جامعة بيرزيت

BIRZEIT UNIVERSITY

Faculty of Engineering and Technology

Electrical and Computer Engineering

Department

Computer Network– ENCS3320

Prepared by:

Aya Dahbour	ID: 1201738	section:2
Hadeel Froukh	ID: 1201585	section:1

Instructor: Dr. Abdalkarim Awad

BIRZEIT

Date: July 2, 2023

Part 1:

1.1 Definitions:

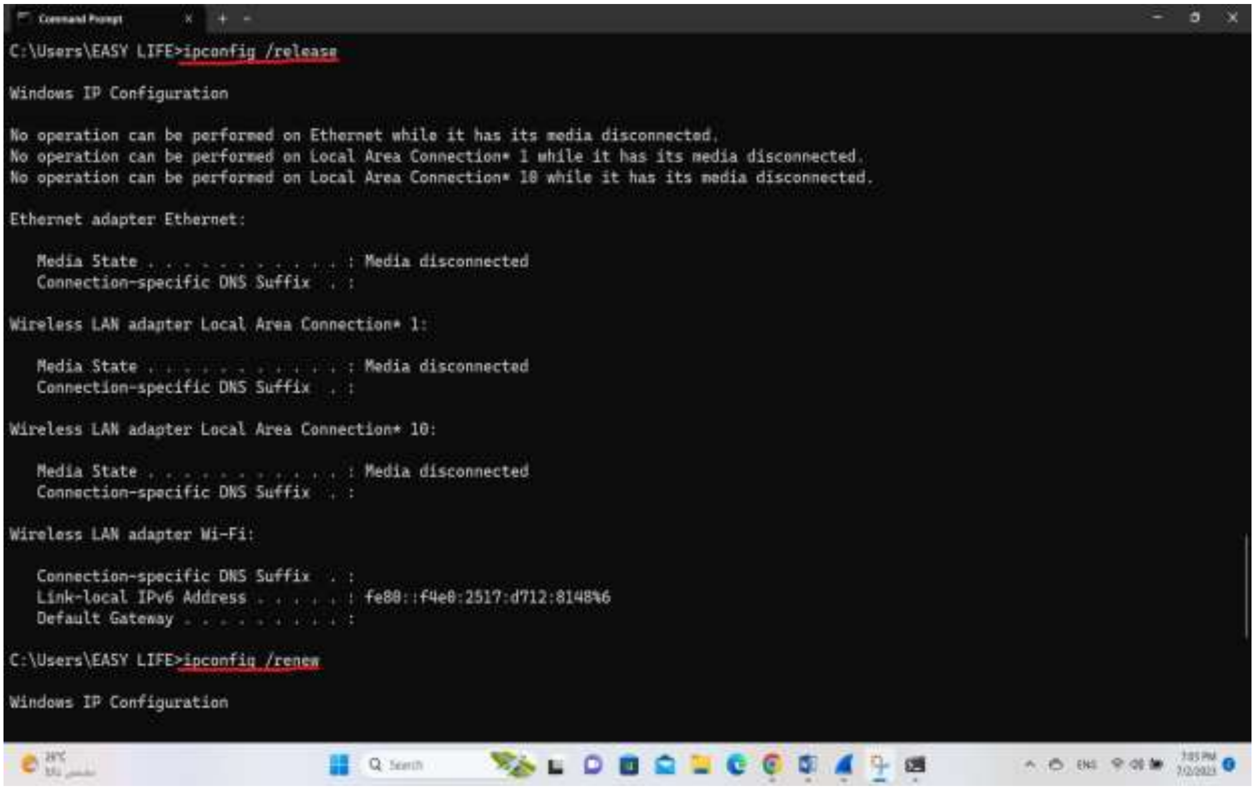
- **DHCP:** DHCP streamlines network setup by automatically assigning IP addresses and network settings.
- **DNS:** DNS translates domain names to IP addresses, allowing users to access websites without the need to recall IP addresses.
- **ICMP:** ICMP is a protocol employed for diagnosing and reporting errors in IP networks, facilitating error communication and network testing.

1.2 Wireshark Software

DHCP:

First, we open the Command Prompt then use "ipconfig /release" command, that releases the current IP address lease assigned to your computer.

Then enter the command "ipconfig /renew", this command requests a new IP address lease from the DHCP server.

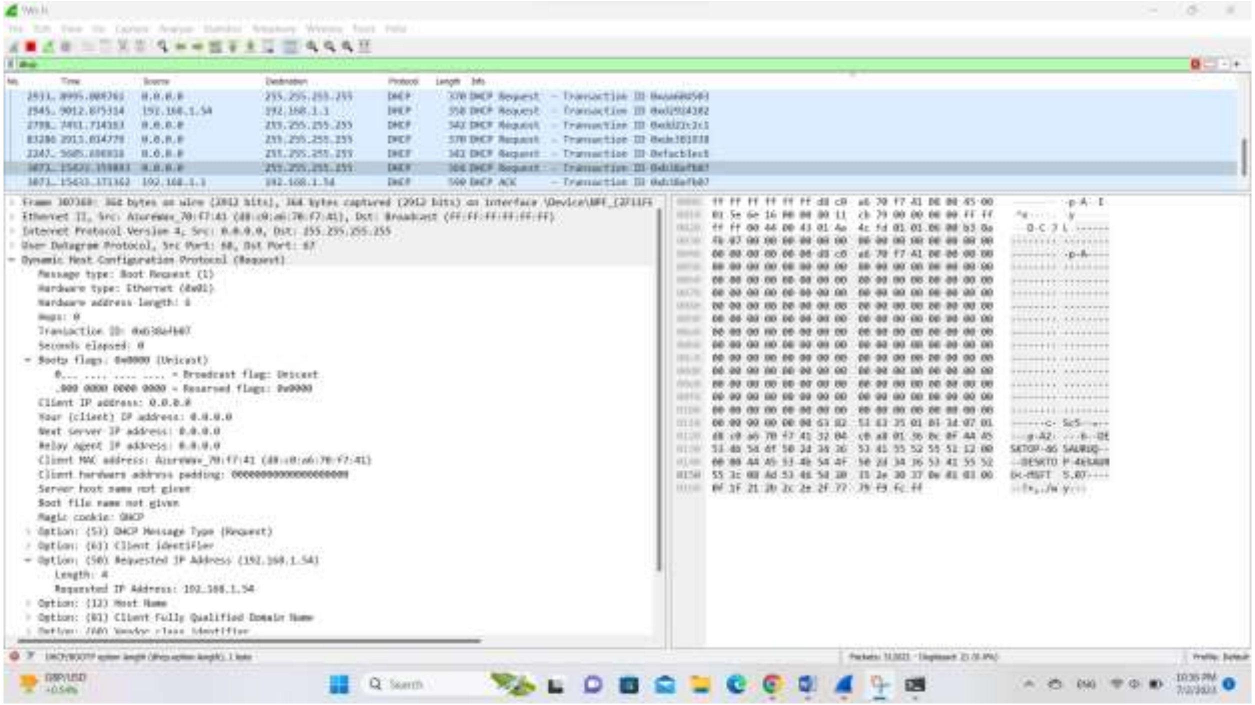


```
C:\Users\EASY LIFE>ipconfig /release

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f4e0:2517:d712:8148%6
   Default Gateway . . . . . . . . . :

C:\Users\EASY LIFE>ipconfig /renew

Windows IP Configuration
```

Figure 1:DHCP commands

Then use Wireshark to capturing packets, and apply "dhcp" filter to display only the packets relevant to DHCP protocols. The output appeared as follow:

- ***Request Packet:***



```
No.     Time              Source          Destination        Protocol  Length Info
2911…  8995.009761       0.0.0.0         255.255.255.255    DHCP       370 DHCP Request  - Transaction ID 0xa6a0d503
2945…  9012.875314       192.168.1.54    192.168.1.1        DHCP       358 DHCP Request  - Transaction ID 0xd2924382
2798…  7451.714183       0.0.0.0         255.255.255.255    DHCP       342 DHCP Request  - Transaction ID 0xb821c2c1
83280  2913.834779       0.0.0.0         255.255.255.255    DHCP       370 DHCP Request  - Transaction ID 0xde381838
2247…  5605.698818       0.0.0.0         255.255.255.255    DHCP       342 DHCP Request  - Transaction ID 0xfacb1ec8
3073…  15422.359883      0.0.0.0         255.255.255.255    DHCP       364 DHCP Request  - Transaction ID 0xd18afb07
3073…  15433.171362      192.168.1.1     192.168.1.54       DHCP       590 DHCP ACK      - Transaction ID 0xd18afb07
```

```
> Frame 307360: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface \Device\NPF_{2F11F6
> Ethernet II, Src: Azurewav_70:f7:41 (48:c0:a6:70:f7:41), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xd18afb07
    Seconds elapsed: 0
  v Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Azurewav_70:f7:41 (48:c0:a6:70:f7:41)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  v Option: (50) Requested IP Address (192.168.1.54)
      Length: 4
      Requested IP Address: 192.168.1.54
  > Option: (12) Host Name
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
```

Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
DHCP/BOOTP option length (dhcp.option.length), 1 byte
GBP/USD
+0.54%
Search

Figure 2: Wireshark screenshot of the Request packet

❖ **Fields:**

➢ Source address: 0.0.0.0
The source IP address is 0.0.0.0, indicating that the client has not yet been allocated a legitimate IP address.

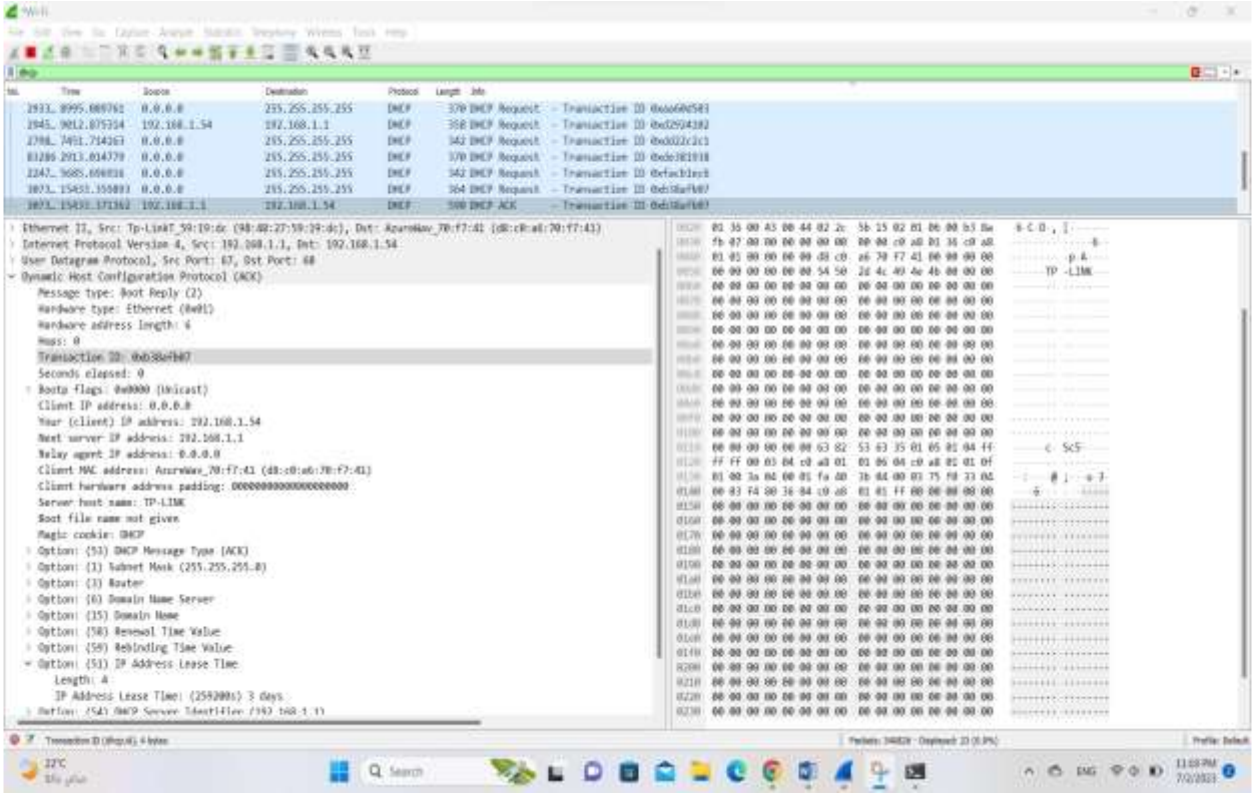
➢ Destination address: 255.255.255.255
This field contains the hardware address of the DHCP server that the request is being sent to. And here it is broadcast address for DHCP packets, reaching all devices on the local network.

➢ DHCP Message Type: Request
The packet type is specified as a Request message, signaling the client's request for the provided IP address and settings.

➢ Client IP address: 0.0.0.0
The client IP address is also 0.0.0.0, indicating that the client is still in the process of receiving an IP address through DHCP.

➢ Requested IP address: 192.168.1.54
This field specifies the IP address that the client requests to obtain from the DHCP server.

- ***Acknowledge Packet:***



```
dhcp
No.     Time            Source          Destination       Protocol  Length Info
2933... 8995.089761     0.0.0.0         255.255.255.255   DHCP      370 DHCP Request  - Transaction ID 0xaa60d503
2945... 9012.875314     192.168.1.54    192.168.1.1       DHCP      358 DHCP Request  - Transaction ID 0xd2924182
2798... 7451.714163     0.0.0.0         255.255.255.255   DHCP      342 DHCP Request  - Transaction ID 0xdd22c2c1
83286 2913.014779       0.0.0.0         255.255.255.255   DHCP      370 DHCP Request  - Transaction ID 0xde381918
2247... 5685.696016     0.0.0.0         255.255.255.255   DHCP      342 DHCP Request  - Transaction ID 0xfacb1ec8
3073... 15451.355093    0.0.0.0         255.255.255.255   DHCP      364 DHCP Request  - Transaction ID 0xb38afb07
3073... 15451.371362    192.168.1.1     192.168.1.54      DHCP      590 DHCP ACK      - Transaction ID 0xb38afb07
```

```
> Ethernet II, Src: Tp-LinkT_59:19:dc (98:48:27:59:19:dc), Dst: AzureWav_70:f7:41 (d8:c0:a6:70:f7:41)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.54
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xb38afb07
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.54
    Next server IP address: 192.168.1.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: AzureWav_70:f7:41 (d8:c0:a6:70:f7:41)
    Client hardware address padding: 00000000000000000000
    Server host name: TP-LINK
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (15) Domain Name
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  v Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (259200s) 3 days
  > Option: (54) DHCP Server Identifier (192.168.1.1)
```

Transaction ID (dhcp.id), 4 bytes

Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
22°C
Search
ENG

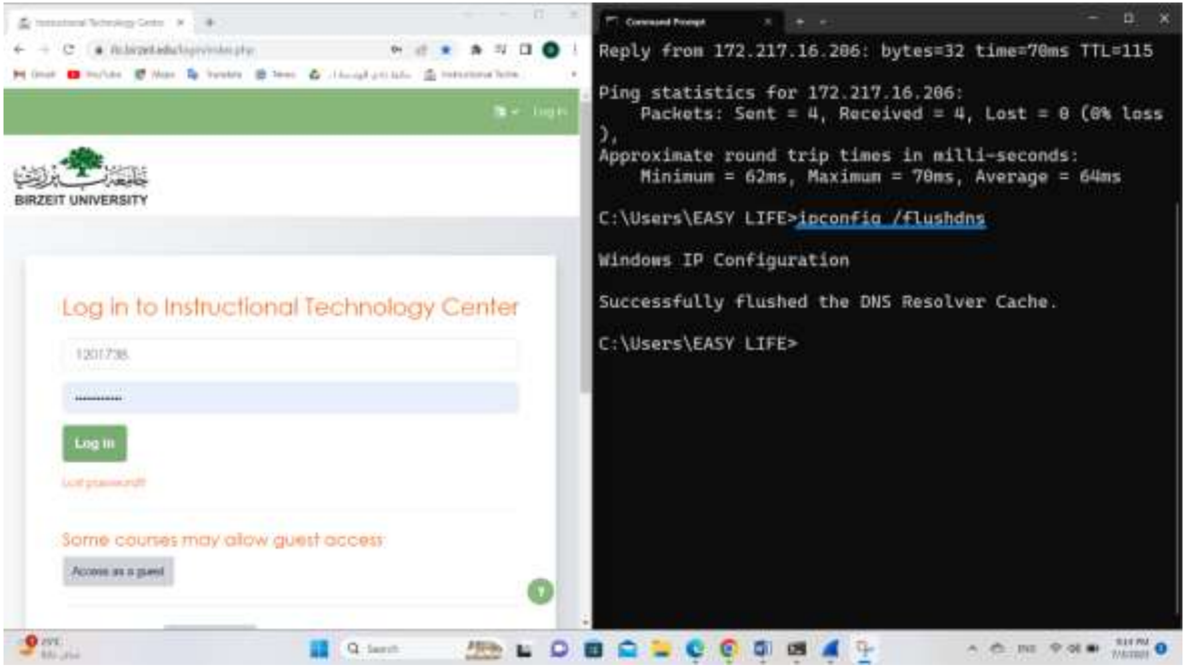
Figure 3: Wireshark screenshot of the Acknowledge Packet

❖ **Fields:**

- ➢ Source address: 192.168.1.1
  This field specifies the DHCP server's address. It indicates which server is sending the DHCP acknowledgement.
- ➢ Destination address: 192.168.1.54
  This field contains the DHCP client's address. It defines who should receive the DHCP acknowledgement packet.
- ➢ DHCP Message Type: ACK
  This field Indicates the packet type as a release message, representing the client's intention to release the IP address lease.
- ➢ Client IP address: 0.0.0.0
  Displays the IP address that the client is releasing from its lease. And here it is 0.0.0.0 in that indicates that the DHCP server was unable to assign an IP address to the client.
- ➢ Lease Time: 259200s (3 days)
  The parameter defines how long the client has the allocated IP address before having to renew the lease.

