جامعة بيرزيت

BIRZEIT UNIVERSITY

Faculty of Engineering & Technology
Electrical & Computer Engineering Department

Computer Networks- ENCS3320

Project#2

Packet Tracer & WireShark

Prepared by:

Abd Khuffash – 1200970

Sami Moqbel – 1200751

Saad Alahmad – 1190326

Raed Al-Adhami – 1180052

Instructor:
Abdalkarim Awad

Section:
1

Date:25-6-2023

Abstract/Objectives

The objective of this project is to gain a comprehensive understanding of the key networking concepts and protocols, specifically DHCP, DNS, and ICMP. Additionally, the objective is to develop practical skills in using Wireshark software to analyze network packets and interpret relevant fields within DHCP, DNS, and ICMP packets. Furthermore, the objective is to design and implement a network using Packet Tracer, incorporating OSPF routing protocol, DHCP, a web server, and a DNS server. The objective also includes configuring proper IP addressing and subnetting based on the university ID, as well as demonstrating connectivity between hosts using the ping command and tracing the path of packets using the tracert command. By achieving these objectives, students will enhance their knowledge of computer networks and gain hands-on experience in network configuration and troubleshooting.

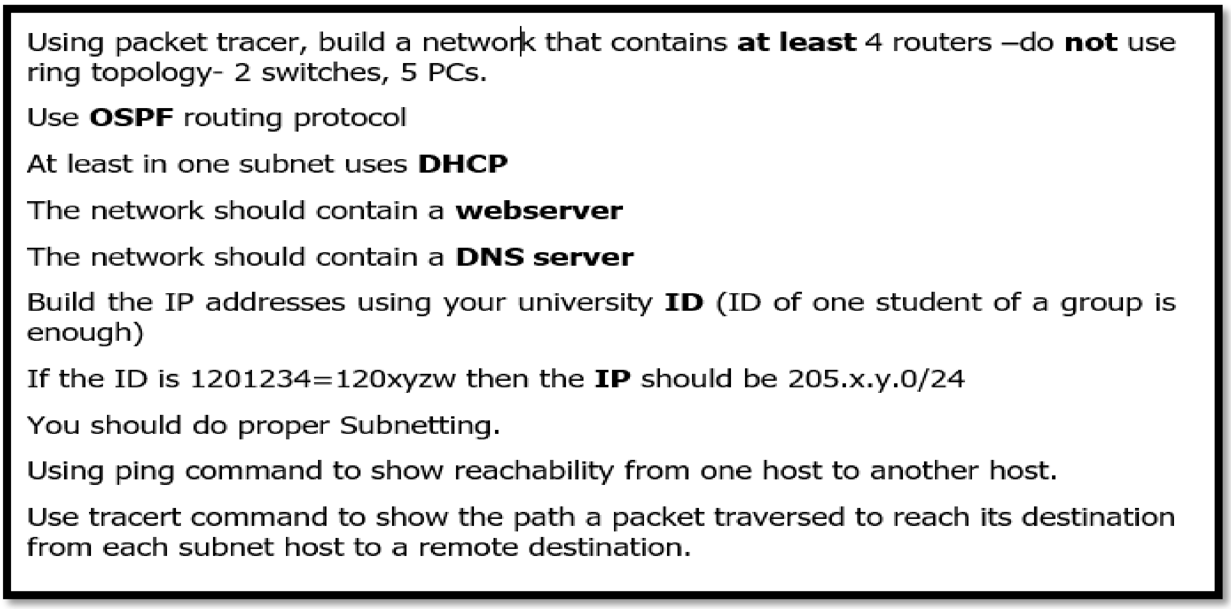
Table of Contents

Contents

Table Of Figures

Procedure

Part 2:



Using packet tracer, build a network that contains **at least** 4 routers –do **not** use ring topology- 2 switches, 5 PCs.

Use **OSPF** routing protocol

At least in one subnet uses **DHCP**

The network should contain a **webserver**

The network should contain a **DNS server**

Build the IP addresses using your university **ID** (ID of one student of a group is enough)

If the ID is 1201234=120xyzw then the **IP** should be 205.x.y.0/24

You should do proper Subnetting.

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

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

Figure 1. Question 2

According to the specification above , 5 PCs , 4 routers(3*2901 , 1 *2811) ,2 switches(2950-24) were used.

At first, PC0, PC1,PC2,PC3 are connected to switch0, switch0 is connected to router0, router0 is connected to router1, router1 is connect to both router2, and router 3, router 3 is connected to switch1 which is connected with PC5.

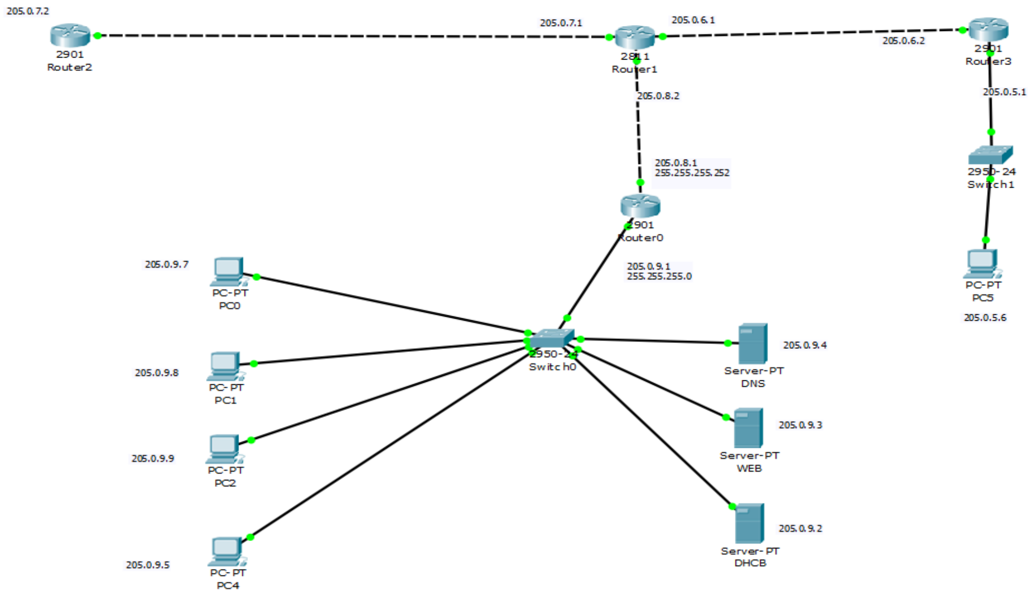


Figure 2.Topology

Starting with this Section:

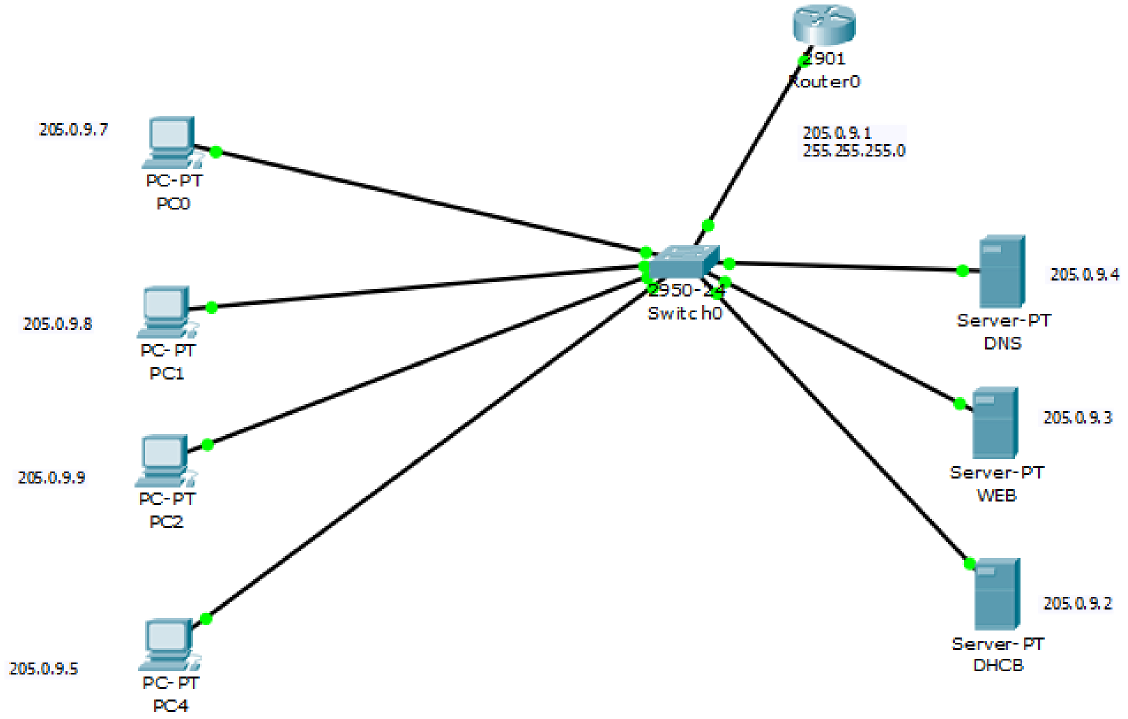
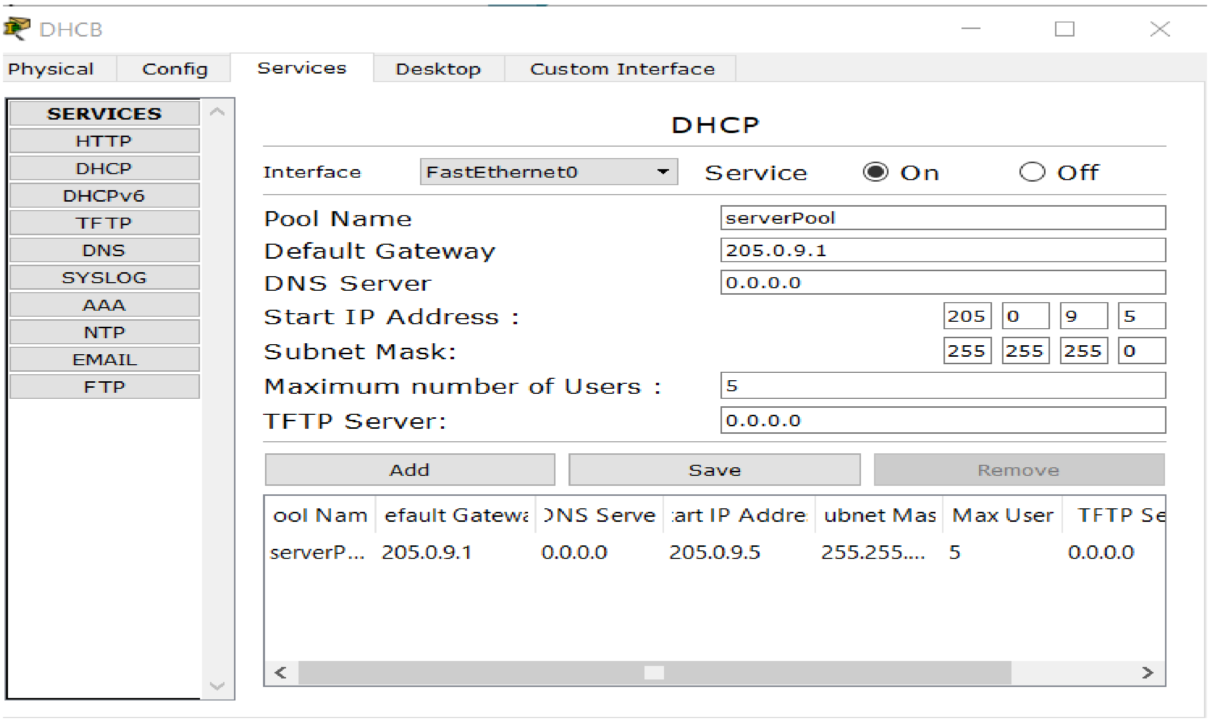


Figure 3.DHCP

Each PC has its IP automatically using DHCP Protocol, DHCP server is connected to switch0 ,first IP starts at 205.0.9.5\24 , maximum number of users are 5, as shown in figure 4:



DHCP

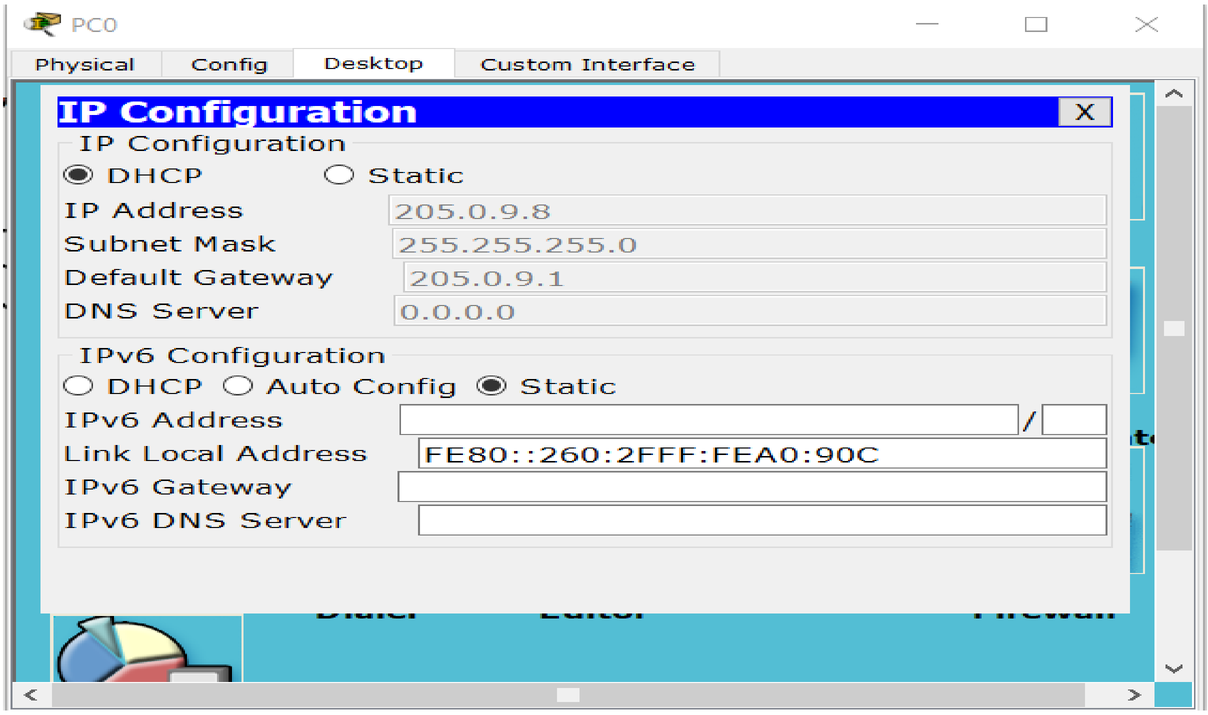
Interface FastEthernet0 Service ● On ○ Off

