



**Faculty of Engineering and Technology**  
**Electrical & Computer Engineering Department**  
**Computer networks ENCS3320**

**Project #2**

---

**Prepared by:**

**Name:** mahmoud nobani

**Id:**1180729

**Instructor:** Dr. Abdelkarim awad

**Section:** 1

**Date:**6/30/2023

## Part1:

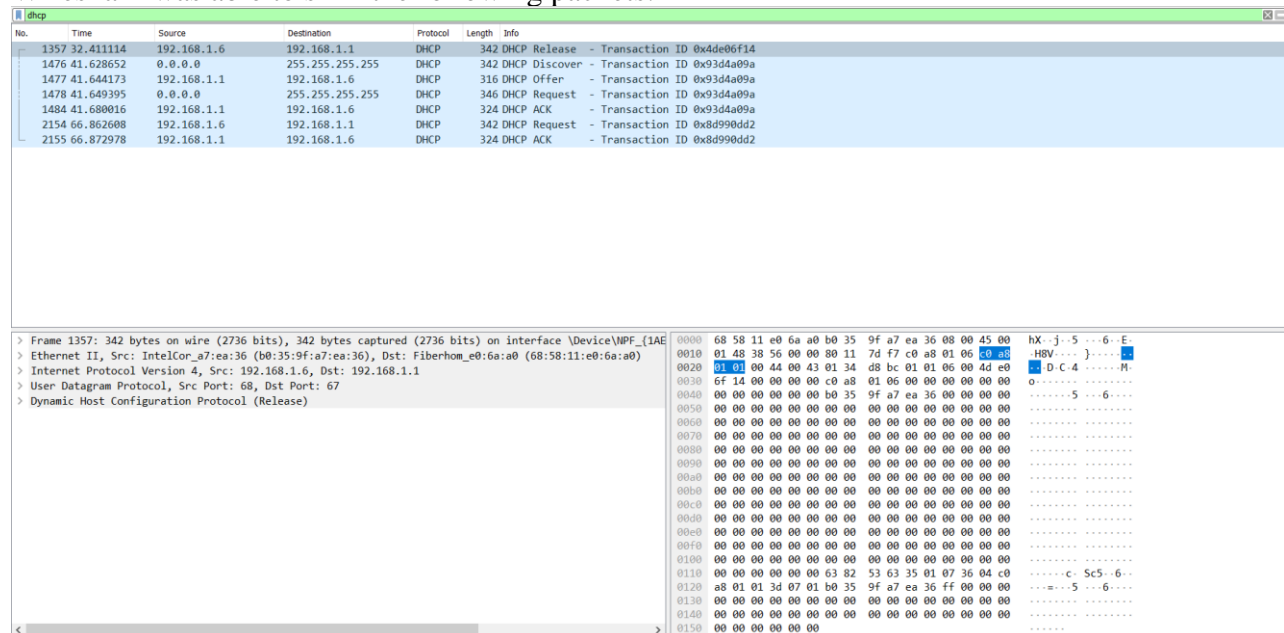
- DHCP (dynamic host configuration protocol): is a protocol that distributes IPs within a network, as when a device connects onto a network it asks an IP from the DHCP server and then DHCP assigns one to it, this whole procedure simplify the of IP assignment.
- DNS (Domain name system): it aims to map domain names into an IP machine can understand, thus allowing people to access website using easy to remember names instead of the machine IPs.
- ICMP (internet control message protocol): it's used for diagnoses and feedbacks as it provides networks a way to exchange control or error messages.

### 1) Sniffing DHCP packets:

First, we have to perform two commands on the CMD which are:

- Ipconfig /release: which release the current IP address from the network
- Ipconfig /renew: which request a new IP address from the DHCP server.