DNS:

In order to study DNS packets with Wireshark, entered "ipconfig /flushdns" into the command prompt. To clears the DNS cache, refreshing the system's DNS records for accurate domain name resolution. Then open the ITC to get packets results.

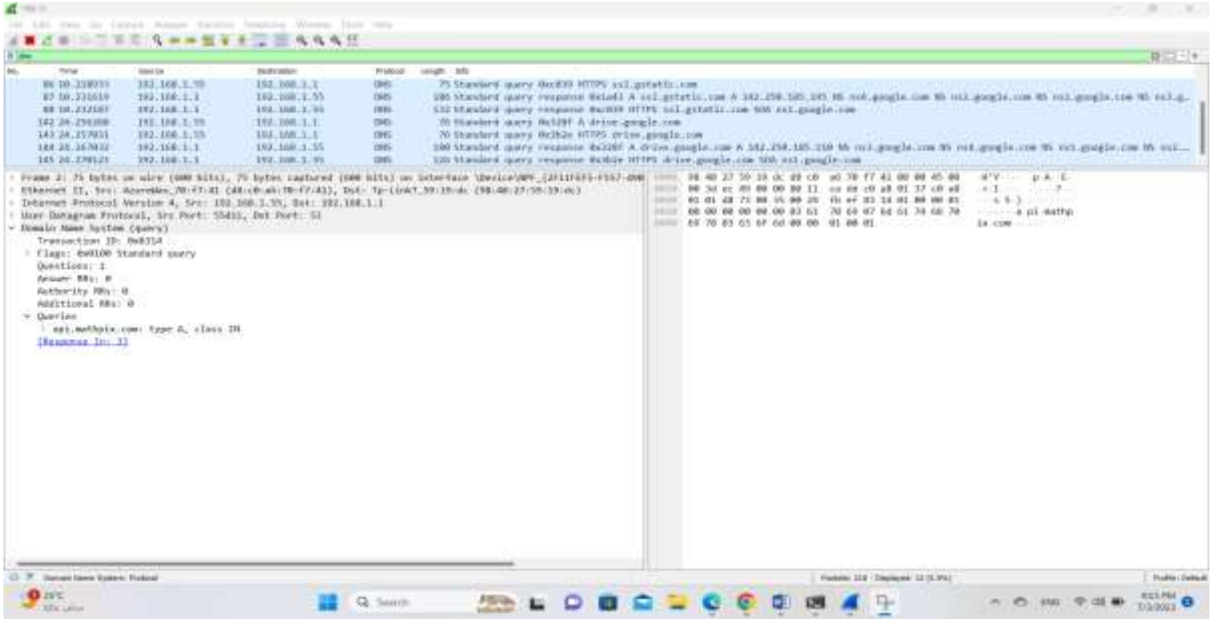

BIRZEIT UNIVERSITY
Log in to Instructional Technology Center
1201738
Log in
Lost password?
Some courses may allow guest access
Access as a guest
Command Prompt

```
Reply from 172.217.16.206: bytes=32 time=70ms TTL=115

Ping statistics for 172.217.16.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss
),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 70ms, Average = 64ms

C:\Users\EASY LIFE>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\EASY LIFE>
```

Figure 4: DNS command

Then collected and studied the DNS query and respond packets using a DNS filter in Wireshark as follows:

- ***Query Packet:***



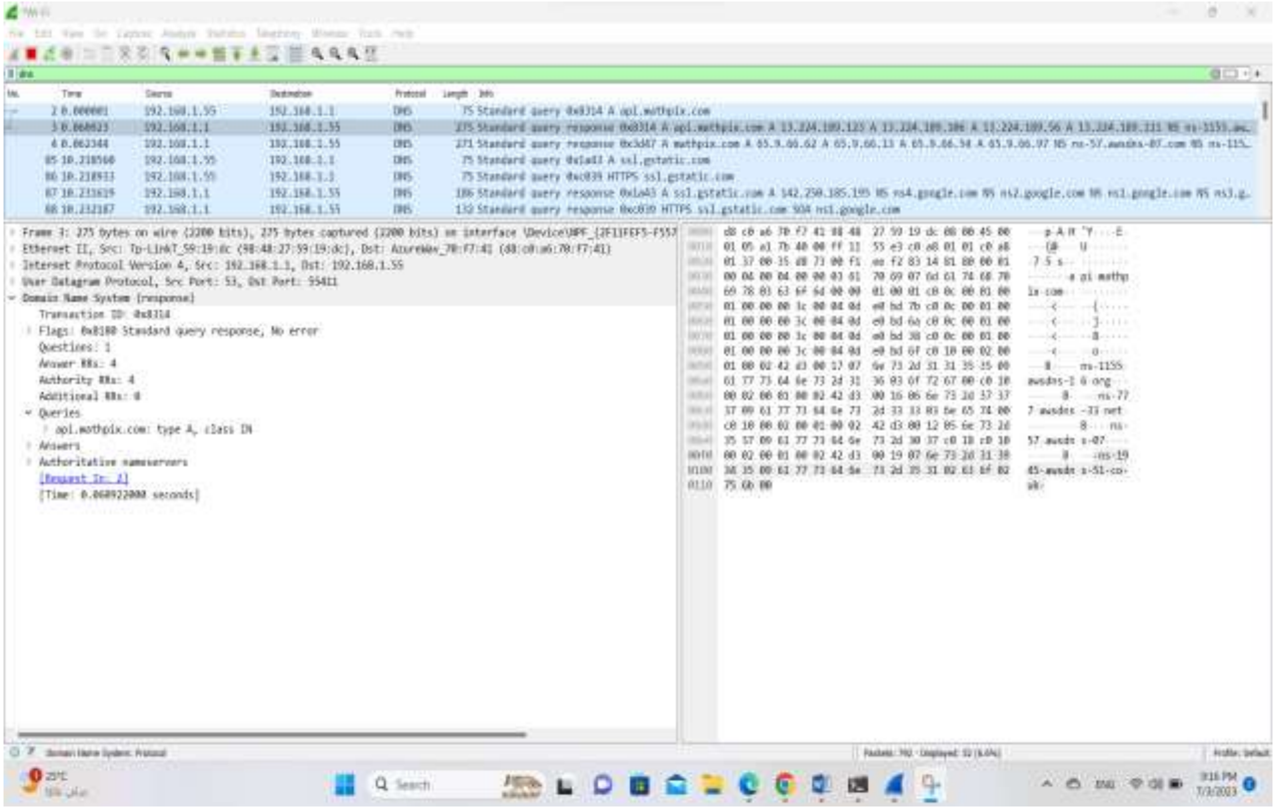
```
No.   Time       Source        Destination   Protocol Length Info
   86 10.230931  192.168.1.55  192.168.1.1   DNS      75 Standard query 0xc839 HTTPS ssl.gstatic.com
   87 10.231619  192.168.1.1   192.168.1.55  DNS     106 Standard query response 0x1e43 A ssl.gstatic.com A 142.250.185.195 NS ns4.google.com NS ns1.google.com NS ns3.g...
   88 10.232107  192.168.1.1   192.168.1.55  DNS     132 Standard query response 0xc839 HTTPS ssl.gstatic.com SOA ns1.google.com
  142 26.256308  192.168.1.55  192.168.1.1   DNS      75 Standard query 0x129f A drive.google.com
  143 26.257031  192.168.1.55  192.168.1.1   DNS      75 Standard query 0x2b2e HTTPS drive.google.com
  144 26.267032  192.168.1.1   192.168.1.55  DNS     180 Standard query response 0x129f A drive.google.com A 142.250.185.110 NS ns1.google.com NS ns4.google.com NS ns2...
  145 26.270121  192.168.1.1   192.168.1.55  DNS     120 Standard query response 0x2b2e HTTPS drive.google.com SOA ns1.google.com

> Frame 2: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{2F11F6F3-F557-...
> Ethernet II, Src: AzureWav_70:f7:41 (48:e7:da:70:f7:41), Dst: Tp-LinkT_59:19:dc (98:48:27:59:19:dc)
> Internet Protocol Version 4, Src: 192.168.1.55, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 55411, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0314
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > api.mathpix.com: type A, class IN
    [Response In: 3]
```

Figure 5:Wireshark screenshot of the Query Packet

- ❖ **Fields:**

- ➢ Source address: 192.168.1.55
  This field specifies the IP address of the client or device that initiated the DNS query.
- ➢ Destination address: 192.168.1.1
  This field contains the IP address of the DNS server that should receive and process the DNS query.
- ➢ DNS Message Type: Query
  This QR field separates DNS query packets and DNS respond packets, enabling for correct packet identification and processing during DNS communication.
- ➢ Answer Section: 0
  In DNS query packets, this section is empty since it is utilized in response packets to deliver the resolved IP address(es) or other desired information for the queried domain name.
- ➢ Authority Section: 0
  This field is often used in response packets to specify resource entries that identify the authoritative DNS servers for the searched domain. It is empty in DNS query packets.

- ***Response Packet:***



```
No.  Time        Source        Destination   Protocol Length Info
   2 0.000001    192.168.1.55  192.168.1.1   DNS       75 Standard query 0x8314 A api.mathpix.com
   3 0.060923    192.168.1.1   192.168.1.55  DNS      275 Standard query response 0x8314 A api.mathpix.com A 13.224.189.123 A 13.224.189.106 A 13.224.189.56 A 13.224.189.111 NS ns-1155.aw…
   4 0.062344    192.168.1.1   192.168.1.55  DNS      271 Standard query response 0x3d47 A mathpix.com A 65.9.66.62 A 65.9.66.13 A 65.9.66.34 A 65.9.66.97 NS ns-57.awsdns-07.com NS ns-115…
  85 10.218560   192.168.1.55  192.168.1.1   DNS       75 Standard query 0x1a43 A ssl.gstatic.com
  86 10.218933   192.168.1.55  192.168.1.1   DNS       75 Standard query 0xc039 HTTPS ssl.gstatic.com
  87 10.231619   192.168.1.1   192.168.1.55  DNS      186 Standard query response 0x1a43 A ssl.gstatic.com A 142.250.185.195 NS ns4.google.com NS ns2.google.com NS ns1.google.com NS ns3.g…
  88 10.232187   192.168.1.1   192.168.1.55  DNS      132 Standard query response 0xc039 HTTPS ssl.gstatic.com SOA ns1.google.com
```

```
> Frame 3: 275 bytes on wire (2200 bits), 275 bytes captured (2200 bits) on interface \Device\NPF_{2F11FEF5-F557
> Ethernet II, Src: Tp-LinkT_59:19:dc (98:48:27:59:19:dc), Dst: AzureWav_70:f7:41 (d8:c0:a6:70:f7:41)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.55
> User Datagram Protocol, Src Port: 53, Dst Port: 55411
v Domain Name System (response)
    Transaction ID: 0x8314
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 4
    Additional RRs: 0
  v Queries
    > api.mathpix.com: type A, class IN
  > Answers
  > Authoritative nameservers
    [Request In: 2]
    [Time: 0.060922000 seconds]
```

```
0000  d8 c0 a6 70 f7 41 98 48  27 59 19 dc 08 00 45 00   ···p·A·H 'Y····E·
0010  01 05 a1 7b 40 00 ff 11  55 e3 c0 a8 01 01 c0 a8   ···{@···U·······
0020  01 37 00 35 d8 73 00 f1  ee f2 83 14 81 80 00 01   ·7·5·s·· ········
0030  00 04 00 04 00 00 03 61  70 69 07 6d 61 74 68 70   ·······a pi·mathp
0040  69 78 03 63 6f 6d 00 00  01 00 01 c0 0c 00 01 00   ix·com·· ········
0050  01 00 00 00 3c 00 04 0d  e0 bd 7b c0 0c 00 01 00   ····<··· ··{·····
0060  01 00 00 00 3c 00 04 0d  e0 bd 6a c0 0c 00 01 00   ····<··· ··j·····
0070  01 00 00 00 3c 00 04 0d  e0 bd 38 c0 0c 00 01 00   ····<··· ··8·····
0080  01 00 00 00 3c 00 04 0d  e0 bd 6f c0 10 00 02 00   ····<··· ··o·····
0090  01 00 02 42 d3 00 17 07  6e 73 2d 31 31 35 35 09   ···B···· ns-1155·
00a0  61 77 73 64 6e 73 2d 31  36 03 6f 72 67 00 c0 10   awsdns-1 6·org···
00b0  00 02 00 01 00 02 42 d3  00 16 06 6e 73 2d 37 37   ······B· ···ns-77
00c0  37 09 61 77 73 64 6e 73  2d 33 33 03 6e 65 74 00   7·awsdns -33·net·
00d0  c0 10 00 02 00 01 00 02  42 d3 00 12 05 6e 73 2d   ········ B····ns-
00e0  35 37 09 61 77 73 64 6e  73 2d 30 37 c0 18 c0 10   57·awsdn s-07····
00f0  00 02 00 01 00 02 42 d3  00 19 07 6e 73 2d 31 39   ······B· ···ns-19
0100  38 35 09 61 77 73 64 6e  73 2d 35 31 02 63 6f 02   85·awsdn s-51·co·
0110  75 6b 00                                           uk·
```

Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Domain Name System: Protocol
Packets: 792 · Displayed: 32 (4.0%)
Profile: Default
Search