Pool Name	serverPool
Default Gateway	205.0.9.1
DNS Server	0.0.0.0
Start IP Address :	205 0 9 5
Subnet Mask:	255 255 255 0
Maximum number of Users :	5
TFTP Server:	0.0.0.0

ool Nam	efault Gatewa	ONS Serve	art IP Addre	ubnet Mas	Max User	TFTP Se
serverP...	205.0.9.1	0.0.0.0	205.0.9.5	255.255....	5	0.0.0.0

Figure 4.DHCP

PC IPS :

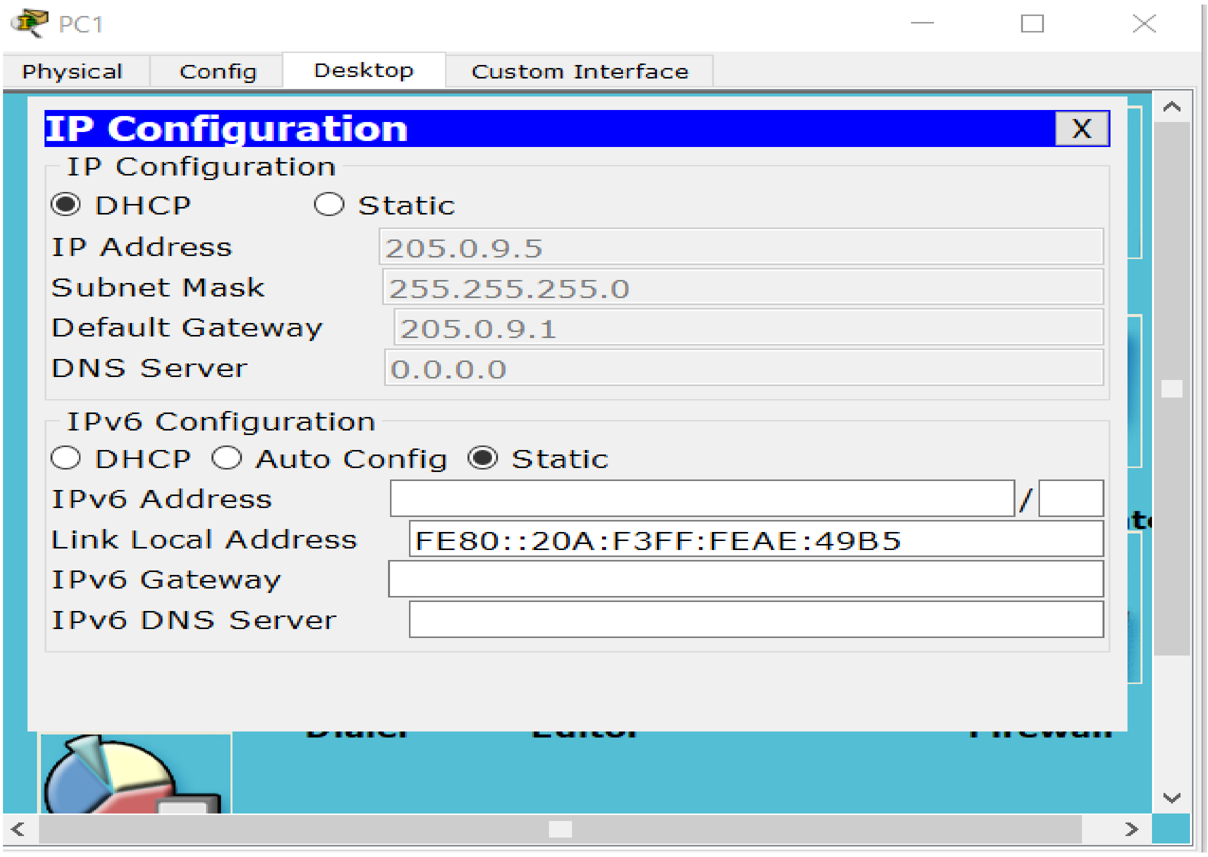


IP Configuration

IP Configuration
● DHCP ○ Static
IP Address 205.0.9.8
Subnet Mask 255.255.255.0
Default Gateway 205.0.9.1
DNS Server 0.0.0.0

IPv6 Configuration
○ DHCP ○ Auto Config ● Static
IPv6 Address /
Link Local Address FE80::260:2FFF:FEA0:90C
IPv6 Gateway
IPv6 DNS Server

Figure 5.PC0 IP

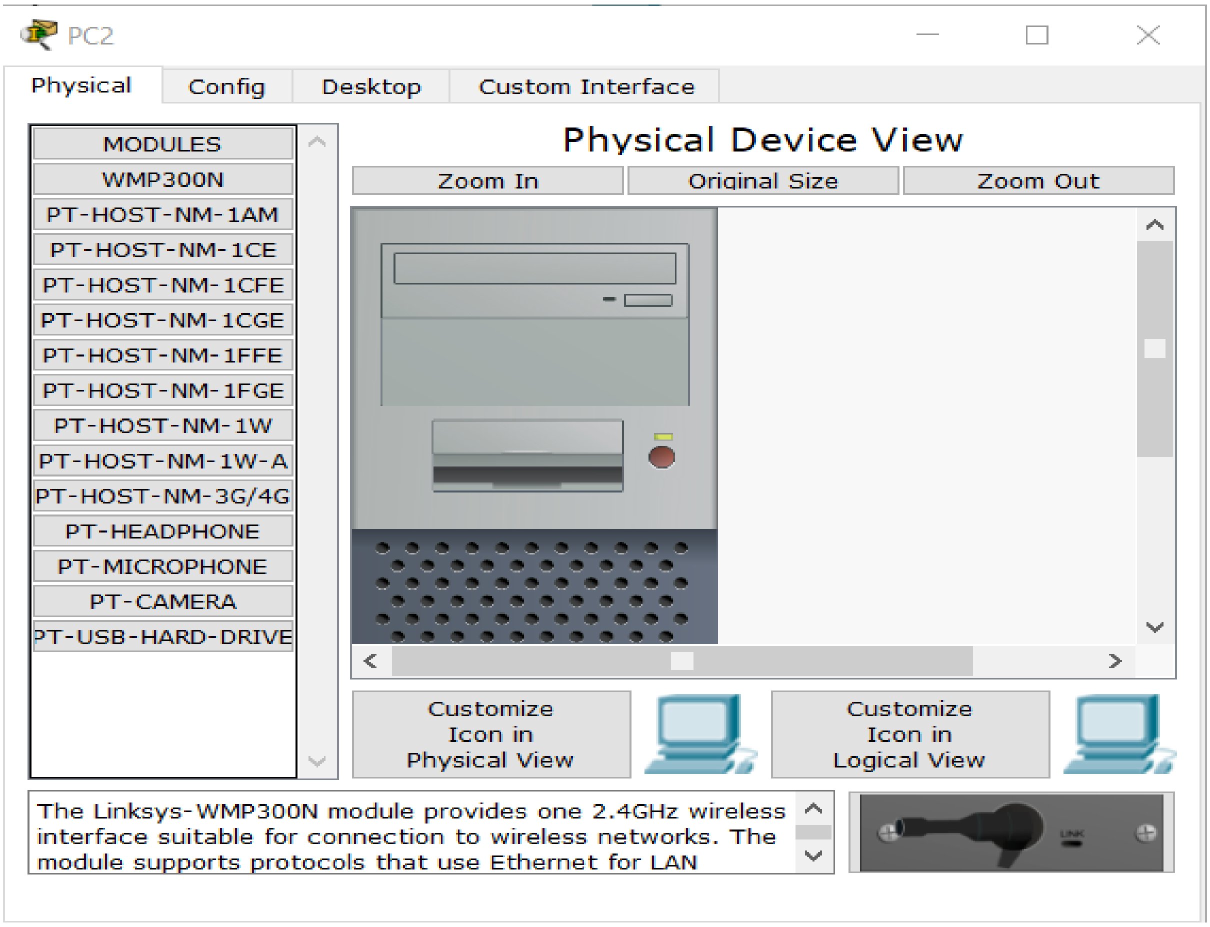


IP Configuration

IP Configuration
● DHCP ○ Static
IP Address 205.0.9.5
Subnet Mask 255.255.255.0
Default Gateway 205.0.9.1
DNS Server 0.0.0.0

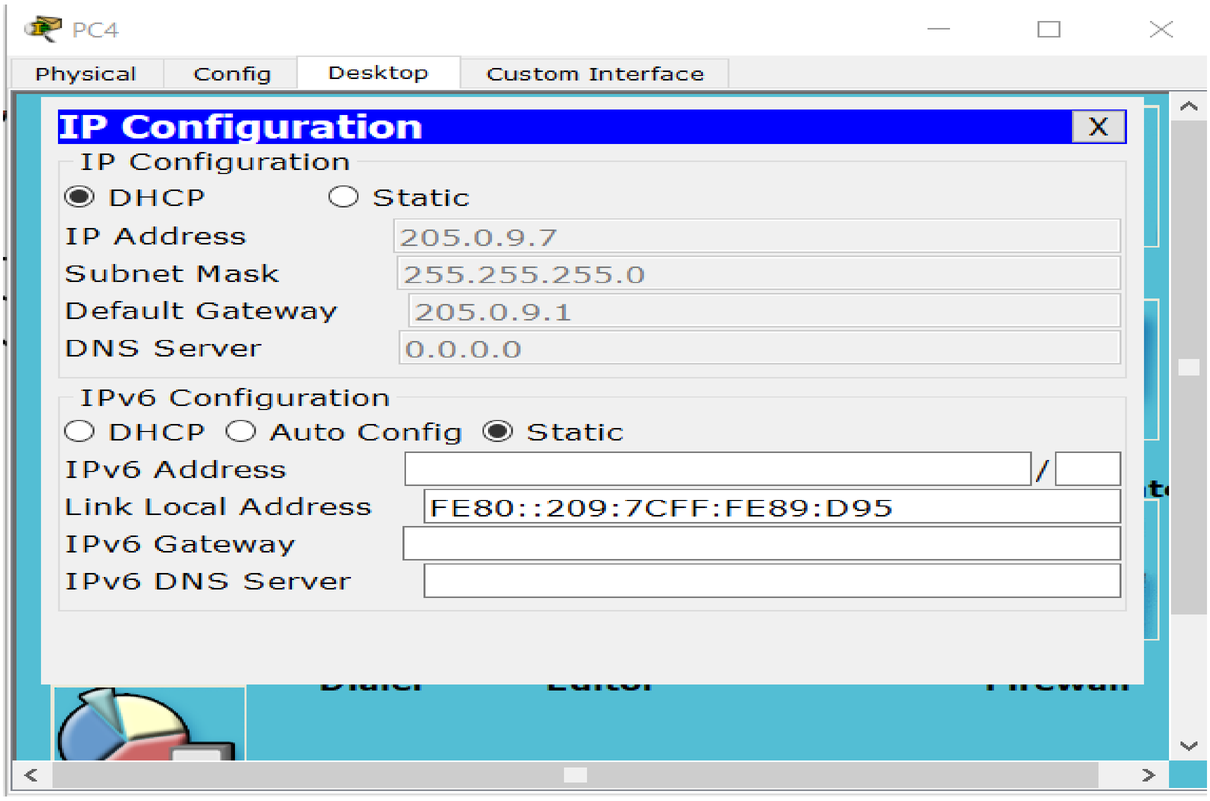
IPv6 Configuration
○ DHCP ○ Auto Config ● Static
IPv6 Address /
Link Local Address FE80::20A:F3FF:FEAE:49B5
IPv6 Gateway
IPv6 DNS Server

Figure 6.PC1 IP



The Linksys-WMP300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN

Figure 7.PC2



IP Configuration

IP Configuration

● DHCP ○ Static

IP Address 205.0.9.7

Subnet Mask 255.255.255.0

Default Gateway 205.0.9.1

DNS Server 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

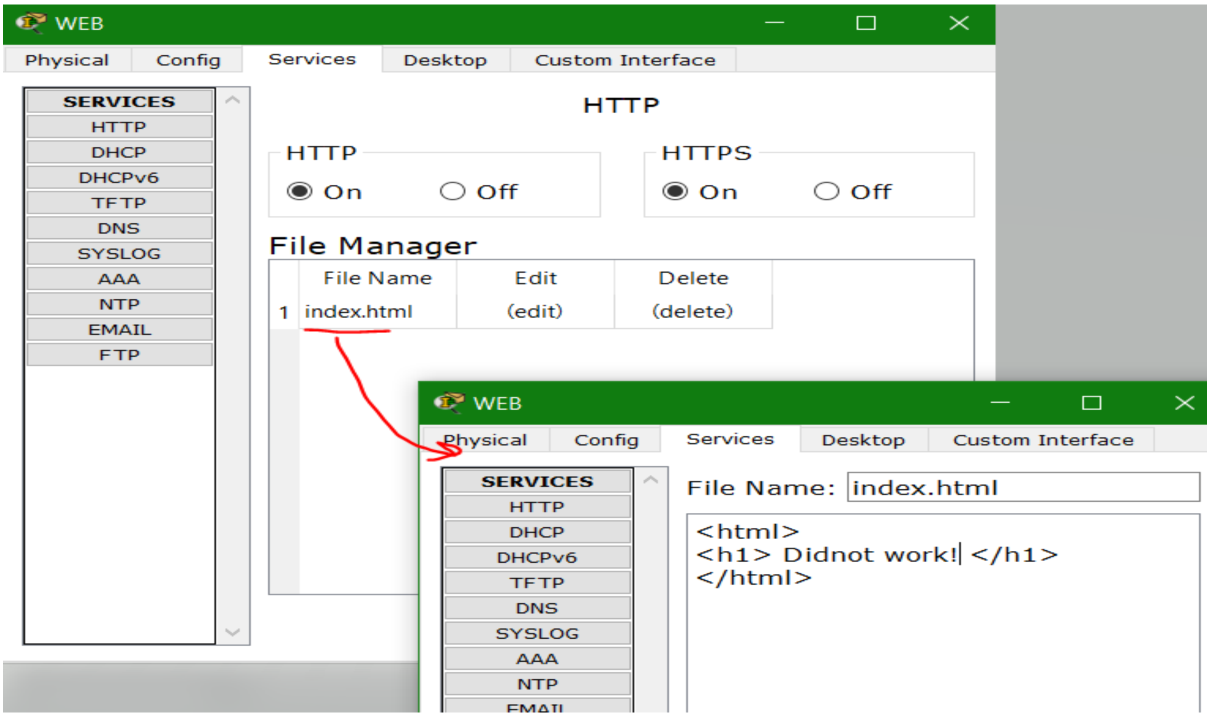
Link Local Address FE80::209:7CFF:FE89:D95