Wireshark was able to sniff the following packets:



No.	Time	Source	Destination	Protocol	Length	Info
1357	32.411114	192.168.1.6	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x4de06f14
1476	41.628652	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x93d4a09a
1477	41.644173	192.168.1.1	192.168.1.6	DHCP	316	DHCP Offer - Transaction ID 0x93d4a09a
1478	41.649395	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x93d4a09a
1484	41.680016	192.168.1.1	192.168.1.6	DHCP	324	DHCP ACK - Transaction ID 0x93d4a09a
2154	66.862608	192.168.1.6	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x8d990dd2
2155	66.872978	192.168.1.1	192.168.1.6	DHCP	324	DHCP ACK - Transaction ID 0x8d990dd2

Frame 1357: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF{1AE...}	0000	68 58 11 e0 6a a0 b0 35 9f a7 ea 36 00 00 45 00	hX - j - 5 - - 6 - E -
Ethernet II, Src: IntelCor_a7:ea:36 (b0:35:9f:a7:ea:36), Dst: Fiberhom_e0:6a:a0 (68:58:11:e0:6a:a0)	0010	01 48 38 56 00 00 80 11 7d f7 c0 a8 01 06 00 a0	.HBV... }... 5 -
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.1	0020	01 01 00 44 00 43 01 34 d8 bc 01 01 06 00 4d e0	.D C 4 ...M-
User Datagram Protocol, Src Port: 68, Dst Port: 67	0030	6f 14 00 00 00 00 c0 a8 01 06 00 00 00 00 00	o...5...6...
Dynamic Host Configuration Protocol (Release)	0040	00 00 00 00 00 00 b0 35 9f a7 ea 36 00 00 00 00	.....5...6....
	0050	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	.....
	0070	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	.....
	0090	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	.....
	00b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	00c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	00d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	00e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	00f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	0100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	0110	00 00 00 00 00 00 63 82 53 63 35 01 07 36 04 c0	.....c-Sc5-6-
	0120	a8 01 01 3d 07 01 b0 35 9f a7 ea 36 ff 00 00 00	.....5...6...
	0130	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	0140	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	0150	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

Figure 1: sniff DHCP.

As we can see we have 7 packets but the most notable ones are the first one (DHCP release) and the 4 and 6 ones (DHCP request) in which the IP address was given.

Looking at the first packet more, we can see that we have the following info about it:

The source: 192.168.1.6 which is my IP

The destination: 192.168.1.1 which is the DHCP IP

The length: 342 which is the number of bits on the datagram message shown

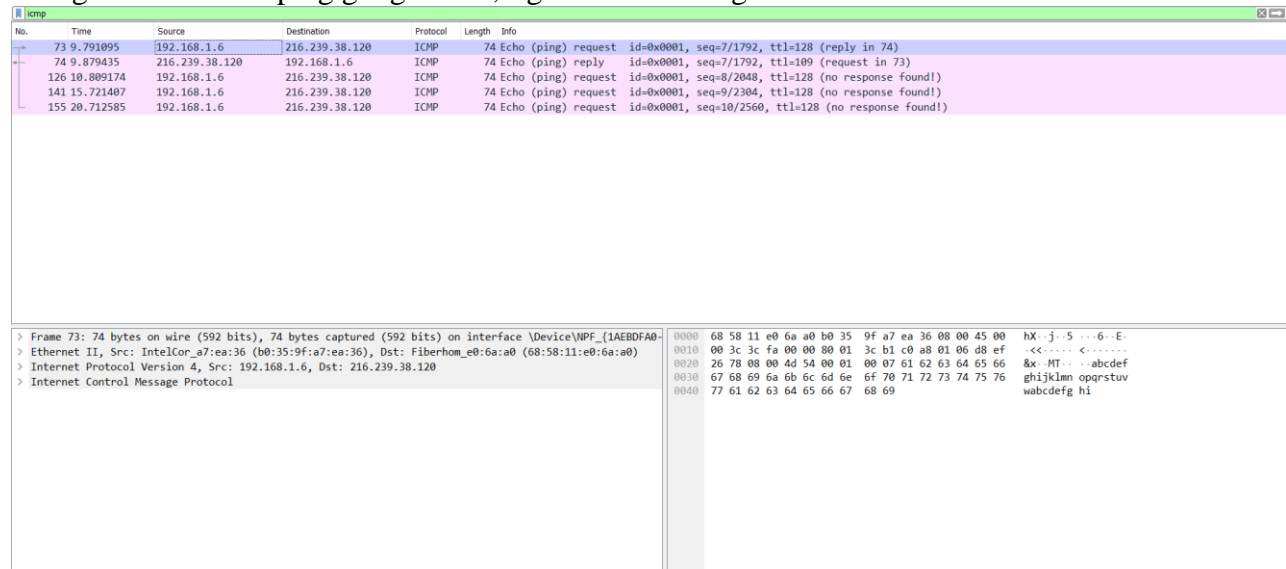
Protocol: which is the protocol used (DHCP)