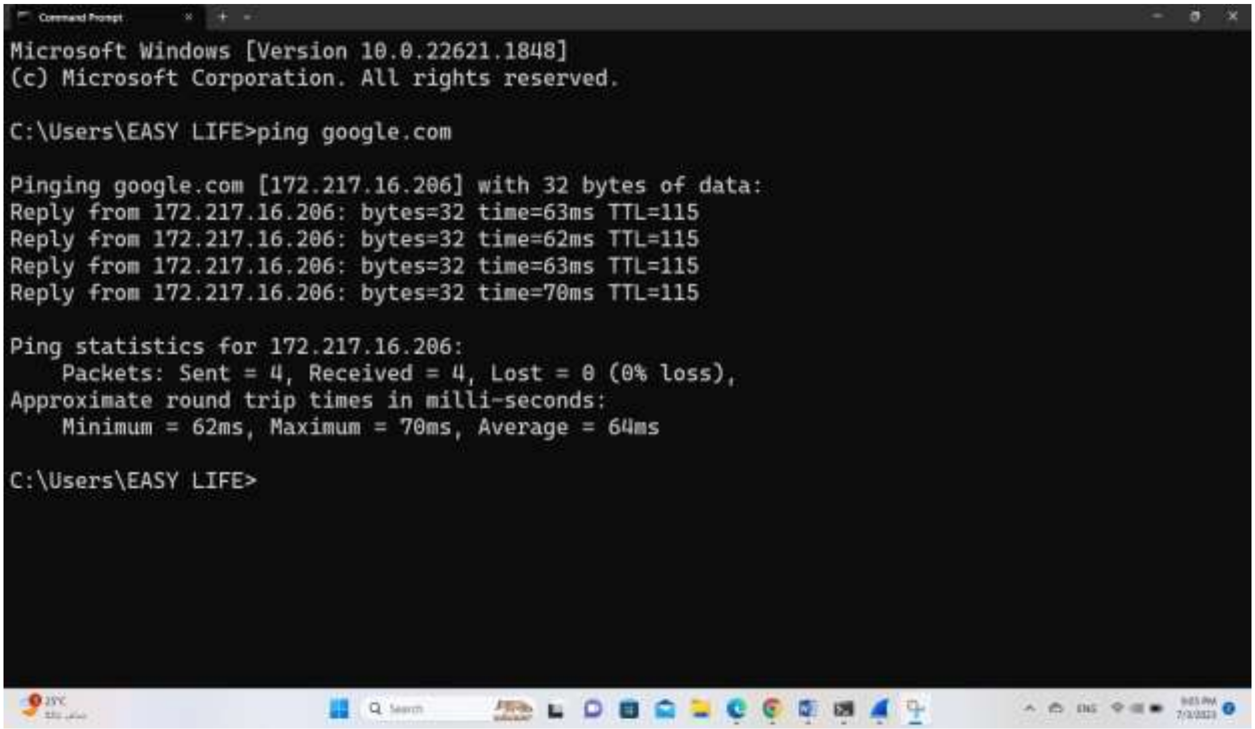
Figure 6: Wireshark screenshot of the Response Packet

❖ Fields:

- Source address: 192.168.11
  This field specifies the IP address of the DNS server that generated and sent the DNS response.
- Destination address: 192.168.1.55
  This field contains the IP address of the client or device that requested the DNS query.
- DNS Message Type: Response
  This QR field separates DNS query packets and DNS respond packets, enabling for correct packet identification and processing during DNS communication.
- Answer Section: 4
  That mean it contains four resource entries for the query domain that provide the resolved IP address(es) or other desired information.
- Authority Section: 4
  The packet provides four resource entries that specify the authoritative DNS servers for the domain in query.

ICMP:

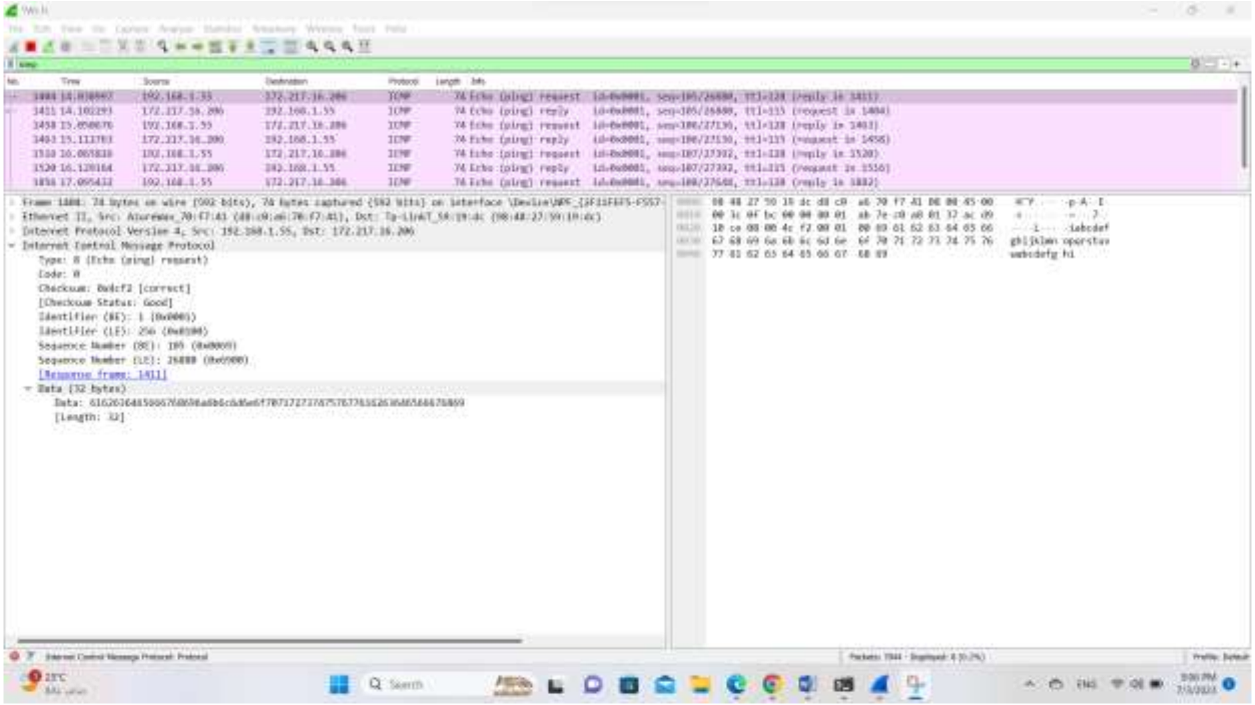
The "ping google.com" command is used to send ICMP echo request packets to the domain name "google.com" to check its reachability and measure the round-trip time.



```
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\EASY LIFE>ping google.com

Pinging google.com [172.217.16.206] with 32 bytes of data:
Reply from 172.217.16.206: bytes=32 time=63ms TTL=115
Reply from 172.217.16.206: bytes=32 time=62ms TTL=115
Reply from 172.217.16.206: bytes=32 time=63ms TTL=115
Reply from 172.217.16.206: bytes=32 time=70ms TTL=115

Ping statistics for 172.217.16.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 70ms, Average = 64ms

C:\Users\EASY LIFE>
```

Figure 7: ICMP command

- ***Request Packet:***



```
1404 14.038997  192.168.1.55    172.217.16.206  ICMP  74 Echo (ping) request  id=0x0001, seq=105/26880, ttl=128 (reply in 1411)
1411 14.102293  172.217.16.206  192.168.1.55    ICMP  74 Echo (ping) reply    id=0x0001, seq=105/26880, ttl=115 (request in 1404)
1458 15.050076  192.168.1.55    172.217.16.206  ICMP  74 Echo (ping) request  id=0x0001, seq=106/27136, ttl=128 (reply in 1463)
1463 15.113703  172.217.16.206  192.168.1.55    ICMP  74 Echo (ping) reply    id=0x0001, seq=106/27136, ttl=115 (request in 1458)
1510 16.065838  192.168.1.55    172.217.16.206  ICMP  74 Echo (ping) request  id=0x0001, seq=107/27392, ttl=128 (reply in 1520)
1520 16.128164  172.217.16.206  192.168.1.55    ICMP  74 Echo (ping) reply    id=0x0001, seq=107/27392, ttl=115 (request in 1510)
1858 17.095432  192.168.1.55    172.217.16.206  ICMP  74 Echo (ping) request  id=0x0001, seq=108/27648, ttl=128 (reply in 1882)
```

```
> Frame 1404: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{3F11FEF5-F557-
> Ethernet II, Src: AzureWav_70:f7:41 (d8:c0:a6:70:f7:41), Dst: Tp-LinkT_59:19:dc (98:48:27:59:19:dc)
> Internet Protocol Version 4, Src: 192.168.1.55, Dst: 172.217.16.206
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4cf2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 105 (0x0069)
    Sequence Number (LE): 26880 (0x6900)
    [Response frame: 1411]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

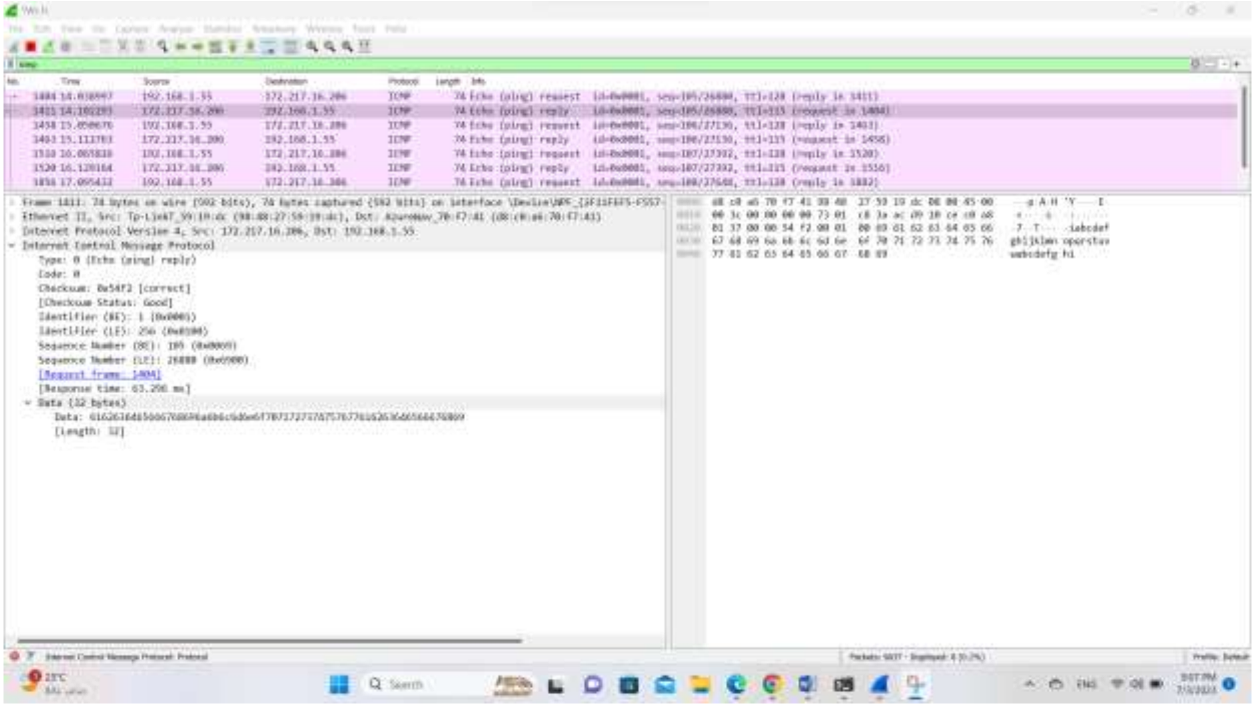
```
0000  98 48 27 59 19 dc d8 c0  a6 70 f7 41 08 00 45 00   .H'Y.....p.A..E.
0010  00 3c 4f bc 00 00 80 01  ab 7e c0 a8 01 37 ac d9   .<O......~...7..
0020  10 ce 08 00 4c f2 00 01  00 69 61 62 63 64 65 66   ....L....iabcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmnopqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefghi
```

Figure 8: Wireshark screenshot of the Request Packet

❖ **Fields:**

- Type: 8 (Echo (ping) request)
  Specifies the ICMP message type. The type value of an Echo Request is 8, indicating a request for an Echo Reply.
- Code: 0
  Improves the ICMP message type. An Echo Request has a code of 0, indicating that it is a standard request.
- Checksum: 0x4cf2 (correct)
  A computed number used to detect errors in an ICMP packet as it is being sent, maintaining data integrity.
- Identifier: BE: 1 (0x0001) LE: 256 (0x0100)
  The ICMP Request's unique identifier, provided in both Big-Endian and Little-Endian byte ordering, for matching with related replies.
- Sequence Number: BE: 105 (0x0069) LE: 26880 (0x6900)
  An ICMP Request sequence number that is shared by both Big-Endian and Little-Endian identifiers that facilitates in matching requests with responses and identifying packet loss.

- ***Reply Packet:***



Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.   Time       Source          Destination     Protocol Length Info
1404 14.038997   192.168.1.55    172.217.16.206  ICMP     74 Echo (ping) request  id=0x0001, seq=105/26880, ttl=128 (reply in 1411)
1411 14.102293   172.217.16.206  192.168.1.55    ICMP     74 Echo (ping) reply    id=0x0001, seq=105/26880, ttl=115 (request in 1404)
1458 15.050676   192.168.1.55    172.217.16.206  ICMP     74 Echo (ping) request  id=0x0001, seq=106/27136, ttl=128 (reply in 1463)
1463 15.113783   172.217.16.206  192.168.1.55    ICMP     74 Echo (ping) reply    id=0x0001, seq=106/27136, ttl=115 (request in 1458)
1510 16.065838   192.168.1.55    172.217.16.206  ICMP     74 Echo (ping) request  id=0x0001, seq=107/27392, ttl=128 (reply in 1520)
1520 16.129164   172.217.16.206  192.168.1.55    ICMP     74 Echo (ping) reply    id=0x0001, seq=107/27392, ttl=115 (request in 1510)
1858 17.095432   192.168.1.55    172.217.16.206  ICMP     74 Echo (ping) request  id=0x0001, seq=108/27648, ttl=128 (reply in 1882)
```

```
> Frame 1411: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{2F11FEF5-F557-
> Ethernet II, Src: Tp-LinkT_59:19:dc (98:48:27:59:19:dc), Dst: AzureWav_70:f7:41 (d8:c0:a6:70:f7:41)
> Internet Protocol Version 4, Src: 172.217.16.206, Dst: 192.168.1.55
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x54f2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 105 (0x0069)
    Sequence Number (LE): 26880 (0x6900)
    [Request frame: 1404]
    [Response time: 63.296 ms]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

```
0000  d8 c0 a6 70 f7 41 98 48  27 59 19 dc 08 00 45 00   ...p.A.H 'Y....E.
0010  00 3c 00 00 00 00 73 01  c8 3a ac d9 10 ce c0 a8   .<....s. .:......
0020  01 37 00 00 54 f2 00 01  00 69 61 62 63 64 65 66   .7..T... .iabcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Figure 9: Wireshark screenshot of the Reply Packet

❖ Fields:

- ➢ Type: 0 (Echo (ping) reply)
  This value indicates the kind of ICMP message. The type value of an Echo Reply is 0, indicating that it is a response to an Echo Request.
- ➢ Code: 0
  The ICMP message type is refined. An Echo Reply has a code value of 0, indicating that it is a standard response.
- ➢ Checksum: 0x54f2 (correct)
  A calculated number used to identify errors during packet transmission and ensure data integrity in the ICMP Reply packet.
- ➢ Identifier: BE: 1 (0x0001)   LE: 256 (0x0100)
  Contains the same unique identification as the associated ICMP Request, and is encoded in both Big-Endian and Little-Endian byte ordering, allowing the recipient to match the reply to the original request.
- ➢ Sequence Number: BE: 105 (0x0069)   LE: 26880 (0x6900)
  Carries the same sequence number as the accompanying ICMP Request, which is shared by both Big-Endian and Little-Endian identifiers, making it easier to match responses to particular requests and identify packet loss.

Part 2:

In this part, we used Packet Tracer to build a network with 4 routers, 2 switches, and 5 PCs. The network employed OSPF routing protocol for dynamic routing. One subnet used DHCP for automatic IP address assignment. The IP address range will be based on the university ID, such as 205.x.y.0/24, where x and y correspond to the numbers in the ID.

Our ID’s 1201585 then the IP is 205.1.5.0/24. We need 5 subnets (networks).