IPv6 Gateway

IPv6 DNS Server

Figure 8.PC4 IP

About other components connected with switch0, Web Server (HTTP) -could been done with the same component in DHCP- , HTTP service was selected , HTML file was made, as shown in figure 9:



HTTP

HTTP: ● On ○ Off

HTTPS: ● On ○ Off

File Manager

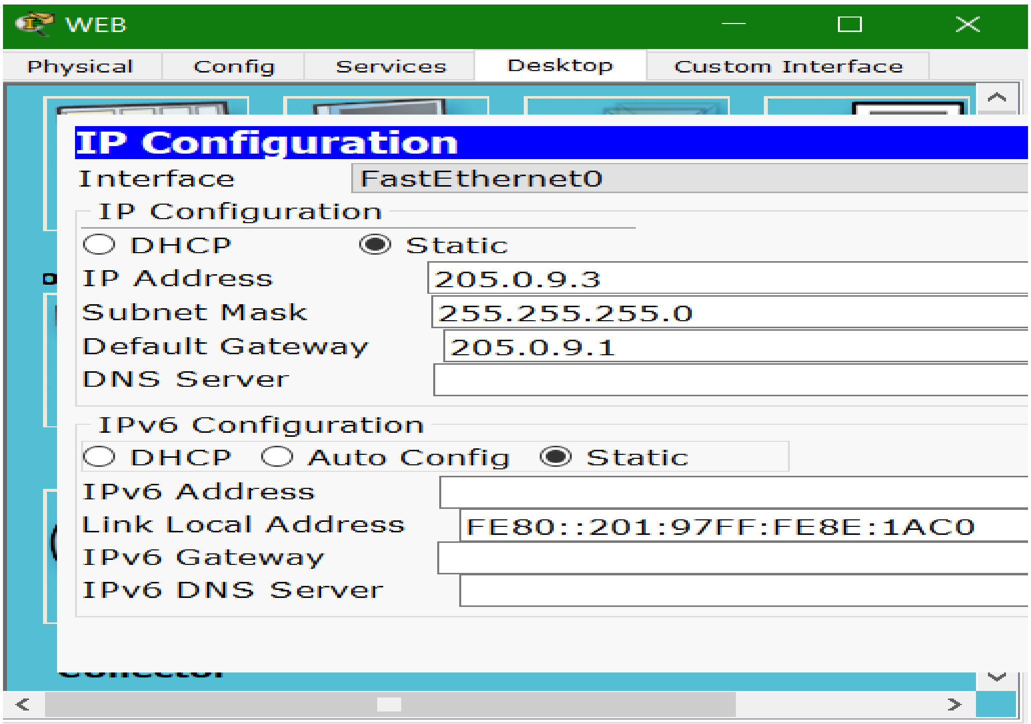
	File Name	Edit	Delete
1	index.html	(edit)	(delete)

File Name: index.html

```
<html>
<h1> Didnot work!| </h1>
</html>
```

Figure 9.Web Server

The IP configuration:



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 205.0.9.3

Subnet Mask: 255.255.255.0

Default Gateway: 205.0.9.1

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address:

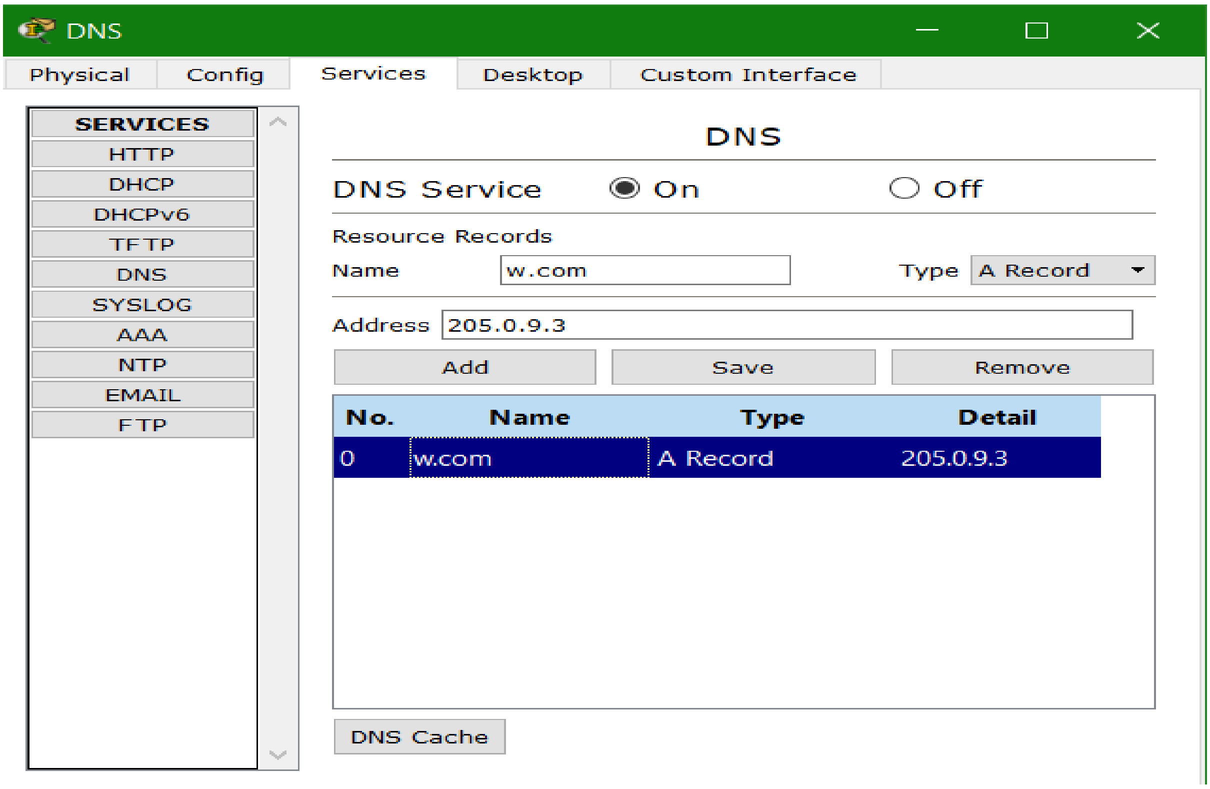
Link Local Address: FE80::201:97FF:FE8E:1AC0

IPv6 Gateway:

IPv6 DNS Server:

Figure 10.WEB Ips

DNS :



DNS

DNS Service ● On ○ Off

Resource Records

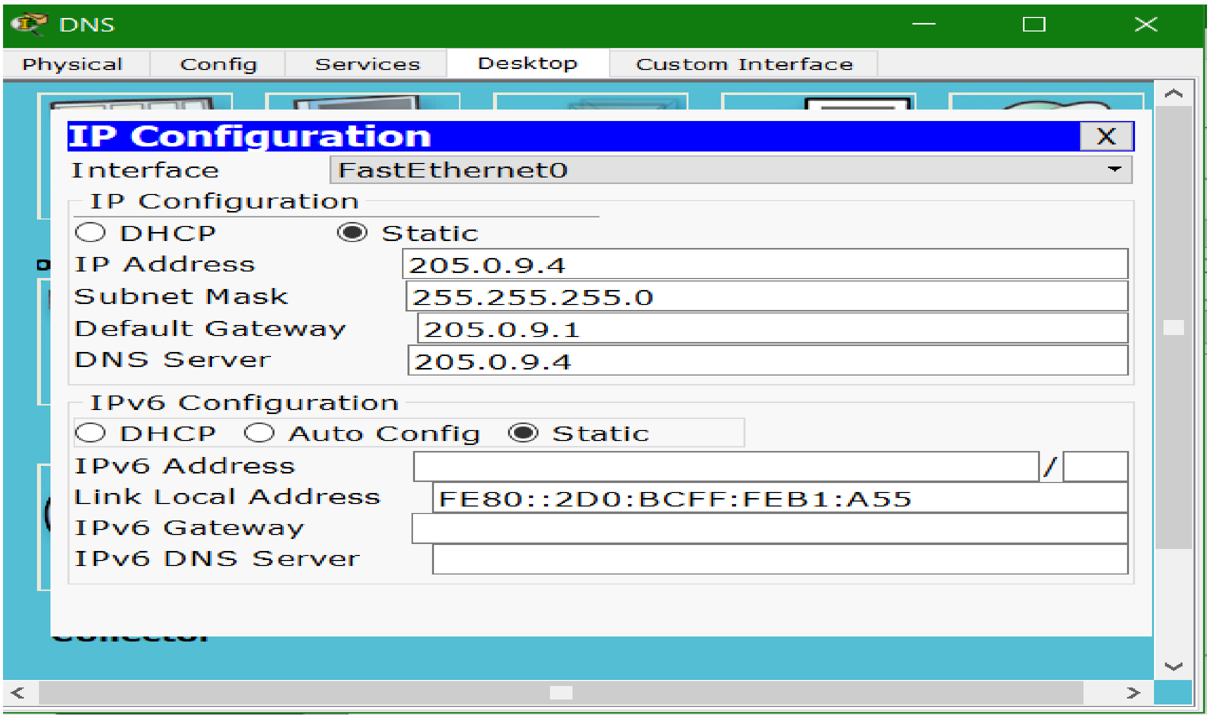
Name w.com Type A Record

Address 205.0.9.3

No.	Name	Type	Detail
0	w.com	A Record	205.0.9.3

Figure 11.DNS

IP Configuration:



IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address 205.0.9.4

Subnet Mask 255.255.255.0

Default Gateway 205.0.9.1

DNS Server 205.0.9.4

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

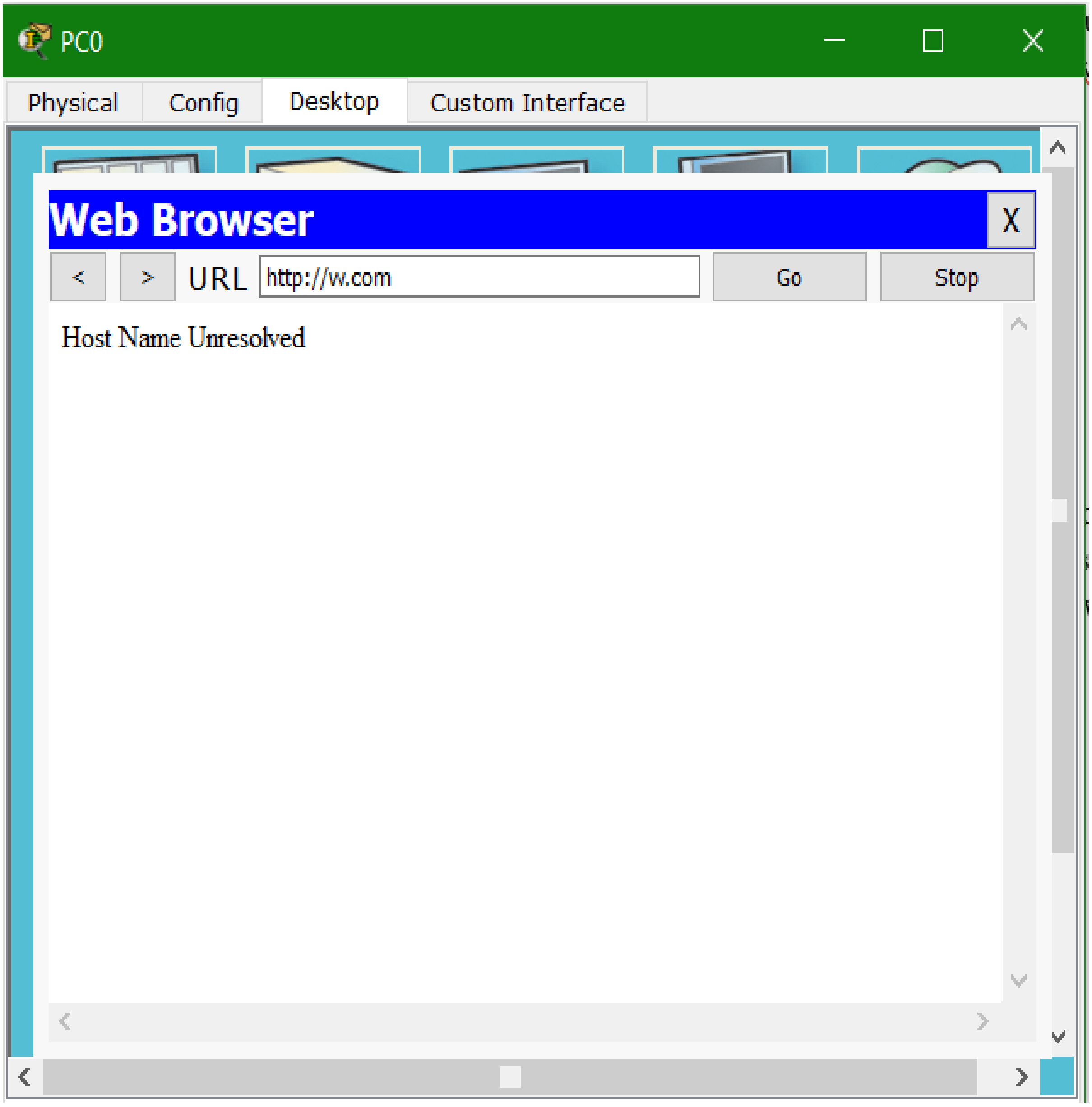
Link Local Address FE80::2D0:BCFF:FEB1:A55

IPv6 Gateway

IPv6 DNS Server

Figure 12.DNS IP

Sadly The DNS/WebServer didn’t work , whenever we try to load the web server its just “ host name unresolved” , we did everything as the tutorials done, but when I ping DNS/WEBServer Component it gives a response.