Info: which specify the type of command

Another interesting property we can point out is the User Datagram protocol (UDP) source port 68 and destination 67 as DHCP uses the UDP protocol.

## 2) Sniffing ICMP:

Using the command `ping google.com`, I got the following result:



The image shows a Wireshark packet capture of ICMP traffic. The top pane displays a list of five packets. The bottom pane shows the details of the selected packet (No. 73), including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol fields. The packet data is also visible in the bottom pane.

No.	Time	Source	Destination	Protocol	Length	Info
73	9.791895	192.168.1.6	216.239.38.120	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 74)
74	9.879435	216.239.38.120	192.168.1.6	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=109 (request in 73)
126	10.809174	192.168.1.6	216.239.38.120	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (no response found!)
141	15.721407	192.168.1.6	216.239.38.120	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (no response found!)
155	20.712585	192.168.1.6	216.239.38.120	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (no response found!)

Frame 73: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{1AEBDAF0-0000-0000-0000-000000000000} interface 0  
> Ethernet II, Src: IntelCor\_a7:ea:36 (b0:35:9f:a7:ea:36), Dst: Fiberhom\_e0:6a:a0 (68:58:11:e0:6a:a0)  
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 216.239.38.120  
> Internet Control Message Protocol

0000 68 58 11 e0 6a a0 b0 35 9f a7 ea 36 08 00 45 00 hX..j..5...6..E-  
0010 00 3c 3c fa 00 00 80 01 3c b1 c0 a8 01 06 d8 ef -<.....<.....  
0020 26 78 08 00 4d 54 00 01 00 07 61 62 63 64 65 66 &x..MT.. ..abcdef  
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 wabdefgh i

Figure 2: sniff ICMP.

As we can see, we have 5 packets, the 4 request ping commands usually make, and only one replay, now if we look as the CMD output:

```
C:\Users\totim>ping google.com

Pinging forcesafesearch.google.com [216.239.38.120] with 32 bytes of data:
Reply from 216.239.38.120: bytes=32 time=88ms TTL=109
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 216.239.38.120:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 88ms, Maximum = 88ms, Average = 88ms
```

Figure 3: ping google.com

We can see that three requests were timed out; thus, it makes sense to have only 5 packets. Now going back to figure 2, lets analyze the first packet more, as it has some interesting fields: The most notable ones are:

Source: 192.168.1.6 which is my IP

Destination: 216.239.38.210 which is google.com IP address

The length was 74 and protocol used is IMCP, with the info specifying the command as request.

### 3) Sniffing DNS:

To sniff DNS, we used nslookup google.com and got the result below:

No.	Time	Source	Destination	Protocol	Length	Info
27	7.273260	192.168.1.1	192.168.1.6	DNS	84	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa
28	7.280912	192.168.1.6	192.168.1.1	DNS	70	Standard query 0x0002 A google.com
29	7.287300	192.168.1.1	192.168.1.6	DNS	189	Standard query response 0x0002 A google.com CNAME forcesafesearch.google.com A 216.239.38.120 SOA opnsense.localdomain
30	7.294072	192.168.1.6	192.168.1.1	DNS	70	Standard query 0x0003 AAAA google.com
31	7.299611	192.168.1.1	192.168.1.6	DNS	138	Standard query response 0x0003 AAAA google.com CNAME forcesafesearch.google.com AAAA 2001:4860:4802:32::78
38	11.010071	192.168.1.6	192.168.1.1	DNS	78	Standard query 0x224f A www.googleapis.com