Subnet 1: 205.1.5.0/27 (Network Address: 205.1.5.0, Broadcast Address: 205.1.5.31)

Subnet 2: 205.1.5.32/27 (Network Address: 205.1.5.32, Broadcast Address: 205.1.5.63)

Subnet 3: 205.1.5.64/27 (Network Address: 205.1.5.64, Broadcast Address: 205.1.5.95)

Subnet 4: 205.1.5.96/27 (Network Address: 205.1.5.96, Broadcast Address: 205.1.5.127)

Subnet 5: 205.1.5.128/27 (Network Address: 205.1.5.128, Broadcast Address: 205.1.5.159)

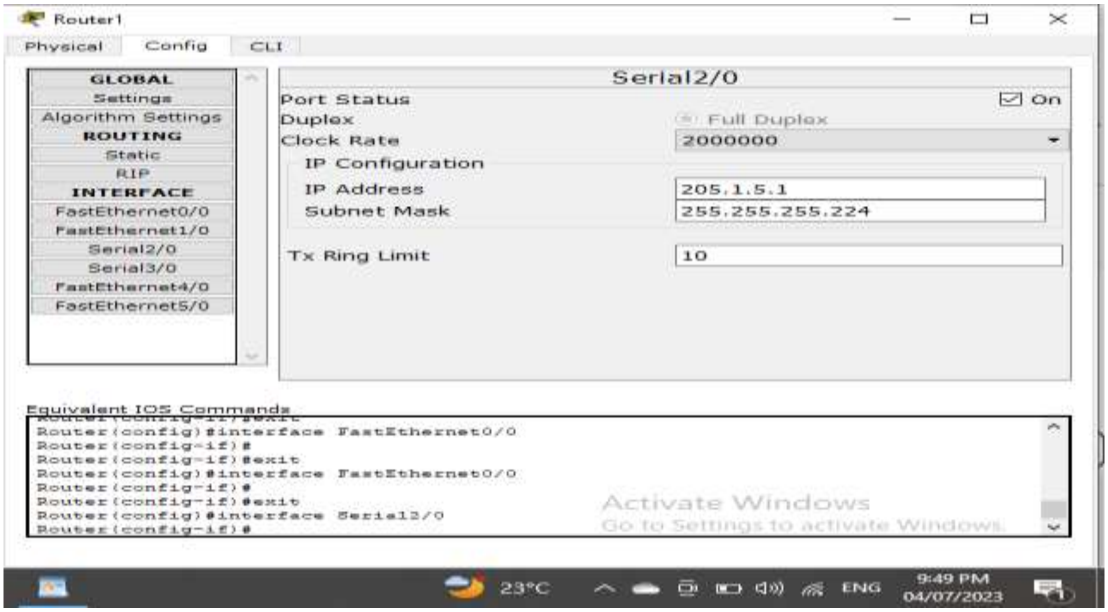
The Subnet Mask: 255.255.255.224

The network included a web server and a DNS server for hosting websites and resolving domain names. We tested connectivity between hosts using the ping command and traced the path taken by packets using the tracert command. By following these steps, we had a functional network with OSPF routing, DHCP for IP assignment, a web server, and a DNS server, allowing for communication between devices and hosting websites within the network.

Building the topology:

Build the topology using packet tracer based on your IPs found above and put the IP address and subnet mask for each router.

- **Interface Router1:**



Serial2/0

Port Status ☑ On

Duplex ○ Full Duplex

Clock Rate 2000000

IP Configuration

IP Address 205.1.5.1

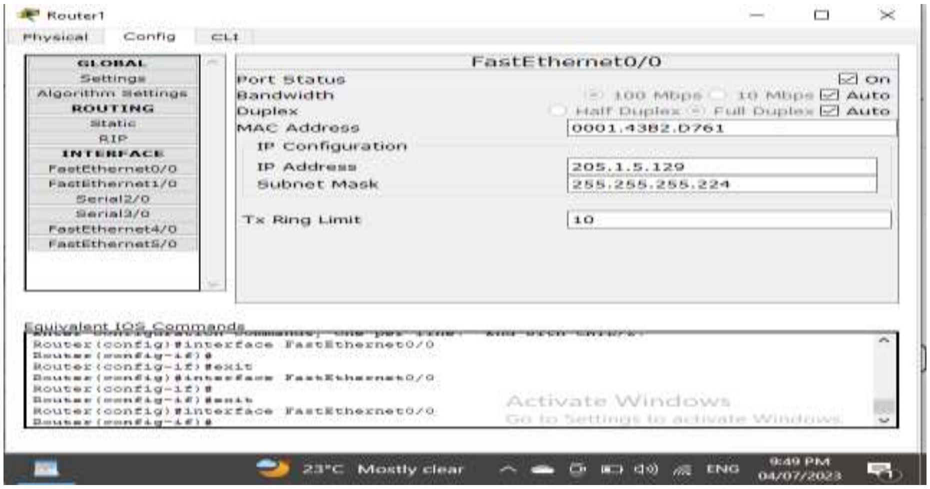
Subnet Mask 255.255.255.224

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
```

Figure 10: Interface Router1 sitting



FastEthernet0/0

Port Status ☑ On

Bandwidth ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0001.4382.D761

IP Configuration

IP Address 205.1.5.129

Subnet Mask 255.255.255.224

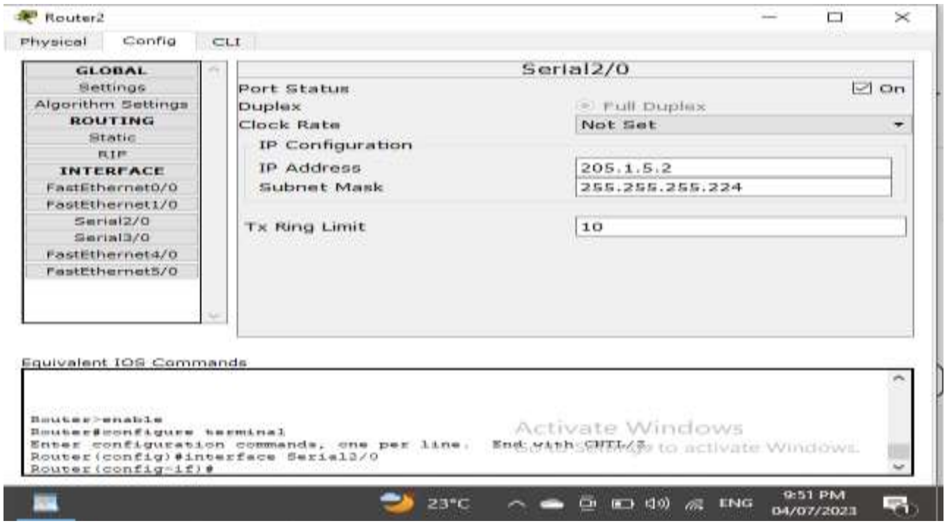
Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

Figure 11: Interface Router1 sitting

- **Interface Router2:**



Serial2/0

Port Status ☑ On

Duplex ● Full Duplex

Clock Rate Not Set

IP Configuration

IP Address 205.1.5.2

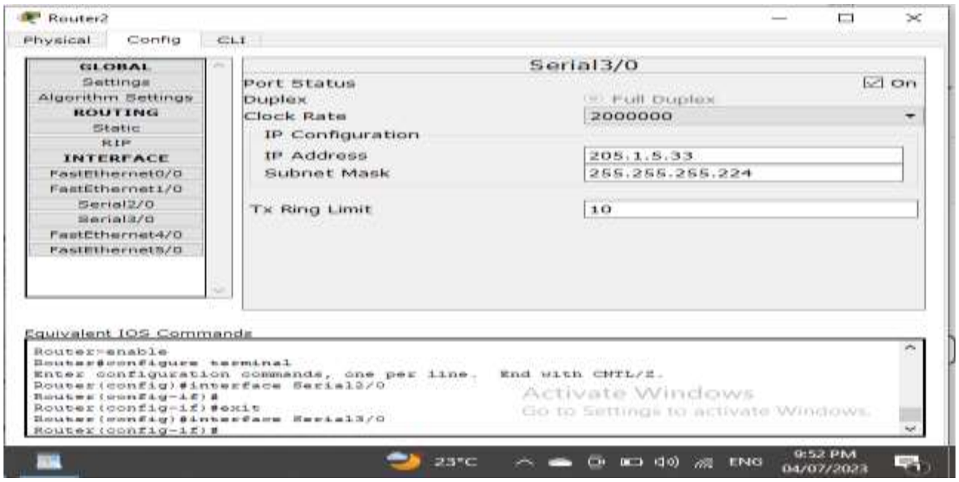
Subnet Mask 255.255.255.224

Tx Ring Limit 10

Equivalent IOS Commands

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial2/0
Router(config-if)#
```

Figure 12: Interface Router2 sitting



Serial3/0

Port Status ☑ On

Duplex ● Full Duplex

Clock Rate 2000000

IP Configuration

IP Address 205.1.5.33

Subnet Mask 255.255.255.224

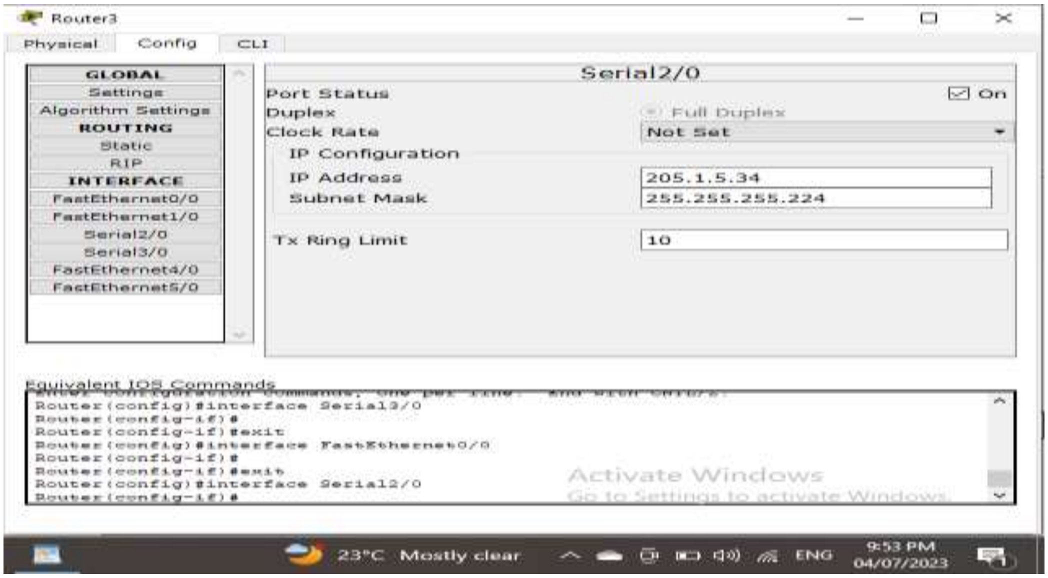
Tx Ring Limit 10

Equivalent IOS Commands

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial3/0
Router(config-if)#
```

Figure 13: Interface Router2 sitting

- **Interface Router3:**



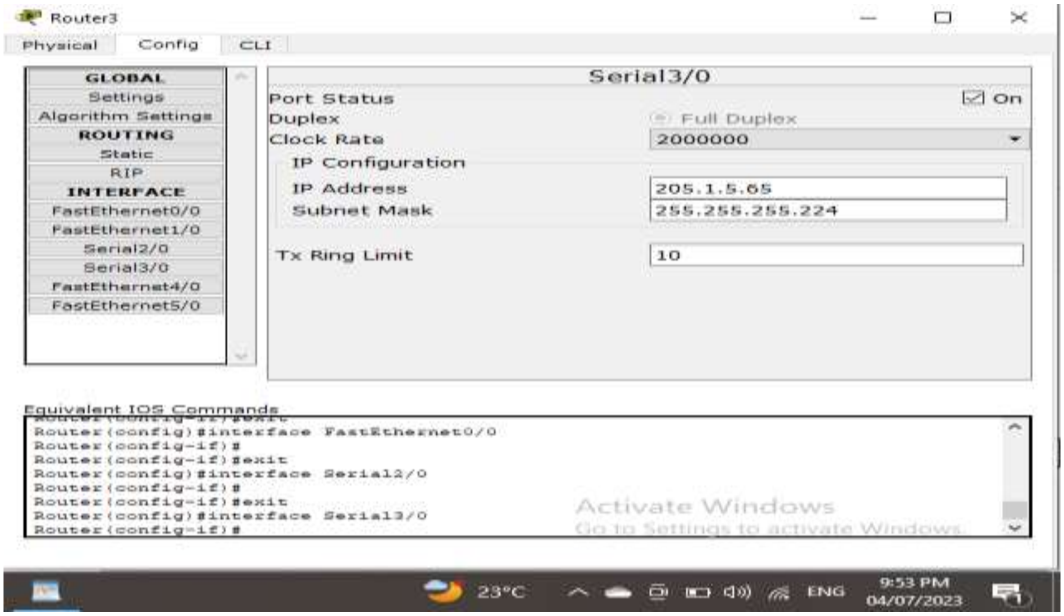
Serial2/0

Port Status ☑ On
Duplex ○ Full Duplex
Clock Rate Not Set
IP Configuration
IP Address 205.1.5.34
Subnet Mask 255.255.255.224
Tx Ring Limit 10

Equivalent IOS Commands

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial3/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
```

Figure 14: Interface Router3 sitting



Serial3/0

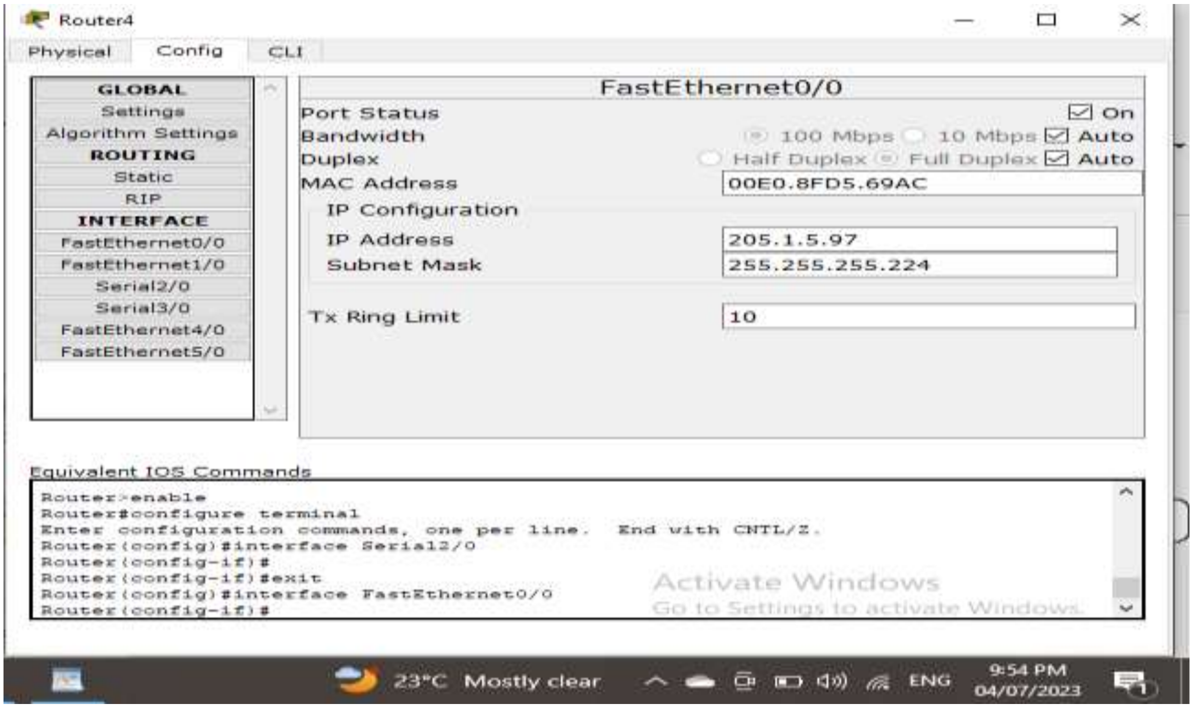
Port Status ☑ On
Duplex ○ Full Duplex
Clock Rate 2000000
IP Configuration
IP Address 205.1.5.65
Subnet Mask 255.255.255.224
Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial3/0
Router(config-if)#
```

Figure 15: Interface Router3 sitting

- **Interface Router4:**



FastEthernet0/0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 00E0.8FD5.69AC

IP Configuration

IP Address 205.1.5.97

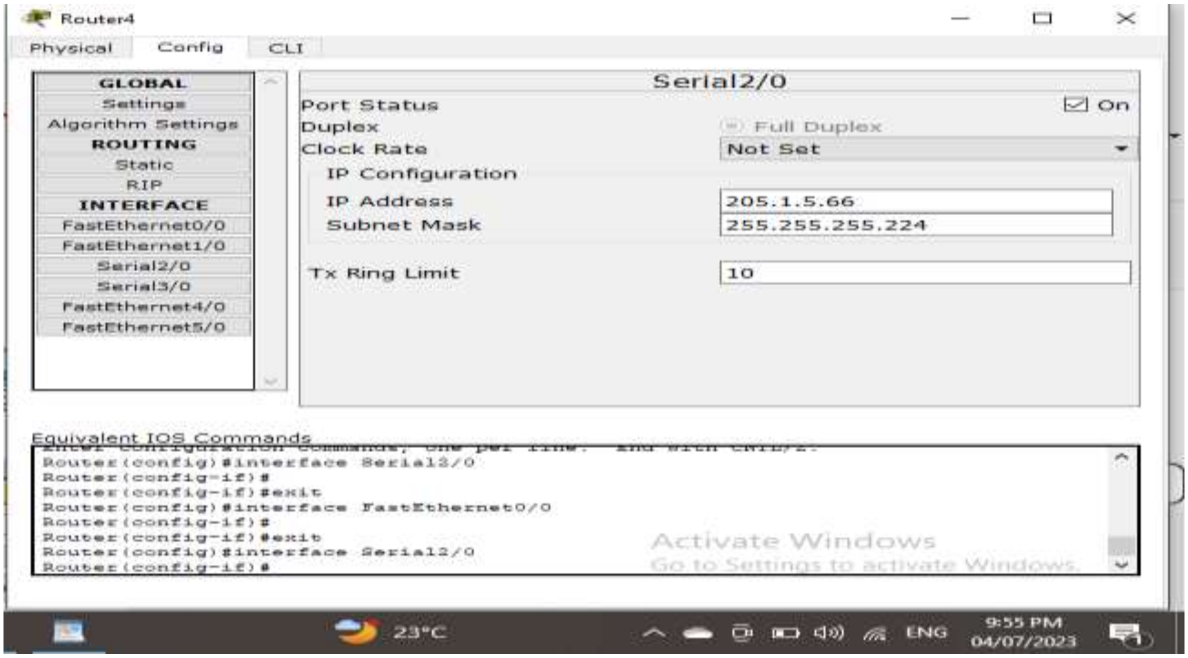
Subnet Mask 255.255.255.224

Tx Ring Limit 10

Equivalent IOS Commands

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

Figure 16: Interface Router4 sitting



Serial2/0

Port Status ☑ On

Duplex ● Full Duplex

Clock Rate Not Set

IP Configuration

IP Address 205.1.5.66

Subnet Mask 255.255.255.224

Tx Ring Limit 10

Equivalent IOS Commands

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
```