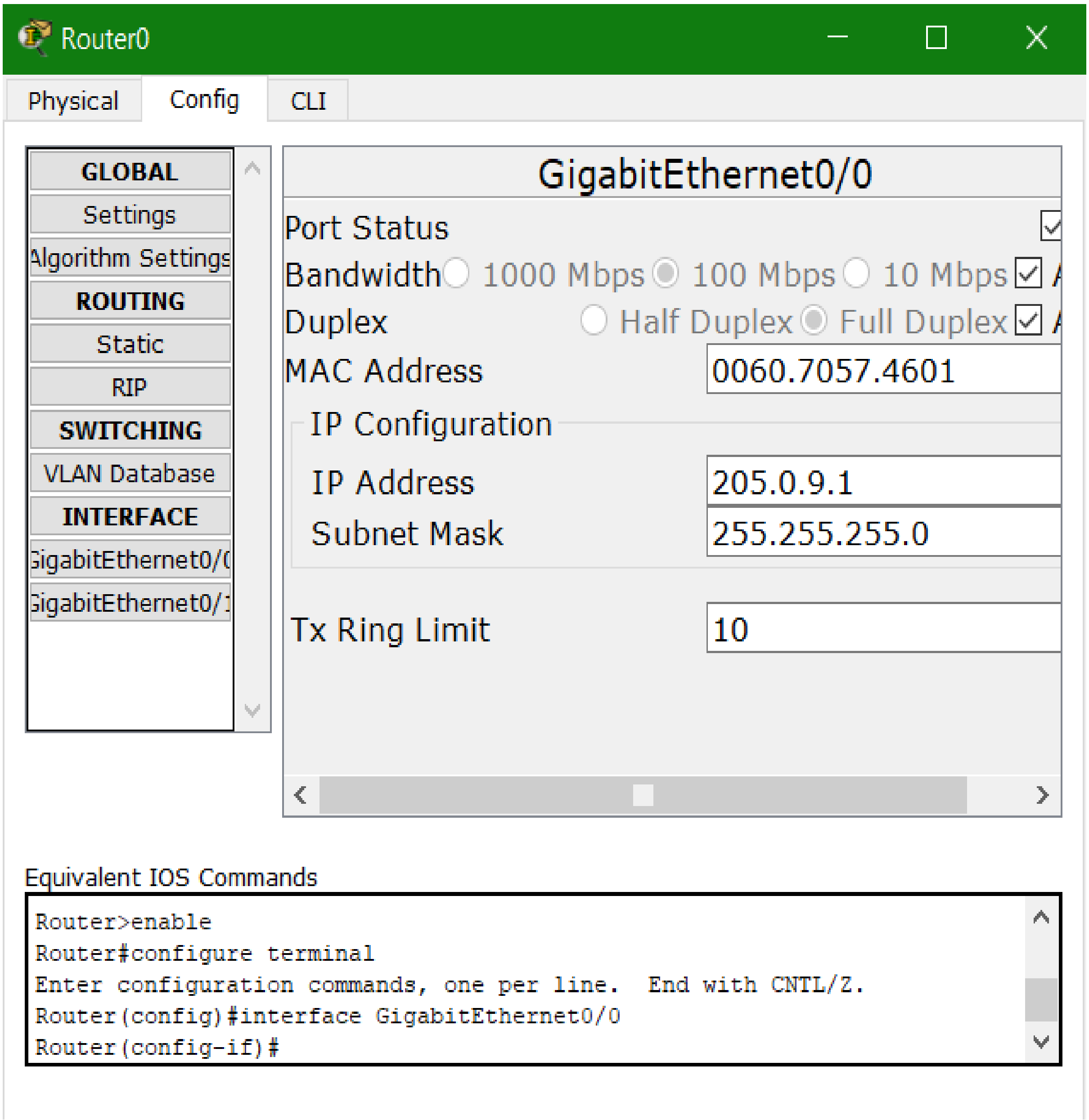


http://w.com

Host Name Unresolved

Figure 13.Error DNS/WEB

Moving on To rounter0, switch0 is connected to rounter0 in GigabitEthernet0/0 and here it's settings:



GigabitEthernet0/0

Port Status ☑

Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ A

Duplex ○ Half Duplex ● Full Duplex ☑ A

MAC Address 0060.7057.4601

IP Configuration

IP Address 205.0.9.1

Subnet Mask 255.255.255.0

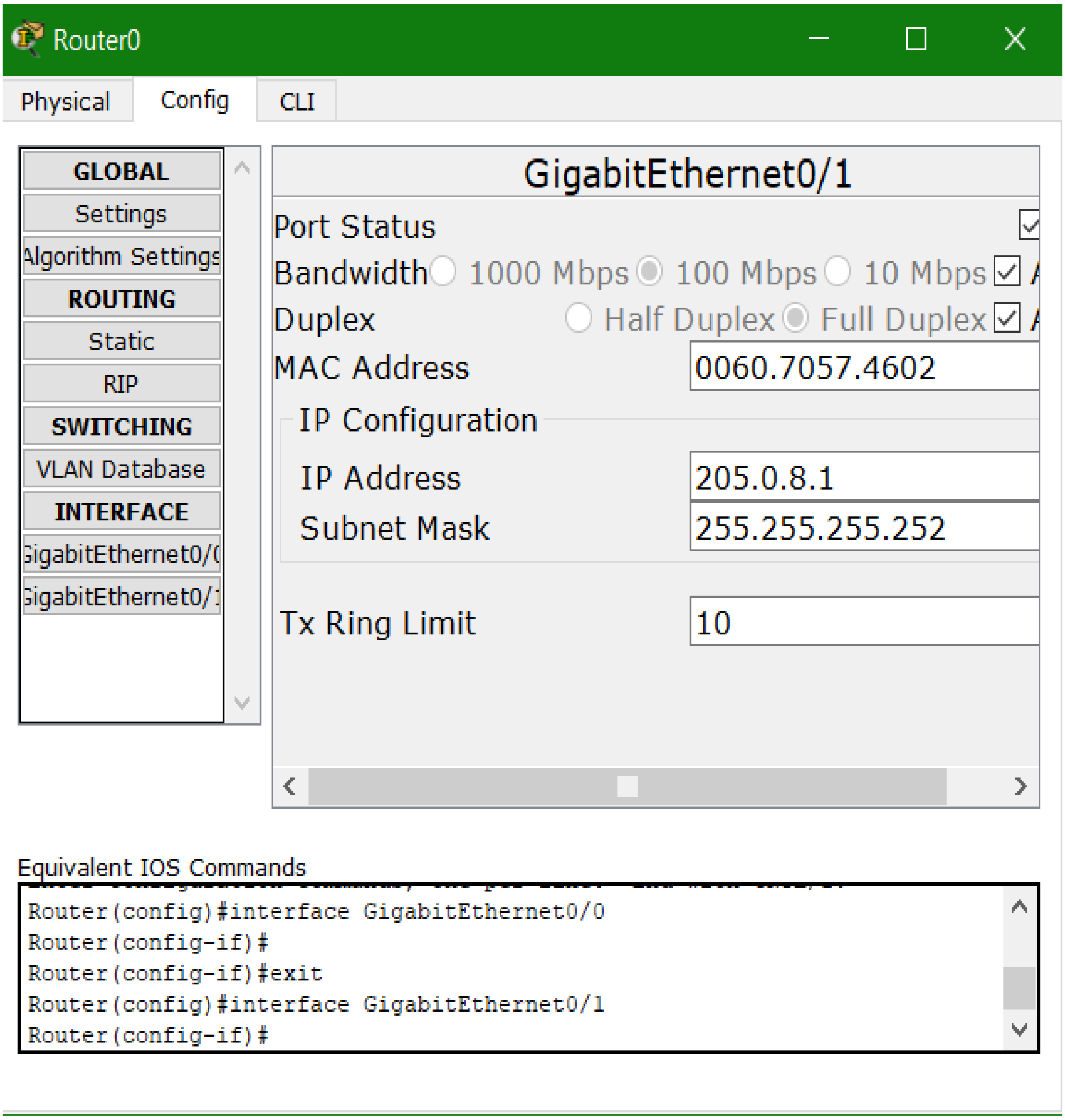
Tx Ring Limit 10

Equivalent IOS Commands

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```

Figure 14.Rounter0 with Swtich0

Router 1 is connected with rounter0 in gigabitEtherenet0/1 and here it’s settings:



GigabitEthernet0/1

Port Status ☑

Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ A

Duplex ○ Half Duplex ● Full Duplex ☑ A

MAC Address 0060.7057.4602

IP Configuration

IP Address 205.0.8.1

Subnet Mask 255.255.255.252

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
```

Figure 15.Router0-Router1

Moving to Router 1 , router 1 has 2 other connection ,which results in adding a module to enable 3 connections:

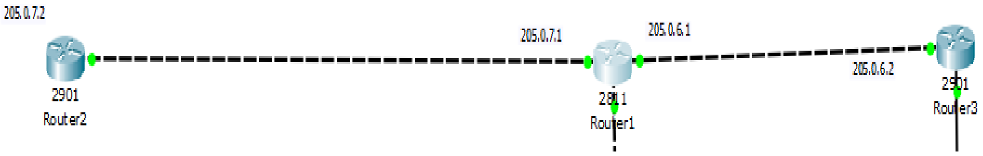
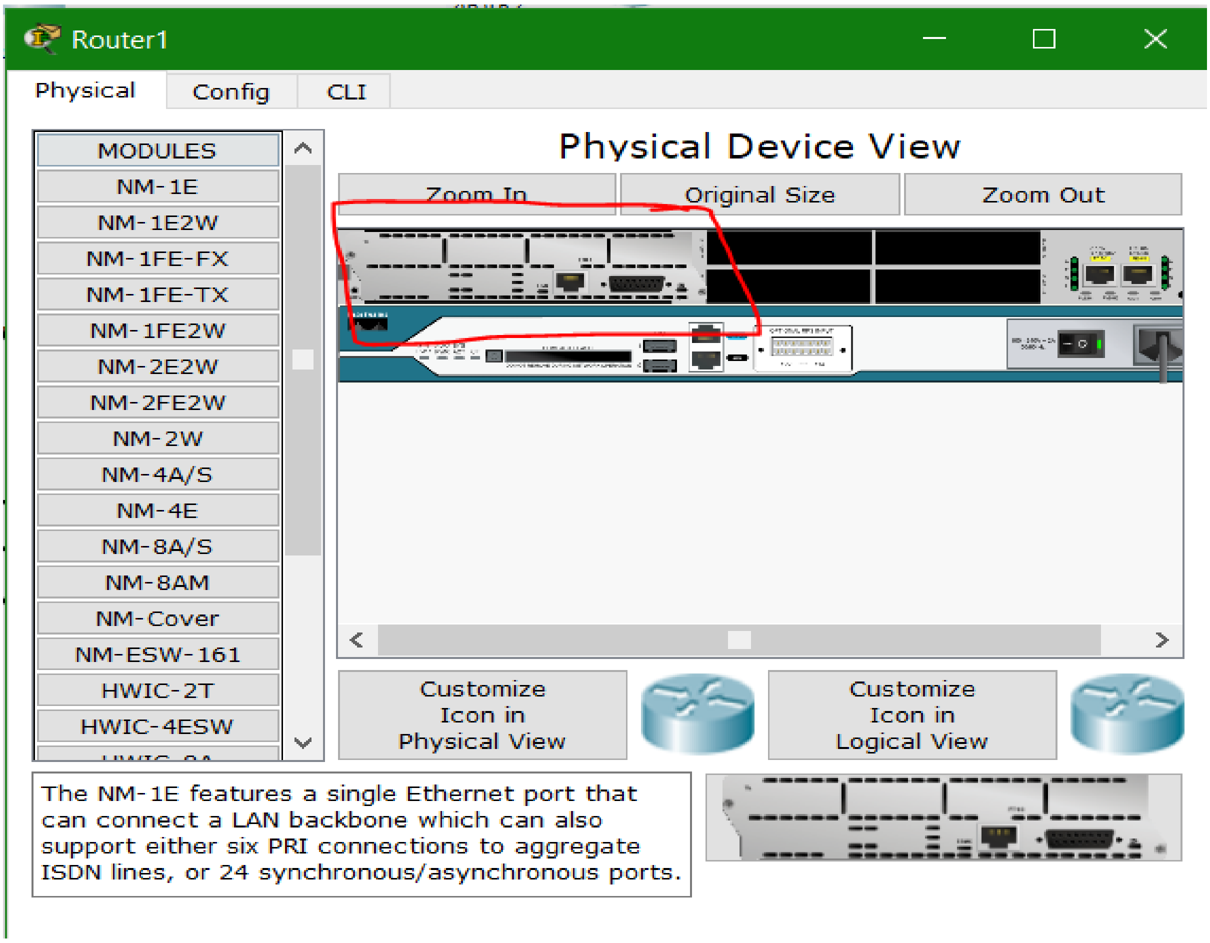


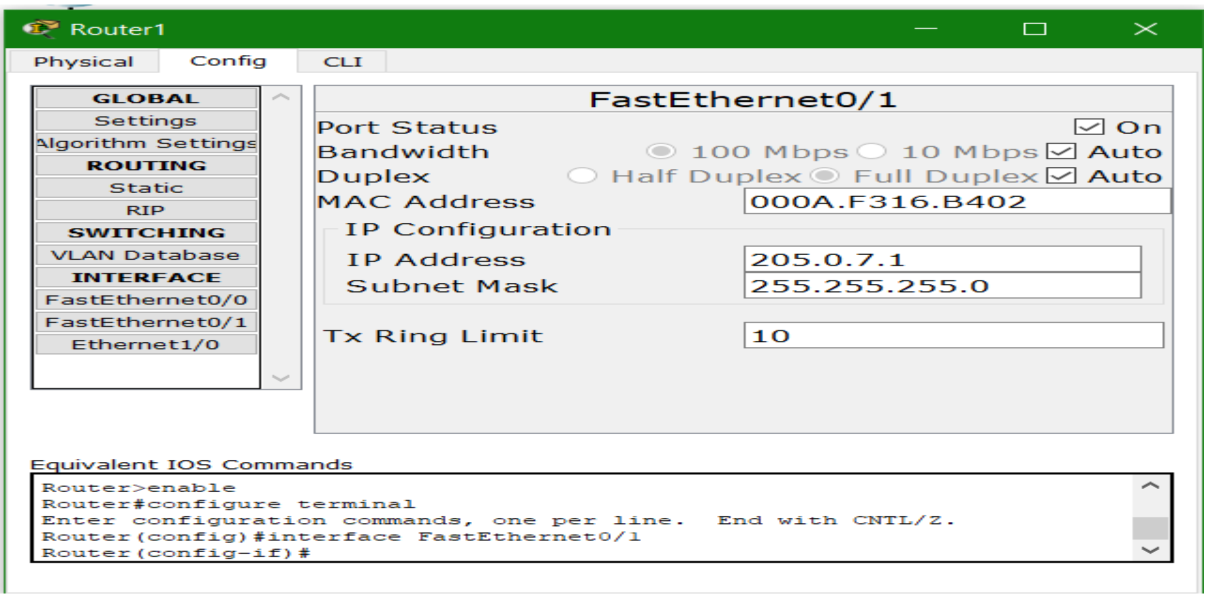
Figure 16.Router 1 Connections



The NM-1E features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.

Figure 17.Router1 Added Module

Connection between router1 and router 2 :



FastEthernet0/1

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 000A.F316.B402

IP Configuration

IP Address 205.0.7.1

Subnet Mask 255.255.255.0

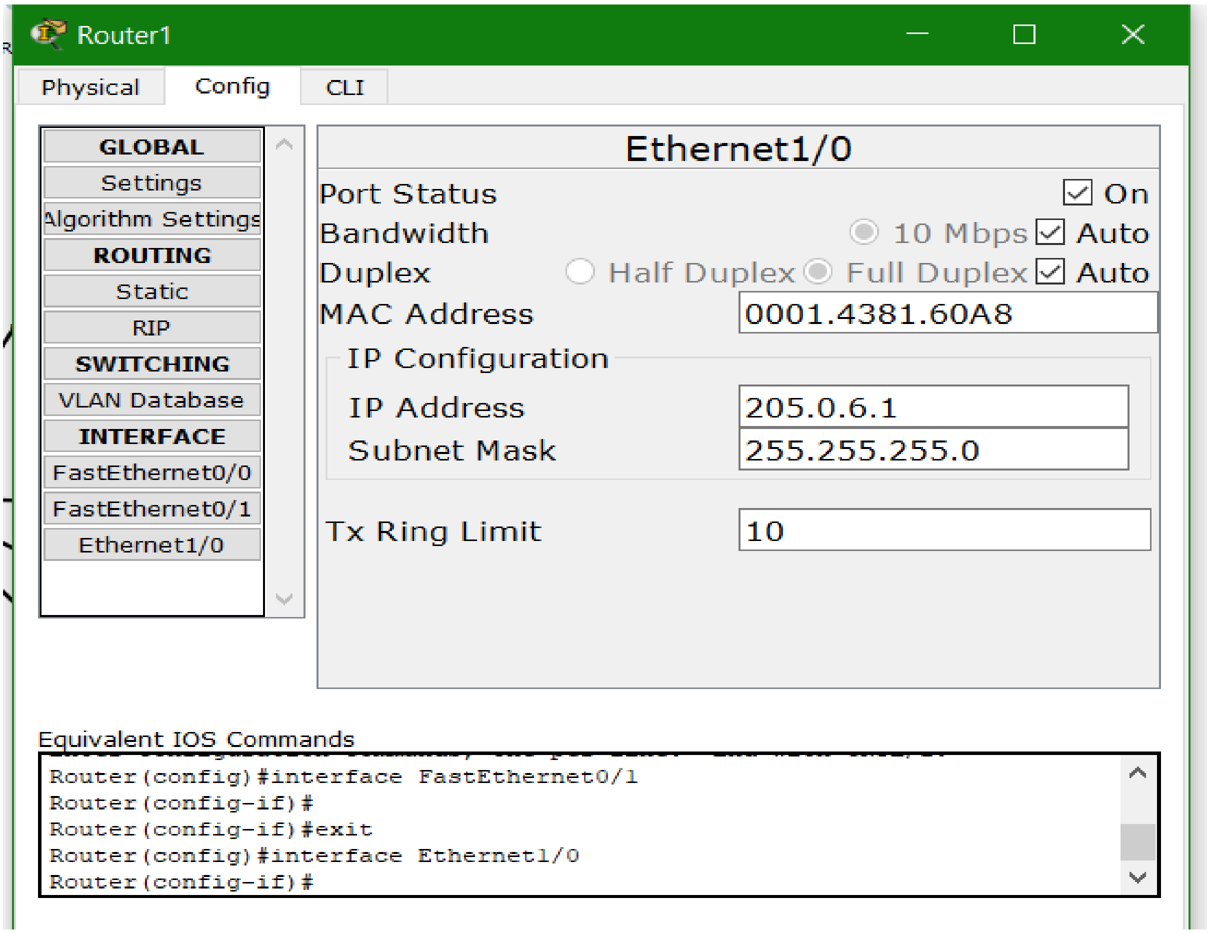
Tx Ring Limit 10

Equivalent IOS Commands

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/1
Router(config-if)#
```