> Frame 29: 189 bytes on wire (1512 bits), 189 bytes captured (1512 bits) on interface \Device\NPF_{1AEBD...}	0000	b0 35 9f a7 ea 36 68 58 11 e0 6a a0 08 00 45 00	5...6hX...j...E-
> Ethernet II, Src: Fiberhom_e0:6a:a0 (68:58:11:e0:6a:a0), Dst: IntelCor_a7:ea:36 (b0:35:9f:a7:ea:36)	0010	00 af e1 8b 40 00 40 11 d5 5a c0 a8 01 01 c0 a8	...@...Z.....
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.6	0020	01 06 20 35 c9 96 00 9b ff cd 00 02 81 80 00 01	...[... ..
> User Datagram Protocol, Src Port: 53, Dst Port: 51606	0030	00 02 00 00 00 01 06 67 6f 6f 67 6c 65 03 63 6f	.....g oogle.co
> Domain Name System (response)	0040	6d 00 00 01 00 01 c0 0c 00 05 00 01 00 00 00 05	m.....
	0050	00 12 0f 66 6f 72 63 65 73 61 66 65 73 65 61 72	...-force safesean
	0060	63 68 c0 0c c0 28 00 01 00 01 00 00 28 11 00 04	ch...(-...(-...
	0070	d8 ef 26 78 06 67 6f 6f 67 6c 65 00 00 06 00 01	...&x goo gle....
	0080	00 00 00 01 00 37 08 6f 70 6e 73 65 6e 73 65 0b	.....7-o pnsense-
	0090	6c 6f 63 61 6c 64 6f 6d 61 69 6e 00 0a 68 6f 73	localdom ain--hos
	00a0	74 6d 61 73 74 65 72 c0 5c 78 49 ef a9 00 00 70	tmaster- \xI....p
	00b0	80 00 00 1c 20 00 0d 2f 00 00 00 0e 10	....../.....

Figure 4:sniff DNS

```
C:\Users\totim>nslookup google.com
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name: forcesafesearch.google.com
Addresses: 2001:4860:4802:32::78
           216.239.38.120
Aliases: google.com
```

Figure 5: nslookup google.com

Now looking at figure one, the most interesting packet for me is the third, first it has the typical stuff a source of 192.168.1.1 which is the home IP, as it sends to my IP the destination IP 192.168.1.6, and info of:

“Standard query response 0x0002 A google.com CNAME forcesafesearch.google.com A 216.239.38.120 SOA opnsense.localdomain”

The info field has CNAME record, which has the alias and the canonical name.

Other fields are the protocol field (DNS) and length field (189)

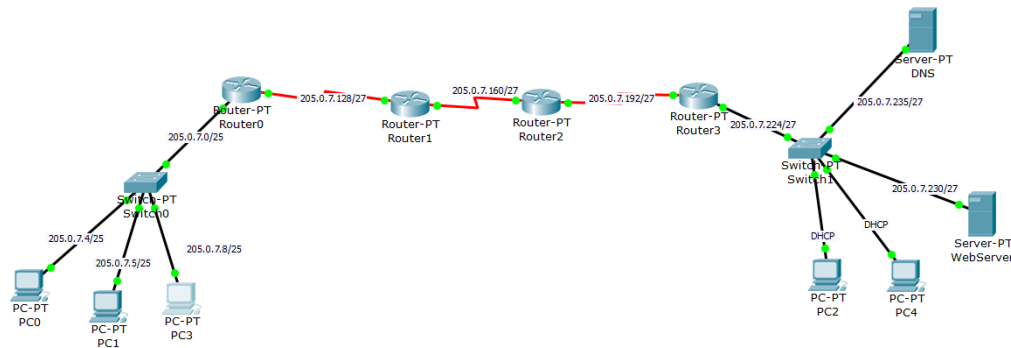
Another interesting thing I want to point out, is that a udp protocol is being used with a src port of 53 (the dns default port) as shown in the figure.