Figure 17: Interface Router4 sitting

- **The network topology:**

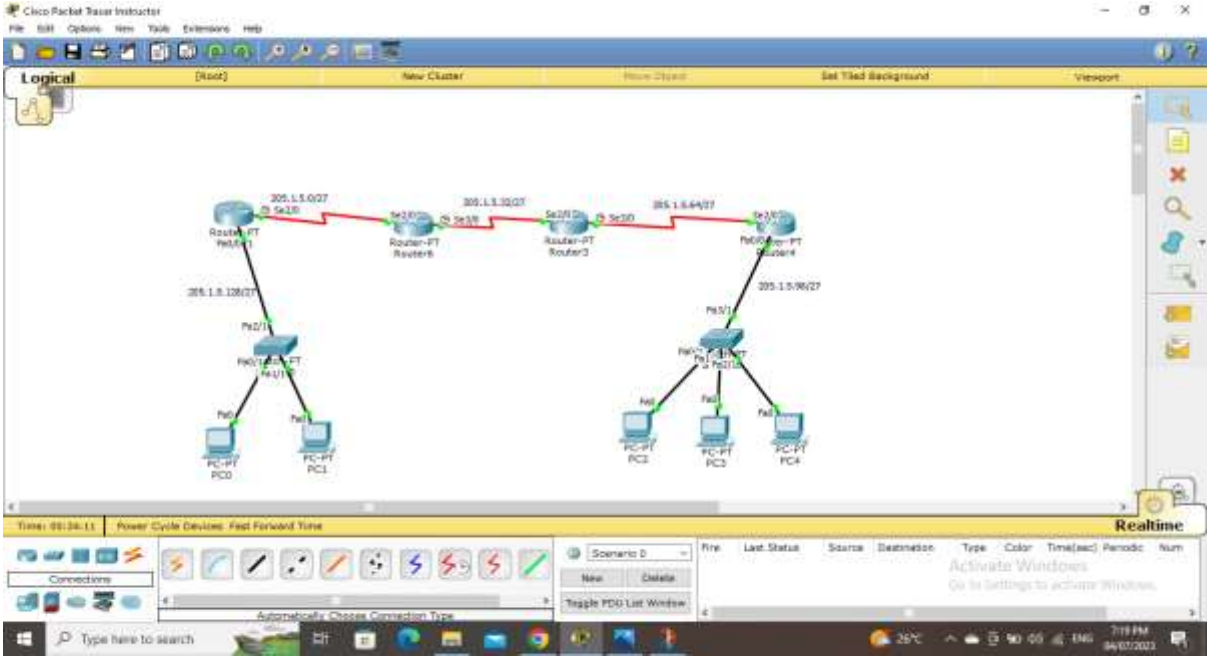
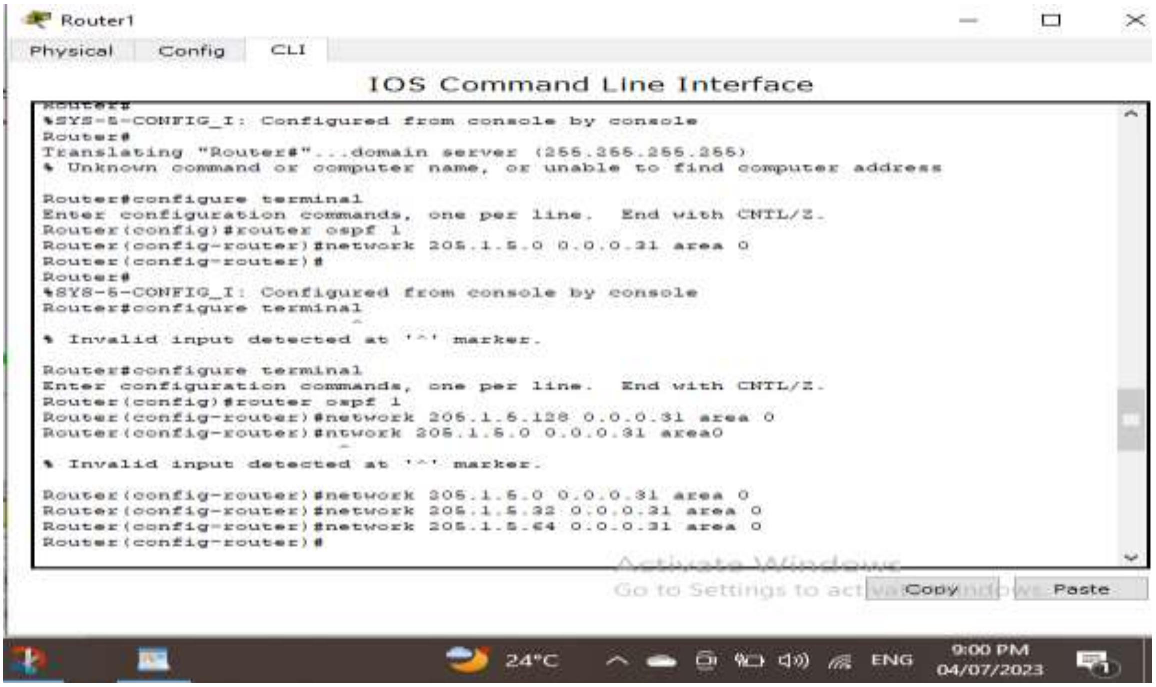


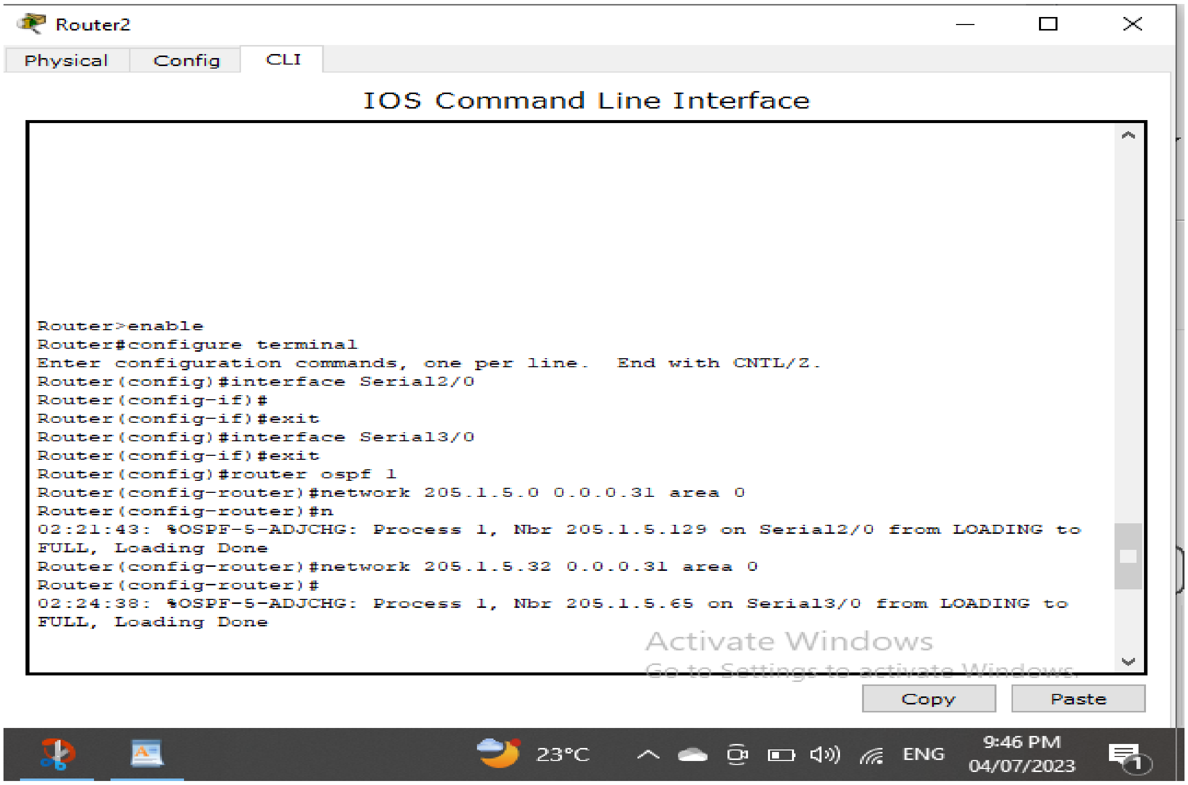
Figure 18: The network topology

- **OSPF routing protocol for each router:**



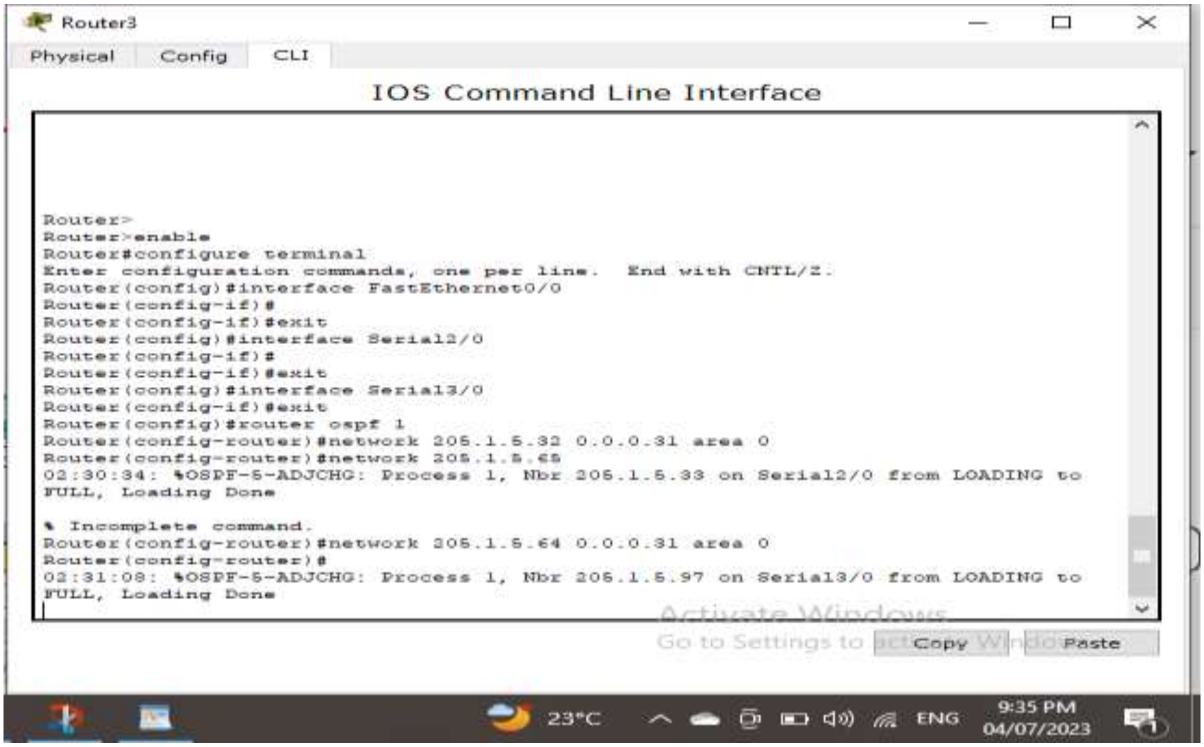
```
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
Translating "Router#"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 205.1.5.0 0.0.0.31 area 0
Router(config-router)#
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#configure terminal
                    ^
% Invalid input detected at '^' marker.

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 205.1.5.128 0.0.0.31 area 0
Router(config-router)#ntwork 205.1.5.0 0.0.0.31 area0
                       ^
% Invalid input detected at '^' marker.

Router(config-router)#network 205.1.5.0 0.0.0.31 area 0
Router(config-router)#network 205.1.5.32 0.0.0.31 area 0
Router(config-router)#network 205.1.5.64 0.0.0.31 area 0
Router(config-router)#
```

