A assets.msn.com	74	DNS	192.168.1.254	192.168.1.109	20.972098	890
…Standard query response 0x0890 A assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net A 95.100.135.250 A	436	DNS	192.168.1.109	192.168.1.254	20.975985	891
Standard query 0xc950 A clients4.google.com	79	DNS	192.168.1.254	192.168.1.109	23.664446	1019
Standard query 0xf037 HTTPS clients4.google.com	79	DNS	192.168.1.254	192.168.1.109	23.665390	1020
….Standard query response 0xc950 A clients4.google.com CNAME clients.l.google.com A 142.250.179.78 NS ns2.google.com NS ns1.google	207	DNS	192.168.1.109	192.168.1.254	23.668117	1021
Standard query response 0xf037 HTTPS clients4.google.com CNAME clients.l.google.com SOA ns1.google.com	153	DNS	192.168.1.109	192.168.1.254	23.671709	1022

1- Address of the source: 192.168.1.109

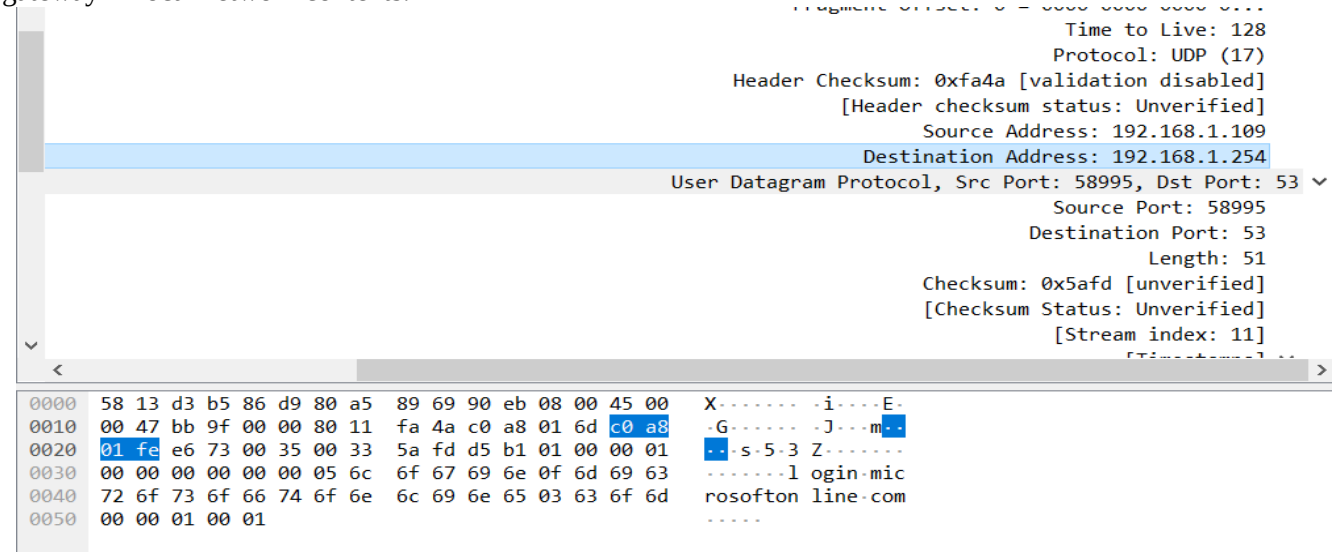
The source IP address of the packet is represented by this field, letting you know where it came from.
The source IP address in this instance is 192.168.1.109, a private IP address that is frequently used in local network contexts.
Address of the destination: 192.168.1.254



```
[Header checksum status: Unverified]
Source Address: 192.168.1.109
Destination Address: 192.168.1.254
User Datagram Protocol, Src Port: 58995, Dst Port: 53
Source Port: 58995
Destination Port: 53
Length: 51
Checksum: 0x5afd [unverified]
[Checksum Status: Unverified]
[Stream index: 11]
```

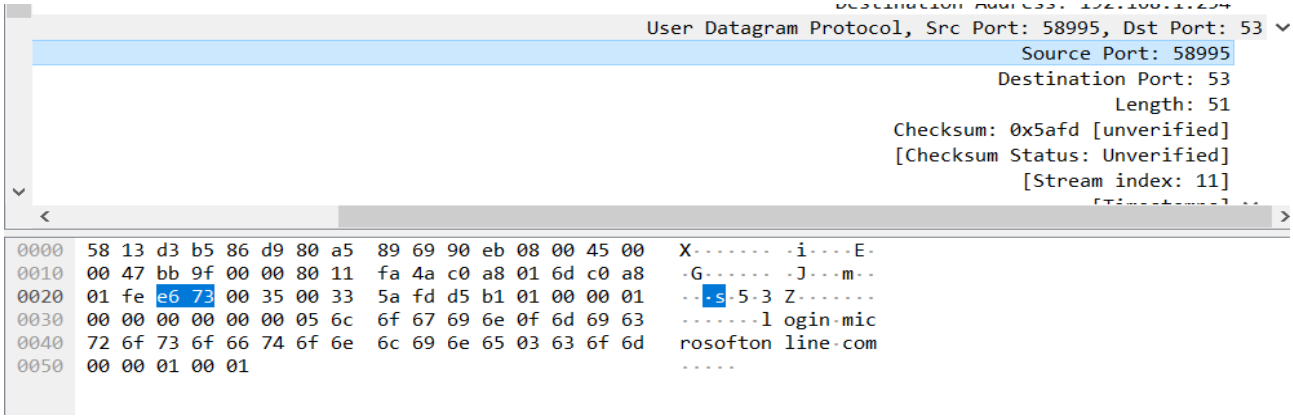
```
0000  58 13 d3 b5 86 d9 80 a5  89 69 90 eb 08 00 45 00   X------- -i----E-
0010  00 47 bb 9f 00 00 80 11  fa 4a c0 a8 01 6d c0 a8   -G------ -J---m--
0020  01 fe e6 73 00 35 00 33  5a fd d5 b1 01 00 00 01   ---s-5-3 Z-------
0030  00 00 00 00 00 00 05 6c  6f 67 69 6e 0f 6d 69 63   -------l ogin-mic
0040  72 6f 73 6f 66 74 6f 6e  6c 69 6e 65 03 63 6f 6d   rosofton line-com
0050  00 00 01 00 01                                    -----
```

2- This part displays the packet's destination IP address, letting you know where it is being sent.
The target IP address in this instance is 192.168.1.254, a private IP address that is frequently used as the default gateway in local network contexts.



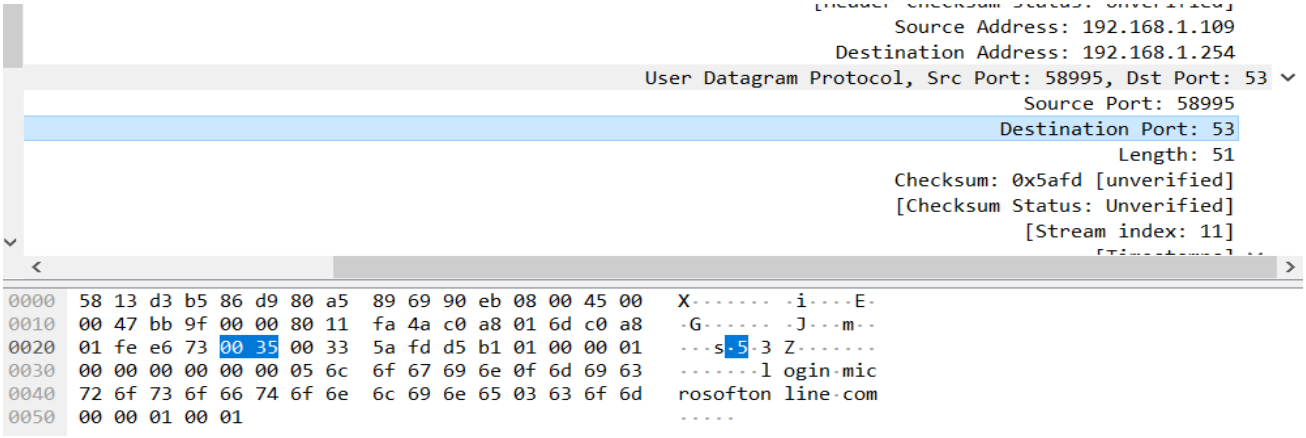
3- Port of source: 58995

This element indicates the packet's source port number, designating the port from which the data in the packet is coming.
The source port in this instance is 58995.



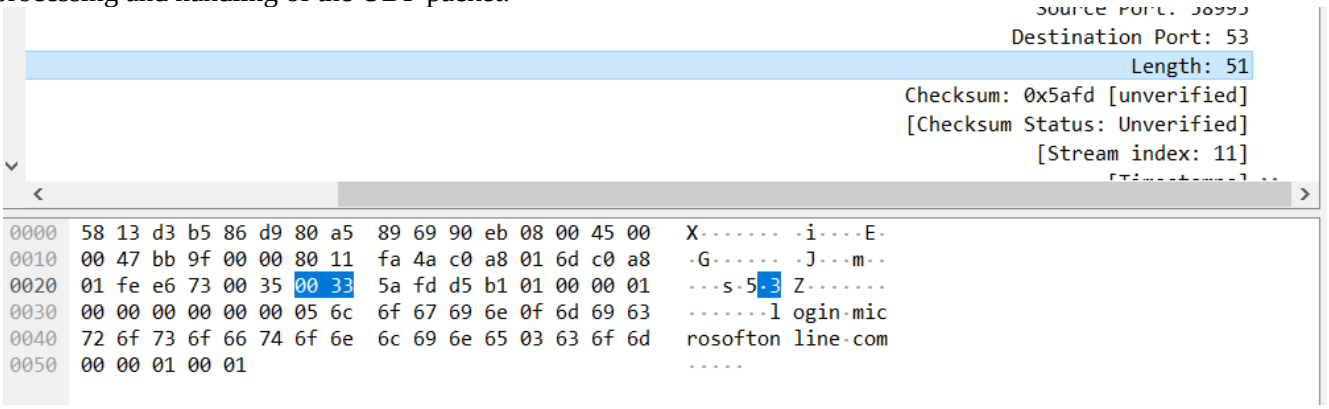
4- Port of Destination: 53

The data being sent in the packet is represented by this field, which is the packet's destination port number. Commonly known as the DNS (Domain Name System) service, port 53 is used to translate domain names into IP addresses.



5- Length : 51

A UDP (User Datagram Protocol) packet's "Length" field gives the packet's size in bytes. The UDP packet in this instance is 51 bytes long. Both the UDP header and the data payload are included in the length. Fast data transfer is made possible by the use of UDP, a lightweight, connectionless transport protocol, in programs like streaming, gaming, DNS, and SNMP. By letting devices know how much data to expect, the length value enables proper processing and handling of the UDP packet.



Sniff DHCP

Info	Length	Protocol	Destination	Source	Time	.No
DHCP Discover - Transaction ID 0xba8d6f5f	342	DHCP	255.255.255.255	0.0.0.0	0.788819	9
DHCP Offer - Transaction ID 0xba8d6f5f	328	DHCP	255.255.255.255	192.168.1.254	0.948965	13
DHCP Request - Transaction ID 0xba8d6f5f	352	DHCP	255.255.255.255	0.0.0.0	0.952068	14
DHCP ACK - Transaction ID 0xba8d6f5f	328	DHCP	255.255.255.255	192.168.1.254	1.053819	23
DHCP Release - Transaction ID 0x22f204ed	342	DHCP	192.168.1.254	192.168.1.109	17.417561	3175
DHCP Discover - Transaction ID 0xde54eead	342	DHCP	255.255.255.255	0.0.0.0	38.997505	3577
DHCP Offer - Transaction ID 0xde54eead	328	DHCP	255.255.255.255	192.168.1.254	39.043164	3579
DHCP Request - Transaction ID 0xde54eead	352	DHCP	255.255.255.255	0.0.0.0	39.044589	3580
DHCP ACK - Transaction ID 0xde54eead	328	DHCP	255.255.255.255	192.168.1.254	39.145548	3582

By using ipconfig /release & ipconfig /renew
The "ipconfig /release" command clears the current IP configuration from all of the computer's network interfaces.
The "ipconfig /renew" command asks a DHCP server to assign new IP addresses to all network interfaces on the machine.
In order to obtain a new IP configuration, you must first release the present one. This procedure can assist in resolving network difficulties or, if required, obtaining an alternative IP address.