## **Part2:**

In this part we will use cisco packet tracer to build a network that contains 4 routers, 2 switches, 5 PCs, a **webserver**, And **DNS server**, at least one subnet will use DHCP.

To connect the different networks/subnets together, OSPF routing algorithm will be used,  
For my network the IP address will be 205.0.7.0000 0000/24

The following figure is a representation of the whole network and its components:



**Figure 6: the network with its own components.**

Figure 6, shows all the component with their IPs, so now I will show you how we get to there. First, we had a network IP of 205.0.7.0/24, our network has 5 subnets, and the closest number of subnet bits to represent is 3 (with 8 subnets) so I combined the first four and left the last four as they are, and got the following result:

- **First subnet:**  
Subnet: 205.0.7.0/25  
Subnet mask: 255.255.255.128
- **Second subnet**  
Subnet: 205.0.7.128/27  
Subnet mask: 255.255.255.224
- **Third subnet**  
Subnet: 205.0.7.160/27  
Subnet mask: 255.255.255.224
- **Fourth subnet**  
Subnet: 205.0.7.192/27  
Subnet mask: 255.255.255.224
- **Fifth subnet**  
Subnet: 205.0.7.224/27  
Subnet mask: 255.255.255.224

After calculating the 5 subnets, the following configuration we applied to each router:

Connected Element	Connection Type	IP/subnet mask
Router 0	Fast Ethernet 0/0	205.0.7.1/255.255.255.128
	Serial 2/0	205.0.7.129/255.255.255.244
Router 1	Serial 2/0	205.0.7.130/255.255.255.244
	Serial 3/0	205.0.7.161/255.255.255.224
Router 2	Serial 2/0	205.0.7.193/255.255.255.224
	Serial 3/0	205.0.7.162/255.255.255.224
Router 3	Fast Ethernet 0/0	205.0.7.225/255.255.255.224
	Serial 2/0	205.0.7.194/255.255.255.224

**Table 1: routers configurations**

Where Fast Ethernet 0/0 represent the ethernet connection to a device (used with LAN)

And Serial 2/0 represents the serial connection to a device (used with WAN)

And Serial 3/0 same as above, but with another device.

After these configurations were set, an IP of 205.0.7.4 was given to PC0, and using it we ping router 0:

```
PC>ping 205.0.7.1

Pinging 205.0.7.1 with 32 bytes of data:

Reply from 205.0.7.1: bytes=32 time=1ms TTL=255
Reply from 205.0.7.1: bytes=32 time=0ms TTL=255
Reply from 205.0.7.1: bytes=32 time=1ms TTL=255
Reply from 205.0.7.1: bytes=32 time=0ms TTL=255

Ping statistics for 205.0.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

**Figure 7: PING with PC0 to router 0**

Everything is working fine, now we will try to ping router 3:

```
Pinging 205.0.7.192 with 32 bytes of data:

Reply from 205.0.7.1: Destination host unreachable.
Reply from 205.0.7.1: Destination host unreachable.
Reply from 205.0.7.1: Destination host unreachable.
Reply from 205.0.7.1: Destination host unreachable.

Ping statistics for 205.0.7.192:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 8: PING with PC0 to router 3 fail

As we can see, we can't reach it as we don't have a routing algorithm, so we will use OSPF (Open Shortest Path First) which is a link-state routing protocol used in computer networks. It determines the shortest path for data packets to travel through an IP network by exchanging routing information among routers and calculating the best routes based on metrics like bandwidth and delay.