Figure 19: OSPF routing protocol for router1



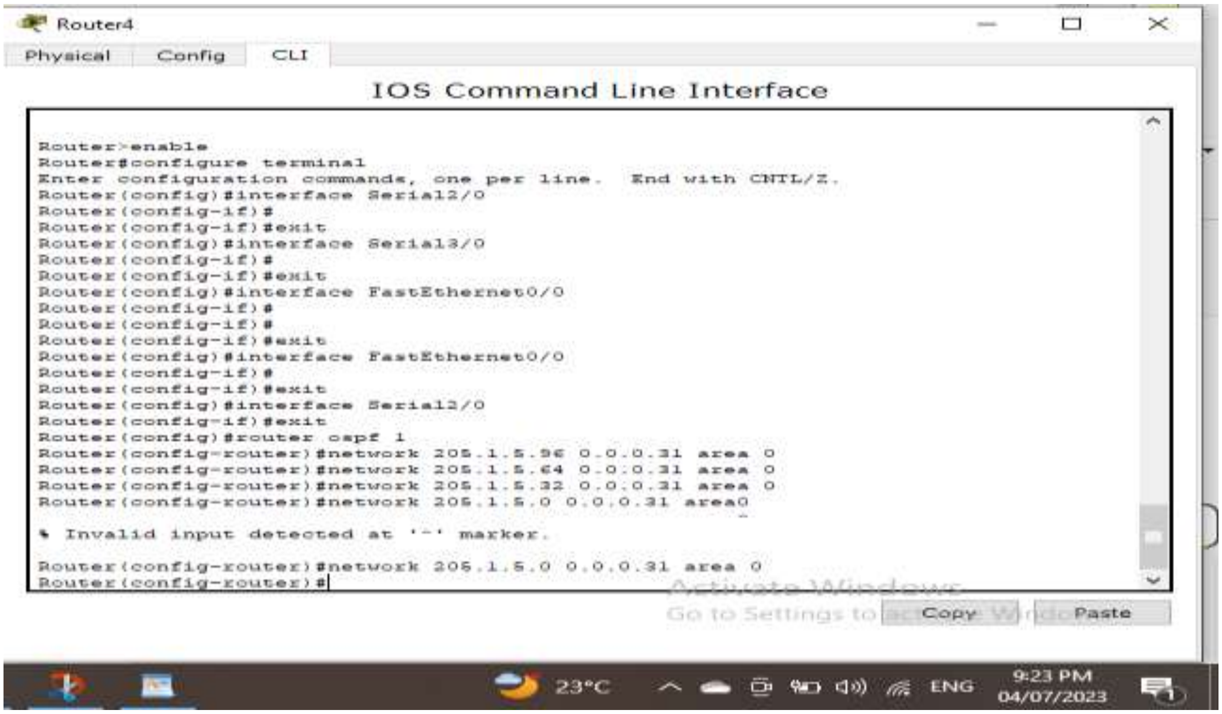
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial3/0
Router(config-if)#exit
Router(config)#router ospf 1
Router(config-router)#network 205.1.5.0 0.0.0.31 area 0
Router(config-router)#n
02:21:43: %OSPF-5-ADJCHG: Process 1, Nbr 205.1.5.129 on Serial2/0 from LOADING to
FULL, Loading Done
Router(config-router)#network 205.1.5.32 0.0.0.31 area 0
Router(config-router)#
02:24:38: %OSPF-5-ADJCHG: Process 1, Nbr 205.1.5.65 on Serial3/0 from LOADING to
FULL, Loading Done
```

Figure 20: OSPF routing protocol for router2



```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial3/0
Router(config-if)#exit
Router(config)#router ospf 1
Router(config-router)#network 205.1.5.32 0.0.0.31 area 0
Router(config-router)#network 205.1.5.65
02:30:34: %OSPF-5-ADJCHG: Process 1, Nbr 205.1.5.33 on Serial2/0 from LOADING to
FULL, Loading Done

% Incomplete command.
Router(config-router)#network 205.1.5.64 0.0.0.31 area 0
Router(config-router)#
02:31:08: %OSPF-5-ADJCHG: Process 1, Nbr 205.1.5.97 on Serial3/0 from LOADING to
FULL, Loading Done
```

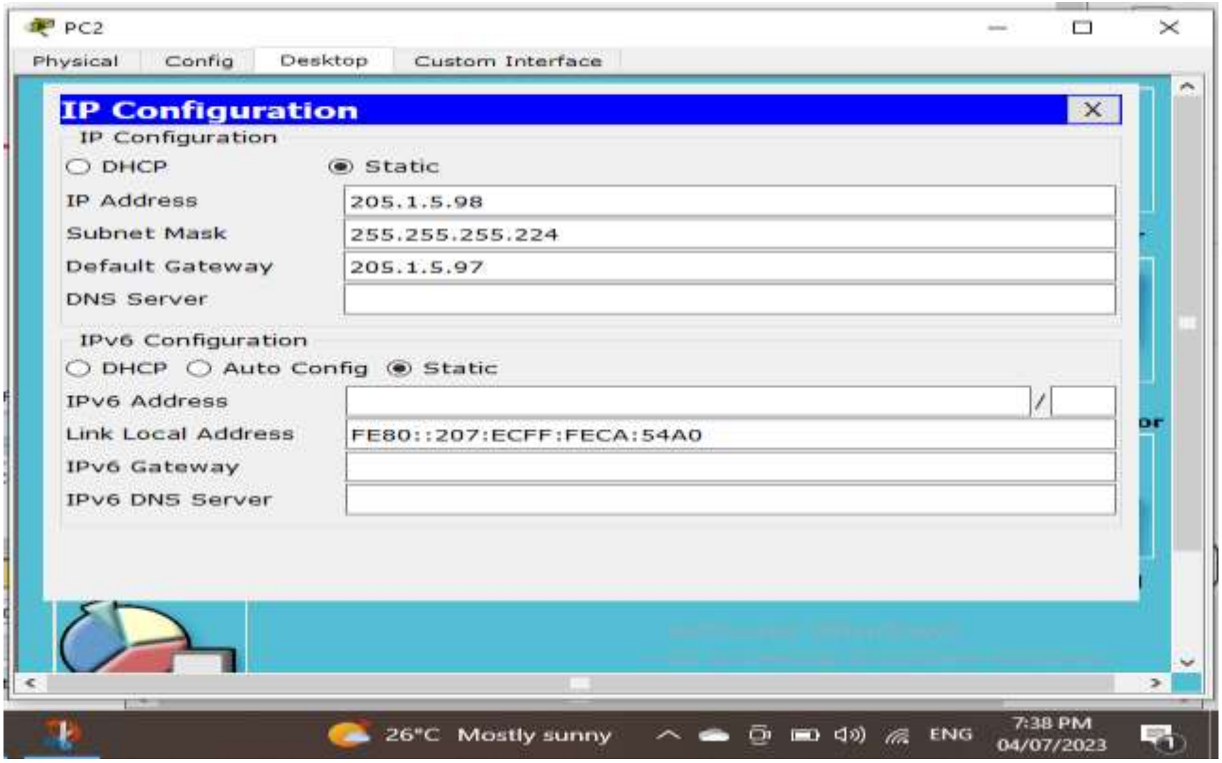
Figure 21: OSPF routing protocol for router3



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial3/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#exit
Router(config)#router ospf 1
Router(config-router)#network 205.1.5.96 0.0.0.31 area 0
Router(config-router)#network 205.1.5.64 0.0.0.31 area 0
Router(config-router)#network 205.1.5.32 0.0.0.31 area 0
Router(config-router)#network 205.1.5.0 0.0.0.31 area0
                                                       ^
% Invalid input detected at '^' marker.

Router(config-router)#network 205.1.5.0 0.0.0.31 area 0
Router(config-router)#
```

Figure 22: OSPF routing protocol for router4

- **IP Configuration for PC2:**



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 205.1.5.98

Subnet Mask 255.255.255.224

Default Gateway 205.1.5.97

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

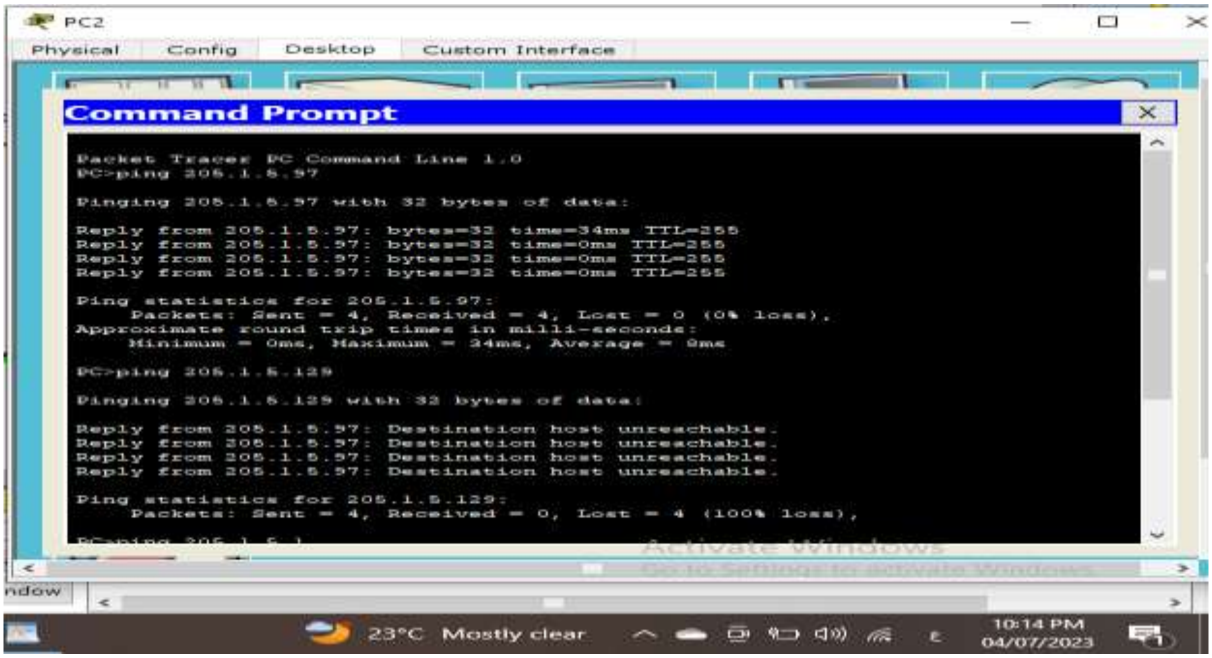
Link Local Address FE80::207:ECFF:FECA:54A0

IPv6 Gateway

IPv6 DNS Server

Figure 23: IP Configuration for PC2

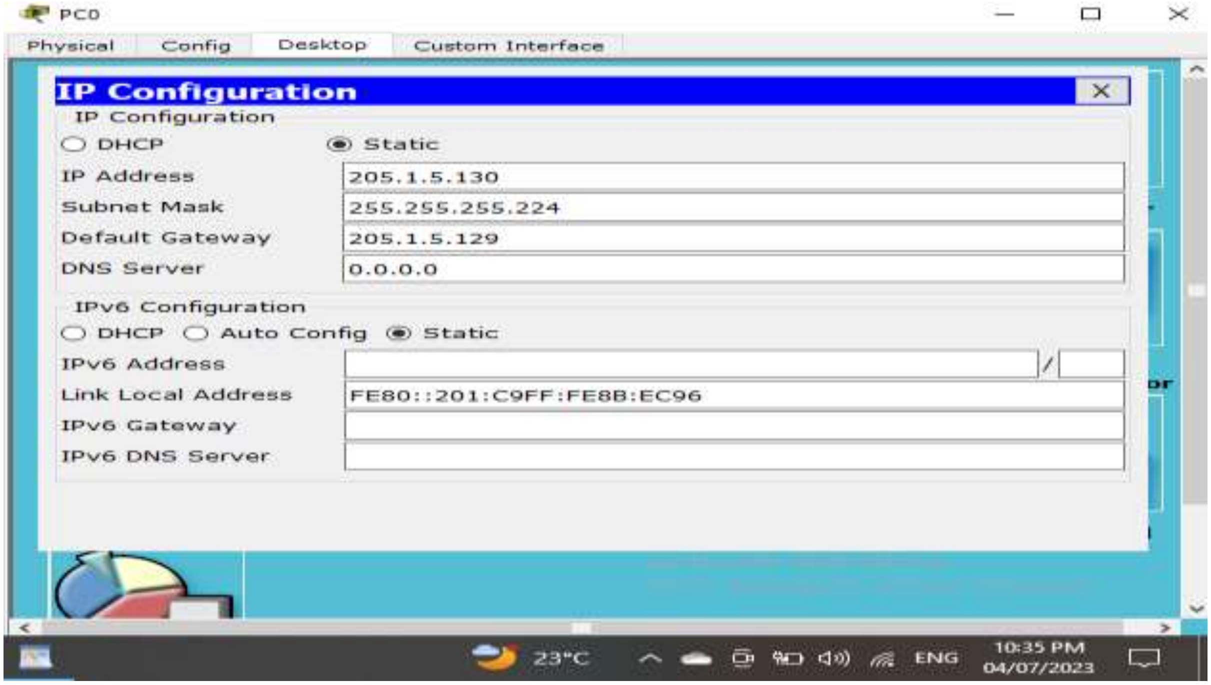
- **Ping after the OSPF routing protocol:**



```
Packet Tracer PC Command Line 1.0
PC>ping 205.1.5.97

Pinging 205.1.5.97 with 32 bytes of data:

Reply from 205.1.5.97: bytes=32 time=34ms TTL=255
Reply from 205.1.5.97: bytes=32 time=0ms TTL=255
Reply from 205.1.5.97: bytes=32 time=0ms TTL=255
Reply from 205.1.5.97: bytes=32 time=0ms TTL=255

Ping statistics for 205.1.5.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 34ms, Average = 8ms

PC>ping 205.1.5.129

Pinging 205.1.5.129 with 32 bytes of data:

Reply from 205.1.5.97: Destination host unreachable.
Reply from 205.1.5.97: Destination host unreachable.
Reply from 205.1.5.97: Destination host unreachable.
Reply from 205.1.5.97: Destination host unreachable.

Ping statistics for 205.1.5.129:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 205.1.5.1
```

Figure 24: Ping after the OSPF routing protocol

- **IP Configuration for PC0:**



IP Configuration

○ DHCP ● Static

IP Address	205.1.5.130
Subnet Mask	255.255.255.224
Default Gateway	205.1.5.129
DNS Server	0.0.0.0

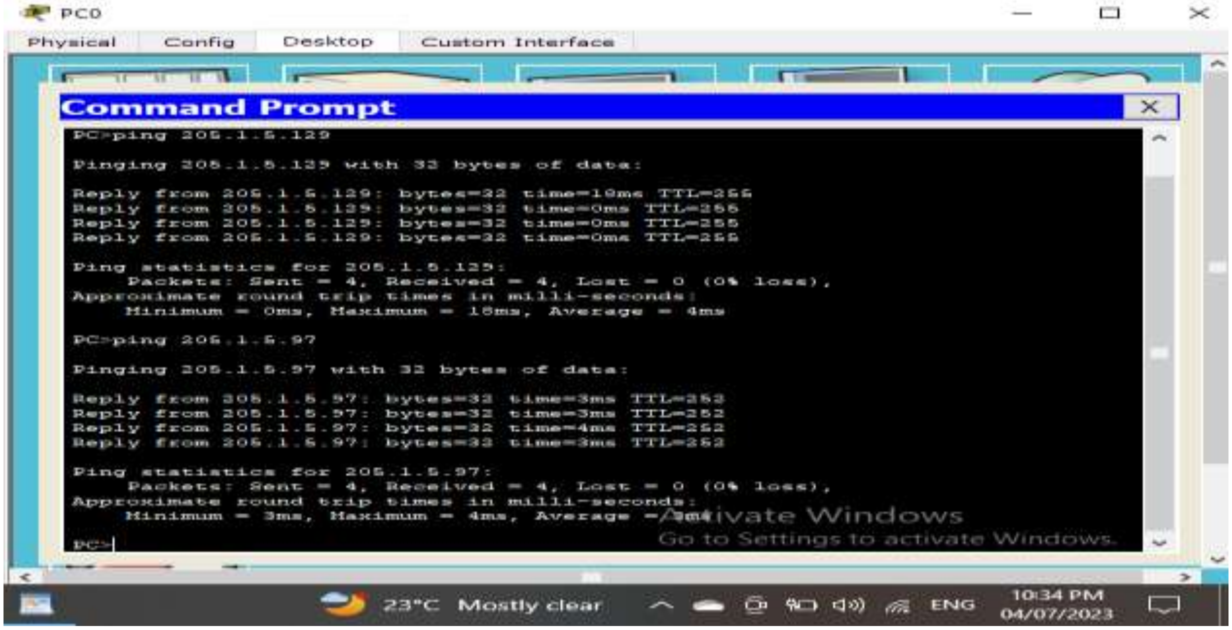
IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address	/
Link Local Address	FE80::201:C9FF:FE8B:EC96
IPv6 Gateway	
IPv6 DNS Server	

Figure 25: IP Configuration for PC0

- **Ping after the OSPF routing protocol:**



```
PC>ping 205.1.5.129

Pinging 205.1.5.129 with 32 bytes of data:

Reply from 205.1.5.129: bytes=32 time=18ms TTL=255
Reply from 205.1.5.129: bytes=32 time=0ms TTL=255
Reply from 205.1.5.129: bytes=32 time=0ms TTL=255
Reply from 205.1.5.129: bytes=32 time=0ms TTL=255

Ping statistics for 205.1.5.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 4ms

PC>ping 205.1.5.97

Pinging 205.1.5.97 with 32 bytes of data:

Reply from 205.1.5.97: bytes=32 time=3ms TTL=252
Reply from 205.1.5.97: bytes=32 time=3ms TTL=252
Reply from 205.1.5.97: bytes=32 time=4ms TTL=252
Reply from 205.1.5.97: bytes=32 time=3ms TTL=252

Ping statistics for 205.1.5.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

PC>
```

Figure 26: Ping after the OSPF routing protocol command

DHCP (Dynamic Host Configuration Protocol) is a network protocol that assigns IP addresses dynamically to devices on a network. When a device connects to the network, it sends a broadcast request for an IP address, and the DHCP server assigns an available IP address along with other network information such as subnet mask, default gateway, and DNS server information. DHCP allows network administrators to manage IP address allocation centrally, saving time and reducing the risk of IP address conflicts. It is widely used in home, office, and enterprise networks and is supported by most operating systems and network devices.