1- Frame Number 3580

In a network packet capture, a sequential identification called the "Frame Number" is assigned to each captured packet. During network analysis, it aids in identifying and referencing certain frames. Effective network behavior troubleshooting, debugging, and documenting are made possible. The frame number is a useful tool for accurate communication and teamwork among network professionals while analyzing network packets.

```
[Time since reference or first frame: 39.044589000 seconds]
Frame Number: 3580
Frame Length: 352 bytes (2816 bits)
Capture Length: 352 bytes (2816 bits)
[Frame is marked: False]
```

2- Frame Length: 2816 bits or 352 bytes

In both bytes and bits, this field indicates the complete frame length, which takes into account all headers, data, and padding.
352 bytes (2816 bits) are the length of the capture.

```
Frame Number: 3580
Frame Length: 352 bytes (2816 bits)
Capture Length: 352 bytes (2816 bits)
```

3- Protocols shown in frame eth:ethertype:ip:udp:dhcp

This field lists the protocols that are contained in the frame's protocol stack. The Ethernet II, IP, UDP, and DHCP protocols are included in this frame.

```
Ethernet II, Src: AzureWav_69:90:eb (80:a5:89:69:90:eb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
        Address: Broadcast (ff:ff:ff:ff:ff:ff)
        LG bit: Locally administered address (this is NOT the factory default) = .... .... .... .... .1.. ....
        IG bit: Group address (multicast/broadcast) = .... .... .... .... 1... ....
    Source: AzureWav_69:90:eb (80:a5:89:69:90:eb)
        Address: AzureWav_69:90:eb (80:a5:89:69:90:eb)
        LG bit: Globally unique address (factory default) = .... .... .... .... .0.. ....
        IG bit: Individual address (unicast) = .... .... .... .... 0... ....
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    Version: 4 = .... 0100
    Header Length: 20 bytes (5) = 0101 ....
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Differentiated Services Codepoint: Default (0) = ..00 0000
        Explicit Congestion Notification: Not ECN-Capable Transport (0) = 00.. ....
    Total Length: 338
    Identification: 0xe286 (57990)
    Flags: 0x0 = .... .000
        Reserved bit: Not set = .... ...0
        Don't fragment: Not set = .... ..0.
        More fragments: Not set = .... .0..
    Fragment Offset: 0 = 0000 0000 0000 0...
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x5715 [validation disabled]
        [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 318
    Checksum: 0x802a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
        [Time since first frame: 38.255770000 seconds]
        [Time since previous frame: 0.047084000 seconds]
    UDP payload (310 bytes)
```

4- Source: 80:a5:89:69:90:eb AzureWav_69:90:eb

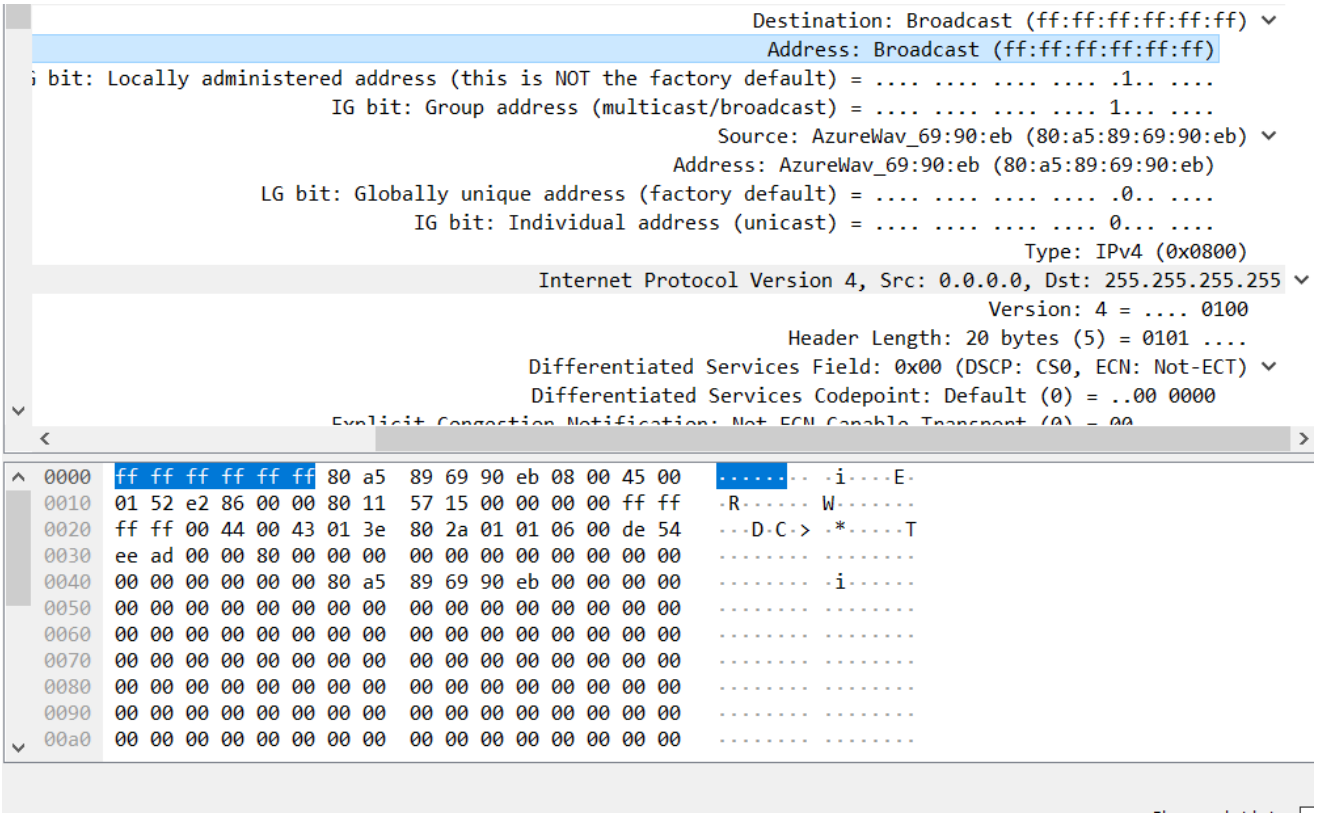
The MAC (Media Access Control) address of the device that supplied the frame is displayed in the source field. The source MAC address in this instance is AzureWav_69:90:eb.

```
    Source: AzureWav_69:90:eb (80:a5:89:69:90:eb)
        Address: AzureWav_69:90:eb (80:a5:89:69:90:eb)
        LG bit: Globally unique address (factory default) = .... .... .... .... .0.. ....
        IG bit: Individual address (unicast) = .... .... .... .... 0... ....
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    Version: 4 = .... 0100
    Header Length: 20 bytes (5) = 0101 ....
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Differentiated Services Codepoint: Default (0) = ..00 0000
        Explicit Congestion Notification: Not ECN-Capable Transport (0) = 00.. ....
    Total Length: 338
    Identification: 0xe286 (57990)
    Flags: 0x0 = .... .000
```

```
0000  ff ff ff ff ff ff 80 a5  89 69 90 eb 08 00 45 00   ·····-·· ·i·-··E·
0010  01 52 e2 86 00 00 80 11  57 15 00 00 00 00 ff ff   ·R····-- W·------
0020  ff ff 00 44 00 43 01 3e  80 2a 01 01 06 00 de 54   ···D·C·> ·*·----T
0030  ee ad 00 00 80 00 00 00  00 00 00 00 00 00 00 00   -------- --------
0040  00 00 00 00 00 00 80 a5  89 69 90 eb 00 00 00 00   -------- -i------
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   -------- --------
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   -------- --------
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   -------- --------
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   -------- --------
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   -------- --------
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   -------- --------
```

5- Broadcast (ff:ff:ff:ff:ff:ff) is the destination.

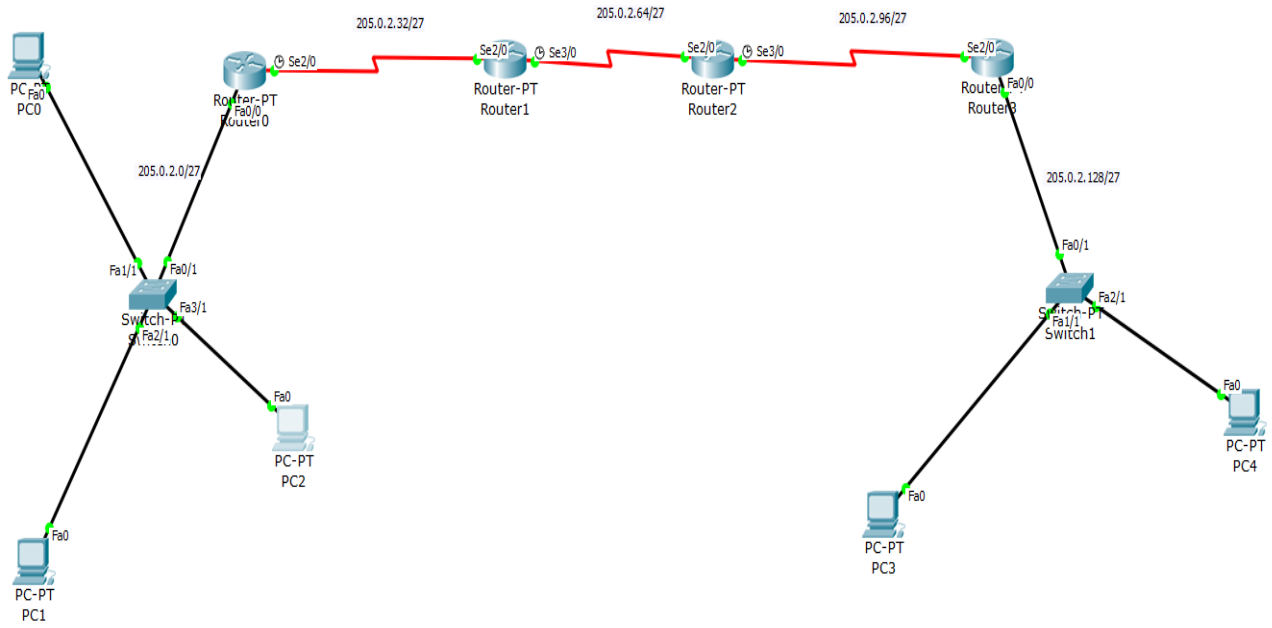
The MAC address of the intended receiver of the frame is displayed in the destination field. In this instance, the frame gets broadcast to every device on the network since the destination MAC address is also the broadcast address.
An IP address designated as a broadcast address can be used to disseminate data to every device connected to a network or subnet. A broadcast address allows for simultaneous communication with several devices since it sends a packet to every device on the network. The broadcast address in IPv4 normally corresponds to the highest address on the network or subnet, with all host bits set to 1. This addressing technique is frequently applied to tasks like DHCP requests, in which a client broadcasts a request to a DHCP server to get details about the network settings. To prevent superfluous traffic from traveling outside the local network, routers block or reject broadcast packets, thus broadcast addresses cannot be routed across multiple networks.



Part b:

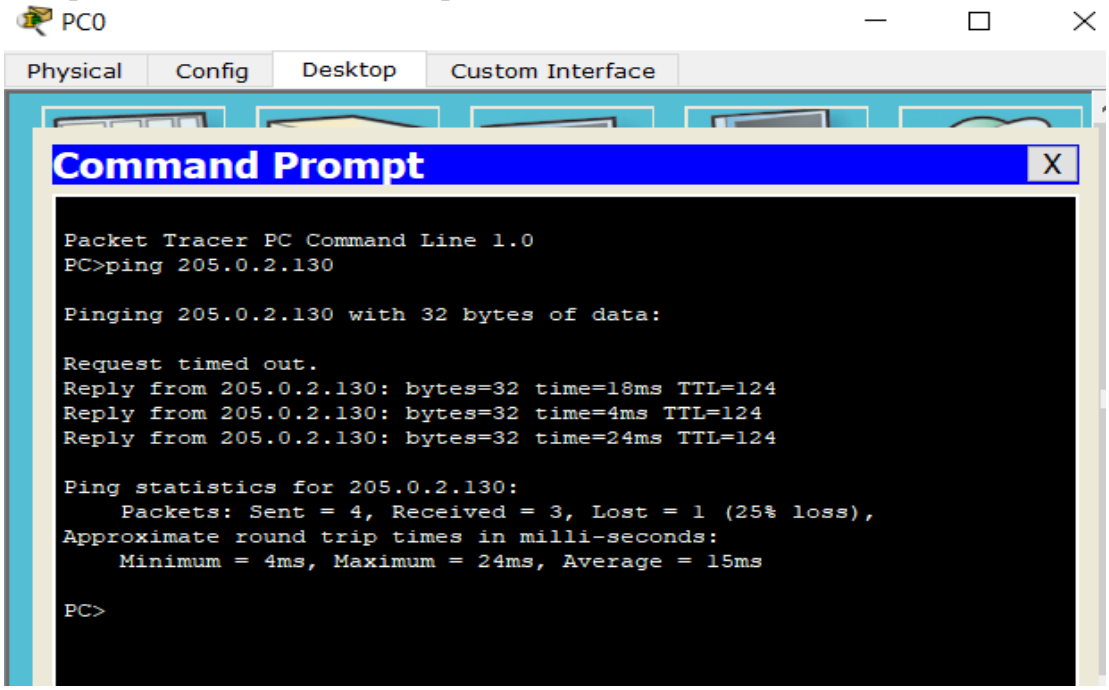
205.0.2.0/24 from this subnet the number of host equal (2^8)-2 = 254 host, from this we can maximum have 4 subnets so to have 5 subnets take 3 bits from host

205.0.2.00000000 -----> 205.0.2.0/27 this is first subnet with subnet mask 255.255.255.224.
205.0.2.00100000 -----> 205.0.2.32/27 this is second subnet with subnet mask 255.255.255.224.
205.0.2.01000000 -----> 205.0.2.64/27 this is third subnet with subnet mask 255.255.255.224.
205.0.2.01100000 -----> 205.0.2.96/27 this is fourth subnet with subnet mask 255.255.255.224.
205.0.2.10000000 -----> 205.0.2.128/27 this is fifth subnet with subnet mask 255.255.255.224.