Figure 18.Router1-2

The Other Connection is to router 3:



Ethernet1/0

Port Status ☑ On

Bandwidth ● 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0001.4381.60A8

IP Configuration

IP Address 205.0.6.1

Subnet Mask 255.255.255.0

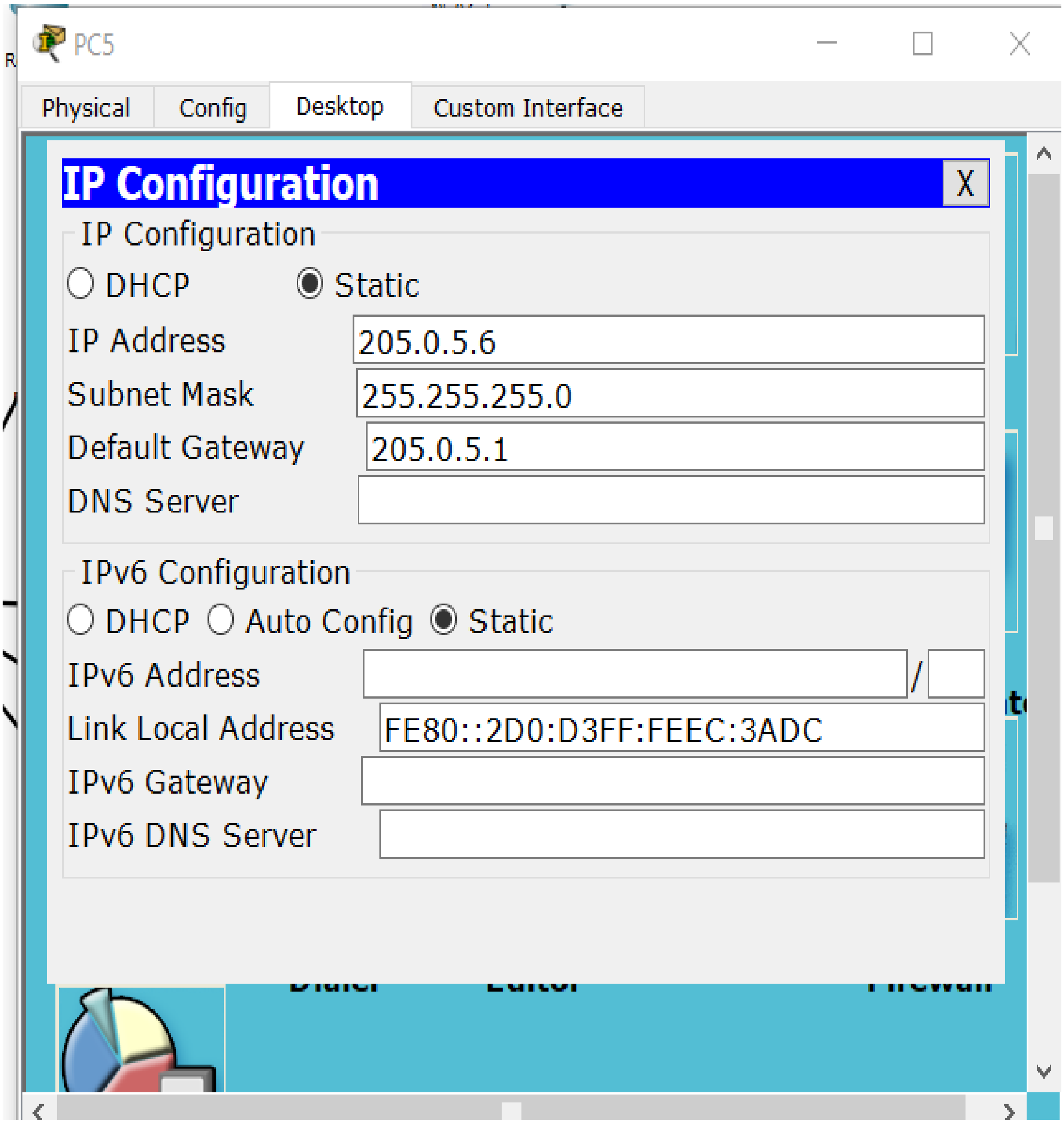
Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Ethernet1/0
Router(config-if)#
```

Figure 19.Router1-3

Moving to router 3 , its connected to a switch and the switch is connected with a PC , the PC IP is manually configured:



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address: 205.0.5.6

Subnet Mask: 255.255.255.0

Default Gateway: 205.0.5.1

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::2D0:D3FF:FEEC:3ADC

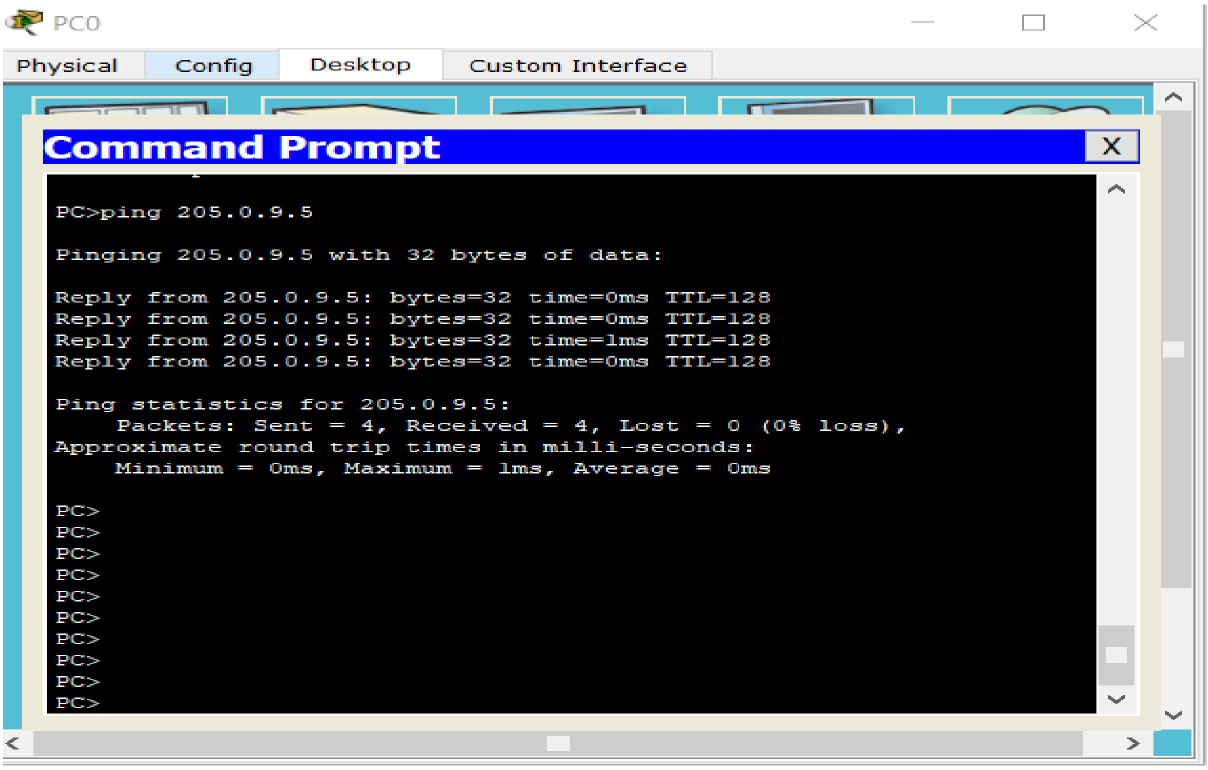
IPv6 Gateway:

IPv6 DNS Server:

Figure 20.PC5 IP

To test the reachability from PC0 to other components :

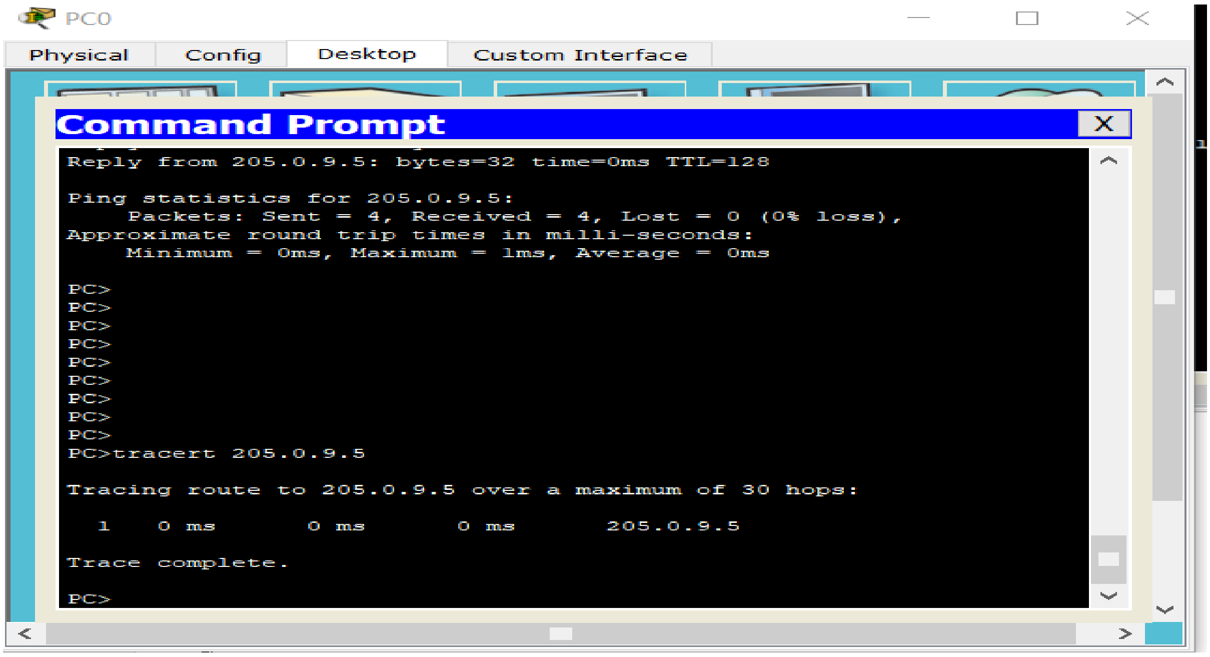
Pinging from PC0 to PC1:



```
PC>ping 205.0.9.5

Pinging 205.0.9.5 with 32 bytes of data:

Reply from 205.0.9.5: bytes=32 time=0ms TTL=128
Reply from 205.0.9.5: bytes=32 time=0ms TTL=128
Reply from 205.0.9.5: bytes=32 time=1ms TTL=128
Reply from 205.0.9.5: bytes=32 time=0ms TTL=128

Ping statistics for 205.0.9.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
```

Figure 21.Ping PC0-1

Tracert PC1:

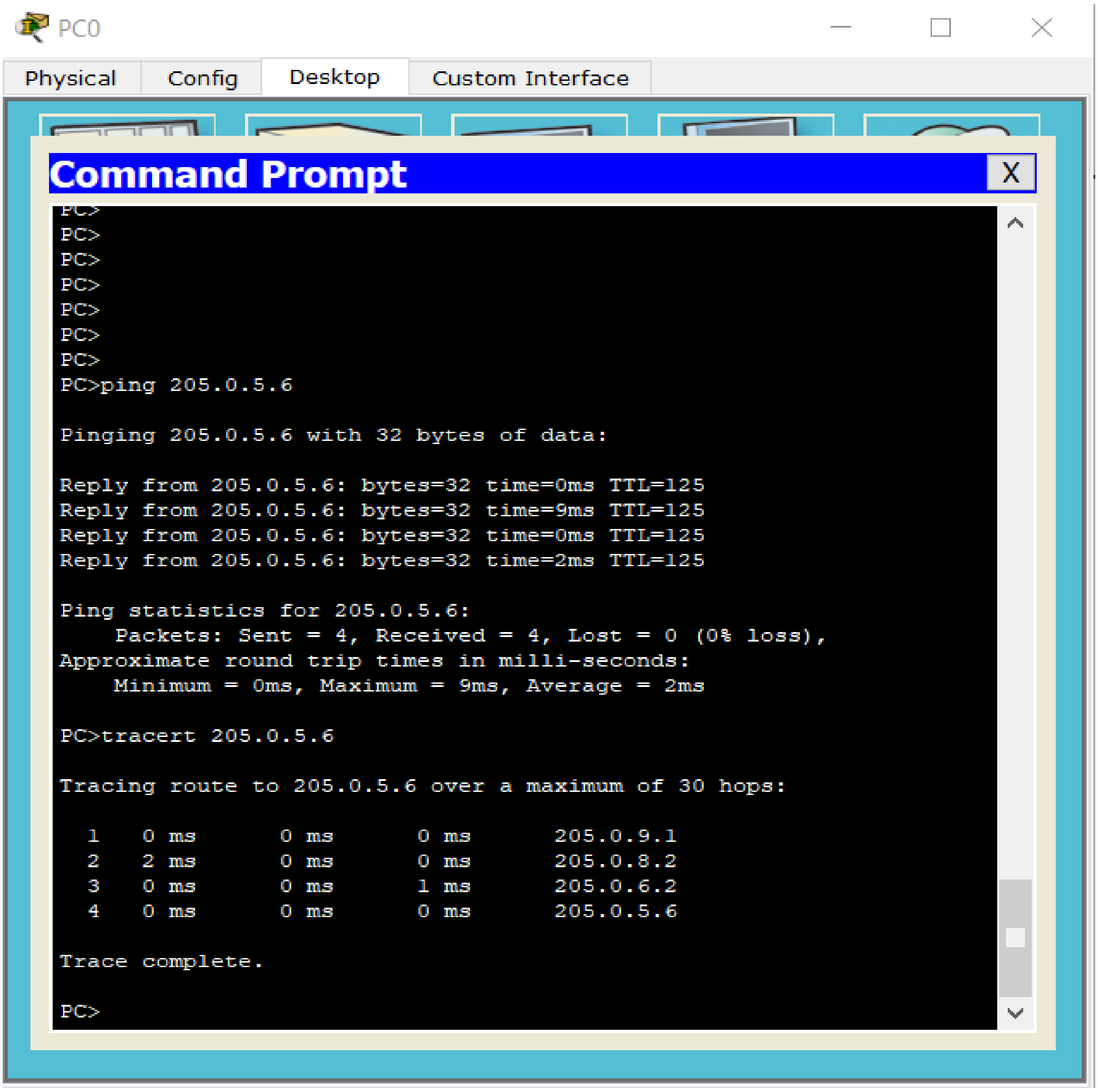


```
Reply from 205.0.9.5: bytes=32 time=0ms TTL=128

Ping statistics for 205.0.9.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>tracert 205.0.9.5

Tracing route to 205.0.9.5 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      205.0.9.5

Trace complete.

PC>
```

Figure 22.Tracert PC0-1

Other component within the switch0 will result the same.

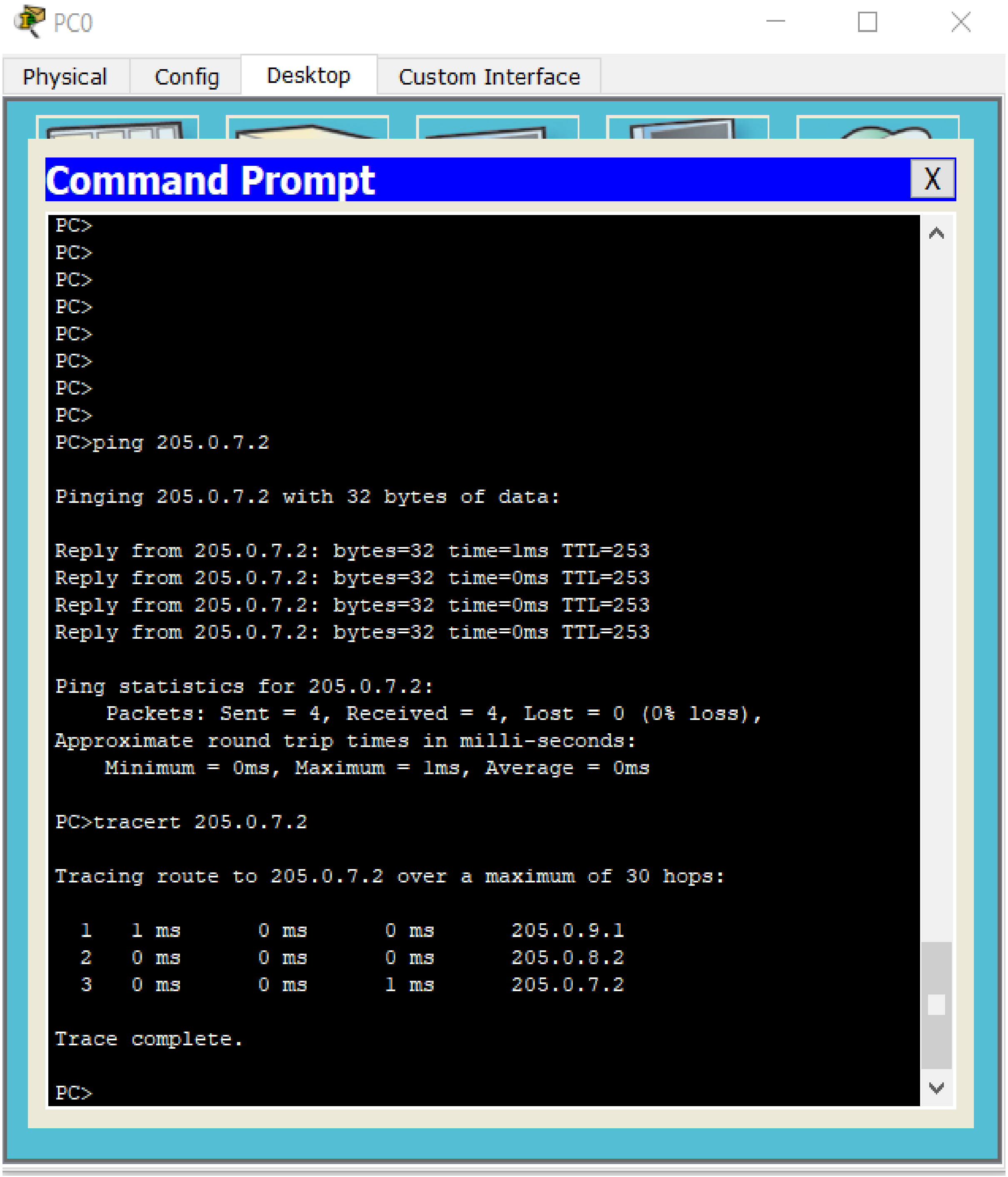
Pinging/tracert PC5:



```
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>ping 205.0.5.6

Pinging 205.0.5.6 with 32 bytes of data:

Reply from 205.0.5.6: bytes=32 time=0ms TTL=125
Reply from 205.0.5.6: bytes=32 time=9ms TTL=125
Reply from 205.0.5.6: bytes=32 time=0ms TTL=125
Reply from 205.0.5.6: bytes=32 time=2ms TTL=125

Ping statistics for 205.0.5.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms

PC>tracert 205.0.5.6

Tracing route to 205.0.5.6 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      205.0.9.1
  2   2 ms      0 ms      0 ms      205.0.8.2
  3   0 ms      0 ms      1 ms      205.0.6.2
  4   0 ms      0 ms      0 ms      205.0.5.6

Trace complete.

PC>
```

Figure 23.Ping/Tracert Pc0-1

Ping/Tracert Router3 :



```
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>ping 205.0.7.2

Pinging 205.0.7.2 with 32 bytes of data:

Reply from 205.0.7.2: bytes=32 time=1ms TTL=253
Reply from 205.0.7.2: bytes=32 time=0ms TTL=253
Reply from 205.0.7.2: bytes=32 time=0ms TTL=253
Reply from 205.0.7.2: bytes=32 time=0ms TTL=253

Ping statistics for 205.0.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>tracert 205.0.7.2

Tracing route to 205.0.7.2 over a maximum of 30 hops:

  1   1 ms      0 ms      0 ms      205.0.9.1
  2   0 ms      0 ms      0 ms      205.0.8.2
  3   0 ms      0 ms      1 ms      205.0.7.2

Trace complete.