When add web server:

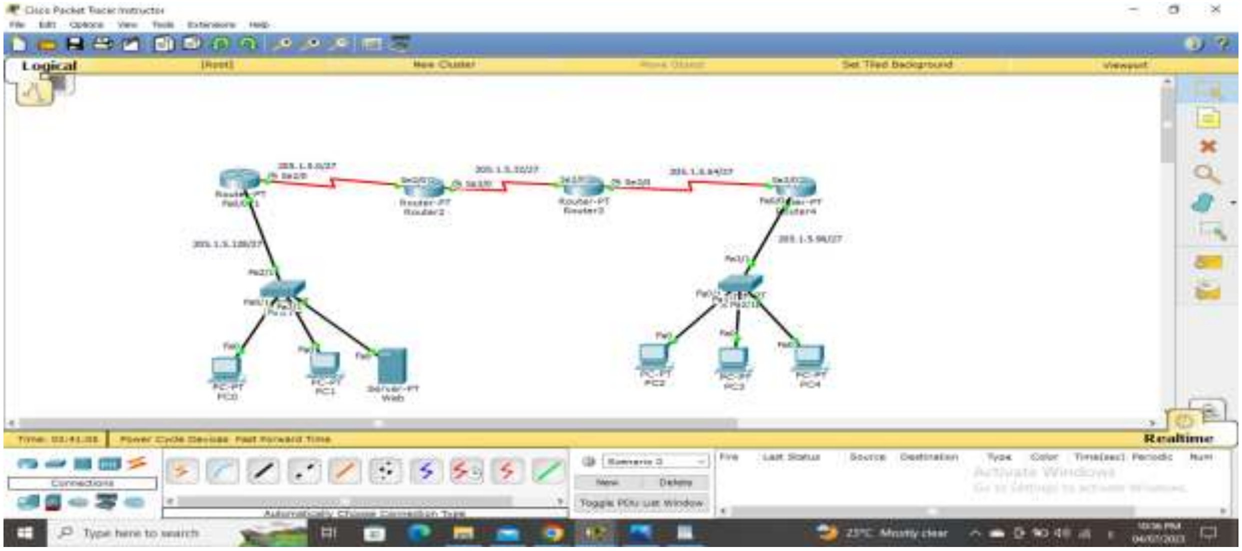
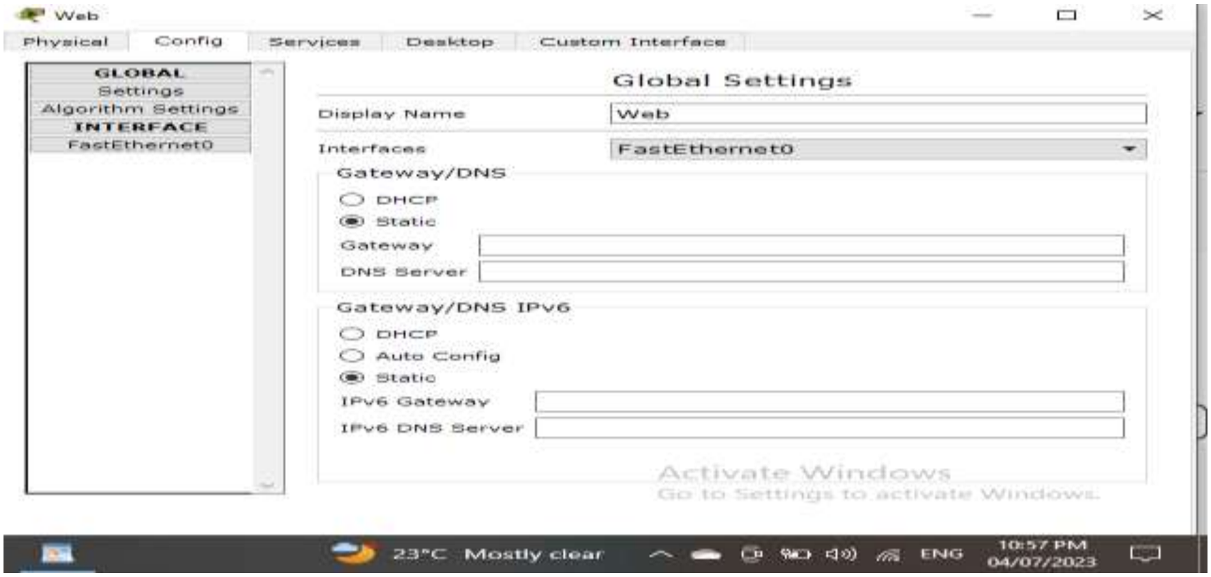


Figure 27: Ping after the OSPF routing protocol when add web server

Configure web:



Global Settings

Display Name: Web

Interfaces: FastEthernet0

Gateway/DNS

○ DHCP
● Static

Gateway:

DNS Server:

Gateway/DNS IPv6

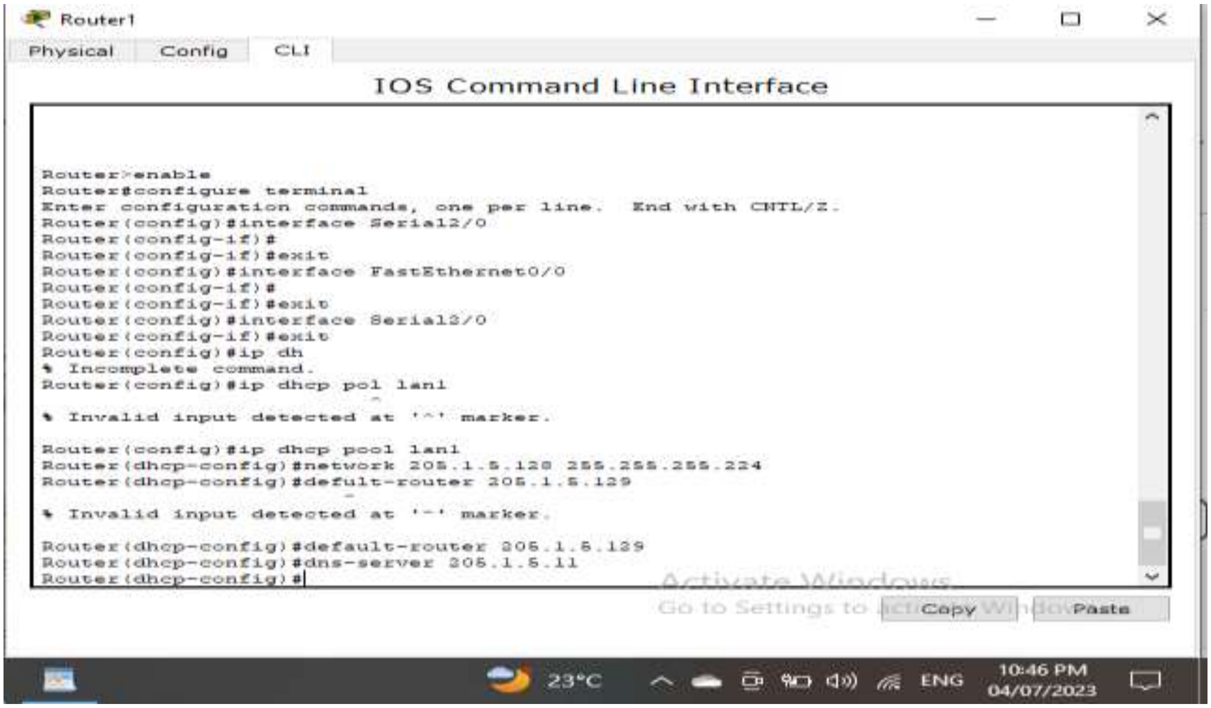
○ DHCP
○ Auto Config
● Static

IPv6 Gateway:

IPv6 DNS Server:

Figure 28: Ping after the OSPF routing protocol configure web

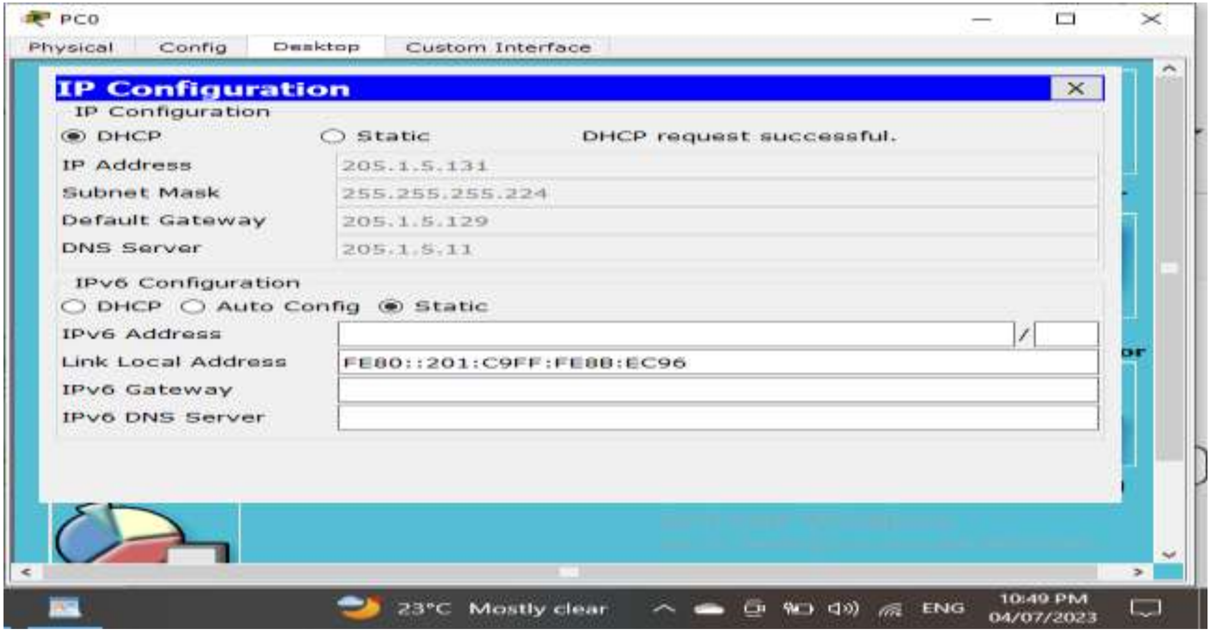
- **The network (Router1) contain a webserver and a DNS server**



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#exit
Router(config)#ip dh
% Incomplete command.
Router(config)#ip dhcp pol lan1
                         ^
% Invalid input detected at '^' marker.

Router(config)#ip dhcp pool lan1
Router(dhcp-config)#network 205.1.5.128 255.255.255.224
Router(dhcp-config)#defult-router 205.1.5.129
                       ^
% Invalid input detected at '^' marker.