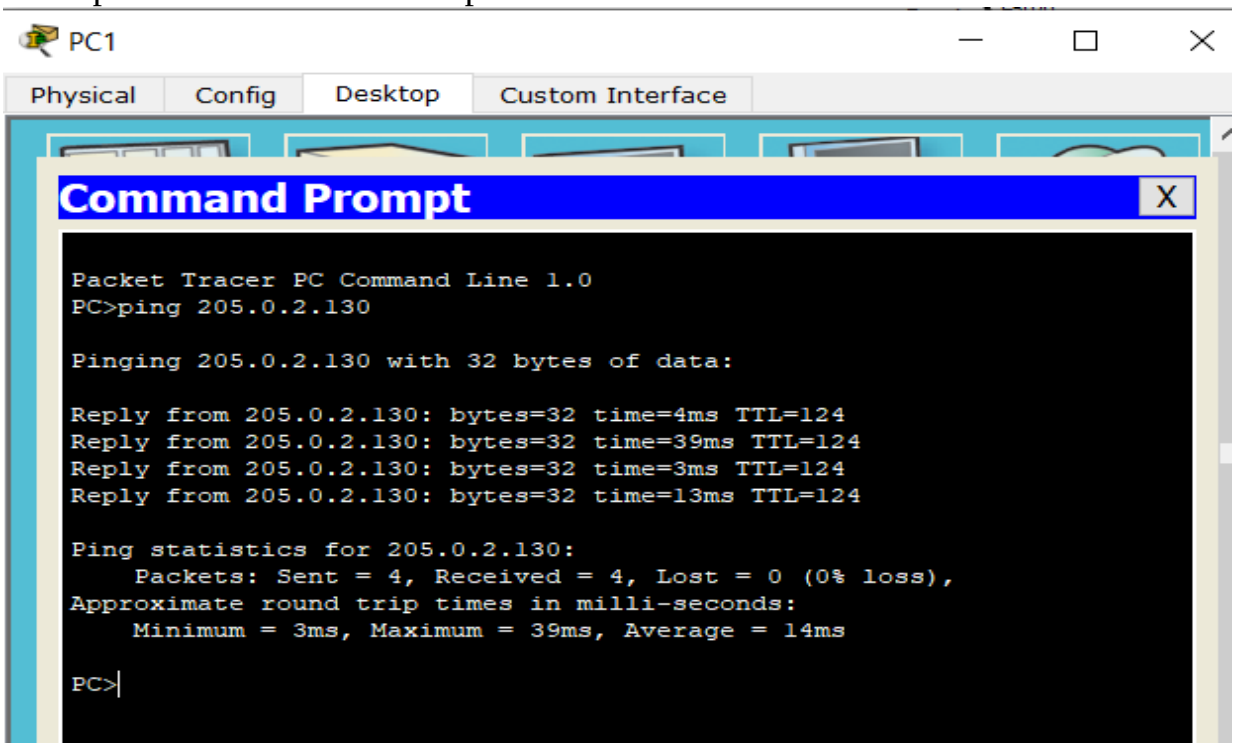


Using ping command to show reachability from one host to another host.