To configure OSPF, these commands has to be put on the CLI of each Router,

Router # conf //to enter configure terminal
---

Router (config) # router ospf 1 #to start OSPF configuration
--

Router (config-router) # network ip wildcard (complement of mask) area 0
--

And so on
-----------

so, for example in Router 2:

Router # conf //to enter configure terminal
---

Router (config) # router ospf 1 #to start OSPF configuration
--

Router (config-router) # network 205.0.7.160 0.0.0.31 area 0
--

Router (config-router) # network 205.0.7.192 0.0.0.31 area 0
--

After OSPF was set, pinging with PC0 to route 3 was successful as shown:

The screenshot shows a PC0 window with a Command Prompt open. The prompt displays the results of a ping command to 205.0.7.192. The output shows four successful replies from 205.0.7.162 with varying times (3ms, 2ms, 2ms, 2ms) and TTL=253. The ping statistics for 205.0.7.192 show 4 packets sent, 4 received, and 0% loss, with an average round trip time of 2ms.

```
PC0
Physical Config Desktop Custom Interface
Command Prompt
Reply from 205.0.7.1: bytes=32 time=1ms TTL=255
Reply from 205.0.7.1: bytes=32 time=0ms TTL=255
Reply from 205.0.7.1: bytes=32 time=1ms TTL=255
Reply from 205.0.7.1: bytes=32 time=0ms TTL=255

Ping statistics for 205.0.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 205.0.7.192

Pinging 205.0.7.192 with 32 bytes of data:

Reply from 205.0.7.162: bytes=32 time=3ms TTL=253
Reply from 205.0.7.162: bytes=32 time=2ms TTL=253
Reply from 205.0.7.162: bytes=32 time=2ms TTL=253
Reply from 205.0.7.162: bytes=32 time=2ms TTL=253

Ping statistics for 205.0.7.192:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

PC>
```

Figure 9: PING with PC0 to router 3 success.

After we added 2 extra PC to 205.0.7.0 connection.

Then add DNS server to 205.0.7.224 connection with IP 205.0.7.235

Then a web server was added to 205.0.7.224, with IP of 205.0.7.230 and it was registered to the DNS server as shown:

**DNS**

---

**DNS Service**    ☒ On    ☐ Off

---

**Resource Records**

Name     Type **A Record** ▼

---

Address

No.	Name	Type	Detail
0	www.web.com	A Record	205.0.7.230

Figure 10: adding web server to DNS

Before adding the last two PC to 205.0.7.224, I want to enable DHCP, to do that we did the following:

```
Router(config)#  
Router(config)#ip dhcp pool MY_LAN  
Router(dhcp-config)#network 205.0.7.224 255.255.255.224  
Router(dhcp-config)#default-router 205.0.7.225  
Router(dhcp-config)#dns-server 205.0.7.235
```

After adding DHCP to the subnet, we requested an IP for the last two PC as shown:

PC4

Physical    Config    Desktop    Custom Interface

**IP Configuration**

IP Configuration  
☒ DHCP    ☐ Static

IP Address    205.0.7.228  
Subnet Mask    255.255.255.224  
Default Gateway    205.0.7.225  
DNS Server    205.0.7.235

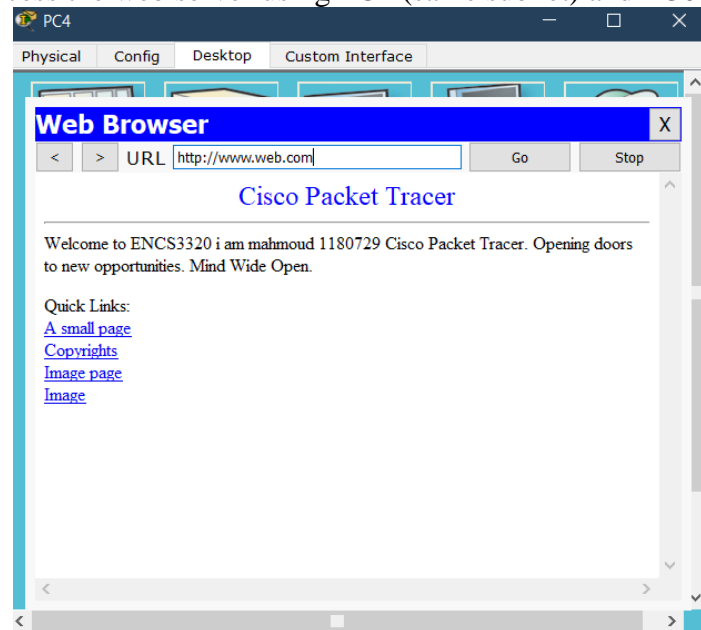
IPv6 Configuration  
☐ DHCP    ☐ Auto Config    ☒ Static