PC>
```

Figure 24.Ping/Tracert PC0-Router3

About OSPF :

In Each Router , CLI , Some lines were written in configuration terminal:

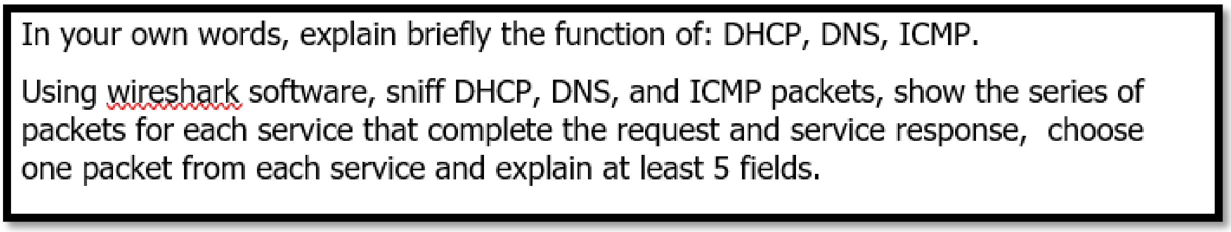
Router ospf 1

Network 0.0.0.0 255.255.255.255 area0

Which means :

- router OSPF 1: This command is used to enter the OSPF configuration mode and configure OSPF process number 1. The process number is an identifier for the OSPF process running on the router. It can be any number from 1 to 65535.
- network 0.0.0.0 255.255.255.255 area 0: This command is used to enable OSPF on specific networks. The network statement determines which networks will participate in OSPF and belong to a specific OSPF area. Which in our case is area 0.
- 0.0.0.0 255.255.255.255 is a wildcard mask that matches all possible IP addresses. This effectively means that OSPF will be enabled on all interfaces of the router.
- The area 0 parameter specifies that the participating networks belong to OSPF area 0. OSPF uses a hierarchical structure where routers are organized into areas. Area 0 (also known as the backbone area) is the central area that connects other areas in the OSPF network.
- By configuring network 0.0.0.0 255.255.255.255 area 0, OSPF will be enabled on all interfaces of the router, and the router will advertise its connected networks to other OSPF routers within area 0.
- This was done for Each router.

Part 1:



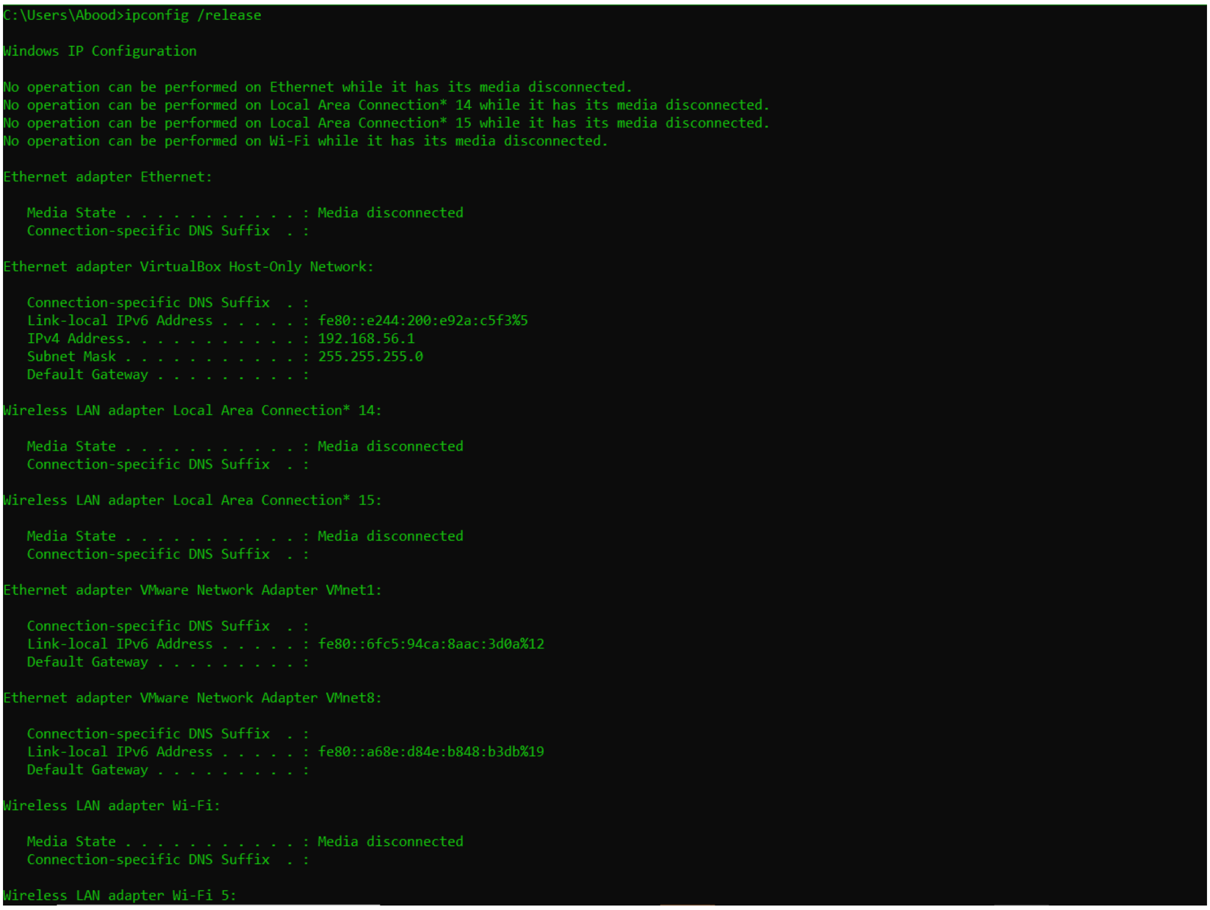
In your own words, explain briefly the function of: DHCP, DNS, ICMP.

Using wireshark software, sniff DHCP, DNS, and ICMP packets, show the series of packets for each service that complete the request and service response, choose one packet from each service and explain at least 5 fields.

Figure 25.Questin 1

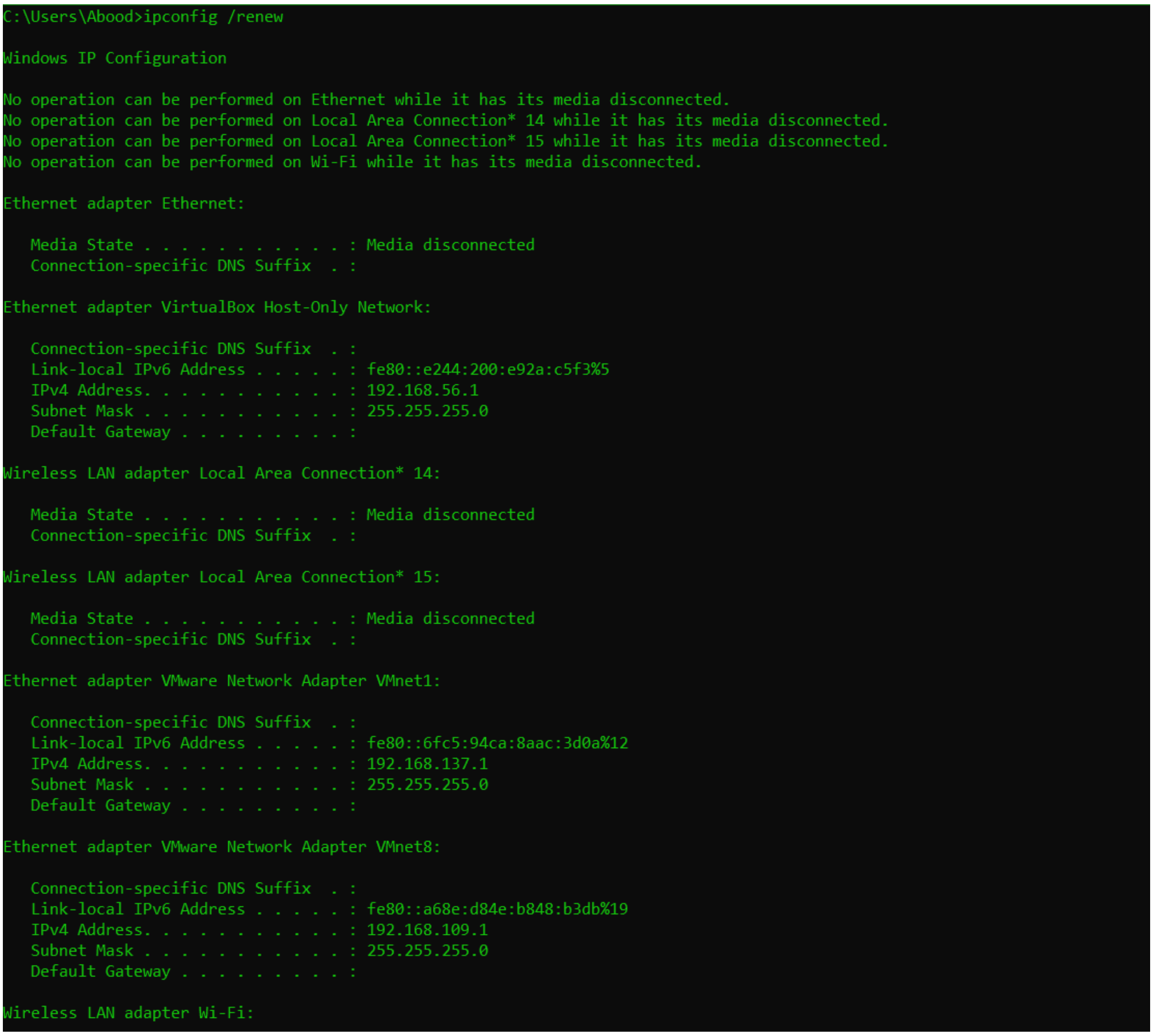
DHCP:(Dynamic Host Configuration Protocol): is a network protocol that simplifies network setup by automatically giving devices their own/unique Ip address , subnet mask, gateway and other settings instead of doing them manually.

To get DHCP, ipconfig/release , then ipconfig/renew



```
C:\Users\Abood>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* 14 while it has its media disconnected.
No operation can be performed on Local Area Connection* 15 while it has its media disconnected.
No operation can be performed on Wi-Fi while it has its media disconnected.

Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e244:200:e92a:c5f3%5
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 14:

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

Wireless LAN adapter Local Area Connection* 15:

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

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6fc5:94ca:8aac:3d0a%12
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a68e:d84e:b848:b3db%19
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

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

Wireless LAN adapter Wi-Fi 5:
```

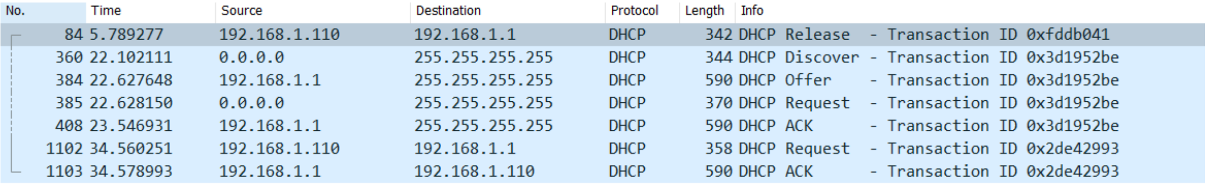
Figure 26. release ip



```
C:\Users\Abood>ipconfig /renew

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* 14 while it has its media disconnected.
No operation can be performed on Local Area Connection* 15 while it has its media disconnected.
No operation can be performed on Wi-Fi while it has its media disconnected.

Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e244:200:e92a:c5f3%5
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 14:

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

Wireless LAN adapter Local Area Connection* 15:

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

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6fc5:94ca:8aac:3d0a%12
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a68e:d84e:b848:b3db%19
   IPv4 Address. . . . . . . . . . . : 192.168.109.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:
```

Figure 27 renew ip

wire shark info:



```
No.   Time       Source          Destination      Protocol  Length Info
   84 5.789277   192.168.1.110   192.168.1.1      DHCP      342 DHCP Release  - Transaction ID 0xfddb041
  360 22.102111  0.0.0.0         255.255.255.255  DHCP      344 DHCP Discover - Transaction ID 0x3d1952be
  384 22.627648  192.168.1.1     255.255.255.255  DHCP      590 DHCP Offer    - Transaction ID 0x3d1952be
  385 22.628150  0.0.0.0         255.255.255.255  DHCP      370 DHCP Request  - Transaction ID 0x3d1952be
  408 23.546931  192.168.1.1     255.255.255.255  DHCP      590 DHCP ACK      - Transaction ID 0x3d1952be
 1102 34.560251  192.168.1.110   192.168.1.1      DHCP      358 DHCP Request  - Transaction ID 0x2de42993
 1103 34.578993  192.168.1.1     192.168.1.110    DHCP      590 DHCP ACK      - Transaction ID 0x2de42993
```

Figure 28.DHCP wireShark

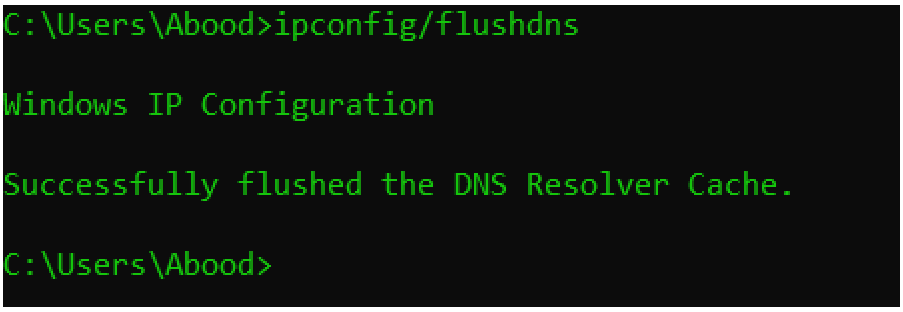
Release/discover/offer/request/ACK.

Packet Analysis for frame 84:

1. Frame Information:
    - Frame 84: Indicates that this is the 84th frame captured.
    - Frame Length: 342 bytes (2736 bits): Indicates the total length of the frame, including headers and payload.
    - Capture Length: 342 bytes (2736 bits): Indicates the length of the captured portion of the frame.
    - Protocols in frame: eth:ethertype:ip:udp:dhcp: Lists the protocols present in the frame, indicating the layered structure of the packet.
    - Ethernet II: Specifies the encapsulation type as Ethernet II (Ethernet version 2).
2. Ethernet Information:
    - Source: Tp-LinkT_00:10:82 (50:3e:aa:00:10:82): MAC address of the source device.
    - Destination: Tp-LinkT_26:21:21 (d8:07:b6:26:21:21): MAC address of the destination device.
    - Type: IPv4 (0x0800): Indicates the encapsulated protocol type as IPv4.
3. IPv4 Information:
    - Source: 192.168.1.110: IP address of the source device.
    - Destination: 192.168.1.1: IP address of the destination device.
    - Protocol: UDP (17): Indicates that the payload is using the UDP protocol.
    - Total Length: 328 bytes: Total length of the IPv4 packet, including headers and payload.
4. UDP Information:
    - Source Port: 68: UDP port number used by the source device.
    - Destination Port: 67: UDP port number used by the destination device.
    - Length: 308 bytes: Length of the UDP packet, including headers and payload.
    - Checksum: 0x3369 [unverified]: UDP checksum value.
5. DHCP Information:
    - Message type: Boot Request (1): Indicates that this is a DHCP release message.
    - Client IP address: 192.168.1.110: IP address of the DHCP client.
    - Your (client) IP address: 0.0.0.0: Client IP address is not assigned.
    - DHCP Server Identifier: 192.168.1.1: IP address of the DHCP server.

DNS:(Domain Name System): is a system that converts domain names (users interact with them ex; www.google.com) into IP addresses (computer interact with them ex; 205.0.9.7).

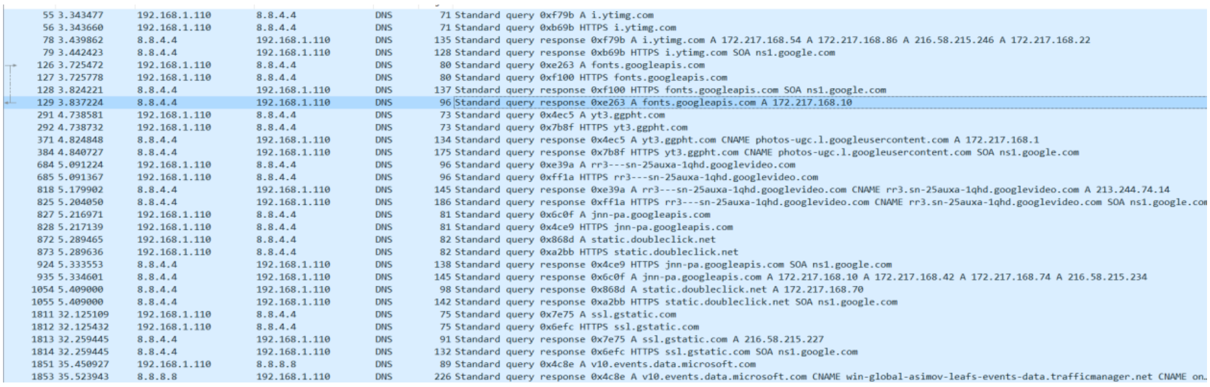
First we used ipconfig/Flushdns to flush dns's:



```
C:\Users\Abood>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Abood>
```

Figure 29.Flush DNS

What we get in wireshark, query response and other queries:



```
  55 3.343477   192.168.1.110  8.8.4.4        DNS   71 Standard query 0xf79b A i.ytimg.com
  56 3.343660   192.168.1.110  8.8.4.4        DNS   71 Standard query 0xb69b HTTPS i.ytimg.com
  78 3.439862   8.8.4.4        192.168.1.110  DNS  135 Standard query response 0xf79b A i.ytimg.com A 172.217.168.54 A 172.217.168.86 A 216.58.215.246 A 172.217.168.22
  79 3.442423   8.8.4.4        192.168.1.110  DNS  128 Standard query response 0xb69b HTTPS i.ytimg.com SOA ns1.google.com
 126 3.725472   192.168.1.110  8.8.4.4        DNS   80 Standard query 0xe263 A fonts.googleapis.com
 127 3.725778   192.168.1.110  8.8.4.4        DNS   80 Standard query 0xf100 HTTPS fonts.googleapis.com
 128 3.824221   8.8.4.4        192.168.1.110  DNS  137 Standard query response 0xf100 HTTPS fonts.googleapis.com SOA ns1.google.com
 129 3.837224   8.8.4.4        192.168.1.110  DNS   96 Standard query response 0xe263 A fonts.googleapis.com A 172.217.168.10
 291 4.738581   192.168.1.110  8.8.4.4        DNS   73 Standard query 0x4ec5 A yt3.ggpht.com
 292 4.738732   192.168.1.110  8.8.4.4        DNS   73 Standard query 0x7b8f HTTPS yt3.ggpht.com
 371 4.824848   8.8.4.4        192.168.1.110  DNS  134 Standard query response 0x4ec5 A yt3.ggpht.com CNAME photos-ugc.l.googleusercontent.com A 172.217.168.1
 384 4.840727   8.8.4.4        192.168.1.110  DNS  175 Standard query response 0x7b8f HTTPS yt3.ggpht.com CNAME photos-ugc.l.googleusercontent.com SOA ns1.google.com
 684 5.091224   192.168.1.110  8.8.4.4        DNS   96 Standard query 0xe39a A rr3---sn-25auxa-1qhd.googlevideo.com
 685 5.091367   192.168.1.110  8.8.4.4        DNS   96 Standard query 0xff1a HTTPS rr3---sn-25auxa-1qhd.googlevideo.com
 818 5.179902   8.8.4.4        192.168.1.110  DNS  145 Standard query response 0xe39a A rr3---sn-25auxa-1qhd.googlevideo.com CNAME rr3.sn-25auxa-1qhd.googlevideo.com A 213.244.74.14
 825 5.204050   8.8.4.4        192.168.1.110  DNS  186 Standard query response 0xff1a HTTPS rr3---sn-25auxa-1qhd.googlevideo.com CNAME rr3.sn-25auxa-1qhd.googlevideo.com SOA ns1.google.com
 827 5.216971   192.168.1.110  8.8.4.4        DNS   81 Standard query 0x6c0f A jnn-pa.googleapis.com
 828 5.217139   192.168.1.110  8.8.4.4        DNS   81 Standard query 0x4ce9 HTTPS jnn-pa.googleapis.com
 872 5.289465   192.168.1.110  8.8.4.4        DNS   82 Standard query 0x868d A static.doubleclick.net
 873 5.289636   192.168.1.110  8.8.4.4        DNS   82 Standard query 0xa2bb HTTPS static.doubleclick.net
 924 5.333553   8.8.4.4        192.168.1.110  DNS  138 Standard query response 0x4ce9 HTTPS jnn-pa.googleapis.com SOA ns1.google.com
 935 5.334601   8.8.4.4        192.168.1.110  DNS  145 Standard query response 0x6c0f A jnn-pa.googleapis.com A 172.217.168.10 A 172.217.168.42 A 172.217.168.74 A 216.58.215.234
1054 5.409000   8.8.4.4        192.168.1.110  DNS   98 Standard query response 0x868d A static.doubleclick.net A 172.217.168.70
1055 5.409000   8.8.4.4        192.168.1.110  DNS  142 Standard query response 0xa2bb HTTPS static.doubleclick.net SOA ns1.google.com
1811 32.125109  192.168.1.110  8.8.4.4        DNS   75 Standard query 0x7e75 A ssl.gstatic.com
1812 32.125432  192.168.1.110  8.8.4.4        DNS   75 Standard query 0x6efc HTTPS ssl.gstatic.com
1813 32.259445  8.8.4.4        192.168.1.110  DNS   91 Standard query response 0x7e75 A ssl.gstatic.com A 216.58.215.227
1814 32.259445  8.8.4.4        192.168.1.110  DNS  132 Standard query response 0x6efc HTTPS ssl.gstatic.com SOA ns1.google.com
1851 35.450927  192.168.1.110  8.8.8.8        DNS   89 Standard query 0x4c8e A v10.events.data.microsoft.com
1853 35.523943  8.8.8.8        192.168.1.110  DNS  226 Standard query response 0x4c8e A v10.events.data.microsoft.com CNAME win-global-asimov-leafs-events-data.trafficmanager.net CNAME on…
```

Figure 30.DNS WireShark

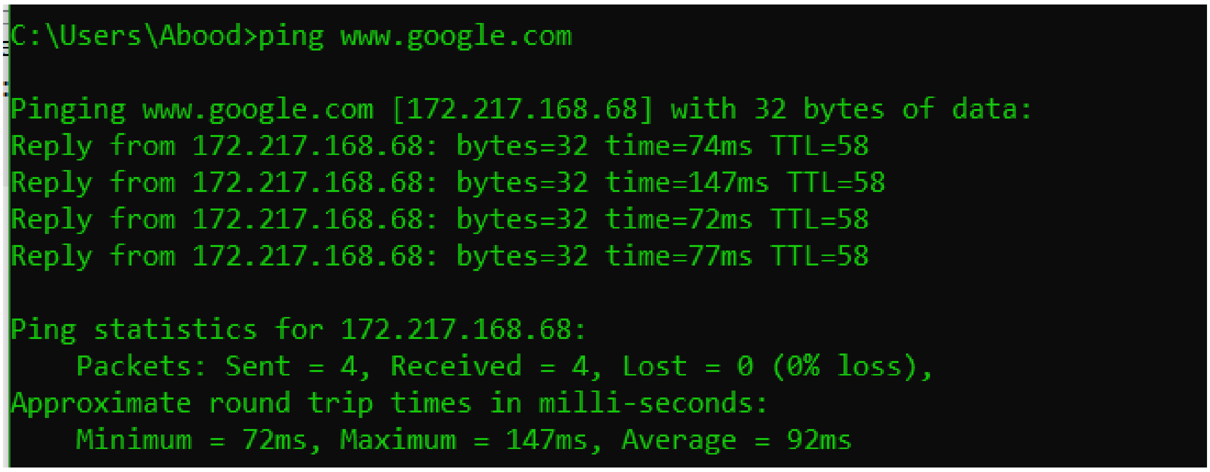
Packet Analysis frame(225):

1. Frame Information:Frame 225:
    - This is the 225th frame captured in the packet capture.
    - Frame Length: The length of the frame is 107 bytes (856 bits).
    - Capture Length: The captured length of the frame is also 107 bytes (856 bits).
    - Protocols in frame: The protocols observed in this frame are Ethernet, IP, UDP, and DNS.
2. Ethernet II:Source:
    - The MAC address of the source device is "d8:07:b6:26:21:21" (Tp-LinkT_26:21:21).
    - Destination: The MAC address of the destination device is "50:3e:aa:00:10:82" (Tp-LinkT_00:10:82).
    - Encapsulation type: Ethernet II.
3. Internet Protocol Version 4 (IPv4):
    - Source: The source IP address is "8.8.8.8".

- Destination: The destination IP address is "192.168.1.110".
- Version: IPv4 (Version 4).
- Header Length: The length of the IPv4 header is 20 bytes (5 words).
- Differentiated Services Field: DSCP (Differentiated Services Codepoint) is set to default.
- Total Length: The total length of the IP packet, including header and payload, is 93 bytes.
- Identification: The identification value is "0xc9d5" (51669).
- Flags: Various flags indicating fragmentation (none set in this case).
- Time to Live: The packet can exist on the network for 60 seconds before being discarded.
- Protocol: The IP packet carries a UDP payload (UDP protocol).
- Header Checksum: The checksum for the IP header is "0xe294" (validation disabled).

4. User Datagram Protocol (UDP):
    - Source Port: The source port is 53.
    - Destination Port: The destination port is 50345.
    - Length: The length of the UDP packet, including header and data, is 73 bytes.
    - Checksum: The checksum for the UDP packet is "0xdebc" (unverified).
5. UDP Payload:
    - Domain Name System (DNS) response.
    - Transaction ID: The ID associated with the DNS transaction is "0x5a11".
    - Flags: The DNS response indicates a standard query response with no error.
    - Questions: The number of questions in the DNS response is 1.
    - Answer RRs: The number of answer resource records in the DNS response is 1.
    - Authority RRs: The number of authority resource records in the DNS response is 0.
    - Additional RRs: The number of additional resource records in the DNS response is 0.
6. Queries:
    - Recursion desired: The sender wants the DNS server to perform recursive queries.
    - Recursion available: The DNS server can perform recursive queries.
7. Answers:
    - The DNS response contains an answer resource record.
    - Name: The name in the DNS response is "signaler-pa.clients6.google.com".
    - Type: The type of resource record is A (Host Address).
    - Class: The class of the resource record is IN (Internet).
    - Time to live: The DNS record can be cached for 72 seconds.
    - Data length: The length of the address data is 4 bytes.
    - Address: The IP address associated with the name is "172.217.168.10".

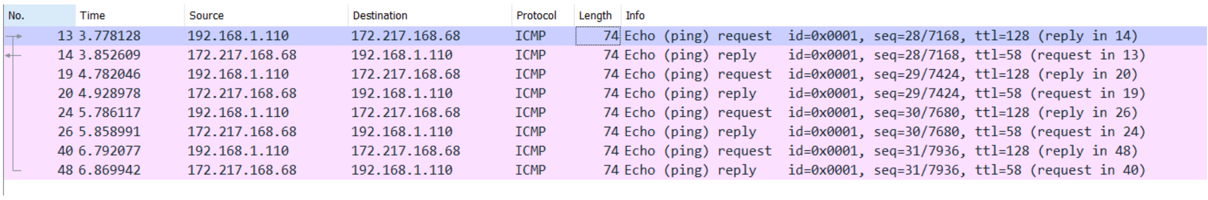
ICMP:(Internet Control Message Protocol): is a network protocol that handles error messages and network troubleshooting by helping devices to communicate and diagnose network issues.



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

Pinging www.google.com [172.217.168.68] with 32 bytes of data:
Reply from 172.217.168.68: bytes=32 time=74ms TTL=58
Reply from 172.217.168.68: bytes=32 time=147ms TTL=58
Reply from 172.217.168.68: bytes=32 time=72ms TTL=58
Reply from 172.217.168.68: bytes=32 time=77ms TTL=58

Ping statistics for 172.217.168.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 72ms, Maximum = 147ms, Average = 92ms
```

Figure 31.Ping Google

4 packets sent , 4 received , 4 requests / 4 replies:



No.	Time	Source	Destination	Protocol	Length	Info
13	3.778128	192.168.1.110	172.217.168.68	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (reply in 14)
14	3.852609	172.217.168.68	192.168.1.110	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=58 (request in 13)
19	4.782046	192.168.1.110	172.217.168.68	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128 (reply in 20)
20	4.928978	172.217.168.68	192.168.1.110	ICMP	74	Echo (ping) reply id=0x0001, seq=29/7424, ttl=58 (request in 19)
24	5.786117	192.168.1.110	172.217.168.68	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (reply in 26)
26	5.858991	172.217.168.68	192.168.1.110	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680, ttl=58 (request in 24)
40	6.792077	192.168.1.110	172.217.168.68	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (reply in 48)
48	6.869942	172.217.168.68	192.168.1.110	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=58 (request in 40)

Figure 32.ICMP WireShark

Packet analysis:

1. Section number: 1 This indicates the section of the packet capture where this frame is located.
2. Frame 75: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{5C297F94-B509-4EB5-9E68-3271DC4CC6D3}, id 0 This line provides information about the frame, including its number, size in bytes, and the interface on which it was captured.
3. Interface name: \Device\NPF_{5C297F94-B509-4EB5-9E68-3271DC4CC6D3} It specifies the name of the network interface from which the packet was captured.
4. Interface description: Wi-Fi 5 This line gives a description of the network interface.
5. Encapsulation type: Ethernet (1) It indicates that the packet is encapsulated within Ethernet frames.
6. Arrival Time: Jul 3, 2023 18:04:25.416195000 West Bank Gaza Daylight Time The timestamp when the packet was captured.
7. Epoch Time: 1688396665.416195000 seconds The timestamp in seconds since the Unix epoch.

8. Time delta from previous captured frame: 0.011502000 seconds The time difference between this packet and the previous captured packet.
9. Time delta from previous displayed frame: 0.000000000 seconds The time difference between this packet and the previous displayed packet.
10. Time since reference or first frame: 7.650424000 seconds The time elapsed since the start of the packet capture or reference frame.
11. Frame Number: 75 The number assigned to this frame in the packet capture sequence.
12. Frame Length: 74 bytes (592 bits) The total length of the frame, including both captured and wire length.
13. Capture Length: 74 bytes (592 bits) The length of the frame as captured.
14. Protocols in frame: eth:ethertype:ip:icmp:data The protocols encapsulated within the frame, listed in the order of encapsulation.
15. Coloring Rule Name: ICMP The name of the coloring rule applied to this frame.
16. Coloring Rule String: icmp || icmpv6 The criteria used by the coloring rule.
17. Ethernet II, Src: Tp-LinkT_00:10:82 (50:3e:aa: 00:10:82), Dst: Tp-LinkT_26:21:21 (d8:07:b6:26:21:21) Information about the Ethernet II header, including source and destination MAC addresses.
18. Internet Protocol Version 4, Src: 192.168.1.110, Dst: 172.217.168.68 Details about the IPv4 header, including source and destination IP addresses.
19. Internet Control Message Protocol Type: 8 (Echo (ping) request) Information about the ICMP packet, indicating that it is an Echo (ping) request.
20. Code: 0 The code associated with the ICMP packet.
21. Checksum: 0x4d38 [correct] The checksum value of the ICMP packet, indicating that it is correct.
22. Identifier (BE): 1 (0x0001) The identifier of the ICMP packet in big-endian format.
23. Identifier (LE): 256 (0x0100) The identifier of the ICMP packet in little-endian format.
24. Sequence Number (BE): 35 (0x0023) The sequence number of the ICMP packet in big-endian format.
25. Sequence Number (LE): 8960 (0x2300) [Response frame: 76] The sequence number of the ICMP packet in little-endian format, and a reference to the response frame.
26. Data (32 bytes) The payload data of the ICMP packet, represented in hexadecimal format.

Conclusion

This project delved into the functions of DHCP, DNS, and ICMP in computer networks. It utilized Wireshark to capture and analyze packets, showcasing the request and response processes for each service. By examining specific packet fields, the project explored their structure and significance. In addition, Packet Tracer was used to construct a network with routers, switches, and PCs, implementing OSPF routing and DHCP in one subnet. The project demonstrated network connectivity through ping and traced the path of packets using tracert. Overall, it provided a practical understanding of network protocols and tools, enhancing knowledge of computer networks.