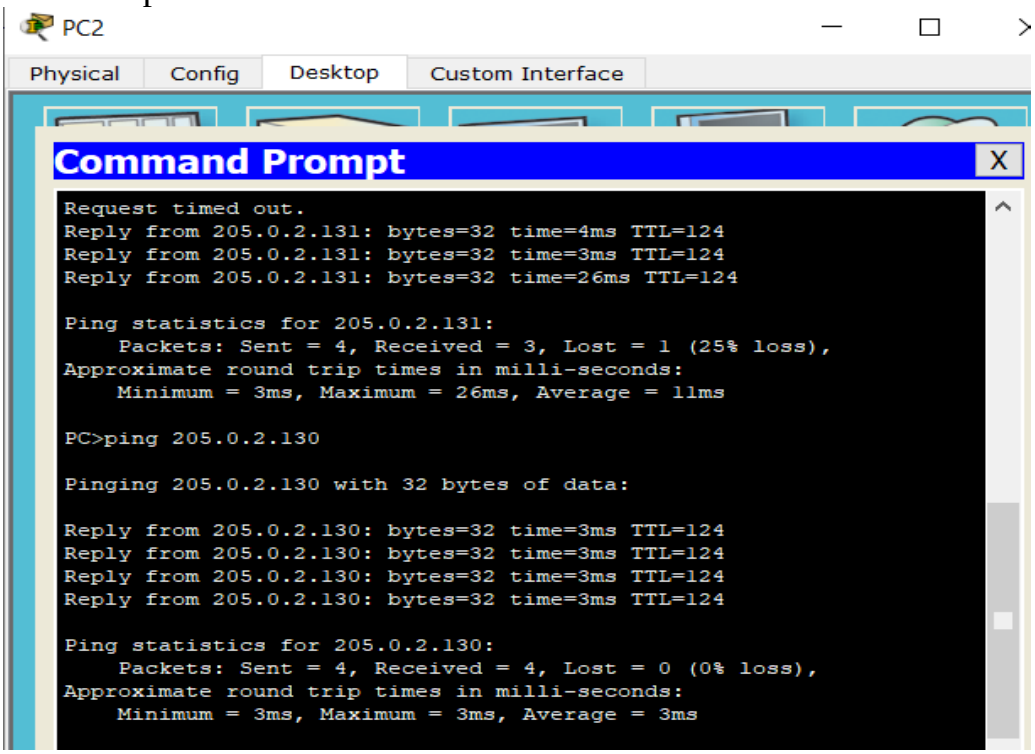
- From pc0 check connection to pc4



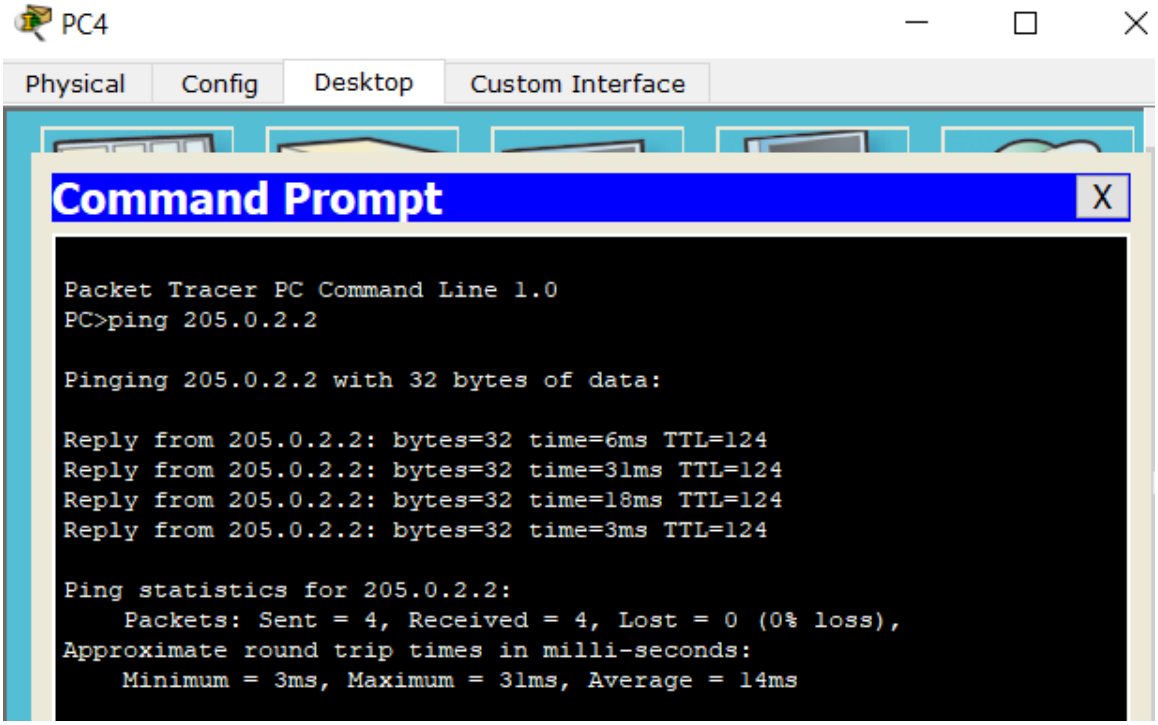
- From pc1 check connection to pc4



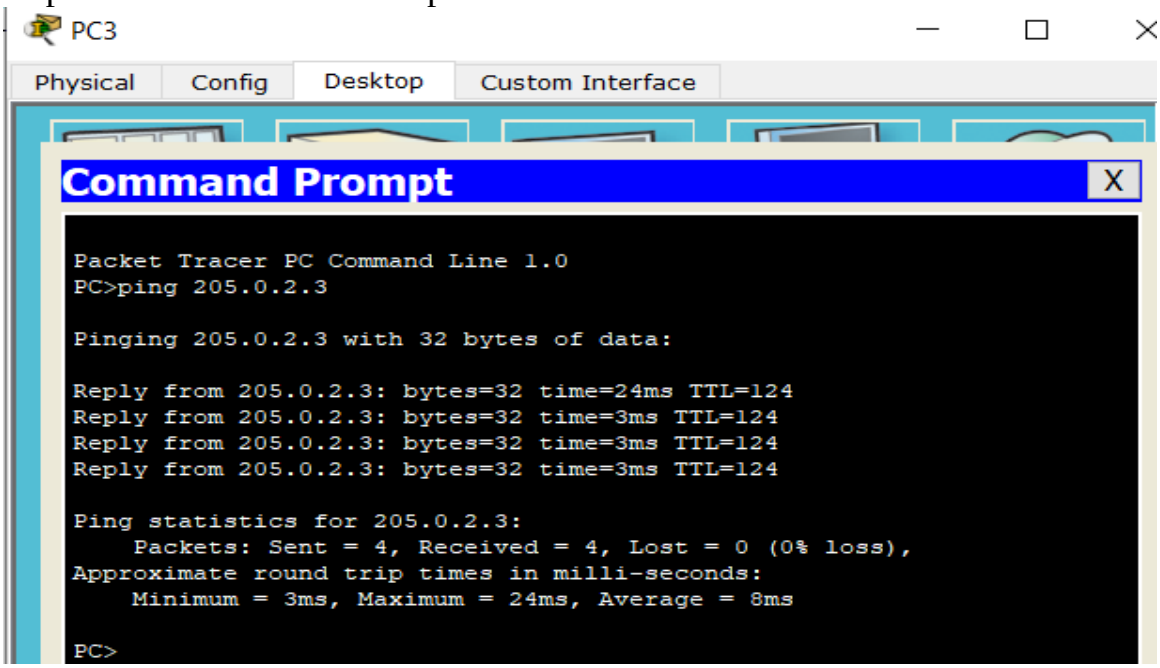
- From pc2 check pc4



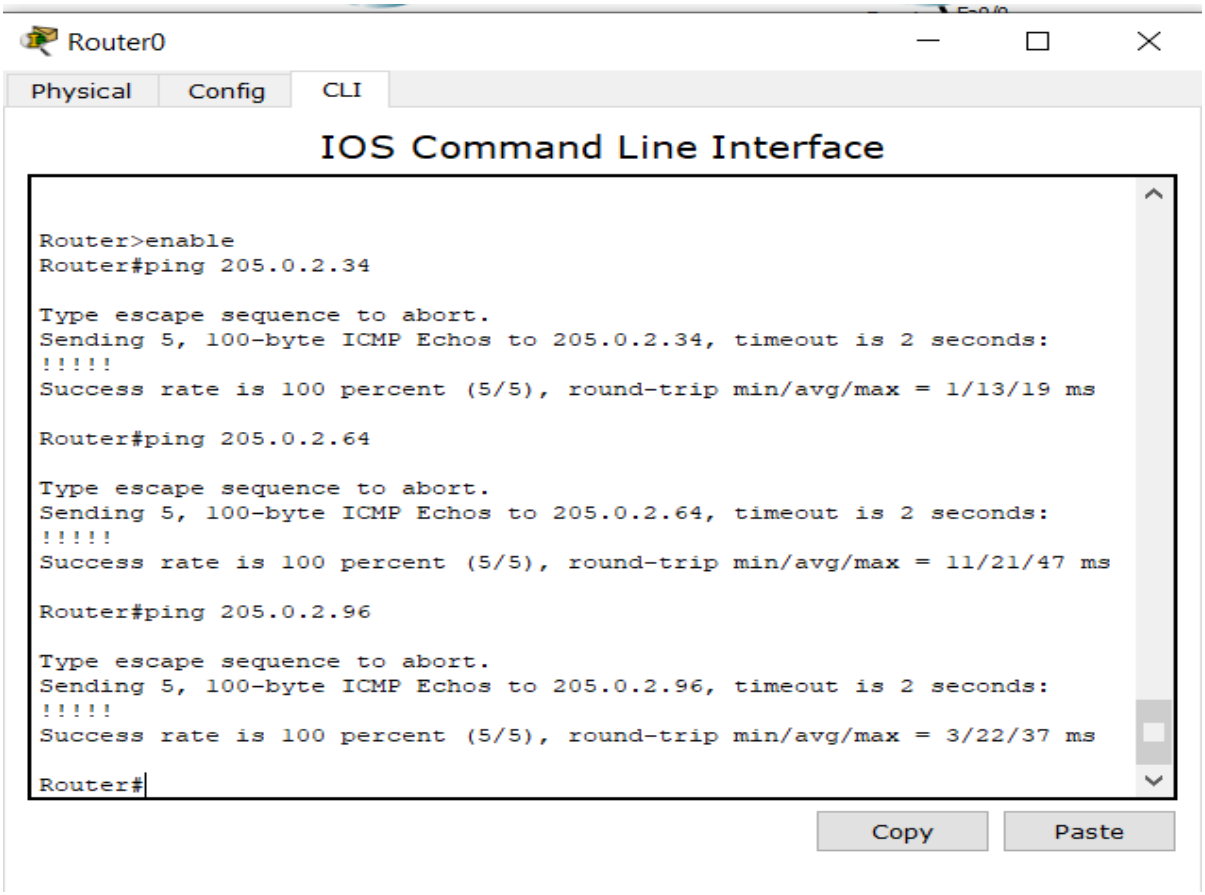
- From pc4 check connection to pc0



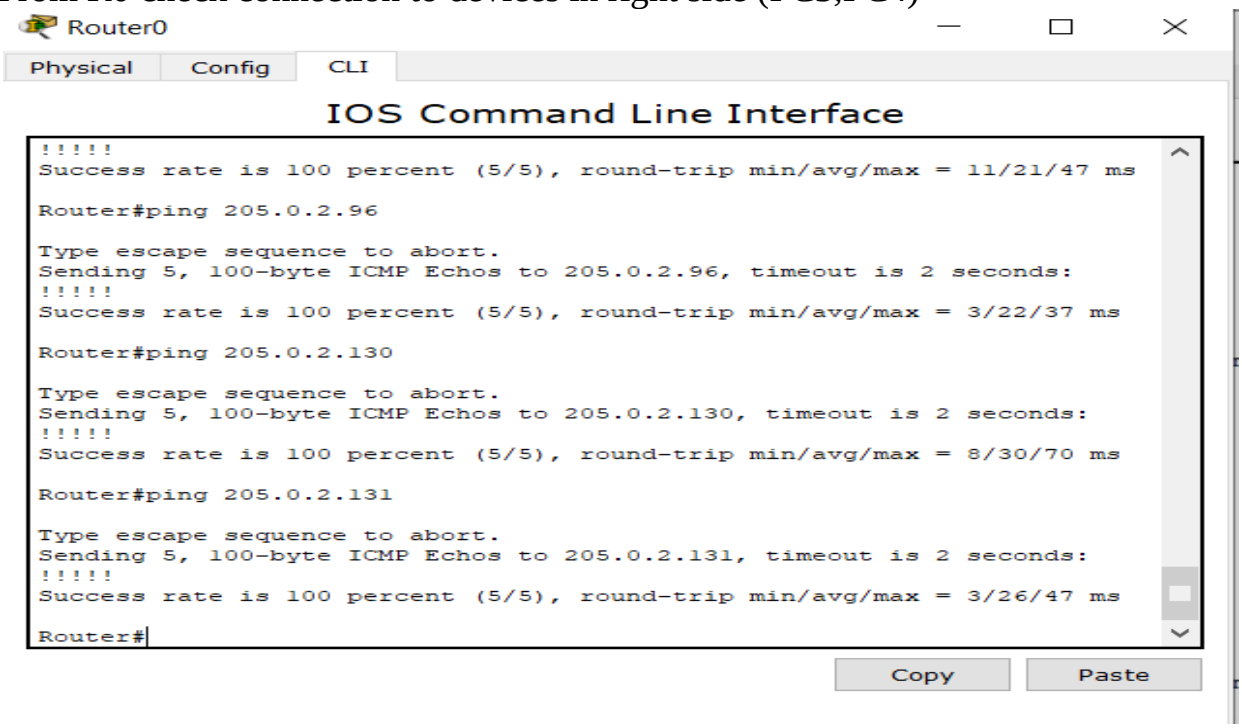
- From pc3 check connection to pc1



- From R0 check connection to all other routers



- From R0 check connection to devices in right side (PC3,PC4)



- Check by router 1 connect to each other routers and other pc we have

Router1

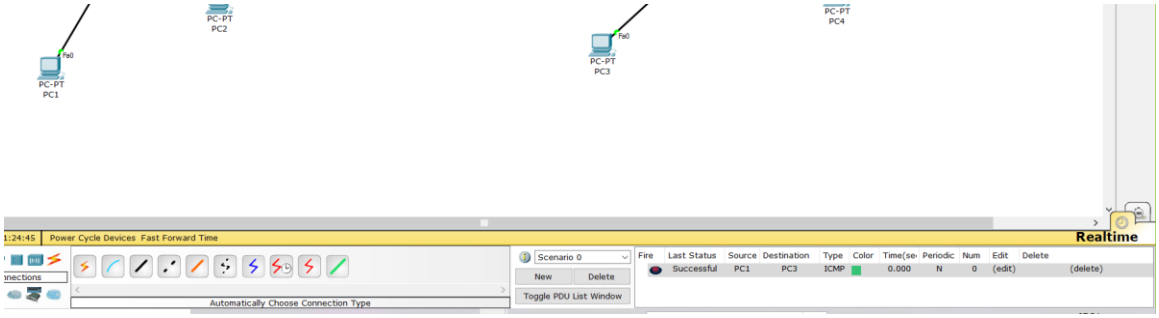
Physical | Config | CLI

```
Router>ENABLE
Router#ping
Protocol [ip]: 205.0.2.0
% Unknown protocol - "205.0.2.0", type "ping ?" for help

Router#ping 205.0.2.0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.0, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/13/22 ms

Router#ping 205.0.2.32

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.32, timeout is 2 seconds:

Reply to request 0 from 205.0.2.33, 2 ms
Reply to request 1 from 205.0.2.33, 10 ms
Reply to request 2 from 205.0.2.33, 6 ms
Reply to request 3 from 205.0.2.33, 19 ms
Reply to request 4 from 205.0.2.33, 21 ms

Router#ping 205.0.2.64

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.64, timeout is 2 seconds:

Reply to request 0 from 205.0.2.70, 19 ms
Reply to request 1 from 205.0.2.70, 10 ms
Reply to request 2 from 205.0.2.70, 12 ms
Reply to request 3 from 205.0.2.70, 1 ms
Reply to request 4 from 205.0.2.70, 7 ms

Router#ping 205.0.2.96

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.96, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/18/37 ms

Router#ping 205.0.2.128

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.128, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 14/20/29 ms

Router#ping 205.0.2.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.130, timeout is 2 seconds:
!!!!!
```

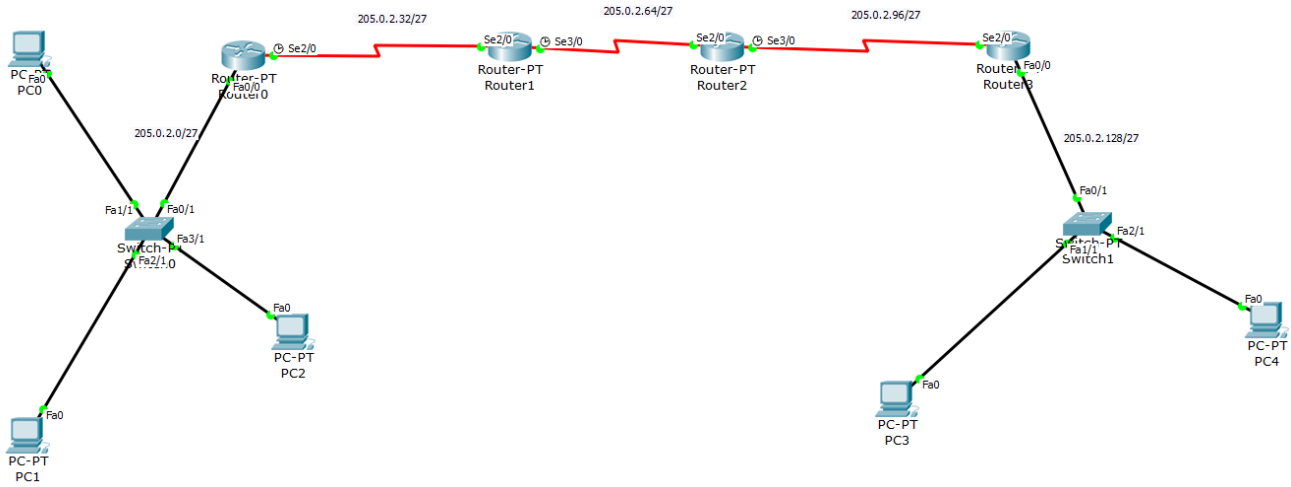
Router1

Physical | Config | CLI

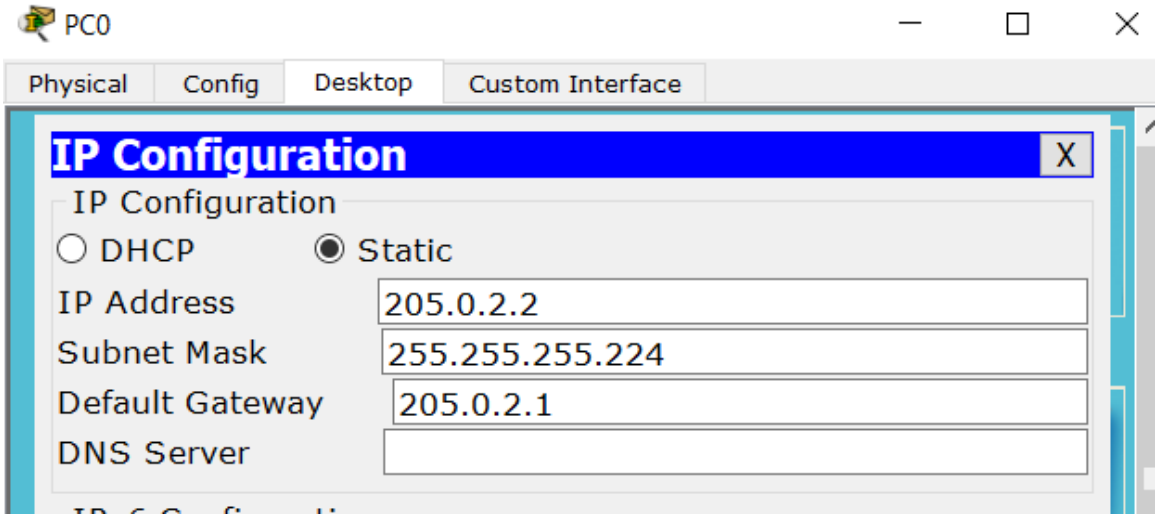
```
Reply to request 2 from 205.0.2.70, 12 ms
Reply to request 3 from 205.0.2.70, 1 ms
Reply to request 4 from 205.0.2.70, 7 ms

Router#ping 205.0.2.96

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.96, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/18/37 ms

Router#ping 205.0.2.128

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.128, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 14/20/29 ms

Router#ping 205.0.2.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.130, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/20/31 ms

Router#ping 205.0.2.131

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.131, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/14/25 ms

Router#ping 205.0.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/12 ms

Router#ping 205.0.2.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/12 ms

Router#ping 205.0.2.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.0.2.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/18 ms

Router#
```

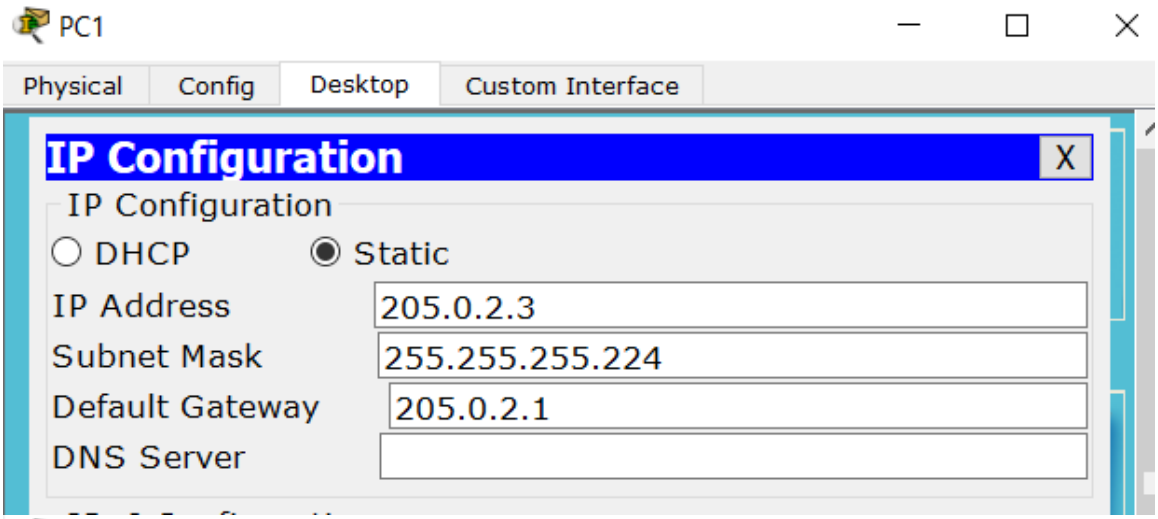


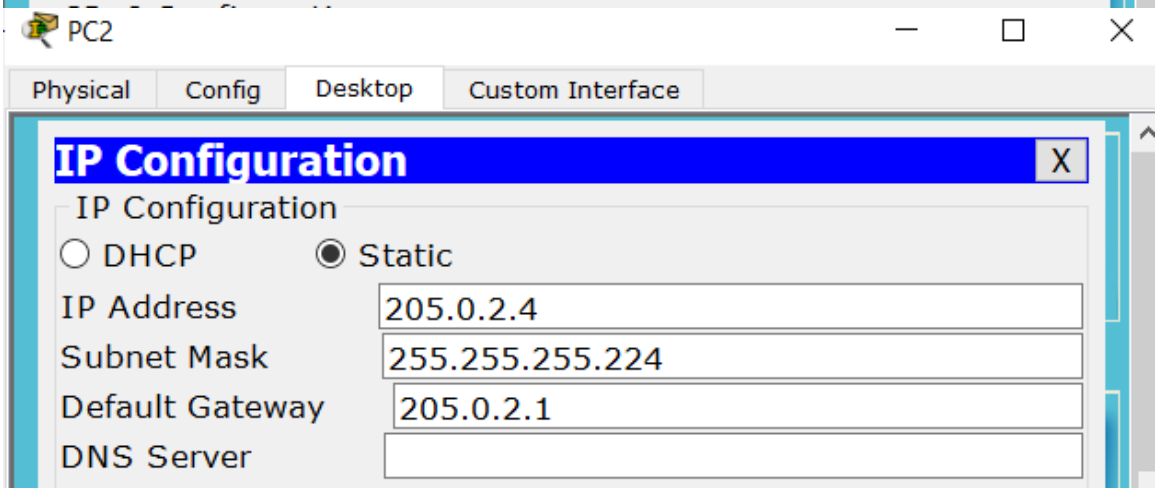
Successful transmit between 2 devices in different subnet.
All the above samples are connected successfully whatever if connection from pc to pc or from pc to router and vice versa.