IPv6 Address      
Link Local Address    FE80::205:5EFF:FEDD:80D1  
IPv6 Gateway      
IPv6 DNS Server   

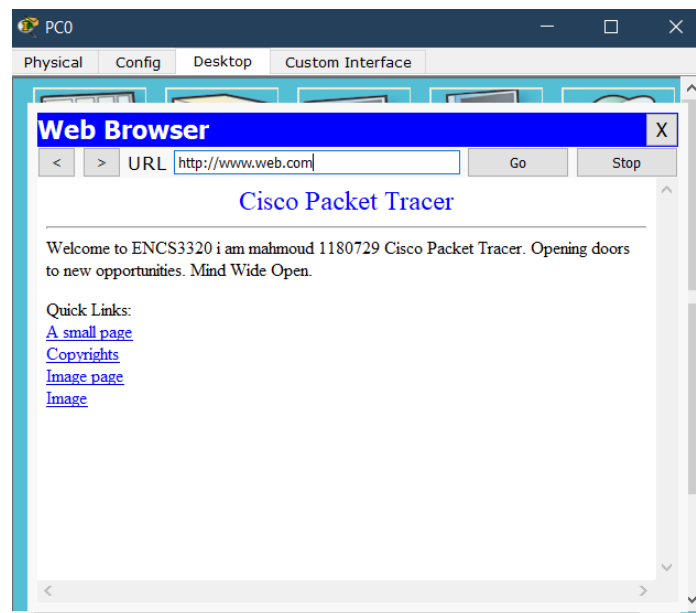
Figure 11: IP requesting for PC4



Now we will try to access the web server using PC4 (same subnet) and PC0 (another subnet):