Router(dhcp-config)#default-router 205.1.5.129
Router(dhcp-config)#dns-server 205.1.5.11
Router(dhcp-config)#
```

Figure 29: The network (Router1) contain a webserver and a DNS server

- **IP Configuration for PC0 (DHCP):**



IP Configuration

IP Configuration

● DHCP ○ Static DHCP request successful.

IP Address 205.1.5.131

Subnet Mask 255.255.255.224

Default Gateway 205.1.5.129

DNS Server 205.1.5.11

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

Link Local Address FE80::201:C9FF:FE8B:EC96

IPv6 Gateway

IPv6 DNS Server

Figure 30: IP Configuration for PC0 (DHCP)

DNS (Domain Name System) is an integral part of the internet infrastructure. It translates human-readable domain names into machine-readable IP addresses. This enables users to access websites and services using easy-to-remember domain names instead of complex IP addresses. When a user enters a domain name, a query is sent to a recursive DNS resolver, which contacts authoritative name servers to retrieve the corresponding IP address.

When add DNS server:

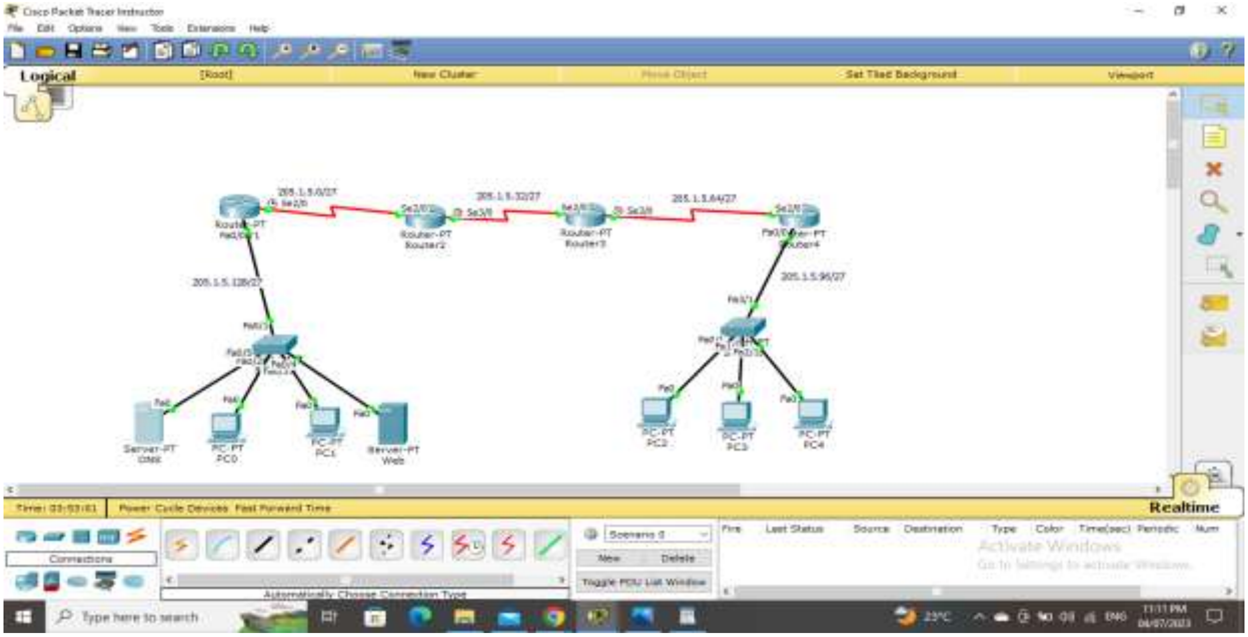
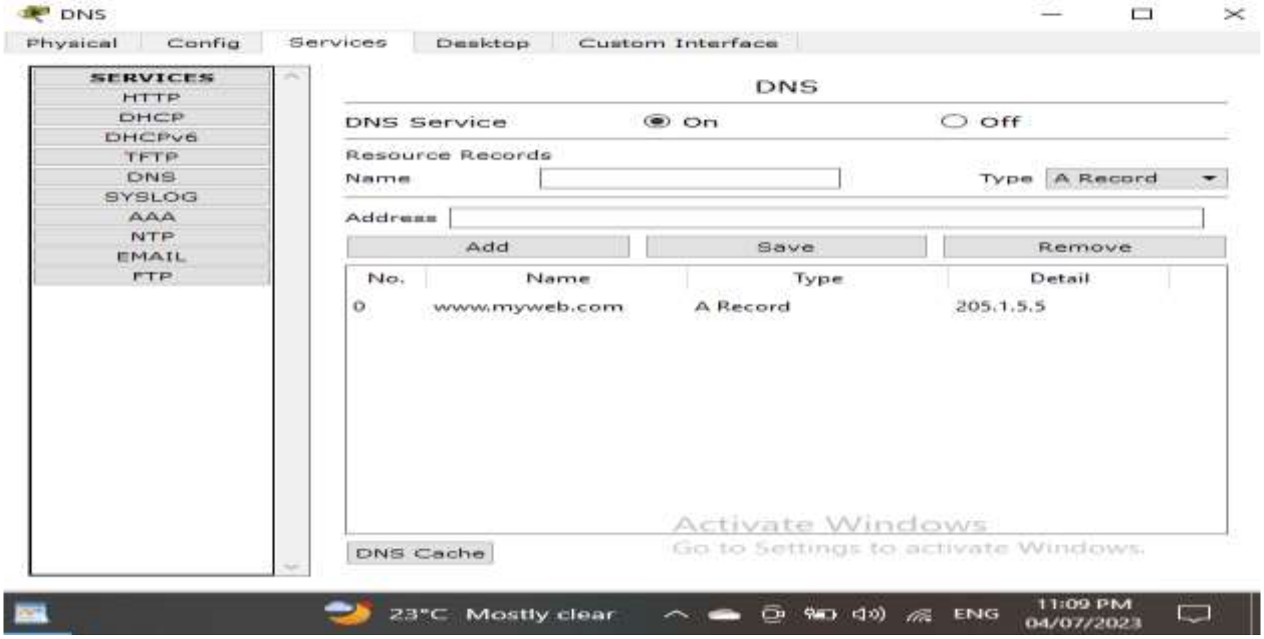


Figure 31: IP Configuration for PC0 (DHCP) when add DNS server

When activated DNS for the DNS server:



DNS

DNS Service ● On ○ Off

Resource Records

Name

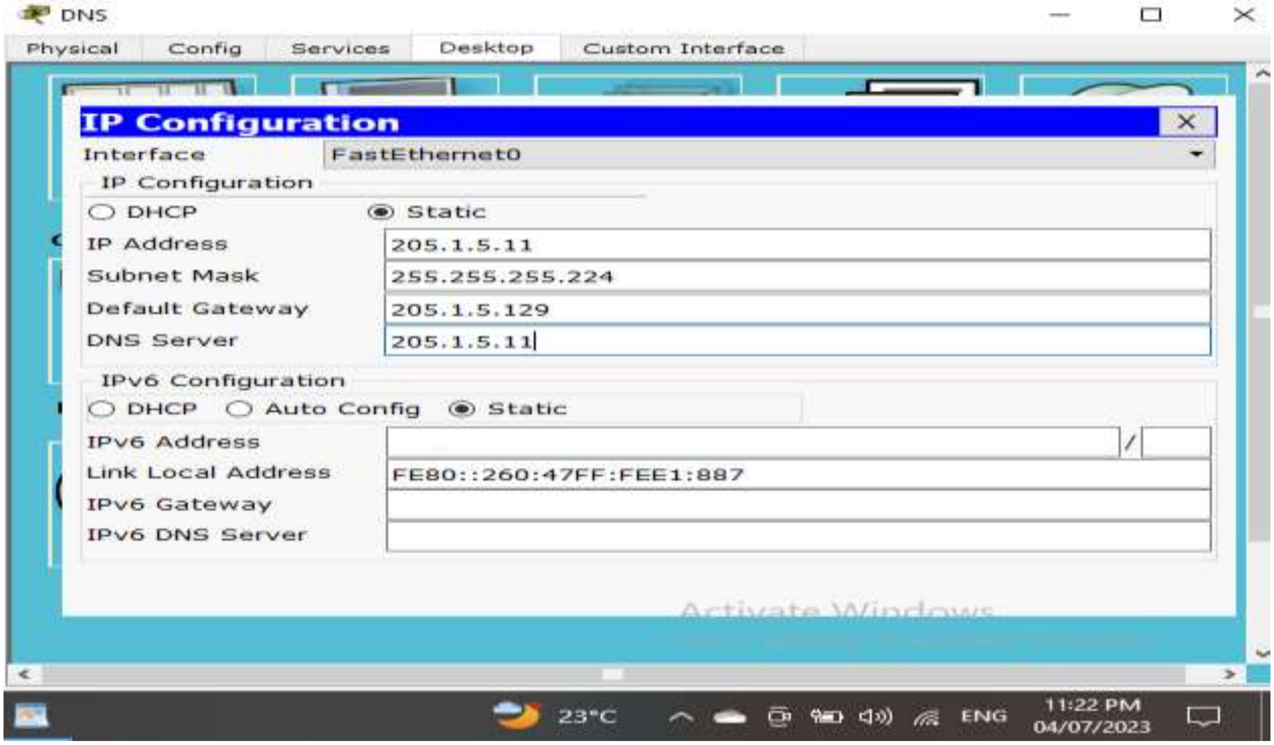
Type A Record

Address

No.	Name	Type	Detail
0	www.myweb.com	A Record	205.1.5.5

Figure 32: IP Configuration for PC0 (DHCP) when activated DNS

- **IP Configuration for DNS server:**



IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address 205.1.5.11

Subnet Mask 255.255.255.224

Default Gateway 205.1.5.129

DNS Server 205.1.5.11

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

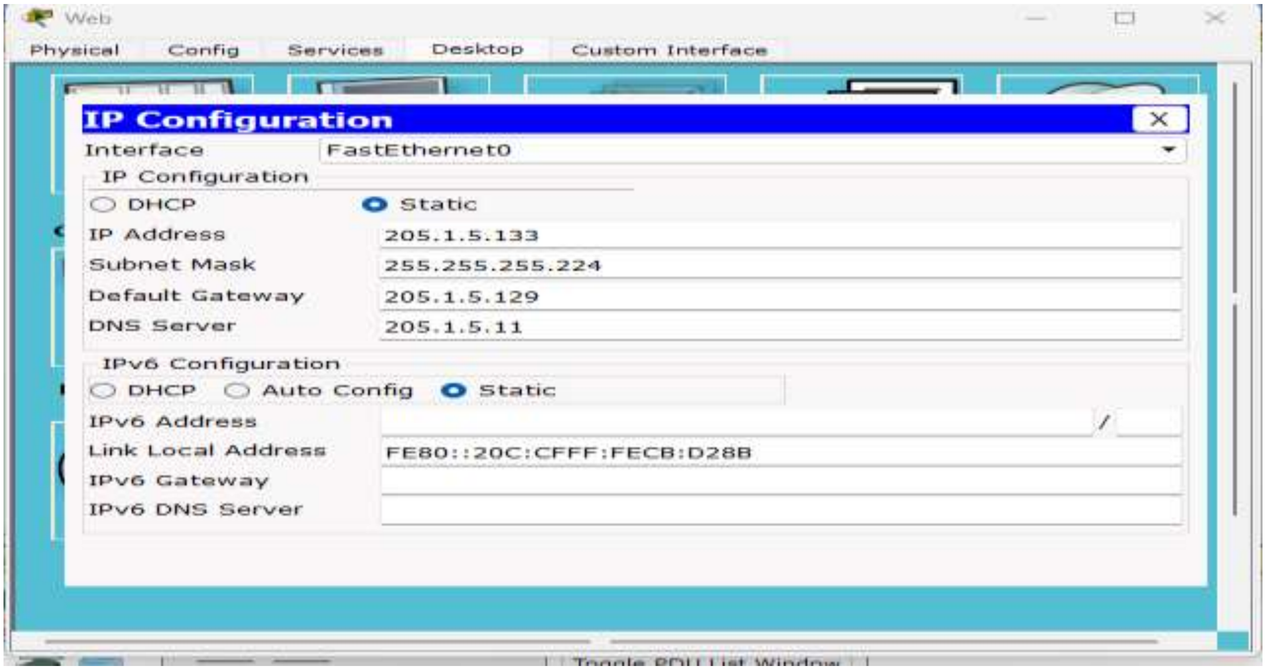
Link Local Address FE80::260:47FF:FEE1:887

IPv6 Gateway

IPv6 DNS Server

Figure 33: IP Configuration for DNS server

When activated DNS, IP Configuration for web server:



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 205.1.5.133

Subnet Mask: 255.255.255.224

Default Gateway: 205.1.5.129

DNS Server: 205.1.5.11

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

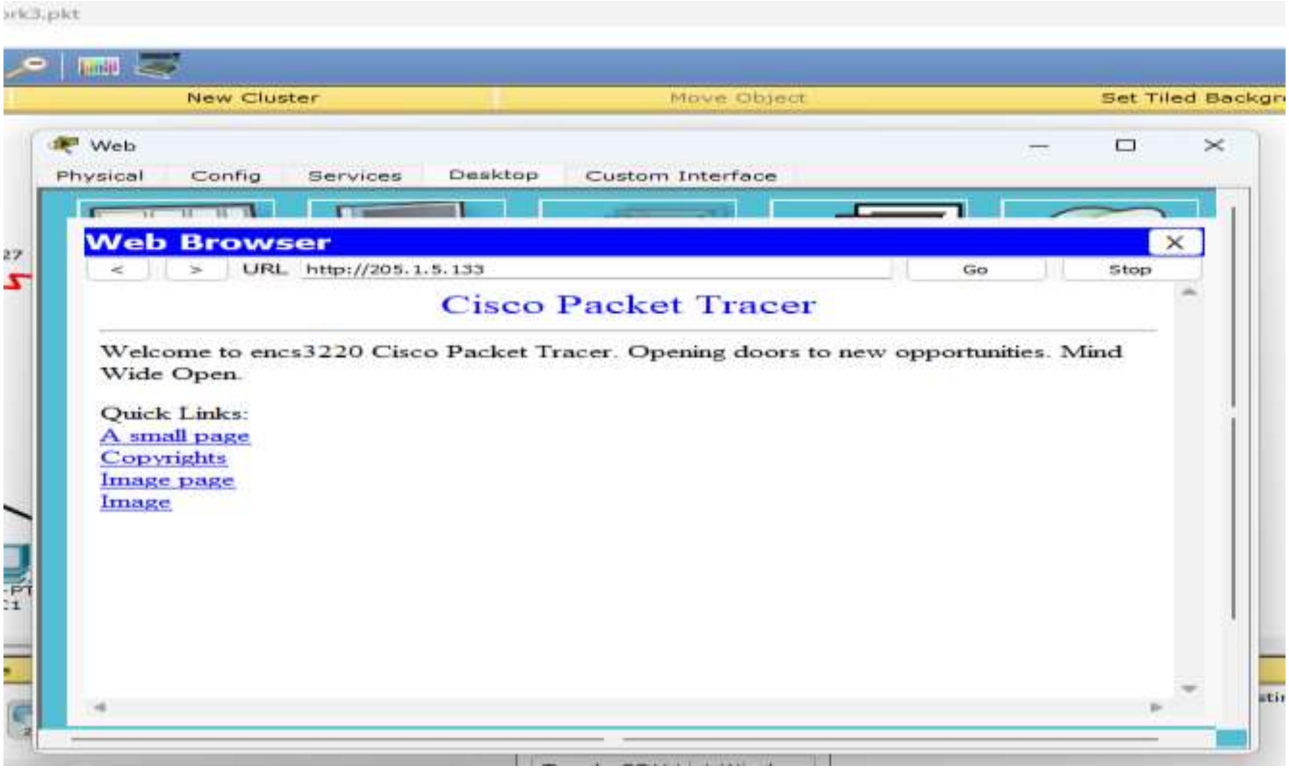
Link Local Address: FE80::20C:CFFF:FECB:D28B

IPv6 Gateway:

IPv6 DNS Server:

Figure 34: IP Configuration for web server when activated DNS

- **Web browser for PC0**



URL http://205.1.5.133

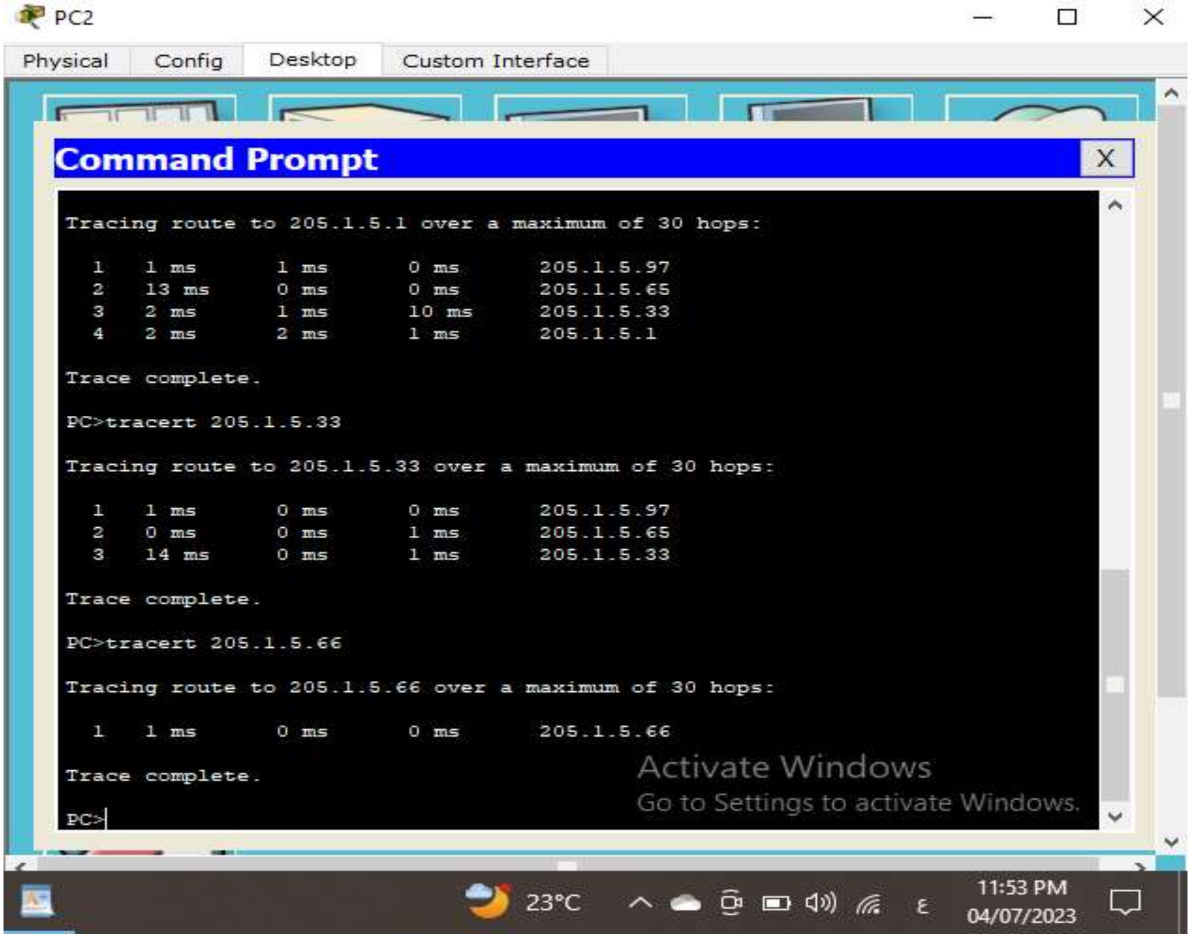
Cisco Packet Tracer

Welcome to encs3220 Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Figure 35: web browser for PC0

When we used tracert command for PC2 to show the path a packet traversed to reach its destination from each subnet host to a remote destination.



```
Tracing route to 205.1.5.1 over a maximum of 30 hops:

  1   1 ms      1 ms      0 ms      205.1.5.97
  2   13 ms     0 ms      0 ms      205.1.5.65
  3   2 ms      1 ms      10 ms     205.1.5.33
  4   2 ms      2 ms      1 ms      205.1.5.1

Trace complete.

PC>tracert 205.1.5.33

Tracing route to 205.1.5.33 over a maximum of 30 hops:

  1   1 ms      0 ms      0 ms      205.1.5.97
  2   0 ms      0 ms      1 ms      205.1.5.65
  3   14 ms     0 ms      1 ms      205.1.5.33

Trace complete.

PC>tracert 205.1.5.66

Tracing route to 205.1.5.66 over a maximum of 30 hops:

  1   1 ms      0 ms      0 ms      205.1.5.66

Trace complete.

PC>
```