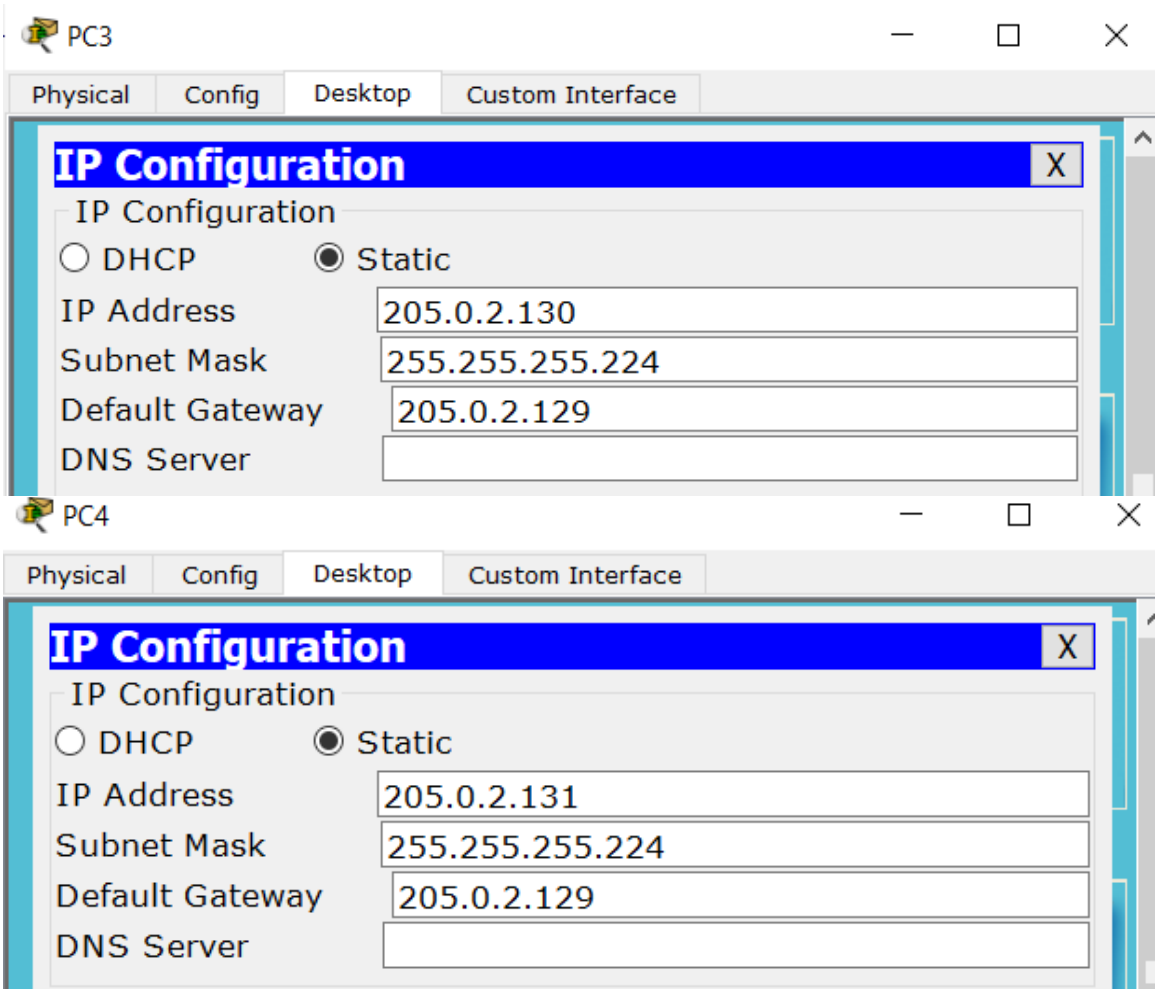


We get this network by make:
These ip’s for all pc we have:

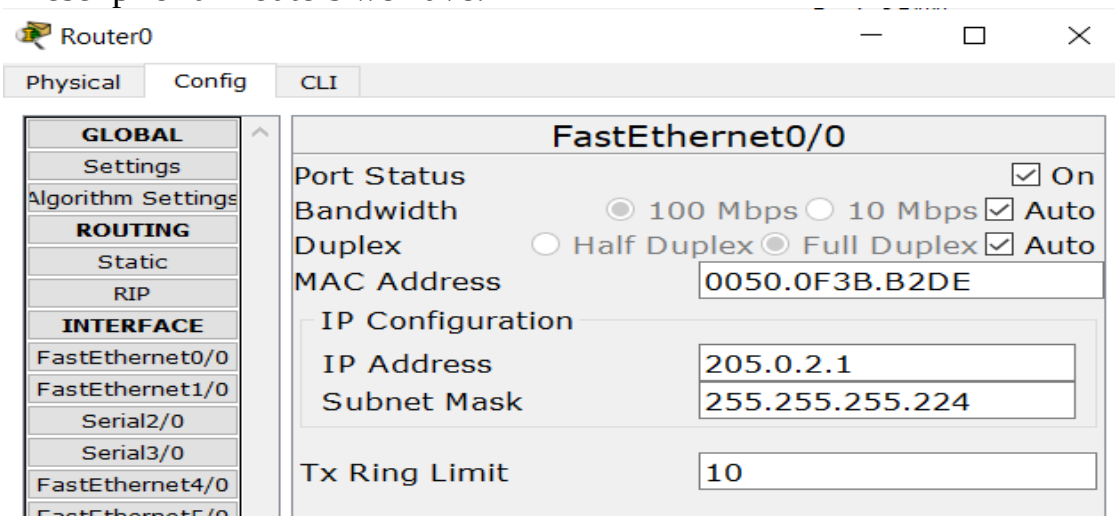

PC0
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
205.0.2.2
Subnet Mask
255.255.255.224
Default Gateway
205.0.2.1
DNS Server

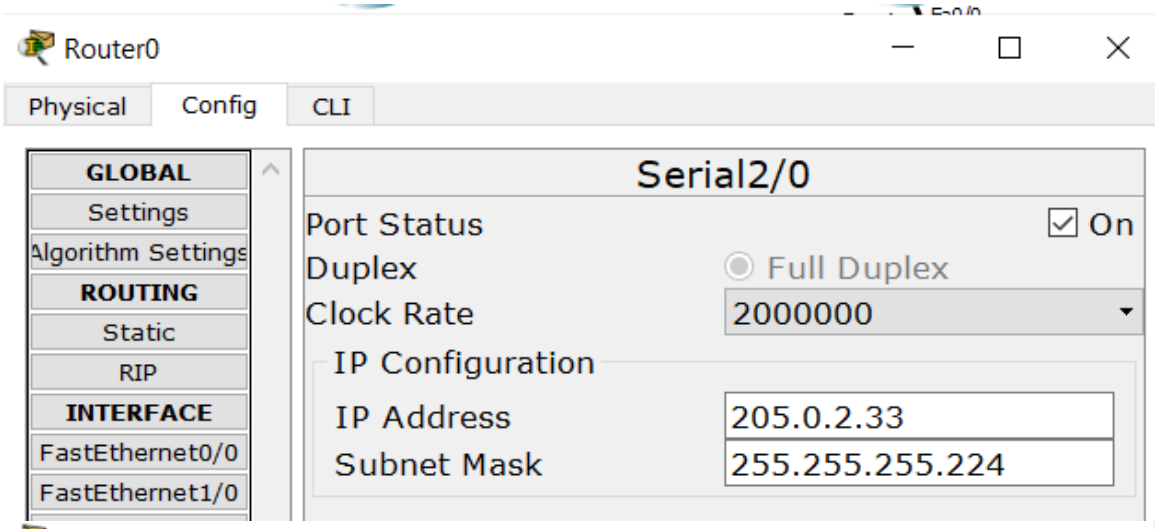

PC1
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
205.0.2.3
Subnet Mask
255.255.255.224
Default Gateway
205.0.2.1
DNS Server

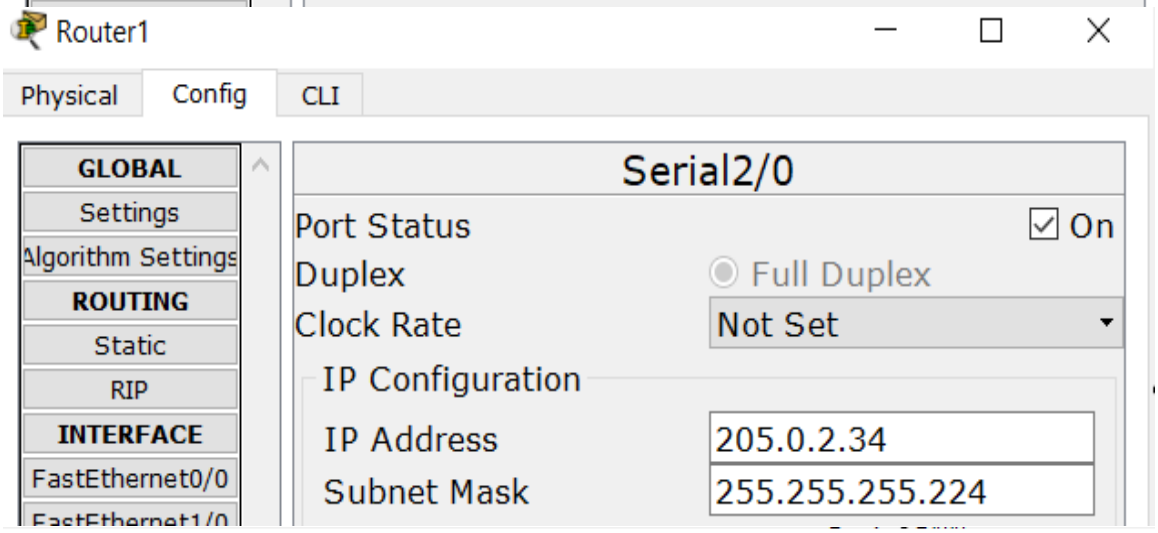

PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
205.0.2.4
Subnet Mask
255.255.255.224
Default Gateway
205.0.2.1
DNS Server

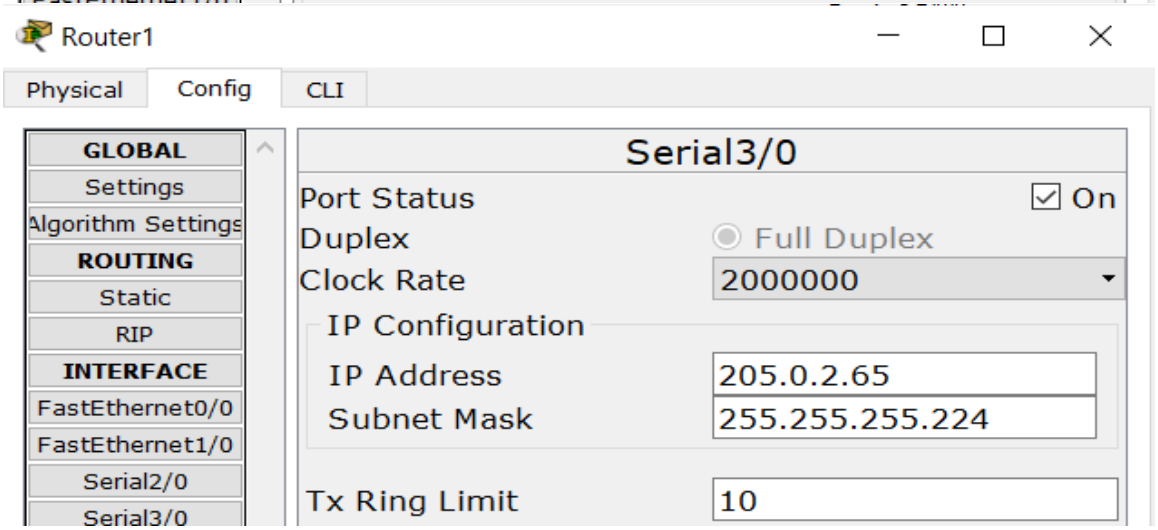


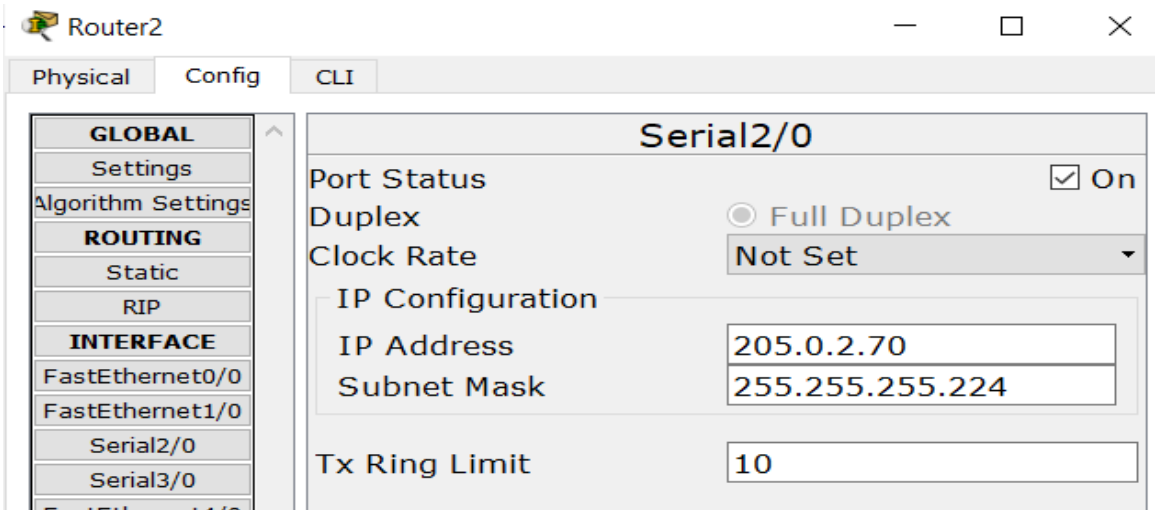
These ip for all routers we have:

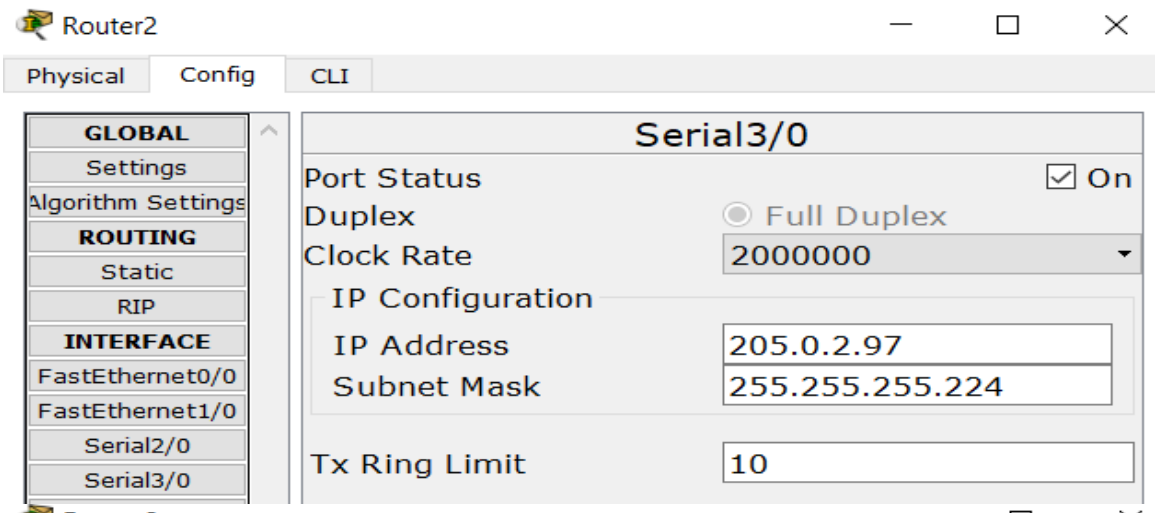


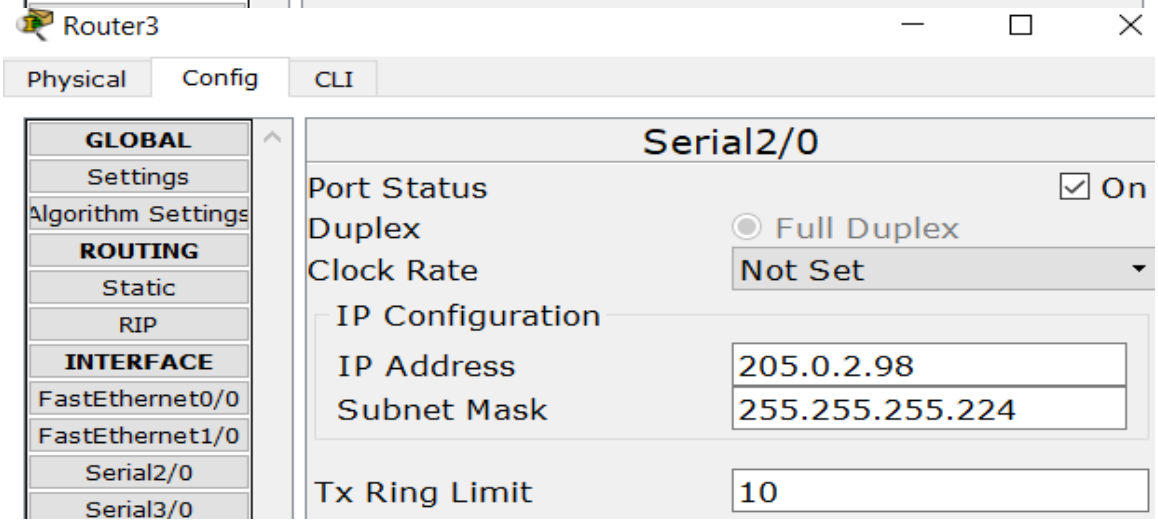

Router0
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IP Address
205.0.2.33
Subnet Mask
255.255.255.224

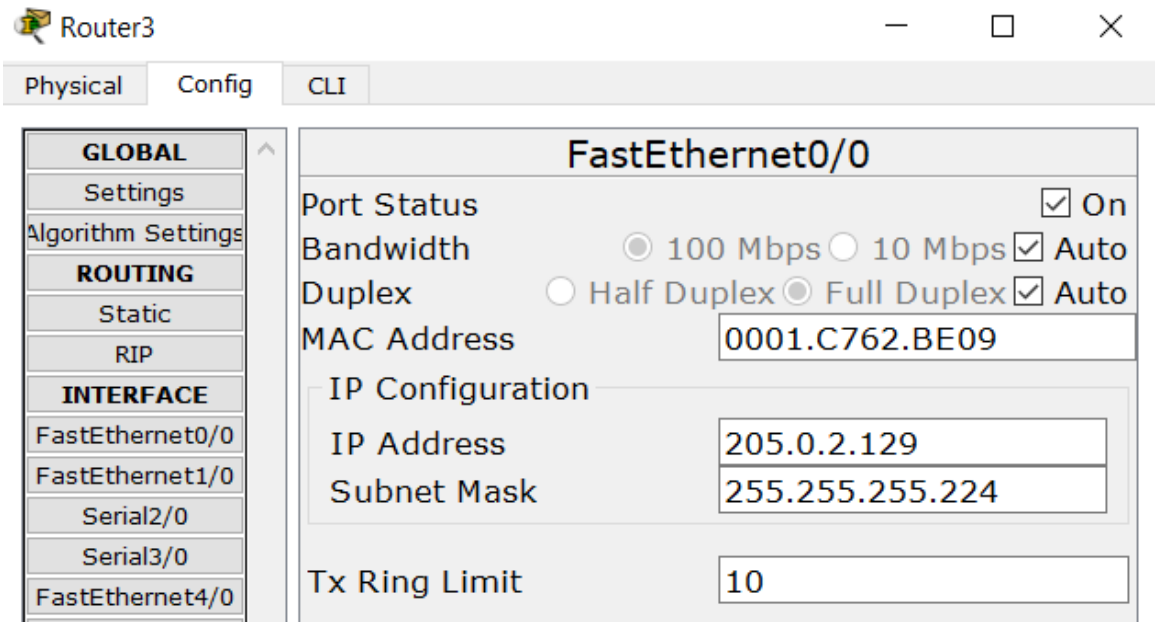

Router1
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
Not Set
IP Configuration
IP Address
205.0.2.34
Subnet Mask
255.255.255.224


Router1
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IP Address
205.0.2.65
Subnet Mask
255.255.255.224
Tx Ring Limit
10


Router2
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
Not Set
IP Configuration
IP Address
205.0.2.70
Subnet Mask
255.255.255.224
Tx Ring Limit
10


Router2
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
Serial3/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IP Address
205.0.2.97
Subnet Mask
255.255.255.224
Tx Ring Limit
10


Router3
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
Not Set
IP Configuration
IP Address
205.0.2.98
Subnet Mask
255.255.255.224
Tx Ring Limit
10


Router3
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.C762.BE09
IP Configuration
IP Address
205.0.2.129
Subnet Mask
255.255.255.224
Tx Ring Limit
10

MAKE DHCP & WEB & DNS

205.0.2.32/27 205.0.2.64/27 205.0.2.96/27

Web

Physical | Config | Services | Desktop | Custom Interface

SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP

File Name: index.html

```
<html>
<center><font size='+2' color='blue'>Cisco Packet
Tracer</font></center>
<hr>Welcome to ENCS3320. Opening doors to new opportunities.
Mind Wide Open.
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>s
```