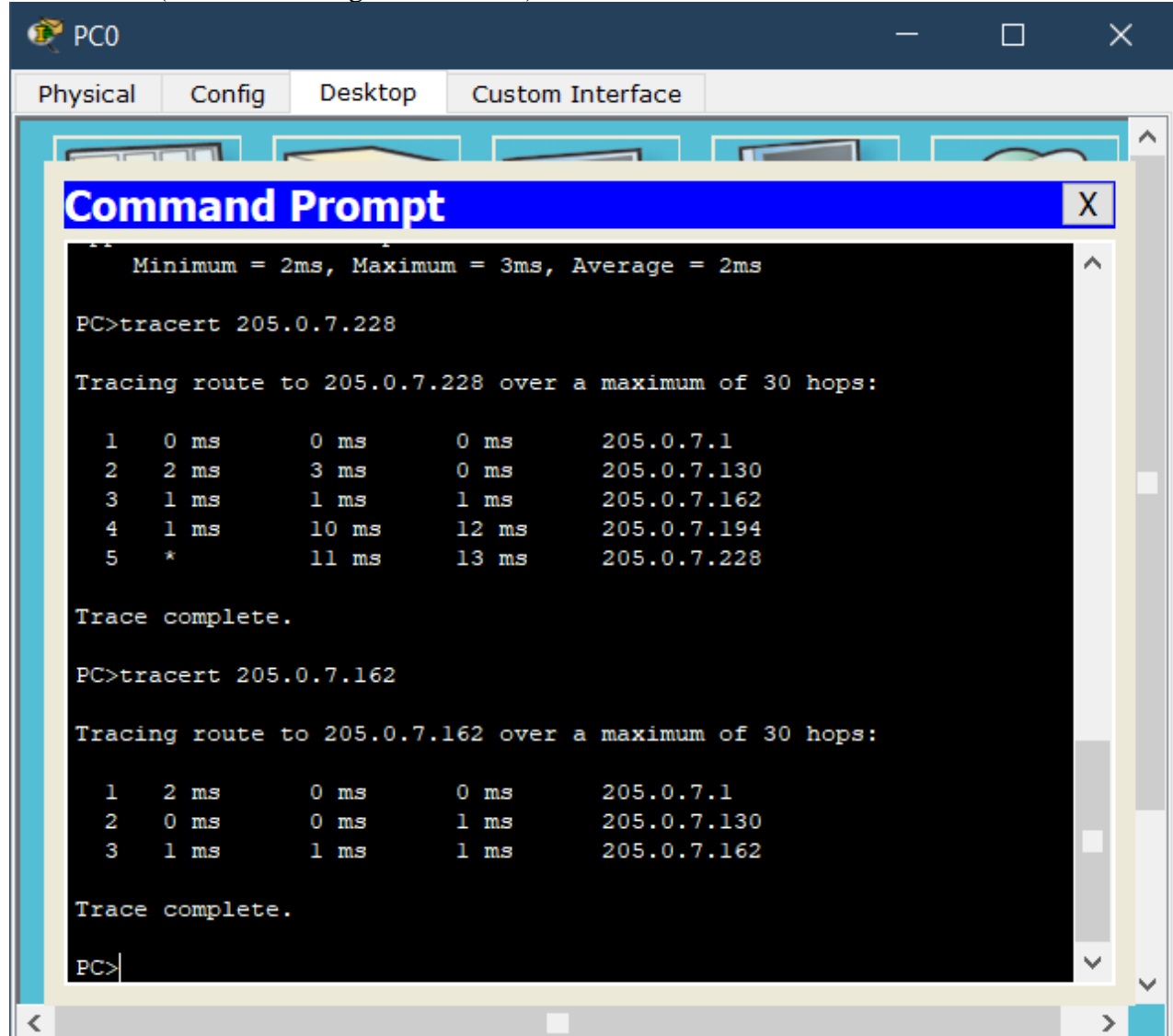
**Figure 12: access web server from PC4**



**Figure 13: access web server PC0**

We can see that it was successful for both, although PC0 took more time (expected)  
NOTE: don't forget to add DNS to PC0.

Lastly let's use tracert command to check the reachability from PC0 to PC4 and from PC0 to 205.0.7.162 (router 2 from right side subnet).



The screenshot shows a Packet Tracer PC0 interface with a Command Prompt window open. The Command Prompt displays the results of two tracert commands. The first command is 'tracert 205.0.7.228', which shows a path of 5 hops. The second command is 'tracert 205.0.7.162', which shows a path of 3 hops. The Command Prompt window has a blue title bar with the text 'Command Prompt' and a close button (X). The background of the PC0 interface shows a network diagram with various devices and connections.

```
Minimum = 2ms, Maximum = 3ms, Average = 2ms

PC>tracert 205.0.7.228

Tracing route to 205.0.7.228 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    205.0.7.1
  2  2 ms    3 ms    0 ms    205.0.7.130
  3  1 ms    1 ms    1 ms    205.0.7.162
  4  1 ms    10 ms   12 ms   205.0.7.194
  5  *        11 ms   13 ms   205.0.7.228

Trace complete.

PC>tracert 205.0.7.162

Tracing route to 205.0.7.162 over a maximum of 30 hops:

  1  2 ms    0 ms    0 ms    205.0.7.1
  2  0 ms    0 ms    1 ms    205.0.7.130
  3  1 ms    1 ms    1 ms    205.0.7.162

Trace complete.

PC>
```

Figure 14: Tracert.

As we can see, packet needed to go through all subnets to reach PC4, but only 3 which is true to our design.