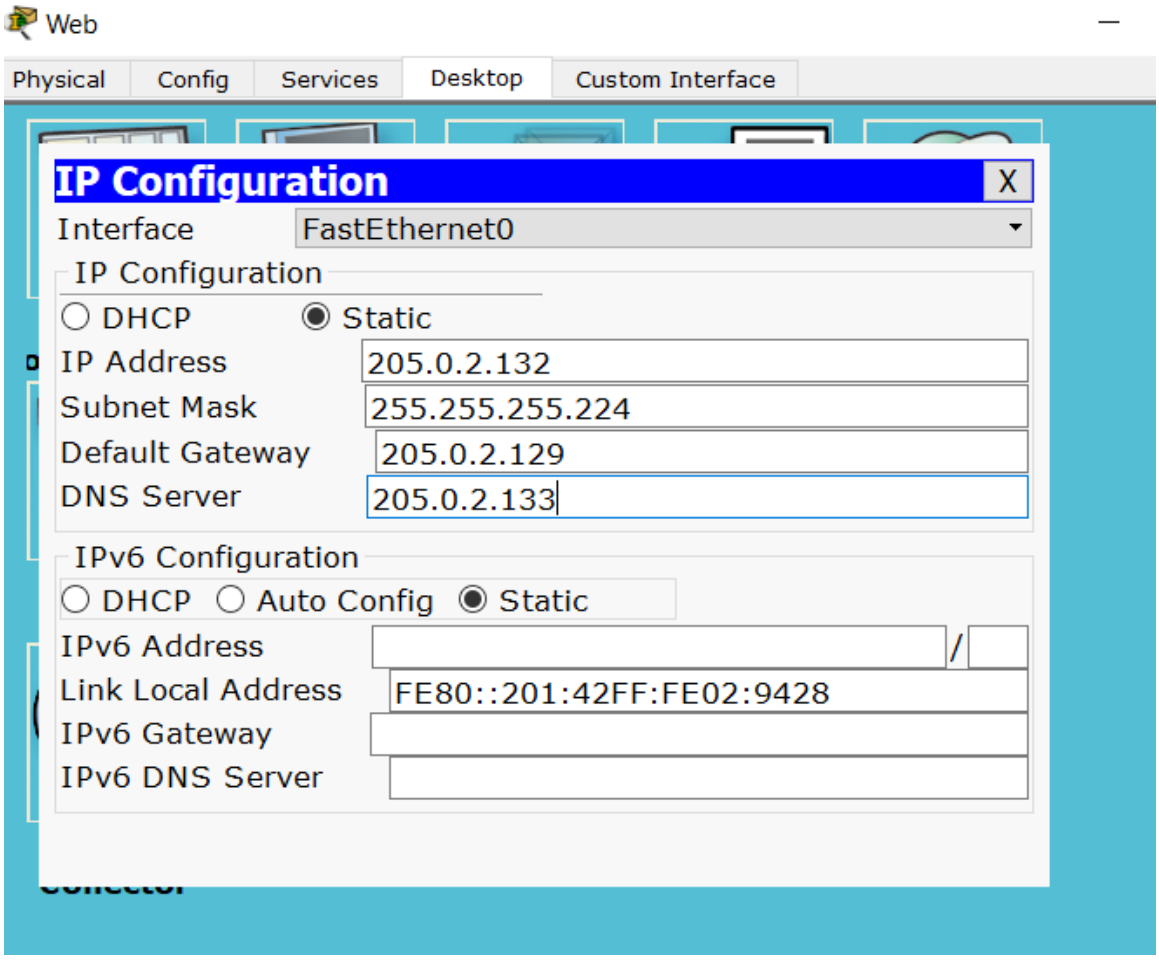
Router3

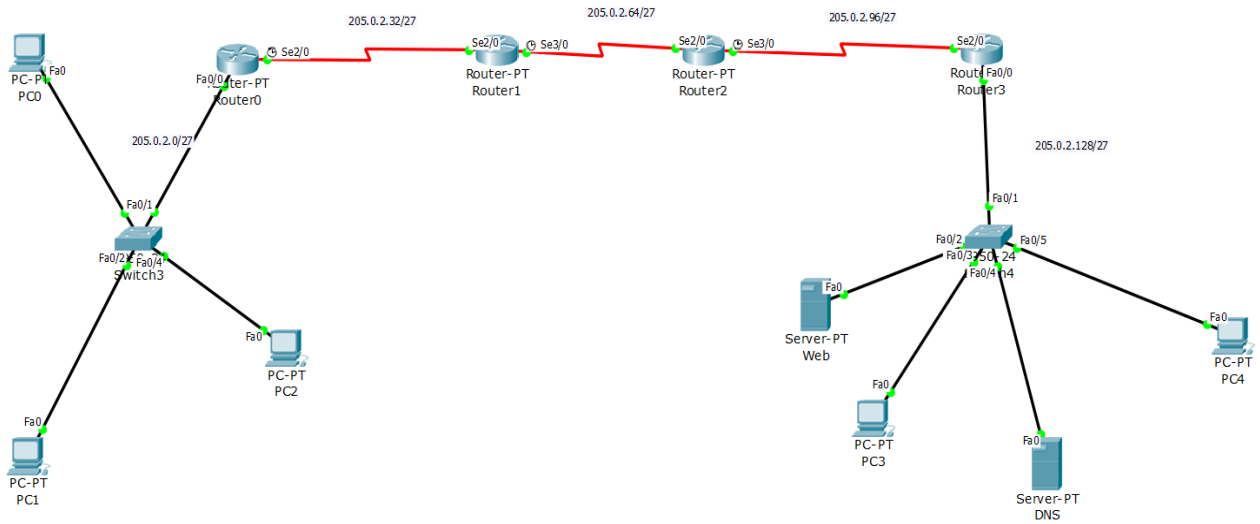
Physical | Config | CLI

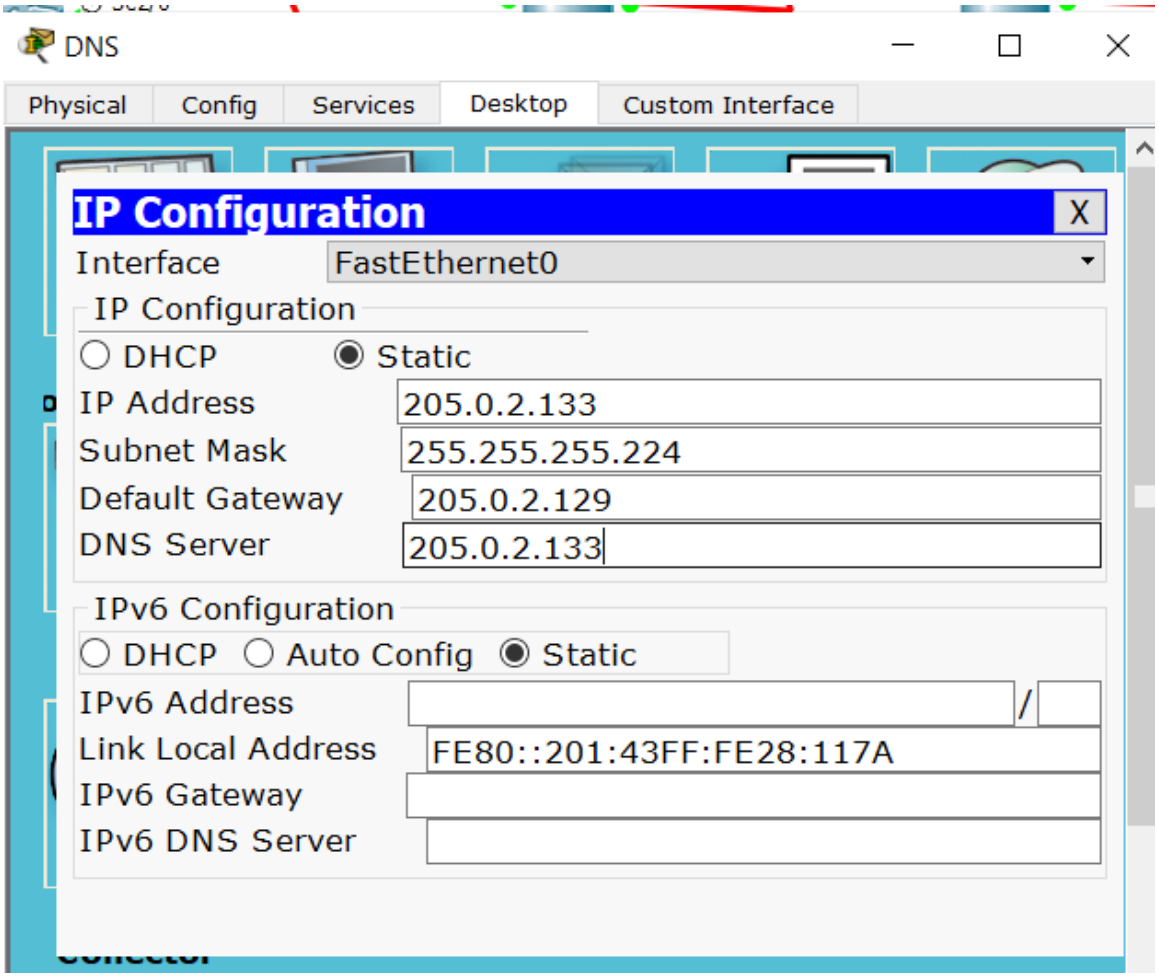
IOS Command Line Interface

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool lan1
Router(dhcp-config)#network 205.0.2.128 255.255.255.224
Router(dhcp-config)#default-router 205.0.2.129
Router(dhcp-config)#dns-server 205.0.2.133
Router(dhcp-config)#%DHCPD-4-PING_CONFLICT: DHCP address conflict:
server pinged 205.0.2.129.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged
205.0.2.130.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged
205.0.2.131.
```

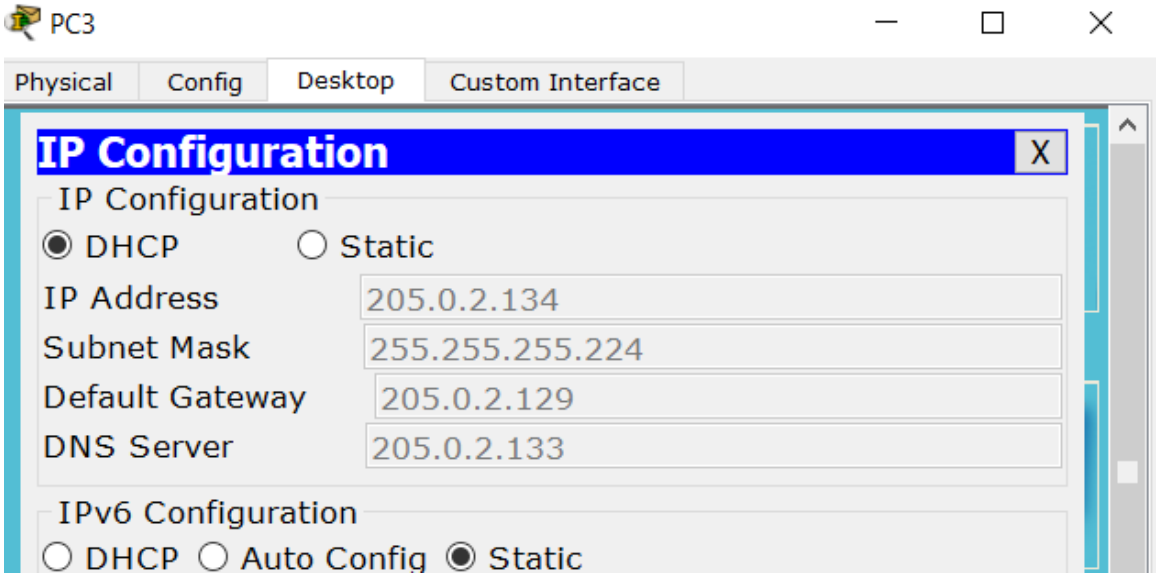
Copy Paste

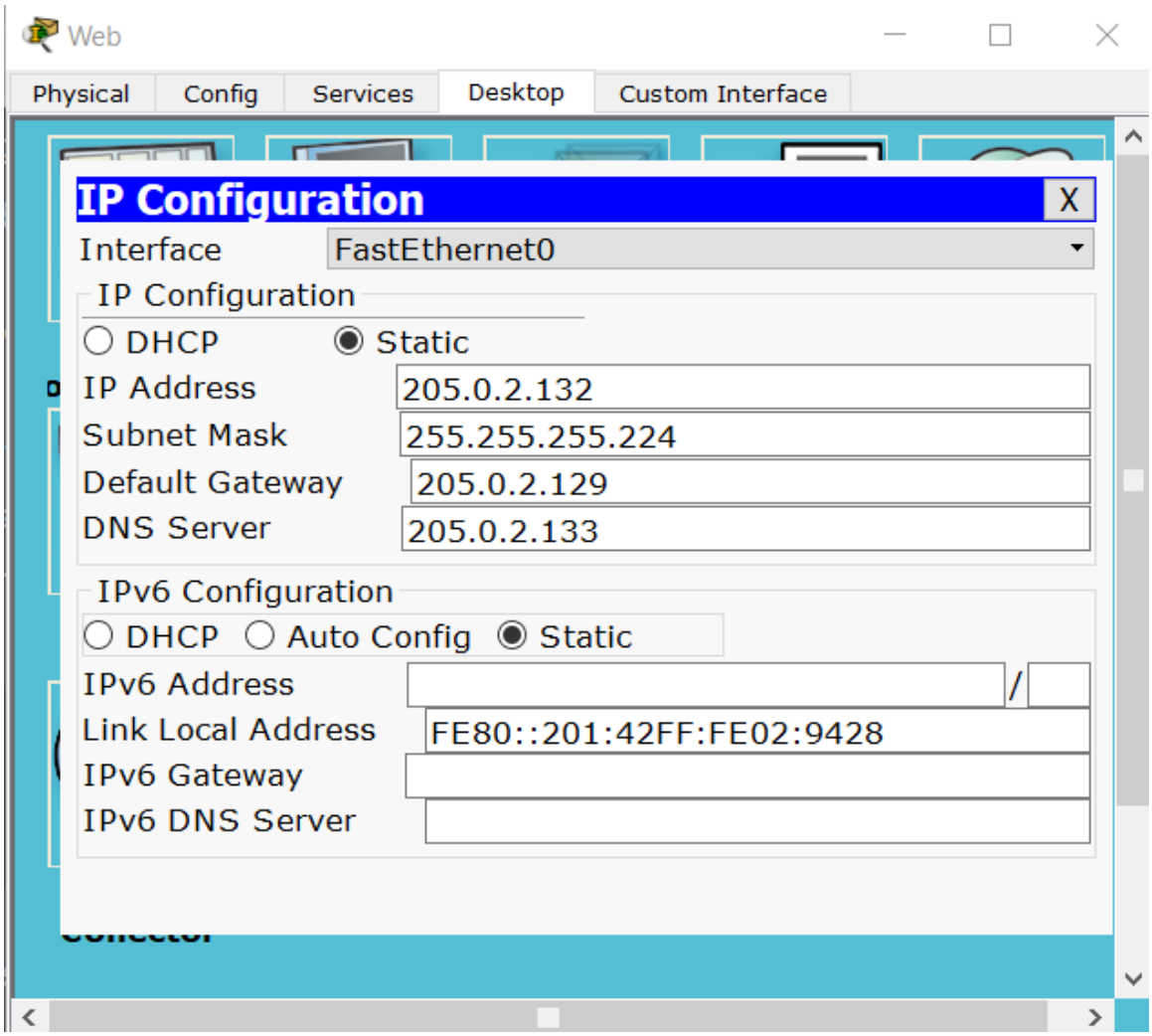

Web
Physical
Config
Services
Desktop
Custom Interface
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
205.0.2.132
Subnet Mask
255.255.255.224
Default Gateway
205.0.2.129
DNS Server
205.0.2.133
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:42FF:FE02:9428
IPv6 Gateway
IPv6 DNS Server

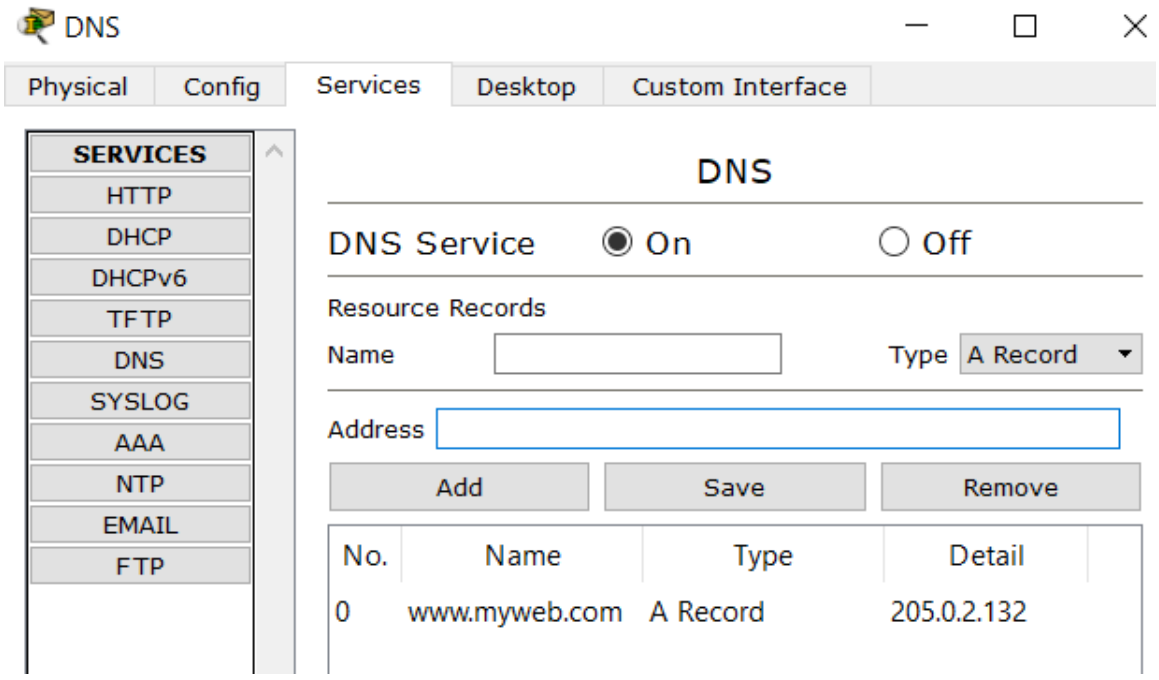

205.0.2.32/27
205.0.2.64/27
205.0.2.96/27
205.0.2.0/27
205.0.2.128/27
Router-PT Router0
Router-PT Router1
Router-PT Router2
Router-PT Router3
Switch3
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
Server-PT Web
Server-PT DNS


DNS
Physical
Config
Services
Desktop
Custom Interface
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
205.0.2.133
Subnet Mask
255.255.255.224
Default Gateway
205.0.2.129
DNS Server
205.0.2.133
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:43FF:FE28:117A
IPv6 Gateway
IPv6 DNS Server

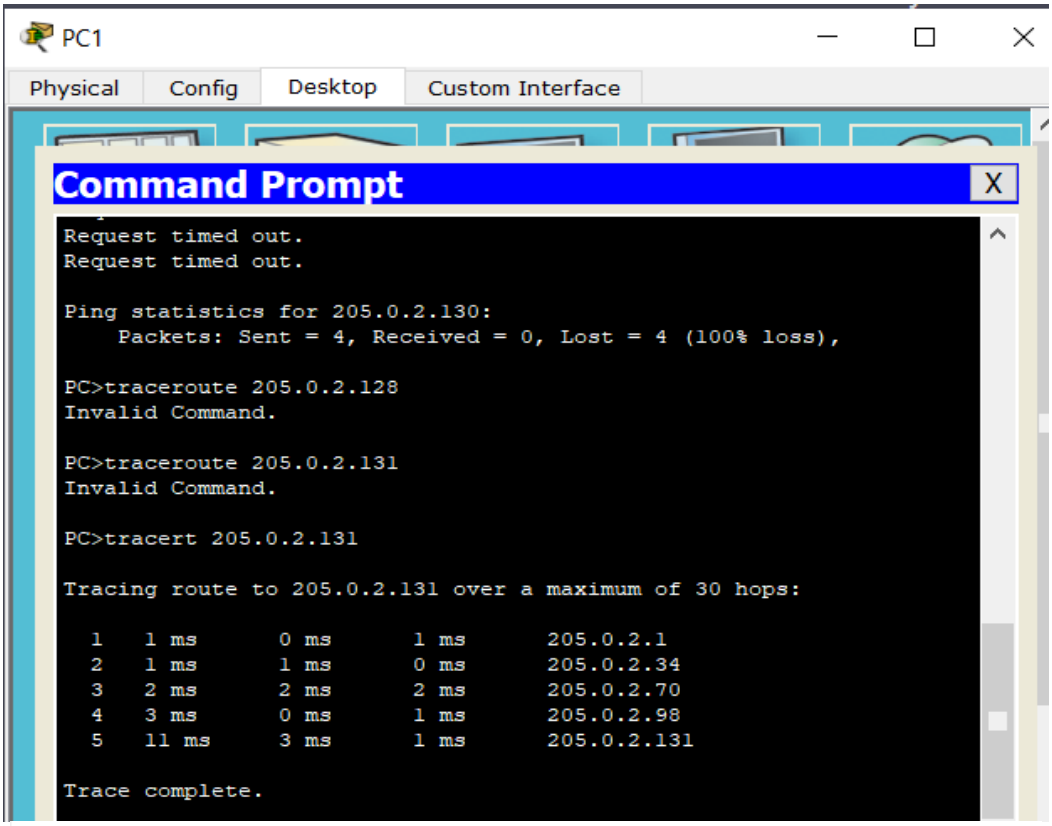

PC3
Physical
Config
Desktop
Custom Interface
Web Browser
X
<
>
URL
http://www.myweb.com
Go
Stop
Cisco Packet Tracer
Welcome to ENCS3320. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image s

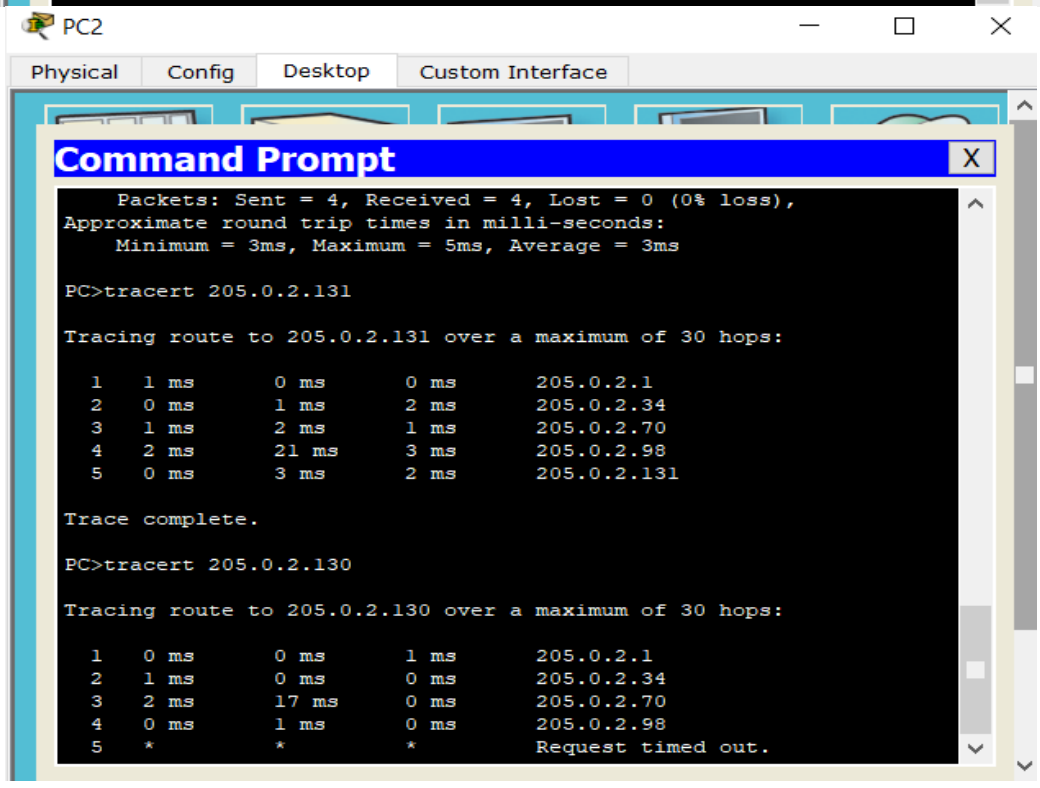

PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
205.0.2.134
Subnet Mask
255.255.255.224
Default Gateway
205.0.2.129
DNS Server
205.0.2.133
IPv6 Configuration
DHCP
Auto Config
Static

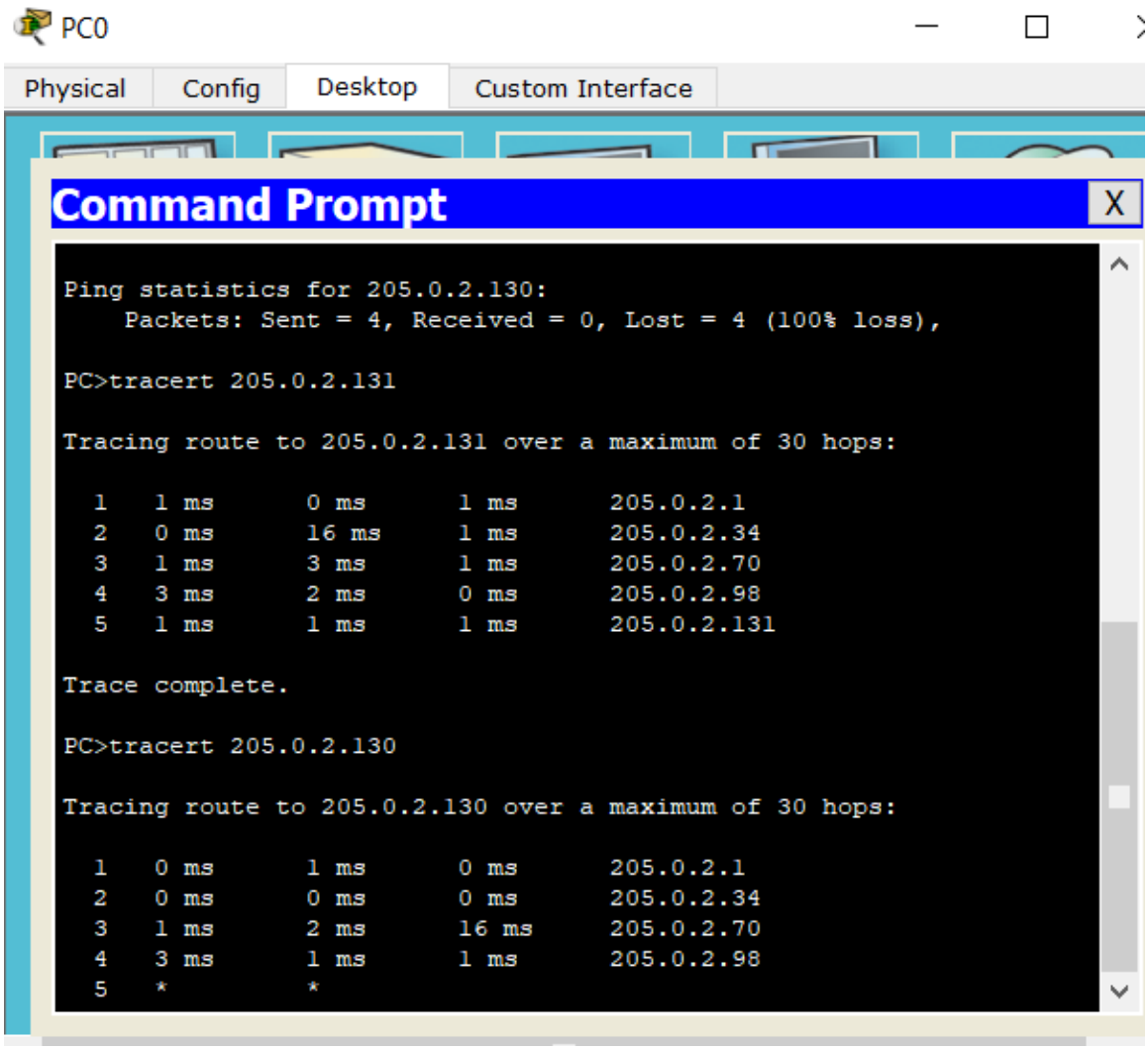

Web
Physical
Config
Services
Desktop
Custom Interface
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
205.0.2.132
Subnet Mask
255.255.255.224
Default Gateway
205.0.2.129
DNS Server
205.0.2.133
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:42FF:FE02:9428
IPv6 Gateway
IPv6 DNS Server


DNS
Physical
Config
Services
Desktop
Custom Interface
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
DNS
DNS Service
On
Off
Resource Records
Name
Type
A Record
Address
Add
Save
Remove
No.
Name
Type
Detail
0
www.myweb.com
A Record
205.0.2.132

Use tracert command to show the path a packet traversed to reach its destination from each subnet host to a remote destination.






PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Ping statistics for 205.0.2.130:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>tracert 205.0.2.131
Tracing route to 205.0.2.131 over a maximum of 30 hops:
1 1 ms 0 ms 1 ms 205.0.2.1
2 0 ms 16 ms 1 ms 205.0.2.34
3 1 ms 3 ms 1 ms 205.0.2.70
4 3 ms 2 ms 0 ms 205.0.2.98
5 1 ms 1 ms 1 ms 205.0.2.131
Trace complete.
PC>tracert 205.0.2.130
Tracing route to 205.0.2.130 over a maximum of 30 hops:
1 0 ms 1 ms 0 ms 205.0.2.1
2 0 ms 0 ms 0 ms 205.0.2.34
3 1 ms 2 ms 16 ms 205.0.2.70
4 3 ms 1 ms 1 ms 205.0.2.98
5 * *

Conclusion

In conclusion, we explored the functions of DHCP, DNS, and ICMP protocols. We learned that DHCP dynamically assigns IP addresses, DNS translates domain names to IP addresses, and ICMP facilitates network diagnostics and control. Using Wireshark, we captured and analyzed packets for each service, examining various fields that provide essential information. Additionally, we designed a network using Packet Tracer, configuring routers, switches, PCs, DHCP, a web server, and a DNS server. We also conducted ping and traceroute tests to verify host reachability and trace the packet paths. This project provided valuable hands-on experience in computer networking concepts and their practical implementation.